Proposta nº 830929

Ligue para H2020-SU-ICT-03-2018

Início do projeto: 1º de fevereiro de 2019

Duração do projeto: 47 meses

Cyber Security for Europe

—

D4.7

Roteiro do Horizonte Futuro

Identificação do Documento	
Data de vencimento	30 de novembro de 2022
Data de envio 30 de novembro de 2022	
Revisão	2

WP **WP4 relacionado**		**Disseminação Nível**	**PU**
Liderar Participante	**ADIANTE**	**Autor principal**	**Evangelos Markatos (ADIANTE)**
ADIANTE, KAU, KUL, NTNU, POLITO,	**FRENTE, KAU, KUL, NTNU, POLITO, TDL, UCY, UM, UMA, UMU, UPRC, UPS-IRIT**	**Relacionado Entregáveis**	**D4.1-D4.6**

Resumo: Depois de realizar investigação durante quase quatro anos, o projeto CyberSec4Europe criou um "Roteiro do Horizonte Futuro" que lista as prioridades de investigação importantes que devem ser exploradas no futuro. Para cada prioridade de investigação, o resultado enumera lacunas específicas de investigação e exemplos de problemas que precisam de ser abordados.

Este documento é emitido no âmbito do projeto CyberSec4Europe. Este projeto recebeu financiamento do Programa Horizonte 2020 da União Europeia ao abrigo do acordo de subvenção nº. 830929. Este documento e o seu conteúdo são propriedade do Consórcio CyberSec4Europe.

Sumário executivo

Ao longo do último ano do projeto CyberSec4Europe, os beneficiários do projeto, tendo em conta os contributos dos associados do projeto e de peritos externos, formularam uma série de direções de investigação que serão importantes para o futuro. Essas instruções incluem:

- **Privacidade e anonimato •**
- **Tecnologias emergentes: metaversos, IoT, aprendizado de máquina, etc. •**
- **Novas abordagens para autenticação: além de senhas, biometria, etc. • Defesas**
- **"por design": desenvolvimento de software, modelagem de ameaças, etc.**
- **comunicações seguras, testes, execução confiável, etc.**

Para cada direção foram definidas uma série de prioridades de pesquisa. Essas prioridades incluem:

- **Fornecer comunicação anônima forte em larga escala • Construir**
- **metaversos confiáveis • Melhorar**
- **métodos de autenticação sem senha • Desenvolver**
- **abordagens de detecção precoce para malware blindado • Fornecer**
- **privacidade em ambientes de IoT • Realizar**
- **modelos de aprendizado de máquina que permaneçam seguros sob diferentes cenários adversários •**
- **Garantir que dados críticos infraestruturas são resilientes a ataques**
- **cibernéticos • Apoiar testes "by-design" e abordagens de certificação integrando abordagens industriais, sociais e valores éticos, sustentabilidade e necessidades de confiabilidade**

Grandes Desafios

Embora os projectos de curto prazo possam ter um impacto imediato no mercado, esse impacto é geralmente incremental e pode não ser duradouro, uma vez que se concentra num problema imediato que pode não ser tão relevante, digamos, cinco a dez anos depois. estrada. Para fazer avanços fundamentais na área da segurança cibernética, propusemos vários problemas de "Grande Desafio" de longo prazo. Para selecionar um pequeno número de "Grandes Desafios", os membros do Grupo de Trabalho, juntamente com os membros do círculo eleitoral mais amplo, propuseram vários desses "Grandes Desafios", dos quais foram selecionados os seguintes:

- **Dar aos usuários garantias sobre a segurança de seus**
- **dispositivos • Se isso pode ser feito anonimamente no mundo off-line, também pode ser feito**
- **anonimamente online • Tornar a inteligência**
- **artificial segura para as pessoas • Tornar**
- **os sistemas resilientes sob ataques • Aumentar a conscientização do público em geral sobre segurança cibernética**

Informações do documento

Colaboradores

Nome	Parceiro
Elias Athanasopoulos	UCY
Panagiotis Bountakas	Universidade do Pireu
Sunil Chaudhary	NTNU
Disse Daoudagh	CNR
Andreas Dionysiou	Universidade de Chipre
Christos Douligeris	UPRC
Afonso Ferreira	IRIT
Simone Fischer-Hübner	Universidade Karlstads
Vasileios Gkioulos	NTNU
Leonardo Horn Iwaya	Universidade Karlstads
Meiko Jensen	Universidade Karlstads
Wouter Joosen	KUL
Marko Kompara	Universidade de Maribor
Panayiotis Kotzanikolaou	Universidade do Pireu
Stephan Krenn	AIT
Antonio Lioy	Politécnico de Turim
Alberto Lluch Lafuente	Universidade Técnica da Dinamarca
Harry Manifavas	ADIANTE
Evangelos Markatos	ADIANTE
Eda Marchetti	CNR
Constantinos Patsakis	Universidade do Pireu
João Roberto Peres	KOMP & Faculdade Getúlio
Laurens Sion	CNR

Silvia Sisini	Politécnico de Torino
Christos Xenakis	Universidade do Pireu

Revisores

Nome	Parceiro
Elias Athanasopoulos	UCY
Javier López	UMA

História

Versão	Data	Autores	Comente
1	15/10/2022	Evangelos Markatos e todos os colaboradores	1st Rascunho – Revisão de alto nível
1.1	12/11/2022	Evangelos Markatos e todos os colaboradores	2e Rascunho
1.2	2022-11-24	Kai Rannenberg e Ahad Niknia	3º Rascunho – Segundo nível alto Análise
1.3	2022-11-28	Evangelos Markatos e todos os colaboradores	Versão final – pronta para submissão
2,0	30/11/2022	Ahad Niknia (GUF)	Verificação final, preparação e processo de envio

HORIZONTE 2020

O

LIVRO AZUL

Um roteiro do horizonte futuro em segurança cibernética

Cyber Security for Europe

Rede de Centros de Competência em Cibersegurança para a Europa

EDITORES

Evangelos Markatos
Líder WP4
Fundação para a Investigação e Tecnologia - Hélade

Kai Rannenberg
Gerente CyberSec4Europe
Universidade Goethe de Frankfurt

AUTORES

Elias Athanasopoulos
Universidade de Chipre

Panagiotis Bountakas
Universidade do Pireu

Sunil Chaudhary
NTNU

Disse Daoudagh
CNR

Antreas Dionysiou
Universidade de Chipre

Christos Douligeris
UPRC

Afonso Ferreira
IRIT

Simone Fischer-Hübner
Universidade Karlstads

Vasileios Gkioulos
NTNU

Leonardo Horn Iwaya
Universidade Karlstads

Meiko Jensen
Universidade Karlstads

Wouter Joosen
KU Leuven

Marko Kompara
Universidade de Maribor

Panayiotis Kotzanikolaou
Universidade do Pireu

Stephan Krenn
AIT

Antonio Lioy
Politécnico de Torino

Alberto Lluch Lafuente
Universidade Técnica da Dinamarca

Harry Manifavas
ADIANTE

Eda Marchetti
CNR

Constantinos Patsakis
Universidade do Pireu

João Roberto Peres
KOMP & Faculdade Getúlio

Laurens Sion
KU Leuven

Silvia Sisini
Politécnico de Torino

Christos Xenakis
Universidade do Pireu

COLABORADORES

Oum-El-Kheir Aktouf, Grenoble INP, França

Spiros Antonatos, Aegis Technologies, Singapura

Universidade , Vilnius Gediminas Técnica

Antanas Cenys cal

Nabin Chowdhury, NTNU

Christoforos Dadoyan, Universidade Jônica

Claudia Diaz, KU Leuven

Nikolaj Goranin, Universidade Técnica de Vilnius Gediminas

Dimitris Gritzalis, Universidade de Atenas Economia e Negócios

Steven Furnell, Universidade de Nottingham

Marit Hansen, Unabhängiges Landeszen-trum für Datenschutz Schleswig-Holstein (ULD SH)

Marko Hÿolbl, Universidade de Maribor

Thorsten Holz, Centro Helmholtz da CISPA para Segurança da Informação

Jaap-Henk Hoepman, Universidade Radboud

Alexandros Kapravelos, Carolina do Norte Universidade Estadual

Marieke Huisman, Universidade de Twente, Holanda

Marc Juarez, Universidade de Edimburgo

Nicolas Kourtellis, Telefónica I+D

Giuseppe Lami, CNR, Itália

Alexios Lekidis, Corporação Pública de Energia

Nicolas Mayer, Instituto Luxemburguês de Ciência e Tecnologia

Weizhi Meng, Universidade Técnica da Dinamarca

Marino Miculan, Universidade de Udine

Panagiotis Papadopoulos, iProov Limited

Jason Polakis, UIC

Lorenzo Pupillo, CEPS e LUISS

João Resende, Universidade NOVA de Lisboa

Konrad Rieck, Universidade Técnica Braunschweig

Vittorio Rosato, ENEA e Universidade Campus Biomédico de Roma

Antonio F. Skarmeta, Universidade de Múrcia

Thomas Schaberreiter, CS-AWARE Corporation

Stefan Schiffner, Universidade de Münster

Roberto Settola, Universidade Campus Biomédico de Roma

Maurice H. ter Beek, CNR, Itália

Denis Trÿcek, Universidade de Liubliana

Andrea Vandin, SSSUP, Itália

Luca Viganò, Kings College Londres

Kim Wuyts, imec-DistriNet, KU Leuven

Apostolis Zarras, Universidade do Pireu

Alejandro Cabrera Aldaya, Rede e Grupo de Segurança da Informação (NISEC), Universidade de Tam-pere

Arttu Paju, Grupo de Segurança de Redes e Informações (NISEC), Universidade de Tampere

Juha Nurmi, Grupo de Segurança de Redes e Informações (NISEC), Universidade de Tampere

Muhammad Owais Javed, Rede e Grupo de Segurança da Informação (NISEC), Universidade de Tam-pere

Nicola Tuveri, Grupo de Segurança de Redes e Informações (NISEC), Universidade de Tampere

Alberto Carelli, Fundação LINKS, Itália

Andrea Vesco, Fundação LINKS, Itália

Lista de siglas

Acrônimo	Explicação
3D	Três dimensões
2FA	Autenticação de dois fatores
IA	Inteligência artificial
API	Interface de programação de aplicativos
APTO	Ameaça persistente avançada
Caixa eletrônico	Caixa eletrônico
AV	Antivírus
C2	Comando e controle
CCC	Consórcio de computação confidencial
IC	Infraestrutura crítica
CI/CD	Integração Contínua e Entrega Contínua
CIOT	Internet das Coisas do Consumidor
CPU	Unidade central de processamento
CVE	Vulnerabilidades e exposições comuns
CWE	Enumeração de fraquezas comuns
DDoS	Negação de serviço distribuída
DevOps	Desenvolvimento de software (Dev) e operação de TI (Ops)
DL	Aprendizado profundo
DNS	Serviço de Nome de Domínio
PD	Privacidade Diferencial
ECCC	Centro Europeu de Competências em Cibersegurança
EDR	Detecção e resposta de endpoint
ENISA	Agência da União Europeia para a Cibersegurança
ESG	Ambiental, Social e Governança
UE	União Europeia
ETSI	Instituto Europeu de Normas de Telecomunicações
FIDO	Identidade rápida on-line
GAN	Rede Adversarial Gerativa
GDPR	Regulamento Geral de Proteção de Dados
HTTP	Protocolo de Transferência de Hipertexto
Hardware	Hardware
KPI	Indicador-Chave de Desempenho
ICS	Sistema de Controle Industrial
IIoT	Internet Industrial das Coisas
IoTEdT	Internet das Coisas Educacionais
IoT	Internet das Coisas Energéticas
IoT	Internet das Coisas Agrícolas

IoT	**Internet das Coisas de Saúde**
IoMT	**Internet de coisas médicas**
IoP	**Internet das Pessoas**
IoT	**Internet das Coisas**
IoTT	**Internet das Coisas de Transporte**
IoV	**Internet de Veículos**
ISP	**Provedor de internet**
PI	**protocolo de internet**
ISTO	**Tecnologia da Informação**
KLoC	**Quilo Linhas de Código**
LOLBin	**Vivendo da Terra Binário**
AMF	**Autenticação multifator**
Desaparecido	**Ataque de inferência de membros**
AM	**Aprendizado de máquina**
MLaaS	**Aprendizado de máquina como serviço**
NCC	**Centros Nacionais de Coordenação**
NFT	**Token Não Fungível**
NEI	**Redes e Sistemas de Informação**
NIS2	**Diretiva de Segurança de Redes e Informações 2**
NIST	**Instituto Nacional de Padrões e Tecnologia**
PNL	**Processamento de linguagem natural**
OES	**Operadores de Serviços Essenciais**
SO	**Sistema operacional**
OTP	**Senha de uso único**
OWASP	**Projeto aberto de segurança de aplicativos da Web**
OPCC	**Cultura e clima de privacidade organizacional**
PbD	**Privacidade desde o projeto**
PC	**Computador pessoal**
ANIMAIS DE ESTIMAÇÃO	**Tecnologias que melhoram a privacidade**
BATER	**Memória de acesso aleatório**
ROM	**Memória somente leitura**
SCADA	**Controle Supervisório e Aquisição de Dados**
SDL	**Ciclo de vida de desenvolvimento de software**
SDK	**Kit de desenvolvimento de software**
SEV	**Virtualização criptografada segura**
SGX	**Extensões de proteção de software**
SIM	**Módulo de identificação de assinante**
PME	**Pequena e Média Empresa**
SMS	**Serviço de mensagens curtas**

SNP	**Paginação aninhada segura**
SOS	**Sistemas de Sistemas**
SSO	**Login único**
SO	**Programas**
TC	**Computação confiável**
TCB	**Base de computação confiável**
TCG	**Grupo de computação confiável**
TDX	**Extensão de domínio confiável**
TE	**Ambiente de execução confiável**
TLS	**Segurança da camada de transporte**
TPM	**Módulo de plataforma confiável**
VM	**Máquina virtual**
RV	**Realidade virtual**
XR	**Realidade Estendida**

Prefácio

Após a conclusão do seu terceiro ano de operação em 2022, o projeto piloto CyberSec4Europe1 (https://cybersec4europe.eu/) produziu este "Livro Azul" (e entregou-o como Entregável D4.7) para servir como um Roteiro de Investigação do Horizonte em na área de segurança cibernética. Para tornar este livro uma realidade, o projeto reuniu uma "Task Force" de investigadores jovens e seniores na área da segurança cibernética.
O Grupo de Trabalho propôs um conjunto inicial de tópicos e referiu-se ao seu grupo constituinte, que é composto por investigadores de topo em segurança cibernética, perguntando-lhes quais deveriam ser os problemas de investigação importantes em relação a estes tópicos.
O resultado desta consulta foi uma descrição de cada tema que continha os seguintes aspectos:

- **Qual é o tema? Descreva o tópico e como ele interage com a cibernética segurança.**
- **Quem será afetado pelos ataques cibernéticos nesta área? pessoas comuns? organizações? o governo? Quem?**
- **O que se espera que aconteça se formos sujeitos a tais ataques cibernéticos? Perda financeira? perda de produtividade? perda de vida? o que?**
- **Qual é a pior coisa que pode acontecer se as coisas correrem realmente mal? perda massiva de vidas? uma guerra? perdas financeiras na ordem dos milhares de milhões de euros? o que?**
- **Quais são as principais lacunas de investigação? O que precisamos fazer do ponto de vista da pesquisa para lidar com esse problema? Quais são as questões de pesquisa importantes que precisam ser abordadas?**
- **Exemplos de problemas. Apresentar problemas de investigação específicos que possam ser abordados numa única tese de doutoramento ou num pequeno número de teses.**

1CyberSec4Europe é financiado pela União Europeia ao abrigo do Acordo de Subvenção do Programa H2020 n.º 830929. Esta publicação reflete apenas a opinião dos autores. A Comissão não é responsável por qualquer uso que possa ser feito das informações nele contidas.

Após esta consulta, o grupo de trabalho também perguntou aos especialistas quais deveriam ser os Grandes Desafios em segurança cibernética. Esses seriam tópicos que precisariam de centenas de pessoas e vários anos para serem resolvidos. No entanto, se resolvidos, mudariam fundamentalmente o problema da segurança ci

Esperamos que este livro forneça orientações úteis aos pesquisadores, dar bons conselhos aos decisores políticos e será útil para todos os que o lerem.

Como ler este livro

Os formuladores de políticas podem querer se concentrar no Capítulo 1 (página 1), que fornece um breve Resumo Executivo do livro, e no Capítulo 16 (página 111), que descreve os Grandes Desafios de Pesquisa na área, que só podem ser resolvidos com a colaboração de diversas organizações de pesquisa e o apoio das principais agências de financiamento.

Jovens pesquisadores interessados em fazer doutorado. em segurança de sistemas deve ler pelo menos a seção final de cada capítulo, que descreve problemas que são apropriados para serem resolvidos no contexto de um doutorado. tese.

Pesquisadores experientes podem querer ler todos os capítulos, mas especialmente o Capítulo 16 (página 111), que descreve os Grandes Problemas de Pesquisa na área.

Conteúdo

1 Resumo Executivo e Principais Recomendações menções

1.1 Direções de Pesquisa

Ao longo do último ano do projeto CyberSec4Europe, os beneficiários do projeto, tendo em conta os contributos dos associados do projeto e de peritos externos, formularam uma série de direções de investigação que serão importantes para o futuro. Essas instruções incluem:

- **Privacidade e anonimato •**
- **Tecnologias emergentes: metaversos, IoT, aprendizado de máquina, etc.**
- **Novas abordagens para autenticação: além de senhas, biometria, etc. • Defesas "por design": desenvolvimento de software, modelagem de ameaças, etc.**
- **Tecnologias fortes: comunicações seguras, testes, execução confiável, etc.**

Para cada direção foram definidas uma série de prioridades de pesquisa. Essas prioridades incluem:

- **Fornecer comunicação anônima forte em grande escala • Construir metaversos confiáveis**
- **Melhorar métodos de autenticação sem senha •**
- **Desenvolver abordagens de detecção precoce para malware blindado**
- **Fornecer privacidade em ambientes IoT •**
- **Realizar modelos de aprendizado de máquina que permanecem seguros sob diferentes anúncios cenários versariais**
- **Garantir que as infraestruturas críticas sejam resilientes a ataques cibernéticos; • Apoiar abordagens de certificação e testes "by-design", integrando valores industriais, sociais e éticos, sustentabilidade e necessidades de confiabilidade**

1.2 Grandes Desafios Embora os

projetos1 de curto prazo possam ter um impacto imediato no mercado, esse impacto é geralmente incremental e pode não ser duradouro, pois se concentra em um problema imediato que pode não ser tão relevante, digamos, daqui a cinco a dez anos. a estrada. Para fazer avanços fundamentais na área da segurança cibernética, propusemos vários problemas de "Grande Desafio" de longo prazo.

Para selecionar um pequeno número de "Grandes Desafios", os membros do Grupo de Trabalho, juntamente com os membros do círculo eleitoral mais amplo, propuseram vários desses "Grandes Desafios", dos quais foram selecionados os seguintes:

- **Dê aos usuários garantia sobre a segurança de seus dispositivos**
- **Se isso pode ser feito anonimamente no mundo offline, também pode ser feito anonimamente online**
- **Tornar a inteligência artificial segura para as pessoas**
- **Tornar os sistemas resilientes sob ataques**
- **Aumentar a conscientização do público em geral sobre segurança cibernética**

1Quando dizemos projetos de curto prazo referimo-nos a projetos que duram dois a três anos e têm um financiamento de dois a três milhões de euros.

2 Introdução

A penetração do ciberespaço na nossa vida quotidiana atingiu níveis sem precedentes. Embora há 30 anos a Internet fosse uma curiosidade principalmente utilizado entre os académicos, hoje mais de 92% dos agregados familiares na União Europeia têm acesso à Internet [2]. Os europeus usam a Internet para vários aspectos da vida quotidiana: mais de 50% utilizam-no nas redes sociais, cerca de 50% utilizam-no para serviços bancários pela Internet, cerca de 66% utilizam-no para encontrar informações sobre bens e serviços, e 55% utilizam-no para procurar informações sobre saúde [81]. O A pandemia de COVID-19 apenas aumentou a utilização da Internet, à medida que ainda mais atividades quotidianas passaram a ser online. Por exemplo, durante a pandemia, a escolaridade, compras e socialização só poderiam ser feitas on-line por longos períodos de tempo. Embora a pandemia seja coisa do passado, a penetração de alguns dessas atividades na Internet veio para ficar.

Embora a movimentação de atividades online tenha certas vantagens, também pode criar ameaças para as pessoas. Na verdade, à medida que mais e mais actividades se deslocam do mundo físico para o mundo digital, isso apenas aumenta a superfície de ataque. Que isto é, os ciberataques têm mais oportunidades de atacar. Isto é simples de entender: se as pessoas fizerem transações bancárias on-line, os ladrões tentarão roubar dinheiro on-line. Da mesma forma, se as pessoas fizerem suas ligações telefônicas usando algum vídeo on-line sistema de conferência, os bisbilhoteiros tentarão ouvir essas conversas online através de uma ampla variedade de opções: eles podem oferecer tal sistema para uso de graça; podem comprometer um desses sistemas; eles podem infectar o software com um vírus próprio; eles podem “comprar” tal bug para comprometer o sistema. Aqui o céu é o limite. O ponto mais importante é que as pessoas transferiram suas conversas para plataformas online. Uma vez que isso movimento foi feito, os invasores pensarão em várias maneiras diferentes de escutar essas conversas. O mesmo se aplica a todas as outras atividades de nossas vidas cotidianas: quando transferimos uma atividade para o ciberespaço, os ciberataques têm uma riqueza de novas oportunidades para atacar.

Tendo percebido esta ameaça crescente na área da cibersegurança, os parceiros do projeto CyberSec4Europe elaboraram uma lista de áreas de cibersegurança nos quais devemos nos concentrar nos próximos anos. Eles explicaram o ameaças à segurança nestas áreas e eles elaboraram sobre que tipo de

pesquisas sobre segurança cibernética precisam ser feitas. As áreas que estudaram são: anonimato, autenticação, infraestruturas críticas, modelagem eficaz de ameaças, segurança IoT, aprendizado de máquina, malware, metaversos, privacidade desde o design, conscientização e treinamento em segurança, ciclo de vida de software, testes e certificação e execução confiável. .

Entre as áreas de pesquisa mais importantes vemos:

- **Fornecer comunicação anônima forte em grande escala**
- **Construa metaversos confiáveis**
- **Melhorar métodos de autenticação sem senha**
- **Desenvolver abordagens de detecção precoce para malware blindado**
- **Fornecer privacidade em ambientes IoT**
- **Realize modelos de aprendizado de máquina que permaneçam seguros sob diferentes anúncios cenários versariais**
- **Garantir que as infraestruturas críticas sejam resilientes a ataques cibernéticos**
- **Apoiar abordagens de testes e certificação “by-design”, integrando valores industriais, sociais e éticos, sustentabilidade e necessidades de confiabilidade**

Para fazer avanços fundamentais na área da segurança cibernética, temos também propôs vários “problemas do Grande Desafio” de longo prazo, incluindo:

- **Dê aos usuários garantia sobre a segurança de seus dispositivos**
- **Se isso pode ser feito anonimamente no mundo offline, também pode ser feito anonimamente online**
- **Tornar a inteligência artificial segura para as pessoas**
- **Tornar os sistemas resilientes sob ataques**
- **Aumentar a conscientização do público em geral sobre segurança cibernética**

3 A erosão do anonimato

3.1 Introdução

Ao longo dos últimos anos temos sido cada vez mais usando o ciberespaço para a maioria das nossas atividades diárias: fazer compras, trabalhar, ver filmes, ouvir música, conversar com amigos, divertir-se, etc.

A pandemia de COVID-19 intensificou este efeito e forçou para fazermos a maior parte de nossas atividades laços on-line: estudar, fazer compras, socializar, manter contato, quase tudo era feito on-line. Em alguns casos, as coisas se tornaram tão extremas que fazer algumas dessas atividades off-line era completamente ilegal. Na verdade, durante esses períodos de confinamento, as visitas presenciais a amigos eram ilegais em alguns países e implicavam pesadas multas. Por isso, durante esses períodos, a única maneira de visitar amigos era através de algum serviço on-line. ferramenta de videoconferência.

Embora tais atividades on-line fossem convenientes (ou mesmo absolutamente necessárias durante a pandemia), geralmente exigiam autenticação forte e identificação de todas as partes envolvidas. Por exemplo, as compras online não eram possível com dinheiro anônimo, mas exigia o uso de cartões de débito/crédito e possivelmente contas bancárias online. Entrega dos produtos adquiridos necessária a divulgação do endereço de entrega, a apresentação de alguns documentos identificativos informações, possivelmente a divulgação de um número de telefone celular, etc.1 A situação não era melhor para outras formas de interação, como manter contato

1Embora esta informação seja necessária para tais transações online, independentemente da pandemia, antes da pandemia as pessoas tinham uma escolha: podiam optar por não participar em tais transações. Du a pandemia a escolha não existia mais.

com a família. Com efeito, como era quase impossível uma “visita” física à família, a única forma de interação era através de videoconferência, o que normalmente implicava a instalação de algum software de videoconferência que necessitava do nome do utilizador, da sua morada e, eventualmente, de um cartão de crédito para efeitos de p E para piorar a situação, este software tinha a capacidade de rastrear quem está falando com quem e o que dizem.

A divulgação de todos estes dados pessoais contrasta fortemente com a era pré-COVID, onde as pessoas podiam realizar todos estes tipos de interações sem a necessidade de divulgar qualquer tipo de informação pessoal. Esta divulgação de informações pessoais geralmente leva à perda do anonimato: as pessoas não podem visitar os seus pais sem informar várias empresas online. A mesma perda de anonimato acontece em outras áreas de nossas vidas. Por exemplo, no passado as pessoas podiam comprar uma lata de refrigerante no seu minimercado, pagar em dinheiro e permanecer relativamente anónimas. Hoje, para comprar uma lata de refrigerante on-line, eles precisam divulgar seu nome, endereço, dados de cartão de crédito, embora possam ser rastreados por dezenas de cookies, rastreadores e anunciantes, que usam seus dados para todo tipo de marketing. propósitos.

Poderíamos ficar tentados a dizer: “Não é necessário realizar estas interações online: podemos sempre voltar às interações físicas”. Embora seja bom ter pontos de vista tão otimistas, tememos que em breve não haja “volta” para onde “voltar”. As interações online continuam a aumentar e não há indicação de que irão diminuir significativamente: as compras online estão a aumentar, a utilização de smartphones continua a aumentar e as pessoas parecem passar cada vez mais tempo online. Como resultado, parece que as interações online vieram para ficar e só precisamos lidar com o rastreamento e a erosão do anonimato que as acompanha.

3.2 Quem será afetado?

Dado que é mais difícil permanecer anónimo online (em comparação com o mundo offline), a maioria dos cidadãos cumpridores da lei que utilizam a Internet sem qualquer software especial de anonimização serão potencialmente afetados por esta erosão do anonimato. Parece, no entanto, que os mais jovens serão os mais afetados, uma vez que se espera que passem uma maior percentagem das suas vidas or Além disso, as pessoas que desempenham algum papel visível ao público (tais como actores, políticos, etc.) também serão desproporcionalmente afectadas, uma vez que as suas vidas (privadas) serão fortemente escrutinadas. Ao contrário do roubo de propriedade física, a erosão do anonimato é muito parecida com o roubo de dados: uma vez que os dados desaparecem, geralmente não há como recuperá-los. Não é como talheres roubados, que o dono receberá de volta se pegar o ladrão. Os dados roubados podem ser copiados e desaparecer para sempre: não há “

seus contatos também serão afetados. Expor as informações pessoais de uma única pessoa não prejudica apenas a própria pessoa, mas pode potencialmente prejudicar qualquer pessoa que interaja online com ela: seus amigos, parentes, etc.

Além disso, as pessoas que necessitam de anonimato para a sua segurança física serão gravemente afetadas. Por exemplo, as pessoas em países não democráticos podem enfrentar um perigo imediato. Mesmo as pessoas nos países democráticos, como os denunciantes e os jornalistas, podem ser gravemente afetadas se não puderem operar anonimamente.

Finalmente, as organizações também serão significativamente afetadas. Na verdade, informações que costumavam ser confidenciais dentro de uma empresa (como número de clientes, número de vendas, horários de pico, etc.) agora podem ser encontradas (ou pelo menos inferidas com alta precisão) por rastreadores e anunciantes que estão envolvidos na interação. Poderíamos pensar que as grandes organizações seriam capazes de examinar minuciosamente os seus sites e erradicar qualquer r Isto provavelmente é verdade. Não está claro, contudo, se as pequenas empresas terão o conhecimento e/ou a capacidade para fazer algo assim.

3.3 O que se espera que aconteça?

Num mundo onde o anonimato não é fácil de alcançar, as pessoas simplesmente não conseguirão agir anonimamente. Todos os aspectos da sua actividade serão registados algures online por alguém que provavelmente não conhecem: a que horas acordam, a que horas vão para o trabalho, que artigos compram, que livros lêem, que notas fazem, que notícias trazem. onde comem, onde passam a noite, com quem passam a noite – tudo será registado online.2 As pessoas continuarão a ter pouca (ou nenhuma) vida privada. Na ausência de um sistema jurídico forte que penalize fortemente o acesso não autorizado à informação, tememos que esta informação possa eventualmente chegar às pessoas erradas. Na verdade, embora inicialmente as informações possam ser partilhadas com uma entidade confiável (como o nosso ISP ou o nosso fornecedor de e-mail), as informações, tal como qualquer outra mercadoria digital, podem eventualmente ser vendidas, adquiridas ou mesmo roubadas. O pior de tudo é que não sabemos realmente se isso vai acontecer, ou mesmo se já aconteceu.

Algumas pessoas podem dizer "Não tenho nada a esconder", por isso podem pensar que é razoável divulgar todas as suas atividades online. No entanto, o ponto principal aqui é que, uma vez divulgada on-line, a informação pode eventualmente chegar às pessoas erradas ou cair nas mãos erradas. Se cair em mãos erradas, a informação pode causar grandes danos às pessoas. Imagine, por exemplo, os sindicatos do crime organizado. Eles adorariam saber o paradeiro de

2Mesmo a hora do dia em que estou digitando esses caracteres e a hora do dia que o leitor lê este texto talvez esteja sendo gravado em algum lugar online.

pessoas: quem está sozinho, quem está de férias, que casa está vazia, que idosos compraram jóias, etc. Estudos recentes sugerem que 78% dos assaltantes utilizam as redes sociais para encontrar os seus alvos [3]. Estes ladrões utilizam as redes sociais para encontrar fotografias de casas, ou mesmo fotografias de chaves de casas [33], para ver se os potenciais alvos estão de férias, para descobrir as suas rotinas diárias e para ver se fizeram check-in num restaurante. Todas essas informações podem ser utilizadas para encontrar os alvos mais promissores e qual o melhor momento para roubá-los.
Alguém pode ficar tentado a pensar "Oh! Eu não publico essas informações on-line, portanto estou seguro." Tememos que isso esteja longe de ser verdade. Na verdade, várias das aplicações dos nossos smartphones (e especialmente aquelas que têm acesso às nossas coordenadas GPS) sabem onde estamos. Eles sabem se estamos de férias, sabem em que restaurante estamos, sabem quando saímos de casa, sabem quando voltamos, etc. O facto de não publicarmos tal informação nas redes sociais não significa que esta informação seja não é gravado on-line por vários atores diferentes que têm acesso a ele. E, como já dissemos, se alguma informação for recolhida online, poderá posteriormente ser partilhada, vendida ou mesmo roubada.

Parece que a maioria das pessoas não está consciente destes perigos. Como resultado, eles não buscam o anonimato e se expõem a atores maliciosos: ladrões, assaltantes ou mesmo assassinos! Por exemplo, uma pesquisa recente sobre 350 homicídios sugere que antes de assassinar as suas vítimas, os assassinos perseguem as suas vítimas nas redes sociais [198]. Estes exemplos sugerem que esta falta de interacção anónima, na qual várias pessoas se envolvem, pode levar a danos graves: roubo, perda de bens e até perda de vidas!

3.4 Qual é a pior coisa que pode acontecer?

Tememos que o impacto na sociedade seja muito maior do que o descrito até agora.
Se o anonimato for completamente perdido, será como viver num mundo onde cada uma das nossas atividades é monitorada o tempo todo. Será como viver numa sociedade distópica "tipo Big Brother", onde cada acção será monitorizada e registada.
E o pior de tudo é que não sabemos realmente quem está registrando e quem tem acesso a essas informações. É um anunciante que quer saber de que cor de calçado gostamos?

É uma gangue criminosa que gostaria de saber quais idosos compraram joias recentemente? É o governo de um país hostil que gostaria de conhecer a rotina diária das pessoas do nosso país e possivelmente incomodá-las quando as visitam nas férias?
Nós realmente não sabemos.

Tememos que esta perda total do anonimato não só transforme as vidas dos indivíduos, mas também transforme sociedades inteiras. As pessoas podem tornar-se extremamente conservadoras e ficar com medo de cada ação que tomam. Num tal ambiente, as pessoas podem abster-se de exercer os seus direitos por medo de que isso possa ter consequências; isso prejudicaria gravemente a própria democracia. As sociedades distópicas do tipo de 1984 que conseguimos evitar voltarão a assombrar-nos através dos nossos próprios erros e da nossa própria negligência.

3.5 Lacunas de Pesquisa

Para resolver o problema precisamos de uma combinação de atividades jurídicas e técnicas nesta área.

3.5.1 Fornecer Comunicação Anônima Forte em Grande Escala Hoje há

muito poucas oportunidades para comunicação anônima. O roteador cebola (Tor) é um dos mais conhecidos [62]. No entanto, menos de 1‰ dos usuários da Internet o utiliza. Precisamos fornecer sistemas fáceis de usar que ofereçam proteção robusta e possam resistir a adversários poderosos sob uma variedade de modelos de ameaças.

3.5.2 Forneça on-line o mesmo nível de anonimato que você espera off-line

Hoje, o anonimato foi implementado apenas em uma pequena parcela das interações on-line, principalmente na navegação anônima na web. Na verdade, a rede Tor mencionada acima vem com um navegador que torna a configuração da instalação muito mais fácil para os usuários. Este anonimato deve ser estendido a todos os tipos de interações, incluindo compras anônimas, entretenimento anônimo, etc. A regra aqui deveria ser: se isso pode ser feito anonimamente offline, devemos tentar fazê-lo anonimamente online também.

3.5.3 Medir/Monitorar a escala do problema - Alcançar Transparência Não está

claro para a maioria das pessoas qual é a escala deste problema: qual é a quantidade de informação pessoal que está a ser partilhada. Os rastreadores da web continuam inventando novas maneiras de rastrear usuários on-line e privá-los da capacidade de operar anonimamente [181]. É basicamente um "jogo de gato e rato", onde os rastreadores inventam novas formas de rastreamento e os pesquisadores tentam detectar essas formas de rastreamento, possivelmente por meio de engenharia reversa. Precisamos compreender melhor a escala e os mecanismos de rastreamento e perda de anonimato. Precisamos de desenvolver mecanismos que monitorizem continuamente esta erosão do anonimato a todos os níveis e de todas as formas possíveis. Estes mecanismos devem poder funcionar frequente

3.5.4 Novas abordagens de anonimização e desanonimização de dados

Precisamos de desenvolver novos mecanismos de anonimização de dados que permitam a partilha de dados em maior escala. Embora já existam algumas abordagens de anonimização de dados (ver [226] e [68]), ainda há um longo caminho a percorrer antes que dados anônimos possam ser compartilhados em grande escala. Precisamos estudar os ataques às abordagens existentes de anonimato de dados que visam desanonimizar os dados e desenvolver defesas que resultarão em melhores abordagens de anonimato.

3.5.5 Resistir à Censura

Vários países em todo o mundo censuram as comunicações na Internet.
Nessas configurações, os usuários têm acesso limitado à Internet ou, em alguns casos, nenhum acesso. Precisamos de desenvolver sistemas robustos e práticos que contornem a censura e permitam às pessoas publicar e aceder à informação de forma segura (e anónima).

3.5.6 Desenvolver métodos robustos contra impressões digitais

Para quebrar o anonimato de seus usuários, vários sites utilizam métodos de impressão digital. Tais métodos tentam identificar vários aspectos do navegador do usuário (por exemplo, tipo de navegador, fontes suportadas) ou do computador do usuário (como idioma local, versão do sistema operacional, tamanho da tela, etc.) para identificar exclusivamente os usuários. enquanto navegam na web. Embora cada um desses recursos por si só (como o tamanho da tela) não seja suficiente para identificar um usuário de maneira exclusiva, a combinação de todos eles geralmente é suficiente. Precisamos desenvolver abordagens fortes contra impressões digitais que permitam a coleta de pouca (ou nenhuma) informação sobre os usuários enquanto eles navegam pela Internet.

3.6 Exemplos de problemas

Exemplos de problemas tangíveis podem incluir:

Vazamentos de identidade. Monitore como os sites usam todos os tipos de mecanismos (como cookies, argumentos de URL, campos de cabeçalho de URL, etc.) para transferir dados pessoais de um site para outro. Desenvolva defesas contra tais mecanismos anismos.

Torne o anonimato de redes mais resistente a ataques. Estudar possíveis ataques que possam comprometer o anonimato nas redes anônimas. Explore a magnitude destes ataques e proponha possíveis soluções.
Inicialmente, concentre-se em ataques de impressão digital de sites no Tor.

Opere com personas anônimas. Desenvolva personas falsas que permitam aos usuários usar a web sem revelar sua verdadeira identidade. Desenvolva um sistema que avalie claramente o compromisso entre usabilidade e privacidade no fornecimento de informações falsas em diferentes ambientes. Explore as situações em que as personas fornecem utilidade adicional.

Compreensão da privacidade. Melhorar a compreensão dos usuários sobre suas decisões relacionadas à privacidade, como os formulários de consentimento de cookies com os quais eles conco Desenvolver ferramentas (semi)automatizadas que melhorem esse entendimento e quantifiquem as escolhas feitas pelos usuários.

Proveniência dos dados. Desenvolva sistemas que permitam aos usuários detectar a procedência dos dados e, assim, descobrir dados roubados/vazados. Resolva o problema para diferentes tipos de dados, incluindo séries temporais, imagens, vídeos, sinais multidimensionais, etc.

4 Aprendizado de Máquina

4.1 Introdução

O aprendizado de máquina (ML) se tornou o
tecnologia que alimenta uma ampla gama de aplicações
e serviços. O desempenho
e a generalização dos modelos de ML feitos
um bom candidato para enfrentar uma série de
problemas da vida real que apresentam alta
complexidade. Tomemos por exemplo os recentes
avanços das Redes Adversariais Generativas
(GANs) que conseguem sintetizar rostos humanos
altamente realistas com um pequeno número de amostras do mundo real [127]. De modo geral,
os sistemas baseados em ML conseguiram atingir altas taxas de sucesso em
problemas onde as abordagens clássicas baseadas em regras não tiveram um bom desempenho.

Hoje em dia, o ML foi implantado em muitos setores da nossa vida cotidiana.
Por exemplo, durante nossas compras online no Ebay ou Amazon, um aplicativo baseado em ML
sistema de recomendação personalizado, executado em segundo plano, propõe produtos de
acordo com diferentes parâmetros relacionados ao usuário, por exemplo, o histórico de
compras anteriores e o tempo gasto olhando um produto específico. Além disso, a indústria
automotiva incorporou tecnologias de ML em seus
carros para fazê-los dirigir sozinhos, sem qualquer supervisão humana. Além disso, técnicas de
processamento de linguagem natural (PNL) baseadas em ML
foram desenvolvidos para melhorar a segurança dos ambientes de discussão on-line, por
exemplo, para detectar conteúdo tóxico, sarcástico, de assédio e abusivo [169]. Em
em geral, as tecnologias de ML beneficiaram vários setores, alguns deles sendo
o seguinte: diagnóstico médico [131], detecção de fraude de cartão de crédito [146],
análise do mercado de ações [41], bioinformática [63], reconhecimento de fala [99], objeto
detecção [40] e locomoção do robô [129].

Para compreender o potencial dos algoritmos de ML, basta dizer que muitos
gigantes da tecnologia, como Google e Amazon, oferecem aprendizado de máquina como serviço
plataformas (MLaaS), onde os usuários podem fazer upload de seus próprios dados para treinar seus
possuir modelos de ML e resolver uma tarefa específica de classificação/previsão. Assim, o

os dados dos usuários – que em muitos casos contêm informações sensíveis, como registros médicos, fotos e outros descritores pessoais – são usados como treinamento dados pelas plataformas MLaaS. Além disso, alguns operadores de MLaaS podem fornecer proprietários de dados a opção de vender acesso aos seus modelos de ML treinados para o público em geral público.

Apesar do enorme sucesso do ML na resolução de numerosos problemas difíceis, foi demonstrado que várias vulnerabilidades de segurança e privacidade coexistem com esses modelos [142, 182]. Por exemplo, pense no caso em que uma PNL modelo classifica erroneamente a crítica de um filme como "excelente" em vez de "ruim". Este erro (classificação incorreta) resulta em uma pontuação mais alta para aquele filme específico. Por isso, os usuários que consultam um site específico para obter classificações de filmes serão atraídos a assisti-lo filme por causa de sua alta classificação. Depois de assistir esse filme, os usuários perceberão que não era tão bom quanto o site de classificação sugeria e, como consequência, evite usar o mesmo site novamente. Falando mais sério, pense no caso onde um modelo de reconhecimento de imagem é implantado em uma condução autônoma veículo para identificar sinais de trânsito. Se um invasor perturbar deliberadamente a entrada (vídeo) do modelo de reconhecimento de imagem, o modelo poderá erroneamente reconheça um sinal de “pare” como um sinal de “limite mínimo de velocidade” e acelere em vez de parar o carro. Como você pode facilmente imaginar, tais ataques podem ter consequências graves, causando até mortes. Em conclusão, uma vez que o ML dominada em muitos setores, precisamos encontrar soluções para garantir a sua operação segura.

4.2 Quem será afetado?

Desde a ampla adoção de modelos de ML em uma variedade de serviços e aplicativos, qualquer pessoa que tenha acesso a um dispositivo moderno (por exemplo, um smartphone, um computador pessoal, um veículo ou mesmo um eletrodoméstico) podem ser afetados. Em em geral, qualquer indivíduo que possua um dispositivo eletrônico pode ser afetado. No entanto, espera-se que os jovens sejam afectados em maior grau em comparação com os indivíduos mais velhos, uma vez que utilizam frequentemente tecnologias mais recentes e aplicativos que geralmente são alimentados por ML [124].

Uma grande parte dos aplicativos baseados em ML são frequentemente treinados em (dados sensíveis. As fugas de tais dados podem ter consequências graves para o indivíduos afetados. Pense no caso em que um modelo de ML é treinado para avaliar associar as informações de um paciente a uma classe específica de doença. Se um adversário sabe que os dados de um paciente foram incluídos no conjunto de dados de treinamento do modelo, eles podem tirar conclusões sobre o estado de saúde da vítima (conhecidos como ataques de inferência de membros [211]). De forma semelhante, se um adversário conseguir para gerar com sucesso entradas semelhantes às originais usadas para treinar o modelo de destino, então isso pode permitir a desanonimização dos usuários

e expor informações pessoais ou sensíveis (conhecidos como ataques de inversão de modelo [85]). Finalmente, ataques de geração de imagens adversárias, onde um adversário introduz pequenas modificações em uma imagem existente para confundir ou enganar um modelo de ML de reconhecimento de imagem para realizar uma classificação incorreta, foram propostos na literatura [96].

Por fim, as empresas que fornecem soluções baseadas em ML também podem ser afetadas, além de indivíduos. Em particular, revelar que os serviços de BC oferecidos por uma empresa são vulneráveis aos ataques acima mencionados pode seriamente prejudicar as finanças e a reputação dessa empresa.

4.3 O que se espera que aconteça?

A capacidade de generalização (desempenho) de aplicações baseadas em ML depende fortemente da quantidade de dados de treinamento disponíveis. Mas, como o treinamento o volume de dados cresce, assim como a chance de dados confidenciais estarem presentes. Assim, é realista assumir que a atenção de potenciais adversários e grupos maliciosos se concentrarão em atacar sistemas que utilizam ML componentes.

O número de incidentes de violação de dados que exploram componentes de ML aumentará aumentar num futuro próximo. Isso ocorre porque os modelos de ML, executados em segundo plano e coletando dados pessoais confidenciais, serão implantados em mais e mais aplicativos e serviços. Assim, os potenciais adversários terão acesso a uma gama mais ampla de alvos exploráveis.

Os modelos de ML podem ser implantados em setores onde a tomada de decisões erradas implica consequências graves (por exemplo, na saúde). Assim, legislações/regulamentos serão elaborados de forma a indicar explicitamente os responsáveis caso algo corra mal ou não conforme o esperado. Além disso, a segurança e a privacidade os padrões que devem ser atendidos pelos modelos de ML implantados serão lançados. Esses os padrões garantirão que os modelos de ML implantados sejam robustos contra ameaças (conhecidas). Finalmente, serão elaboradas diretrizes para melhores práticas, a fim de para ajudar desenvolvedores não especialistas em ML que desejam incorporar tecnologias de ML em suas aplicações.

4.4 Qual é a pior coisa que pode acontecer?

Como já mencionado, espera-se que o número de incidentes de violação de dados causados pela exploração de componentes de ML aumente. A fim de evitar potenciais explorações que possam ter sérias repercussões, as autoridades competentes, como a União Europeia (UE), devem continuar a tomar medidas ousadas. etapas (por exemplo, ver Pupillo et al. [144] e comunicados de imprensa da ENISA sobre segurança de IA/ML [73, 74, 76]) para fortalecer a segurança e a privacidade de sistemas baseados em ML

itens e serviços. Somente com tais regulamentações/políticas concretas em vigor a comunidade experimenta todo o potencial das tecnologias de ML.

Além disso, para empresas que oferecem soluções baseadas em ML, potenciais ataques aos seus sistemas podem implicar milhões de dólares em danos financeiros e perda de reputação. Além disso, ataques como os descritos na seg. 4.2 pode inutilizar uma grande parte dos sistemas baseados em ML.

Por último, mas não menos importante, o grau de em que as pessoas confiam nos sistemas baseados em ML diminuirá bastante, se apropriado medidas de segurança e privacidade não são consideradas. Isto é importante, porque a tração (uso) de tais sistemas também diminuirá. As pessoas vão hesite em fornecer seus dados valiosos para treinar modelos de ML. Por isso, os avanços no ML e na inteligência artificial (IA) em geral diminuirão significativamente. Na verdade, as pessoas ficarão tão desconfiadas da tecnologia que hesite em usá-lo. Tal como no caso do 5G, poderemos até ver revoltas e movimentos de protesto contra as tecnologias de ML.

4.5 Lacunas de Pesquisa

A fim de melhorar a operação segura de sistemas baseados em ML, vários ações podem ser tomadas.

4.5.1 Explorando a robustez da segurança e da privacidade do ML de última geração modelos sob diferentes cenários adversários

Até agora, a comunidade científica identificou uma série de questões de segurança/privacidade vulnerabilidades que coexistem com modelos de ML de última geração. No entanto, expor esses modelos em diferentes cenários adversários pode revelar informações adicionais vulnerabilidades das quais possam sofrer. Descobrindo essas fraquezas ajudará significativamente a comunidade no desenvolvimento de defesas de aplicação geral ou no projeto de arquiteturas melhoradas em termos de fornecimento de garantias específicas de segurança/privacidade. Nesse sentido, as estruturas de auditoria de ML podem ser desenvolvido que será o único responsável por avaliar a robustez do ML modelos contra ameaças específicas de segurança/privacidade.

4.5.2 Projetando arquiteturas e algoritmos de treinamento para aumentar a generalização e robustez dos modelos de ML contra ataques de segurança/privacidade

Vários atributos dos modelos de ML podem estar relacionados à sua vulnerabilidade a ataques específicos de segurança/privacidade. Por exemplo, os ataques de inferência de membros (MIAs) demonstraram ser mais eficazes em modelos sobreajustados (ou seja, modelos que demonstram baixa generalização) do que em modelos bem generalizados [211]. Além disso, foi demonstrado que a própria arquitetura do modelo desempenha um papel importante na sua vulnerabilidade contra MIAs. Nesse sentido, os pesquisadores demonstraram que um modelo ingênuo de Bayes é muito mais resiliente aos MIAs em comparação com uma árvore de decisão e, portanto, pode ser o tipo de modelo preferido para um serviço de ML específico [234]. Assim, devem ser desenvolvidas arquiteturas de modelos de ML que ofereçam maior robustez contra ataques de segurança e privacidade.

De forma semelhante, o treinamento de modelos de ML deve ser otimizado para oferecer maiores garantias de segurança e privacidade. Por exemplo, Privacidade Diferencial (DP) [68] oferece garantias probabilísticas sobre a privacidade de registros individuais em um banco de dados. O DP mantém a distribuição estatística global de um conjunto de dados e sua contribuição para os pesos de um modelo de ML, ao mesmo tempo que reduz a influência de cada instância de treinamento. Da mesma forma que o k-anonimato [139] e a diversificação [9], o DP pode ser usado para mitigar o risco contra vários ataques à privacidade, como inferência de adesão e reidentificação. A aplicação do DP, no entanto, impõe um compromisso entre segurança e utilidade (utilidade). Ou seja, quanto mais fortes forem as garantias de segurança que o DP oferece, maior será o impacto negativo no desempenho do modelo. Assim, devem ser desenvolvidos novos algoritmos e técnicas de treino que maximizem as garantias de segurança/privacidade, ao mesmo tempo que sacrifiquem o mínimo de desempenho possi

4.5.3 Sobre a transparência e interpretabilidade dos modelos de ML profundo

Os modelos de ML são frequentemente vistos como caixas pretas que podem tomar uma decisão com base em qualquer variante de entrada possível. A natureza complexa dos modelos de ML torna seu funcionamento interno difícil de compreender. No entanto, o que é difícil de compreender também é difícil de auditar. E o que é difícil de auditar também é difícil de confiar. De modo geral, o nível de transparência do modelo depende do conhecimento necessário para compreender a mecânica interna do algoritmo de ML.

Existem alguns algoritmos de ML que produzem direta ou indiretamente resultados compreensíveis por humanos, como um modelo linear ou uma árvore de decisão. Suponha que possamos traçar a cadeia de raciocínio de cada decisão tomada por um algoritmo. Podemos afirmar que o algoritmo é transparente? A resposta

infelizmente não. A cadeia de raciocínio apenas nos diz “como” uma decisão foi feito para uma determinada entrada, mas não para “por quê”. Por exemplo, saber “como” não é suficiente para justificar que a decisão seja tomada de forma consistente, precisa e de forma confiável e válida. Assim, para que um modelo de aprendizagem seja verdadeiramente transparente, precisa saber “como” e “por quê”. Devido à alta complexidade de profundidade Modelos de ML, que muitas vezes incorporam centenas de camadas total (ou parcialmente) interconectadas, uma abordagem promissora para aumentar sua transparência e interpretabilidade é fornecer justificativas e insights para as decisões que pode ser medido externamente.

4.6 Exemplos de problemas

Exemplos de problemas tangíveis podem incluir:

Explorando ataques de segurança e privacidade em modelos de ML. Uma direção importante para melhorar a segurança e a privacidade dos algoritmos de ML é revelar vulnerabilidades ocultas adicionais. Além dos ataques já estabelecidos à segurança/ privacidade, como inversão de modelo, inferência de associação, extração de modelo e geração de amostras adversárias, esforço adicional é necessário para determinar outras possíveis ameaças. Além disso, precisamos de conceitos e técnicas para medir a vulnerabilidade/robustez do ML.

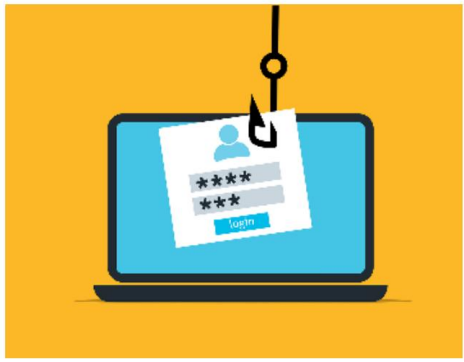
Propor estratégias de defesa de aplicação geral. Outra direção interessante é o desenvolvimento de defesas de aplicação geral, mais especificamente, defesas que podem ser aplicadas a modelos de ML treinados existentes sem a necessidade de retreinamento, o que é um processo demorado e exigiria grandes recursos computacionais ou quaisquer modificações sua arquitetura/algoritmo de treinamento, o que exigiria intervenção manual de especialistas na área de IA e ML.

Aplicar modelos de aprendizagem vulneráveis de forma segura. Alguém poderia dizer que O ML perfeitamente seguro é provavelmente uma ilusão. Assim, em vez de focar aumentando sua robustez, uma direção alternativa é focar em como aplicá-los de forma tão segura que a exploração desses modelos de ML torna-se significativamente mais difícil.

Desenvolver técnicas de interpretabilidade amigáveis ao ser humano. Este ângulo envolve o desenvolvimento de sistemas e serviços que sejam capazes de fornecer explicações amigáveis para as decisões do atual estado da arte sobre ML modelos. Quando nos referimos a “explicações amigáveis ao ser humano”, queremos dizer justificativas que sejam de preferência simples o suficiente para pessoas que não são especialistas nas áreas de IA e ML para entender.

5 Autenticação – Além das Senhas

5.1 Introdução



Atualmente, o uso crescente de o ciberespaço exige que cada pessoa ter várias contas para acessar os sistemas e aplicativos web necessários às atividades cotidianas. Um dos mais antigos mecanismos de proteção de sistemas e aplicações web é o método de autenticação, onde o usuário é solicitado provar sua identidade para obter acesso. O método mais comum de autenticação por um sistema ou uma aplicação é feita através do chamado método nome de usuário-senha. Neste método, o usuário deve fornecer o nome de usuário e a senha que foram escolhidos durante o processo de criação da conta (cadastro). Apesar do nome de usuário-senha ser um dos mais antigos métodos de autenticação, ainda é usado por quase todos os sistemas e aplicativos (tanto on-line quanto off-line). Por exemplo, um médico em um hospital implanta o método nome de usuário-senha para acessar sua conta no hospital e em um loja online. Durante os últimos anos, o número de contas que cada usuário mantém aumentou muito; conseqüentemente, os usuários têm dificuldade em memorizar e gerenciar todas essas senhas. Um estudo recente da NordPass mostrou que uma pessoa média tem 100 senhas diferentes para lembrar, levando a um problema chamado sobrecarga de senha [199]. Além disso, o nome de usuário-senha paradigma está sujeito a diversos ataques cibernéticos, como recuperação de senha de seu hash vazado por meio de força bruta (quebra de senha), recuperando um senha quando transmitida através de um canal não confiável (espionagem), enganar um usuário para que ele insira sua senha em um endpoint não confiável ou comprometido (sites de phishing, skimmers de caixas eletrônicos) ou permitir o uso de senhas padrão que podem ser usadas por adversários [28] [174] [8] [83].

Portanto, para que uma senha seja considerada forte, conforme sugerido pela Microsoft, ela deve conter pelo menos 12 caracteres, ser complexa (ou seja, conter caracteres alfanuméricos, números, símbolos e palavras que não sejam do dicionário), ser diferente de outras senhas que o usuário usado no passado e ser difícil para outros adivinharem [152]. Todas essas condições, juntamente com o elevado número de contas diferentes, afetaram os usuários que têm dificuldade em memorizar (Força dos Segredos Memorizados [173]) e gerenciar todas essas senhas. Para resolver este problema de sobrecarga de senhas, os usuários criaram soluções que afetam diretamente a segurança de suas contas e a privacidade de seus dados; eles simplificam suas senhas para serem fáceis de lembrar, reutilizam a mesma senha em diferentes serviços ou armazenam suas senhas em um local "seguro", por exemplo, em papel ou usando um gerenciador de senhas. Mas mesmo que a senha seja forte e o usuário a administre adequadamente, os provedores de serviços também precisam cumprir sua parte no acordo e armazenar as senhas de seus usuários com segurança. O NIST fornece sugestões sobre como armazenar senhas adequadamente em bancos de dados (Memorized Secret Verifiers [173]), embora muitos softwares de servidor de código aberto populares não ofereçam segurança adequada por padrão [170] e uma série de violações de dados expuseram senhas armazenadas incorretamente [113] .

Vários métodos foram introduzidos para aumentar a robustez do processo de autenticação, especialmente em sistemas e aplicações críticas; sendo a mais conhecida a autenticação de dois fatores (2FA), também recomendada pela ENISA para melhorar a segurança das senhas [77] [5]. Durante um método 2FA, o usuário deve provar sua identidade com base em dois fatores e não em um. Por exemplo, para acessar uma conta web banking, além de fornecer o nome de usuário e a senha, o usuário também é solicitado a fornecer uma senha de uso único (OTP) que é recebida por meio de um serviço de mensagens curtas (SMS) para ser autenticado.
Embora este método melhore a segurança do processo de autenticação, carece de facilidade de utilização [148], o que é um factor importante no procedimento de autenticação, e também pode ser explorado através de ataques de troca de SIM (onde o adversário consegue clonar o cartão SIM do vítima, permitindo-lhe roubar o SMS) ou induzindo o utilizador a revelar o código OTP através de uma chamada, website ou e-mail falso (phishing).

5.2 Quem será afetado?

Qualquer pessoa que use um computador ou smartphone será afetada pela fraca segurança dos métodos de autenticação baseados em senha. No entanto, as pessoas com mais contas têm maior probabilidade de serem afetadas, uma vez que a superfície de ataque é mais ampla, ou seja, os invasores têm maiores chances de comprometer uma conta. Por exemplo, se Bob tiver uma conta (por exemplo, uma conta de e-mail) e Alice tiver três contas (por exemplo, e-mail, loja online e contas de streaming), então

um invasor pode ter como alvo Bob em um aplicativo, enquanto Alice pode ter como alvo três aplicativos diferentes. Além dos indivíduos, as empresas/organizações também podem ser afetadas, uma vez que se a conta protegida apenas por senha de um funcionário for comprometida, os dados corporativos poderão ser roubados ou software malicioso poderá ser plantado, resultando em risco para a reputação da empresa/organização. , o que levará à perda de dinheiro. Por último, mas não menos importante, os governos e as infraestruturas críticas serão os mais afetados, porque se um invasor obtiver acesso não autorizado, as suas ações maliciosas também poderão ter um efeito grave nos cidadãos europeus. Por exemplo, o comprometimento de uma rede eléctrica afectará significativamente o público.

5.3 O que se espera que aconteça?

Caso a autenticação de um sistema seja comprometida, não só os dados do usuário estarão em risco, mas também o invasor terá acesso ao sistema para realizar diversas ações maliciosas, como roubar informações ou documentos pessoais, instalar algum tipo de malware, ou realizar um ataque de Ameaça Persistente Avançada (APT). Assim, as consequências irão variar dependendo da criticidade do sistema e das ações do invasor. Na maioria dos casos, o comprometimento do processo de autenticação leva à violação de dados e à perda de dinheiro. Contudo, quando o processo de autenticação de uma infraestrutura crítica está em jogo, as consequências podem ser muito mais graves do que a perda de dinheiro.
O pior é que não podemos saber de antemão as ações maliciosas que um invasor realizará.

5.4 Qual é a pior coisa que pode acontecer?

A maioria dos nossos serviços digitais depende da autenticação segura dos utilizadores e, portanto, temos de garantir que utilizamos métodos de autenticação adequadamente seguros. Supondo que continuaremos a basear todos os nossos métodos de autenticação em senhas, eventualmente todos os sistemas serão comprometidos pelo menos uma vez. Todas as empresas serão afetadas por incidentes e violações de dados, resultando na perda de milhões de euros. Grandes quantidades de dados vazados de pessoas (por exemplo, e-mail, fotos, residência, número social, telefone, números de cartão de crédito, situação financeira, registros médicos, etc.) estarão disponíveis on-line para quem fizer o lance mais alto, afetando significativamente a privacid

As infra-estruturas críticas também serão profundamente afectadas. Tais infra-estruturas (como a rede eléctrica, sistemas de água, hospitais, comunicações telefónicas) ainda ligadas à Internet representarão possivelmente uma ameaça devido ao elevado risco de serem comprometidas. Os ataques cibernéticos terão como alvo esses sistemas, criando um elevado risco de espionagem, terrorismo cibernético ou mesmo perda d

5.5 Lacunas de Pesquisa

Para garantir que mantemos os módulos de autenticação adequadamente seguros, as ações precisam a serem tomadas nesta área.

5.5.1 Melhorar os métodos de autenticação sem senha

Embora métodos de autenticação sem senha — como o desbloqueio por impressão digital de nossos telefones — já estejam disponíveis (por exemplo, FIDO [6] e WebAu-thn [110]), há vários pontos que podem ser melhorados. Para começar, devemos garantir que a autenticação sem senha seja acessível a todos (através de nossos dispositivos pessoais, como smartphones ou computadores pessoais) de uma forma fácil de usar, mas segura, aumentando a adoção de métodos de autenticação sem senha (por exemplo, aumentar o número de aplicativos e sites que suportam login sem senha) e melhorar a interoperabilidade entre dispositivos autenticadores e serviços que exigem autenticação (por exemplo, usar o sensor de impressão digital do seu smartphone para autenticar no seu laptop).

Dado que vários métodos populares de autenticação sem palavra-passe dependem da biometria (por exemplo, leitura da íris, leitura da impressão digital, leitura do rosto), procurar garantir a segurança e a fiabilidade dos métodos de autenticação biométrica (por exemplo, reduzindo os falsos positivos quando uma entidade não autorizada pode ser falsamente identificada como um autorizado) e ao mesmo tempo respeitar a privacidade do usuário (por exemplo, armazenar localmente com segurança os dados relacionados à biometria apenas para uso para autenticar o usuário) é de grande importância, ao mesmo tempo que analisa como eles podem ser usados junto com a criptografia difusa (onde os dados biométricos podem ser usado como entrada para funções criptográficas). Além disso, a utilização de autenticação sem palavra-passe em cenários de autenticação avançada (por exemplo, autenticação multipartidária sem palavra-passe, onde a autenticação/autorização é realizada por mais de uma entidade) deve ser investigada, a fim de satisfazer necessidades especializadas que os métodos existentes não cobrem (por exemplo, permitir a autorização de uma transação ou a assinatura de um documento por 2 ou mais pessoas). Deveríamos também considerar novas abordagens de autenticação sem senha para uso on-line (por exemplo, login em um site on-line) e off-line (por exemplo, login em seu laptop). Por último, mas não menos importante, é necessário investigar a melhoria da autenticação dos utilizadores, aproveitando as tecnologias existentes (por exemplo, Single Sign On) e novos esquemas de identidade digital (por exemplo, identidade auto-soberana, identificadores descentralizados [219], credenciais verificáveis [220]). em combinação com autenticação sem senha (quando necessário), bem como recuperação segura ou mecanismos de fallback para uso quando o mecanismo de autenticação principal não estiver disponível (por exemplo, no caso de você perder seu smartphone ou sua chave de segurança USB).

5.5.2 Medir/monitorar o uso de métodos de autenticação inseguros

É de grande importância monitorizar o estado de segurança dos métodos de autenticação na Europa, medindo tanto a adoção de autenticação sem palavra-passe como a utilização de métodos de autenticação inseguros baseados em palavra-passe. Com Com uma melhor compreensão do problema, poderão ser tomadas medidas para reduzir o risco de segurança. Por exemplo, podemos introduzir novos regulamentos ou melhorar os existentes, visando sistemas críticos afectados pelo problema, bem como definir requisitos mínimos de segurança (por exemplo, certificação apropriada, avaliações de segurança e auditoria) para garantir um nível apropriado de segurança para proteger cidadãos europeus e a nossa sociedade como um todo. A pesquisa também poderia se concentrar em o lado econômico da questão e investigar se mecanismos de autenticação melhores e mais novos são acessíveis a todos os tipos de organizações ou se tais soluções tecnológicas não atendem aos requisitos.

5.5.3 Compreender a psicologia do usuário relacionada à autenticação

Uma importante lacuna de pesquisa está relacionada à psicologia humana e à autenticação. Mais pesquisas sobre a psicologia do usuário durante a autenticação deve fornecer mais informações relacionadas a ataques fraudulentos (ataques relacionados à engenharia social), bem como fornecer informações valiosas sobre o usuário percepção sobre a usabilidade de um mecanismo de autenticação.

5.5.4 Melhorar os métodos de autenticação biométrica utilizando métodos de IA

Métodos de autenticação biométrica, como impressão digital, reconhecimento facial e de voz, são amplamente utilizados em smartphones para fazer login de usuários sem senhas. No entanto, esses mecanismos apresentam suas próprias limitações. Para citar alguns, sujo as mãos afetarão o reconhecimento de impressões digitais, as condições climáticas, o reconhecimento facial, e reconhecimento de voz em ambientes barulhentos. Assim, mais pesquisas são necessárias para aliviar essas restrições. Uma abordagem poderia ser empregar métodos de IA, como aprendizado de máquina (ML) e aprendizado profundo (DL), na autenticação processo para aproveitar ao máximo os dados recebidos nos casos em que as condições não são ideais.

5.5.5 Autenticação contínua

As características únicas do usuário podem ser implantadas para autenticação sem precisando de sua interação. Por exemplo, no caso de um telemóvel, cada pessoa segura seu telefone de maneira diferente, digita de maneira diferente, desliza de ângulos diferentes, etc. Utilizando todos esses dados sobre o comportamento de cada pessoa e aproveitar a IA pode resultar em autenticação contínua sem o uso de senhas ou biometria. A investigação sobre este tema deverá centrar-se no aumento a precisão dos mecanismos de autenticação comportamental, ao mesmo tempo

reduzindo os falsos positivos e falsos negativos, ao mesmo tempo que analisa como
para preservar a privacidade e o controle do usuário.

5.5.6 Treinamento de pessoas em tópicos relacionados à autenticação

Existem vários métodos 2FA que podem ser usados hoje em combinação com
senhas para fornecer segurança adequada aos sistemas, mas a maioria dos usuários opta por não
para usá-los. A comunidade científica terá de analisar as razões
por que muitos usuários não habilitam a autenticação sem senha ou multifator
(MFA) e desenvolver treinamento eficiente de usuários para resolver o problema. Além disso,
embora existam várias recomendações sobre como lidar com senhas, ambas
usuários e engenheiros de software ainda não conseguem segui-los, resultando no manuseio
de forma insegura (por exemplo, os usuários continuam a compartilhar senhas, os engenheiros continuam
para armazenar senhas de forma insegura). Realizar treinamento relacionado (ou aumentar
sua eficiência) garantirá que todos tenham acesso e saibam como usar
mecânica de autenticação forte de maneira correta e fácil, minimizando o risco de
suas contas sendo comprometidas.

5.6 Exemplos de problemas

Exemplos de problemas tangíveis podem incluir:

Facilidade de uso. Devem ser realizadas pesquisas sobre como a facilidade de uso

A qualidade dos métodos de autenticação sem senha poderia ser melhorada. Separado
desde tornar os métodos mais fáceis de usar para o público em geral, novos métodos fáceis
a utilização de metodologias para transferir ou fazer backup de credenciais utilizadas por
dispositivos autenticadores devem ser testadas.

Transição de baseado em senha para sem senha. Em muitos casos, a transição para métodos

mais recentes de autenticação sem senha não é trivial, pois muitos
os sistemas não os suportam imediatamente. Além disso, os usuários não familiarizados
com a tecnologia sem senha podem enfrentar dificuldades na preparação
seu ambiente para usar os novos métodos de autenticação. Pesquisas futuras no tópico
podem investigar como introduzir a autenticação sem senha de uma forma amigável e
como uma camada de segurança que envolve o legado
sistema.

Resistência a ataques. Para garantir o nosso futuro, devemos também analisar a forma como

podem ser mitigadas e como as medidas podem ser integradas na nossa
métodos de autenticação sem senha. Em muitos casos, tais problemas
podem surgir como resultado de configuração insegura ou implementação defeituosa,
enquanto em outros casos estão entre as desvantagens do método selecionado (por
exemplo, alguns métodos de autenticação sem senha não são
resistente a phishing).

Autenticação fraca em dispositivos IoT. A introdução de dispositivos IoT em nossos vidas e sua interconexão e exposição à Internet criaram uma nova superfície de ataque para os invasores, ou seja, os invasores, além de visarem a autenticação do usuário, os invasores agora podem direcionar o processo de autenticação do dispositivo. Novos métodos de autenticação sem senha devem ser introduzidos para esses pequenos dispositivos inteligentes (por exemplo, câmeras IP acessíveis remotamente) que geralmente apresentam recursos limitados.

6 Conscientização e Treinamento em Segurança

6.1 Introdução

É amplamente reconhecido que a segurança cibernética organizacional depende de três pilares: nomeadamente, tecnologias, processos e pessoas. Além disso, transformar matérias-primas dados em informações elegíveis e informações em inteligência acionável, é um componente cada vez mais significativo para manter a consciência situacional cíber segurança.

As pessoas são frequentemente vistas como o elo mais fraco na cadeia de segurança cibernética [32] [164]. Embora esta caracterização negativa da natureza humana seja discutível [123], é inegável que o ser humano é um fator importante que contribui para o maioria das violações de segurança cibernética [128]. Os cibercriminosos frequentemente empregam técnicas, como a engenharia social, que exploram as fraquezas humanas inatas para realizar ataques e aumentar suas chances de sucesso.

O desenvolvimento de competências em segurança cibernética centra-se em permitir que as pessoas estabeleçam barreiras técnicas e operacionais às ameaças à segurança cibernética e se comportem adequadamente, através do processamento vigilante de ações acionáveis. inteligência. É um processo iterativo de melhoria contínua e incremental [249] direcionado para transformar o fator humano de um potencial vetor de ataque para um multiplicador de preparação organizacional para proteção contra, detectar, responder e se recuperar de ataques cibernéticos. Competência em segurança cibernética desenvolvimento é baseado em um continuum que expande a educação formal por meio de atividades de valor agregado, como i) experiência prática, ii) programas de conscientização e iii) programas de treinamento, com cada um desses multiplicadores servindo funções específicas na manutenção da higiene cibernética organizacional.

Aproveitar os fatores humanos na segurança cibernética vai além dos métodos tradicionais de treinamento e conscientização. Exige abordagens modernas que se baseiem na compreensão do comportamento humano e na implementação de ferramentas que forneçam treinamento e conscientização cibernética. Experiência prática (também conhecida como aprendizagem fazendo) é uma abordagem extremamente eficaz para ensinar e aprender segurança cibernética [213]. Envolve os alunos e melhora a compreensão do conhecimento e retenção, bem como a possibilidade de traduzir o conhecimento adquirido em ação [90]. Muitas estratégias de sucesso são usadas para esse propósito, incluindo exercitar habilidades de detecção e defesa de ataques cibernéticos em um ambiente de alcance cibernético

[42], participando de competições de segurança cibernética [162], participando de exercícios emblemáticos de segurança cibernética [55] e aprendendo por meio de jogos (por exemplo, jogos sérios) [207]. No entanto, a integração da sensibilização e formação em segurança cibernética apenas reduz, e não elimina, a possibilidade de negligência e erros humanos, o que implica que intervenções técnicas inteligentes para verificar e regular os erros dos funcionários continuam a ser vitais para a postura geral de segurança

6.2 Quem será afetado?

Conforme mencionado anteriormente, é amplamente reconhecido que a segurança cibernética assenta em três pilares: nomeadamente, tecnologias, processos e pessoas. Os humanos podem ser negligentes, propensos a erros e podem representar, intencionalmente ou não, um elo fraco [164]. Portanto, as tecnologias e os processos visam reduzir a carga ou a responsabilidade geral, automatizando e demarcando procedimentos, como vemos através da transformação digital em curso [161]. No entanto, são as pessoas que desenvolvem, operacionalizam e mantêm tecnologias e processos. Assim, embora as tecnologias e os processos constituam ferramentas essenciais para o reforço da segurança cibernética, o factor humano desempenha o papel mais crítico na garantia da higiene cibernética. Independentemente de quantas soluções de segurança tecnológica dispendiosas e sofisticadas tenham sido implementadas, estas não podem ser consideradas seguras enquanto os fatores humanos não funcionarem e se comporta Além disso, as soluções tecnológicas de segurança requerem a intervenção humana para um funcionamento adequado e eficaz: por exemplo, as firewalls devem ser activadas, o software deve ser actualizado e os avisos de segurança devem ser reconhecidos e postos em prática.

A falta de ênfase na sensibilização e formação em segurança tem ramificações pessoais, organizacionais e até nacionais, enquanto a melhoria da vigilância, ou a falta dela, permeia e se espalha entre as esferas pessoal e profissional. Vemos os efeitos em cascata da baixa conscientização e conhecimento em quase todos os tópicos e setores de segurança cibernética [179], desde implicações de privacidade até segurança de infraestrutura crítica [43]. O comportamento humano, na maioria das vezes, é o ponto fraco dos projetos e arquiteturas de segurança, apresentando aos potenciais invasores um caminho de menor resistência, se não um ponto de entrada claro, com um limiar técnico limitado. Portanto, o desafio não é determinar quem será afetado pela sensibilização e formação limitadas em matéria de cibersegurança, mas identificar quem não será afetado.

Deve também notar-se que o impacto global da transformação digital depende muito da aceitação das tecnologias digitais recentemente desenvolvidas, referindo-se tanto às que são desenvolvidas com foco na segurança cibernética como às que não o são. A sensibilização e a formação em matéria de cibersegurança podem facilitar a aceitação e a adoção de tecnologias digitais inovadoras pelas partes interessadas, uma vez que

melhora a compreensão dos riscos de segurança cibernética relacionados e desenvolve barreiras contra eles.

6.3 O que se espera que aconteça?

Sistemas automatizados e autônomos foram desenvolvidos em vários setores, incluindo segurança cibernética [161], para ajudar humanos ou mesmo para removê-los. do circuito. No entanto, este processo ainda está na sua infância, e mesmo em no desenvolvimento desses sistemas, as pessoas são os principais contribuintes [221]. Além disso, as melhores práticas de segurança cibernética foram desenvolvidas em todas as fases de engenharia de sistemas seguros, desde o planejamento até o descarte. No entanto, estes processos, quer se refiram a sistemas, políticas ou processos, incluem frequentemente dados que são influenciados pelo conhecimento especializado qualitativo [101], ou exigem compromissos para atender aos requisitos e restrições. A conscientização e o treinamento limitados em segurança cibernética representam as causas profundas das vulnerabilidades introduzidos nos sistemas, tecnologias, processos e políticas implantados. Isso ocorre em todas as fases do seu ciclo de vida, decorrente de diversos fatores, como falhas de projeto, erros de integração ou negligência operacional. O impacto e as consequências exactas só podem ser estimados caso a caso. No entanto, é fundamental reconhecer que a promoção da segurança cibernética direcionada conscientização e treinamento em um processo iterativo de desenvolvimento contínuo é essencial para garantir a ciber-higiene, a preparação e a resiliência.

6.4 Qual é a pior coisa que pode acontecer?

A extensão do potencial impacto e das consequências devido à sensibilização e formação limitadas em matéria de cibersegurança só pode ser estimada caso a caso. O A principal consideração a esse respeito tem a ver com o facto de a falta de competências relevantes ter um efeito de arrastamento na segurança cibernética e na resiliência dos tecnologias, sistemas, processos e políticas. Portanto, embora o impacto e as consequências dependem das especificidades de um incidente (por exemplo, setor, escopo, objetivos, capacidades do atacante), as limitações nas competências de segurança cibernética desempenham um papel crítico na probabilidade de ocorrência de um incidente e terá um impacto na eficácia das ações de resposta e recuperação tomadas. Por isso, é natural considerar a conscientização e o treinamento em segurança cibernética como um fator positivo ou multiplicador negativo em toda a higiene cibernética geral.

Os benefícios da conscientização e do treinamento em segurança cibernética vão além do detecção e mitigação de problemas de segurança cibernética [151]. Para começar, com profissionais qualificados funcionários que estão familiarizados com os princípios de segurança cibernética e entendem seu papel em manter o negócio seguro, o tempo de inatividade de sistemas críticos de negócios devido a falhas ou incidentes de segurança poderia ser evitado. Isso vai economizar organizações do processo caro e demorado de reparo e restabelecendo as operações comerciais normais. Em seguida, os funcionários que estão familiarizados

com os regulamentos de conformidade e ter uma compreensão clara de como lidar com dados e informações confidenciais podem ajudar a minimizar as infrações de conformidade regulatória e seu impacto negativo na reputação e nas finanças das empresas. Finalmente, as organizações que implementam medidas proativas de segurança cibernética e demonstraram que a resiliência cibernética aumenta a confiança do cliente.

Vejamos o impacto das violações de dados nas organizações para ter uma ideia melhor dos problemas que podem surgir como resultado da falta de segurança cibernética conscientização e treinamento. Consideramos as violações de dados como um exemplo simplesmente porque 82% das violações de dados envolveram um fator humano [240]. Essas violações ocorreu porque as pessoas foram vítimas de ataques sociais, e deliberadamente (uso indevido) ou inadvertidamente (erros) agiu ou deixou de agir quando necessário. Mais importante, eles poderiam ter sido evitados em maior medida se as pessoas envolvidos estavam devidamente conscientes e treinados em relação às suas operações e responsabilidades de segurança. Agora vamos avaliar o que poderia acontecer se há uma violação de dados em alguma organização. Quando se trata de dados hospitalares, um a violação pode pôr em risco e prejudicar a saúde e a segurança do paciente, ou seja, pôr em perigo a vida humana. No caso de dados de serviços financeiros, a sua violação pode resultar em uma enorme perda financeira. E no caso de dados governamentais, uma violação poderia comprometer a segurança nacional. Por último, mas não menos importante, independentemente do tipo de organização, uma violação de dados causaria uma perda de clientes e parceiros. confiança, diminuição da reputação no mercado, perda de negócios e penalidades impostas, o que pode levar à falência.

6.5 Lacunas de Pesquisa

6.5.1 Necessidades de conscientização e treinamento em segurança cibernética em todos os níveis e áreas de estudo

A digitalização contínua de produtos, serviços, cadeias de abastecimento e valor destaca a necessidade de aumentar a literacia técnica dos nativos digitais. Portanto, além de programas de estudo dedicados ao desenvolvimento de competências profissionais específicas (por exemplo, ciência da computação, engenharia de redes), módulos relevantes são integrados na maioria dos programas de estudo e níveis e campos de estudo [246]. No entanto, os temas relacionados com a segurança cibernética dificilmente são introduziu programas externos que são particularmente direcionados ao desenvolvimento de profissionais de segurança cibernética.

Assim, é essencial identificar as aptidões e competências de cibersegurança necessárias, bem como os métodos de ensino adequados, desde o ensino primário até ao ensino superior e áreas de estudo especializadas.
Isto requer examinar os componentes universais relacionados com a segurança cibernética que visam aumentar a sensibilização do público em geral para a segurança cibernética,

bem como tópicos especializados específicos para ocupações distintas. Além disso, requer a avaliação de mecanismos de entrega que sejam ajustados e otimizado em relação aos atributos dos grupos-alvo relevantes.

6.5.2 A conscientização e o treinamento em segurança cibernética exigem investigações de abordagem multidisciplinar

Foi e é apropriado neste momento perguntar: “Por que a conscientização e o treinamento em segurança cibernética não estão produzindo os resultados esperados?” [22] A questão tem sido objeto de inúmeras investigações, mas nenhuma resposta clara foi encontrado ainda. Isto pode ser resultado da perspectiva estreita ou limitada de que vemos a questão.

A conscientização e o treinamento em segurança cibernética giram principalmente em torno da compreensão e da transformação do pensamento e do comportamento humanos, que são, sem dúv temas complexos. Portanto, enquanto os pesquisadores e profissionais de segurança cibernética tentarem especificar e controlar o pensamento e o comportamento humanos por meio de um pequeno conjunto de motivadores, que a maioria dos psicólogos e cientistas sociais consideraria considerar enganosa, a probabilidade de sucesso na conscientização e na segurança cibernética o treinamento provavelmente permanecerá baixo [22]. Isto também implica que abordar o problema questão exigiria uma abordagem mais abrangente e holística que utilizasse conhecimento e experiência de diversas disciplinas, incluindo engenharia, pedagogia, economia comportamental, marketing e psicologia social, cognitiva e organizacional, entre outros.

6.5.3 A conscientização e o treinamento em segurança cibernética baseados em computadores precisam da implementação de algoritmos de IA e ML para fins de automação

Quase não existem disciplinas que não utilizem as capacidades da inteligência artificial (IA) e do ML, ou pelo menos tentem fazê-lo. Cíber segurança a sensibilização e a formação não podem ser uma exceção. Na verdade, existem numerosos maneiras pelas quais a IA e o ML podem ser úteis para elevar o padrão e o impacto do conscientização e treinamento em segurança cibernética [207].

Ao utilizar algoritmos de IA e ML, muitas atividades de conscientização e treinamento em segurança cibernética poderiam ser automatizadas. A automação ajudaria a alcançar conscientização e treinamento sob demanda em segurança cibernética. Além disso, eles poderiam facilitar a concepção e a entrega de uma experiência de sensibilização e formação mais personalizada, personalizada e optimizada para o público. Por exemplo, IA e testes baseados em computador assistidos por ML poderiam ser desenvolvidos e usados para identificar grupos vulneráveis. Além disso, com base nos resultados dos testes, e mais uma vez com a aplicação de algoritmos de IA e ML, mais customizados, personalizados e recursos otimizados de conscientização e treinamento poderiam ser preparados para o público.

6.6 Exemplos de Problemas

Exemplos de problemas tangíveis podem incluir:

Módulos de treinamento e conscientização sobre segurança cibernética da IoT O uso da tecnologia da Internet das Coisas (IoT) está se expandindo diariamente em todas as esferas dos negócios e da sociedade, desde bens e serviços voltados ao consumidor até a IoT industrial. Isto também introduziu riscos de segurança e privacidade sem precedentes [23]. A maioria das implantações de segurança de IoT ocorre no nível da unidade de negócios, onde a TI participa, embora de forma insuficiente. Isto também implica que vários intervenientes importantes na segurança da IoT não estão familiarizados com o lado da segurança de TI. Para agravar ainda mais a situação, os riscos relacionados com a IoT muitas vezes não são bem articulados, resultando numa baixa sensibilização entre utilizadores e funcionários. Assim, a segurança da IoT não pode ser robusta se as pessoas envolvidas não tiverem um bom entendimento, e isso exige que tenham a conscientização e o t

Conscientização sobre ataques adversários de IA Ao contrário do uso de métodos de IA/ ML para fortalecer a segurança cibernética, os atores de ameaças estão aproveitando métodos de IA/ML para fins maliciosos, por exemplo, para aumentar o número de superfícies de ataque e reforçar suas capacidades de ataque [154].

Métodos adversários de IA são usados para criar dados ou comportamentos enganosos com a intenção de manipular e interromper sistemas críticos de IA. Há evidências crescentes de que métodos adversários de IA foram implementados em ataques no mundo real. Apesar disso, o esforço para defender os sistemas de IA contra ataques adversários de IA é geralmente uma reflexão tardia. É lamentável que muitas empresas ainda não tenham conhecimento dos ataques adversários de IA e da falha dos sistemas de IA que os ataques podem causar. Portanto, é urgente aumentar a sensibilização das empresas para os ataques adversários de IA e motivá-las a estarem alertas e preparadas para defender os seus sistemas de IA, especialmente aqueles utilizados em setores cruciais, contra os ataques.

Módulos de conscientização e treinamento em segurança cibernética para usuários móveis O telefone celular ganhou ampla aceitação como uma ferramenta comum para acessar a Internet e realizar trabalhos delicados. Estas podem ser as causas do aumento diário de ataques cibernéticos e crimes dirigidos a utilizadores de telemóveis [200] [31]. No entanto, a sensibilização e a formação adequadas em matéria de cibersegurança para utilizadores de telemóveis ainda são raras. Existe uma suposição comum de que o uso do telefone celular é semelhante ao uso de um desktop ou laptop, o que é apenas parcialmente correto. Na verdade, eles compartilham algo em comum como dispositivos de computação; no entanto, ao mesmo tempo Por exemplo, os telemóveis apresentam um risco mais elevado de roubo ou perda, a autenticação utilizada para bloquear um telemóvel é muitas vezes fraca como resultad

a alta frequência de logins em telefones celulares e o tamanho menor da tela dos telefones celulares muitas vezes dificultam a percepção de avisos de segurança. Além disso, os usuários de telefones celulares são muito mais diversos do que os de laptops ou desktops. Pessoas de diversas origens, desde urbanas a rurais, de instruídas a não instruídas, de colarinhos brancos a operários, e assim por diante, usam telefones celulares. Não houve muitas investigações sobre por que e como esses diversos indivíduos usam um telefone celular e quais podem ser suas expectativas em relação à conscientização e treinamento em segurança cibernética.

Avaliação de conscientização e treinamento em segurança cibernética com foco na mudança comportamental.

As avaliações da conscientização e do treinamento em segurança cibernética são frequentemente restritas à avaliação do conhecimento de segurança e às mudanças de atitude relatadas pelo Na verdade, a melhoria do conhecimento e da atitude é importante, mas a avaliação deve realmente medir a mudança no comportamento em matéria de cibersegurança; afinal, a mudança de comportamento é o que os programas de sensibilização e formação pretendem alcançar em última análise [39]. Os estudos que examinam o comportamento real da cibersegurança são pouco comuns (a maioria dos estudos limita-se frequentemente à avaliação da intenção) e aqueles que o fazem são frequentemente incompreensíveis e incompletos. Lamentavelmente, embora estejam a ser discutidos numerosos componentes de sensibilização e formação em segurança cibernética, ainda não existe um método adequado e fiável para medir as mudanças comportamentais em segurança cibernética.

7 Execução Confiável

7.1 Introdução

Nas últimas duas décadas, quase todos os aspectos da vida quotidiana das pessoas e de todas as áreas da actividade humana foram permeadas e revolucionadas pela tecnologia digital. Setores vitais para a sociedade e as nações, como a economia, a indústria, a cultura, a saúde, os setores sociais e As atividades governamentais, hoje em dia, utilizam enormes quantidades de software para entregar seus serviços, beneficiando-se de vantagens indiscutíveis em termos de tempo, custo e eficiência. No entanto, os sistemas de TI são vulneráveis a um grande número de ataques cibernéticos, que estão crescendo constantemente em número e gravidade, portanto, software confiável execução é o objetivo que a indústria e a academia buscam para proteger a TI sistemas e seus dados confidenciais contra ataques de crimes cibernéticos.

Tradicionalmente, mecanismos de isolamento de hardware foram introduzidos para fornecer vários mecanismos de proteção: espaços de endereço virtual e unidades de controle de memória protegem as aplicações dos usuários umas das outras, instruções privilegiadas proteger o software do sistema contra aplicativos do usuário e virtualização de hardware cria ambientes de execução isolados e protegidos uns dos outros. No entanto, as aplicações do usuário permanecem desprotegidas pelo software privilegiado do sistema operacional e do hipervisor, composto por milhões de linhas de código que hospedam um número muito alto de bugs [53, 88], exploráveis por invasores para obter privilégios acesso à plataforma [187].

Este cenário é ainda mais complicado pelo advento da computação em nuvem, hoje cada vez mais utilizado pelas empresas devido ao seu indiscutível vantagens. Neste caso, os aplicativos do usuário devem confiar na honestidade do provedor de infraestrutura, os funcionários com contas privilegiadas ou físicas acesso aos nós da nuvem e aos outros locatários que executam suas cargas de trabalho a mesma plataforma.

Ambientes de Execução Confiáveis (TEEs) foram introduzidos para permitir que aplicativos de usuários sensíveis à segurança, ou as partes mais críticas deles, confiem apenas

o suporte de hardware para o TEE mais uma camada de software que é executada isoladamente e constitui a Base de Computação Confiável (TCB) para a aplicação. O menor o TCB e melhor sua segurança, pois isso reduz o ataque superfície e o número provável de vulnerabilidades. Os TEEs também protegem as aplicações contra invasores físicos, por exemplo, aqueles que podem ler dados confidenciais carregado claramente na RAM da plataforma. Essa proteção é alcançada por por meio de camadas criptográficas que protegem os dados enquanto eles são processados.

Na década de 2000, o Trusted Computing Group (TCG) propôs o Trusted Platform Module (TPM) como um coprocessador seguro para executar serviços específicos definido pelo TCG, visando principalmente a verificação do estado de integridade da plataforma e a proteção de chaves privadas contra acessos não autorizados. Contudo, o TPM não se destina a executar aplicações arbitrárias em seu ambiente isolado, nem pode ser instalado em qualquer tipo de dispositivo. Encontrar a necessidade de proteger códigos e dados de usuários arbitrários, o mundo da indústria começou a trabalhar para a criação de soluções TEEs baseadas em modos especiais de segurança do processador principal, sendo o primeiro o TrustZone [17], proposto em 2002 pela ARM, seguida em 2014 pela Intel com Software Guard Extensions (SGX) [119], e em 2016 pela AMD com Secure Encrypted Virtualization (SEV) [125]. No ao mesmo tempo, a academia também procurou soluções de software adequadas para criar ETEs, entre os quais encontramos AEGIS [225], proposto em 2003, Bastion [37] em 2010, Sanctum [54] em 2016 e Keystone [138] em 2020.

Apesar das melhorias introduzidas pelas soluções TEE para buscar soluções confiáveis execução de software por meio de TCB menor e forte isolamento, alcançar a segurança depende não apenas da tecnologia TEE adotada, mas também da confiabilidade do código da aplicação que roda dentro dela. Identificar vulnerabilidades presentes no código em execução no TEE, bem como detectar seu comprometimento em tempo de execução, constituem desafios que os atuais TEEs de última geração enfrentam. não abordam, mas precisam ser considerados pela comunidade científica nos próximos anos [166].

7.2 Quem será afetado?

À medida que os sistemas de TI estão se tornando mais difundidos, distribuídos e vitais no mundo atual, não há nenhum setor da nossa sociedade que possa viver sem confiança em a execução de seus componentes de software e proteção de dados confidenciais.

É claro que existe uma escala relativa de importância. Se os indivíduos não forem oferecem execução confiável em seus sistemas pessoais, então os riscos são limitados aos ativos desse indivíduo específico. Por outro lado, se o sistema informático da uma empresa comercial ou um órgão governamental não apoia a execução confiável, então os riscos são muito maiores, dependendo da área de aplicação do o sistema afetado. Em particular, esses grandes sistemas são os alvos preferidos para ataques de ransomware (ou seja, um malware que criptografa dados e pede resgate

para descriptografá-los) e injeção de APT (Ameaça Persistente Avançada, ou seja, um aplicativo malicioso permanente que permanece oculto para exfiltrar informações continuamente ou aguardar um momento crítico para realizar um ataque destrutivo). A recuperação do ransomware pode levar muito tempo, de dias a meses (observe que pagar o resgate não é garantia de ter todos os dados de volta). Os APT são ainda mais insidiosos, pois podem passar despercebidos durante anos.

7.3 O que se espera que aconteça?

Se os componentes de software forem executados sem a proteção adequada, os resultados gerados não serão confiáveis para qualquer finalidade. Portanto, qualquer tipo de dano pode ser esperado.

Se usado em um sistema de controle industrial (ICS), a produção pode ser bloqueada ou os produtos podem ser fabricados de maneira errada, eventualmente levando a defeitos ou danos em outros sistemas que utilizam esses produtos como componentes.

Se o elemento de software atacado for um aplicativo que manipula dinheiro (direta ou indiretamente) (como um aplicativo de banco pela Internet ou um sistema de pagamento de uma empresa), então podem ser esperadas perdas financeiras.

A execução confiável é particularmente importante para sistemas ciberfísicos que interagem com humanos. Por exemplo, é o caso dos sistemas de controlo de tráfego ferroviário ou aéreo ou dos veículos autónomos. A injeção de malware ou a modificação da configuração desses sistemas pode causar danos físicos às pessoas, até mesmo a morte.

Outro cenário possível diz respeito ao roubo de dados sensíveis dos usuários, como identidade digital, credenciais bancárias ou planos comerciais. Se essas informações não forem devidamente protegidas e utilizadas em ambientes de execução confiáveis, ficam vulneráveis ao roubo por um invasor, que pode usá-las para se passar por outra pessoa para obter dinheiro ilegalmente por meio de transações bancárias não autorizadas, cometer fraudes, desacreditar ou colocar uma pessoa em uma situação difícil. má luz, realizando ações ilegítimas em seu nome.

No domínio da espionagem comercial, as empresas podem sofrer danos económicos e de imagem consideráveis se os atacantes conseguirem roubar dados de clientes ou informações confidenciais, relacionadas com processos de produção ou novos projetos dos quais depende o desenvolvimento futuro da empresa, trazendo assim vantagens ilícitas para empresas concorrentes. .

7.4 Qual é a pior coisa que pode acontecer?

As piores consequências possíveis dependem da aplicação controlada pelo sistema visado pelo invasor. Portanto, é óbvio que quanto mais crítico o sistema e pior o efeito do ataque.

O estudo "Cost of a Data Breach Report 2022" [116] mostra que ran-somware e ataques destrutivos representaram 28% das violações contra o

infra-estruturas críticas examinadas, destacando que os atacantes pretendem interromper os serviços financeiros e danificar organizações industriais, de transportes e de saúde. A criticidade destas infraestruturas exige a adoção de técnicas de segurança de ponta, como a criação de ambientes de execução confiáveis e a deteção atempada de qualquer violação do código e configuração dos sistemas.

Por exemplo, no caso de um grupo de atacantes conseguir bloquear a rede eléctrica de um país, milhões de famílias ficariam no escuro, a produção das empresas seria bloqueada, as comunicações seriam cortadas, os bancos ficariam offline, os hospitais seriam Se não fosse possível garantir cuidados de saúde, o tráfego aéreo e ferroviário pararia. Um desses ataques ocorreu em dezembro de 2015 na Ucrânia, quando três empresas de serviços públicos foram atacadas simultaneamente pelo malware BlackEnergy, deixando centenas de milhares de casas sem eletricidade durante seis horas. Outro ataque de considerável gravidade ocorreu no Irão em 2010, quando o programa nuclear iraniano foi bloqueado devido à sabotagem da central de enriquecimento de Natanz através do vírus Stuxnet, que provocou a destruição das centrífugas da central ao mesmo tempo que impediu a detecção do mau funcionamento do próprio sistema. A execução do aplicativo crítico que supervisiona a operação das centrífugas dentro de um TEE o teria protegido contra um vírus que infecta o Rich OS.

Este último ataque é um exemplo claro do que é o pior cenário: a aplicação maliciosa injetada não se limita a bloquear o comportamento normal do sistema, mas subverte-o completamente para realizar operações erradas que danificariam diretamente o próprio sistema ou as pessoas que o utilizam. .

7.5 Lacunas de Pesquisa

Nas últimas duas décadas, muito trabalho tem sido feito para construir ambientes de execução capazes de garantir confidencialidade e integridade à execução e permitir que entidades externas avaliem o nível de confiabilidade dos sistemas. No entanto, os próprios TEE colocam novos desafios que precisam de ser enfrentados pela comunidade científica.

7.5.1 Vetores de ataque contra garantias de segurança do TEE

Um TEE pode ser exposto a vulnerabilidades típicas de software, com a adição de vulnerabilidades arquitetônicas nativas de uma solução TEE específica. Um TEE deve ter um TCB pequeno com uma interface estreita para minimizar a superfície de ataque. Ao longo dos anos, diversas vulnerabilidades estruturais e de software foram encontradas em implementações específicas de TEE. No entanto, equipes mais experientes estão desenvolvendo TEEs menores e mais seguros, graças à adoção escrupulosa das melhores práticas de desenvolvimento de software seguro e à validação rigorosa do design e do código do TEE. Isso fez com que os invasores mudassem

ataques sofisticados na fronteira entre hardware e software [197]. Um importante área de pesquisa para os próximos anos será o estudo de ataques microarquiteturais de canal lateral, ou seja, ataques que exploram informações vazamento da infraestrutura de hardware para revelar informações confidenciais, como como chaves privadas.

7.5.2 Mecanismos de proteção contra aplicações TEE comprometidas

Os TEEs representam uma solução tecnológica válida para executar cargas de trabalho em um ambiente protegido. No entanto, se o código do aplicativo implantado neles contiver vulnerabilidades, eles poderão ser explorados por um invasor para comprometer a segurança de todo o TEE. Este problema está se tornando cada vez mais concreto, e sua solução mais urgente, porque os desenvolvedores começam a usar TEEs para executar aplicações complexas contendo uma grande base de código, portanto aumentando a probabilidade de bugs exploráveis estarem presentes no TEE. Isto também foi observado que os recursos de segurança dos próprios TEEs podem ajudar os invasores a instalar rootkits furtivos de nível superior que são extremamente difíceis de detectar através dos mecanismos de defesa atuais [166]. Por exemplo, as ferramentas antivírus em execução no sistema operacional não conseguem detectar códigos maliciosos aninhado em um TEE porque, por design, o sistema operacional não pode acessar a memória do TEE, que muitas vezes também é criptografado.

Pelo que foi dito, a segurança de um TEE não pode ser dada como certa porque é um assunto complexo, não garantido apenas por uma arquitetura perfeita design e implementação. Portanto a criação de soluções capazes de detectar bugs no código da aplicação desenvolvida para um TEE e monitorar sua confiabilidade em tempo de execução representa uma importante área de pesquisa.

7.5.3 TEEs e computação em nuvem: desafios de interoperabilidade e gestão lentes

Alguns dos principais fornecedores de infraestrutura em nuvem incluíram TEEs em seus oferta de serviços, uma vez que os TEEs são capazes de melhorar as garantias de segurança e privacidade da computação em nuvem. No entanto, dois modelos de TEEs conceitualmente diferentes pode ser adotado para computação em nuvem [94]: o modelo baseado em máquina virtual criptografa toda a memória do sistema de uma máquina virtual; o processo baseado O modelo criptografa seletivamente uma zona de memória do aplicativo implantado, delegando ao desenvolvedor a decisão de escolher qual seção do código de um aplicativo proteger. Implementações concretas desses modelos foram desenvolvido para diferentes plataformas – SGX e a nova extensão de domínio confiável (TDX) para plataformas Intel, SEV e o próximo Secure Nested Paging (SNP) para plataformas AMD, TrustZone e Realms para ARM – e arquiteturas de CPU (x86, RISC-V, ARM). A grande variedade de propostas apresentadas pela pesquisa e indústria causa problemas de interoperabilidade ao mover um serviço de um local

arquitetura para outra e problemas de compatibilidade na implantação de aplicativos escrito para sistemas tradicionais dentro de TEEs. Uma importante área de pesquisa é o estudo e desenvolvimento de frameworks que oferecem um nível de abstração capaz de tornar transparente a heterogeneidade das soluções TEE para o desenvolvedor da aplicação, mantendo as mesmas garantias de segurança oferecidas pelo TEE subjacente.

Outro aspecto que ganha cada vez mais importância é o desenvolvimento de soluções que permitam combinar tecnologias TEE com contentores tecnologias, a fim de promover o uso de TEEs em cenários nativos da nuvem e facilitar a implantação de aplicações baseadas em TEEs dentro de contêineres, em ao mesmo tempo, oferecendo a mesma experiência de usuário que os contêineres comuns e um integração suave com o ecossistema Kubernetes.

7.5.4 Primitivas criptográficas dos TEEs na era pós-quântica

Nos últimos anos, temos testemunhado avanços notáveis no campo dos computadores quânticos, que nos permitem levar as capacidades computacionais muito além das clássicas. Isso inevitavelmente causou consequências importantes em o campo da criptografia, pois os computadores quânticos permitem a execução de algoritmos que oferecem velocidade quântica à solução dos problemas matemáticos nos quais se baseiam os criptossistemas clássicos. Esta ameaça foi destacada com o apelo do NIST, em 2016, para apresentar novos algoritmos criptográficos resistentes a ataques de computadores quânticos. Em julho de 2022, o NIST selecionou os primeiros quatro algoritmos que se tornarão parte do padrão criptográfico pós-quântico do NIST [168]: CRYSTALS-Kyber para criptografia geral, CRYSTALS-Dilithium, FALCON e SPHINCS+ para assinaturas digitais.

Os TEEs baseiam sua segurança em primitivas criptográficas implementadas no raiz de confiança do hardware da plataforma, atualmente baseada em criptossistemas clássicos. Uma importante área de investigação para os próximos anos será a concepção e implementação de raiz de confiança de hardware baseada em criptografia pós-quântica, a fim de resistir à computação quântica e ao canal lateral quântico ataques.

7.6 Exemplos de problemas

Exemplos de problemas tangíveis podem incluir os seguintes:

Detectando um aplicativo TEE comprometido. Uma aplicação rodando em um TEE pode ser comprometido por um invasor devido à presença de vulnerabilidades em seu código. As fortes garantias de segurança e isolamento oferecidas por TEEs podem ser explorados por invasores para implementar e instalar rootkits avançados difíceis de detectar em uma plataforma [166]. Objetivo da pesquisa é desenvolver soluções capazes de detectar aplicações TEE comprometidas em tempo de execução.

Soluções TEE independentes de tecnologia em computação em nuvem. Em 2019, um grupo de empresas, incluindo Intel, Microsoft, Google e ARM, fundaram o Consórcio de Computação Confidencial (CCC) com o objetivo de promover a adoção de soluções TEE na Cloud. O CCC patrocina vários projetos de código aberto que oferecem soluções para os problemas de compatibilidade e interoperabilidade que as tecnologias TEE representam, como Enarx [70], Gramine [98] e Occlum [172]. O objetivo desta pesquisa é analisar a eficácia das atuais soluções de computação confidencial independentes de tecnologia, avaliar seu desempenho, estudar suas possíveis deficiências de segurança e aplicá-las ao domínio da computação em nuvem.

Aplicações TEE em cenários nativos da nuvem. Hoje, muitos prestadores de serviços oferecer soluções técnicas para facilitar o desenvolvimento e execução de Aplicações TEE no Asylo [97] da nuvem e no OpenEn-clave do Azure [21] são dois exemplos importantes deles. No entanto, enquanto eles simplificar o desenvolvimento de aplicações baseadas em TEE, eles ainda exigem o desenvolvedor adquira novas habilidades de programação e desenvolva o código usando os SDKs correspondentes. Além disso, embora o objetivo dessas estruturas é apoiar TEEs heterogêneos usando o mesmo API, eles ainda dependem principalmente da tecnologia Intel SGX. O objetivo do pesquisa é projetar e desenvolver soluções que permitam aos usuários executar seus serviços dentro de "contêineres baseados em TEE", sem necessidade de modificações ao código do aplicativo, ao mesmo tempo em que oferece suporte a back-ends TEE heterogêneos e fornecendo fácil integração com o orquestrador Kubernetes.

Execução confiável em dispositivos IoT de baixo custo. Hoje em dia, a segurança dos dispositivos IoT é essencial, uma vez que são cada vez mais utilizados em vários campos (por exemplo, veículos, indústria, cidades inteligentes, saúde). No entanto, os sistemas Io desafios especiais de segurança devido à sua heterogeneidade, considerando não apenas os dispositivos embarcados, mas também as redes, o gerenciamento e serviços de análise de dados e armazenamento. Além disso, embora de alta /dispositivos intermediários podem se beneficiar das garantias de segurança oferecidas por TEEs, dispositivos de baixo custo, normalmente não possuem mecanismos de segurança de hardware para proteger aplicativos sensíveis à segurança. Uma área de pesquisa no O campo IoT diz respeito ao design de arquiteturas TEE que atendam aos desafios colocados por dispositivos de baixo custo e baixo consumo de energia, para garantir a confiabilidade de uma gama mais ampla de aplicações IoT e dos dados que elas produzem. Isto deverá acompanhar o desenvolvimento de soluções para uma gestão remota e automatizada segura dos dispositivos IoT, muitas vezes instalados em ambientes não controlados.

Integração das funções de segurança da TEE na rede. O objetivo da pesquisa é a integração de tecnologias TEEs dentro da rede comum de operações

mecanismos operacionais e o reforço da sua segurança graças às garantias de hardware e software da TEE. Por exemplo, um aspecto importante diz respeito à criação de canais mutuamente confiáveis entre aplicações baseadas em TEE, alargando o protocolo TLS com mecanismos que permitam a verificação da integridade e autenticidade dos endpoints do canal de comunicação, portáveis para TEEs heterogéneos.

Raízes de confiança resistentes à quântica para TEEs. OpenTitan [177] é uma estrutura de código aberto que suporta o design e a integração de raízes de confiança de silício independentes de fornecedor e plataforma para integração em servidores, dispositivos de armazenamento, periféricos ou outros tipos de plataformas. O objetivo desta pesquisa é realizar uma extensão OpenTitan capaz de usar criptografia pós-quântica no projeto de silício e implementação de firmware de uma raiz de confiança, a fim de suportar TEEs resistentes a quantum.

Detecção em tempo de execução da manipulação das condições do sistema Alterar a configuração correta na qual um chip deve operar pode levar a um comportamento inesperado do software ou a alterações no fluxo de execução do código; isso normalmente é conseguido modificando fisicamente a potência do dispositivo, o relógio, o campo eletromagnético ou as interfaces físicas [197].
O objetivo desta pesquisa é a criação de mecanismos de tempo de execução capazes de enviar alertas dinamicamente quando for detectada uma mudança nas condições do sistema.

8 Privacidade desde o projeto

8.1 Introdução

Num mundo cada vez mais digitais, grandes quantidades de dados pessoais os dados são coletados e processados, muitas vezes de forma onipresente e intransparente, e usado pelos governos e/ou comercializados entre diversos prestadores de serviços, corretores de dados e anunciantes. Esta mercantilização de dados pessoais tem corroeu ainda mais os direitos dos indivíduos à privacidade. Durante muitas décadas, pesquisadores investigaram isso crescente tendência orwelliana de criação de perfis e vigilância, tentando encontrar um equilíbrio entre os avanços em tecnologia e na proteção de privacidade. Visando o cerne da o design dos sistemas, Ann Cavoukian cunhou o termo Privacidade desde o Design (PbD) na década de 90, propondo um uma série de sete princípios fundamentais, incutindo a garantia de privacidade como o modo de operação padrão de uma organização [35] (ver Figura 8.1). Atrás destes princípios é também a observação de que a privacidade é melhor alcançada quando abordada nos estágios iniciais do desenvolvimento tecnológico, ou seja, no projeto conceitual Estágio.

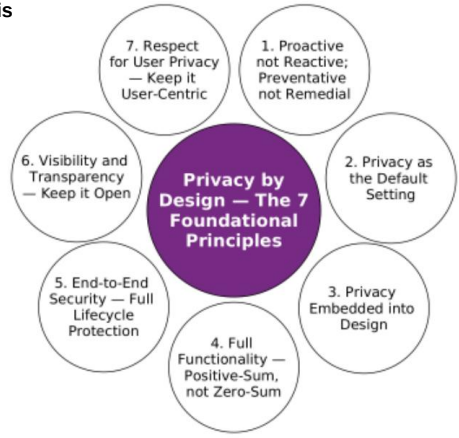


Figura 8.1: Os 7 Princípios Fundamentais do PbD de Cavoukian [35]

Embora aclamado por muitos investigadores e decisores políticos, o PbD é frequentemente criticado por ser demasiado vago e difícil de traduzir em software concreto. práticas de engenharia [239]. Na verdade, hoje ainda existe uma lacuna significativa entre a pesquisa e a prática, por exemplo, na tradução dos princípios de alto nível do PbD em práticas concretas de engenharia que os profissionais de software podem efetivamente e adotar com eficiência. Com o objetivo de colmatar esta lacuna, a disciplina emergente da Privacidade

Foi formada uma engenharia que se concentra em projetar, implementar, adaptar e avaliar teorias, métodos, técnicas e ferramentas para sistematicamente capturar e abordar questões de privacidade no desenvolvimento de sistemas sociotécnicos [102]. Portanto, desenvolver ainda mais esta área de Engenharia de Privacidade é um desafio significativo para pesquisadores, bem como para organizações que desejam integrar e operacionalizar o PbD. Para as organizações, este desafio é também um questão de conformidade regulatória agora que as noções de proteção de dados desde a concepção e proteção de dados por padrão foram incorporadas como parte do Regulamento Geral Europeu de Proteção de Dados (RGPD), em vigor desde 2018.

8.2 Quem será afetado?

Conforme mencionado, o GDPR elevou o padrão de privacidade, incluindo o PbD como parte do Artigo 25 “Proteção de dados desde a concepção e por padrão” para proteger os direitos fundamentais dos indivíduos na Europa. Este regulamento afecta todos organizações que recolhem e processam dados pessoais de cidadãos e residentes da UE, o que significa que pode ser aplicado mesmo que uma organização esteja sediada fora da UE. No entanto, a legislação deixa em aberto quais medidas de proteção técnicas e organizacionais exatas devem ser tomadas para cumprir os requisitos da PbD.
Isto, claro, cria desafios adicionais para as organizações, mas mais especificamente, para os arquitetos e desenvolvedores de software, que são os responsáveis finais. para projetar os sistemas.

Além disso, grandes organizações de tecnologia começaram a contratar serviços de privacidade engenheiros e estabelecer operações de equipe vermelha de privacidade, que ajudam a incorporar a privacidade no design do sistema e testar proativamente processos e sistemas para identificar riscos de privacidade. No entanto, não são muitas as organizações que têm a capacidade recursos para contratar engenheiros de privacidade, muito menos para manter toda uma privacidade Departamento de Engenharia. Pelo que vemos, este é especialmente o caso de pequenas e médias empresas que constituem a maioria das organizações hoje em dia.
Embora os efeitos práticos do GDPR sejam benéficos para os indivíduos e para a sociedade como um todo, representam desafios significativos para as organizações e, por sua vez, para a comunidade de pesquisa que visa fazer do PbD um realidade em um cenário tecnológico em constante mudança.

8.3 O que se espera que aconteça?

No nosso dia a dia estamos rodeados de tecnologia, com uma vasta gama de sistemas de software com uso intensivo de dados usados para atividades pessoais e profissionais. Não conseguir cumprir o PbD nos sistemas de trabalho atuais pode comprometer os indivíduos e a sociedade democrática como um todo [205]. A falta da privacidade tem impactos negativos para os indivíduos, desde constrangimento e danos à reputação devido a diversas formas de discriminação que afetam negativamente os direitos e liberdades dos indivíduos e a saúde física e mental. Com um

No nível social, a privacidade também é considerada um componente essencial para o funcionamento de uma sociedade democrática [26, 69]. Se as pessoas não puderem exercer plenamente os seus direitos e liberdades, tais como a liberdade de associação (por exemplo, política e religiosa) e a liberdade de opinião e expressão (incluindo a restrição das próprias opiniões), haverá impactos negativos na participação democrática dos indivíduos, prejudicando também a sua capacidade humana. dignidade e autonomia pessoal.

Por tais razões, espera-se que as organizações criem e adaptem de forma responsável sistemas de software seguindo os princípios PbD, aderindo aos direitos de privacidade consagrados nas regulamentações atuais. Como resultado, as pessoas poderiam considerar a privacidade como garantida, com a plena expectativa de que quaisquer dados recolhidos e processados tenham sido adquiridos legalmente, que as finalidades específicas do processamento sejam comunicadas e respeitadas de forma transparente, e que quando-sempre que possível, os utilizadores podem exercer vários direitos sobre os seus dados, por exemplo, acesso, correção, eliminação, tratamento de objetos, etc.

8.4 Qual é a pior coisa que pode acontecer?

O GDPR é por vezes referido como um regulamento que tem “verdadeira força”, aplicando multas pesadas a organizações que violam os direitos de privacidade. O incumprimento do RGPD pode levar a multas até 20 milhões de euros ou até 4% do volume de negócios anual mundial de uma organização, consoante o que for mais elevado. Estudos mostram um número crescente de multas baseadas no GDPR desde a sua publicação em 2018 [190.250], com a maior multa até agora de 746 milhões de euros imposta pela Autoridade de Proteção de Dados do Luxemburgo contra o gigante tecnológico Amazon em julho de 2021 [141] .

No entanto, pode-se argumentar que os custos sociais colectivos das violações da privacidade podem ser muito mais elevados do que quaisquer multas legais. Como mencionado, a deterioração dos direitos individuais à privacidade incorre no próprio enfraquecimento da democracia. Se não forem controladas, as organizações podem explorar tecnologias avançadas, como a inteligência artificial, para elaborar e direcionar cuidadosamente os anúncios, gerando um cenário de manipulação social [147]. Evidências desse uso explorador de perfis de usuários baseados em IA foram vistas na manipulação de mídias sociais, na disseminação de notícias falsas e desinformação e na segmentação de eleitores com a intenção de influenciar os resultados das eleições – o escândalo Cambridge Analytica provavelmente é o caso mais conhecido , mas também há evidências de interferência no referendo e nas eleições do Brexit no Brasil, na Suécia e na Índia [15].

8.5 Lacunas de Pesquisa

8.5.1 Metas de privacidade versus outras metas

Resolver os compromissos que precisam ser feitos entre a proteção da privacidade e outros objetivos constitui um grande desafio, conforme ilustrado em [104]. Além disso, nossos inter-

opiniões conduzidas na fase de elicitação de requisitos do CyberSec4Europe [82] transmitiram que para o domínio do gerenciamento de identidade que aumenta a privacidade sistemas, pesquisas e desafios práticos para abordar adequadamente os compromissos que precisam ser feitos entre proteção da privacidade, usabilidade e necessidade de confiança a ser abordado. As preferências de compensação de privacidade também diferem culturalmente, o que também precisa ser considerado para alcançar privacidade utilizável e soluções de gerenciamento de identidade desde o projeto [121].

8.5.2 Construindo a Teoria da Cultura e Clima de Privacidade Organizacional

Conforme defendido por [24], as organizações podem ser vistas como entidades humanas vivas, e como estrutura de grupo humano, eles têm uma cultura. Esta cultura de grupo é um reflexo da consciência dos seus líderes. Portanto, os valores e comportamentos dos líderes influenciará em grande parte a cultura de toda a organização. Se uma cultura é "tóxica" em uma ou mais de suas facetas, é importante olhar atentamente nos valores e comportamentos apresentados pelos líderes e pela alta administração. E isso inclui a faceta da privacidade e como ela é percebida dentro da organização.

Muitos pesquisadores abordaram os temas da cultura de privacidade organizacional [57] e do clima [16, 103], mostrando que esses componentes influenciam fortemente as percepções, atitudes e comportamentos dos funcionários em relação à privacidade. Essa pesquisa enfatiza que os líderes devem criar um ambiente propício para integrar com sucesso o PbD nos processos organizacionais. No entanto, uma vez que esta área da Cultura e Clima de Privacidade Organizacional (OPCC) é em seu estágio embrionário [122], ainda é necessária mais pesquisa primária para construir solidamente a teoria em torno do tema, bem como definir formas de mensurar e incorporar a privacidade nas organizações de forma confiável.

8.5.3 Contra-impressão digital do dispositivo

Ataques de impressão digital de dispositivos, que podem recuperar um dispositivo por meio de dados coincidentes que o dispositivo sai enquanto se comunica em uma rede, tornam-se graves ameaça à privacidade do local. Os dispositivos de rede tornam-se cada vez mais heterogêneos, o que permite uma diversidade de impressões digitais que podem ser exploradas para ataques. Mais pesquisas são necessárias para compreender e medir a precisão dos ataques de impressão digital, por exemplo, medindo quanta entropia está contida em uma fonte específica de impressão digital para fornecer orientação sobre como alcançar minimização de dados em um processo PbD.

8.5.4 Engenharia de Direitos do Titular dos Dados

De acordo com art. 15-21 GDPR, os cidadãos europeus cujos dados pessoais são processados em qualquer organização a nível mundial têm um conjunto de direitos em relação a esses dados organizações de processamento. Por exemplo, o direito de acesso permite-lhes

ser informado sobre a natureza e finalidade do tratamento, bem como sobre o conjunto de dados armazenados e tratados. Até certo ponto, isso se espalha até mesmo para subprocessadores que também estão envolvidos no processamento de dados. O direito ao apagamento, muitas vezes também chamado de direito ao esquecimento, permite exigir a exclusão de todos (ou parte dos) dados pessoais armazenados em uma organização - a menos que outro raciocínio explícito restrinja isso (por exemplo, no que diz respeito a registros pessoais em autoridades policiais agências). O direito à retificação permite aos indivíduos em causa alterar os seus dados, por exemplo, corrigir informações falsas num registo de dados.

No entanto, quando se trata da aplicação destes direitos dos titulares de dados concedidos pelo RGPD, surgem muitas questões em aberto. Como pode a transparência exigida pelo direito de acesso ser concretizada num fluxo de trabalho distribuído e multiorganizacional? Como podem as restrições ao processamento de acordo com o Art. 18 do GDPR seja implementado em tal fluxo de trabalho? Como pode um pedido de apagamento ou retificação ser propagado ao longo de uma cadeia de processamento e que parte do processamento constitui o mesmo fluxo de trabalho no que diz respeito à finalidade específica do processamento? Quando duas atividades de processamento pertencem ao mesmo fluxo de trabalho e quando instanciam uma instância de processamento de dados separada, com necessidades distintas de consentimento do usuário e de aplicação dos direitos do titular dos dados?

8.6 Exemplos de problemas Ao

abordar estes e outros desafios de investigação abertos no domínio da privacidade desde a concepção ou da engenharia de privacidade, os seguintes domínios de problemas específicos precisam de ser abordados mais de perto.

Identificação de fatores e definição de construtos na área do OPCC. As organizações podem beneficiar muito de instrumentos práticos, como questionários [57], que as podem ajudar a medir ou avaliar aspectos organizacionais como a “cultura de privacidade” e o “clima de privacidade”. Para tal, os investigadores ainda precisam de compreender e identificar os factores-chave que formam os construtos do OPCC e testar os instrumentos em termos de validade e fiabilidade.

Justiça algorítmica versus minimização de dados. As compensações entre minimização de dados e justiça para modelos de aprendizado de máquina foram discutidas recentemente [38] e ainda são, em grande medida, uma questão não resolvida.

Medindo riscos na impressão digital de dispositivos. Mais pesquisas são necessárias sobre mecanismos de defesa contra riscos de impressão digital de dispositivos que podem ser evitados (por exemplo, com base em comportamento definido por software, como APIs) e sobre riscos remanescentes que serão difíceis de defender (por exemplo, ataques de impressão digital baseados em propriedades do dispositivo físico, como desvio de relógios físicos).

Medir o nível de proteção de privacidade oferecido. Muitas vezes não é claro qual o nível de protecção que é efectivamente proporcionado por um determinado dispositivo que aumenta a privacid

tecnologia de decisão de design com consciência de privacidade. Juntamente com esta incerteza surge a questão de saber se um determinado conjunto de medidas que melhoram a privacidade medidas foi suficiente para ser considerado o estado da arte no sentido do GDPR, ou que outros níveis de proteção teriam sido adequados. Portanto, a seleção de Tecnologias que Aumentam a Privacidade (PETs) para aplicar em um determinado contexto e cenário, juntamente com a determinação de a protecção alcançada, é uma questão de investigação em aberto. Existem metodologias iniciais (como Privacy Design Strategies [111], LINDDUN [60] ou o Modelo Padrão de Proteção de Dados [51]), mas estes não são suficientes em detalhando a medição do nível de proteção fornecido.

Modelagem de ameaças como facilitadora “por design”. A privacidade precisa ser integrada em todas as etapas do desenvolvimento de software desde o design. De acordo com o GDPR abordagem baseada no risco, é crucial primeiro determinar os problemas de privacidade que podem surgir para resolvê-los adequadamente. Modelagem de ameaças é uma abordagem bem conhecida no domínio da segurança[1] e também vem ganhando impulso na comunidade de privacidade. A modelagem de ameaças à privacidade permite identificar e mitigar sistematicamente problemas de privacidade em o nível arquitetônico. Ao identificar esses problemas precocemente, eles podem ser abordadas no núcleo do sistema de uma forma mais eficiente. O modelo de ameaça deve informar decisões em projeto, desenvolvimento, testes e e fases pós-implantação[2] (por exemplo, determinar os principais alvos de verificação para testes de software). A avaliação de riscos deve orientar a priorização. A automação da modelagem de ameaças é o próximo passo para facilitar uma crescente adoção. Desenvolvimentos em tempo de execução e modelagem adaptativa de ameaças também fortalecer a incorporação em ambientes de Integração Contínua e Entrega Contínua (CI/CD).

Custodiantes de dados e direitos delegados aos titulares dos dados. Utilizando os direitos do titular dos dados contra um controlador de dados requer um tipo específico de interação de acordo com as regras descritas no GDPR. Os controladores de dados devem fornecer meios de comunicação para tais solicitações em conformidade, e pode ter um grande incentivo para automatizar ou pelo menos estruturar tais solicitações, tanto quanto possível, por exemplo, para poupar mão-de-obra. Ao mesmo tempo, o fardo de utilizar os direitos dos titulares dos dados ao longo do tempo pode facilmente tornar-se pesado, por exemplo, se as solicitações de exclusão precisarem ser feitas repetidamente devido a dados processos de coleta não devidamente controlados pelo controlador de dados, ou se solicitações de direito de acesso devem ser pré-processadas para se tornarem compreensíveis para leitores humanos. Nesses casos, a instanciação de um banco de dados dedicado custodiante que faz cumprir os direitos do titular dos dados em nome do titular dos dados

[1] veja, por exemplo, o top 10 do OWASP: https://owasp.org/Top10/
[2] veja também www.threatmodelingmanifesto.org

pode tornar-se essencial. Tal como previsto na Lei Europeia de Governação de Dados, os intermediários de dados que fazem cumprir os direitos dos titulares dos dados devem cumprir requisitos especiais e também podem ser tentados a automatizar as suas operações, tanto quanto possível. Aqui, podem ser identificados desafios de investigação abertos nestes aspectos, tais como engenharia de direitos dos titulares de dados, transparência desde a concepção, direito de acesso como serviço ou modelos de delegação de confiança de custodiantes de dados.

9 Infraestruturas Críticas

9.1 Introdução

Embora a protecção de infra-estruturas críticas (IC) tenha recebido a atenção da comunidade de investigação durante mais de uma década, proteger os CI de Os ataques cibernéticos e híbridos (ciberfísicos) emergentes ainda constituem um desafio em aberto. Diversas definições de ICs podem ser encontradas na literatura científica, nas normas internacionais e nos documentos regulatórios. Em termos simples e de acordo com De acordo com a directiva relevante do Conselho Europeu [64], os CI são sistemas ou sistemas de grande escala. sistemas de sistemas, que são essenciais para o bom funcionamento de atividades sociais vitais funções e para o bem-estar das pessoas.

Tomemos por exemplo o setor de saúde: este setor é composto, entre outros coisas, de hospitais, centros de saúde, indústrias farmacêuticas laboratórios, instalações de fornecimento de sangue, serviços de emergência e instalações de pesquisa. A interrupção ou destruição de tais instalações, especialmente se forem extensas ou por uma duração significativa, podem ter um impacto grave na saúde pública. Como outro exemplo, consideremos o sector dos transportes: neste caso, os aeroportos, os portos, as infra-estruturas ferroviárias e os sistemas de controlo do tráfego rodoviário desem na mobilidade das pessoas, bem como no bom funcionamento da cadeia de abastecimento. Outros exemplos de setores de IC incluem tecnologia de informação e comunicação infraestruturas, como redes de telecomunicações e infraestruturas em nuvem; instalações de energia, incluindo redes de produção, armazenamento, transmissão e distribuição de energia elétrica, de gás, de petróleo ou nuclear; instalações de água, incluindo barragens, armazenamento, gestão e redes de água; finanças, como instalações bancárias e comunicações interbancárias; gestão de alimentos, incluindo alimentos produção, sistemas de segurança alimentar, cadeia de fornecimento atacadista e muito mais.

Poder-se-ia argumentar que, “uma vez que os IC existem há várias décadas (ou mesmo séculos), já devem estar suficientemente maduros e adequadamente protegidos”. Infelizmente, isto está longe de ser verdade, por várias razões. a maior acessibilidade dos CIs modernos e seu maior acoplamento com sistemas de informação e comunicação. Há algumas décadas, os CIs costumavam ser sistemas fechados. Hoje em dia, a conectividade com a Internet oferece aos administradores de CI um gerenciamento mais eficiente, em tempo real e remoto, sem exigindo proximidade física com a infraestrutura. Além disso, os CIs também se tornaram mais acessíveis aos usuários finais e estreitamente conectados com sistemas de Internet das Coisas (IoT). Por exemplo, embora há alguns anos a medição do consumo na rede elétrica exigisse física acesso aos sistemas de medição do usuário final, hoje em dia os sistemas de medição inteligentes permitem não apenas a medição remota, mas também o controle remoto. Embora mudanças como as descritas acima tenham aumentado a eficiência das operações de CI, ao mesmo tempo aumentaram seu ataque superfície e perm

Por último, mas não menos importante, o aumento da conectividade dos CI também aumentou as dependências entre essas infraestruturas. Existem diferentes tipos de dependências de infraestrutura. Por exemplo, um fornecedor de energia que recebe serviços de comunicação de um operador de telecomunicações tem uma dependência cibernética. Por outro lado, a operadora de telecomunicações necessitará de energia eléctrica para apoiar as suas operações de rede. Qualquer dependência de um recurso físico, tal como o fornecimento de energia descrito acima, é uma dependência física. Outros tipos de dependências incluem geográficas (quando dois ICs dependem um do outro devido à sua localização física) e lógicas (quando algum tipo de dependência diferente das

9.2 Quem será afetado?

Qualquer pessoa que atue como “consumidor” dos serviços fornecidos por um IC será afetada se um IC for comprometido, incluindo pessoas, empresas e outras organizações. Infelizmente, as dependências entre os fornecedores de IC também aumentam a importância de ataques potenciais. como a extensão das organizações e pessoas que eventualmente serão afetadas. Considere, por exemplo, um ataque cibernético contra uma rede de distribuição elétrica, que suporta muitos outros ICs próximos (dependências geográficas e físicas), como fornecedores de telecomunicações, semáforos sistemas, serviços governamentais, instalações de dados, hospitais, data centers ou aeroportos. A interrupção ou degradação do fornecimento elétrico afetará simultaneamente, até certo ponto, todos os ICs que dependem da rede de distribuição elétrica específica sob ataque. Tais tipos de dependências simultâneas de múltiplas infraestruturas em um único IC pode resultar no que é conhecido como falhas de causa co

múltiplas organizações, tanto no sector público como no privado, bem como muitas pessoas que "consomem" os serviços afectados.

Outro tipo de dependências que podem afetar simultaneamente um número considerável de pessoas, empresas e organizações são aquelas dependências que se propagam de um IC para outro. Um dos casos mais famosos e bem estudados é o apagão da Califórnia [196], onde a falha de uma central eléctrica causou múltiplas falhas em cascata, devido a uma série de dependências de CI. Por exemplo, a redução de energia causou uma diminuição na quantidade de petróleo que foi canalizada para as instalações aeroportuárias, causando graves problemas aos serviços aeroportuários e, em última análise, aos horários dos voos dos operadores aeroportuários. Ao mesmo tempo, a perda de energia elétrica levou à degradação das unidades de injeção de vapor que eram utilizadas para alimentar as unidades de recuperação de petróleo. Este último levou a um efeito de feedback, uma vez que o óleo produzido também foi utilizado como combustível pelo operador de energia eléctrica inicialmente afectado! Finalmente, a redução da energia eléctrica também afec

9.3 O que se espera que aconteça?

Os ataques contra ICs podem levar a todos os tipos de consequências, como perda de vidas, perdas financeiras, desordem pública ou interrupção das operações comerciais [222]. Ataques contra hospitais podem afetar o tratamento dos pacientes. Por exemplo, um ataque de ransomware num hospital alemão causou um atraso no tratamento de emergência de uma paciente, que acabou por perder a vida1 . Embora a investigação policial relevante tenha concluído que "o atraso não teve relevância , para o resultado final"2, também alertou que é uma questão de tempo até que a pirataria informática em hospitais conduza a resultados trágicos. , e a graves perdas económicas, especialmente se forem também considerados os efeitos em cascata noutras infra-estruturas. Exemplos de ataques cibernéticos deste tipo, alegadamente causados por adversários do Estado-nação, incluem os ataques contra a rede eléctrica da Ucrânia em 2015 e em 20163. Infra-estruturas de telecomunicações As infraestruturas também são alvos de ataque muito atrativos, uma vez que elas e a energia são os dois setores com o maior nível de dependências de entrada de outras infraestruturas (quase qualquer CI depende de serviços de energia e telecomunicações). Ataques contra infra-estruturas de gestão do tráfego rodoviário ou ataques directos a

1A história não contada de um ataque cibernético, um hospital e uma mulher moribunda: https://www.wired.co. reino unido/artigo/ransomware-hospital-death-lemany

2Ataque de ransomware em hospital alemão. Um relatório sobre as descobertas e avisos da investigação pode ser encontrado em: https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital-paciente/

3Hackers provocam mais um corte de energia na Ucrânia: https://arstechnica.com/tecnologia da informação/2017/01/o-novo-normal-ainda-outro-hacker-causou- queda-de-energia-atinge-ucrânia/

veículos de qualquer tipo (automóveis, navios ou aviões) podem causar perturbações no trânsito ou mesmo acidentes letais.

9.4 Qual é a pior coisa que pode acontecer?

Como os IC são vitais para o bem-estar das pessoas e a sua perturbação pode levar a graves consequências sociais, financeiras e de segurança, são alvos muito atraentes para atacantes mal-intencionados.

A preparação de ataques cibernéticos contra ICs requer elevada motivação, geralmente elevados recursos e competências e algum tipo de capacidade de acesso inicial por parte dos adversários. Infelizmente, existem vários desses adversários no atual cenário de ameaças. Por exemplo, os Estados-nação adversários podem estar suficientemente motivados e ter o tempo, os recursos e as competências necessários para implantar Ameaças Persistentes Avançadas (APT) contra CIs visados, com a intenção de causar danos graves aos CIs de um Estado inimigo. Isto pode ser usado como um ataque assimétrico ou como parte de uma guerra ciberfísica híbrida. Os terroristas também podem ser motivados a causar perturbações graves e perda de confiança do público.
Por último, os cibercriminosos podem ser motivados a atacar os CI, visando um elevado ganho económico, por exemplo, através de ataques de ransomware e de chantagem.

A maior conectividade de rede e a interconectividade dos CIs estão aumentando a superfície de ataque, pois podem fornecer aos adversários vários pontos de entrada iniciais. Além disso, a falta de formação e sensibilização em segurança também pode ser explorada pelos adversários para obter acesso inicial. Por exemplo, as campanhas de spear phishing destinadas a utilizadores-alvo podem ser uma acção preparatória para um APTO.

9.5 Lacunas de Pesquisa

Obviamente, a proteção dos ICs contra ataques como os descritos acima não é uma tarefa trivial. A proteção de IC é um processo multidisciplinar. Do ponto de vista técnico, requer uma melhor compreensão das ameaças, vulnerabilidades e exposições, bem como uma proteção eficiente e eficaz.
Do ponto de vista social e empresarial, requer uma melhor compreensão das dependências entre os ICs e do impacto relacionado com os ataques específicos, bem como uma maior formação e sensibilização das pessoas envolvidas.

9.5.1 Modelagem, análise e simulação de ameaças não triviais, incluindo APTs, desastres ciberfísicos e relacionados com as alterações climáticas

Espera-se que as APTs se tornem mais poderosas, ainda mais sofisticadas e mais frequentes. O mesmo se aplica a outros tipos de ataques híbridos (ciberfísicos) provocados pelo homem ou mesmo a catástrofes naturais e provocadas pelas alterações climáticas. Devido à sua complexidade [209], os CIs não estão atualmente equipados com ferramentas de modelagem avançadas que lhes permitam preparar-se adequadamente para tal

ameaças não triviais e para gerenciar eficazmente qualquer ataque provável [242]. Há necessidade de novas abordagens para apoiar a modelização, análise e simulação de tais ameaças, por exemplo [254], a fim de preparar melhor os IC para lidar com elas no mundo real, mas também para propor tácticas de resposta rápidas, eficientes e fiáveis. .

9.5.2 Desenvolver metodologias de avaliação e gestão de riscos para riscos sistêmicos e da cadeia de suprimentos

Tal como foi salientado muito claramente através dos acontecimentos desencadeados pela guerra na Ucrânia, vários sectores de IC, como a energia e os transportes, podem desencadear riscos sistémicos, intersectoriais e transfronteiriços para a sociedade e a economia (por exemplo, perturbando a energia ou suficiência alimentar à escala europeia ou global). Dadas as suas características especiais [256], é necessário desenvolver novos métodos para a identificação precoce e a gestão proativa de tais riscos, especialmente num contexto intersetorial e transfronteiriço.

9.5.3 Resiliência de Infraestruturas Críticas

Aumentar a resiliência dos ICs é um objetivo de pesquisa em andamento, tanto em nível “microscópico” quanto “macroscópico” [193]. Do ponto de vista dos componentes, há necessidade de investigação adicional sobre sistemas incorporados resilientes e tolerantes a falhas, que são essenciais para a monitorização e controlo adequados de sistemas ciberfísicos críticos. Do ponto de vista sistémico, garantir um nível de resiliência para operações e serviços críticos de uma forma rentável é um desafio em aberto. Há uma necessidade de (re)projetar infraestruturas resilientes desde o projeto, desenvolvendo soluções quase ótimas em termos de custo que garantam a redundância controlada, a desenvoltura e a recuperação rápida de operações críticas Uma concepção resiliente deve também considerar a integração de capacidades de resposta (semi) automatizadas e económicas para minimizar eficazmente o impacto dos ataques cibernéticos na fase mais precoce possível.

9.5.4 Modelos aprimorados assistidos por IA/ML para análise de (inter)dependência

Apesar dos esforços de investigação passados e recentes (por exemplo, [204, 208, 224, 243]), ainda há necessidade de modelos melhorados para a análise de (inter)dependências de IC, explorando ameaças em tempo real e sistemas de monitorização de riscos assistidos por inteligência artificial (IA) e aprendizado de máquina (ML). Por exemplo, há necessidade de desenvolver modelos para compreender o fluxo de perturbação de um sistema para outro, que englobe efeitos não locais com grandes diferenças nas escalas de tempo. Como a formação de modelos deve basear-se em dados reais de sistemas reais, isto requer um envolvimento mais dir

9.5.5 Previsão de eventos baseada em todos os tipos de dependências

Embora as dependências cibernéticas e físicas sejam geralmente capturadas em profundidade nos atuais modelos de previsão de eventos, as dependências geográficas não são capturadas de forma adequada. Por conta disso, a previsão de eventos disruptivos não é mapeada com precisão em um território específico. Esforços devem ser feitos nesse sentido, por exemplo, usando sistemas de informação geográfica para capturar o máximo nível possível de resolução espacial e mapear essas informações em dados no que diz respeito à deslocação de activos, considerando também os tipos de perturbação mais importantes para cada activo (por exemplo, tremores de terra, chuva, vento ou temperatura).

9.5.6 Consciência situacional colaborativa para o ecossistema de CI

Como uma quantidade cada vez maior de dados de segurança cibernética (por exemplo, dados emergentes ameaças, vulnerabilidades de dia zero) ficam disponíveis diariamente, torna-se mais difícil utilizar efetivamente esses dados para melhorar a situação de segurança cibernética em uma organização [11]. Melhorar a consciência situacional para Os operadores de IC requerem uma abordagem sociotécnica multidisciplinar, que inclua pessoas como parte da solução. São necessários métodos e ferramentas para facilitar a cooperação e a colaboração dentro e entre os operadores de IC e as autoridades sectoriais, nacionais e europeias relevantes.

9.6 Exemplos de problemas

Exemplos de problemas tangíveis podem incluir:

Gêmeos digitais de ICs. Desenvolver modelos quadridimensionais para monitorar continuamente o comportamento da infraestrutura, recebendo informações constantemente de dispositivos IoT. Esta poderá ser uma prioridade para as infra-estruturas que sofrem dos problemas do envelhecimento, a fim de analisar continuamente as suas expectativas estado e perceber possíveis desvios de seu estado estrutural normal comportamento.

Segurança da cadeia de suprimentos para CIs. Os operadores de IC dependem de várias cadeias de abastecimento para entregar seus serviços aos usuários finais. Os invasores estão usando cada vez mais toda a cadeia de abastecimento para realizar ataques. Como a segurança da cadeia de abastecimento é também exigida pelo NIS/NIS2, a segurança da cadeia de abastecimento para ICs exige Investigação aprofundada.

Desenvolva ferramentas para apoiar a recuperação eficaz de eventos críticos com todos os riscos. O aumento do número de interdependências exige o desenvolvimento de ferramentas inovadoras de apoio à decisão para auxiliar na identificação precoce de eventos críticos e na estratégia de recuperação mais eficaz, tendo em conta consideração suas dependências e outras restrições.

Desenvolver métodos e ferramentas para a detecção precoce de eventos ciberfísicos. Como os ICs são sistemas ciberfísicos com dimensões fortemente restritas, há necessidade de desenvolver métodos e ferramentas para detectar e avaliar ataques ciberfísicos, considerando simultaneamente as suas vulnerabilidades cibernéticas e físicas a partir de uma perspectiva holística.

Conceber um quadro regulamentar multidisciplinar melhorado. As autoridades competentes, conforme definidas nas NIS/NIS2, desempenham um papel fundamental na proteção dos IC. É necessário desenvolver políticas regulatórias sustentáve estruturas que podem considerar todos os riscos pertinentes e lidar com incidentes envolvendo diversas dimensões, como aspectos técnicos, sociais ou jurídicos.

10 Metaversos

10.1 Introdução

Apesar do que muitos leitores possam pensar, o metaverso não é um produto, nem mesmo uma marca de alguma empresa de rede social, mas sim um nome dado a um conjunto de tecnologias aplicadas em plataformas para a Web na Internet. Na verdade, o conceito de mundos virtuais remonta pelo menos ao século **XIX [27]. Ainda assim, o termo metaverso foi usado para nomear um conceito futurista, descrito em um livro de ficção científica em 1992, que o popularizou [223], e foi mostrado em formato visual em um filme 20 anos depois (ou seja, 10 anos atrás) [159]. O Metaverso, na prática hoje, refere-se a um novo tipo de plataforma Web, que se suporta num conjunto abrangente de tecnologias, algumas já consolidadas e outras em evolução, que permitirão aos utilizadores uma maior interactividade e socialização em ambientes digitais 3D imersivos, representado por um universo de novos mundos virtuais digitais, preferencialmente espelhados no mundo físico.**

A pesquisa do metaverso testemunhou uma primeira onda de "hype" entre os anos 2000 e 2006, com muitos resultados e visibilidade. Atualmente, em 2022, passa por uma segunda onda de interesse, agora provocada por players comerciais que passaram a comercializar seus metaversos e eventos realizados dentro deles, mas também por um anúncio público relacionado ao metaverso amplamente divulgado por uma das grandes empresas ocidentais. -Tecnologias no final de 2021.

Hoje é possível entender o que são, ou poderiam ser, metaversos navegando por plataformas Web como Second Life, Decentraland, Som-nium Space, The Sandbox, Roblox, Horizon Worlds, Avakin Life, Mesh, entre outras.

Os conceitos de mundos virtuais digitais dos metaversos atuais são tipicamente baseados em tecnologias Web 2.0 que incluem espaços de Realidade Virtual 2D e 3D, com imagens de computação gráfica que variam de baixa a alta resolução, e algumas plataformas que utilizam tecnologias de Realidade Aumentada em diversas atividades. A representação dos utilizadores é sempre através de avatares, e, como o acesso às plataformas depende de um login exclusivo, falta interoperabilidade, pois os avatares ficam confinados a um único metaverso e aos seus mundos, não sendo permitidos

passar de um metaverso para outro, em outra plataforma, sem fazer login novamente no mundo físico.

O acesso às plataformas pode ser feito por meio de diversos dispositivos que incluem smartphones, tablets, laptops, desktops, estações de trabalho e até head-mounted displays ou óculos de realidade virtual. Algumas plataformas já utilizam a monetização por meio de blockchain e criptomoedas, com adoção de contratos inteligentes e tokens fungíveis e não fungíveis (NFTs) que viabilizam atividades mercantis. Note-se, no entanto, que hoje ainda existem poucas plataformas para metaversos que utilizam tecnologias Web 3.0, o protocolo HTTP/3 e outros recursos tecnológicos mais avançados e seguros, mas este é claramente o caminho para o futuro.

Para apoiar esses recursos, as tecnologias mais avançadas, como Web 3.0 (versão mais recente da Internet), Inteligência Artificial, Interfaces Cérebro-Computador, IoT (Internet das Coisas), Blockchains e Realidade Virtual, Aumentada, Estendida e Mista, darão início a uma grande número de oportunidades que provavelmente terão impacto em grandes partes das nossas sociedades, tal como fizeram as R

10.2 Quem será afetado?

Para analisar o impacto plausível dos metaversos no futuro, vamos abraçar neste capítulo a sua visão completa como mundos digitais massivos, imersivos, persistentes, abertos e economicamente desenvolvidos, como se segue [95].

- Massivos: Podem hospedar um número ilimitado, ou pelo menos um número muito elevado de usuários simultâneos, à medida que o poder computacional das plataformas Web e das máquinas dos usuários evolui em termos de processamento gráfico e conectividade.

- Imersivos: Oferecem experiências tridimensionais e incorporadas, baseadas em Realidade Virtual (VR) e Realidade Estendida (XR). Imagine que depois do trabalho você vai até um quartinho da sua casa ou bairro, se veste com um “traje sensorial” conectado, e conta ao computador o metaverso de sua escolha e, a partir daí, você entra no site, tendo a sensação -ção de estar presente e viver “dentro” de um mundo virtual digital escolhido, controlando muitas coisas com seus pensamentos. Isto contrasta com a experiência atual da maioria dos universos de jogos, que são bidimensionais, confinados a telas e mediados por cliques, digitação e tela ou tela.
  rato.

- Persistente: os metaversos nunca serão interrompidos ou reiniciados. Ou pelo menos essa será a percepção dos seus usuários. A vida e a sociedade de um metaverso evoluirão continuamente, mesmo que alguns avatares não estejam presentes, como acontece com a vida normal em nosso mundo.

- **Aberto: qualquer pessoa com boa conectividade com a Internet e computação VR/XR o poder pode entrar em metaversos, mover-se dentro deles como um avatar, interagir com outros avatares, socializar, negociar, construir, produzir intelectualmente e assim sobre.**

- **Economicamente desenvolvido: Haverá um amplo comércio de bens e serviços dentro dos metaversos, que podem ou não ter um impacto em o mundo físico fora deles. Provavelmente serão apoiados por arquiteturas de Finanças Descentralizadas (DeFi) e sistemas monetários digitais que abrangem tecnologias blockchain, criptomoedas, contratos inteligentes e tokens fungíveis e não fungíveis que permitirão a propriedade práticas de garantia de direitos.**

É evidente que uma visão tão ambiciosa aponta para uma elevada probabilidade de uma renovação colisão entre a Governança da Era Industrial e a Governança da Era Digital, o que afetaria todas as camadas da população, desde simples usuários do metaverso aos formuladores de políticas.

Na verdade, os governos já estão nervosos. Na UE, o Parlamento Europeu está preocupado principalmente com a concorrência, a proteção de dados, as responsabilidades, as transações financeiras, a cibersegurança, a saúde, a acessibilidade e a inclusão [145], enquanto os principais pontos de preocupação do Conselho da UE são a geopolítica. , Crescimento económico, Jurisdição, Saúde, Defesa do consumidor, Civil e Códigos penais e mudanças climáticas [19]. Observamos que seria necessário um investimento intelectual massivo para que soluções práticas fossem encontradas e implementadas em cada uma destas áreas. Além disso, haverá questões espinhosas em torno de chegar a um consenso em qualquer um desses tópicos. Estas são algumas razões por que a Comissão Europeia acaba de incluir a política do metaverso entre seus prioridades [44, 50].

10.3 O que se espera que aconteça?

Uma análise da evolução das tecnologias de suporte do metaverso, como aqueles descritos acima, a Internet e a Web – a partir da versão Web 1.0 e da atual Web 2.0, para o novo patamar da Web 3.0, principalmente quando pensar em plataformas Web com grande interatividade e maior alcance social traz muitas dúvidas e –, preocupações, principalmente no que diz respeito à segurança cibernética, privacidade e proteção de dados (pessoais), regulamentos e vários aspectos do governança de tais mundos digitais [216].

Tomemos como exemplo a governança dentro dos metaversos. O conceito de “in-side” é destacado por ser diferente do conceito de interface entre o mundo digital de um metaverso e o nosso mundo físico, uma vez que tal

interface está sendo regulamentada, pelo menos na União Europeia (UE), desde 2016.

Na UE, o Estado de direito é dominante e as suas instituições são, na sua maioria, adequadas à sua finalidade. Porém, nesta nova fronteira tecnológica que são os metaversos, não está claro o que será regulamentado, quem estabelecerá e fará cumprir as regras, ou como isso será feito. Mas qualquer lugar, físico ou digital, em algum ponto de densidade populacional, necessitará de algum tipo de manutenção da ordem, incluindo a noção de direitos fundamentais.

Na verdade, pensar em universos digitais paralelos não regulamentados é preocupante. E como o comércio será omnipresente, os produtos, as transações, os direitos de propriedade e outros negócios necessitarão de algum tipo de protocolo para que os mercados prosperem Então, todos os tipos de situações conflitantes terão de ser resolvidos por alguma forma de autoridades, polícia e tribunais. Da mesma forma, deve haver regras de comércio, tributação, renda, etc. Mas então, se um grande conjunto de regras tiver que ser estabelecido, outra questão importante é quem irá estabelecê-las: serão elas próprias? -ers das plataformas de metaversos, uma vez que esses universos são de propriedade privada? Eles colocarão usuários para ajudar a definir regras locais? Ou estarão as autoridades públicas do mundo físico a começar e a expandir o seu alcance também para o mundo digital? Por quais autoridades públicas começar? Ou estarão os libertários a pensar em tecnologias criativas para governar os metaversos, promovendo a ideologia de que “código é lei”? Da mesma forma, que forma assume tal conjunto de regras? Assim, podemos pensar nas seguintes formas de regulação.

- Assinatura de contratos de utilização. No entanto, podem ser tão longas quanto constituírem ções.

- Replicação de leis e regulamentos do mundo físico. No entanto, isto pode dificultar a inovação, e seriam esperadas boas justificações para a escolha de um modelo em detrimento de outro.

- Modelos distribuídos, baseados em tecnologias digitais, como blockchain, bitcoins, NFTs, contratos inteligentes (ou seja, scripts persistentes).

Além disso, a própria oferta tecnológica de interatividade e imersão dos metaversos da próxima geração dependerá fortemente de dispositivos vestíveis que monitorem dados biométricos (por exemplo, marcha, expressões faciais, temperatura) e neurométricos (por exemplo, medo, satisfação, atenção). o que implicará uma vigilância contínua e completa dos utilizadores. Nas sociedades ocidentais, onde a privacidade e a protecção dos dados pessoais são direitos fundamentais, os interesses comerciais e públicos terão uma relação muito difícil relativamente a este tema.

Para agravar esses problemas, a superfície de ataque para violações de segurança e invasões de privacidade pode se tornar muito grande no metaverso, porque integra uma variedade de tecnologias e sistemas mais antigos, atuais e também não testados.

cujas vulnerabilidades e falhas intrínsecas serão herdadas pelo sistema maior. Como consequência, as ameaças à segurança existentes serão amplificadas, com mais efeitos graves. Eles incluem o seguinte (não exaustivo) [244]:

- Falta de cultura de segurança por parte dos usuários neste novo ambiente mentos,
- Má gestão de fluxos massivos de dados,
- Atividades generalizadas de criação de perfis de usuários,
- Resultados injustos de algoritmos de Inteligência Artificial (IA),
- Segurança de gêmeos digitais,
- Segurança das infraestruturas físicas do metaverso,
- Os dados pessoais envolvidos no metaverso serão mais granulares e biométricos, incluindo emocionais, etc.

Finalmente, a ampliação da superfície de ataque trazida pelos metaversos irá facilitar ameaças existentes em espaços físicos e cibernéticos, como perseguição, assédio e espionagem, que podem aumentar em frequência e impacto. O o uso de tecnologias emergentes aumentará a probabilidade de incidentes de segurança, como sequestro de dispositivos vestíveis ou armazenamento em nuvem, roubo de moeda virtual ou má conduta de IA para produzir notícias falsas de forma autônoma dentro de metaversos [67].

10.4 Qual é a pior coisa que pode acontecer?

Muitas coisas podem dar errado se o fornecimento e o uso de metaversos ficarem descontrolados no futuro, e a maioria deles está relacionada com a noção de confiança neles.

É certo que a grande maioria dos utilizadores do metaverso são e serão cidadãos cumpridores da lei e pessoas que valorizam o comportamento civilizado. No entanto, entre os usuários também têm certeza de que haverá trapaceiros e outras pessoas menos honestas que participarão apenas para tentar ganhar dinheiro fácil com o que seria ser definida na maior parte do mundo físico como atividade criminosa. Tal ambiente não atrairia a confiança dos usuários e geraria retornos comerciais Como consequência, o excesso de investimento pode cair, enquanto os empreendimentos ilícitos podem florescer.

Num outro registo, talvez mais importante, os metaversos colocam grandes desafios à privacidade e à governação e podem ter o potencial de acelerar a mudança geopolítica de poder dos Estados-nação para empresas privadas.
Lembre que já hoje algumas empresas de redes sociais possuem populações que são maiores do que o do maior país da Terra. Se os governos nacionais não puderem confiar que os metaversos tratarão os seus cidadãos de forma legal,

então os governos podem decidir regulamentar excessivamente os metaversos, dificultando a inovação e aumentando a fragmentação.

Conseqüentemente, a falta de governança confiável e de regulamentações de segurança e privacidade dentro dos metaversos pode transformar este Eldorado de alta tecnologia em um O Velho Oeste do século **21 , onde fortunas serão feitas e a ilegalidade será a regra e não a exceção.**

10.5 Lacunas de Pesquisa

Como visto acima, o campo para a regulação estatal dos metaversos é vasto, variando desde questões em níveis macro (por exemplo, geopolítica) até níveis micro (por exemplo, vender uma pulseira digital no metaverso). Em poucas palavras, a principal legislação actual da UE e as políticas que regem a esfera digital são as seguintes.

- **Lei dos Mercados Digitais: Regulamentação da concorrência nos mercados online. Isto estabelece regras harmonizadas que definem e proíbem práticas desleais, como a utilização de dados dos concorrentes e a falta de interoperabilidade, parte dos "gatekeepers" da Web.**

- **Lei dos Serviços Digitais: obrigações de devida diligência em todos os serviços digitais que conectam os consumidores a bens, serviços ou conteúdos, incluindo procedimentos para remoção mais rápida de conteúdo ilegal, bem como procedimentos abrangentes protecção dos direitos fundamentais dos utilizadores em linha [46].**

- **GDPR: Proteção de dados pessoais. Due diligence e cibersegurança [49].**

- **Regulamento de Governança de Dados e Lei de Dados: Enquanto a Governança de Dados A regulamentação cria os processos e estruturas para facilitar os dados, a A Lei de Dados esclarece quem pode criar valor a partir dos dados e sob quais condições condições. [48]**

- **Diversos em segurança cibernética: Lei de Segurança Cibernética (por exemplo, certificação), NIS2, ENISA, ECCC/NCCs, Unidade Cibernética Conjunta, Lei de Resiliência Cibernética, etc.**

No entanto, do ponto de vista da governação e da política, tal legislação existente provavelmente não é suficiente para induzir confiança no domínio, e talvez nem mesmo adequado para metaversos. Consequentemente, muitas pesquisas são necessárias em estas áreas num futuro próximo. Por exemplo, será necessário regulamentar segurança e privacidade em múltiplos universos que estão sendo construídos do zero. As questões podem ser simples extensões de preocupações existentes, como se os metaversos deveriam estar sujeitos às leis existentes para o mundo físico e, em caso afirmativo, como para não impedir a inovação e a criatividade. Ou eles podem ser virados muito mais em direção a conceitos futuros, como se os avatares deveriam receber o status de cidadão.

Da mesma forma, as tecnologias necessárias para construir metaversos, tal como aqui previstos, estão apenas a emergir e será necessária muita investigação tecnológica nos próximos anos. Além disso, um resultado provável das forças de mercado é a criação de vários metaversos, representando universos paralelos, não apenas entre eles, mas também ao universo físico em que estamos habituados a viver.

O que é certo é que uma nova corrida ao ouro já começou. As áreas de pesquisa necessárias podem ser apresentadas em grupos, como segue.

10.5.1 Construindo metaversos confiáveis

Uma área de pesquisa sobre governança deveria analisar todos os aspectos dentro dos metaversos que impactariam os usuários individuais. Estas abrangem, entre outros, a protecção de dados, a responsabilidade, as identidades digitais, a cibersegurança ao nível do utilizador, a saúde mental e física, a acessibilidade, a inclusão, as transacções financeiras e a protecção do consumidor.

10.5.2 Metaversos e o mundo físico Outra área

de investigação sobre governação deveria propor novos sistemas sociais para metaversos e a sua inter-relação com formas existentes de governação e governo. Estes incluiriam segurança cibernética a nível de infra-estruturas físicas e a nível de sistemas, privacidade, concorrência, governação global, jurisdição, direitos civis, código penal, alterações climáticas, inovação.

10.5.3 Conformidade desde a

concepção O surgimento de metaversos levanta uma ampla gama de preocupações quanto à sua compatibilidade com a lei, como visto acima. Portanto, será necessário ir além dos conceitos bem conhecidos de segurança desde a concepção e privacidade desde a concepção, em direcção a um paradigma abrangente de conformidade desde a concepçã Por exemplo, será necessária investigação sobre regulamentos técnicos adaptados para orientar os fabricantes de hardware e os criadores de software no que diz respeito à conformidade, incluindo regras de governação de dados e de governação operacional.

Esses tópicos de governação devem ser abordados juntamente com a investigação nas novas tecnologias e na integração de sistemas que serão necessários para alcançar o conceito de metaverso completo descrito acima neste capítulo. Algumas áreas de pesquisa tecnológica e de sistemas são as seguintes. Observe que eles são intrinsecamente transdisciplinares.

10.5.4 Interatividade e tecnologias imersivas Tornar o

metaverso totalmente interativo e imersivo é uma área de pesquisa evolutiva. deve estar focada na captura massiva e na análise rápida de dados (telemetria, rastreamento biométrico e neurométrico, entre outros) de

usuários e seus avatares. Os dados serão coletados por meio de “interfaces vestíveis” (dispositivos vestíveis) de diferentes tipos que gradualmente trarão para o metaverso Plataformas XR informam cada vez mais informações pessoais confidenciais, que precisarão proteção sistêmica.

10.5.5 Design de metaversos

A área de pesquisa sobre o estabelecimento de projetos estruturados e design de mundos virtuais digitais em um ambiente de metaverso agora tem um grande potencial estudar e estabelecer uma arquitetura mínima necessária. Podem ser infraestruturas de plataforma, padrões de protocolo usuais, sistemas de segurança ou mesmo aspectos construtivos e operacionais da aplicação de XR em 3D. O estabelecimento de um padrão mínimo não deve inviabilizar a criatividade, mas encorajar a construção eficaz de metaversos interoperáveis com regras para coexistência social entre avatares, que são aceitáveis em termos éticos e morais termos, universalmente, seja no mundo digital ou físico.

10.5.6 Interoperabilidade entre plataformas do metaverso

A interoperabilidade dos metaversos precisa ser intensificada, para que seja possível para avatares (usuários) que estão vivenciando um mundo virtual digital em um plataforma específica do metaverso de uma empresa, para poder passar, sem impedimentos e de forma transparente, para outra plataforma do metaverso, de outra empresa, sem a necessidade de se identificar novamente no mundo físico. A pesquisa sobre interoperabilidade em ambientes de metaverso seria abordar identidades digitais e permitir o estabelecimento de uma coleção contínua de metaversos, talvez usando o conceito de identidades digitais autossoberanas e passaportes digitais [248].

10.5.7 Metaversos e Meio Ambiente, Social e Governança (ESG) são-

processa

Um dos principais pontos de pesquisa sobre metaversos está relacionado ao seu impacto sobre as alterações climáticas, devido à sua necessidade de contar com enormes centros de dados, alta computação de desempenho e até plataformas blockchain, que necessitam de um consumo de eletricidade muito elevado. Esta área de pesquisa requer avanços em arquiteturas e algoritmos, mas também em outras áreas como refrigeração técnicas que possam permitir o uso dessas tecnologias sem grande impacto ambiental. As considerações ESG desempenharão um papel importante no fornecimento e adoção de metaversos no futuro.

Vale ressaltar que nas áreas citadas acima já estão em andamento ações isoladas e não consolidadas, que visam suprir as lacunas existentes na pesquisa do metaverso. Podemos citar as ações da: Organização Econômica Mundial Fórum [84], o Fórum de Padrões de Metaversos [150], o Open Metaverses In-

Grupo de teroperabilidade [175] e a Comunidade de Interoperabilidade de Metaversos Grupo no W3C [229], entre outros.

10.6 Exemplos de problemas

Exemplos de problemas tangíveis incluem:

Proteção de dados dentro do metaverso. Os dados pessoais coletados no metaverso serão mais granulares, biométricos e neurométricos. A questão é então como conciliar a necessidade fundamental de imersão no metaverso tecnologias para implementar perfis de usuários generalizados e o direito fundamental à proteção de dados, incluindo a bioética. Observe que tal questão aborda a proteção dos dados tanto do usuário físico e o avatar digital. Mais especificamente, deveria ser investigado como para garantir que os metaversos não farão uso ilegal de tais dados, por exemplo, para vendas e monetização (como as redes sociais já fazem), para promover a influência da mídia, ou na produção eficaz de anúncios subliminares, entre outros aspectos de atividade ativa e interativa persuasão.

Protegendo avatares contra roubo de identidade. A proteção da identidade dos avatares é uma questão muito importante a ser resolvida. Embora já existam vários propostas e estratégias para aplicação de segurança em bancos de dados, com o uso de tecnologias como livros-razão distribuídos e árvore de dispersão ou hash estruturas, como Merkle Trees (que são, aliás, elementos-chave do Blockchain), ainda não há consenso sobre como manter as identidades digitais dos avatares sem comprometer seu Lifelogging (metaversos de vida história).

Regulamentação da criação de metaversos. As tecnologias atualmente aplicadas pela muitas plataformas Web já fornecem ferramentas fáceis de usar que permitem aos usuários para criar seus próprios metaversos. Mesmo que sejam simples, são totalmente sob o controle dos usuários. O problema aqui está centrado na má criação de metaversos que camuflam mundos digitais destinados a abrigar gangues de avatares por práticas criminosas, ativismo social, racismo e terrorismo, entre outras práticas antiéticas e ilegais.

Oportunidades iguais no metaverso. Garantir acessibilidade e inclusão em o metaverso para salvaguardar a igualdade de oportunidades. As plataformas Web que hospedam metaversos serão capazes de segregar avatares com base em características de hardware de seus usuários físicos, capacidade computacional, perfil pessoal ou de acordo com a região geográfica de seu acesso, conferindo mais privilégios a uns do que a outros.

Uso de criptomoedas e NFTs no metaverso. Questões de propriedade, uso indevido, interoperabilidade e portabilidade. Como as plataformas Web são proprietárias, elas mantêm controle sobre os ativos digitais pertencentes aos avatares, l bem como determinar os padrões monetários utilizados. Algumas plataformas têm suas próprias criptomoedas internas, fato que pode comprometer a portabilidade e a interoperabilidade dos ativos digitais dos avatares entre plataformas.

11 malwares

11.1 Introdução

O malware moderno vem em diferentes formas: vírus, worms, spyware, adware, trojans, backdoors e ransomware, para citar alguns. Embora os vírus de computador fossem a forma mais frequente de malware há algumas décadas, hoje em dia é o ransomware que parece ser o mais prevalente. Isso ocorre porque o ransomware fornece uma maneira altamente lucrativa e direta para que atores maliciosos monetizem os sistemas infectados. Na verdade, ao usar ransomware, estes atores infectam os sistemas das vítimas, encriptam todos os dados e depois pedem dinheiro (resgate) para fornecer a chave de desencriptação. Sem a chave de descriptografia, os legítimos proprietários dos sistemas vítimas não podem realmente usá-los, pois todas as informações são criptografadas.

Para se defenderem contra malware, os profissionais de segurança de computadores geralmente precisam de uma maneira de detectá-lo. Detectar um arquivo contendo malware costumava ser fácil: as empresas de segurança de computadores computavam um hash (um resumo) do arquivo malicioso e apenas tentavam encontrar arquivos que correspondessem a esse valor de hash. Os sistemas antivírus costumavam ser nada mais do que um conjunto de valores hash

(um valor de hash para cada malware) e apenas pesquisou arquivos que correspondessem a qualquer um desses valores de hash. Para evitar esse tipo de detecção (estática), o malware moderno sofre mutações para que duas “cópias” do mesmo malware não sejam iguais. Por exemplo, em cada “cópia” do malware introduzem pequenas alterações que, embora não alterem a funcionalidade principal do software, alteram a sua aparência e, consequentemente, o seu valor de hash. Seguindo esta phi-

Segundo a filosofia, os autores de malware ofuscam seu código para impedir ou pelo menos impedir a engenharia reversa de seus binários, mas também para remover possíveis padrões de código que poderiam ser usados para detectar o malware. Isso pode vir na forma de compactadores, programas que tentam compactar e/ou criptografar o código do malware para que o código malicioso seja descompactado e executado após várias etapas que dificultariam a vida do autor do malware. Por fim, o malware moderno é blindado no sentido de que possui funcionalidades anti-análise, como antidepuração, anti-hooking e anti-VM, para citar alguns.

Deixando de lado as diferenças de escopo que o malware pode ter, por exemplo, worms, trojans, mineradores, é importante destacar algumas diferenças na sofisticação e alcance dos alvos. Na prática, malware altamente sofisticado, do Pegasus ao Stuxnet, concentra-se principalmente em atacar um indivíduo específico ou criado para uma única organização. Neste caso, é utilizada uma cadeia de explorações, muitas das quais podem ser de dia zero, mas o atacante não está motivado financ No entanto, a sofisticação do malware diminui significativamente quando o ataque é direcionado a sistemas de informação gerais. Essa sofisticação é o que pode fazer com que o malware fique fora do radar e aumente seu impacto sobre suas vítimas.

11.2 Quem será afetado?

A prática comum prova que o malware pode infectar praticamente qualquer dispositivo de computação. Na verdade, nos últimos anos temos testemunhado uma longa lista de organizações de alto perfil a serem comprometidas: por exemplo, Colonial Pipeline [236], Uber [52], AXA [194], para citar alguns, no entanto, os casos de ransomware são os aqueles que aparecem nas notícias principalmente por causa do método de monetização adotado pelos grupos de ransomware. Em essência, além de criptografar os dados e pedir resgate em troca do fornecimento da chave de descriptografia, os invasores também exfiltram os dados para que ainda possam ameaçar a vítima com a publicação dos dados confidenciais. O malware também pode tentar exfiltrar informações confidenciais do usuário por meio de keyloggers, mídia de gravação comprometida (por exemplo, câmeras e microfones), etc.

Os invasores também podem usar malware para infectar milhares de hosts e usá-los como um exército que executa obedientemente todas as tarefas que lhe são atribuídas. A rede é chamada de botnet e também pode ser usada para ataques de negação de s Um exemplo marcante que se destaca nesta categoria, não pelo tamanho, mas pelos dispositivos que o compõe, é o Mirai. Mirai [14] é uma botnet que infecta principalmente dispositivos IoT inseguros e os utiliza para realizar ataques de negação de serviço. O tamanho da largura de banda produzida tinha como alvo um provedor de DNS popular, DYN e, como resultado, sites e serviços de alto perfil, como GitHub, Twitter e Netflix, ficaram inacessíveis [34, 251]. Além do Mirai, existem vários botnets atualmente ativos, por exemplo, Emotet [185] que

foi ressuscitado [117] após seu desligamento [80] após comprometer um host usado para distribuir vários outros malwares, como Trickbot e Ryuk, Mozi [20] e Mantis [252]. Notavelmente, eles também têm sido usados por atores estatais para lançar ataques de guerra cibernética [237].

11.3 O que se espera que aconteça?

O impacto do malware é multifacetado. Existem vários custos diretos que podem ser quantificados com relativa facilidade, como o valor do resgate solicitado. No entanto, também existem custos que são mais difíceis de quantificar, como perda de clientes, perda de produtividade, etc. De acordo com a Sophos, o custo médio de recuperação de um ataque de ransomware é da ordem de 810.000 dólares para organizações que não pagaram resgate e o dobro para organizações que pagaram [218]. Esses custos cobrem todos os custos operacionais e de tempo de inatividade causados pelo ransomware. Na verdade, estima-se que os danos causados pelo ransomware atinjam a espantosa quantia de 265 mil milhões de dólares até 2031 [29].

Mesmo as organizações que não são orientadas para TI podem sofrer com malware. Consideremos, por exemplo, o caso de um hotel. Embora o seu negócio principal não seja o fornecimento de produtos e serviços de TI, os hotéis que sofreram um ataque de ransomware [160] testemunharam os seus hóspedes serem bloqueados no acesso aos seus quartos e os seus sistemas de faturação, reservas e check-in/out tornaram-se inúteis, bloqueando efetivamente qualquer possível transação comercial. Da mesma forma, várias organizações de saúde sofreram ataques de malware e chegámos a um ponto em que é apenas uma questão de tempo até que haj

Com base no que foi dito acima, há perdas monetárias e de reputação óbvias para organizações e indivíduos cujos sistemas estão comprometidos por malware. Considere que, para os indivíduos, outros mecanismos, como a sextorção, podem ser usados para prejudicar ainda mais a vítima no nível pessoal [183].

11.4 Qual é a pior coisa que pode acontecer?

Conforme destacado no parágrafo anterior, estamos prestes a ter vítimas devido a ataques de malware. No entanto, este não é o único cenário nefasto. O Stuxnet [137] era um worm destinado a perturbar o programa nuclear do Irão. Embora isto possa ter acontecido há mais de uma década, tendo em conta a actual turbulência no cenário político, espera-se que os ataques de malware sejam ainda mais utilizados como meio de atacar a infra-estrutura digital de um país. A este respeito, espera-se que os ataques de malware para paralisar cidades inteligentes, infraestruturas críticas ou grandes prestadores de serviços aumentem, como provado pelos recentes ataques cibernéticos à HSE [191], ao Oleoduto Colonial e ao operador ferroviário dinamarquês [195]. Infelizmente, isso está alinhado com o modus operandi de vários sistemas pe

grupos de ameaça (APT) que não são necessariamente motivados financeiramente, mas são atores estatais ou apoiados pelo Estado. Na verdade, conforme relatado recentemente pela ENISA, os grupos APT foram responsáveis por mais de metade dos ataques à cadeia de abastecimento que foram investigados [75]. Na verdade, isto leva a vários ataques sem precedentes, por exemplo, o recente ataque Sandworm que teve como alvo a rede de uma empresa agrícola ucraniana para perturbar a produção e as exportações de cereais [155]. A presença de grupos APT, em conjunto com as mudanças para a IoT e o trabalho remoto, está a aumentar significativamente o impacto potencial de um ataque cibernético. Na verdade, usando o scanner de rede Zmap [66], pode-se facilmente ver que milhões de dispositivos vulneráveis estão conectados à Internet. Para piorar a situação, uma busca rápida em mecanismos de busca, como o Shodan(https://shodan.io/) **e Censys** (https://censys.io/), **revela resultados semelhantes. Tais técnicas foram usadas, por exemplo, pelo APT41 para atingir governos estaduais dos EUA [30]. Tudo isso cria uma mistura perigosa onde atores de ameaças estrategicamente motivados têm acesso a uma miríade**

de dispositivos vulneráveis que podem acessar, direta ou indiretamente, sistemas que armazenam , trocar e processar informações sensíveis e/ou críticas. Portanto, nos próximos anos, a guerra cibernética como uma extensão da turbulência geopolítica, e a utilização resultante de malware, irá conduzir a ataques cibernéticos em grande escala a infra-estruturas críticas, com impacto significativo em sectores como a banca, a energia, as telecomunicações, para citar apenas alguns, ou mesmo organizações da indústria de defesa [92]. Esta última implica que podemos enfrentar ataques sem precedentes que podem paralisar sistemas e serviços de missão crítica e impactar organizações, indivíduos e o tecido social, tanto na camada cibernética como na camada física.

11.5 Lacunas de Pesquisa

11.5.1 Sistemas comprovadamente seguros

Conforme discutido, o malware geralmente explora vulnerabilidades do sistema. Portanto, uma questão óbvia é como construir sistemas livres de quaisquer vulnerabilidades que o malware possa explorar? Embora esta linha de pesquisa possa ser muito ampla, ainda há muita segurança em contêineres ou caixas de areia impermeáveis.
Por exemplo, embora alguns malwares possam comprometer o sistema operacional ou firmware subjacente, a questão de pesquisa é se podemos construir arquiteturas de microkernel e sandbox que sejam comprovadamente seguras. É claro que isso ainda nos deixaria vulneráveis a malware que comprometa o software no nível do aplicativo, mas conter o adversário em uma sandbox nos permitiria manter a funcionalidade central do sistema segura e também manter a separação entre diferentes aplicativos e serviços executados em diferentes sandboxes. seL4 (https:

//sel4.systems/) **como microkernel e Qubes** (https://www.qubes-os.org/) **como SO podem ser considerados exemplos bem conhecidos nessa direção.**

11.5.2 Detecção de malware

Atualmente há uma corrida armamentista contínua entre os autores de malware e os "defensores", sejam eles analistas de malware, investigadores forenses digitais, SOCs, CERTs, CSIRTs etc. furtivo. Portanto, a detecção de malware ainda é uma questão central neste campo de pesquisa. Embora o software antivírus (AV) moderno possa ser muito mais preciso do que no passado, não é suficiente para prevenir a infecção de milhões de dispositivos, principalmente porque os AVs são focado em recursos estáticos. Um novo fluxo de mecanismos antimalware, nomeadamente sistemas de detecção e resposta de endpoints, surgiu durante os últimos anos. Estes, juntamente com suas variantes, por exemplo, sistemas estendidos de detecção e resposta (XDR), tentam explorar recursos comportamentais e mecanismos de IA/ML para detectar e bloquear ataques de malware. Embora sejam mais eficientes que os AVs, pois podem detectar técnicas avançadas e movimentos laterais, os EDRs estão longe de serem considerados soluções mágicas [126]. Para esse fim, uma questão crítica de pesquisa é como determinar se um arquivo é malicioso em tempo de execução e bloqueá-lo quando ele executa uma ação maliciosa sem alocar m

Esta questão de pesquisa também tem muito mais extensões. Por exemplo, ao analisar malware, muitas vezes o executamos em sandboxes para registrar e compreender suas capacidades em um ambiente altamente monitorado. Essa execução baseada em sandbox tem duas desvantagens principais: (i) consome muitos recursos e (ii) se o malware perceber que está sendo executado em uma sandbox, poderá alterar seu comportamento para evitar ser detectado. Portanto, a pesquisa aqui reside em como realizar análises dinâmicas de malware sem desperdiçar recursos preciosos e como isso pode ser realizado contra malware evasivo [132, 133]. Além disso, precisamos encontrar métodos para acionar automaticamente o malware de forma adequada, sem criar longos caminhos de execução e desbloquear sua funcionalidade. Para este fim, a emulação binária e a execução simbólica podem ajudar. Por fim, devemos destacar que muitas chamadas de sistema realizadas por malware, se tratadas individualmente, nem sempre diferem muito daquelas emitidas por programas benignos; portanto, o malware evasivo ainda pode ignorar muitos classificadores que não

11.5.3 Aprendizado de máquina na detecção e classificação de malware

O uso contínuo de aprendizado de máquina e inteligência artificial na segurança cibernética também abriu caminho para sua aplicação na detecção e análise de malware. No entanto, temos que considerar que também pode ser aproveitado pelos autores de malware para contornar os mecanismos de detecção. Portanto, é essenci

considere que os autores de malware tentarão explorar algoritmos de seleção de recursos para tornar seu malware indetectável por alguns classificadores. Como resultado, o aprendizado de máquina e a inteligência artificial não podem simplesmente ser usados e esperar que forneçam resultados excelentes. Em primeiro lugar, temos de dedicar grandes esforços de investigação para compreender como preencher a lacuna nos conjuntos de dados desequilibrados, onde uma família de malware pode estar sub-representada. Em seguida, temos que estudar o aprendizado de máquina adversário e como tornar nossos mecanismos robustos contra possível injeção ou cegamento de recursos [255]. Deve-se também considerar a explicabilidade e a interpretabilidade dos resultados dos algoritmos de aprendizado de máquina e de inteligência artificial e como a engenharia de recursos pode afetá-los, já que amostras de malware podem ter milhares de recursos distribuídos de maneira esparsa. Finalmente, deve-se também considerar a relevância dos conjuntos de dados e modelos ao longo do tempo. O uso de conjuntos de dados e modelos mais antigos que podem ser o que há de mais moderno agora poderá em breve ter desempenho inferior ou inferior de

11.5.4 Ampliar o escopo da plataforma

Embora a maioria dos usuários de computadores pessoais use o Windows e represente um dos maiores alvos de ataques de malware, eles não são os únicos. Da mesma forma, nos dispositivos móveis o Android pode ter a maior participação nos smartphones, mas não é a única plataforma para dispositivos móveis. Além disso, todos sabemos que uma parte significativa da Internet não funciona apenas nestas duas plataformas e que malware foi desenvolvido para, por exemplo, dispositivos IoT, hosts baseados em Linux e MacOS, entre outros, concentrando a investigação apenas em Windows e O Android cria uma enorme lacuna que é explorada por agentes de ameaças que consideram muitas das plataformas menos focadas despreparadas. Por exemplo, a maior parte da pesquisa concentra-se em arquivos PE32, negligenciando, por exemplo, arquivos ELF direcionados a hosts Unix e Linux. Mesmo quando os investigadores tentam estudar ficheiros ELF, os conjuntos de dados são altamente desequilibrados, uma vez que a maioria das amostras provém de uma única família, ou seja, Mirai, o que pode distorcer gravemente os resultados. Portanto, há uma necessidade definitiva de ampliar o escopo das plataformas e arquiteturas usadas na pesquisa de a

11.5.5 Servidores de comando e controle

Finalmente, uma questão bastante espinhosa é a integração gradual de mecanismos descentralizados por malware para controlar a botnet, mas também para entregar cargas úteis. Por exemplo, blockchains e armazenamento descentralizado (por exemplo, IPFS) provaram ser mecanismos muito robustos para atuar como servidores de comando e controle, mas também para hospedar cargas úteis [12.184.188]. O ponto crucial aqui é que a maioria destes mecanismos descentralizados não são regulamentados (na verdade, alguns deles não podem ser) e os mecanismos de remoção podem nã

está comprometido no blockchain do bitcoin, não pode ser apagado. Assim, há muita pesquisa sobre como se proteger contra esse tipo de malware e como minimizar a exploração de tais ecossistemas.

11.5.6 Gestão pós-infecção

Reconhecer que não há 100% de precisão na detecção e prevenção de malware significa que, na prática, um determinado sistema será infectado por malware pelo menos uma vez. Naturalmente, pode-se perguntar quais devem ser os próximos passos quando um malware é detectado. A maioria das soluções antimalware existentes tenta impedir tentativas de infecção e limpeza. Talvez haja outras coisas que possamos fazer após a infecção para minimizar os danos ou facilitar a análise forense digital. Isso pode envolver a reversão automática do sistema para um estado imediatamente anterior à infecção. Embora para o armazenamento a opção de sistemas de arquivos incrementais possa fornecer uma solução, o mesmo não se aplica à memória.

11.6 Exemplos de problemas

Exemplos de problemas tangíveis podem incluir:

Servidores de comando e controle (C2) e mecanismos de defesa Para gerenciar os hosts comprometidos, muitos autores de malware usam servidores C2, alguns dos quais são comerciais, por exemplo, Cobalt Strike, cujas cópias vazaram, mas são legitimamente usadas em cenários de equipe vermelha. Independentemente da sua origem, os servidores C2 permitem que os agentes de ameaças coordenem as ações dos seus bots, emitam comandos, exfiltrem dados e realizem outros ataques. Atualmente, existem muitos servidores C2, muitos dos quais são de código aberto, e seria interessante estudar como diferentes mecanismos de segurança, por exemplo, AVs, EDRs, firewalls, tratam esses beacons e se eles são detectados como maliciosos. Padrões maliciosos na memória e nas chamadas do sistema podem ser aproveitados por meio de scanners de memória e conexões para bloquear imediatamente suas funcionalidades.

Classificadores de malware A grande quantidade de amostras de malware diariamente impõe muitas restrições de recursos e tempo. A classificação binária (benigna e malware) é um problema tradicional na área. Indo um passo além, a classificação e agrupamento familiar são muito importantes. Independentemente de estas análises serem realizadas com base em medidas de similaridade binária, características estáticas ou dinâmicas, é crucial determinar a sua precisão e robustez, especialmente num cenário adversário onde os atores da ameaça podem querer contornar os mecanismos de segurança, mas se isso falhar, levante uma bandeira falsa [25].

Mecanismos anti-evasão e mecanismos de acionamento O malware pode tentar escapar à detecção e à análise de várias maneiras. Automatizar o desvio de tais mecanismos e coletar resultados robustos de malware por meio da correlação de recursos estáticos e dinâmicos é um grande desafio. Como acionamos o malware adequadamente para exibir seu comportamento quando a análise estática indica que um arquivo é malicioso, mas a análise dinâmica não consegue detectar a maldade do arquivo em questão?

Canais de comunicação ocultos e malware Muitas ocorrências de malware tentariam ocultar seus canais de comunicação misturando suas intervenções com tráfego legítimo, por exemplo, usando uma rede social ou outro serviço legítimo para comunicação entre o servidor C2 e o host comprometido. No entanto, o malware pode usar esteganografia e outros canais secretos para exfiltrar dados ou disseminar comandos. Detectar possíveis comunicações secretas maliciosas e estegomalware é um problema desafiador.

Abuso de processos legítimos Living Off The Land Binários e Scripts (e também Bibliotecas)1 , comumente chamados de LOLBin/Script/Lib são arquivos enviados pela Microsoft no Windows e outras ferramentas (por exemplo, Office, Visual Studio), que possuem a assinatura da Microsoft e podem executar funcionalidades adicionais àquelas com as quais foram inicialmente projetados, por exemplo, baixar arquivos, executar conteúdo arbitrário, etc. incluído na lista de permissões da maioria dos mecanismos de segurança e pode ser encontrado em quase todas as máquinas Windows.

Os agentes de ameaças usaram repetidamente esses arquivos em campanhas maliciosas para trojanizar documentos do Microsoft Office e executar cargas maliciosas. Essa abordagem tem sido gradualmente abusada por outros malwares, especialmente ataques de malware sem arquivo [230]. Além disso, eles são abusados por ransomware para excluir cópias de sombra, por exemplo, cmd **para iniciar** o vssadmin **e excluir as cópias de sombra [136].**

Com base no exposto, o problema de pesquisa consiste em encontrar maneiras, baseadas, por exemplo, no contexto de chamada de API, nos pais e filhos dos processos e nos argumentos de chamada, para determinar se uma chamada para um processo legítimo, API, biblioteca ou binário está sendo abusado por malware ou se é de fato uma chamada benigna.

1https://lolbas-project.github.io/

12 Ciclo de Vida do Software

12.1 Introdução

O software está na base de todas as tecnologias digitais, portanto, está no centro de as infra-estruturas, serviços e produtos que impulsionam as nossas sociedades. O ciclo de vida de um software consiste em diversas fases, desde a concepção até através do projeto, realização, implantação, operação, manutenção e, eventualmente, descomissionamento. As abordagens atuais de desenvolvimento de software priorizam implantação rápida sobre segurança, o que muitas vezes resulta em soluções inseguras e caras reparo [202], aplicações. As preocupações de segurança ainda não são, infelizmente, totalmente e adequadamente integrados no ciclo de vida dos sistemas cada vez mais complexos de hoje sistemas de software [241]. Além disso, o software geralmente é construído através da montagem de componentes de fontes de terceiros, o que levanta preocupações de confiança (por exemplo, como evidenciado em ataques à cadeia de abastecimento [72]), dificulta o cumprimento das normas de segurar requisitos e legislação, e compromete a soberania digital. O aumento Espera-se que o uso de software sintetizado artificialmente agrave esta situação. Por último, segurança e regulamentações de privacidade, como o GDPR [93] ou a Lei de Segurança Cibernética [7], conforme bem como as expectativas dos cidadãos mudam frequentemente e o software está sujeito a atualizações contínuas. Como consequência, a conformidade do software não pode ser avaliada de uma vez por todas e precisa ser uma parte inerente do seu ciclo de vida [135]. O campo viu avanços desde as primeiras iniciativas para construir segurança em software sistemas [149] e esforços nessa direção foram feitos, como o Secure Software Development Framework do NIST [167], o Software Assurance do OWASP Modelo de maturidade [201], SDL da Microsoft [153] e padrão 303 645 do ETSI [78] (ver também o Capítulo 12 do Conjunto de Conhecimentos sobre Segurança Cibernética [56]). No entanto, muitos desafios permanecem (ver a última parte deste capítulo e também [135], como exemplos).

12.2 Quem será afetado?

Tradicionalmente, a garantia de software de alta qualidade era considerada principalmente relevante para infraestruturas críticas: finanças, cuidados de saúde, energia, etc. Contudo, o software está se tornando mais difundido e intrínseco, a tal ponto que pode ser visto como o sistema circulatório do corpo da nossa sociedade: você não pode

perceba que ele está ali, até que sua qualidade comece a afetar sua saúde. Hoje em dia, utilizamos software para regular o clima interior das nossas casas, para planear as nossas deslocações para o trabalho e para a escola, para realizar as nossas atividades diárias, para comunicar com colegas, familiares e amigos, para aceder a serviços e tratamentos médicos. , e assim por diante. Em última análise, a qualidade de vida de cada cidadão dependerá altamente da qualidade de vida do software que facilita as suas atividades.

12.3 O que se espera que aconteça?

Vulnerabilidades de software em sectores críticos podem ter consequências catastróficas para as nossas vidas: empresas e indivíduos podem perder dinheiro devido a falhas no software financeiro, o acesso a tratamentos pode ser atrasado por mau funcionamento em plataformas de software utilizadas em hospitais, vidas podem ser perdidas como resultado de software bugs em dispositivos médicos ou sistemas de assistência automóvel. O Capítulo 13 fornece uma amostra representativa de casos (in)famosos, como o desastre do Ariane 5 e a perda da sonda climática de Marte, e muitos outros podem ser acrescentados. Apenas para mencionar um exemplo recente, uma vulnerabilidade no contrato inteligente da Poly Network levou à perda de 600 milhões de dólares [89]. Mas mesmo as vulnerabilidades em casos que tradicionalmente não consideramos críticos podem ter consequências graves para os cidadãos individuais: a violação da privacidade pessoal é sem dúvida o exemplo mais ar

12.4 Qual é a pior coisa que pode acontecer?

As vulnerabilidades de software podem ter todo tipo de consequências catastróficas e certamente precisam ser abordadas. No entanto, garantir a qualidade do software é o mínimo que podemos fazer. O software também pode ser de alta qualidade e aderir aos mais rigorosos regulamentos de segurança e privacidade, como os mais altos níveis dos Critérios Comuns [36], mas ainda podem ser obtidos danos se houver falta de confiabilidade na forma como é desenvolvido, adquirido, usado, mantido e desmontado. Consideremos, por exemplo, o que pode acontecer se os cidadãos não confiarem no software que será utilizado nas próximas eleições democráticas. Até mesmo todo o sistema democrático de um país pode estar em risco.

12.5 Lacunas de Pesquisa

A segurança deve ser melhor integrada em todo o ciclo de vida do software, desde a concepção até ao desmantelamento. Consideramos as seguintes lacunas e possíveis caminhos a seguir para resolver isso.1

[1] Inspirado em parte pelo Manifesto VERSEN [241]

12.5.1 Software Verificável e Auditável

Grande parte dos componentes de software que constituem um produto ou serviço de software é obtida de terceiros; portanto, é potencialmente não confiável, pois pode não cumprir os requisitos de segurança esperados. Para alcançar a soberania digital, é necessário poder contar com software que possa ser verificado e auditado. O potencial ganho de segurança da utilização de software de código aberto passível de análise automatizada deve ser mais explorado.

12.5.2 Avaliação Contínua de Software

As regulamentações de segurança e privacidade e as expectativas dos cidadãos mudam frequentemente e o software está sujeito a atualizações contínuas. Portanto, a conformidade dos sistemas de software não pode ser avaliada de uma vez por todas e, portanto, são necessários métodos e ferramentas para realizar avaliações contínuas. Dado o elevado custo das avaliações de segurança e software, a utilização de procedimentos automatizados é fundamental para garantir a sustentabilidade e a escalabilidade. Se isto não for implementado de forma eficaz, o software torna-se demasiado complexo e a manutenção e a evolução tornam-se demasiado caras, até deixarem de ser sustentáveis. Temos de quebrar este ciclo vicioso e encontrar novas formas de criar software que seja duradouro e que possa ser atualizado, avaliado e migrado de forma rentável para novas tecnologias.

12.5.3 Desenvolvimento ágil de software seguro desde o projeto

As abordagens dominantes ao desenvolvimento são ágeis e dão prioridade à implementação rápida em detrimento das garantias de segurança. É necessária mais investigação para desenvolver de forma eficaz e eficiente ferramentas e técnicas que apoiem técnicas seguras desde a concepção no âmbito de abordagens ágeis, para que a competitividade e a rápida implementação não sejam comprometidas por requisitos de segurança e para que as alterações nesses requisitos possam ser reavaliadas de forma eficiente em qualquer momento, mesmo enquanto o software estiver em execução.

12.5.4 Métodos Formais Leves

Muitas tecnologias de métodos formais foram desenvolvidas para melhorar a confiabilidade do software, como verificação de modelos, prova de teoremas e sistemas de monitoramento, mas aplicá-los em larga escala a sistemas de software modernos continua sendo um desafio. São necessários mais esforços para desenvolver e promover métodos formais leves e acessíveis que possam ser gradualmente aplicados para aumentar os níveis de garantias obtidos. Devem ser desenvolvidos métodos para apoiar um espectro de níveis de garantia, cada um proporcionando maior garantia, de uma forma mais acessível do que os critérios comuns. Eventuais aplicações regulatórias devem ser graduais, a fim de não fechar a oportunidade para as PME fornecerem produtos e serviços de software, e é necessário um suporte de ferramentas adequado.

12.5.5 Governança Descentralizada de Software

Softwares com governança descentralizada, como contratos inteligentes, tecnologias blockchain e criptoativos, apresentam diversos desafios à gestão do ciclo de vida do software. Nesses sistemas, não está claro se e como as vulnerabilidades devem ser comunicadas e reparadas de uma forma que harmonize o consenso e a segurança ao longo da história do sistema.

12.5.6 Ciclo de vida de software confiável baseado em IA

Técnicas de inteligência artificial já estão sendo utilizadas para sintetizar pequenos pedaços de código. Deve-se esperar que num futuro próximo todas as atividades do ciclo de vida do software (elicitação de requisitos, síntese de código, verificação, monitoramento, etc.) sejam apoiadas por agentes inteligentes. Embora isto certamente traga enormes avanços em termos de escalabilidade e produtividade, ainda não está claro como os componentes de software e metodologias com componentes inteligentes podem ser analisados com rigor.

12.5.7 Segurança da Cadeia de Fornecimento de Software

Hoje em dia, a criação e implantação de software envolve a integração de códigos e componentes de terceiros, cujo desenvolvimento está fora do nosso controle. Estes componentes podem ser alvo de ataques cibernéticos (por exemplo, o incidente SolarWind). Precisamos definir uma metodologia para reduzir os riscos de segurança da cadeia de abastecimento, através da avaliação e garantia da confiabilidade dos componentes. Esta metodologia deve basear-se em modelos formais de desenvolvimento e integração de linhas de software baseadas em contratos, de forma a permitir a implementação de ferramentas (semi)automáticas para a verificação de propriedades de segurança. O desenvolvimento destes modelos e dos métodos formais correspondentes são uma impo

12.5.8 Arquiteturas e Plataformas Seguras

Para construir sistemas críticos de segurança, não basta ter uma cadeia de fornecimento de software confiável: precisamos implantar esse software em plataformas confiáveis. Isto inclui o nível de hardware, mas em particular o nível do sistema operacional. Portanto, uma importante prioridade de pesquisa é desenvolver uma plataforma verificada que forneça controle de acesso refinado por meio de capacidades e controle a comunicação entre os componentes do sistema. Este tipo de plataformas é muito procurada em cenários operacionais (ex. SCADA de infraestruturas críticas) mas também em datacenters que prestam serviços cloud. Isto ajudaria a recuperar a soberania dos dados n

12.5.9 Economia Segura

Outra direção interessante de pesquisa está relacionada à economia da segurança, ou seja, a estudo dos incentivos enfrentados pelos diferentes intervenientes [71]. Agora está bem estabelecido que soluções puramente tecnológicas não serão adequadas. Assim, cada mecanismos alternativos devem ser examinados em função da dinâmica do mercado.

12.6 Exemplos de problemas

Exemplos de problemas tangíveis podem incluir:

Verificação na escala de repositórios públicos de código-fonte aberto. As técnicas formais de verificação oferecem o mais alto nível de garantia para a segurança do software. Os principais desafios das técnicas atuais são, sem dúvida, devido problemas de escalabilidade em termos de experiência computacional e humana necessário. Como podemos elevar as técnicas de verificação bem-sucedidas à escala de bases de código do tamanho de repositórios de código público populares médios?

DevSecOps baseado em métodos formais O DevSecOps tem sido defendido como um abordagem ideal para combinar DevOps e segurança, a fim de fornecer um ciclo de vida contínuo, ágil e com rápida adaptação, consciente da segurança. No por outro lado, métodos formais, que fornecem o nível mais alto possível de garantia em termos de segurança, proteção e desempenho, foram tradicionalmente concebido com uma mentalidade de cascata, enraizada em especificações formais como primeiro passo. Podemos desenvolver metodologias ágeis de métodos formais no que poderia ser chamado de DevSecOps formal?

Análise Formal de Sistemas de Software Sócio-Técnicos e Ciber-Físicos. Os sistemas sociotécnicos, cuja segurança depende intrinsecamente da usuários e sistemas ciberfísicos, onde é necessário considerar explicitamente os processos físicos subjacentes, colocam vários desafios à modelagem, análise e testes automatizados formais. Podemos desenvolver ferramentas formais e automatizadas eficazes e escaláveis para análise e teste de tais sistemas?

Verificação de aplicativos de ML. Componentes de software probabilísticos e aleatórios estão no centro de muitas aplicações de software, desde criptografia até aprendizado de máquina (ML) e proteção de privacidade. Os últimos anos vimos avanços nas técnicas de programação probabilística e verificação técnicas para ML. No entanto, o campo ainda está na sua infância, enquanto, no por outro lado, a aplicação do BC tem avançado rapidamente. Como pode estendemos a programação probabilística para lidar com o mundo real baseado em ML formulários?

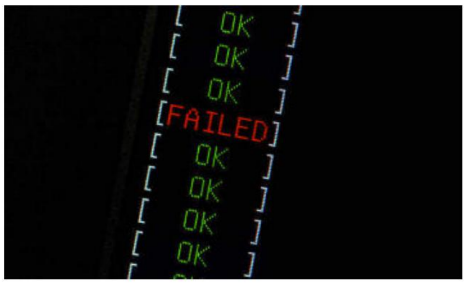
Reparo de contrato inteligente resiliente Se uma vulnerabilidade de segurança for descoberta em um contrato inteligente, denunciá-lo -ou tentar repará-lo- poderia desencadear uma corrida por

sua exploração, que provavelmente resultará em ganhos financeiros para agentes maliciosos. Podemos projetar técnicas de divulgação e reparo que permitam que agentes maliciosos resilientes tentem obter lucro?

Explicabilidade segura e amigável à privacidade. A segurança explicável estende a IA explicável com a necessidade de considerar aspectos de segurança e privacidade do processo de explicação e das próprias explicações. Como podemos adaptar as abordagens à explicabilidade para levar em conta considerações de segurança e privacidade?

13 Testes e Certificação

13.1 Introdução



A tecnologia da informação (TI) está difundida tanto nos setores laborais como sociais. Casas, indústrias, escritórios, carros, ruas e edifícios públicos estão cheios de dispositivos de TI, aplicativos de sistemas ou equipamentos eletrônicos. No nosso dia a dia, em condições normais, normalmente não nos preocupamos com a tecnologia que nos rodeia. Temos razoável certeza de que nosso celular, PC, geladeira, dispositivo eletrônico, carro ou mesmo aplicativos não podem prejudicar nossa vida, roubar dados ou causar problemas de segurança ou proteção, porque deveriam ter sido construídos de acordo com os padrões exigidos , devidamente testado e totalmente certificado.

No entanto, assistimos recentemente a vários exemplos de avarias ou problemas como os seguintes: Tesla teve uma falha num dispositivo de memória flash, causando um risco de segurança em mais de 135.000 veículos [163]; o bug no sistema de agendamento de vacinas hospitalares de Nova Jersey causou de 10 a 11 mil consultas duplicadas [65]; o aplicativo Zoom sofreu problemas de segurança durante a pandemia de coronavírus em 2020 [1].

Conforme relatado na recente lei de segurança cibernética, "os produtos de hardware e software estão cada vez mais sujeitos a ataques cibernéticos bem-sucedidos, levando a um custo anual global estimado do crime cibernético de 5,5 trilhões de euros até 2021" [79]

Os seres humanos e a sociedade geralmente confiam nas indústrias e nas melhores práticas que adotam nos processos de testes e certificação. No entanto, considerando que o custo global dos testes é de cerca de 40% dos custos totais de desenvolvimento de um projeto de software típico [91], se não forem rigorosos e sem riscos concretos de segurança, muitas vezes os procedimentos de verificação, validação e avaliação são os primeiros a serem reduzido ou ignorado para economizar tempo e custo. Além disso, a pressão da necessidade de pesquisar novos produtos, o tempo de colocação no mercado e as forças

indústrias e desenvolvedores em direção à integração massiva e generalizada e ao uso de componentes disponíveis de terceiros ou de código aberto que poderiam aumentar subrepticiamente os riscos de segurança cibernética se não forem devidamente testados e certificados.

Em um mundo de TI que será mais centrado no ser humano e focado nas necessidades das pessoas (como o manifesto Internet of People [IoP] [157]), a presença de evidências da atividade de teste e certificação realizada precisa se tornar uma prática comum. Precisamos aumentar a nossa conscientização para evitar produtos de TI "envenenados", bem como alimentos envenenados. Portanto, o nível de qualidade avaliado ou certificado deve ser um rótulo para cada produto de TI, a fim de estabelecer confiança e reduzir riscos à segurança e à privacidade.

A qualidade dos produtos digitais (combinação de software e hardware) deve tornar-se um selo de garantia, da mesma forma que o rótulo que encontramos nos alimentos que compramos nos supermercados.

13.2 Quem será afetado?

Todos que utilizam direta ou indiretamente produtos ou tecnologias podem ser afetados pela falta de processos de testes e certificação. Por exemplo, os bebés podem ser danificados por um brinquedo fora de controlo, a Geração Alfa ou Zeta podem ser inconscientemente enganadas por aplicações apelativas que roubam maliciosamente as suas imagens, as empresas podem ser afetadas por ransomware escondido em plug-ins ou bibliotecas úteis, organizações e governos podem ser alvo de ataques de segurança cibernética. É claro que os testes e a certificação não são os únicos meios de evitar tais situações críticas. Tudo deve ser executado corretamente em todas as fases do processo de desenvolvimento (veja o Capítulo 12 para detalhes). Conceber e desenvolver produtos de qualidade (por design) é crucial, mas não é suficiente por si só para atender aos requisitos finais: construir o produto certo não garante a construção do produto certo [217]. Os testes e a certificação continuam a ser atividades essenciais para a garantia da fiabilidade e da segurança cibernética e para garantir que um produto é concebido e fabricado tendo a qualidade como objetivo principal.

No entanto, enquanto as partes interessadas (pessoas comuns, empresas, organizações e governos) não exigirem firmemente produtos transparentes, rotulados, testados e certificados, a situação dificilmente mudará e os riscos de segurança cibernética continuarão na agenda.

13.3 O que se espera que aconteça?

Qual é o dano esperado na ausência de um processo adequado de testes e certificação? Infelizmente, há muitos aspectos a serem considerados:

Falha de hardware/software: Estima-se que quase 80% do tempo de inatividade inesperado pode ser atribuído a falhas de HW/SW e cortes de energia. Backups de armazenamento adequados podem ser uma solução ad hoc na maioria dos casos, mas prevenir o fracasso seria menos dispendioso e arriscado.

Desastres naturais e situações de emergência: Falta de testes e certificação dos processos e procedimentos para a retomada das operações/dados e sistemas em caso de desastre (natural) ou situações de emergência podem ser extremamente dispendiosos e causar a perda de continuidade dos negócios.

Fator humano: mesmo que não intencionalmente, os humanos podem inevitavelmente causar erros ou execução de procedimentos inesperados. Testes baseados em perfis de usuário ou a exploração de abordagens de aprendizado de máquina poderia evitar ou prever possíveis comportamentos inadequados ou situações acidentais. Avaliação centrada no usuário processos e programas de treinamento podem ser essenciais para minimizar danos humanos e evitando perdas permanentes.

Ataque à cibersegurança: Porque a sociedade e as organizações dependem cada vez mais de informações digitais para operações diárias, os ataques à segurança cibernética podem ser mais perigoso. Atualmente, 95% das empresas investem em testes e atividades de certificação somente após um desastre e então acionar um plano de recuperação (comportamento reativo). Prever vulnerabilidades antecipadamente e fornecer soluções antes de um ataque à segurança cibernética é, portanto, obrigatório (comportamento proativo). O teste de penetração é fundamental para evitar e antecipar ataques cibernéticos de hackers que tentam explorar vulnerabilidades potenciais para acessar redes de empresas e roubar dados confidenciais ou para injetar códigos maliciosos.

Altas expectativas: : Em nosso mundo hiperconectado, onde os produtos de TI precisam estar disponível 24 horas por dia, 7 dias por semana, sem interrupções, falhas e perdas de serviços são desastres dispendiosos para as empresas e favorecem os seus concorrentes. Portanto, processos robustos de testes e certificação, que possam garantir a qualidade dos serviços e permitir estabelecer uma recuperação adequada plano, são atividades essenciais.

Danos à confiança ou à reputação: A perda de confiança ou danos à reputação são principalmente traduzido em perda de clientes e, portanto, perda de receita: confiança e reputação são quase impossíveis de recuperar. Testes e certificação são entre os meios mais eficazes para evitar este problema.

Requisitos de conformidade: Hoje em dia, a continuidade dos negócios não é apenas uma mera desejo: está se tornando uma exigência, especialmente para Operadores de Serviços Essenciais (OESs) [47]. Todos eles devem seguir regras específicas e rigorosas regulamentos e normas. Isso significa que adotar processos de certificação e manter a certificação de seus produtos está se tornando uma obrigação legal.

obrigação e oferece uma vantagem competitiva no mercado de referência.

13.4 Qual é a pior coisa que pode acontecer?

Descobrir o que poderia acontecer sem testes e certificação não deveria apontam para o futuro, mas simplesmente para o passado. A maioria dos piores cenários tem já foram cobertos nos jornais, nos relatórios de inadimplência e na documentação sobre desastres. A história dos piores bugs começou assim que o primeiro computador foi massivamente usado e incluiu:

- O desastre do Ariane 5, 4 de junho de 1996. Durante o lançamento do Ariane 5, 37 segundos após o primeiro foguete ser acionado, ele começou a virar na direção errada, e menos de dois segundos depois o mundo inteiro observou sua autodestruição. O problema foi rapidamente identificado como um bug de software no sistema de referência inercial do foguete e, infelizmente, poderia ter sido facilmente resolvido com um teste de integração trivial procedimento [247].

- The Mars Climate Orbiter, 23 de setembro de 1999. Durante sua descida na atmosfera marciana, o Mars Climate Orbiter foi reorientado passar por trás de Marte e entrar com sucesso em sua órbita. Infelizmente, isso Isso não aconteceu: a nave não estava na trajetória correta e finalmente se perdeu sem deixar rastros. A análise da causa raiz deste erro produziu um longa cadeia de eventos errados ou inesperados, que incluíram: a disposição acidental de painéis solares na embarcação devido ao efeito vela solar; o uso de duas unidades diferentes no software Ground Control (dados fornecidos usando unidades imperiais e libras-segundos no lado do remetente, mas esperado em unidades métricas no lado do receptor); e, finalmente, erros humanos nas comunicações. Novamente, procedimentos adequados de teste de integração e o uso correto de padrões e procedimentos de avaliação teria evitou um desastre tão crítico [105].

- Therac-25 Durante o período de 1992 a 1998, foram publicados os relatórios sobre overdoses de radiação causadas pela radioterapia controlada por computador dos anos 80. Em particular, ocorreram seis acidentes documentados, resultando em mortes ou ferimentos graves. As causas foram identificadas como aplicação de procedimentos incorretos por parte do pessoal e as fraquezas do software utilizado para garantir a segurança. Em particular, todos os acidentes envolvendo software resultaram de requisitos de software falhos. Aplicação de processos de certificação e sistema adequado e aceitação O processo de teste teria novamente evitado perdas significativas de vidas [140].

- Knight Capital Group Em 1º de agosto de 2012, durante uma atualização de software do o servidor de produção, uma configuração incorreta de um sistema antigo (2003)

causou 97 notificações por e-mail e a execução de 4 milhões de negociações inesperadas. Isso levou a uma perda de US$ 460 milhões e ao risco de falência. A pós-análise destacou que o programa acreditava estar em um ambiente de teste e executou as negociações o mais rápido possível, sem se preocupar em perder o valor do spread. Como nos casos anteriores, o processo de teste teria descoberto esse mau comportamento e evitado o uso de software obsoleto e não alinhado [189].

É provável que os erros do passado tenham sido resolvidos e as lições aprendidas, mas desafios, vulnerabilidades e novos cenários surgem constantemente. Quem não se lembra do bug do Milénio [4]? Ou o ataque cibernético de 2018 que interrompeu as comunicações no Midcontinent Independent System Operator? Ou mesmo as seis/sete horas de indisponibilidade global da rede social Facebook e das suas subsidiárias em outubro de 2021 [228]? Ou os recentes ataques de ransomware na rede de TI?

A descoberta e o fornecimento inteligente e rápido de novas tecnologias, linguagens de programação e sistemas obrigam os testes e a certificação a saltar continuamente "De volta ao futuro" e a fornecer novos meios, estratégias e processos para prevenir futuros piores cenários. Na verdade, a história ensina que o passado pode sempre transformar-se no futuro e vice-versa.

O que pode acontecer de pior? Uma vida sem testes e certificações, porque significa falta de qualidade, eficiência e confiança em cada sistema e pacote de software.

Na verdade, os testes e a certificação procuram mitigar os riscos de perda ou ausência de segurança, proteção e privacidade para qualquer pessoa em todo o mundo. Quem usaria uma máquina sem que ela fosse testada? Quem estaria disposto a abrir um centro médico sem ser certificado? Quem poderia pensar em dar a uma criança brinquedos que colocassem a sua vida em risco?

Produtos, elementos, componentes e bibliotecas de HW ou SW inseguros, não seguros ou não confiáveis tornam o mundo perigoso: eles podem causar desastres ambientais; podem desempenhar um papel no incumprimento ou na falência de empresas, indústrias e até de nações; podem ter impacto em serviços essenciais (ou seja, energia, transportes, serviços financeiros e bancários, cuidados de saúde, abastecimento e distribuição de água potável e infraestruturas digitais); podem comprometer os sistemas de saúde ou os dispositivos médicos. A actual situação internacional também pode criar cenários ainda mais dramáticos: as vulnerabilidades de HW/SW e as ameaças à segurança poderiam ser exploradas para permitir ataques terroristas a centrais nucleares e bases militares.

Felizmente, neste cenário apocalíptico catastrófico, aprendendo com o passado e concentrando-se no futuro, a investigação e a indústria estão a começar a compreender a importância de uma colaboração rigorosa em testes e certificação para prevenir eficazmente os desastres antes que estes aconteçam.

13.5 Lacunas de Pesquisa

Considerando que “Os testes de programas podem ser utilizados para mostrar a presença de bugs, mas nunca para mostrar a sua ausência. (Dijkstra)“ [61], testes exaustivos são geralmente impossíveis, e as questões e problemas nos testes e na certificação estão longe de estarem esgotados. Novos desafios são continuamente adicionados em paralelo ao desenvolvimento de novas tecnologias, recursos, linguagens e domínios de aplicação, e à descoberta de novas vulnerabilidades e ameaças. Em particular, as seguintes áreas são tendências recentes nas a

13.5.1 Testes e Certificação Centrados no Ser

Humano Apoiar abordagens de testes e certificação centrados no ser humano que sejam capazes de orientar, melhorar e avaliar o desenvolvimento tecnológico em linha com valores sociais e éticos, sustentabilidade e confiabilidade. Além disso, aumentar a inclusão através do apoio ao equilíbrio de género e da diversidade das diferentes partes interessadas envolvidas na abordagem de testes e certificação pode garantir uma sensibilização pública confiável, a ampla adoção de métodos de TI e a adoção de normas para aumentar a transparência e a abertura.

13.5.2 Certificação integrada de segurança cibernética e segurança funcional

Além de intercalar e sobrepor vários aspectos da segurança e cibersegurança, ainda existe uma lacuna no fornecimento de um quadro abrangente e de normas técnicas para a sua plena integração. Na verdade, a garantia/certificação de segurança não pode ser alcançada sem considerar o impacto das vulnerabilidades e ameaças de segurança cibernética no sistema. Assim, há necessidade de fornecer uma abordagem integrada baseada em riscos de garantia de segurança funcional/cil

13.5.3 Testes e certificação quantitativos e qualitativos A

responsabilização e a replicabilidade são características essenciais das abordagens de modelagem, teste e certificação de segurança cibernética e exigem métodos e meios para a coleta quantitativa e qualitativa e a análise de resultados e dados. Assim, a disponibilidade de conjuntos de dados de código aberto e conjuntos de testes de conformidade, uma vez que as instalações para a configuração e execução de experimentos controlados devem ser melhoradas. Em particular, os desafios centram-se em: (1) Melhorar os métodos formais para a modelação e análise quantitativa da segurança e a sua aplicação à gestão de riscos, enriquecendo os seus aspectos baseados em dados, por exemplo, sintetizando e refinando modelos de cenários de ataque (possivelmente subespecificados) e validando-os relativos a dados de ataques anteriores. (2) Realização de abordagens de modelagem, teste e certificação impulsionadas por riscos de segurança cibernética (3) Tornar a coleta de dados, abordagens/ ferramentas de quantificação e análise de resultados mais acessíveis aos profissionais e com

tornando-os mais focados em propriedades qualitativas. (5) Fazendo testes e certificação desde o design, guiada por histórias de usuários, requisitos de necessidades específicas de domínio e padrões. (6) Fornecer métricas, diretrizes e abordagens para proteger produtos e serviços durante toda a sua vida.

13.5.4 Automação de Testes e Certificação

Testes e certificação são atividades complexas, caras e demoradas. Reduzir o esforço e mitigar os custos e riscos da segurança cibernética é um desafio significativo para a automação alcançável. Orientações importantes são:

1. Desenvolver técnicas avançadas, encontrar procedimentos de apoio inovadores para automatizar (totalmente) as diferentes atividades, ou fornecer métricas, diretrizes e abordagens aplicáveis ao longo de todo o ciclo de vida do processo

2. Fornecer uma metodologia holística que integre tempo de execução e design métodos de tempo aplicáveis em diferentes níveis de especificação - como firmware, protocolos de comunicação, pilhas, sistemas operacionais (SOs) e interfaces de programação de aplicativos (APIs) - e isso considera a integração de software e hardware.

3. Especificar e desenvolver KPIs, métricas, procedimentos e ferramentas gerenciáveis e centrados no ser humano para segurança cibernética dinâmica e automática certificação do chip ao software e níveis de serviço.

13.5.5 Diversidade, heterogeneidade e flexibilidade de ambientes

Diversidade, heterogeneidade e flexibilidade são atributos desafiadores dos testes e propostas de certificação. Em particular, quaisquer abordagens e soluções fornecidas devem evoluir de acordo com os níveis de investigação verticais e horizontais. Na verdade, ecossistemas e sistemas de sistemas (SoS) dependem da integração contínua de componentes, aplicativos e dispositivos desenvolvidos em diferentes linguagens e sistemas operacionais, e na combinação e acesso a milhares de combinações de dispositivos-navegador-plataforma simultaneamente. Para evitar o risco de se tornar desatualizados, os testes e a certificação necessitam de esquemas altamente flexíveis e modulares que se adaptam rapidamente às mudanças e atualizações do ambiente tecnológico e dos elementos em cada nível horizontal ou vertical. Além disso, para seguir a evolução rápida e generalizada dos diferentes ambientes da cadeia de abastecimento (como as infraestruturas críticas descritas no Capítulo 9) e novas tecnologias (como os metaversos descritos no Capítulo 10), propostas holísticas e modulares necessários, capazes de validar, verificar e certificar de forma eficaz e eficiente o diferentes elementos HW/SW sob condições reais de usuário e considerando outros sistemas interativos e domínios de aplicação.

13.5.6 Incluindo aspectos legais nos testes e certificação

A interação entre os elementos HW e SW nos sistemas atuais promove uma nova direção para testes de segurança cibernética e pesquisa de certificação: incluir aspectos legais nos procedimentos de verificação, validação e avaliação. O o quadro jurídico e os padrões técnicos devem ser considerados parâmetros necessários durante o ciclo de vida do desenvolvimento (para mais detalhes, consulte o Capítulo 12). Na verdade, as vulnerabilidades de segurança cibernética podem causar violações legais, especialmente em aplicações sensíveis, como os cuidados de saúde. A direção futura é garantir que a cibersegurança, a segurança e os requisitos legais sejam testados e certificados como aspectos inseparáveis do mesmo processo.

13.6 Exemplos de problemas

Exemplos de problemas tangíveis podem incluir:

Testando o desconhecido. SoSs integram continuamente vários novos dispositivos e componentes; alguns deles podem não ter sido testados e quaisquer falhas intrínsecas será herdado. A pesquisa deve abrir caminho para novos testes paradigmas para alcançar metodologias de teste auto-adaptativas visando garantir que componentes e dispositivos desconhecidos e não testados sejam confiáveis e ter boa qualidade antes de ingressar no SoS. Por outras palavras, esta investigação deve promover a "Qualidade Plena – soma positiva, não soma zero".[1]

Teste de AI/ML/DL. Fornecer metodologias e ferramentas de teste que possam ser adequado para revelar bugs em aplicações de inteligência artificial (IA), aprendizado de máquina (ML) ou aprendizado profundo (DL). O estudo deve considerar os seguintes três aspectos principais: as condições exigidas (correção, robustez, segurança e privacidade); os itens AI, ML ou DL (por exemplo, os dados, o programa de aprendizagem ou a estrutura utilizada); e os testes envolvidos atividades (geração de casos de teste, identificação e definição do oráculo de teste, e critérios de adequação dos casos de teste).

Usando AI/ML/DL para testes. Fornece metodologias baseadas em AI/ML/DL e ferramentas que podem ajudar a realizar a maioria das tarefas de teste, como geração de casos de teste, classificação de casos de teste, derivação de oráculo ou análise de mutação, para citar alguns. Portanto, esta pesquisa visa alavancar o estado da arte Tecnologias AI/ML/DL para ajudar os testadores de software e hardware a alcançar a qualidade desejada impulsionada pelos dados de teste.

Compreendendo a testabilidade do metaverso. Melhorar a compreensão dos desafios de testar o metaverso considerando três testes

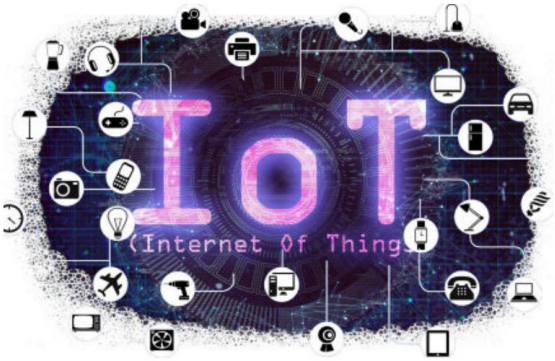
1Este termo é inspirado no conhecido princípio de privacidade desde o design "Funcionalidade total: soma positiva, não soma zero" [35]. Consulte também o Capítulo 8.

pilares: segurança cibernética, voltada para testes de segurança; Testes de API, cruciais para garantir a interoperabilidade, característica fundamental da metaexperiência; e testes interativos e imersivos, que colocam o ser humano no centro dos testes de metaexperiências.

Somos todos testadores. Melhorar a compreensão do papel dos humanos no processo de teste. A investigação deverá fornecer teorias, conhecimentos e soluções práticas para envolver as pessoas nos testes e na avaliação de produtos e serviços digitais, considerando diferentes dimensões da etnografia (digital). O ponto de partida para este tipo de pesquisa deve ser a gamificação, que visa converter tarefas de teste em componentes de jogabilidade, e testes de crowdsourcing (também conhecidos como crowdtesting), que é uma abordagem emergente para envolver usuários e especialistas em testes de ações. atividades.

14 Segurança de IoT

14.1 Introdução



A Internet das coisas (IoT) é uma coleção de dispositivos (ou seja, coisas) que contêm sensores e/ou atuadores, software e recursos de comunicação para enviar e trocar dados com outros dispositivos na Internet. . A ideia da IoT já nos acompanha há algum tempo e a sua segurança sempre foi e ainda é um dos seus principais desafios.

Com o tempo, os tipos e capacidades dos dispositivos diários conectados a uma rede continuam a crescer rapidamente. IoT Analytics [106] estimou que o número de dispositivos IoT conectados em 2021 foi de 12,2 bilhões globalmente. Enquanto isso, o Statista [238] estimou um número mais modesto de 11,3 bilhões de dispositivos IoT conectados em 2021. A previsão é que o número de dispositivos mais que dobre até 2030, com o Statista estimando 29,4 bilhões de dispositivos IoT conectados A IoT representa uma das maiores preocupações de segurança no momento e no futuro, uma vez que se prevê que o número de tais dispositivos cresça e permeie todos os aspectos da vida ainda mais profundamente. Isto é corroborado pelo fato de que os dispositivos IoT, em média, são atacados cinco minutos após serem conectados à Internet [158].

Embora a maioria possa pensar em frigoríficos inteligentes, aspiradores robóticos ou relógios inteligentes quando ouvem a palavra IoT, existem muitos mais dispositivos deste tipo que nos apoiam e rodeiam na nossa vida quotidiana, bem como nas indústrias. A IoT pode ser usada em muitas áreas para ajudar a otimizar e/ou automatizar processos através da coleta de dados em tempo real. As aplicações mais comuns da IoT incluem casas inteligentes, cidades inteligentes, gestão de resí

indústria (ou seja, Indústria 4.0), agricultura, cuidados de saúde inteligentes, armazéns inteligentes, transportes e logística inteligentes, etc. Do ambiente onde são utilizados e da sua finalidade, podemos derivar diferentes tipos de IoTs. Por exemplo, Internet das Coisas Industriais ou Internet das Coisas Industrial (IIoT), Internet das Coisas do Consumidor (CIoT), Internet das Coisas Médicas (IoMT) ou Internet das Coisas da Saúde (IoHT), Internet das Coisas Agrícolas ou Internet das Coisas Agrícolas (IoT), Internet das Coisas Energéticas (IoET), Internet dos Veículos (IoV), Internet das Coisas de Transporte (IoTT), Internet das Coisas Educacionais (IoEdT), etc.

Há uma lista considerável de propriedades que tornam vulneráveis os dispositivos e redes IoT. Por exemplo, a omnipresença dos dispositivos IoT torna difícil protegê-los contra o acesso físico. Ao mesmo tempo, a diversidade de dispositivos torna difícil projetar construções de segurança “de tamanho único” que possam ser aplicadas livremente aos dispositivos. Ainda mais, o rápido ciclo de vida (dos próprios dispositivos e do processo de desenvolvimento) também torna difícil rastrear os dispositivos no mercado e aplicar patches de software. As vulnerabilidades descobertas podem ficar sem correção por um longo período de tempo e, mesmo que haja uma correção, a maioria dos usuários não consegue atualizar regularmente os dispositi

Para piorar a situação, os dispositivos IoT muitas vezes ficam com as configurações de segurança padrão (por exemplo, senhas de fábrica), o que os deixa ainda mais vulneráveis. E, finalmente, vários dispositivos IoT são bastante pequenos, com potência, memória e capacidades computacionais limitadas. Isso geralmente significa que eles não são capazes de executar os melhores mecanismos e protocolos de segurança e, em vez disso, devem usar soluções menos exigentes em termos computacionais e com uso intensivo de recursos, que geralmente não são tão seguras.

Enfrentar desafios comuns no ecossistema IoT, dos quais a segurança é certamente um dos mais importantes, é fundamental para o futuro da IoT, especialmente à medida que a IoT se torna cada vez mais enraizada nas nossas vidas e já não representa uma ameaça apenas às nossas informações sensíveis, mas também aos nossos bens físicos e saúde. Apesar de toda a conveniência e valor que a IoT oferece, os riscos também são incomparáveis.

14.2 Quem será afetado?

Os dispositivos IoT afetam quase todas as pessoas. Por exemplo, os indivíduos podem ser afetados de muitas maneiras. Se uma casa inteligente for atacada e parar de funcionar corretamente, os habitantes podem perder energia, aquecimento, luz, entretenimento, etc. Câmeras web e monitores de bebês também são dispositivos IoT domésticos muito comuns que são atacados regularmente e já foram usados para espionar seus proprietários ou fazer parte de uma botnet. Os indivíduos também podem ser afetados indiretamente se o ataque visar a sua organização, o seu governo ou qualquer outra entidade da qual façam parte.

As indústrias também podem ser afetadas negativamente pelos ataques à IoT. Na verdade, um ataque bem-sucedido a esse sistema IoT causaria a cessação das operações. Qualquer organização na cadeia de abastecimento também sofreria consequências, especialmente se o ataque foi dirigido a organizações postais/de transporte que gerem o transporte de mercadorias. Embora isso seja mais verdadeiro para organizações ou indústrias que lidam com a manufatura, os serviços online são mais vulneráveis a coisas como DDoS Ataques de negação de serviço distribuída (Distributed Denial of Service), que tornam os serviços on-line inacessíveis, sobrecarregando os provedores de serviços com solicitações falsas. Alguns dos maiores desses ataques foram lançados a partir de dispositivos IoT sequestrados que formaram um botnet (uma grande coleção de dispositivos que foram atacados e subvertidos com sucesso para atender às ordens do invasor: por exemplo, [178, 206]).

Para eficiência e transparência, muitas infraestruturas críticas e serviços governamentais (por exemplo, energia, água e gestão de resíduos) estão se tornando IoT suportado. Qualquer ataque que possa prejudicar qualquer um deles por um período prolongado quantidade de tempo causaria estragos na população e ressentimento em relação o governo. Ataques contra IoT também poderiam ser usados para espionar políticos ou, novamente, usando ataques DDoS, para tornar indisponíveis serviços governamentais suportados digitalmente (por exemplo, eHealth).

14.3 O que se espera que aconteça?

À medida que a IoT progride para se tornar parte de tudo, muitas coisas poderão ser afetado quando algo dá errado. Câmeras web, babás eletrônicas, voz assistentes, brinquedos inteligentes e ferramentas semelhantes podem monitorar as atividades das pessoas e conversas (por exemplo, [108, 165, 192]). Os dispositivos médicos coletam informações altamente confidenciais, incluindo dados de saúde protegidos. Sensores de temperatura inteligentes podem diga às pessoas quando alguém está em casa, e as fechaduras inteligentes podem deixá-las entrar quando eles não são. Dispositivos IoT usados na fabricação podem ser usados para fins industriais espionagem para obter informações confidenciais sobre processos de fabricação e procedimentos, ou todo o processo de fabricação poderá ser interrompido. Os ataques à IoT no transporte e armazenamento inteligentes perturbarão as cadeias de abastecimento. Os ataques podem afetar o tráfego onde o gerenciamento inteligente de tráfego é usado, e os invasores podem assumir o controle de carros inteligentes se conseguirem obter acesso (por exemplo, [100]). Ao ata gestão inteligente da água e das redes eléctricas, grandes regiões podem ficar sem energia e água, o que paralisa qualquer indústria e faz com que as pessoas há dificuldades para cozinhar e manter-se aquecido no inverno. Na agricultura, um ataque bem-sucedido que não seja notado com rapidez suficiente pode levar à ruína colheitas ou gado morto. Ter dispositivos IoT expande a superfície de ataque, por isso podemos esperar ataques mais bem-sucedidos por invasores que obtêm acesso a áreas protegidas redes através de dispositivos IoT aparentemente inconsequentes (por exemplo, [245]). Grande quantidades de dispositivos IoT corrompidos com sucesso serão mescladas em botnets

que serão então usados para mineração de criptografia ou para realizar grandes ataques, como DDoS, para paralisar serviços online ou partes inteiras da Internet (por exemplo, [58]). Os ataques de IoT virão regularmente na forma de resgate, onde os invasores exigirão dinheiro para interromper um ataque ou não iniciá-lo.

Dados estes poucos exemplos, o dano potencial que poderia ser causado pela perda de segurança nos sistemas IoT é imenso. As consequências incluem perda de privacidade, roubo de identidade, efeitos sobre a saúde ou mesmo perda de vidas, roubo de propriedade intelectual/vantagem competitiva, perda de propriedade, escassez de bens, diminuição da produção de alimentos, indisponibilidade de serviços online, dificuldades com o fornecimento de eletricidade e outras fontes de energia, etc.

14.4 Qual é a pior coisa que pode acontecer?

Na seção anterior, tentamos mostrar o quanto poderia dar errado se os sistemas IoT fossem comprometidos. Nesta seção, entretanto, queremos apresentar alguns dos piores casos de escalada desses exemplos. No caso de perda de privacidade, existem dois resultados muito ruins. A primeira é a perda do anonimato, que já foi abordada num capítulo de livro anterior, enquanto a segunda é o roubo de identidade, que é consideravelmente alarmante, especialmente se acontecer em grande número. Dispositivos médicos maliciosos de IoT podem causar degradação da saúde ou até mesmo a morte, mas pior ainda são os dispositivos implantados em humanos (ou seja, marca-passos). O ransomware nesses dispositivos é basicamente um sequestro remoto que não deixa a vítima com nenhuma opção de negociação ou alternativa ao pagamento do resgate. A perda de água corrente e de energia é má, mas se uma área suficientemente grande for afectada, isso mergulharia os habitantes numa era das trevas, que nos tempos modernos seria catastrófica. Um ataque ao abastecimento de água pode não só parar a água corrente, mas também pode torná-la venenosa, alterando o tratamento da água na estação de tratamento de água. Qualquer ataque generalizado e bem sucedido a infra-estruturas críticas teria consequências devastadoras para a segurança geral (por exemplo, militar), para a segurança económica nacional, para a saúde ou segurança pública nacional. Ataques maliciosos a fábricas também podem causar a quebra das máquinas de produção, paralisando a produção por um longo período de tempo ou até mesmo causando ferimentos ou mortes entre os funcionários. A utilização de botnets suficientemente grandes para realizar ataques DDoS ou outros tipos de ataques poderia paralisar grandes secções da Internet e, com isso, tudo o que depende dessa infra-

14.5 Lacunas de Pesquisa

A segurança da IoT é um problema e irá piorar à medida que a superfície de ataque potencial se expandir com muito mais dispositivos e com dispositivos mais críticos (por exemplo, dispositivos médicos).

14.5.1 Inteligência Artificial e Aprendizado de Máquina

A inteligência artificial (IA) e o aprendizado de máquina (ML) prometem ser uma grande ajuda na segurança e identificação de ataques na IoT [10, 114, 203]. A introdução de IA e ML no ambiente IoT tem algumas dificuldades associadas, como a implantação em dispositivos restritos e distribuídos e a necessidade de atualização de modelos de IA/ML ao longo do tempo, o que pode ser problemático por razões de acessibilidade e práticas gerais de atualização - como discutiremos mais adiante nesta seção. Superando esses problemas, a IA e o ML podem fornecer muito em termos de segurança para sistemas IoT. A IA e o ML podem lidar com dados heterogéneos e analisar grandes volumes de dados produzidos pela IoT muito mais rapidamente (ou seja, em tempo real) do que os métodos tradicionais, permitindo-lhes descobrir ataques à medida que ocorrem. Essas soluções podem ser utilizadas para controle de acesso, segurança, detecção e análise de malware, avaliação de riscos, análise de ameaças, privacidade, detecção de ataques e, potencialmente, rastreamento do ataque através do sistema. AI/ML também é uma boa base para fornecer resiliência adicional do sistema. A aprendizagem profunda já mostrou resultados promissores na identificação de ataques de falsificação de IP e DDoS, e a aprendizagem automática descentralizada pode ser especialmente compatível com a IoT. Precisamos de soluções que sejam capazes de identificar as sutilezas das violações de segurança e mitigá-las, ao mesmo tempo que se adaptam aos recursos limitados dos dispositivos IoT. Isto inclui rotulagem eficiente de fluxos de entrada e aprendizagem com conjuntos menores de dados de treinamento. Precisamos de métodos para que tais soluções funcionem não apenas em empre

14.5.2 Padrões de segurança fortes e universais para tecnologia de IoT Os

padrões de segurança em IoT e sua aplicação, em geral, precisam de algum trabalho [13]. O rápido desenvolvimento de soluções e a heterogeneidade dos dispositivos certamente não facilitam a padronização da segurança da IoT. Padrões ou diretrizes universais devem ser definidos para dispositivos IoT, incluindo proteção de dados em repouso e durante a comunicação, autenticação e autorização de dispositivos IoT, manutenção e gerenciamento de dispositivos IoT, auditoria e registro e interfaces seguras (web, API de aplicativos, nuvem e dispositivos móveis) e processos de resposta a incidentes de segurança de IoT. Em geral, um maior desenvolvimento da IoT deve seguir o paradigma de “segurança e privacidade desde a conceção”, especialmente para dispositivos que recolhem dados pessoais e/ou podem ter um impacto significativo na saúde ou nos ativos dos seus pro

14.5.3 Desenvolver criptografia forte e leve para IoT

Alguns dispositivos IoT têm recursos severamente limitados e, para manter total funcionalidade, segurança e usabilidade, exigem protocolos leves (criptográficos). Soluções leves devem ser eficientes em termos computacionais, de memória e

consumo de energia. Para isso, precisamos de soluções IoT leves (padronizadas) para criptografia de dados (em repouso e em trânsito), gerenciamento de chaves, roteamento, autenticação e controle de acesso. Além disso, o malware também é um grande problema para os sistemas IoT e, pelas mesmas razões de recursos limitados, as soluções de detecção de malware que podem ser eficazes em tais ambientes têm de ser mais desenvolvidas.

14.5.4 Estabelecer Confiança e Rastreabilidade

Tendo em conta as preocupações de segurança em torno da IoT, é importante estabelecer confiança nos dispositivos, nos seus processos e nos dados recolhidos e transmitidos. Os atuais sistemas IoT carecem de transparência, tornando impossível para os utilizadores comuns saberem o que se passa, que dados estão a ser recolhidos e o que lhes acontece. Isso inclui monitoramento ao vivo que pode notificar os usuários em tempo real sobre qualquer comportamento malicioso em sistemas IoT. O monitoramento também é muito importante para sistemas IoT de segurança cibernética auto-recuperáveis que têm o potencial de automatizar a segurança cibernética.

A rastreabilidade e integridade dos dados são vitais para aumentar a confiança nos dados e, consequentemente, em todo o sistema IoT. Os livros-razão distribuídos tornaram-se a principal solução para rastreabilidade de dados; no entanto, ainda é necessário algum desenvolvimento, especialmente em escalabilidade, antes que possam ser aplicados livremente a redes IoT maiores. Ao mesmo tempo, a confiança também é necessária entre os dispositivos IoT numa rede. Isso evita que invasores ingressem na rede ou se façam passar por um dos dispositivos da rede. Para isso, precisamos de sistemas de gestão de confiança mais seguros e melhores.

14.5.5 Conscientização e educação sobre segurança de IoT

Atualmente, os usuários da IoT não estão bem conscientes dos riscos de segurança e especialmente dos controles de mitigação disponíveis para reduzir esses riscos [115]. Isto é especialmente verdade em ambientes pessoais/domésticos e pequenas empresas, mas infelizmente também é frequentemente verdade em ambientes empresariais. O problema mais comum, e que tem sido explorado com muito sucesso mesmo no passado recente, é o uso de senhas padrão que acompanham os dispositivos ou o uso de senhas fracas. São necessários mais esforços para desenvolver métodos e ferramentas de conscientização eficazes para informar o público sobre os perigos da IoT insegura (sejam dispositivos inseguros ou configurações fracas). Os produtos IoT devem vir com instruções mais claras para os usuários sobre como configurar seus dispositivos, com ênfase na importância das configurações de segurança e privacidade (isso pode fazer parte do manual e/ou como políticas fixas, por exemplo, senhas padrão teriam a ser alterada durante a configuração para uma senha de alguma qualidade mínima). Alegadamente, há também uma grande escassez de profissionais para implementar

Redes IoT em empresas, incluindo talentos em segurança cibernética [118]. Devem ser concebidos e implementados programas adequados de formação e melhoria de competências.

14.5.6 Segurança de hardware

Com os dispositivos IoT, é importante lembrar que eles cobrem uma ampla gama de casos de uso e, em alguns deles (por exemplo, quando os dispositivos são instalados fora de ambientes protegidos), a segurança física ou de hardware do próprio dispositivo é tão importante quanto qualquer outra coisa. [18]. Este aspecto muitas vezes parece ser esquecido e os dispositivos IoT carecem de segurança de hardware, como coprocessadores criptográficos ou tecnologias anti-adulteração. Portanto, precisamos de mais módulos de baixo custo, eficientes e bem testados, que incluam segurança de hardware que os fabricantes possam usar de forma confiável em seus produtos IoT, e devemos fornecer incentivos para que eles sejam usados. Nesta seção, gateways confiáveis também podem ser mencionados como forma de minimizar a superfície de ataque e os dan

14.5.7 Privacidade na IoT

A privacidade é um desafio importante na IoT [107]. A preservação da privacidade restringe o tratamento de dados apenas ao estritamente necessário e de uma forma que evita que dados sensíveis adicionais sejam inferidos ao longo do ciclo de vida dos dados. Deve também encontrar um equilíbrio entre a utilidade dos dados e a privacidade. Precisamos de mais ênfase na privacidade durante a concepção e desenvolvimento da IoT e de melhores técnicas de preservação da privacidade (por exemplo, anonimização) que possam ser amplamente adoptadas na IoT.

14.5.8 Gestão do ciclo de vida

Um dispositivo pode ser seguro hoje, mas esta condição pode mudar durante o seu ciclo de vida devido a uma vulnerabilidade recentemente descoberta. A gestão da segurança deve ser escalável e tão automática quanto possível se quisermos lidar com um grande número de dispositivos IoT heterogêneos [109]. No entanto, isso nem sempre é possível. Como os dispositivos IoT geralmente não são equipados com interfaces tradicionais e as atualizações não são enviadas aos dispositivos, os usuários não sabem que há novas atualizações ou patches que devem instalar. Precisamos de métodos para notificar os proprietários de dispositivos quando há atualizações ou patches cruciais que precisam ser instalados sem que percam qualquer funcionalidade dos sistemas que configuraram (se a atualização significar perda de dados ou configuração do dispositivo, muitos optarão por não atualizar). Finalmente, um desafio adicional que necessita de mais investigação é o desenvolvimento de procedimentos de atualização eficientes para dispositivos IoT com recursos muito limitados (por exemplo, memória insuficiente para descarregar u

14.5.9 Regulamentação e políticas de IoT No

final das contas, mesmo que exista tecnologia que possa tornar a IoT segura, ainda é importante que a tecnologia seja implementada. Como é frequentemente o caso, a regulamentação leva algum tempo para acompanhar os avanços tecnológicos e, embora tenhamos visto recentemente algum movimento na regulamentação das soluções IoT e dos níveis de segurança esperados que devem fornecer, deveria haver mais. Precisamos de alguma forma de impor padrões mínimos de segurança para dispositivos IoT (por exemplo, certificação).

Uma questão crucial que poderia ser atenuada com a regulamentação é o suporte a longo prazo dos dispositivos IoT. Hoje você pode comprar um aparelho, e o fabricante encerrará seu suporte (se houver) a qualquer momento no futuro, sem sequer avisar os proprietários do aparelho. Dadas as atuais políticas de desenvolvimento sustentável, o suporte mínimo de segurança crítica poderia ser prescrito por regulamento, ou poderia haver uma exigência de que os produtos tivessem uma duração de suporte claramente marcada em suas embalagens no momento da venda, que o fabricante garantirá.

14.6 Exemplos de problemas

Exemplos de problemas tangíveis podem incluir:

Cibersegurança baseada em aprendizado de máquina para IoT. Estude padrões de ataque de IoT e desenvolva métodos de rotulagem de dados brutos compatíveis com IoT para novas soluções de aprendizado de máquina para reconhecer ataques. Crie conjuntos de dados de anomalias. Desenvolva novas soluções de aprendizagem profunda para detectar ataques e/ou malware em redes IoT.

Classificações de segurança de dispositivos IoT. Para aliviar o problema da heterogeneidade dos dispositivos IoT, desenvolva um esquema de classificação para dispositivos IoT com base em suas limitações de recursos e finalidade (ou seja, quão crucial é a segurança para o dispositivo, com base no que ele deve fazer e nos tipos de dados envolvidos). A classificação poderia ser usada para determinar quais são os recursos mínimos de segurança (por exemplo, protocolos de segurança) que o dispositivo deve suportar para ser considerado como tendo um nível de segurança aceitável, dada a sua classe de segurança.

Honeypots inteligentes para IoT. Estabeleça a emulação de dispositivos IoT em plataformas informáticas universais. Habilite o monitoramento e a coleta de dados da rede IoT honeypot distribuída.

Protocolos leves para IoT. Encontre ou adapte protocolos existentes adequados ou desenvolva novos protocolos de criptografia para IoT (potencialmente para cada classificação de segurança de dispositivo IoT do exemplo anterior). A seleção

de protocolos (para encriptação de dados, tanto para dados em repouso como em trânsito, gestão de chaves, encaminhamento, autenticação mútua de dispositivos na rede, etc.) podem ser promovidos como boas práticas e/ou normalizados.

Notificações de atualização e patch para usuários comuns. Compilar um banco de dados de dispositivos e hardware IoT usados e quaisquer atualizações ou patches consequentes lançados para seu software ou firmware. Dê aos usuários opções para encontrar seus dispositivos no banco de dados e assinar para serem notificados se atualizações ou patches estiverem disponíveis para seus dispositivos. Forneça instruções sobre onde obtê-los e como instalá

Autenticação aprimorada. Os dispositivos IoT sofrem com o uso excessivo de senhas padrão e fracas. Devem ser envidados esforços no desenvolvimento de formas convenientes de incorporar a autenticação multifatorial em dispositivos IoT e no desenvolvimento e implementação de autenticação sem senha para d

15 Modelagem Eficaz de Ameaças

15.1 Introdução

Há uma tendência crescente na segurança de mudar para a esquerda, ou seja, aplicar atividades de segurança mais cedo no ciclo de vida de desenvolvimento de software. A modelagem de ameaças começa a partir de uma descrição em nível de arquitetura (ou em nível de design) do sistema de software ou serviço que está sendo desenvolvido, e se esforça para melhorias iniciais em termos de segurança e privacidade (1) identificando ameaças, (2) priorizando essas ameaças em termos de risco e possíveis danos, e (3) sugerir/oferecer possíveis mitigações no nível arquitetônico. Tal abordagem é benéfica, pois permite a identificação precoce de falhas de segurança para reduzir o impacto de mudanças [232]. A relevância e utilidade de técnicas como segurança e a modelagem de ameaças à privacidade é demonstrada pelo crescente interesse em ameaças modelagem. Na verdade, organizações como a Microsoft fizeram grandes progressos na abordagem da segurança nas fases iniciais do ciclo de vida do desenvolvimento como parte do seu esforço de segurança no início dos anos 2000 [112, 130, 227], com a introdução da modelagem de ameaças à segurança e do ciclo de vida de desenvolvimento da segurança. A relevância e importância de considerar a segurança nestas fases continua a ser reconhecido e confirmado com o lançamento de 2021 do top 10 do Owasp [180] **que inclui explicitamente o design inseguro como uma das 10 principais entradas e especifica o necessidade de realizar mais modelagem de ameaças [212]. Além disso, tem sido aplicado a muitos sistemas na prática. Para vários deles, modelos concretos de ameaças estão disponíveis, como o sistema de envio de denúncias SecureDrop [86] e Kubernetes [233]. Uma análise tão sistemática e abrangente pode ser uma ferramenta indispensável para identificar fluxos de dados problemáticos em aplicações que são posteriormente aproveitados como parte de ataques de ransomware para se propagarem ainda mais.**

15.2 Quem será afetado?

Claramente, a atividade de modelagem de ameaças envolve arquitetos de software e especialistas em segurança. Introduz uma actividade adicional e possivelmente dispendiosa para o processo de desenvolvimento, mas o rendimento pode ser um nível de garantia relativamente alto: muitas falhas clássicas de segurança e privacidade podem ser evitadas "por design". Se este

Figura 15.1: Desafios em cada fase de modelagem de ameaças

não fossem cobertas, as mesmas falhas poderiam ser ocultadas e só serem descobertas mais tarde, ao nível da implementação. Isto implicaria investimentos e esforços muito maiores para lidar com estes problemas específicos de segurança. Na verdade, o fornecedor de serviços ou software (empresa) continua necessitando de um processo de modelagem de ameaças com boa relação custo-benefício. Os usuários e organizações de usuários do produto ou serviço correspondente podem não estar cientes deste assunto, mas ainda assim teriam que pagar a conta no final da jornada de

Embora as técnicas de modelagem de ameaças já tenham demonstrado grande potencial no apoio ao projeto e desenvolvimento de sistemas de software seguros, a aplicação mais ampla dessas técnicas como parte dos processos de desenvolvimento de software introduz uma série de desafios (mostrados na figura 15.1). para os profissionais no que diz respeito ao custo de aplicação dessas técnicas em processos de desenvolvimento contemporâneos [214]. Primeiro, a aplicação destas técnicas é tipicamente uma atividade que inclui o envolvimento de especialistas em segurança, um recurso escasso em muitas empresas, o que dificulta a aplicação mais ampla e frequente destas técnicas [253]. Em segundo lugar, a aplicação destas técnicas implica algum esforço manual na criação e manutenção de uma representação do sistema e na análise de tal representação para identificar ameaças à segurança. Qualquer esforço manual como parte de uma atividade que é, idealmente, frequentemente repetida à medida que um sistema de software é desenvolvido e ampliado, introduz uma sobrecarga não trivial que impede a sua aplicação frequente. Além disso, o custo de manter e reanalisar esta representação é exacerbado no contexto das práticas de desenvolvimento contemporâneas que são caracterizadas por iterações frequentes e desenvolvimento acelerado.

15.3 O que se espera que aconteça?

A desvantagem de não realizar modelagem de ameaças foi sugerida acima. No entanto, o custo actual da modelização de ameaças é elevado e os desafios de investigação apresentados neste capítulo são da maior importância para aumentar a relação custo-eficácia das práticas actuais e futuras de modelização de ameaças.

Conforme mencionado acima, a aplicação de modelagem de ameaças à segurança e à privacidade geralmente envolve uma entrada manual ou avaliações por modeladores de ameaças, como a criação de um modelo de representação do sistema em consideração, a elicitação das ameaças à segurança e à privacidade, a priorização de essas ameaças para determinar as mais importantes e, finalmente, sugerir mitigações apropriadas para enfrentar as ameaças identificadas. Encontro de praticantes vários desafios ao aplicar essas atividades de modelagem de ameaças: (i) uma análise abrangente de um sistema de software envolve uma quantidade significativa de trabalho, tanto na construção do modelo do sistema como na elicitação real da ameaça; (ii) as análises podem frequentemente levar a longas listas de ameaças, mas estes resultados carece de informações sobre a relevância dessas ameaças, dificultando a identificação das mais críticas; (iii) é essencial garantir que o modelo utilizado pois a análise permanece consistente com a implementação real do sistema em desenvolvimento. Cada um desses desafios será explicado com mais detalhes detalhe abaixo.

15.3.1 Trabalho manual

Um dos maiores desafios para a relação custo-benefício da segurança e da privacidade modelagem de ameaças é a dependência do esforço manual tanto na criação do modelos e a análise para detectar ameaças à segurança e à privacidade. Desde o a modelagem de ameaças depende do uso de uma representação de design do sistema (normalmente um diagrama de fluxo de dados [59,112]) para analisar ameaças à segurança e à privacidad tal representação deve ser recuperada ou construída antes que a análise da ameaça possa começar. No entanto, frequentemente essa documentação de projeto não está disponível para os sistemas que foram construídos ou estão sendo ampliados. Por causa disso, o desenho do sistema em análise terá que ser reconstruído com base na documentação (na medida em que esteja disponível) e passando pelos implementação da aplicação. Este esforço de reconstrução já impõe custo adicional ao realizar um exercício de modelagem de ameaças, e esse esforço pode ter que ser repetido frequentemente se a documentação do modelo não for mantida atualizado com o aplicativo à medida que ele é desenvolvido. Uma segunda fonte do esforço manual pode ser a própria análise. A quantidade de esforço introduzida nesta etapa depende de até que ponto os profissionais podem confiar na ferramenta suporte para a análise ou, em vez disso, execute a análise manualmente. O mais informais forem as descrições do sistema, mais a análise terá que se basear em uma avaliação manual por um modelador de ameaças, pois as ferramentas automatizadas exigem um entrada de modelo mais rica, incluindo mais informações, para permitir que a ferramenta faça as decisões de elicitação de ameaças automaticamente.

15.3.2 Priorização

O segundo desafio está relacionado com a utilização dos resultados da análise de ameaças nas fases subsequentes para apoiar decisões sobre a aplicação de contramedidas de segurança e privacidade na aplicação em desenvolvimento. Como os recursos disponíveis para enfrentar as ameaças à segurança e à privacidade são limitados, os profissionais precisam ser capazes de determinar quais ameaças são mais relevantes e importantes para enfrentar. No entanto, a elicitação de ameaças à segurança e à privacidade apenas apresenta uma (grande) lista de ameaças aplicáveis. Não fornece qualquer apoio na identificação das ameaças mais relevantes entre aquelas que devem ser abordadas primeiro. Essas ameaças provocadas geralmente carecem das informações necessárias para priorizar as ameaças resultantes. Como consequência, a priorização das ameaças envolve uma atividade manual em que cada ameaça deve ser avaliada manualmente para determinar a sua relevância. Embora tal abordagem possa ser apropriada para uma análise única, ela é ineficaz se a elicitação da ameaça for repetida com frequência e a lista resultante de ameaças também mudar. Além disso, o apoio ao rastreamento da prioridade ou importância dos tipos de ameaças é frequentemente limitado a uma classificação muito grosseira (por exemplo, baixa, média ou alta) que não inclui qualquer tipo de informação de rastreabilidade quando tal decisão de classificação tiver que ser tomada. reavaliado posteriormente. Devido à falta de informação, não é possível avaliar porque é que essa prioridade específica foi atribuída a essa ameaça na altura. Se certos pressupostos subjacentes a essa decisão se revelarem inválidos, não será possível identificar todas as ameaças relevantes que exigiriam

uma reavaliação.

15.3.3 Garantindo resultados atualizados

Um último desafio para os profissionais é garantir que os resultados da análise de ameaças permaneçam atualizados e relevantes para a aplicação em desenvolvimento. Especialmente com práticas de desenvolvimento contemporâneas que envolvem desenvolvimento em ritmo acelerado e iterações frequentes, o design do aplicativo pode mudar com frequência. O resultado é que os resultados da análise de ameaças de versões anteriores do design não são mais relevantes, pois algumas ameaças podem não ser mais aplicáveis (por exemplo, devido à remoção de certos elementos do design). Isto introduz um desafio em manter as representações de design do sistema atualizadas com a implementação à medida que evolui durante o desenvolvimento, levando a custos adicionais de manutenção para garantir que os resultados da ameaça sejam atuais.

15.4 Qual é a pior coisa que pode acontecer?

A seção anterior descreveu os diferentes desafios e problemas enfrentados pelos profissionais na aplicação da modelagem de ameaças, especialmente em termos de sobrecarga e custo-benefício dessas abordagens. embora um grande número de cenários possa ser construído para ilustrar o impacto de vários

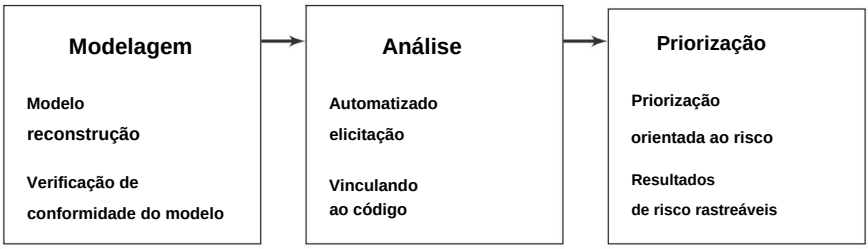


Figura 15.2: Oportunidades e melhorias em cada fase de modelagem de ameaças

falhas de segurança perdidas no desenvolvimento de um produto de software concreto. O pior caso é, na verdade, desconhecido, uma vez que o impacto real da não realização de qualquer uma destas análises de segurança não pode ser previsto devido às incertezas nas aplicações, nas organizações, nos contextos em que as aplicações são utilizadas, nos tipos de dados processados, etc. Assim, o foco principal está no papel da automação na redução de despesas gerais e de esforço como forma de permitir o uso e aplicação mais amplos dessas técnicas. O aprimoramento bem-sucedido da modelagem de ameaças, em grande parte por meio da automação, será necessário para impulsionar a adoção, o que, por sua vez, permitirá evitar os dispendiosos cenários de pior caso na reengenharia e correção de sistemas e serviços de software complexos. É difícil estimar os piores cenários em termos de

15.5 Lacunas de pesquisa A

agenda de pesquisa essencial para conduzir este subdomínio do ciclo de vida de desenvolvimento de software seguro é relativamente simples. Inclui principalmente atividades relacionadas ao conhecimento reutilizável, automação e suporte de ferramentas, etc. Os temas e atividades essenciais de pesquisa estão resumidos abaixo.

15.5.1 Automação

Um elemento-chave na estratégia para enfrentar esses desafios é fortalecer a automação e aplicá-la em muitas atividades de modelagem de ameaças para reduzir as etapas manuais e permitir reavaliações frequentes como parte de práticas de desenvolvimento iterativas. Na verdade, a automação pode desempenhar um papel crucial na redução do custo da modelagem de ameaças, automatizando muitas etapas que envolvem entradas manuais e dispendiosas de desenvolvedores e especialistas. Descrevemos brevemente cada uma das fases (mostradas na figura 15.2) dos processos de modelagem de ameaças nas quais a automação pode melhorar significativamente a relação custo-benefício, reduzindo ou eliminando o trabalho manual.

Modelagem Uma das primeiras etapas onde a automação pode ser aplicada é na construção da representação do modelo que serve de entrada para a ameaça

atividade de modelagem. Esta também é uma das áreas mais desafiadoras para aplicar a automação. Existem duas abordagens principais que podem ser adotadas e que proporcionam diferentes graus de redução do esforço manual. Primeiro, após a construção de uma representação inicial do modelo do sistema, a verificação de conformidade do modelo [186] ou a análise de desvio arquitetural [231] podem ser usadas para verificar se a representação do modelo realmente corresponde à implementação do código-fonte do sistema. Tal abordagem ainda requer um modelo inicial, mas pode reduzir o custo de manter o modelo atualizado à medida que o sistema continua a ser desenvolvido. Em segundo lugar, uma abordagem mais complexa e totalmente automatizada é basear-se na construção de modelos. Esta abordagem emprega ferramentas para criar automaticamente um modelo a partir da origem da aplicação, eliminando assim o esforço inicial na construção do modelo. É claro que estas técnicas podem ser combinadas com a verificação de conformidade para verificar a precisão dos modelos reconstruídos.

Elicitação de ameaças A segunda etapa em que a automação pode ser aproveitada é durante a elicitação de ameaças. Existem duas áreas em que a automação reduz o esforço e a entrada manual: a própria elicitação e a aplicação automatizada do conhecimento especializado. Para a elicitação da ameaça em si, o uso da automação pode garantir uma análise abrangente, sistemática e repetível do sistema.
Muitas ferramentas de modelagem de ameaças existentes [120, 156] já fornecem essa funcionalidade, variando de critérios simples a padrões de modelo mais complexos [235]. Ferramentas automatizadas podem aplicar consistentemente conjuntos de regras complexos a projetos de sistemas para garantir a elicitação repetível de ameaças. O segundo benefício da automação no contexto da elicitação de ameaças é que ela permite que o conhecimento especializado sobre ameaças à segurança e à privacidade seja codificado no suporte da ferramenta, permitindo a aplicação automatizada desse conhecimento sem ter que depender de especialistas em segurança e privacidade para auxiliar nas avaliações. , pois são recursos escassos para as organizações.

Priorização A terceira etapa em que a automação introduz benefícios é a priorização das ameaças à segurança e à privacidade suscitadas. Dado o número substancial de ameaças à segurança e à privacidade que podem ser suscitadas, ser capaz de priorizá-las torna-se essencial. O grande número de ameaças torna cada vez mais difícil analisá-las para definição de prioridades, especialmente se a análise for repetida frequentemente em resposta a alterações na concepção do sistema. A automação oferece dois benefícios principais neste contexto. Primeiro, como a automação dependerá de informações adicionais nos modelos de entrada para determinar as prioridades da ameaça, ela na verdade força a especificação explícita dessas informações nos modelos de entrada. Embora isto introduza alguma sobrecarga para fornecer dados adicionais, também permite a rastreabilidade dos resultados, uma vez que as prioridades resultantes podem ser explicadas através dos dados e revisitadas posteriormente. Em segundo lugar, elimina a necessidade de avaliação manual e priorização das ameaças, tornando muito

mais econômico reanalisar frequentemente um sistema. Essa automação requer a construção de modelos de risco [87, 215] que possam ser aplicados sistematicamente.

15.5.2 Suporte de

ferramentas Conforme ilustrado acima, há muitas oportunidades de automação para reduzir o esforço manual e permitir uma análise de ameaças de um sistema com melhor custo-benefício. O suporte de ferramentas é crucial para alcançar a automação nessas diferentes fases da modelagem de ameaças. O suporte de ferramentas necessário abrange: (1) ferramentas de análise de código-fonte para realizar verificação de conformidade ou reconstrução de modelo; (2) elicitação automatizada de ameaças, aproveitando conhecimento especializado codificado; e (3) priorização automatizada de ameaças prov

15.5.3 Educação e treinamento Uma

área final de melhoria é fornecer educação e treinamento para permitir que todo o pessoal participe na modelagem de ameaças e reduzir ainda mais a dependência de especialistas em segurança e privacidade para atividades de modelagem de ameaças. Juntamente com o suporte de ferramentas, a educação e o treinamento facilitam a incorporação da modelagem de ameaças nos processos de desenvolvimento de software existentes.

15.6 Exemplos de problemas

Exemplos de problemas tangíveis podem incluir:

Criação e manutenção de modelos. Qualquer atividade de modelagem de ameaças depende da criação de um modelo inicial do sistema a ser analisado. A criação e manutenção desses modelos podem introduzir custos significativos para os modeladores de ameaças, dificultando a aplicação frequente dessas técnicas durante o desenvolvimento. Houve vários avanços [186] que tornam mais fácil determinar se esses modelos ainda estão em conformidade com o código, reduzindo assim o esforço envolvido na manutenção. A análise do código-fonte para construir modelos que sejam prontamente utilizáveis na análise de modelagem de ameaças ainda é um problema desafiador.

Automatizando o conhecimento sobre ameaças. Existem muitos recursos disponíveis publicamente com informações sobre bugs, pontos fracos e falhas de segurança previamente identificados (por exemplo, cves, cwes, etc.). Esses recursos são altamente dinâmicos, pois são atualizados frequentemente quando novos problemas são identificados. Embora alguns desses recursos já tenham sido integrados com sucesso em atividades de análise automatizadas, como a detecção de dependências vulneráveis, nem todos os recursos são facilmente traduzidos e aplicados em um contexto de modelagem de ameaças.

Integração em processos de desenvolvimento. A aplicação da modelagem de ameaças geralmente é uma atividade que acontece de forma isolada. Isto introduz alguns

sobrecarga e complexidade adicionais na tradução das ameaças identificadas no design do sistema em itens muito concretos e acionáveis para desenvolvedores para trabalhar. Existem vários desafios para melhorar a capacidade de ação dos resultados das análises de ameaças, apoiando uma abordagem mais rígida integração nos processos de desenvolvimento e relacionar os resultados da modelagem de ameaças a artefatos concretos do código-fonte, por exemplo, orientando pa pontos de partida para mitigar as ameaças identificadas.

16 Grandes Desafios

Nesta secção descrevemos alguns “grandes desafios” que teremos de enfrentar nos próximos anos. Esses desafios exigem a colaboração de centenas de pessoas de diversas áreas da ciência. A maioria destes desafios não envolve apenas investigação inovadora, mas também necessita de regulamentação adequada e, possivelmente, de quadros jurídicos em vigor. Esperamos que as agências financiadoras forneçam apoio a estas áreas e que a comunidade de investigação comece a trabalhar para enfrentar estes desafios.

16.1 Dê aos usuários garantia sobre a segurança de seus dispositivos

A maioria dos dispositivos de computação hoje oferece pouca ou nenhuma garantia sobre o nível de segurança que fornecem. Embora alguns deles (como dispositivos médicos) possam aderir a padrões de segurança, a maioria deles não adere a nenhum padrão de segurança. Como resultado, eles não oferecem garantias aos seus usuários: podem travar a qualquer momento; eles podem ficar comprometidos a qualquer momento; eles podem se tornar hostis a qualquer momento. Acreditamos que devemos proporcionar aos utilizadores (i) melhor transparência e (ii) melhores garantias sobre a segurança dos seus dispositivos. Embora isto pareça uma tarefa que pode ser alcançada através de regulamentação, tem dimensões significativas de investigação e desenvolvimento, incluindo monitorização contínua, testes de penetração agr

16.2 Se isso pode ser feito anonimamente no mundo offline, também pode ser feito anonimamente online

Nos últimos anos, transferimos várias das nossas atividades diárias para o ciberespaço. A pandemia da COVID-19 intensificou esta tendência, de modo que, no auge da pandemia, as únicas formas de interagir com outras pessoas envolviam, em algum nível, o mundo digital. Como resultado, começamos a fazer todas as no

nossas visitas passaram para teleconferências, nossa escolaridade foi feita via Zoom, vários aspectos do trabalho também passaram para online, etc. O que não percebemos facilmente, porém, foi que para realizar essas atividades online tínhamos que fornecer um ótimo grande quantidade de informações pessoais e, dessa forma, sacrificar nossa privacidade. Por exemplo, no passado era possível fazer a maior parte das nossas compras praticamente anonimamente. Poderíamos visitar lojas anonimamente, procurar vários produtos anonimamente, poderíamos até pagar anonimamente usando dinheiro. Em nenhum momento deste processo tivemos que revelar o nosso nome, a nossa morada, o nosso número de telefone, etc. Poderíamos revelar esta informação (se quiséssemos), mas não foi necessário. Hoje é quase impossível fazer compras online sem revelar uma grande quantidade de informações pessoais, como o nosso nome, o nosso número de telefone, a nossa morada, etc. Essas informações pessoais são reveladas a uma vasta gama de diferentes intervenientes, incluindo o comerciante, anunciantes on-line, empresas de courier, etc. Acreditamos que agora é hora de reivindicar nossa privacidade e revelar o mínimo de informações possível. O princípio orientador aqui é que, se isso pode ser feito anonimamente offline, também pode ser feito anonimamente online. Esta não é uma tarefa fácil e pode envolver vários aspectos além da investigação, incluindo, por exemplo, a sensibilização e a implantação. Pode nem ser possível em alguns casos e com alguns fornecedores. No entanto, ter isto como princípio orientador ajudar-nos-á a reduzir todos os casos em que a privacidade foi sacrificada desnecessariamente.

16.3 Torne a IA segura para as pessoas

A IA está se espalhando ampla e rapidamente. Por exemplo, um white paper recente da Deloitte mostrou que o mundo verá um crescimento do PIB impulsionado pela IA de US$ 15,7 trilhões até 2030. A capacidade da IA, e dos modelos de ML em particular, de extrair/aprender recursos complexos de grandes volumes de (frequentemente) dados não estruturados são o que os torna uma escolha popular para resolver vários problemas. No entanto, conforme discutido no Capítulo 4, os aplicativos baseados em ML oferecem todo um novo espectro de explorações de segurança e privacidade para possíveis adversários.

Primeiro, os modelos de ML são frequentemente aplicados a setores onde a tomada de decisão errada pode ter sérias implicações. No entanto, muitas vezes pode não ser possível oferecer garantias formais de segurança, dada a natureza não determinística desses modelos. Em segundo lugar, os modelos de ML são frequentemente treinados em dados pessoais/sensíveis, especialmente modelos implantados na área de saúde. Por isso,

revelar ocorrências de formação constitui uma grave violação da privacidade dos indivíduos.

Como resultado, precisamos de desenvolver técnicas e mecanismos para tornar a IA segura para as pessoas. Note-se que fazê-lo não é uma tarefa fácil e envolve reunir investigadores e profissionais de uma vasta gama de áreas, tais como matemática, linguística, informática, etc. garantias desejadas sem sacrificar o desempenho do modelo. No entanto, trabalhar nesta direção certamente levará a melhorias significativas e a novas técnicas que oferecem soluções de compromisso aceitáveis.

16.4 Tornar os sistemas resilientes sob ataque

Os sistemas informáticos podem ser notavelmente frágeis. Na verdade, uma instrução if **errada ,** uma instrução de atribuição **errada** ou uma variável global **indefinida é tudo o que é necessário para travar uma aplicação ou mesmo comprometer um computador. Para piorar a situação, se um programa com a** instrução if errada **for executado em milhões de computadores, todos esses computadores poderão ser comprometidos em questão de horas ou até minutos! O grande desafio aqui é desenvolver sistemas informáticos capazes de tolerar ataques cibernéticos. Gostaríamos de ter sistemas que falhassem perfeitamente quando fossem atacados por ciberataques. Não podemos evitar ter milhões (ou mesmo bilhões) de cópias de um programa em execução em vários dispositivos. Na verdade, existem milhares de milhões de pessoas e dezenas de milhares de milhões de dispositivos que executam um pequeno número de aplicações ultrapopulares. O desafio neste ambiente é tornar estes programas ultrapopulares (e todos os computadores em geral) resilientes a ataques cibernéticos. Existem vários caminhos diferentes que podem ser explorados para alcançar essa resiliência. Embora os caminhos possam ser diferentes, a maioria deles concorda que um aplicativo deve falhar normalmente sob ataque. Esta falha normal pode significar que apenas uma pequena fração dos computadores será comprometida, ou que apenas uma pequena parte da funcionalidade será comprometida, ou algo mais. O ponto unificador, contudo, é tornar os sistemas mais resilientes aos ataques cibernéticos; uma** declaração if errada **não deveria ser capaz de comprometer milhões de computadores. Deveríamos fazer muito melhor do que isso.**

16.5 Aumentar a sensibilização do público em geral para a segurança cibernética As pessoas são muitas vezes vistas como o elo mais fraco na cadeia da segurança cibernética.
São um importante factor que contribui para a maioria das violações da segurança cibernética, uma vez que os cibercriminosos empregam frequentemente técnicas que exploram as capacidades humanas ina

pontos fracos para realizar ataques. A melhoria do desenvolvimento de competências em segurança cibernética através de iniciativas de formação e sensibilização centra-se em permitir que as pessoas estabeleçam barreiras técnicas e operacionais às ameaças à segurança ciber operarem como tal, através do processamento vigilante de ações acionáveis inteligência. Aumentar o impacto potencial de tais iniciativas requer a personalização e a adaptação da experiência de sensibilização ou formação. Isso deve levar em conta, entre outras coisas, funções pessoais, bases de conhecimento, competências e experiências. Deverá também incluir o desempenho operacional contexto das organizações envolvidas, incluindo políticas, processos e quadros regulamentares aplicáveis.

O primeiro grande desafio aqui tem a ver com a criação de um mapeamento do parâmetros de referência de competências que devem ser alcançados, dependendo dos contextos organizacionais distintos e das funções pessoais correspondentes. Isto também reflete na esfera pessoal quando se refere ao endurecimento e à consciência social.
O segundo grande desafio tem a ver com a implementação de programas de desenvolvimento de competências, o que significa estruturar a mensagem apropriada para atingir os objetivos de aprendizagem almejados, selecionando um meio de comunicação adequado e determinando os intervalos de tempo e outros parâmetros que são depende dos participantes e pode afetar significativamente a participação e retenção. Enfrentar estes desafios requer uma abordagem multidisciplinar, envolvendo expertise não apenas em ciências pedagógicas e segurança cibernética, mas também psicologia, experiência em domínio (ou seja, específico do setor) e outras áreas. Além disso, as ciências sociais e a análise de dados podem contribuir para que pode melhorar e facilitar o mapeamento acima mencionado, ao mesmo tempo que contribui para uma entrega personalizada.

Bibliografia

[1] 8 questões de segurança de zoom que você precisa conhecer. https://www.sigmundsoftware.com/blog/zoom-questões-de-segurança-coronavirus/. Acesso: 2022-11-119.

[2] Estatísticas da economia digital e da sociedade - famílias e indivíduos. https://ec.europa.eu/eurostat/statistics-explained/index.php?title= Acessado: Digitaleconomyandsocietystatistics-householdsandindividuals. 2022-11-119.

[3] Como os ladrões usam as redes sociais para encontrar alvos? https://www.homewatchgroup.com/how-do-burglars-use-social-media-to-find-targets/ . Acesso: 2022-11-119.

[4] Problema do ano 2000. https://en.wikipedia.org/wiki/Year_2000_problem. Acessado: 2022-11-119.

[5] Securesme: dicas cibernéticas para senhas, setembro de 2021.

[6] Padrões de autenticação abertos mais seguros que senhas, novembro de 2022.

[7] N. Achiaga e MD Mar. A Diretiva NIS2: Um elevado nível comum de cibersegurança na UE. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333. [Acessado em: 07 de novembro de 2022].

[8] A. Adams e MA Sasse. Os usuários não são o inimigo. Comum. ACM, 42(12):40–46, dezembro 1999.

[9] R. Agrawal e R. Srikant. Mineração de dados com preservação de privacidade. SIGMOD Rec., 29(2):439–450, maio de 2000.

[10] R. Ahmad e I. Alsmadi. Abordagens de aprendizado de máquina para segurança de IoT: uma abordagem sistemática revisão da literatura. Internet das Coisas, 14:100365, 2021.

[11] C. Alcaraz e J. López. Consciência situacional em ampla área para proteção de infraestrutura crítica. Computador, 46(4):30–37, 2013.

[12] ST Ali, P. McCorry, PH-J. Lee e F. Hao. Zombiecoin 2.0: gerenciando botnets de próxima geração usando bitcoin. Jornal Internacional de Segurança da Informação, 17(4):411–422, 2018.

[13] E. Andrukiewicz, S. Cadzow e S. Górniak. Análise de lacunas nos padrões de segurança. = https://www.enisa.europa.eu/publications/iot-security-standards-gap-análise, 1 2019. [Acesso em: 07 de novembro de 2022].

[14] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, JA Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Men-scher, C. Seaman, N. Sullivan, K. Thomas e Y. Zhou. Compreendendo a rede de bots mirai. Em Anais da 26ª Conferência USENIX sobre Simpósio de Segurança, SEC'17, páginas 1093–1110, EUA, 2017. Associação USENIX.

[15] S. Aral e D. Eckles. Proteger as eleições da manipulação das redes sociais. Ciência, 365(6456):858–861, 2019.

[16] R. Arizona-Peretz, I. Hadar, G. Luria e S. Sherman. Compreender as mentalidades de privacidade e segurança dos desenvolvedores através da teoria climática. Software Empírico. Eng., 26(6), nov. 2021.

[17] BRAÇO. Construindo um sistema seguro usando tecnologia trustzone. Em tecnologia de segurança ARM. ARM, abril de 2009. [Acessado em: 16 de novembro de 2022].

[18] Flecha. Compreender a crescente importância da segurança de hardware em tecnologias IoT. = https:// www.arrow.com/en/research-and-events/articles/understanding-the-importance-of-hardware-security, 5 2020. [Acessado em 07 de novembro de 2022].

[19] ARTE. Metaverso: Mundo virtual, desafios reais. Relatório técnico, análise e pesquisa Equipa do Conselho da União Europeia, março de 2022. [Acesso em: 07 de novembro de 2022].

[20] D. Atch, G. Regev e R. Bevington. https://www.microsoft.com/en-us/security/ blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/, 2021.

[21] M. Azure. Abra o SDK do Enclave. https://openenclave.io/sdk/. [Acessado em: 17 de novembro 2022].

[22] M. Bada, A. Sasse e J. Enfermeira. Campanhas de conscientização sobre segurança cibernética: por que falham mudar o comportamento? Na Conferência Internacional sobre Segurança Cibernética para uma Sociedade Sustentável, páginas 118–131, 01 2015.

[23] O. Barajas. Como a Internet das coisas (iot) está mudando o cenário da segurança cibernética. https:// securityintelligence.com/how-the-internet-of-things-iot-is- Changing-the-cybersecurity-landscape/, 09 2014. [Acessado em 07 de novembro de 2022].

[24] R. Barrett. Construindo uma Organização Orientada por Valores: Uma Abordagem de Sistema Integral para a Transformação Cultural. Butterworth-Heinemann, 2006.

[25] B. Bartolomeu e JA Guerrero-Saade. Agite suas bandeiras falsas! táticas de engano, atribuição de morte na lama em ataques direcionados. Na Virus Bulletin Conference, páginas 1–9, 2016.

[26] V. Boehme-Neßler. Privacidade: uma questão de democracia. por que a democracia precisa de privacidade e Proteção de dados. Lei Internacional de Privacidade de Dados, 6(3):222–229, 2016.

[27] T. Boellstorff. O metaverso ainda não chegou, mas já tem uma longa história. Técnico Relatório 186083, The Conversation, agosto de 2022. [Acessado em 07 de novembro de 2022].

[28] J. Bonneau, C. Herley, PC v. A busca para substituir senhas: Uma estrutura para avaliação comparativa de esquemas de autenticação web. Em 2012 IEEE Simpósio sobre Segurança e Privacidade, páginas 553–567, 2012.

[29] D. Braue. Custos globais de danos causados por ransomware devem ultrapassar US$ 265 bilhões até 2031. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031 , junho de 2022. [Acessado em 07 de novembro 2022].

[30] R. Brown, V. Ta, D. Bienstock, G. Ackerman e J. Wolfram. Isso parece infectado? Um resumo do APT41 direcionado aos governos estaduais dos EUA. https://www.mandiant.com/ recursos/blog/apt41-us-state-governments, 2022. [Acessado em: 07 de novembro de 2022].

[31] MAS Bubukayr e MA Almaiah. Preocupações de segurança cibernética em smartphones e aplicações: Uma pesquisa. Na Conferência Internacional de Tecnologia da Informação (ICIT) de 2021, páginas 725–731, 2021.

[32] B. Bulgurcu, H. Cavusoglu e I. Benbasat. Conformidade com a política de segurança da informação: uma estudo empírico de crenças baseadas na racionalidade e consciência de segurança da informação. MIS Q., 34(3):523–548, setembro de 2010.

[33] M. BULL. Ex-ladrões alertam proprietários sobre postagens nas redes sociais que colocam propriedades em risco de um arrombamento. https://www.express.co.uk/life-style/property/1559309/burglar-tips-hacks-social-media-posts-break-ins-property . Acesso: 2022-11-119.

[34] E. Bursztein. Por dentro do infame Mirai IOT Botnet: uma análise retrospectiva. https:// blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospectiva-análise , setembro de 2021. [Acessado em 07 de novembro de 2022].

[35] A. Cavoukian et al. Privacidade desde a concepção: Os 7 princípios fundamentais. Informação e comissário de privacidade de Ontário, Canadá, 5:2009, 2009.

[36] CC. Critérios comuns para avaliação da segurança da tecnologia da informação. https://www. google.com/search?client=safari&rls=en&q=common+criteria&ie=UTF-8&oe=UTF-8. [Acesso em: 07 de novembro de 2022].

[37] D. Champagne e RB Lee. Suporte arquitetônico escalável para software confiável. Em HPCA - 16 2010 O Décimo Sexto Simpósio Internacional sobre Arquitetura de Computadores de Alto Desempenho, páginas 1–12, 2010.

[38] H. Chang e R. Shokri. Sobre os riscos de privacidade da justiça algorítmica. Em 2021, Simpósio Europeu IEEE sobre Segurança e Privacidade (EuroS&P), páginas 292–303, 2021.

[39] S. Chaudhary, V. Gkioulos e S. Katsikas. Desenvolvimento de métricas para avaliar a eficácia do programa de conscientização sobre segurança cibernética. Jornal de Segurança Cibernética, 8(1), 05 2022. tyac006.

[40] G. Cheng, P. Zhou e J. Han. Aprendendo redes neurais convolucionais invariantes à rotação para detecção de objetos em imagens de sensoriamento remoto óptico vhr. Transações IEEE sobre Geociências e Sensoriamento Remoto, 54(12):7405–7415, 2016.

[41] R. Choudhry e K. Garg. Um sistema híbrido de aprendizado de máquina para previsão do mercado de ações. Academia Mundial de Ciência, Engenharia e Tecnologia, 39, 01 2008.

[42] N. Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou e MA Ferrag. Gamas cibernéticas e bancos de testes para educação, treinamento e pesquisa. Ciências Aplicadas, 11(4), 2021.

[43] N. Chowdhury e V. Gkioulos. Treinamento em segurança cibernética para proteção de infraestrutura crítica: uma revisão da literatura. Revisão de Ciência da Computação, 40:100361, 2021.

[44] E. Comissão. Programa de trabalho da Comissão para 2023. https://ec.europa.eu/info/sites/default/files/cwp_2023.pdf . [Acesso em: 07 de novembro de 2022].

[45] E. Comissão. Políticas de cibersegurança. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies . [Acesso em: 07 de novembro de 2022].

[46] E. Comissão. O pacote da lei sobre serviços digitais. https://digital-strategy.ec. europa.eu/en/policies/digital-services-act-package. [Acesso em: 07 de novembro de 2022].

[47] E. Comissão. Diretiva (eu) 2016/1148 do parlamento europeu e do conselho de 6 de julho de 2016 relativa a medidas para um elevado nível comum de segurança das redes e dos sistemas de informação em toda a união (NIS). = https://eur-lex.europa.eu/eli/dir/2016/1148/oj. [Acesso em: 07 de novembro de 2022].

[48] E. Comissão. Lei europeia sobre governação de dados. https://digital-strategy.ec.europa.eu/en/policies/data-act. [Acesso em: 07 de novembro de 2022].

[49] E. Comissão. Regulamento geral de proteção de dados. https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Acesso em: 07 de novembro de 2022].

[50] E. Comissão. Pessoas, tecnologias e infraestruturas – o plano da Europa para prosperar no metaverso. https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_5525 . [Acesso em: 07 de novembro de 2022].

[51] Conferência das Autoridades Independentes de Supervisão da Protecção de Dados da Federação e dos Länder. O modelo padrão de proteção de dados – um método para aconselhamento e controle de proteção de dados com base em objetivos de proteção uniformes, versão 2.0b (versão em inglês). https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_ V2.0b.pdf, 2020. [Acessado em 07 de novembro de 2022].

[52] K. Conger e K. Roose. Uber investiga violação de seus sistemas de informática. https: //www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html, setembro de 2022. [Acesso em: 07 de novembro de 2022].

[53] M. Corporação. Detalhes de vulnerabilidades e exposições comuns (cve): A fonte de dados de vulnerabilidade de segurança definitiva. https://www.cvedetails.com/browse-by-date.php. [Acessado em: 20 de novembro de 2022].

[54] V. Costan, I. Lebedev e S. Devadas. Sanctum: Extensões mínimas de hardware para forte isolamento de software. No 25º Simpósio de Segurança USENIX (USENIX Security 16), páginas 857–874, Austin, TX, agosto de 2016. Associação USENIX.

[55] CyberSec4Europe. Emblema 2: O segundo exercício de cibersegurança bem-sucedido organizado pela cybersec4europe. https://cybersec4europe.eu/flagship-2-the-successful-second-cybersecurity-exercise-hosted-by-cybersec4europe/ , 03 2022. [Acessado em 07 de novembro de 2022].

[56] CyBOK. O corpo de conhecimento sobre segurança cibernética. https://www.cybok.org. [Acesso em: 07 de novembro de 2022].

[57] A. Da Veiga e N. Martins. Cultura de segurança da informação e cultura de proteção da informação: um instrumento de avaliação validado. Revisão de Legislação e Segurança da Computação, 31(2):243–256, 2015.

[58] S. Dange e M. Chatterjee. Botnet Iot: A maior ameaça à rede IoT. Avanços Sistemas Inteligentes e Computação, 1049:137–157, 2020.

[59] T. DeMarco. Análise Estruturada e Especificação de Sistemas. Yourdon Press, 1979.

[60] M. Deng, K. Wuyts, R. Scandariato, B. Preneel e W. Joosen. Uma estrutura de análise de ameaças à privacidade: apoiando a obtenção e o cumprimento de requisitos de privacidade. Exigir. Eng., 16(1):3–32, março de 2011.

[61] EW Dijkstra et al. Notas sobre programação estruturada. Seção 3 Sobre a confiabilidade dos mecanismos, corolário no final, 1970.

[62] R. Dingledine, N. Mathewson e P. Syverson. Tor: O roteador cebola de segunda geração. Em Anais da 13ª Conferência sobre Simpósio de Segurança USENIX - Volume 13, SSYM'04, página 21, EUA, 2004. Associação USENIX.

[63] A. Dionysiou, M. Agathocleous, C. Christodoulou e V. Promponas. Redes neurais convolucionais em combinação com máquinas de vetores de suporte para classificação sequencial complexa de dados. Em V. K ÿurková, Y. Manolopoulos, B. Hammer, L. Iliadis e I. Maglogian-nis, editores, Artificial Neural Networks and Machine Learning – ICANN 2018, páginas 444–455, Cham, 2018. Springer International Publishing .

[64] C. Diretiva. Diretiva 2008/114/ce do Conselho, de 8 de dezembro de 2008 – relativa à identificação e designação de infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção. Jornal Oficial da União Europeia. L, 345:75–82, 2008.

[65]J. Drees. Bug de software no sistema de agendamento de vacinas do hospital de Nova Jersey causa milhares de consultas duplicadas. https://www.beckershospitalreview.com/healthcare-information-technology/software-bug-in-new-jersey-hospital-s-vacine-scheduling-system-causes-thousands-of-duplicate-appointments.html . Acesso: 2022-11-119.

[66] Z. Durumeric, E. Wustrow e JA Halderman. {ZMap}: Varredura rápida em toda a Internet e seus aplicativos de segurança. No 22º Simpósio de Segurança USENIX (USENIX Security 13), páginas 605–620, Washington, DC, 2013. Associação USENIX.

[67] YK Dwivedi, L. Hughes, AM Baabdullah, S. Ribeiro-Navarrete, M. Giannakis, MM Al-Debei, D. Dennehy, B. Metri, D. Buhalis, CM Cheung, K. Conboy, R. Doyle, R. Dubey, V. Dutot, R. Felix, D. Goyal, A. Gustafsson, C. Hinsch , I. Jebabli, M. Janssen, Y.-G. Kim, J. Kim, S. Koos, D. Kreps, N. Kshetri, V. Kumar, K.-B. Ooi, S. Papagiannidis, IO Pap-pas, A. Polyviou, S.-M. Park, N. Pandey, MM Queiroz, R. Raman, PA Rauschnabel, A. Shirish, M. Sigala, K. Spanaki, G. Wei-Han Tan, MK Tiwari, G. Viglia e SF Wamba. Metaverso além do hype: Perspectivas multidisciplinares sobre desafios emergentes, oportunidades e agenda para pesquisa, prática e política. Jornal Internacional de Gestão da Informação, 66:102542, 2022.

[68]C.Dwork. Privacidade diferencial: uma pesquisa de resultados. Em M. Agrawal, D. Du, Z. Duan e A. Li, editores, Teoria e Aplicações de Modelos de Computação, páginas 1–19, Berlim, Heidelberg, 2008. Springer Berlin Heidelberg.

[69] C. Dwork e DK Mulligan. Não é privacidade e não é justo. Stan. Online, 66:35, 2013.

[70] Enarx. https://enarx.dev/. [Acesso em: 07 de novembro de 2022].

[71] ENISA. Economia da segurança e mercado interno. https://www.enisa.europa.eu/publications/archive/economics-sec . [Acesso em: 07 de novembro de 2022].

[72] ENISA. Compreender o aumento dos ataques à segurança da cadeia de abastecimento. https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks . [Acesso em: 07 de novembro de 2022].

[73] ENISA. Desafios da segurança cibernética da inteligência artificial. Agência da União Europeia para o Ciberespaço segurança (ENISA), agosto de 2021.

[74] ENISA. Desafios da cibersegurança na adoção da inteligência artificial na condução autónoma. Agência da União Europeia para a Cibersegurança (ENISA), agosto de 2021.

[75] ENISA. Cenário de ameaças da ENISA para ataques à cadeia de abastecimento. Agência da União Europeia para Cibersegurança (ENISA), 2021.

[76] ENISA. Protegendo algoritmos de aprendizado de máquina. Agência da União Europeia para a Cibersegurança (ENISA), dezembro de 2021.

[77] ENISA. Dicas para autenticação segura de usuário, agosto de 2021.

[78] ETSI. Etsi em 303 645. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf. [Acesso em: 07 de novembro de 2022].

[79] Comissão Europeia. Lei de resiliência cibernética. https://digital-strategy.ec.europa. eu/en/library/cyber-resilience-act. Acesso: 2022-11-119.

[80] Europol. O emotet de malware mais perigoso do mundo foi interrompido por ação global. https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80% 99s-most-dangerous-malware-emotet-disrupted-through-global-action, 2021.

[81] Eurostat. Pessoas físicas - atividades na internet. https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_ac_i/default/table?lang=en . Acesso: 2022-11-119.

[82] S. Fischer-Hübner, C. Alcaraz, A. Ferreira, C. Fernandez-Gago, J. Lopez, E. Markatos, L. Islami e M. Akil. Perspectivas e requisitos das partes interessadas em matéria de cibersegurança na Europa. Jornal de Segurança da Informação e Aplicações, 61:102916, 2021.

[83] D. Florêncio e C. Herley. Um estudo em larga escala sobre hábitos de senha na web. Em Anais da 16ª Conferência Internacional sobre World Wide Web, WWW '07, páginas 657–666, Nova York, NY, EUA, 2007. Association for Computing Machinery.

[84] Fórum TWE. Definindo e construindo o metaverso. Relatório técnico, weforum.org, jan. 2022. [Acessado em 28 de setembro de 2022].

[85] M. Fredrikson, S. Jha e T. Ristenpart. Ataques de inversão de modelos que exploram informações confiáveis e contramedidas básicas. Em Anais da 22ª Conferência ACM SIGSAC sobre Segurança de Computadores e Comunicações, CCS '15, páginas 1322–1333, Nova York, NY, EUA, 2015. Association for Computing Machinery.

[86] Fundação para a Liberdade de Imprensa. Modelo de ameaça SecureDrop. https://docs. securedrop.org/en/stable/threat_model/threat_model.html, 2022. [Acessado em: 07 de novembro de 2022].

[87] J. Freund e J. Jones. Medindo e gerenciando o risco da informação: uma abordagem justa. Butterworth-Heinemann, 2014.

[88] JE Gaffney. Estimando o número de falhas no código. Transações IEEE em Engenharia de Software, SE-10(4):459–464, 1984.

[89] T. Gagliardoni. O hack da rede poli explicado. https://pesquisa. kudelskisecurity.com/2021/08/12/the-poly-network-hack-explained. [Acesso em: 07 de novembro de 2022].

[90] B. Gardner e V. Thomas. Construindo um Programa de Conscientização sobre Segurança da Informação: Defesa contra Engenharia Social e Ameaças Técnicas. Publicação Syngress, 1ª edição, 2014.

[91] V. Garousi, A. Rainer, P. Lauvås e A. Arcuri. Educação em teste de software: um mapeamento sistemático da literatura. Jornal de Sistemas e Software, 165:110570, 2020.

[92] S. Gatlán. Hackers chineses usam novo malware do Windows para fazer backdoor em organizações governamentais e de defesa. https://www.bleepingcomputer.com/news/security/chinese-hackers-use-new-windows-malware-to-backdoor-govt-defense-orgs/ , agosto de 2022. [Acessado em 07 de novembro de 2022].

[93] RGPD. Regulamento Geral de Proteção de Dados. https://gdpr-info.eu. [Acesso: 07 novembro de 2022].

[94] T. Geppert, S. Deml, D. Sturzenegger e N. Ebert. Ambientes de execução confiáveis: aplicativos e desafios organizacionais. Fronteiras na Ciência da Computação, 4, 2022.

[95] S. Gilberto. A economia política do metaverso. Relatório técnico, Briefings de l'IFRI, IFRI, junho de 2022. [Acesso em: 07 de novembro de 2022].

[96] I. Goodfellow, J. Shlens e C. Szegedy. Explicando e aproveitando exemplos adversários. arXiv 1412.6572, 12 2014.

[97] Google. Asilo. https://asylo.dev/. [Acessado em: 17 de novembro de 2022]. [98]

gramina. Gramina. https://gramineproject.io/. [Acesso em: 07 de novembro de 2022].

[99] A. Graves, A.-r. Mohamed e G. Hinton. Reconhecimento de fala com redes neurais recorrentes profundas. Em 2013, Conferência Internacional IEEE sobre Acústica, Fala e Processamento de Sinais, páginas 6645–6649, 2013.

[100] A. Greenberg. Hackers matam remotamente um jipe na estrada – comigo nele. https: //www.wired.com/2015/07/hackers-remotely-kill-jeep-highway, 7 2015. [Acessado em 07 de novembro de 2022].

[101] L. Grindstaff. Através da sua mente: quais preconceitos estão impactando sua postura de segurança? https://www.mcafee.com/blogs/other-blogs/executive-perspectives/through-your-minds-eye-what-biases-are-impacting-your-security-posture/ , 05 2021. [Acesso em: 07 de novembro de 2022].

[102] S. Gürses e JM Del Alamo. Engenharia de privacidade: moldando um campo emergente de pesquisa e prática. Segurança e privacidade IEEE, 14(2):40–46, 2016.

[103] I. Hadar, T. Hasson, O. Ayalon, E. Toch, M. Birnhack, S. Sherman e A. Balissa. Privacidade dos designers: a mentalidade de privacidade dos desenvolvedores de software. Software Empírico. Eng., 23(1):259–289, fevereiro de 2018.

[104] M. Hansen, M. Jensen e M. Rost. Metas de proteção para engenharia de privacidade. Em Proceedings of the 2015 IEEE Security and Privacy Workshops, SPW '15, páginas 159–166, EUA, 2015. Sociedade de Computação IEEE.

[105] A. Harish. Quando a NASA perdeu uma espaçonave devido a um erro matemático métrico. https://www.simscale.com/blog/nasa-mars-climate-orbiter-metric/. Acesso: 2022-11-119.

[106] Sr. Hasan. Número de dispositivos IoT conectados crescendo 18%, para 14,4 bilhões em todo o mundo. https://iot-analytics.com/number-connected-iot-devices/, 5 2022. [Acessado em 07 de novembro de 2022].

[107] N. Hasan, A. Chamoli e M. Alam. Desafios de privacidade e suas soluções em IoT. Internet das Coisas (IoT): Conceitos e Aplicações, páginas 219–231, 1 2020.

[108] J. Haworth. Falhas de dia zero em monitores para bebês iot podem dar aos invasores acesso às imagens das câmeras. https://portswigger.net/daily-swig/zero-day-flaws-in-iot-baby-monitors-could-give-attackers-access-to-camera-feeds , 9 2021. [Acessado em: 07 de novembro de 2022] .

[109] JL Hernández-Ramos, G. Baldini, SN Matheu e A. Skarmeta. Atualizando dispositivos IoT: desafios e abordagens potenciais. GIoTS 2020 - Cúpula Global da Internet das Coisas, Anais, páginas 1–5, 2020.

[110] J. Hodges, J. Jones, MB Jones, A. Kumar e E. Lundberg. Autenticação da Web: uma API para acessar credenciais de chave pública nível 2.

[111] J.-H. Hoepman. Estratégias de design de privacidade. Em N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam e T. Sans, editores, ICT Systems Security and Privacy Protection, páginas 446–459, Berlim, Heidelberg, 2014. Springer Berlin Heidelberg.

[112] M. Howard e S. Lipner. O ciclo de vida do desenvolvimento de segurança. Microsoft Press, 2006.

[113] T. Caça. Sites possuídos.

[114] F. Hussain, R. Hussain, SA Hassan e E. Hossain. Aprendizado de máquina em segurança IoT: soluções atuais e desafios futuros. Pesquisas e tutoriais de comunicações IEEE, 22(3):1686–1721, 2020.

[115] COLHER. A segurança da Internet e o consumidor: os desafios e a questão da educação. = https://www.i-scoop.eu/iot-security-consumer-education/. [Acesso: 07 de novembro 2022].

[116] IBM. Custo de um relatório de violação de dados de 2022. https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time- Alto, Julho de 2022. [Acesso em: 07 de novembro de 2022].

[117] J. Inclán. Emotet exposto: uma visão da cadeia de suprimentos do cibercrime. https://blogs.vmware.com/security/2022/10/emotet-exposed-a-look-inside-the-cybercriminal-supply-chain.html , 2022.

[118]Inmarsat. Iot industrial na época do covid-19. https://www.inmarsat.com/en/insights/enterprise/2021/research-programme-2021-industrial-iot-covid- 19.html, 2021. [Acessado em 07 de novembro de 2022].

[119] Informações. Na referência de programação das extensões Intel Software Guard. ARM, outubro de 2014. [Acencerrado: 16 de novembro de 2022].

[120] IriusRisco. Risco Irius. https://www.iriusrisk.com/, 2022. [Acessado em: 07 de novembro de 2022].

[121] L. Islami, S. Fischer-Hübner e P. Papadimitratos. Capturando as preferências de privacidade dos motoristas para sistemas de transporte inteligentes: uma perspectiva intercultural. Computadores & Segurança, 123:102913, 2022.

[122] LH Iwaya, GH Iwaya, S. Fischer-Hübner e AV Steil. Cultura de privacidade organizacional e clima: uma revisão do escopo. Acesso IEEE, 10:73907–73930, 2022.

[123] J. Jalkanen. O ser humano é o elo mais fraco na segurança da informação? Revisão Sistemática da Literatura. Universidade de Jyväskylä, Jyväskylä, Finlândia, 2019.

[124] SV Joshi, D. Stubbe, S.-TT Li e DM Hilty. O uso da tecnologia pelos jovens: Implicações para educadores psiquiátricos. Psiquiatria Acadêmica, 43(1):101–109, 2019.

[125] D. Kaplan, J. Powell e T. Woller. Na criptografia de memória AMD. AMD, abril de 2016. [Acencerrado: 16 de novembro de 2022].

[126] G. Karantzas e C. Patsakis. Uma avaliação empírica de sistemas de detecção e resposta de endpoint contra vetores de ataque de ameaças persistentes avançadas. Jornal de Segurança Cibernética e Privacidade, 1(3):387–421, 2021.

[127] T. Karras, S. Laine e T. Aila. Uma arquitetura geradora baseada em estilo para redes adversárias generativas. Em 2019 Conferência IEEE/CVF sobre Visão Computacional e Reconhecimento de Padrões (CVPR), páginas 4396–4405, 2019.

[128] Kaspersky. O fator humano na segurança de TI: como os funcionários estão tornando as empresas vulneráveis por dentro. https://www.kaspersky.com/blog/the-human-factor-in-it-security/ , 11 2022. [Acessado em 07 de novembro de 2022].

[129] N. Kohl e P. Stone. Aprendizagem por reforço de gradiente de política para locomoção quadrúpede rápida. Na Conferência Internacional IEEE sobre Robótica e Automação, 2004. Anais. ICRA '04. 2004, volume 3, páginas 2619–2624 Vol.3, 2004.

[130] L. Kohnfelder e P. Garg. As ameaças aos nossos produtos. Interface da Microsoft, Microsoft Corporação, 33, 1999.

[131] I. Kononenko. Aprendizado de máquina para diagnóstico médico: história, estado da arte e perspectiva. Inteligência Artificial em Medicina, 23(1):89–109, 2001.

[132] V. Koutsokostas e C. Patsakis. Python e malware: desenvolvendo furtividade e evasão malware sem ofuscação. Em SDC di Vimercati e P. Samarati, editores, Proceedings da 18ª Conferência Internacional sobre Segurança e Criptografia, SECRYPT 2021, 6 a 8 de julho, 2021, páginas 125–136. SCITEPRESS, 2021.

[133] A. Küchler, A. Mantovani, Y. Han, L. Bilge e D. Balzarotti. Cada segundo conta? evolução baseada no tempo do comportamento do malware em sandboxes. No 28º Simpósio Anual de Segurança de Redes e Sistemas Distribuídos, NDSS 2021, virtualmente, de 21 a 25 de fevereiro de 2021. A Internet Sociedade, 2021.

[134] I. Kuzminykh, B. Ghita e JM Tal. Os desafios da internet das coisas para os negócios. https://arxiv.org/abs/2012.03589, 12 2020. [Acessado em 07 de novembro de 2022].

[135] AL Lafuente, F. Nielson, S. Mödersheim, A. Schlichtkrull, A. Sforzin, C. Sorientea, L. Kamm, R. Martins, J. Soares, L. Antunes, L. Durante, M. Cheminod, E. Athanasopou-los, B. Hamid, A. Omerovic, K. Bernsmed e RS Per H Meland. Desafios de pesquisa e requisitos para desenvolvimento seguro de software. https://cybersec4europe.eu/wp-content/uploads/2020/09/CS4E-D3.9-Research-challenges-and-requirements-for-secure-software-development-v1.1-Submitted.pdf , 2020. [Acesso: 07 novembro de 2022].

[136] T. LAMBERT e B. DONOHUE. É tudo diversão e jogos até que o ransomware seja excluído as cópias de sombra. https://redcanary.com/blog/its-all-fun-and-games-until-ransomware-deletes-the-shadow-copies , 2022. [Acessado em: 07 de novembro de 2022].

[137] R. Langner. Stuxnet: Dissecando uma arma de guerra cibernética. Segurança e privacidade IEEE, 9(3):49–51, 2011.

[138] D. Lee, D. Kohlbrenner, S. Shinde, K. Asanovi´c e D. Song. Keystone: Uma estrutura aberta para arquitetar ambientes de execução confiáveis. Em Anais da Décima Quinta Conferência Europeia sobre Sistemas de Computador, EuroSys '20, Nova York, NY, EUA, 2020. Associação para máquinas de computação.

[139] K. LeFevre, D. DeWitt e R. Ramakrishnan. K-anonimato multidimensional de Mondrian. Na 22ª Conferência Internacional sobre Engenharia de Dados (ICDE'06), páginas 25–25, 2006.

[140] NG Leveson. O therac-25: 30 anos depois. Computador, 50(11):8–11, 2017.

[141] MN Lintvedt. Colocar um preço na violação da proteção de dados. Privacidade de dados internacionais Lei, 12(1):1–15, 12 2021.

[142] B. Liu, M. Ding, S. Shaham, W. Rahayu, F. Farokhi e Z. Lin. Quando o aprendizado de máquina encontra a privacidade: uma pesquisa e perspectivas. ACM Computação. Sobrev., 54(2), março de 2021.

[143] J. Lopez, C. Alcaraz e R. Roman. Controle inteligente de ameaças operacionais em subestações de controle. Computadores e Segurança, 38:14–27, 2013. Crime Cibernético na Economia Digital.

[144] P. Lorenzo, F. Stefano, A. Ferreira e P. Carolina. Inteligência artificial e segurança cibernética: desafios tecnológicos, de governança e políticos. https://www.ceps.eu/wp-content/uploads/2021/05/CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf, 2021. [Acessado em: 07 de novembro de 2022].

[145] T. Madiega, P. Car e MN com Louise Van de Pol. Metaverso: oportunidades, riscos e implicações políticas. Relatório Técnico PE 733.557, Investigação do Parlamento Europeu Serviço, junho de 2022. [Acesso em: 07 de novembro de 2022].

[146] S. Maes, K. Tuyls, B. Vanschoenwinkel e B. Manderick. Detecção de fraude de cartão de crédito usando redes bayesianas e neurais. Nos Anais do 1º Congresso Internacional Naiso sobre tecnologias neuro fuzzy, páginas 261–270, 08 2002.

[147] K. Manheim e L. Kaplan. Inteligência artificial: riscos para a privacidade e a democracia. Yale JL & Tech., 21:106, 2019.

[148] K. Marky, K. Ragozin, G. Chernyshov, A. Matviienko, M. Schmitz, M. Mühlhäuser, C. Eghtebas e K. Kunze. "não, é simplesmente irritante!" um mergulho profundo nas percepções do usuário de autenticação de dois fatores. Transações ACM sobre interação computador-humano, 29(5), out 2022.

[149]G. McGraw. Segurança de software: construindo segurança. Addison-Wesley Profissional, 2006.

[150] metaverso standards.org. O fórum de padrões do metaverso. Relatório técnico, metaverse-standards.org, junho de 2022. [Acessado em: 07 de novembro de 2022].

[151] MicroAge. Os benefícios do treinamento de conscientização em segurança cibernética. https://microage.ca/the-benefícios do treinamento de conscientização sobre segurança cibernética /, 10 de 2022. [Acessado em: 07 de novembro 2022].

[152]Microsoft. Crie e use senhas fortes — support.microsoft.com. https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb . 2022]. [Acesso: 07 de novembro

[153]Microsoft. Microsoft sdl. https://www.microsoft.com/en-us/securityengineering/ sdl/práticas. [Acesso em: 07 de novembro de 2022].

[154]Microsoft. Aplicações para inteligência artificial no departamento de defesa cibernética missões. https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial- intelligence-department-of-defense-cyber-missions/, 05 2022. [Acessado: 07 novembro de 2022].

[155]Microsoft. Relatório Especial: Ucrânia: Uma visão geral da atividade de ataque cibernético da Rússia em Ucrânia. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd, 2022. [Acessado em: 07 de novembro de 2022].

[156] Microsoft Corporação. Ferramenta de modelagem de ameaças da Microsoft 7. https://aka.ms/ ferramenta de modelagem de ameaças, 2022. [Acessado em: 07 de novembro de 2022].

[157] J. Miranda, N. Mäkitalo, J. Garcia-Alonso, J. Berrocal, T. Mikkonen, C. Canal e JM Murilo. Da internet das coisas à internet das pessoas. Computação na Internet IEEE, 19(2):40–47, 2015.

[158] H. Modi. Relatório de inteligência de ameaças da Netscout. https://www.netscout.com/ sites/padrão/arquivos/2019-02/SECR_001_EN-1901%20-%20NETSCOUT%20Threat% 20Intelligence%20Report%202H%202018.pdf, 2018. [Acessado em 07 de novembro de 2022].

[159] Filme. Jogador um pronto, 2018. [Acessado em: 07 de novembro de 2022].

[160] P. Muncaster. Hóspedes de hotel trancados fora dos quartos após ataque de ransomware. https://www. infosecurity-magazine.com/news/hotel-guests-locked-out-rooms, dezembro de 2021. [Acesso: 07 de novembro de 2022].

[161] S. Muppidi, L. Fisher e G. Parham. IA e automação para segurança cibernética. Técnico relatório, IBM Corporation, junho de 2022. [Acessado em 07 de novembro de 2022].

[162] AS Namin, Z. Aguirre-Muñoz e KS Jones. Ensinando segurança cibernética por meio da competição: um relato de experiência sobre uma oficina de treinamento participativo. Na Conferência Internacional sobre Inovação e Tecnologia em Educação em Ciência da Computação (CSEIT). Processo, página 98. Fórum Global de Ciência e Tecnologia, 2016.

[163] Administração Nacional de Segurança no Trânsito Rodoviário. Relatório de recall de segurança Parte 573. https: //static.nhtsa.gov/odi/rcl/2021/RCLRPT-21V035-4682.PDF. Acesso: 2022-11-119.

[164] T.Ncubukezi. Erros humanos: uma preocupação de segurança cibernética e o elo mais fraco para as pequenas empresas. Conferência Internacional sobre Guerra Cibernética e Segurança, 17:395–403, 03 2022.

[165] LH Newman. Milhões de imagens de câmeras web e monitores de bebês são expostas. https: // www.wired.com/story/kalay-iot-bug-video-feeds/, 2017. [Acessado em 07 de novembro de 2022].

[166] Z. Ning, F. Zhang, W. Shi e W. Shi. Documento de posição: Desafios para proteger ambientes de execução assistidos por hardware. Em Proceedings of the Hardware and Architectural Support for Security and Privacy, HASP '17, Nova York, NY, EUA, 2017. Association for Computing Machinery.

[167]NIST. Estrutura segura de desenvolvimento de software. https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-218.pdf . [Acesso em: 07 de novembro de 2022].

[168] NIST. Nist anuncia os primeiros quatro algoritmos criptográficos resistentes a quantum. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistente-cryptographic-algorithms , julho de 2022. [Acessado em 07 de novembro de 2022].

[169] C. Nobata, J. Tetreault, A. Thomas, Y. Mehdad e Y. Chang. Detecção de linguagem abusiva em conteúdo de usuários online. Em Anais da 25ª Conferência Internacional sobre World Wide Web, WWW '16, páginas 145–153, República e Cantão de Genebra, CHE, 2016. Comitê Diretor de Conferências Internacionais da World Wide Web.

[170] C. Ntantogian, S. Malliaros e C. Xenakis. Avaliação de esquemas de hashing de senhas em plataformas web de código aberto. Computadores e Segurança, 84:206–224, 2019.

[171] M. Nunes, P. Burnap, P. Reinecke e K. Lloyd. Bane ou benção: Medindo o efeito do malware evasivo nos classificadores de chamadas do sistema. J. Inf. Seguro. Requerimento, 67(C), junho de 2022.

[172] oclulo. Oclum. https://occlum.io/. [Acesso em: 07 de novembro de 2022].

[173] NI de Padrões e Tecnologia. Diretrizes de identidade digital: Autenticação e gerenciamento do ciclo de vida. Relatório técnico, Departamento de Comércio dos EUA, Washington, DC, 2017.

[174] L. O'Gorman. Comparando senhas, tokens e biometria para autenticação de usuários. Anais do IEEE, 91(12):2021–2040, 2003.

[175] Grupo OMI. Grupo de interoperabilidade do metaverso aberto. Relatório técnico, Grupo OMI, set. 2022. [Acessado em: 07 de novembro de 2022].

[176] PH O'Neill. O ransomware não matou um paciente de hospital alemão. https: //www.technologyreview.com/ 2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital- Patient, novembro de 2020. [Acessado em 07 de novembro de 2022].

[177] opentitã. Opentitã. https://opentitan.org/. [Acesso em: 07 de novembro de 2022].

[178] C. Osborne. Botnets fragmentados Mirai dominam a cena de ataque iot. https:// www.zdnet.com/article/mirai-splinter-botnets-dominate-iot-attack-scene/, 1 2022. [Acessado em 07 de novembro de 2022].

[179] M. Ovelgönne, T. Dumitra¸s, BA Prakash, VS Subrahmanian e B. Wang. Compreendendo a relação entre o comportamento humano e a suscetibilidade a ataques cibernéticos: uma abordagem baseada em dados. ACM Trans. Intel. Sist. Technol., 8(4), março de 2017.

[180] OWASP. Top 10 do OWASP - 2021. https://owasp.org/Top10/, 2021. [Acessado em: 07 de novembro de 2021. ber 2022].

[181] E. Papadogiannakis, P. Papadopoulos, N. Kourtellis e EP Markatos. Rastreamento de usuários na era pós-cookie: como os sites ignoram o consentimento do GDPR para rastrear usuários. Em Proceedings of the Web Conference 2021, WWW '21, páginas 2130–2141, Nova York, NY, EUA, 2021. Association for Computing Machinery.

[182] N. Papernot, P. McDaniel, A. Sinha e MP Wellman. Sok: Segurança e privacidade em aprendizado de máquina. Em 2018, Simpósio Europeu IEEE sobre Segurança e Privacidade (EuroS&P), páginas 399–414, 2018.

[183] M. Paquet-Clouston, M. Romiti, B. Haslhofer e T. Charvat. Spams encontram criptomoedas: Sextorção no ecossistema bitcoin. Em Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT '19, páginas 76–88, Nova York, NY, EUA, 2019. Association for Computing Machinery.

[184] C. Patsakis e F. Casino. Hydras e ipfs: um playground descentralizado para malware. Jornal Internacional de Segurança da Informação, 18(6):787–799, 2019.

[185] C. Patsakis e A. Chrysanthou. Analisando a campanha de emotet do outono de 2020. Pré-impressão do arXiv arXiv:2011.06479, 2020.

[186] S. Peldszus, K. Tuma, D. Strüber, J. Jürjens e R. Scandariato. Verificações seguras de conformidade de fluxo de dados entre modelos e códigos com base em mapeamentos automatizados. Em 2019, 22ª Conferência Internacional ACM/IEEE sobre Linguagens e Sistemas de Engenharia Orientados a Modelos (MOD-ELS), páginas 23–33, 2019.

[187]RP Pires. Sistemas distribuídos e ambientes de execução confiáveis: compensações e desafios. https://arxiv.org/pdf/2001.09670.pdf, dezembro de 2019. [Acessado em 20 de novembro de 2022].

[188] S. Pletinckx, C. Trap e C. Doerr. Coordenação de malware usando blockchain: uma análise do cerber ransomware. Na Conferência IEEE de 2018 sobre Comunicações e Segurança de Rede (CNS), páginas 1–9, 2018.

[189] N. Popper. A Knight Capital diz que uma falha comercial lhe custou US$ 440 milhões. https: // archive.nytimes.com/dealbook.nytimes.com/2012/08/02/knight-capital-diz-trading-mishap-cost-it-440-million/ . Acesso: 2022-11-119.

[190] W. Presthus e KF Sønslien. Uma análise das violações e sanções decorrentes do GDPR. Jornal Internacional de Sistemas de Informação e Gerenciamento de Projetos, 9(1):38–53, setembro de 2021.

[191] pcc. Conti ataque cibernético ao HSE. https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf , 2021. [Acessado em 07 de novembro de 2022].

[192] D. Leitura. Câmeras IoT populares precisam de patches para evitar ataques catastróficos. https://www.darkreading.com/attacks-breaches/popular-iot-cameras-patching-catastrophy-attacks , 9 2022. [Acessado em 07 de novembro de 2022].

[193] D. Rehak, P. Senovsky, M. Hromada e T. Lovecek. Abordagem complexa para avaliar a resiliência de elementos críticos de infraestrutura. Jornal internacional de proteção de infraestrutura crítica, 25:125–138, 2019.

[194]Reuter. Divisão AXA na Ásia atingida por ataque cibernético de ransomware. https://www.reuters. com/article/us-axa-cyber-idUSKCN2CX0B0, maio de 2021. [Acessado em 07 de novembro de 2022].

[195]Reuter. Paralisação dos trens dinamarqueses no sábado causada por ataque cibernético. https: // www.reuters.com/technology/danish-train-standstill-saturday-caused-by-cyber-attack-2022-11-03/ , novembro de 2022. [Acessado em 07 de novembro de 2022].

[196] S. Rinaldi, J. Peerenboom e T. Kelly. Identificar, compreender e analisar interdependências críticas de infraestrutura. Revista IEEE Control Systems,

21(6):11–25, 2001. [197] risco. Armadilhas de segurança no desenvolvimento de tees. https://www.riscu armadilhas de segurança no desenvolvimento tee/. [Acesso em: 07 de novembro de 2022].

[198] A. ROBERTSON. A maioria dos assassinos persegue as suas vítimas nas redes sociais antes de as assassinar, dizem os criminologistas. https://www.dailymail.co.uk/news/article-4439130/Most-killers-stalk-victims-social-media-murder.html . Acesso: 2022-11-119.

[199] A. Rowe. Estudo revela que uma pessoa média tem 100 senhas | Tech.co — tech.co. https: //tech.co/password-managers/how-many-passwords-average-person, 2021. [Acesso: 07 de novembro de 2022].

[200] P. Ruggiero e J. Foote. Ameaças cibernéticas a telefones celulares. https://www.cisa.gov/uscert/sites/default/files/publications/cyber_threats_to_mobile_phones.pdf , 2011. [Acessado em 07 de novembro de 2022].

[201] O. SAMM. Modelo de maturidade de garantia de software. https://owaspsamm.org/model/. [Acacessado: 07 de novembro de 2022].

[202] Sanket. O custo exponencial da correção de bugs. https://deepsource.io/blog/exponencial-cost-of-fixing-bugs/ . [Acesso em: 07 de novembro de 2022].

[203] IH Sarker, AI Khan, YB Abushark e F. Alsolami. Inteligência de segurança da Internet das coisas (iot): uma visão geral abrangente, soluções de aprendizado de máquina e orientações de pesquisa. Redes Móveis e Aplicações, 1:1–17, 3 2022.

[204] T. Schaberreiter, K. Kittilä, K. Halunen, J. Röning e D. Khadraoui. Avaliação de riscos em modelagem de segurança de infraestrutura crítica baseada em análise de dependência. No Workshop Internacional sobre Segurança de Infraestruturas Críticas de Informação, páginas 213–217. Springer, 2011.

[205] PM Schwartz. Privacidade e democracia no ciberespaço. Vand. L. Rev., 52:1607, 1999.

[206] T. Selos. O botnet Mozi é responsável pela maior parte do tráfego iot. = https://threatpost.com/mozi-botnet-majority-iot-traffic/159337/, 9 2020. [Acessado em 07 de novembro de 2022].

[207] FT Segurança. Aumente o envolvimento com treinamento em jogos sérios. https://terranovasecurity.com/serious-game/ , 10 2022. [Acessado em 07 de novembro de 2022].

[208] R. Setola, S. De Porcellinis e M. Sforna. Avaliação da dependência de infra-estruturas críticas utilizando o modelo de inoperabilidade de entradas-saídas. Jornal Internacional de Proteção de Infraestruturas Críticas, 2(4):170–178, 2009.

[209] R. Setola, V. Rosato, E. Kyriakides e E. Roma. Gerenciando a complexidade de infraestruturas críticas: uma abordagem de modelagem e simulação. Natureza Springer, 2016.

[210] M. Shahraeini, P. Kotzanikolaou e M. Nasrolahi. Resiliência de comunicação para redes inteligentes com base em gráficos de dependência e análise autoespectral. Diário de Sistemas IEEE, páginas 1–11, 2022.

[211] R. Shokri, M. Stronati, C. Song e V. Shmatikov. Ataques de inferência de membros contra modelos de aprendizado de máquina. Em 2017 Simpósio IEEE sobre Segurança e Privacidade (SP), páginas 3–18, 2017.

[212] A.Shostack. Modelagem de ameaças: projetando para segurança. John Wiley & Sons, Indianápolis, Indiana, 2014.

[213] J. Sigholm, G. Falco e A. Viswanathan. Melhorar a educação em segurança cibernética por meio de exercícios ao vivo de alta fidelidade (hiflix). Em HICSS, 01 2019.

[214] L. Sion, D. Van Landuyt, K. Yskout, S. Verreydt e W. Joosen. Análise e gerenciamento automatizados de ameaças em um pipeline de integração contínua. Em 2021 IEEE Secure Development Conference (SecDev), páginas 30–37, 2021.

[215] L. Sion, K. Yskout, D. Van Landuyt e W. Joosen. Análise de segurança de projeto baseada em risco. In Proceedings - 2018 IEEE/ACM First International Workshop on Security Awareness from Design to Deployment, SEAD 2018, páginas 11–18, Nova York, NY, EUA, 2018. Association for Computing Machinery.

[216] J. Smart, N. Cascio e J. Paffendorf. Roteiro do metaverso - caminhos para a web 3D: um projeto de previsão pública intersetorial. https://metaverseroadmap.org/MetaverseRoadmapOverview.pdf . [Acesso em: 07 de novembro de 2022].

[217] I. Sommerville. Engenharia de software 10. Harlow: Pearson Education Limited, 2016.

[218] Sófos. O estado do ransomware 2022. https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf, 2022. [Acessado em 07 de novembro de 2022].

[219] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele e C. Allen. Descentralizado identificadores (dids).

[220] M. Sporny, G. Noble, D. Longley, DC Burnett, B. Zundel e KD Hartog. Verificável modelo de dados de credenciais.

[221] R. Steen. 5 razões pelas quais a automação não pode assumir o controle da segurança cibernética. https://www.securitymagazine.com/articles/98396-5-reasons-automation-cant-take-over-cybersecurity , 9 2022. [Acessado em 07 de novembro de 2022].

[222] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz e J. Lopez. Uma pesquisa sobre ataques cibernéticos habilitados para IoT: avaliando caminhos de ataque a infraestruturas e serviços críticos. IEEE Pesquisas e tutoriais de comunicação, 20(4):3453–3495, 2018.

[223] N. Stephenson. Queda de neve. Bantam Books, Estados Unidos da América, 1992.

[224] G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, G. Lykou e D. Gritzalis. Análise de dependência de infraestrutura crítica baseada no tempo para falhas em grande escala e intersetoriais. Jornal Internacional de Proteção de Infraestruturas Críticas, 12:46–60, 2016.

[225] GE Suh, D. Clarke, B. Gassend, M. van Dijk e S. Devadas. Aegis: Arquitetura para processamento inviolável e resistente à violação. Em Anais da 17ª Conferência Internacional Anual sobre Supercomputação, ICS '03, páginas 160–171, Nova York, NY, EUA, 2003. Associação de Máquinas de Computação.

[226] L. Sweeney. K-anonimato: um modelo para proteger a privacidade. Internacional J. Incerto. Imprecisão Knowl.-Based Syst., 10(5):557–570, outubro de 2002.

[227] F. Swiderski e W. Snyder. Modelagem de ameaças. Microsoft Press, 2004.

[228] J.Taylor. Interrupção do Facebook: o que deu errado e por que demorou tanto para consertar depois que a plataforma social caiu? https://www.theguardian.com/technology/2021/oct/05 / facebook-outage-o que deu errado e por que demorou tanto para consertar. Acessado: 2022-11-119.

[229] Equipe WCD. Grupo comunitário de interoperabilidade do metaverso. Relatório técnico, w3c.org, Setembro de 2022. [Acessado em: 07 de novembro de 2022].

[230] W. Tecnologias. Nova pesquisa: Ataques de malware sem arquivo aumentam em 900% e os criptomineradores estão de volta, enquanto os ataques de ransomware diminuem. https://www.watchguard.com/wgrd-about/press-releases/new-research-fileless-malware-attacks-surge-900-and-cryptominers-make , 2021. [Acessado: 07 novembro de 2022].

[231] B. Tekinerdogan. Análise de desvio arquitetônico usando o ponto de vista de reflexão de arquitetura e matrizes de reflexão de estrutura de projeto. Em Garantia de Qualidade de Software, páginas 221–236. Elsevier, 2016.

[232] P.Torr. Desmistificando o processo de modelagem de ameaças. Segurança e Privacidade IEEE, 3(5):66–70, 2005.

[233] Trilha de Bits. Modelo de ameaça do Kubernetes. https://github.com/kubernetes/community/raw/683ec8f8a392522933b8950a052dfdce6da6a812/sig-security/security-audit- 2019/findings/Kubernetes%20Threat%20Model.pdf, 2019. [Acessado em 07 de novembro 2022].

[234] S. Truex, L. Liu, ME Gursoy, L. Yu e W. Wei. Desmistificando ataques de inferência de associação no aprendizado de máquina como serviço. Transações IEEE em Computação de Serviços, 14(6):2073–2089, 2021.

[235] K. Tuma, L. Sion, R. Scandariato e K. Yskout. Automatizando a detecção precoce de falhas de projeto de segurança. Em Anais da 23ª Conferência Internacional ACM/IEEE sobre Linguagens e Sistemas de Engenharia Acionados por Modelos, MODELS '20, páginas 332–342, Nova York, NY, EUA, 2020. Association for Computing Machinery.

[236] W. Turton e K. Mehrotra. Ataque cibernético ao gasoduto colonial: hackers usaram senha comprometida. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breasted-colonial-pipeline-using-compromised-password , junho de 2021. [Acessado em 07 de novembro de 2022].

[237] Departamento de Justiça dos EUA. Departamento de Justiça Anuncia Interrupção Autorizada pelo Tribunal de Botnet Controlada pela Diretoria Principal de Inteligência da Federação Russa (GRU). https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation , 2022.

[238] LS Vailshery. Número de dispositivos conectados à Internet das coisas (iot) em todo o mundo de 2019 a 2021, com previsões de 2022 a 2030. https://www.statista.com/statistics/ 1183457/iot-connected-devices-worldwide/, 8 2022. [Acesso em: 07 de novembro de 2022].

[239] J. van Rest, D. Boonstra, M. Everts, M. van Rijn e R. van Paassen. Projetando privacidade por design. Em B. Preneel e D. Ikonomou, editores, Privacy Technologies and Policy, páginas 55–72, Berlim, Heidelberg, 2014. Springer Berlin Heidelberg.

[240] Verizon. Relatório de investigações de violação de dados. https://www.verizon.com/business/resources/reports/dbir/ , 06 2022. [Acesso: 07 novembro 2022].

[241] Versículo. Manifesto sobre pesquisa e educação de software na Holanda. https://www.versen.nl/assets/manifesto/digitalfolder.pdf , 2020. [Acessado em 07 de novembro de 2022].

[242] N. Virvilis, D. Gritzalis e T. Apostolopoulos. Computação confiável versus ameaças persistentes avançadas: um defensor pode vencer este jogo? Em 2013, 10ª Conferência Internacional IEEE sobre Inteligência Ubíqua e Computação e 10ª Conferência Internacional IEEE sobre Computação Autonômica e Confiável de 2013, páginas 396–403, 2013.

[243] S. Wang, X. Gu, S. Luan e M. Zhao. Análise de resiliência de sistemas de infraestrutura crítica interdependentes considerando aprendizagem profunda e teoria de redes. Jornal Internacional de Proteção de Infraestruturas Críticas, 35:100459, 2021.

[244] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, TH Luan e X. Shen. Uma pesquisa sobre metaverso: fundamentos, segurança e privacidade. Pesquisas e tutoriais de comunicações IEEE, páginas 1–1, 2022.

[245] W. Wei. O cassino é hackeado por meio de seu termômetro de aquário conectado à Internet. https: // thehackernews.com/2018/04/iot-hacking-thermometer.html, 4 2018. [Acessado em 07 de novembro de 2022].

[246] R. Weiss, X. Mountrouidou, S. Watson, J. Mache, E. Hawthorne e A. Chattopadhyay. Cibersegurança em todas as disciplinas em 2020. Em Proceedings of the 51st ACM Technical Symposium on Computer Science Education, SIGCSE '20, página 1404, Nova York, NY, EUA, 2020. Associação de Máquinas de Computação.

[247] E. Weyuker. Testando software baseado em componentes: um conto de advertência. Software IEEE, 15(5):54–59, 1998.

[248] Wikipédia. Identidade autossoberana. https://en.wikipedia.org/wiki/Self-sovereign_identidade . [Acesso em: 07 de novembro de 2022].

[249] M. Wilson e J. Hash. Sp 800-50. construir um programa de conscientização e treinamento em segurança de tecnologia da informação. Relatório técnico, Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD, EUA, 2003.

[250] J. Wolff e N. Atallah. Penalidades antecipadas do GDPR: Análise da implementação e multas até maio de 2020. Journal of Information Policy, 11(1):63–103, 2021.

[251] N. Woolf. O ataque DDoS que interrompeu a Internet foi o maior desse tipo na história, Especialistas dizem. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet , outubro de 2016. [Acessado em 07 de novembro de 2022].

[252] O. Yoachimik. https://blog.cloudflare.com/mantis-botnet/, 2022.

[253] K. Yskout, T. Heyman, D. Van Landuyt, L. Sion, K. Wuyts e W. Joosen. Modelagem de ameaças: da infância à maturidade. Nos Anais da 42ª Conferência Internacional ACM/IEEE sobre Engenharia de Software: Novas Idéias e Resultados Emergentes, páginas 9–12. ACM, junho de 2020.

[254] K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, AK Bashir e FA Khan. Protegendo infraestruturas críticas: Detecção de ameaças baseada em aprendizagem profunda em iot. Revista IEEE Communications, 59(10):76–82, 2021.

[255] F. Zhang, PPK Chan, B. Biggio, DS Yeung e F. Roli. Seleção de recursos adversários contra ataques de evasão. Transações IEEE sobre Cibernética, 46(3):766–777, 2016.

[256] E. Zio. Desafios na análise de vulnerabilidade e risco de infraestruturas críticas. Confiança- Engenharia de bilidade e segurança de sistemas, 152:137–150, 2016.

Cyber Security for Europe

Acordo de subvenção do Programa Horizonte 2020 n.º 830929

A CyberSec4Europe está a conceber, testar e demonstrar potenciais estruturas de governação para uma futura Rede Europeia de Competências em Cibersegurança, utilizando exemplos de melhores práticas derivados de conceitos como o CERN, bem como os conhecimentos e a experiência dos parceiros. Os 43 parceiros da CyberSec4Europe, de 22 Estados-Membros da UE e países associados, abordam domínios-chave de cibersegurança, elementos críticos de tecnologia/aplicação e vários setores verticais importantes, incluindo finanças, educação, cidades inteligentes, cuidados de saúde, cadeia de a

hps://cybersec4europe.eu

Fundado por
a União Europeia