



Segurança da Informação: o que é preciso saber

Gerson Luiz Camillo
Prof. cursos ENC e TIC
Abril 2023

TECH

A full federal appeals court will rehear a legal challenge to whether charges against former Trump national security adviser Michael Flynn must be dropped

Widespread Twitter Hack Reaches Bill Gates, Kanye West, Elon Musk, Joe Biden and Barack Obama

Personal accounts of famous users, tech companies and cryptocurrency exchanges steer followers to send money



RECOMMENDED VIDEOS

1. In Miami, Long Lines for Covid-19 Tests Frustrate Residents
2. Amazon, Google, Apple, and Facebook CEOs Make Opening Statements
3. Can Wearables Detect Covid-19 Symptoms? I Wore Six to Find Out
4. NASA's Perseverance Rover Rockets Toward Mars
5. Vietnam's First Coronavirus Cases in Months Highlight Global Challenges



Estamos prontos para atualizar seu PC.

Analise a lista de atualizações abaixo e clique em [Histórico](#).

Selecionar todos

Atualizações importantes:

Intel Rapid Storage Technology Driver

Dell Inspiron 5490/5498/5590/5598 and Vostro 5490/5590

SupportAssist OS Recovery Tools

Atualização(ões) recomendada(s)

Dell SupportAssist OS Recovery Plugin for Dell Upda

Detalhes do driver

Dell Inspiron 5490/5498/5590/5598 and Vostro 5490/5590 System BIOS

This package contains the Dell system BIOS update. BIOS is a firmware package that is embedded on a small memory chip on the system board. It controls the keyboard, monitor, disk drives, and other devices. This update addresses Common Vulnerabilities and Exposures (CVE). Common Vulnerabilities and Exposures (CVE) is a list of security vulnerabilities and exposures that are publicly disclosed.

Versão: 1.22.0

Categoria: BIOS

Data da versão: February 10, 2023

Última atualização:

Importância: Urgent

Formato do arquivo:

Nome do arquivo: Inspiron_5490_5498_5590_5598_Vostro_5490_5590_1.22.0.exe

Tamanho do arquivo: 13,82 MB

Fechar



Estamos prontos para atualizar seu PC.

Analisar a lista de atualizações abaixo e clique em [Histórico](#).

Selecionar todos

Atualizações importantes:

Intel Rapid Storage Technology Driver

Dell Inspiron 5490/5498/5590/5598 and Vostro 5490/5590

SupportAssist OS Recovery Tools

Atualização(ões) recomendada(s)

Dell SupportAssist OS Recovery Plugin for Dell Upda

Detalhes do driver

Dell Inspiron 5490/5498/5590/5598 and Vostro 5490/5590 System BIOS

This package contains the Dell system BIOS update. BIOS is a firmware package that is embedded on a small memory chip on the system board. It controls the keyboard, monitor, disk drives, and other devices. This update addresses Common Vulnerabilities and Exposures (CVE). Common Vulnerabilities and Exposures (CVE) is a list of security vulnerabilities and exposures that are publicly disclosed.

Versão: 1.22.0

Categoria: BIOS

Data da versão: February 10, 2023

Última atualização:

Importância: Urgent

Formato do arquivo:

Nome do arquivo: Inspiron_5490_5498_5590_5598_Vostro_5490_5590_1.22.0.exe

Tamanho do arquivo: 13,82 MB

Fechar

```
$ cat /proc/cpuinfo
```

```
processor: 0
```

```
vendor_id: GenuineIntel
```

```
cpu family : 6
```

```
model : 142
```

```
model name : Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz
```

```
stepping : 9
```

```
microcode : 0x0
```

```
cpu MHz : 800.003
```

```
cache size : 4096 KB
```

```
physical id : 0
```

```
siblings : 4
```

```
core id : 0
```

```
cpu cores : 2
```

```
apicid : 0
```

```
initial apicid : 0
```

```
fpu : yes
```

```
fpu_exception : yes
```

```
cpuid level : 22
```

```
wp : yes
```

```
flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe  
syscall nx pdpe1gb rdtscp lm constant_tsc art arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc cpuid aperfmpf perf_pni pclmulqdq  
dtes64 monitor ds_cpl vmx est tm2 ssse3 sdbg fma cx16 xtrp pdcm pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave  
avx f16c rdrand lahf_lm abm 3dnowprefetch cpuid_fault epb invpcid_single pti ssbd ibrs ibpb stibp tpr_shadow vnmi flexpriority ept vpid  
ept_ad fsgsbase tsc_adjust bmi1 avx2 smep bmi2 erms invpcid mpx rdseed adx smap clflushopt intel_pt xsaveopt xsavexc xgetbv1 xsaves  
dtherm ida arat pln pts hwp hwp_notify hwp_act_window hwp_epp md_clear flush_l1d arch_capabilities
```

```
bugs :
```

```
cpu_meltdown
```

```
spectre_v1
```

```
spectre_v2
```

```
spec_store_bypass
```

```
l1tf
```

```
mds
```

```
swaps
```

```
itlb_multihit
```

```
srbds
```

```
mmio_stale_data
```

```
retbleed
```



Lierre Bourguignon C. Jr • 3º e +

Chief Security Officer (CSO) @ ISH Tecnologia | CISO | Keyno...

3 sem • Editado •

+ Seguir ...

Na minha semana sempre tem uma ligação de desespero de alguém que foi ou está sendo invadido, e quer saber o que fazer. Então dando sequência a série de artigos que havia prometido, segue o segundo: O que fazer DURANTE um ataque.

Neste material que faz parte de uma série, você vai encontrar os 10 grandes passos a qual deve ser seguido religiosamente durante um ataque:

- 1) Isolar os sistemas afetados;
- 2) Preservar a garantir que seu backup esteja funcional;
- 3) Identificar a ameaça e ponto de entrada;
- 4) Identificar os sistemas afetados;
- 5) Definição de hipóteses para resolução do incidente;
- 6) Mitigar a ameaça;
- 7) Restaurar os sistemas afetados;
- 8) Hardening do ambiente;
- 9) Migrando o ambiente para produção;
- 10) Lições aprendidas e correções definitivas;

Em geral um ambiente impactado por um ransomware demora em média cerca de 8 semanas para voltar a sua normalidade, este documento vai te ajudar a transformar este tempo em 15 dias.

Lembre-se! O ideal é que você tenha executado as ações presentes no artigo - O que fazer ANTES de um ataque, a qual publiquei no início deste ano. As ações presentes neste artigo, vão te ajudar evitar a chegar neste momento.

Ah! Como sempre meu intuito aqui compartilhar um pouco da minha experiência e do time de DFIR (Digital Forensics and Incident Response) do SOC da **ISH Tecnologia**, então curta, comente e compartilhe com todos.

#ransomware #evento #ishtecnologia #cibersegurança

#segurançadainformação #ishtecnologia

#empresasegura #ciberataques #ataqueshacker #dadospessoais

#proteçãodedados #vazamento #digital #ciberataque

Ataque de **ransomware**
Tempo médio para voltar à normalidade:
8 semanas ~ 15 dias (com métodos adequados)



Fonte: <https://www.linkedin.com/feed/update/urn:li:activity:7046099678118952960/>

Sumário

- Conceituações
- Introdução à LGPD
- Princípios em segurança
- Medidas de segurança

Segurança da Informação

Termos e Definições

Definição de segurança

Diz-se que um programa é **correto** quando satisfaz os requisitos.

Um sistema é seguro se as propriedades de segurança permanecem preservadas em face de ataques

Postura de segurança

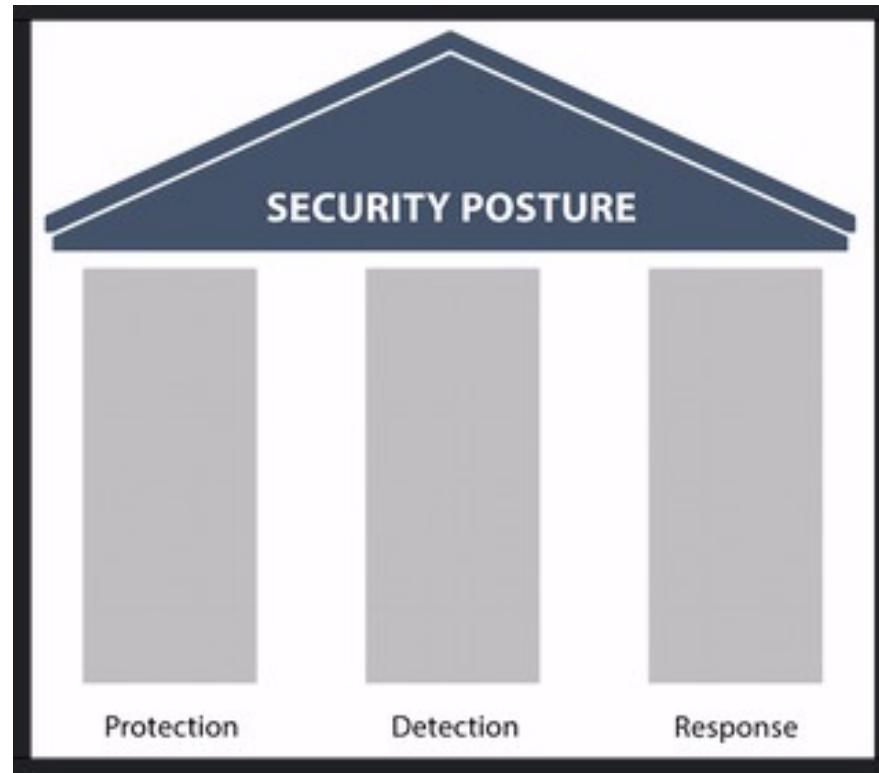
Definição conforme o NIST.gov

“É o status de segurança das redes, informações e sistemas de uma empresa com base nos **recursos** de segurança da informação (p.ex., **pessoas, hardware, software, políticas**) e capacidades existentes para gerenciar a defesa da empresa e reagir conforme a situação muda.”

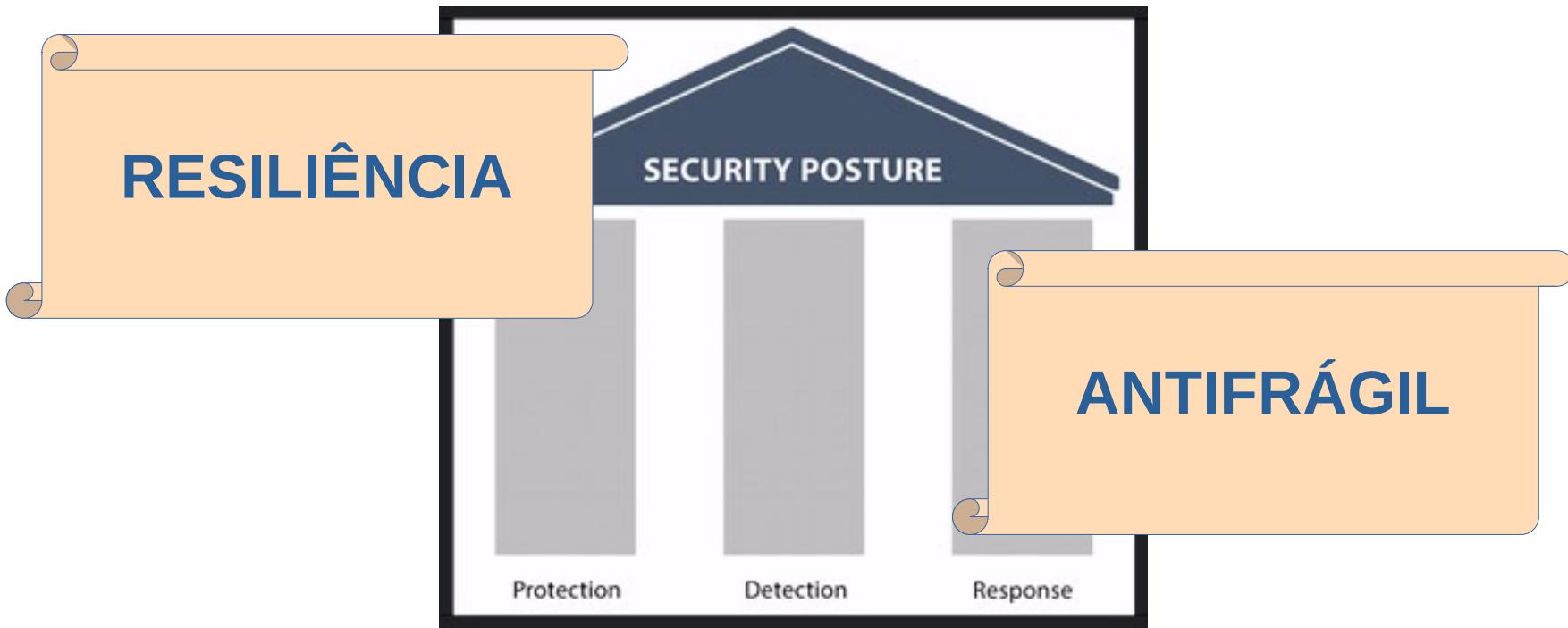
Fonte: https://csrc.nist.gov/glossary/term/security_posture

Postura de segurança

Três estratégias
para segurança
igualmente
importantes



Postura de segurança



TSA Requires Aviation Sector to Enhance Cybersecurity Resilience

TSA instructs airport and aircraft operators to improve their cybersecurity resilience and prevent infrastructure disruption and degradation.



By [Eduard Kovacs](#)
March 8, 2023



TRENDING

- 1 Google Patches Second Chrome Zero-Day Vulnerability of 2023
- 2 VMware Patches Pre-Auth Code Execution Flaw in Logging Product
- 3 Capita Confirms Data Breach After Ransomware Group Offers to Sell Stolen Information

Fonte: <https://www.securityweek.com/tsa-requires-aviation-sector-to-enhance-cybersecurity-resilience/>

Postura de segurança

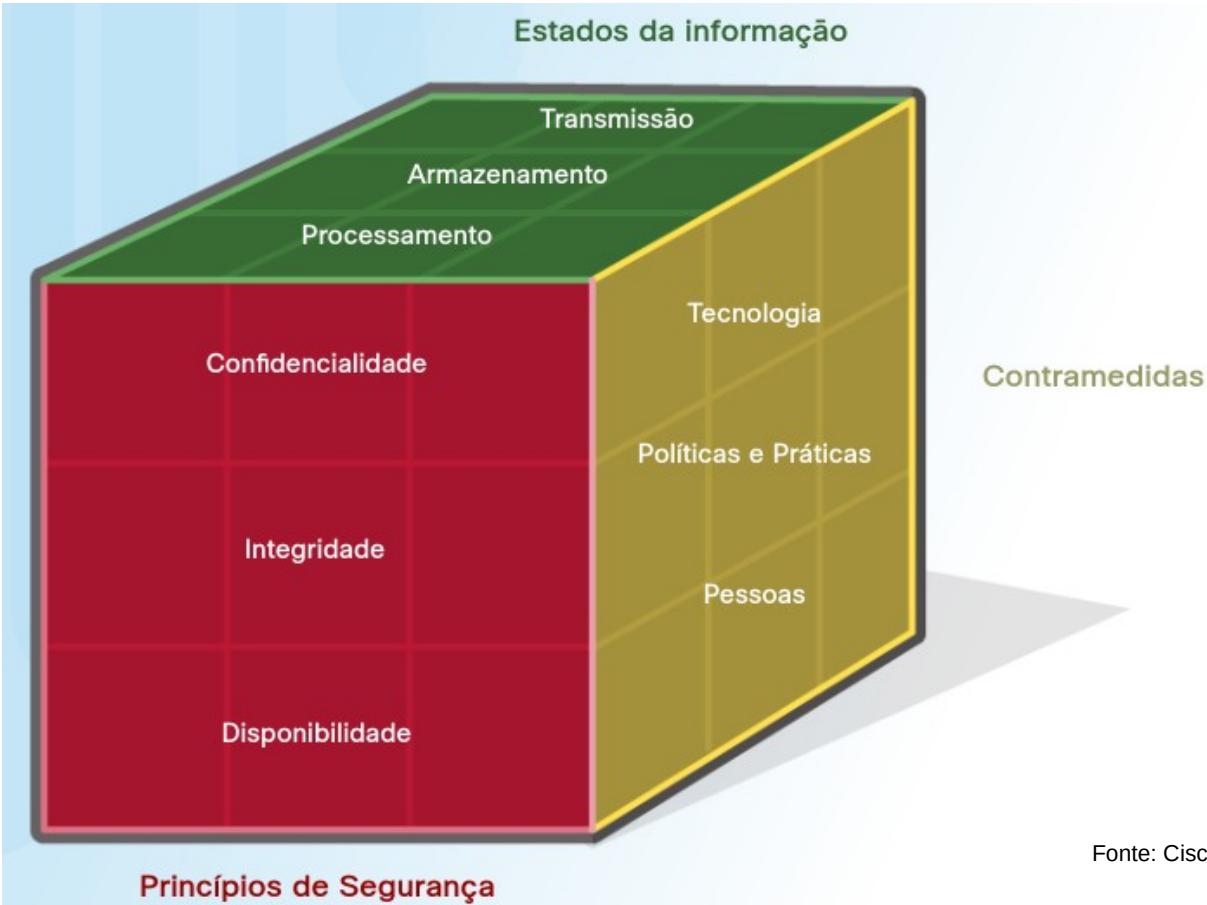
Prevenção (proteção) implementação de mecanismos de segurança: autenticação, autorização, etc.

Detecção quando um ataque não pode ser prevenido, mas pode ser monitorado para prover dados de sua natureza, severidade e resultados.

Recuperação (resposta):

- parar o ataque
- salvar evidências
- recuperar dados
- assumir violação
- executar plano de remediação + medidas (p.ex., correção das vulnerabilidades)

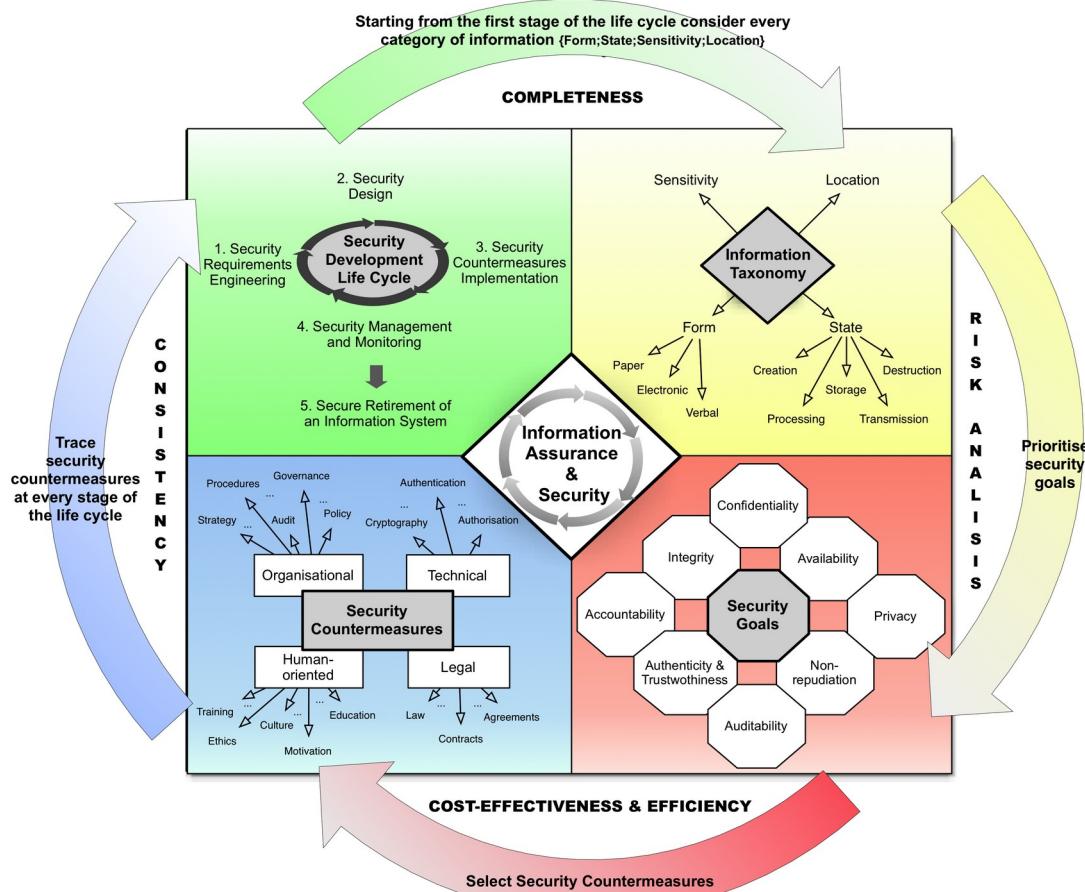
Cubo da cibersegurança



Fonte: Cisco (curso de cibersegurança)

A Reference Model of Information Assurance & Security (RMIAS)

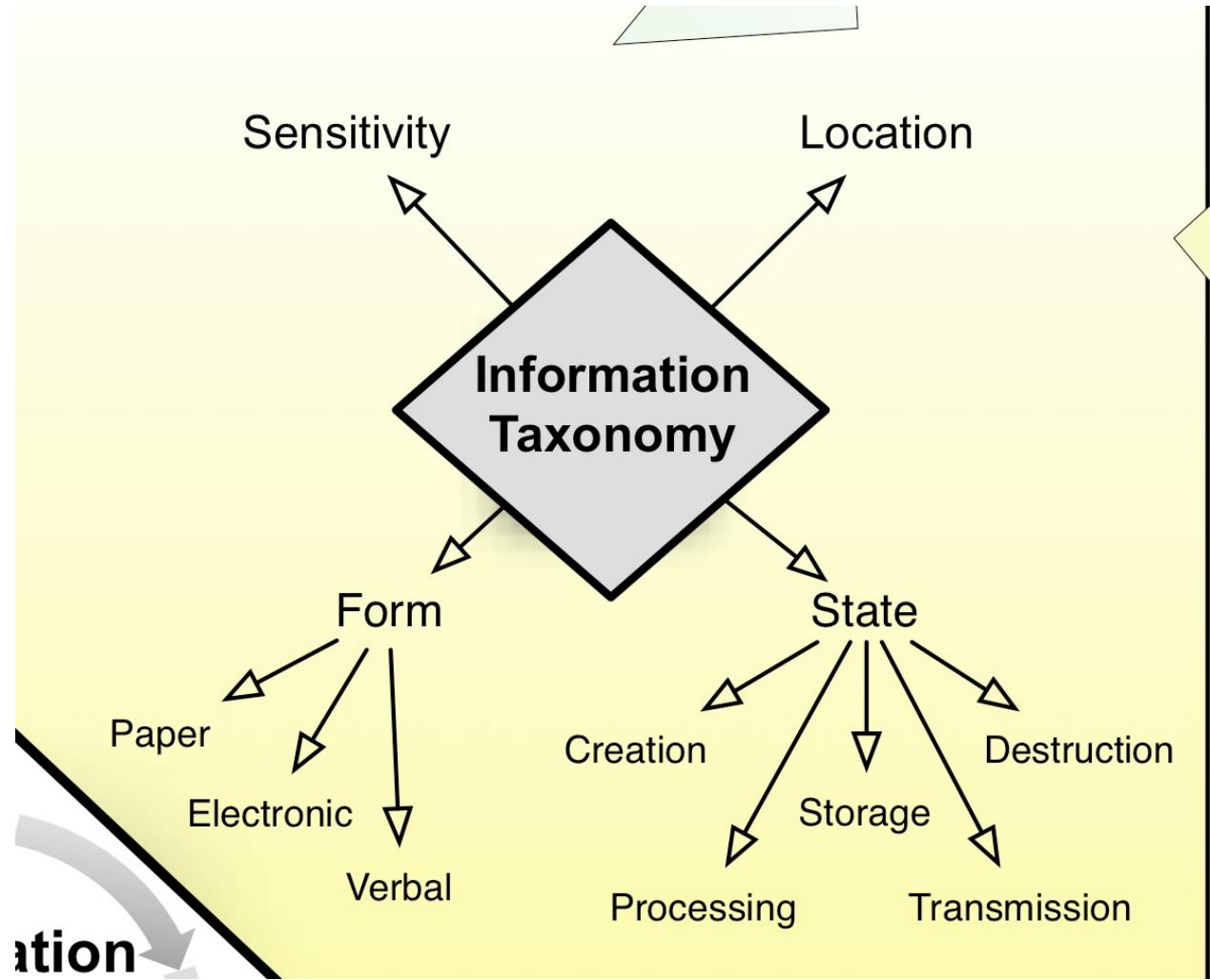
Y. Cherdantseva and J. Hilton

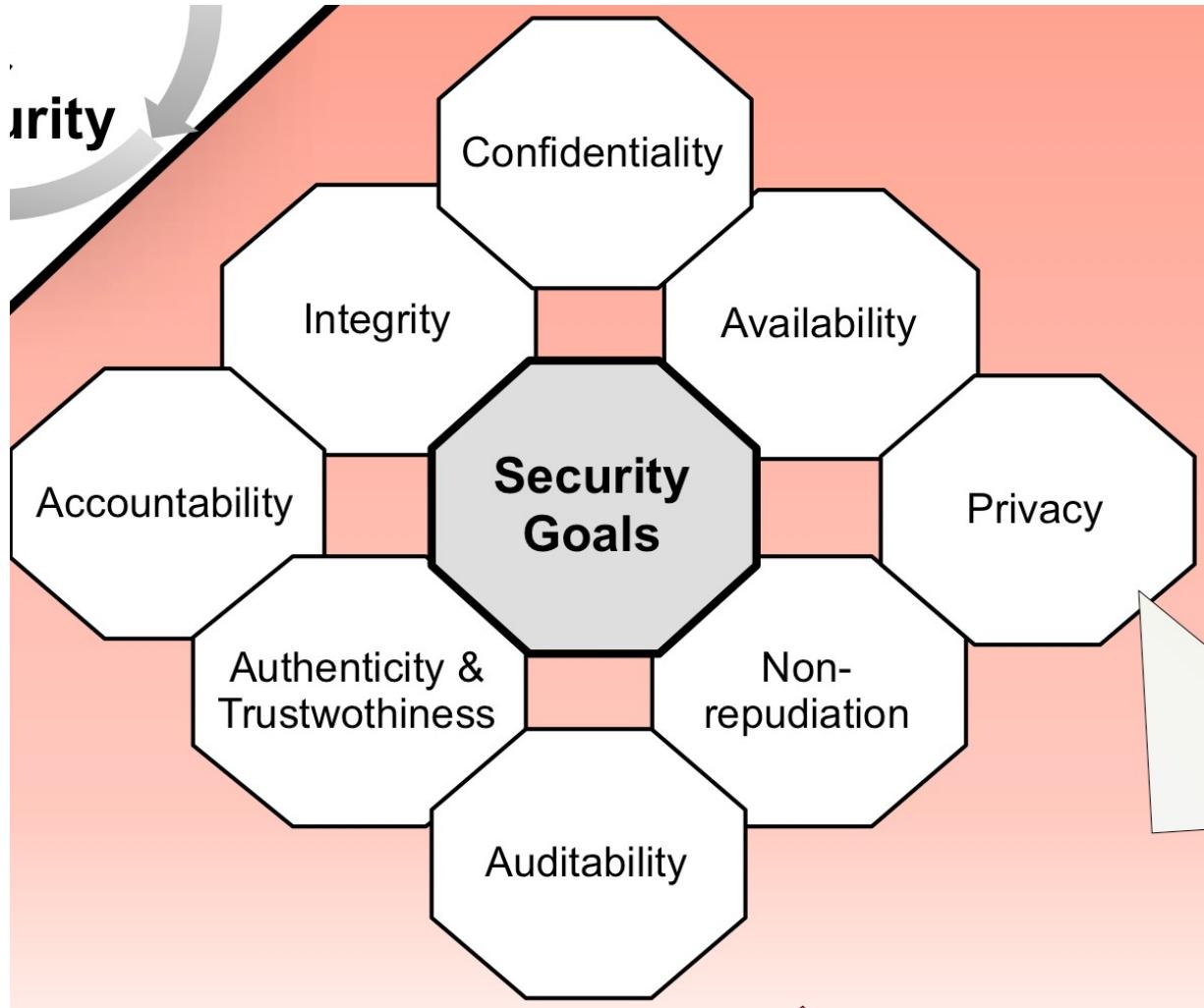


- Ciclo de vida da segurança dos sistemas de informação
- Taxonomia em informação
- Objetivos de segurança
- Contramedidas em segurança

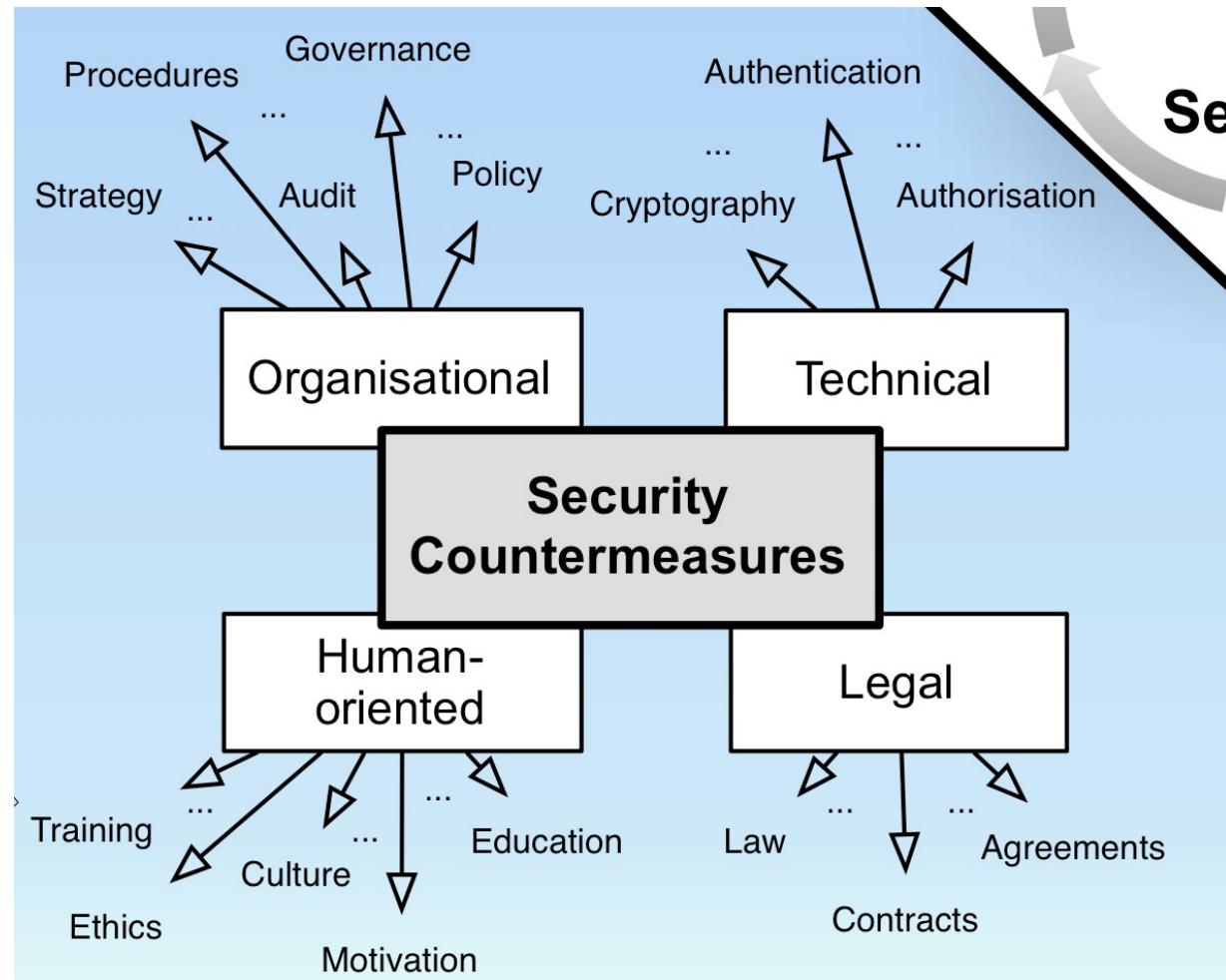
<https://rmias.cs.cf.ac.uk/>

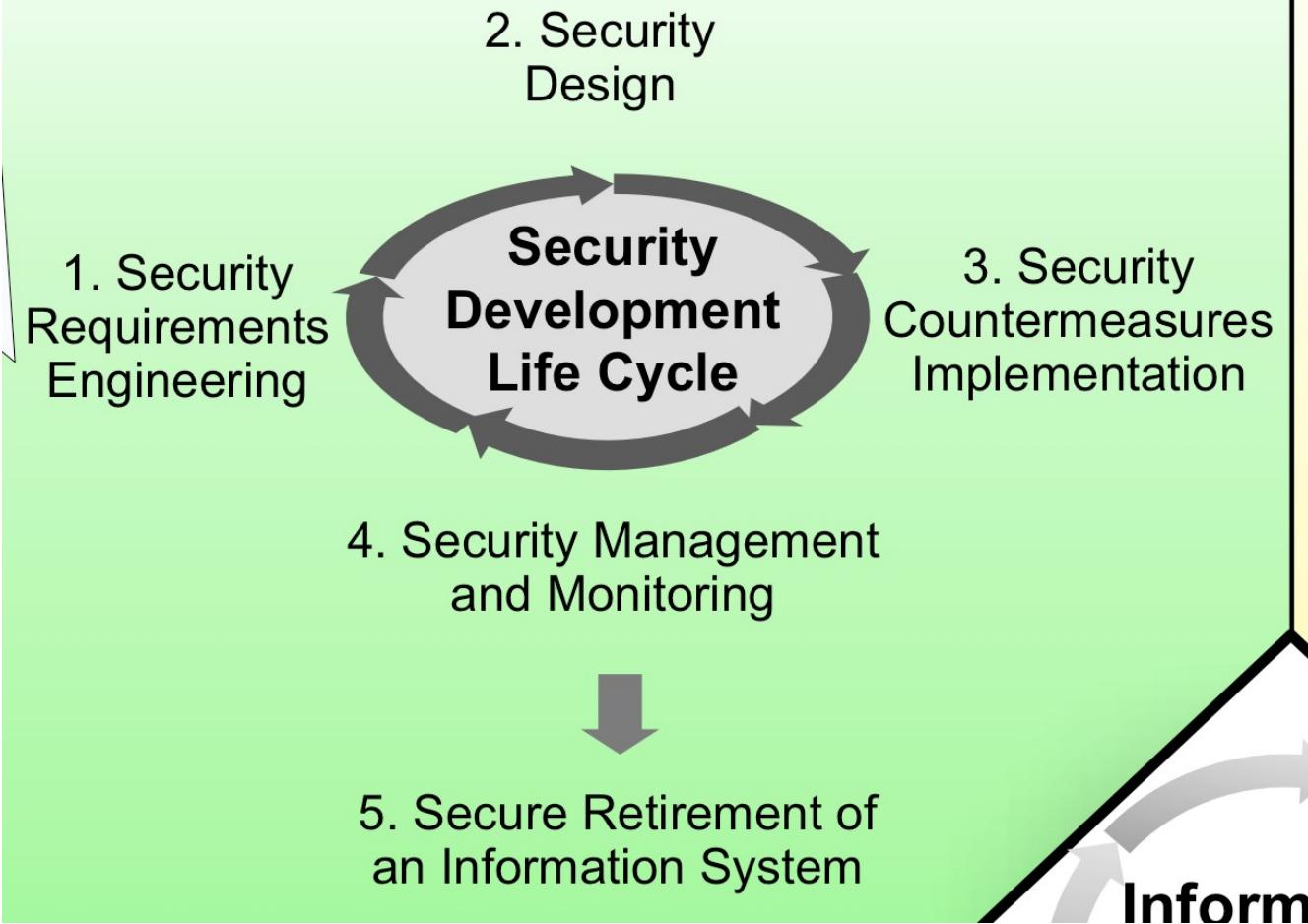
Cherdantseva Y. and Hilton J. "A Reference Model of Information Assurance & Security," Accepted to SecOnt 2013 workshop which will be held in conjunction with the 8th International Conference on Availability, Reliability and Security (ARES) 2013, University of Regensburg, Germany. September 2nd - 6th, 2013.





urity



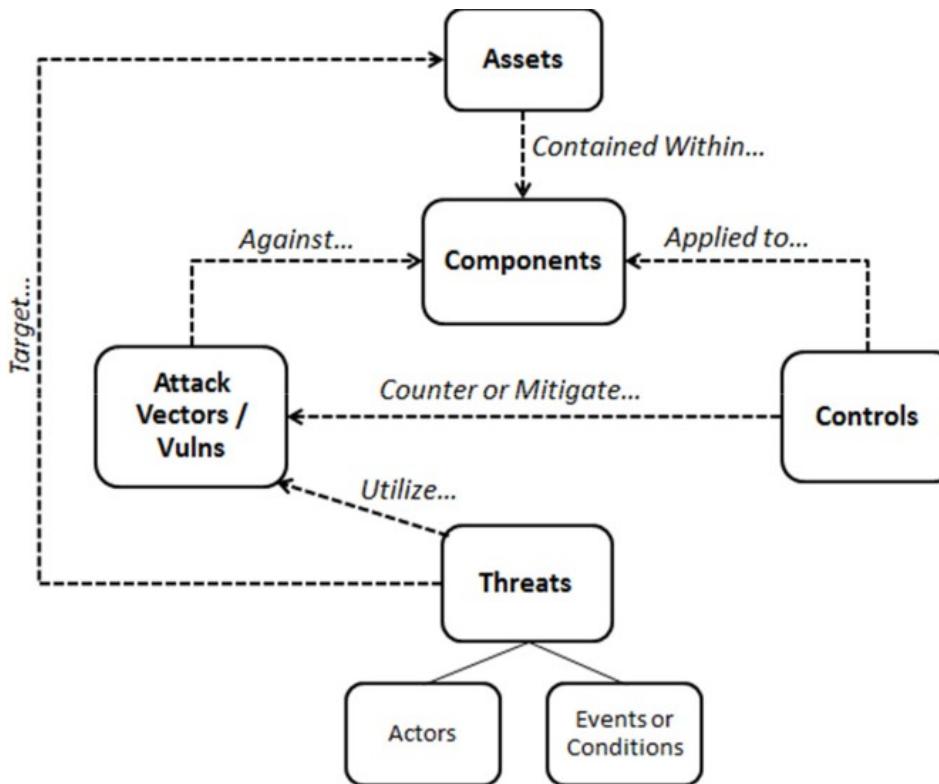


Segurança da Informação (dados)

Garantia de que a informação ou dados que estão sendo acessados são válidos. Mecanismos de integridade devem garantidos. **Ausência de modificações não-autorizadas** implica:

- Que o sistema **identifica e autentica** o usuário/entidade e **registre** a informação de acesso;
- Que o sistema possua **mecanismos de checagem das permissões** das entidade nos eventos de acesso aos objetos e que os mesmos sejam registrados; e
- Que o sistema possua mecanismos de **rastreamento (*logging*)** em nível alto de confiabilidade.
- Então para uma **informação íntegra**, há necessidade de autenticar um usuário e checar seus níveis de autorização e para todo acesso e fazer um registro (log) para auditoria futura.

Segurança da Informação



Política: LGPD

GDPR: General Data Protection Regulation (2018) – EU

**Consentimento
Acesso
Minimização**

Para dados de cidadãos europeus,
independentemente do lugar onde
estejam sendo processados.



LGPD: Lei n. 13.709/2018

Lei Geral de Proteção de Dados Pessoais

Sancionada: ago 2018. Vigência: ago 2020

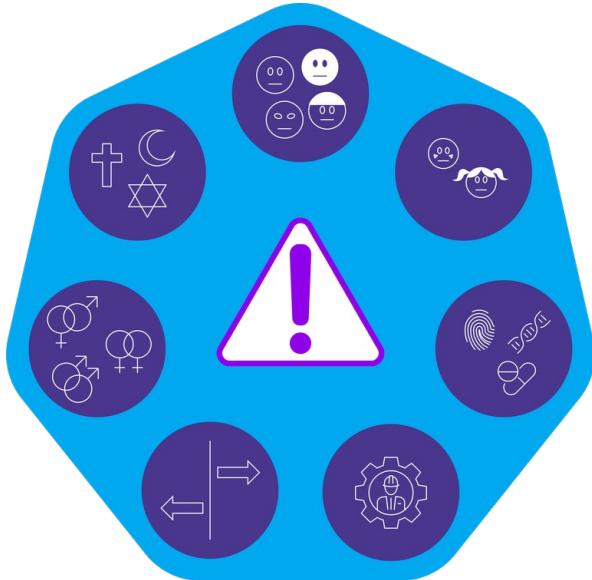
LGPD - Lei Geral de Proteção de Dados Pessoais

Dados Pessoais

Uma informação permite identificar, direta ou indiretamente, um indivíduo que esteja vivo

Dados Anonimizados

Dados Pessoais Sensíveis



LGPD - Lei Geral de Proteção de Dados Pessoais

Princípios

- 01 **Finalidade** especificada e informada explicitamente ao titular
- 02 **Adequação** à finalidade previamente acordada e divulgada
- 03 **Necessidade** do tratamento, limitado ao uso de dados essenciais para alcançar a finalidade inicial
- 04 **Acesso livre**, fácil e gratuito das pessoas à forma como seus dados são tratados
- 05 **Qualidade dos dados**, deixando-os exatos e atualizados, segundo a real necessidade no tratamento
- 06 **Transparência**, ao titular, com informações claras e acessíveis sobre o tratamento e seus responsáveis
- 07 **Segurança** para coibir situações acidentais ou ilícitas como invasão, destruição, perda, difusão
- 08 **Prevenção** contra danos ao titular e a demais envolvidos
- 09 **Não discriminação**, ou seja, não permitir atos ilícitos ou abusivos
- 10 **Responsabilização** do agente, obrigado a demonstrar a eficácia das medidas adotadas

LGPD - Lei Geral de Proteção de Dados Pessoais

Bases Legais para Tratamento de Dados Pessoais



Fonte: obtido de <https://globalgcs.com.br/blog/bases-legais-lgpd/>

Princípios de segurança e princípios de projeto seguro

Fontes: Bishop (2019, p. 457) e Saltzer e Schroeder (1978)

Segurança é economia

Nenhum sistema é 100% contra todos os ataques. Sistemas devem resistir a um determinado nível de ataque.

Adi Shamir: “*There are no secure systems, only degrees of insecurity*”

Segurança no enlace mais fraco.

Segurança é economia

Nenhum sistema é 100% contra todos os ataques. Sistemas devem resistir a um determinado nível de ataque.

Adi Shamir: "There are no secure systems, only degrees of insecurity"

Segurança no enlace mais fraco.

The New York Times

Cyberattack Forces a Shutdown of a Top U.S. Pipeline

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.



What is the Colonial Pipeline hack?

The Colonial Pipeline hack is the largest publicly disclosed cyber attack against critical infrastructure in the U.S.

Fonte: obtido de <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know>

Schneier on Security

Blog Newsletter Books Essays News Talks

[Home](#) > [Blog](#)

Ransomware Shuts Down US Pipeline

This is a [major story](#): a probably Russian cybercrime group called DarkSide shut down the Colonial Pipeline in a ransomware attack. The pipeline supplies much of the East Coast. This is the new and improved ransomware attack: the hackers [stole](#) nearly 100 gig of data, and are threatening to publish it. The White House has declared a [state of emergency](#) and has [created a task force](#) to deal with the problem, but it's unclear what they can do. This is bad; our supply chains are so tightly coupled that this kind of thing can have disproportionate effects.

EDITED TO ADD (5/12): It seems that the [billing system](#) was attacked, and not the physical pipeline itself.

Segurança é economia

Nenhum sistema é 100% contra todos os ataques. Sistemas devem resistir a um determinado nível de ataque.

Adi Shamir: “*There are no secure systems, only degrees of insecurity*”

Segurança no enlace mais fraco.

TECH / SECURITY

Hackers reportedly used a compromised password in Colonial Pipeline cyberattack

The VPN apparently didn't use multi-factor authentication



By KIM LYONS / @socialkimly

Jun 5, 2021, 4:18 PM UTC | 0 Comments

Segurança é economia

Segurança no enlace mais fraco

O que pode dar errado?

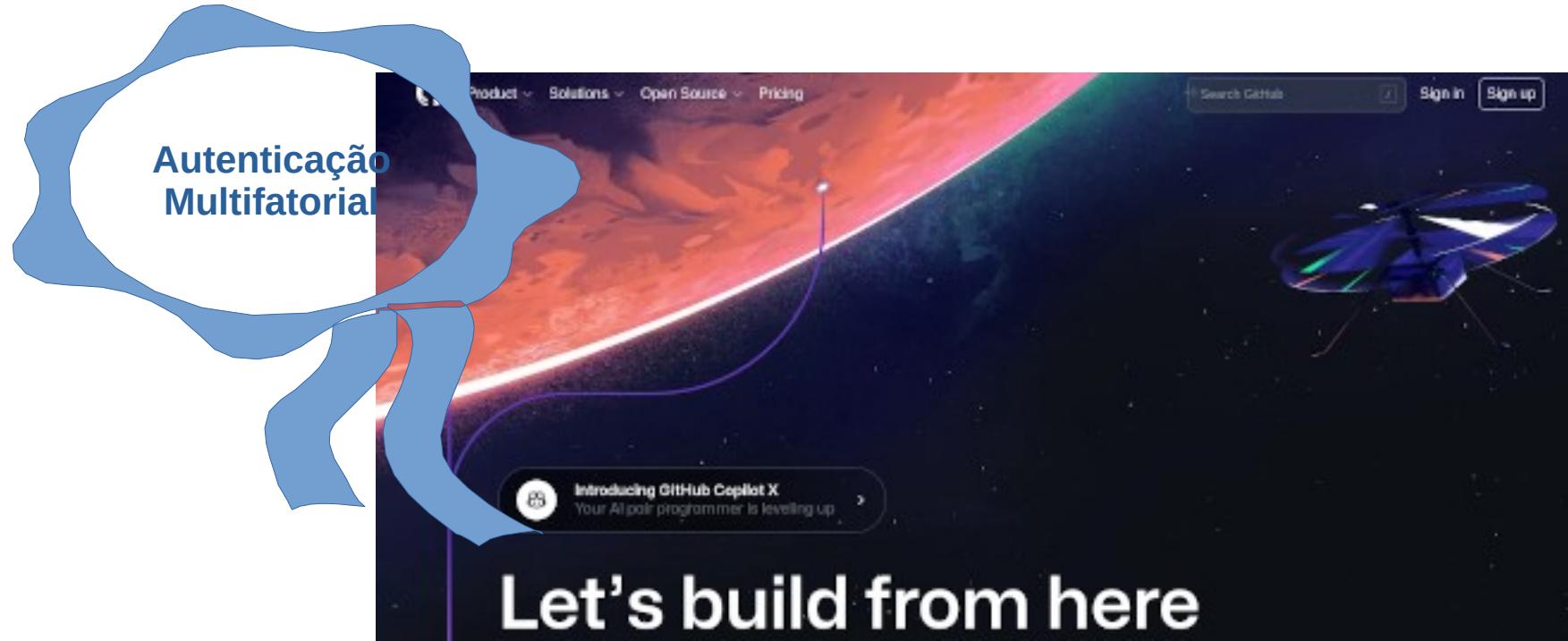
82%

of breaches involved the Human Element,
including Social Attacks, Errors and Misuse.

Fonte: relatório 2022
(<https://www.verizon.com/business/resources/reports/dbir/>)

Segurança é economia

Segurança no enlace mais fraco



Segurança é economia

Segurança no enlace mais fraco



Two-factor authentication

Enabled

Two-factor authentication adds an additional layer of security to your account by requiring more than just a password to sign in. [Learn more about two-factor authentication.](#)

Two-factor methods

- Authenticator app** Enabled Preferred Edit
Use an authentication app or browser extension to get two-factor authentication codes when prompted.
- SMS/Text message** Add
Get one-time codes sent to your phone via SMS to complete authentication requests.
- Security keys**
Security keys are hardware devices that generate one-time codes.
- Github Mobile**
Github Mobile can be used to sign in to your account.

 Microsoft Authenticator
Microsoft Corporation

Princípio do privilégio mínimo *(least privilege)*

- A um sujeito deve ser dada somente a autorização (privilégio) aos recursos de TI compatíveis com a função e responsabilidade de um indivíduo, e não super ou subautorizá-lo.
- Sistemas não costumam possuir granularidade suficiente para aplicar esse princípio precisamente.
- Questão da natureza humana.
- Exemplos de mecanismos para elevação de privilégios para realizar determinada tarefa no sistema: sudo e UAC.

Princípio do privilégio mínimo *(least privilege)*

Linux sudo
(superuser do)

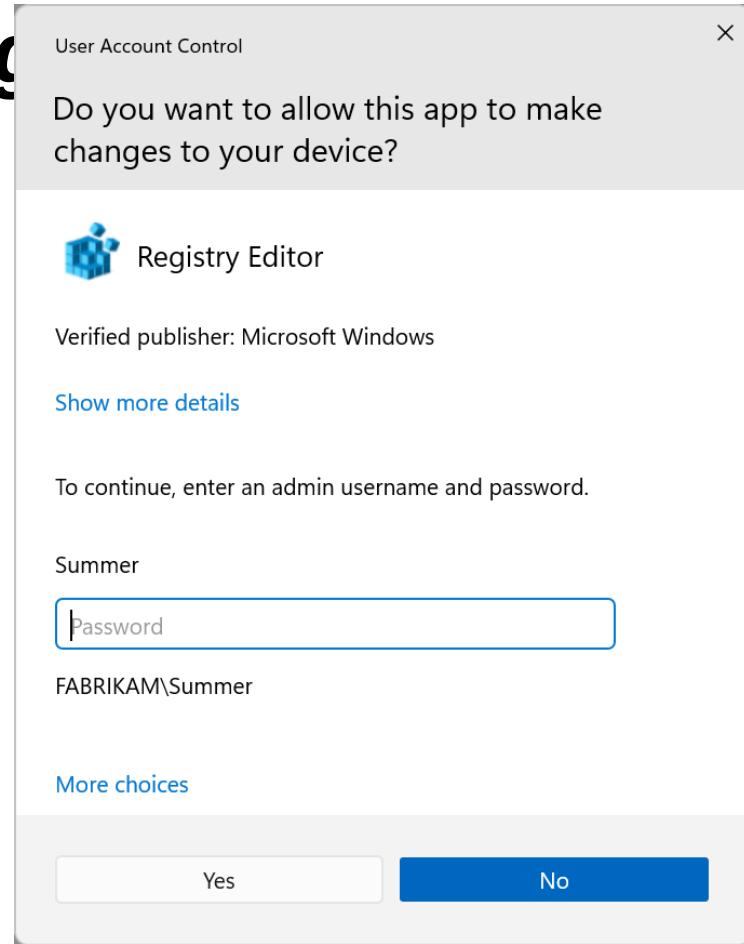
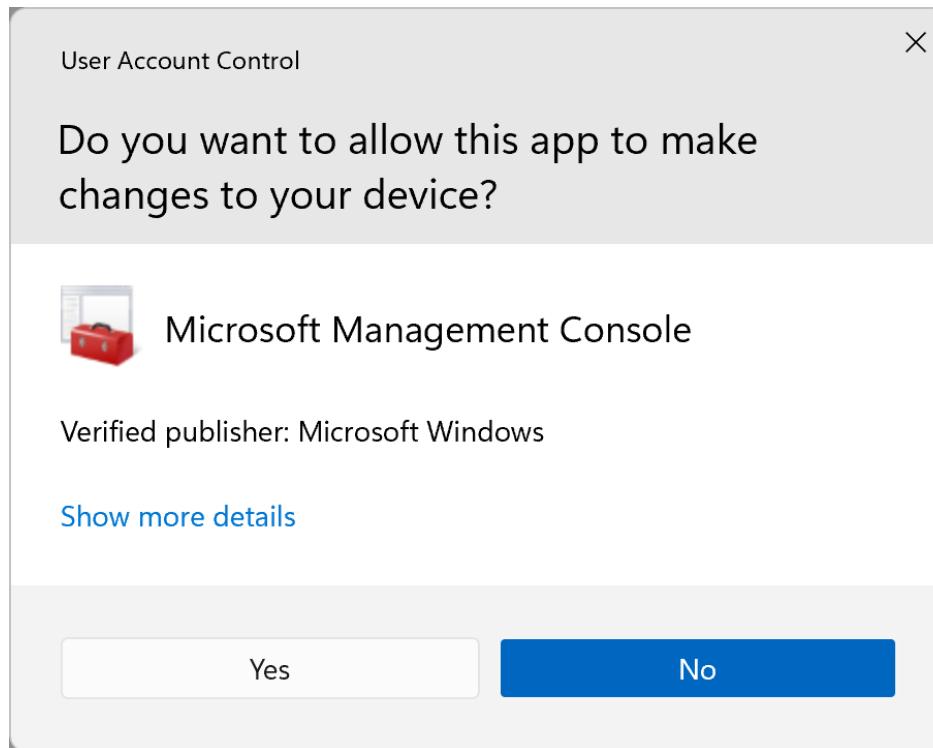


O que pode dar errado?
Bug CVE-2019-14287
Vulnerability CVE-2017-1000367

Princípio do privilégio mínimo *(least privilege)*

Windows UAC

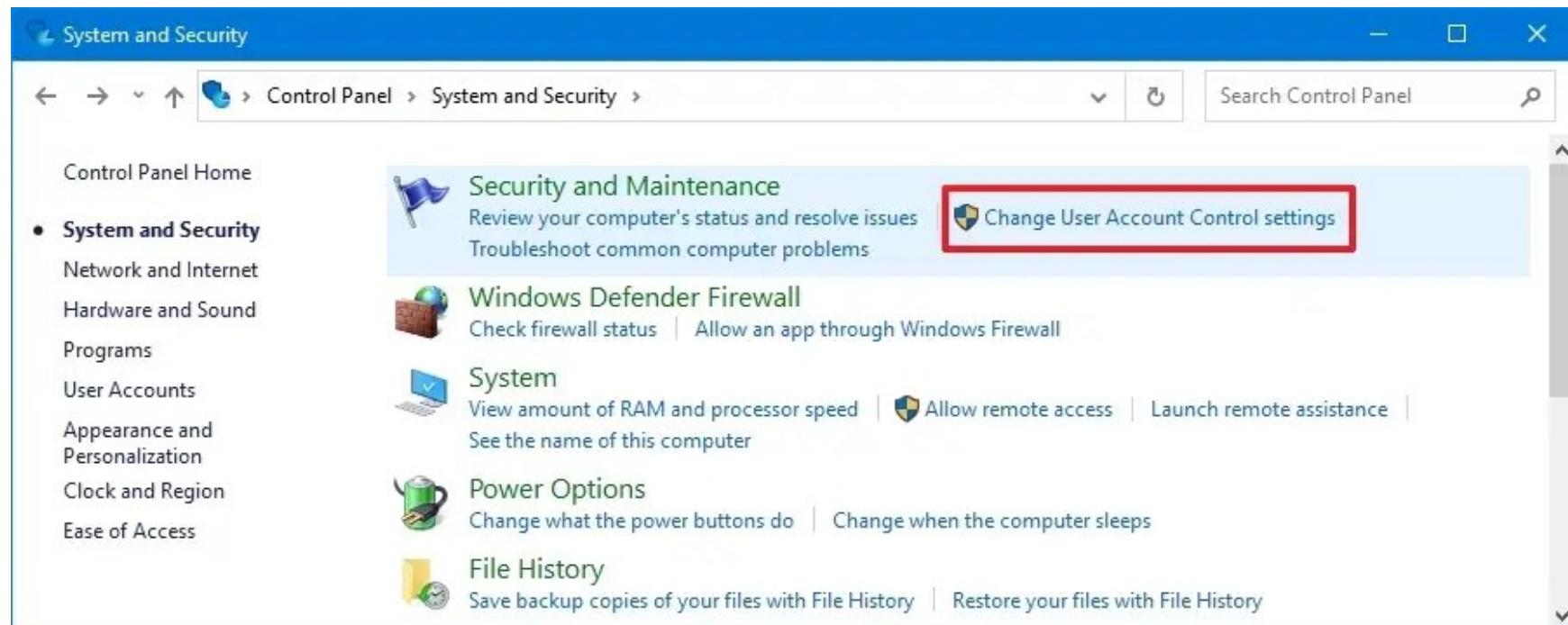
(User Account Control)



Princípio do privilégio mínimo *(least privilege)*

Windows UAC

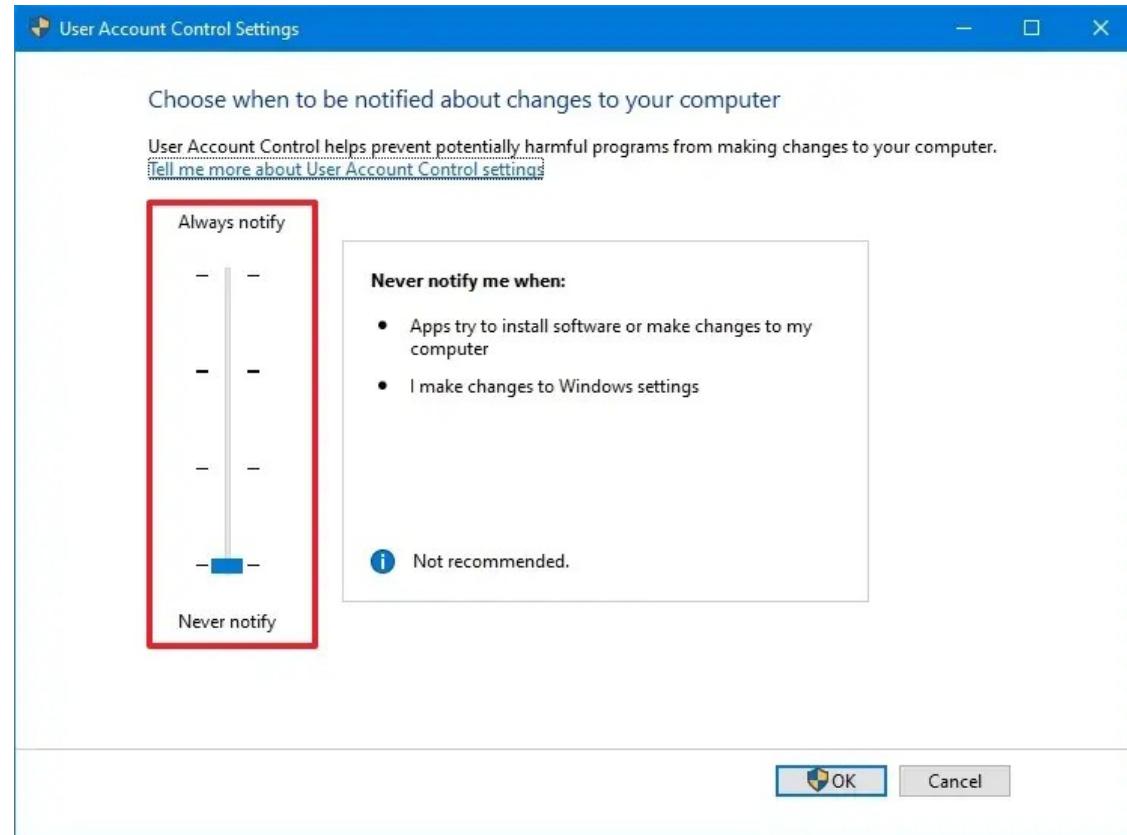
(User Account Control)



Princípio do privilégio mínimo (*least privilege*)

Windows UAC

(User Account Control)



Defesa em profundidade

Múltiplos sistemas de proteção (redundantes).

Segmentação rede: firewall; VLANs; IDS

Segmentação host: autenticação e autorização; proteção do endpoint

Aplicação/dados: firewall de aplicação; criptografia



Defesa em profundidade

Múltiplos sistemas de pr

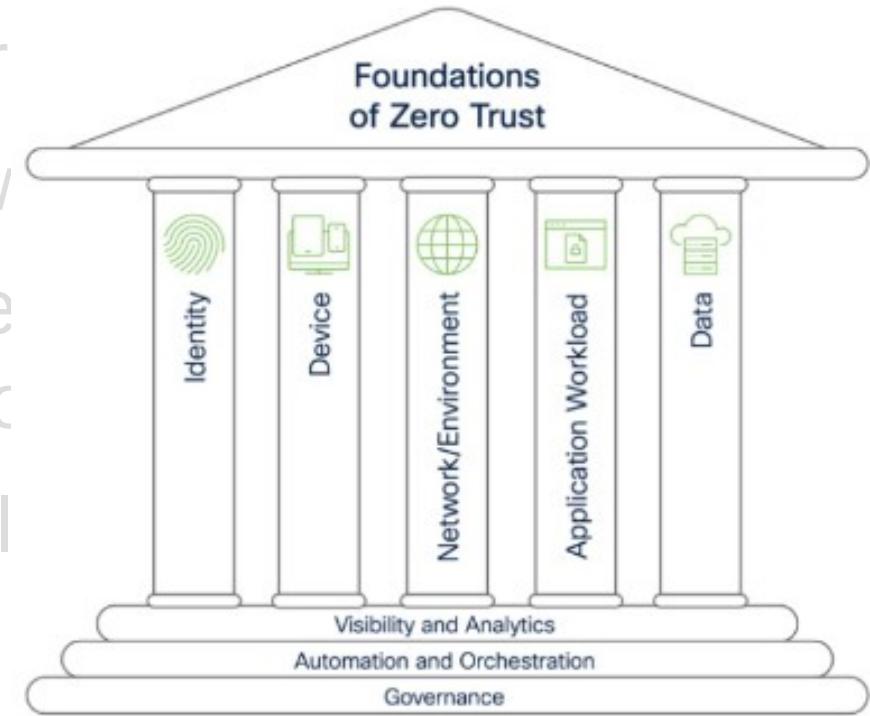
Segredos: firev

Segredos: autênci
autORIZAÇÃO, proteção dc

**Arquitetura/
Segurança
Zero Trust**

NIST: SP 800-207 Zero Trust Architecture
August 2020

<https://csrc.nist.gov/publications/detail/sp/800-207/final>

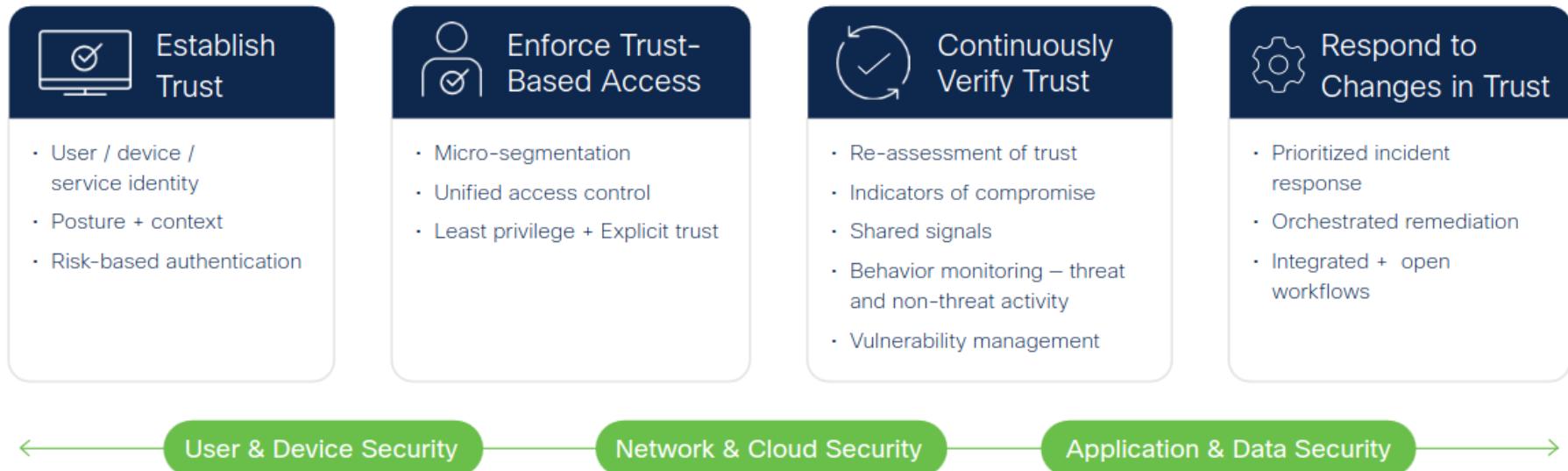


Fonte: extraído de <https://www.cisco.com/c/dam/en/us/products/collateral/security/trust-agent/zero-trust.pdf>

Defesa em profundidade

Arquitetura/Segurança Zero Trust

Cisco Zero Trust Capabilities



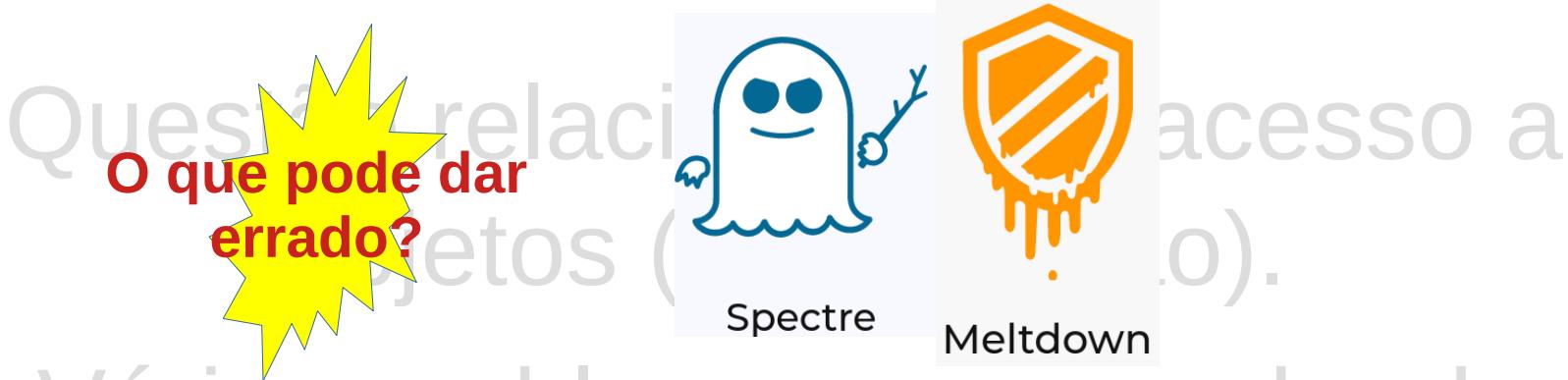
Fonte: extraído de <https://www.cisco.com/c/dam/en/us/products/collateral/security/trust-agent/zero-trust.pdf>

Princípio da mediação completa

Questão relacionada ao acesso a objetos (autorização).

Problemas com cache de informações de permissões.

Princípio da mediação completa



Meltdown and Spectre

Vulnerabilities in modern computers leak passwords and sensitive data.

O que pode dar errado? Ataques envenenamento de cache

Fontes

- [https://en.wikipedia.org/wiki/Spectre_\(security_vulnerability\)](https://en.wikipedia.org/wiki/Spectre_(security_vulnerability))
- <https://spectreattack.com/>
- <https://meltdownattack.com/>

Princípio da separação dos privilégios

- Separação de responsabilidades ou separação de tarefas (*separation of duties*): um sistema não deve conceder permissão baseada em uma única condição.
- Tarefas que precisam ser executadas em etapas e por diferentes usuário (com diferentes níveis de privilégio).
- Conceito de papéis (roles).

Princípio dos padrões à prova de falhas *(fail-safe defaults)*

A menos que um sujeito é dado um acesso explícito a um objeto, qualquer acesso deve ser bloqueado por padrão.

Estados de segurança: mesmo que um programa falhe, o sistema ainda continuará em estado seguro.

Princípio dos padrões à prova de falhas *(fail-safe defaults)*

A menos que
exp... a p...
**O que pode dar
errado?**

What was the software problem on the 737 Max?

It's been widely reported that Boeing's decision to use a flight control software fix known as MCAS in its 737 MAX planes was one of the key factors that led to two crashes that killed 346 people.

Boeing 737 Max, O que Deu ERRADO? - Ft. Lito Aviões e Músicas - PARTE 1



Aero Por Trás da Aviação 1.66M subscribers

Join

Subscribe

<https://www.youtube.com/watch?v=63E0VS55zt4>

Problemas em Segurança

e

Como encontrar informação

Fontes: sítios na internet

e

<https://glcamillo.github.io/aulas-ufsc-materiais/>

Problemas em segurança

Violação de rede ou dados



Interrupção da rede ou do sistema

Evento de ransomware

Ataque de DDoS

Divulgação acidental

Abuso mal-intencionado interno

Destruição física

Problemas em segurança

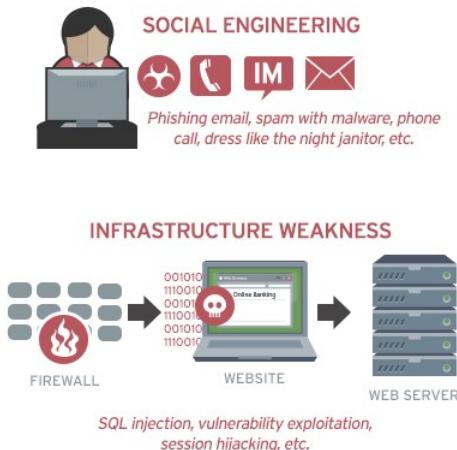
How Data Breaches Occur

1 Research



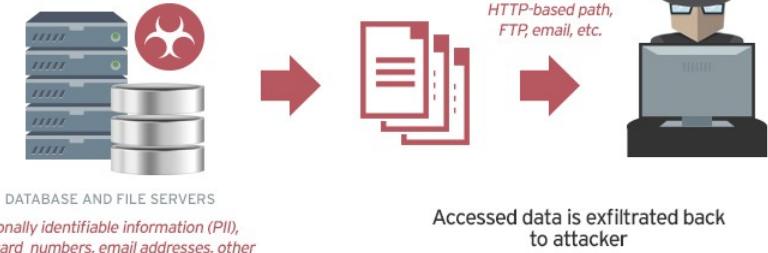
Attacker looks for weaknesses he can exploit

2 Stage Attack



Attacker may need to keep staging attacks until the desired information is obtained or the desired access to the network is achieved

3 Exfiltrate



Once the attacker maintains access to the system, exfiltration can indefinitely proceed

Problemas em segurança

Riscos do
Fator humano

70%

das fraudes estão
vinculadas à
engenharia social

Fonte: Febraban

Fontes

<https://gtergts.nic.br/files/apresentacao/arquivo/1491/05-Desafios-Conscientizacao.pdf>
e <https://portal.febraban.org.br/noticia/3522/pt-br/>

Problemas em segurança

Vulnerabilidades

“Uma fraqueza de um ativo ou grupo de ativos que pode ser explorado por uma ou mais ameaças.” (ISO 27002)

“A flaw in a software, firmware, hardware, or service component resulting from a weakness that can be exploited, causing a negative impact to the **confidentiality, integrity, or availability** of an impacted component or components.”

(<https://www.cve.org/ResourcesSupport/Glossary?activeTerm=glossaryVulnerability>)

CVE (Common Vulnerabilities and Exposures) e CVSS (Common Vulnerability Scoring System)

<https://cve.mitre.org/> <https://www.cve.org/> <https://nvd.nist.gov/>
<https://www.first.org/cvss/v3.1/specification-document>

Organizações envolvidas: MITRE, CVE, CISA e NIST
<https://www.mitre.org/> <https://www.cisa.gov/> <https://www.nist.gov/>

OSV (Open Source Vulnerability Database)

<https://osv.dev/> <https://osv.dev/list>

Atividade de descoberta vulnerabilidades

Atividade: descoberta de ativos e respectivas vulnerabilidades

Descoberta de ativos de rede

```
# nping -c 1 --icmp endereço_rede/prefixo Descobrir hosts na rede  
# nmap --script-updatedb Atualizar a base de scripts  
# nmap -v -ST IP Quais serviços estão ativos no destino  
# nmap -sV -A IP Info sobre serviços/portas; detecção OS, versão, script
```

Serviço SSH

```
# telnet IP 22  
# nmap -p 22 --script ssh2-enum-algos IP  
# ssh -v IP
```

Serviço HTTP na porta 80

```
# curl --head IP:porta  
# nmap -p 80 --script discovery IP  
# nmap -p 80 --script vuln IP
```

Atividade de descoberta vulnerabilidades

Scanning (descoberta vulnerabilidades) de serviço HTTP (PORTA=normalmente 80)

```
# whatweb IP:PORTA
# nikto -h IP:PORTA
# wapiti --update
# wapiti -u http://IP:PORTA -o
DIR_SAIDA
```

Problemas em segurança

OWASP Top 10

2021

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures*

A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

Fonte:
<https://owasp.org/Top10/>

Fonte: https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html

CWE (Common Weakness Enumeration)



Problemas em segurança



Weaponization do Log4j

[4] UNIT 42
RANSOMWARE THREAT
REPORT 2022

Fonte: extraído de <https://gtergts.nic.br/files/apresentacao/arquivo/1493/07-Detectao-agnostica-ransomware.pdf>

Atividade de análise arquivos

Atividade: dados três arquivos disponíveis no sítio a seguir, usar as ferramentas e sítios para analisar tipo e conteúdos dos mesmos. Finalidade: suspeita de malware.

Comandos de análise no Linux:

- \$ xxd -l 16 arquivo Mostra os bytes iniciais do arquivo em binário e hexadecimal
- \$ file arquivo Informa o tipo de arquivo
- \$ ldd arquivo Lista as bibliotecas que o programa chama (Linux)
- \$ strings arquivo Lista todos as strings encontradas no arquivo
- \$ objdump -d arquivo Ferramenta para obter o código assembly equivalente

<https://www.virustotal.com/gui/home/upload>

<https://hybrid-analysis.com>

<https://onlinedisassembler.com>

<https://github.com/glcamillo/aulas-ufsc-materiais/blob/gh-pages/run-a.exe>
<https://github.com/glcamillo/aulas-ufsc-materiais/blob/gh-pages/run-b>
<https://github.com/glcamillo/aulas-ufsc-materiais/blob/gh-pages/run-c.txt>

Problemas em segurança

2021

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures*
- A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

Fonte: <https://owasp.org/Top10/>

Criptografia e Protocolos Criptográficos

- Geração de números aleatórios sem usar CSPRNG (Cryptographic Secure PRNG);
- Funções com falhas em entropia (seed)
- Uso de funções de hashing descontinuadas (*deprecated*) como MD5 ou SHA1

Problemas em segurança

- Confused Deputy: mau uso da autoridade por programas; autoridade não é levada junto com objetos; “situação em que uma entidade não privilegiada invoca uma entidade privilegiada para realizar operações que violam a política de segurança” (GOLLMANN, 2011)
- Exemplos: CSRF e XSS (browser), Clickjacking (usuário), FTP bounce attack (servidor ftp)

Problemas em segurança

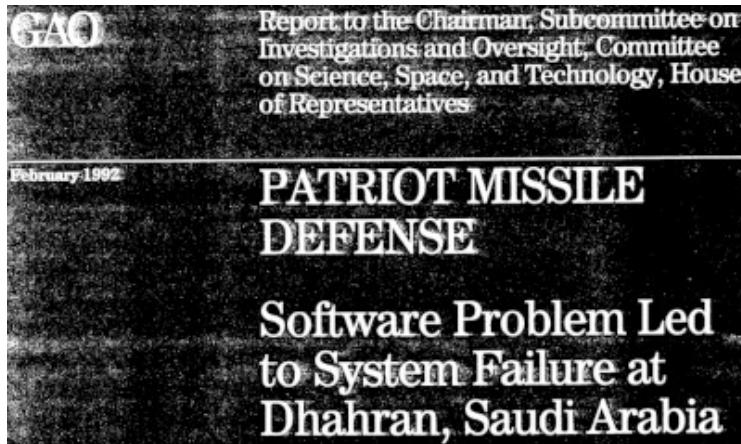
Dados misturados com código (DU, 2019a):

- heap: código + dados
- HTML + JavaScript

Buffer Overflow: das vulnerabilidades totais:
90% (~2000), 50% (2008)

Problemas em segurança

Código Seguro: aritmética de números inteiros e de ponto flutuante



**Problemas de
PRECISÃO e
representação
dados**

Descrição da falha: <https://www.cs.unc.edu/~smp/COMP205/LECTURES/ERROR/lec23/node4.html>

Problemas no Software

737 Max crashes: Boeing says not guilty to fraud charge

Fonte: extraído de <https://www.bbc.com/news/business-64390546> (2023)

⌚ 26 January

MONDAY, OCTOBER 28, 2019

Flawed Assumptions Pave a Path to Disaster

When MCAS (Maneuvering Characteristics Augmentation System) was implicated after Lion Air JT610 plunged into the sea, tragically taking 189 lives, the spotlights converged on the malfunction of a single Angle of Attack (AoA) vane. My first thoughts were that Boeing had somehow overlooked this scenario or viewed it as inconsequential, based on blind faith that no matter what, the pilot would remain vigilant taking correct and timely action as the safety backstop. I could not wrap my head on how repeated applications of MCAS did not create unlimited authority in malfunction which would create a HAZARDOUS hazard.

Fonte: extraído de <https://www.satcom.guru/2019/10/flawed-assumptions-pave-path-to-disaster.html>

Problemas no Software

Caso do Boeing 737 Max

- 1. Keep software and systems in complex machines as simple as possible, but not too simple.** Engineers call this the Goldilocks approach, when things are “just right.”
- 2. Don’t impose software on an intractable hardware problem.** MCAS didn’t fundamentally change the way the 737 MAX would fly. Keeping the engines further back on the wing would have.
- 3. Remember redundancy.** Do not rely on data readings from just one angle of attack sensor or any single data input.
- 4. Communicate with empathy.** Boeing executives and engineers seem to have failed on that point.

Problemas em segurança

Falhas e descuidos; má operação/configuração

A05:2021-Security Misconfiguration moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration, with an average incidence rate of 4.5%, and over 208k occurrences of CWEs mapped to this risk category. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for **A4:2017-XML External Entities (XXE)** is now part of this risk category.

Fonte: <https://owasp.org/Top10/>

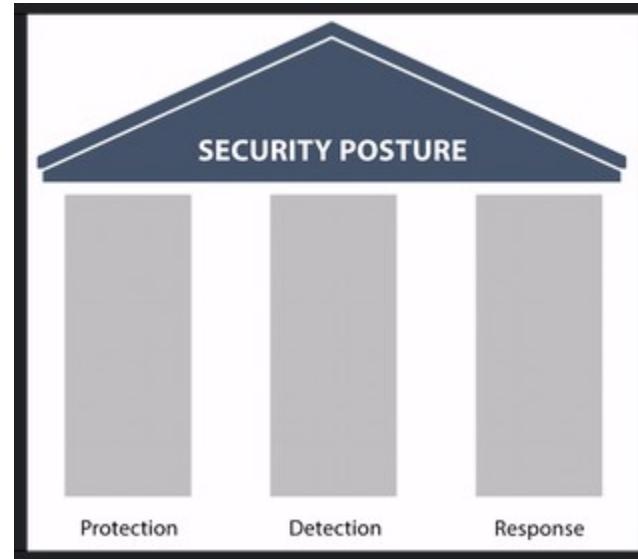
Incident Review - An Account Of The Telia Outage And Its Ripple Effect

Telia, a major backbone carrier in Europe, suffered from a network routing issue between 16:00 and 17:05 UTC. We investigate the BGP misconfiguration behind it.

Redmond elaborated on the root cause on January 27, saying the global outage was caused by a single router IP address change that led to packet forwarding issues between all other routers in its WAN. “As part of a planned change to update the IP address on a WAN router, a command given to the router caused it to send messages to all other routers in the WAN, which

Postura de segurança

Proteção
Mecanismos
Técnicas
Treinamento



Direções para melhorar a segurança

Ser objetivo e conhecer os quesitos de segurança: CIA + privacidade + não-repúdio

Conhecer o ambiente ou ser claro quanto às suposições do mesmo

Direções para melhorar a segurança

- Ser objetivo e conhecer os quesitos de segurança: CIA + privacidade + não-repúdio => através de **POLÍTICAS** (organizacionais e técnicas) de **segurança**
- Conhecer o ambiente ou ser claro quanto às suposições do mesmo => através de **modelos de ameaça**

Direções para melhorar a segurança

- Ser objetivo e conhecer a segurança: CIA + privacidade + repúdio => através de controles (organizacionais e técnicos)
- Conhecer o ambiente e fazer baseadas às suposições do me

Política de Segurança uma declaração que define os objetivos de segurança de uma organização; ela deve definir o que precisa ser protegido; ela pode também indicar como será atingido.

Escopo medidas para melhorar a segurança

- **Técnicas:** autenticação, autorização, criptografia
- **Legais:** contratos, acordos (confidencialidade), leis
- **Orientados a Pessoas:** cultura, treinamento, ética, motivação, educação
- **Organizacionais:** governança, procedimentos, políticas, estratégias, auditorias

Frameworks de Segurança

Como implementar ou melhorar a infraestrutura de segurança da informação em uma organização?

- Adotando um **framework para implementar um sistema de gerenciamento de segurança da informação**: consiste em um **conjunto de padrões e práticas** que podem ser implementadas para aumentar a segurança. Além disso, os processos e as posturas de segurança poderiam ser validadas ou certificadas perante uma determinada norma padrão de segurança.
- **Framework** arcabouço de conhecimento anterior que já foi usado e testado, de forma que permite guiar no processo de se criar uma infraestrutura de segurança. Classificados em genéricos ou específicos.

Frameworks de Segurança

- **PCI/DSS**: padrão específico voltado para operadores de financeiros de cartões de crédito.
- **HITECH**: padrão específico para a área de saúde nos EUA.
- **NIST** Cybersecurity Framework, NIST SP 800-53, NIST SP 800-171: padrões gerais emitidos pelo órgão normativo americano (NIST) que pode ser adotado tanto por organizações federais do governo quanto por empresas privadas. (<https://csrc.nist.gov>)
- **CIS** (Center for Internet Security): fornece de forma gratuita documentos com controles de segurança (CIS Critical Security Controls v8) e também Benchmarks (www.cisecurity.org)
- **COBIT**: padrão genérico criado pela ISACA para gerenciamento e governança de TI. Apesar de não ter propósito principal a segurança, a abordagem de gerenciamento de riscos pode ser implementada para definir os controles de segurança.
- **ISO/IEC 27000**: a série de padrões de segurança 27000 da ISO/IEC abrange padrões para: definições (27000), requisitos para implementar segurança (27001, 27006, 27009), guias e códigos de prática (27002, 27003, 27004, 27005, 27007, 27013 e 27014), setores específicos (27010, 27011, 27015, 27017, 27018, 27019) e controles de segurança específicos, como segurança de redes e de aplicações (2703x, 2704x).

Controles de Segurança

- É uma medida que visa reduzir o risco de exploração e obter os objetivos de segurança da organização.
- Especificamente, podem ser encontrados em:
- ISO/IEC 27002 (2022): contém uma lista de controles de segurança e de boas práticas para implementação das mesmas. Elas são organizadas em categorias:
- **Control de acesso; Criptografia; Segurança das comunicações, operações, física e do ambiente**
- **Gestão de ativos; Aquisição, desenvolvimento e manutenção de sistemas**
- **Segurança em recursos humanos; Políticas de segurança da informação**
- **Relacionamento na cadeia de suprimentos**
- **Gestão de incidentes de segurança da informação**
- **Aspectos de segurança da informação na gestão da continuidade de negócio; Conformidade**

Controles de Segurança

5.4 Responsabilidades da direção

Tipo de controle	Propriedades de segurança da informação	Conceitos de segurança cibernética	Capacidades operacionais	Domínios de segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificar	#Governança	#Governança_e_ecossistema

Controle

Convém que a direção requeira que todo o pessoal aplique a segurança da informação de acordo com a política de segurança da informação estabelecida, com as políticas específicas por tema e com os procedimentos da organização.

Frameworks de Segurança

NIST Cybersecurity Framework, NIST SP 800-53, NIST SP 800-171:

- Identificar: ativos e ameaças
- Proteger ativos
- Detectar ataques
- Responder/Mitigar
- Recuperação

Proteger – Detectar – Responder

Incident Management ou Incident Response Process

Medidas de Segurança orientados a PESSOAS

Microsoft (2002): iniciativa de segurança

<https://www.microsoft.com/en-us/securityengineering/sdl/practices>

Practice #1 - Provide Training

Security is everyone's job. **Developers, service engineers, and program and product managers** must understand security basics and know how to build security into software and services to make products more secure while still addressing business needs and delivering user value.

Effective training will complement and re-enforce security policies, SDL practices, standards, and requirements of software security, and be guided by insights derived through data or newly available technical capabilities.

Although security is everyone's job, it's important to remember that not everyone needs to be a security expert nor strive to become a proficient penetration tester. However, ensuring everyone understands the attacker's perspective, their goals, and the art of the possible will help capture the attention of everyone and raise the collective knowledge bar.

Medidas de Segurança orientados a PESSOAS

TRAINING DEVELOPERS IN WRITING SECURE CODE

OWASP-SKF is a fully open-source Python-Flask web-application that uses the OWASP Application Security Verification Standard to train you and your team in writing secure code, by design.



Fonte: <https://owasp.org/www-project-security-knowledge-framework/>

Medidas de Segurança

O que pode dar errado?

“A Cultura come a Estratégia no café da Manhã”. Peter Drucker

SDL Timeline

The perfect storm



SDL ramp up



Setting a new bar



Collaboration



Selective tooling and Automation



2000 — 2001 — 2002 — 2003 — 2004 — 2005 — 2006 — 2007 — 2008 — 2009 — 2010 — 2011 —————— 2018+ ——————>

- Growth of home PC's
- Rise of malicious software
- Increasing privacy concerns
- Internet use expansion

- Bill Gates' TwC memo
- Microsoft security push
- Microsoft SDL released
- SDL becomes mandatory policy at Microsoft
- Windows XP SP2 and Windows Server 2003 launched with security emphasis

- Windows Vista and Office 2007 fully integrate the SDL
- SDL released to public
- Data Execution Prevention (DEP) & Address Space Layout Randomization (ASLR) introduced as features
- Threat Modeling Tool

- Microsoft joins SAFECode
- Microsoft Establish SDL Pro Network
- Defense Information Systems Agency (DISA) & National Institute Standards and Technology (NIST) specify features in the SDL
- Microsoft collaborates with Adobe and Cisco on SDL practices
- SDL revised under the Creative Commons License

- Additional resources dedicated to address projected growth in Mobile app downloads
- Industry-wide acceptance of practices aligned with SDL
- Adaption of SDL to new technologies and changes in the threat landscape
- Increased industry resources to enable global secure development adoption

Identidade e Autenticação (AuthN)

Identidade

novo perímetro de segurança

É o recurso mais direto para um atacante realizar:

- Movimentos laterais na rede
- Movimento vertical no sistema (aumento do nível de privilégio)
- Credenciais como informação para crimes de engenharia social

Informações relacionadas à identidade possuem um valor muito alto, tornando-se alvo de furto.

Autenticação de Usuários

Processo de determinar se alguém ou alguma coisa é, de fato, quem ou o que declarou ser. Ela ocorre em duas etapas:

- **Identificação:** apresentar um identificador (pode ser o mesmo ou não usado pelo SO para as atividades de controle de acesso).
- **Verificação:** apresentar ou gerar informações de identificação que corroboram o vínculo entre a entidade e o identificador.

Autenticação de Usuários: alguns meios

- Algo que o indivíduo sabe: senha, PIN. apresentar um identificador (pode ser o mesmo ou não usado pelo SO para as atividades de controle de acesso).
- Algo que o indivíduo possui: chaves criptográficas, chaves físicas, cartões de senha.
- Biometria
- O que está fazendo
- Localização



Autenticação de Usuários: alguns meios

Single Sign-On (SSO)

Multi-factor Authentication (MFA)

Two-Factor Authentication (2FA)

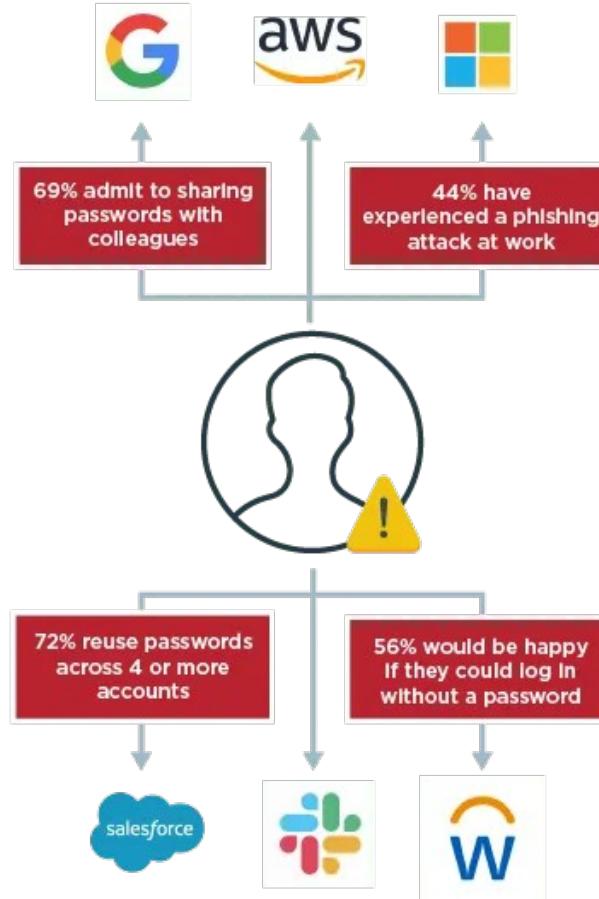
Autenticação de Usuários: variações

- LDAP: serviço de diretório X.500
- Kerberos: autenticação centralizada usando criptografia simétrica (KDC)
- TLS: autenticação de servidor via certificado de chave pública (permite também autenticação de cliente)
- SSH: também usa chaves digitais públicas para realizar identificação de indivíduos e máquinas.
- Sistemas de Gerenciamento de Identidade (IDM ou IDAM).
- Os sistemas operacionais usam funções de derivação (KDF) de chaves a partir das senhas dos usuários, executando centenas/milhares de operações com a inclusão de salts.

Certificados Digitais: documento (arquivo digital) que vincula um NOME a uma chave pública e que é assinado por uma terceira parte de confiança (autoridade certificadora)

The Truth About Your Users' Password Practices

O que pode dar
errado?



O que fazer

NIST SP 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management

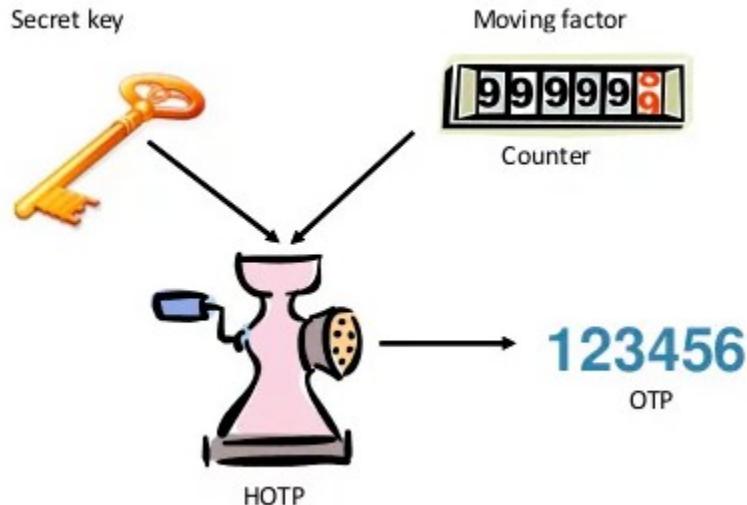
- Políticas de senhas
- Autenticação multi-fatorial (MFA ou 2FA)
- Habilitar uso de criptografia assimétrica para autenticar alguns serviços
- Tecnologias sem senha (passwordless): FIDO

O que fazer

Autenticação 2FA e MFA

HOTP (HMAC-based One-time Password)

[RFC4226] M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm", RFC 4226, December 2005.

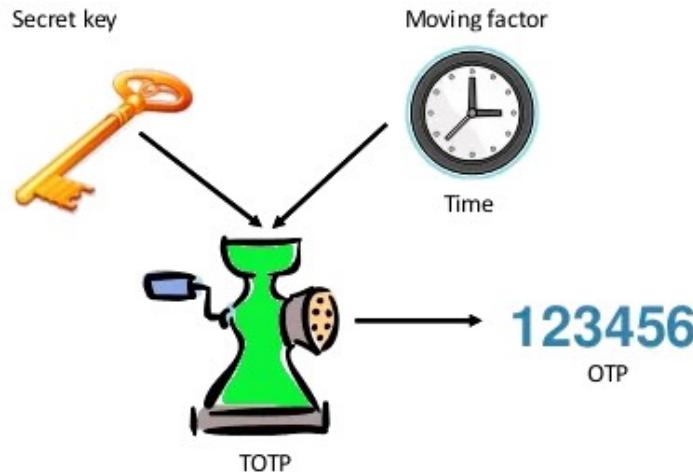


Fonte: obtido de <https://www.protectimus.com/blog/hotp-algorithm/>

O que fazer

Autenticação 2FA e MFA TOTP (Time-Based One-time Password)

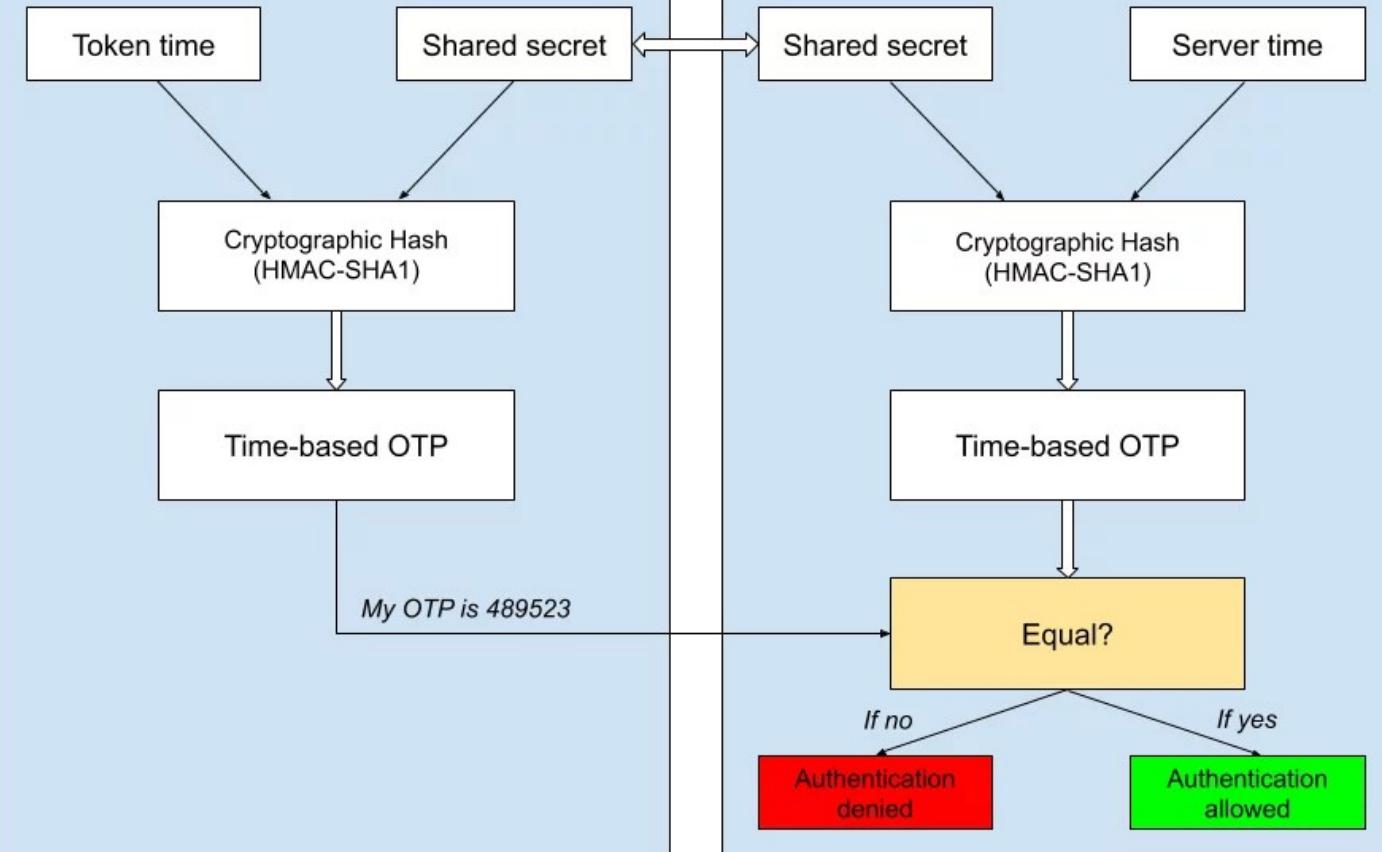
<https://tools.ietf.org/html/rfc6238> D. M'Raihi, Inc.; S. Machani; M. Pei; J. Rydell; May 2011



Fonte: obtido de <https://www.protectimus.com/blog/totp-algorithm-explained/>

TOTP token

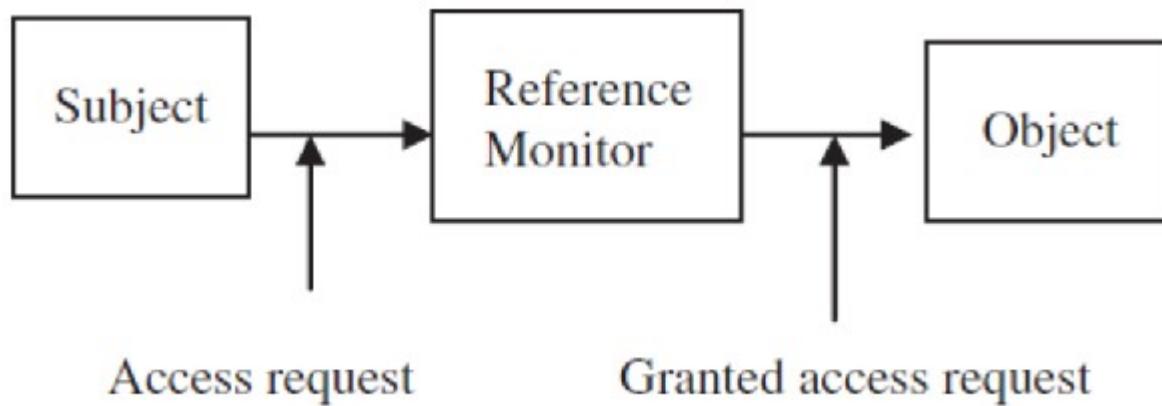
Server



Fonte: obtido de <https://www.protectimus.com/blog/totp-algorithm-explained/>

Autorização (AuthZ)

Modelo de Controle de Acesso



Monitor de Referência: entidade (geralmente do sistema operacional) com algo nível de confiabilidade e que aplica um conjunto de regras (baseadas nas políticas) para permitir ou negar um acesso.

Política versus Mecanismos

Política representa os objetivos gerais em termos de propriedades de segurança da informação.

Mecanismos são as formas como aplicações e sistemas operacionais implementam as políticas.

Autorização

Abstrações e nomenclaturas

Sujeitos: atores que realizam determinada operação

Objetos: agentes passivos que sofrem a ação

Direitos: observar (leitura somente), alterar (acesso de escrita)

Autorização

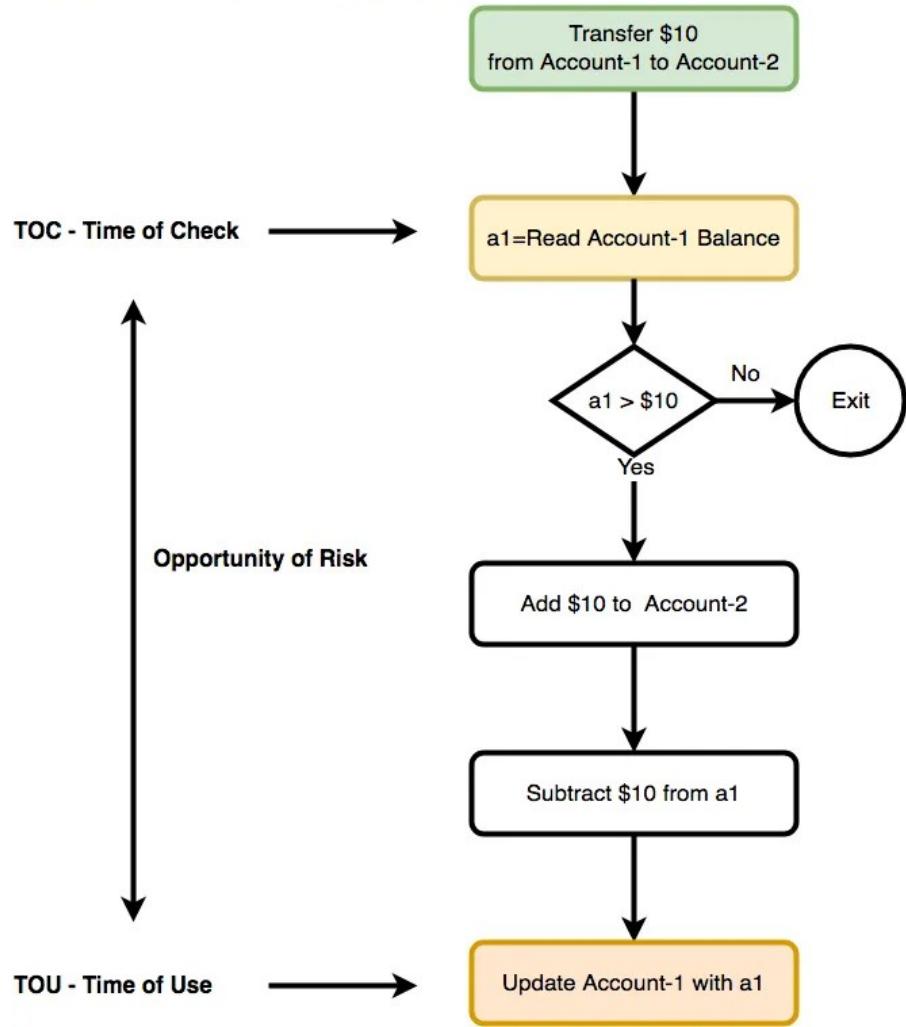
Vulnerabilidade **Time-of-check-to-time-of-use (TOCTTOU)** is a file-based **race condition** that occurs when a resource is checked for a particular value, such as whether a file exists or not, and that value then changes before the resource is used, invalidating the results of the check.

O que pode dar errado?

Autorização

O que pode dar errado?

Fonte: extraído de <https://medium.com/@schogini/toctou-time-of-check-and-time-of-use-a-demonstration-and-mitigation-609c999042cb>



Capacidades

Cada sujeito (processo/thread) deve conter a referência de um objeto e um conjunto de direitos.

Principais problemas quando usado em sistemas de arquivos: difícil saber quem tem permissão para acessar um objeto; difícil de revogar uma capability.

O Windows usa tokens associados a usuários logados que são usados durante o controle de acesso. Mas eles não especificam operações específicas sobre todos os objetos, mas direitos gerais.

O Linux implementa capabilities no kernel e atualmente há 30 diferentes capacidades que podem ser atribuídas a certas threads para realizar determinar determinadas ações. Bastante usada para segurança em containers (docker e kubernetes).

Discretionary Access Control (DAC)

Controle de Acesso Discricionário

Cada objeto (recurso) de um sistema DAC possui uma lista de controle de acesso (*Access Control List – ACL*). [coluna da matriz]

Uma ACL contém um usuário ou um grupo de sujeitos que possuem um nível de acesso a este objeto.

O usuário (proprietário) pode ajustar as permissões, concedendo ou negando acesso a outros usuários (por isso discricionário).

Mais flexível e implementado nos principais sistemas de arquivos.

Mandatory Access Control (MAC)

Controle de Acesso Mandatório

Define regras mais rígidas do que um usuário ou processo pode fazer.

Dois exemplos práticos:

- **SELINUX**: Fedora, RedHat, CentOS

Define contextos de segurança e cria labels para arquivos, processos e rede (portas). O SO controla os acessos e as permissões não estão mais associadas com a identidade (ID de usuário).

- **AppARMOR**: OpenSUSE, Debian e Ubuntu

Define uma forma diferente de controlar execução: através de caminhos.

- Outro modelo: Modelo Biba de Integridade: implementado parcialmente no Windows.

Usuários e Sujeitos

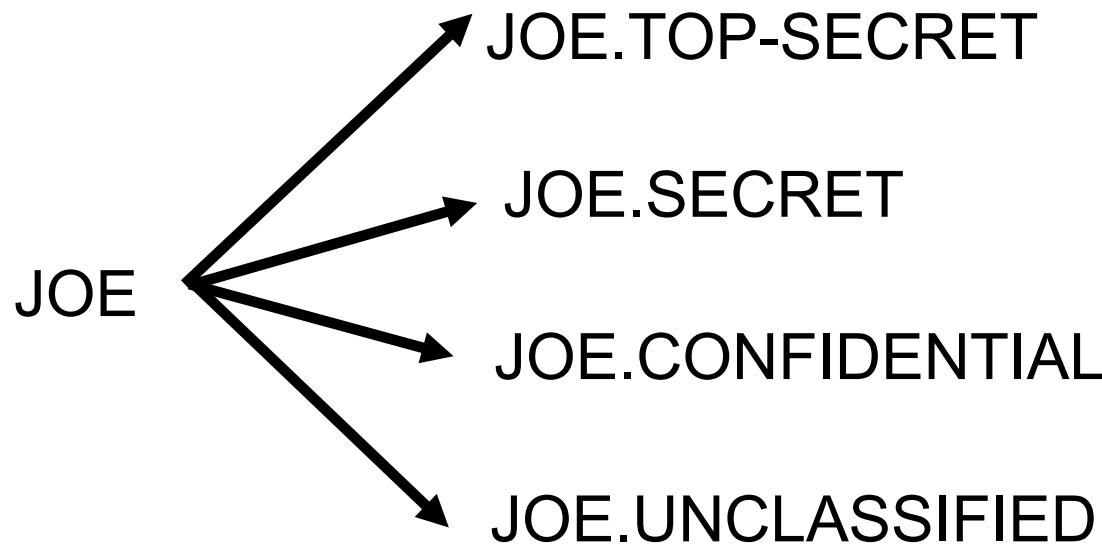
Até o momento, um sujeito representava unicamente uma única entidade (usuário ou aplicação).

Mas, em termos empresariais, um único sujeito pode estar executando tarefas associadas a diferentes papéis.

Então, é necessário distinguir um usuário do sujeito e da mesma forma dos direitos associados a este sujeito.

Um usuário humano pode se manifestar como múltiplos usuários (*principals, accounts*) no sistema.

Usuários e Sujeitos



USER

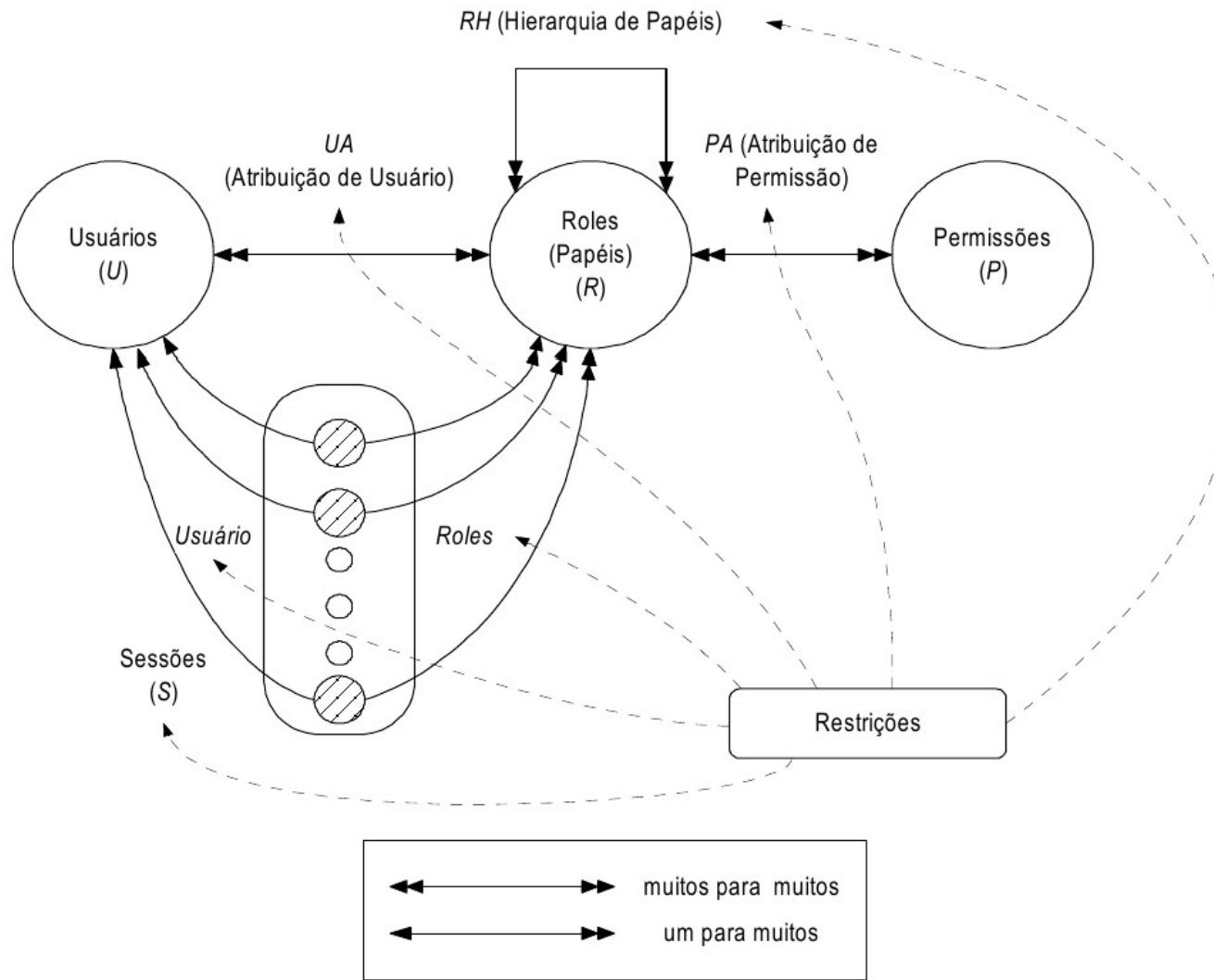
SUBJECTS

Role-Based Access Control (RBAC)

Controle de Acesso Baseado em Papéis

Regula o acesso dos usuários à informação com base nas atividades que os usuários desempenham no sistema:

- Papel (*role*) – pode ser definido como um conjunto de ações e responsabilidades associadas com uma atividade particular
- As autorizações de acesso a objetos são especificadas para os papéis
- Usuários são associados aos papéis



Role-Based Access Control (RBAC): vantagens

- Independentes de política
- Atribuição de direitos aos papéis (mais fácil gerenciar)
- Usuários podem trabalhar com privilégio mínimo
- Permite separação de tarefas

Attribute-Based Access Control (ABAC)

Controle de Acesso Baseado em Atributos

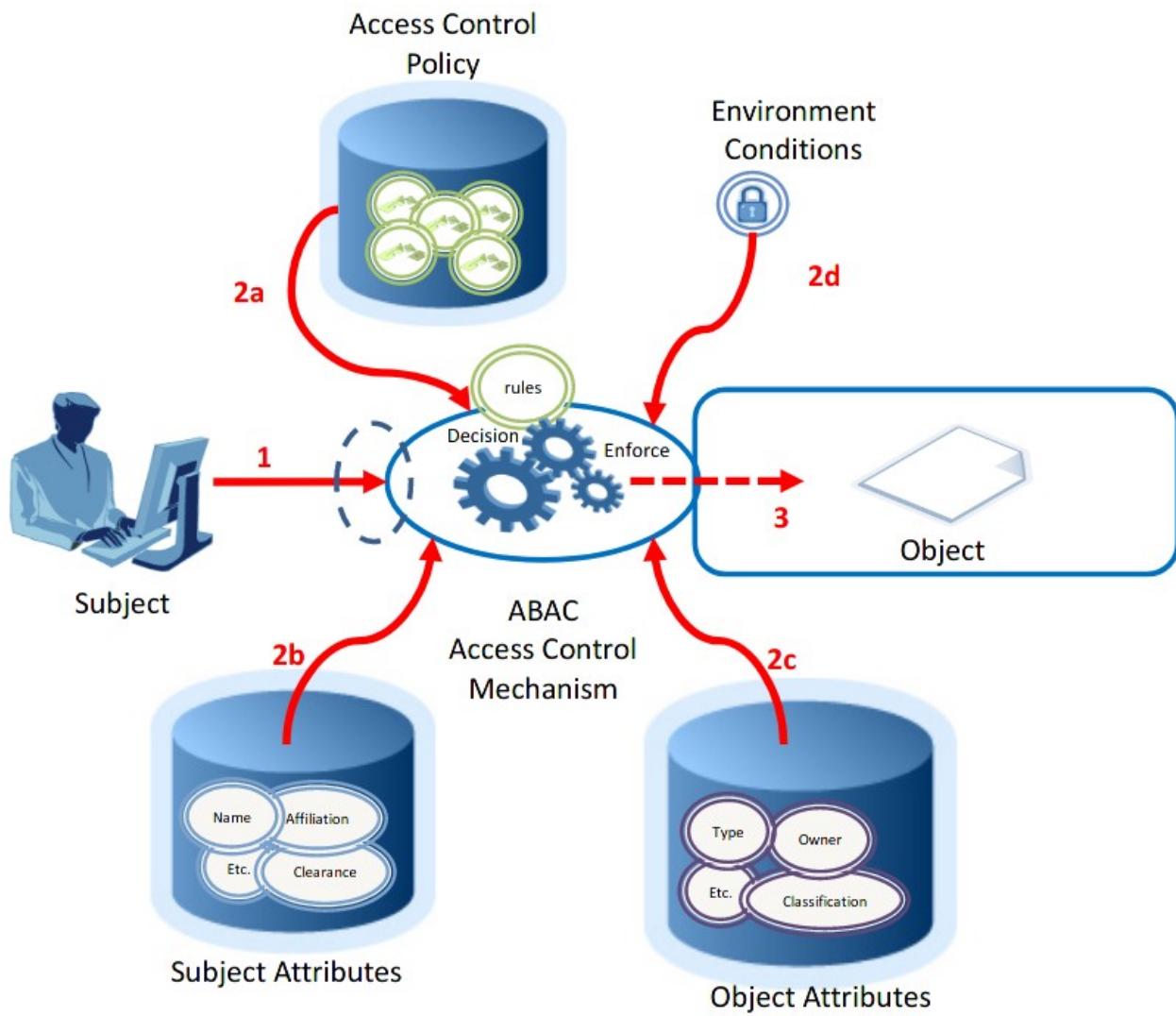
O controle de acesso é baseado em atributos.

Decisão de controle de acesso leva em conta: política, condições ambientais, atributos do sujeito e atributos do objeto.

Separação clara entre o mecanismo e a política.

Superconjunto dos outros mecanismos.

A implementação mais conhecida é o XACML (*Extensible Access Control Markup Language*)



Autorização e OAuth 2.0

É um protocolo IETF que transporta asserções de autorização (delegação de autorização) na forma de escopos (*scopes*). O token é opaco ao cliente, ou seja, o acesso é garantido a quem tiver a posse do mesmo (**bearer**).

Ele não contém informações de autenticação de usuário. Alguns problemas:

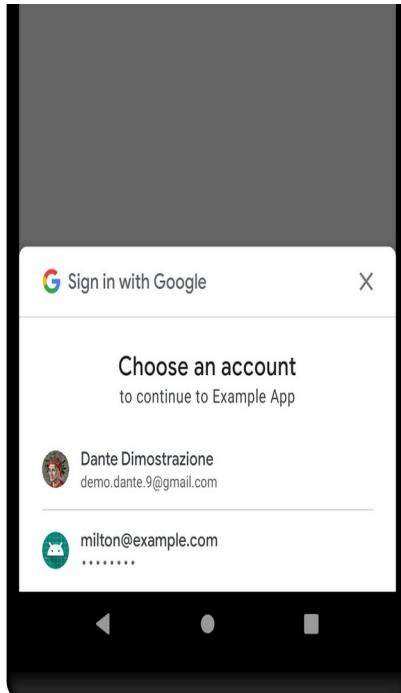
- Considerar que a posse de um token de acesso não é prova de autenticação.
- Considerar que o acesso a uma API protegida é prova de autenticação.

OpenID Connect: construído sobre o Oauth 2.0 e é usado para autenticar clientes. Além disso, os tokens de ID transportam informações específicas. <https://openid.net/connect/>

OAuth 2.0 e OpenID Connect

OpenID Connect implementado pelo Google

<https://developers.google.com/identity/protocols/oauth2/openid-connect>



```
{  
  "iss": "https://server.example.com",  
  "sub": "24400320",  
  "aud": "s6BhdRkqt3",  
  "nonce": "n-0S6_WzA2Mj",  
  "exp": 1311281970,  
  "iat": 1311280970,  
  "auth_time": 1311280969,  
  "acr": "urn:mace:incommon:iap:silver"  
}
```

Certificados de Identidade

Documento (arquivo digital) que vincula um **NOME** (**cname**) a uma **chave pública** e que é assinado por uma terceira parte de confiança (autoridade certificadora).

Mecanismo confiável obtido pela criptografia.

Problemas:

- Confiança entre-domínios e intra-domínios;
- Dificuldade em criar esquemas de nomes globais;
- Gerenciamento da PKI

Certificado Digital

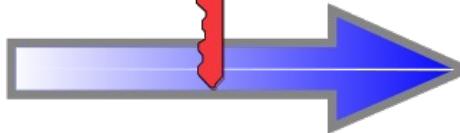
Identity Information and
Public Key of Mario Rossi

Name: *Mario Rossi*
Organization: *Wikimedia*
Address: *via*
Country: *United States*



Public Key
of
Mario Rossi

Certificate Authority
verifies the identity of Mario Rossi
and encrypts with its Private Key



Certificate of Mario Rossi

Name: *Mario Rossi*
Organization: *Wikimedia*
Address: *via*
Country: *United States*
Validity: *1997/07/01 - 2047/06/30*



Public Key
of
Mario Rossi

Digital Signature
of the Certificate Authority

Esquema de como um indivíduo/sítio
solicita um certificado digital de uma
autoridade (atualmente, a Let's Encrypt
fornecerá certificados gratuitos) <https://letsencrypt.org>

Digitally Signed by
Certificate Authority

Common Name	bcp.nic.br
<hr/>	
Issuer Name	
Country	US
Organization	Let's Encrypt
Common Name	R3
<hr/>	
Validity	
Not Before	Sat, 25 Mar 2023 06:16:32 GMT
Not After	Fri, 23 Jun 2023 06:16:31 GMT
<hr/>	
Subject Alt Names	
DNS Name	bcp.nic.br
DNS Name	bcpadmin-prod.devsy.s nic.br
DNS Name	ceptroadmin.devsy.s nic.br
DNS Name	credenciamento.nic.br
DNS Name	criancaseadolescentesnainternet.nic.br
DNS Name	cursointernetc.comresponsa.nic.br
DNS Name	gtergts.nic.br
DNS Name	intrarede.nic.br
DNS Name	minhaagenda.cursoeventos.nic.br
DNS Name	minhaagenda.nic.br
DNS Name	recibos.nic.br
DNS Name	semanacap.bcp.nic.br
DNS Name	storm.devsy.nic.br
DNS Name	tutoriais.semanainfrab.r.nic.br
DNS Name	www.bcp.nic.br
<hr/>	
Public Key Info	
Algorithm	Elliptic Curve
Key Size	384
Public Value	04:55:6E:C4:2D:5C:5E:B0:E8:04:C5:16:88:7B:EE:13:AD:50:BA:96:D4:53:E3:83...

Certificado Digital de <https://bcp.nic.br>



Warning: Potential Security Risk Ahead

Firefox detected an issue and did not continue to **demo.securityknowledgeframework.org**. The website is either misconfigured or your computer clock is set to the wrong time.

It's likely the website's certificate is expired, which prevents Firefox from connecting securely. If you visit this site, attackers could try

Fonte: <https://demo.securityknowledgeframework.org/>

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.

[Learn more...](#)

[Go Back \(Recommended\)](#)

[Advanced...](#)

Websites prove their identity via certificates, which are valid for a set time period. The certificate for demo.securityknowledgeframework.org expired on 1/3/2023.

Error code: [SEC_ERROR_EXPIRED_CERTIFICATE](#)

[View Certificate](#)

[Go Back \(Recommended\)](#)

[Accept the Risk and Continue](#)

Autorização com Certificados de Atributos

Certificados Digitais de Atributos: documento (arquivo digital) que vincula um **NOME+ATRIBUTOS** a uma chave pública e que é assinado por uma terceira parte de confiança (autoridade certificadora).

Pode ser usado em sistemas para controle de acesso (ex. Smartcards).

Apresenta os mesmos problemas de gerenciamento dos certificados de identidade.

Autorização: observações

Autorização assume a existência de uma política de segurança.

Ao fornecer autorização a alguém:

- Os privilégios devem ser determinados para a tarefa
- Deve possuir escopo
- Deve, de preferência, possuir uma janela temporal

Criptografia

De que trata segurança em rede?

Serviços fornecidos
pela criptografia

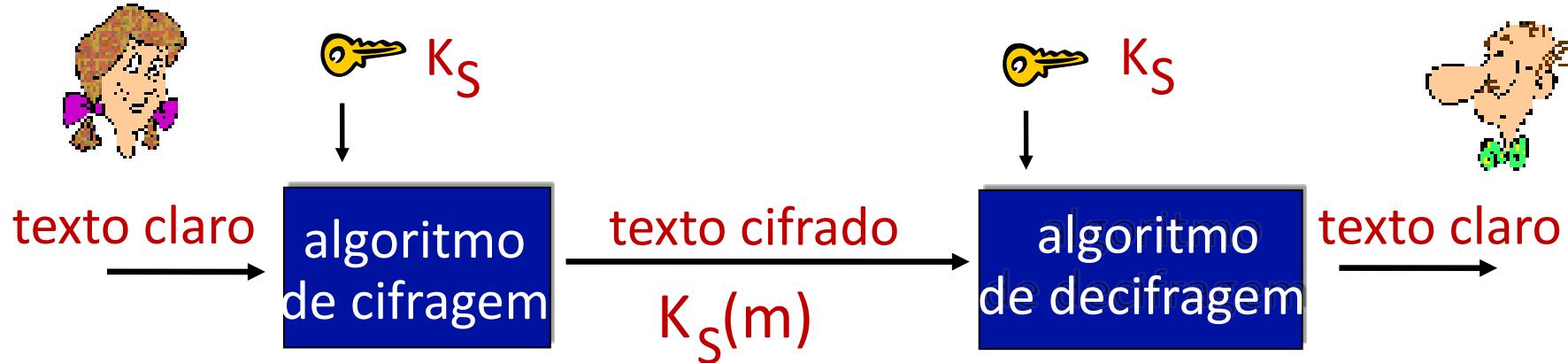
Confidencialidade: somente o destinatário deve ser capaz de ler o conteúdo de uma mensagem. É o serviço mais básico e o primeiro oferecido pela criptografia. O remetente cifra a mensagem e o destinatário decifra.

Autenticação: o destinatário quer confirmar a identidade do remetente.

Integridade: o destinatário possui garantias de que não houve violação ou alteração sem que seja detectada.

Disponibilidade: garantia de que serviços não sofram descontinuidade ou diminuição no nível de atendimento a seus usuários legítimos.

Criptografia de chave simétrica



Criptografia de chave simétrica: Bob e Alice compartilham a mesma (simétrica) chave K

Questão: como Bob e Alice concordam com o mesmo valor de chave?

Algoritmos de criptografia simétrica: AES

- Existem diversos algoritmos de criptografia que são classificados como de chave simétrica: a mesma chave K_s é usada tanto para cifrar quanto para decifrar.
- Em 2001 o NIST americano lançou um programa de submissões para substituição do DES: dos vários algoritmos, seis foram os finalistas e que podem ser usados atualmente: Serpent, RC6, MARS, Twofish e CAST-256. O vencedor acabou sendo o RIJNDAEL, que seria nomeado como AES.
- **AES** (*Advanced Encryption Standard*): padrão NIST para criptografia de chave simétrica (Nov 2001).
- Processa dados em blocos de 128 bits (um mensagem grande precisa ser processada em blocos e a forma determina os modos de cifragem).
- Chaves podem ser de tamanho: 128, 192 ou 256 bits.

Qual o problema fundamental da criptografia de chave simétrica?

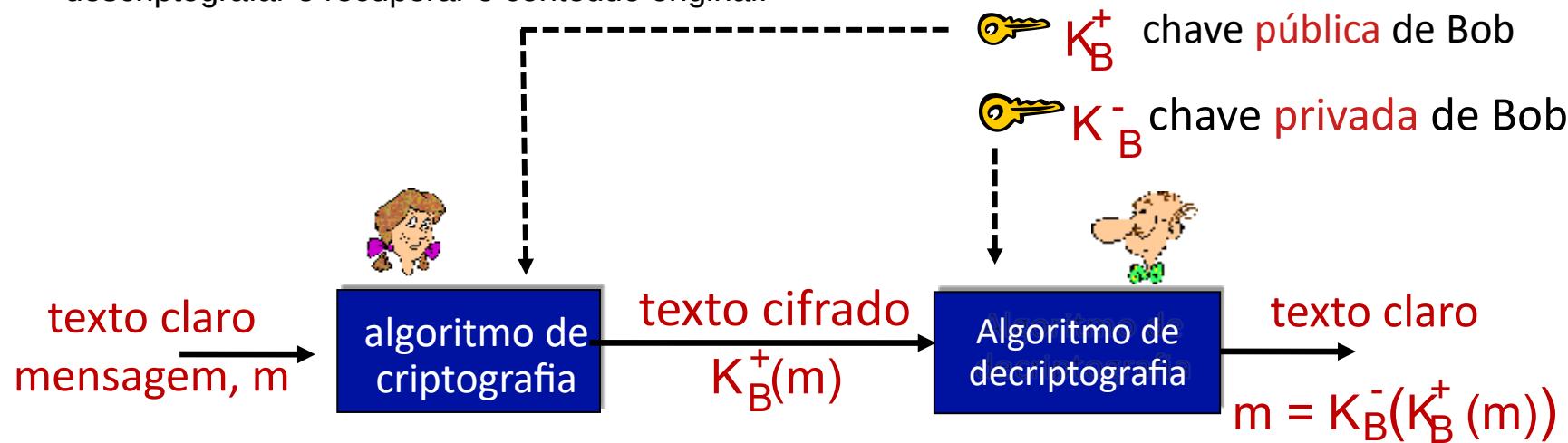
Problema fundamental da criptografia de chave simétrica: gerenciamento de chaves secretas.

- Como compartilhar a mesma chave entre Bob e Alice, principalmente para a situação em que nunca se encontraram (como ocorre atualmente na Internet)?
- E, quando o número de entidades aumenta?
- E, se uma entidade comprometer uma chave, como será a substituição?

Criptografia de chave assimétrica

Funcionamento básico da **criptografia de chave pública** para **cifragem**:

- Alice quer enviar uma mensagem que somente Bob possa descriptografar. Para isto, Bob precisa enviar sua chave pública (K_B^+) para Alice.
- Alice usa a chave pública de Bob para criptografar o conteúdo da mensagem m , gerando o texto cifrado.
- Para operação reversa de descriptografia, é necessário o conhecimento da respectiva chave privada. Neste caso, o único que possui a cópia é Bob, de forma que com sua chave privada (K_B^-) consegue descriptografar e recuperar o conteúdo original.



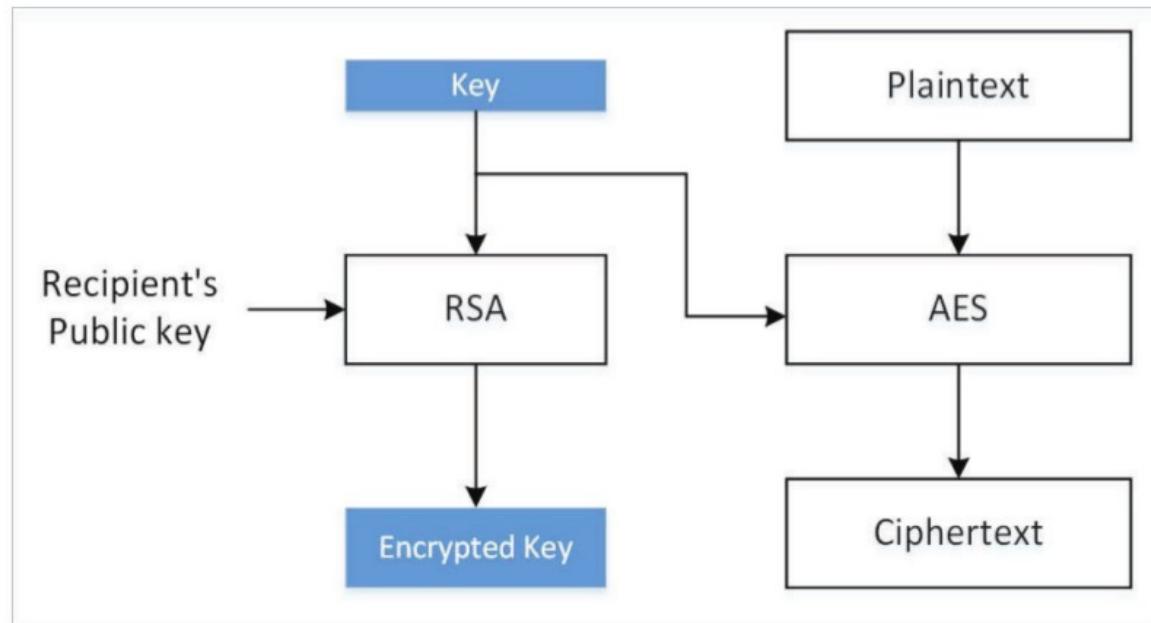
Alguns algoritmos de criptografia de chave pública

- O algoritmo **DH (Diffie-Hellman)** foi originalmente criado para gerar uma chave compartilhada. Mas, com pequena variação, pode-se tornar um algoritmo de chave pública. O algoritmo é baseado na dificuldade de calcular logaritmos discretos (outro esquema que usa essa construção é o **El Gamal**).
- O DH pode ser usado sobre curvas elípticas, o que dá origem ao **ECDH (Elliptic-curve Diffie–Hellman)**, protocolo usado para acordo e estabelecimento de chave secreta.
- Um algoritmo somente para assinatura foi criado pelo NIST, baseado em logaritmos discretos: **DSA (Digital Signature Algorithm)**.
- A variação do DSA sobre curvas elípticas gerou o **ECDSA (Elliptic Curve Digital Signature Algorithm)**.
- Um algoritmo mais recente e que tem sido incorporado em diversos protocolos (p.ex. OpenSSL 1.1.1) é o **Edwards-curve Digital Signature Algorithm (EdDSA)**, baseado no esquema de assinatura Schnorr sobre curvas Twisted Edwards (curvas elípticas). Reporta possuir mesmo nível de segurança que outros, mas em maior velocidade.

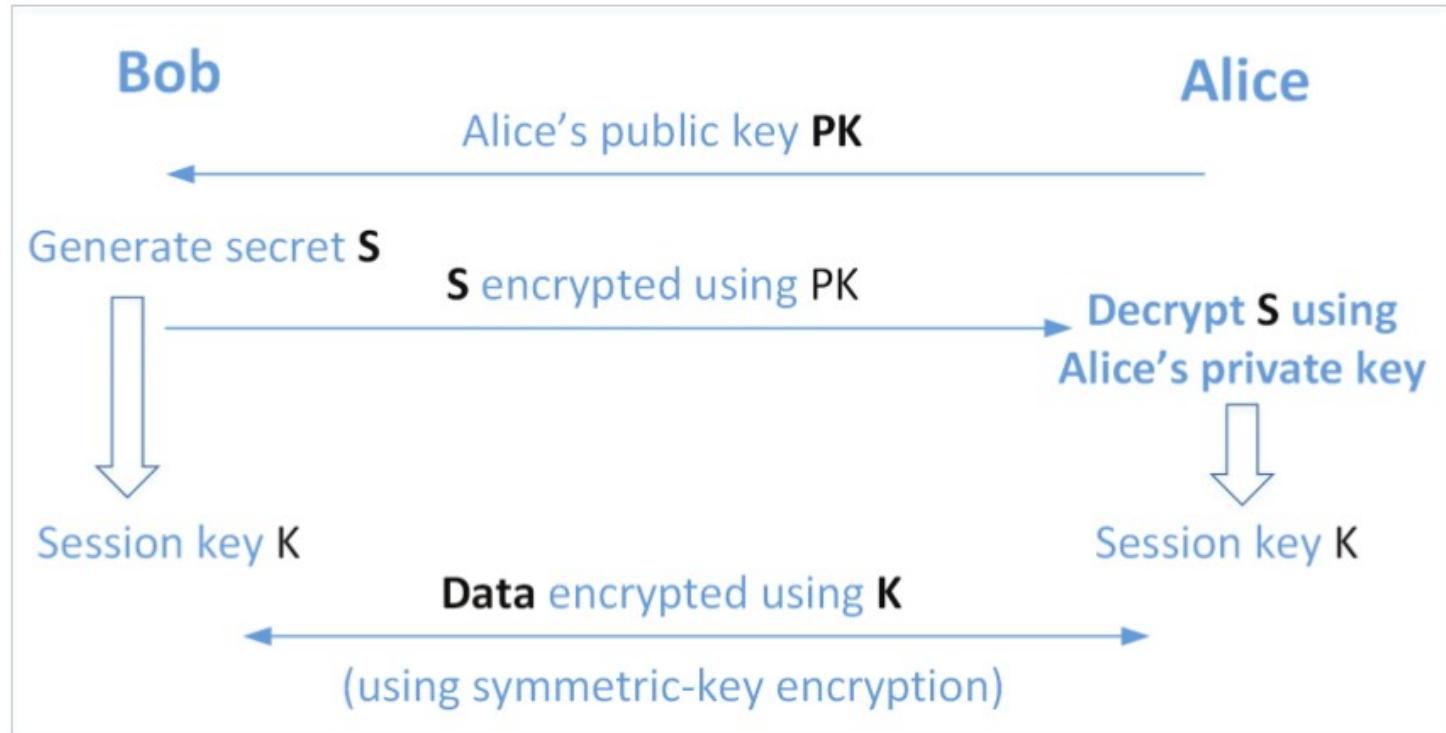
Observação: o problema da fatorização de números grandes, além do RSA, deu origem a vários outros protocolos de chave pública.

Algoritmos de criptografia de chave pública: como são implementados nos protocolos

Esquema de criptografia híbrida



TLS: princípio de funcionamento



PKI (*Public Key Infrastructure*)

- **Autoridade Certificadora (*Certificate Authority – CA*):** uma **terceira parte confiável** que deve verificar a identidade do sujeito e emitir certificados digitais assinados.
- **Certificados Digitais (*Digital Certificates*):** um documento certificando que a chave pública incluída no documento pertence à identidade descrita neste documento. Chama-se de ligar o sujeito à chave pública (bind). O padrão adotado foi o X.509 (originalmente ITU-T X.509 ou ISO/IEC 9594-8), cuja padronização atual está a cargo da IETF através da RFC 5280 (<https://tools.ietf.org/html/rfc5280>).

Exemplo de um certificado digital X.509

Identidade de quem
Emitiu o certificado (CA):

Symantec

Identificação de quem
tem a posse da chave
pública: paypal

```
Certificate:  
Data:  
    Serial Number:  
        2c:d1:95:10:54:37:d0:de:4a:39:20:05:6a:f6:c2:7f  
    Signature Algorithm: sha256WithRSAEncryption  
Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network,  
        CN=Symantec Class 3 EV SSL CA - G3  
Validity  
    Not Before: Feb  2 00:00:00 2016 GMT  
    Not After : Oct 30 23:59:59 2017 GMT  
Subject: 1.3.6.1.4.1.311.60.2.1.3=US/  
        1.3.6.1.4.1.311.60.2.1.2=Delaware/  
        businessCategory=Private Organization/  
        serialNumber=3014267, C=US/  
        postalCode=95131-2021, ST=California,  
        L=San Jose/street=2211 N 1st St,  
        O=PayPal, Inc., OU=CDN Support, CN=www.paypal.com
```

Atividade de análise TLS e certificados digitais

Scanning (descoberta vulnerabilidades) de serviço HTTP (PORTA=normalmente 80)

Quais cifras/algoritmos um servidor HTTS suporta
nmap --script ssl-enum-ciphers -p443 ufsc.br

Simula um cliente TLS

openssl s_client -connect ufsc.br:443 | tee ufsc.br-x509.txt

Extrai e apresenta os diversos campos do certificado digital x.509 do servidor ufsc.br

openssl x509 -tex -noout < ufsc.br-x509.txt

Bibliografia

- DIOGENES, Yuri; OZKAYA, Erdal. **Cybersecurity – Attack and Defense Strategies: Improve your security posture to mitigate risks and prevent attackers from infiltrating your system.** Third Edition. Packt Publishing Ltd, 2022.
- DU, Wenliang. *Computer Security: A Hands-on Approach*. 2nd Edition. Independent Published, 2019a.
- DU, Wenliang. *Internet Security: A Hands-on Approach*. 2nd Edition. Independent Published, 2019b.
- GOLLMANN, D. *Computer Security*. 3. ed. UK: John Wiley & Sons, 2011. 456 p.
- KUROSE, Jim e ROSS, Keith. *Computer Networking: A Top-Down Approach*. 8th edition. Pearson, 2020
- STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. Tradução de Daniel Vieira. 6. ed. São Paulo: Pearson Education do Brasil, 2015. 558p.