Conceitos Introdutórios de Criptografia

Referencial Teórico

- Base para estudos
  - Stallings, William. Criptografia e segurança de redes; tradução Daniel Vieira; revisão técnica Ákio Barbosa e Marcelo Succi. – 4. ed. – São Paulo: Pearson Prentice Hall, 2008. Págs. 2-12

Introdução

Capítulo 2

1.1 Tendências de segurança

1.2 A arquitetura de segurança OSI

1.3 Ataques à segurança

1.4 Serviços de segurança

1.5 Mecanismos de segurança

1.6 Um modelo para segurança de rede

Introdução

- Segurança da Informação, dentro da organização passaram por duas mudanças importantes:

1. Antes do uso generalizado de equipamentos de processamento de dados, a segurança da informação considerada valiosa para uma organização era fornecida principalmente por meios físicos e administrativos.
   - Com a introdução do computador, tornou-se evidente a necessidade de ferramentas automatizadas para proteger arquivos e outras informações armazenadas no computador.

Introdução

2. A segunda mudança importante que afetou a segurança é a introdução de sistemas distribuídos e o uso de redes e recursos de comunicação para transmitir dados entre o usuário do terminal e o computador e entre computadores.
   - As medidas de segurança de rede são necessárias para proteger dados durante sua transmissão

Introdução

- A segurança envolvendo comunicações e redes não é tão simples quanto pode parecer a princípio para o iniciante.
- A maioria dos principais requisitos para serviços de segurança pode receber rótulos autoexplicativos de uma palavra: confidencialidade, autenticação, irretratabilidade, integridade. Mas os mecanismos usados para atender a esses requisitos podem ser muito complexos.

Introdução

- Ao desenvolver um mecanismo ou algoritmo de segurança específico, é preciso considerar sempre os ataques em potencial a esses recursos de segurança. Em muitos casos, os ataques bem-sucedidos são planejados examinando-se o problema de um modo completamente diferente, explorando assim um ponto fraco inesperado no mecanismo.

Introdução

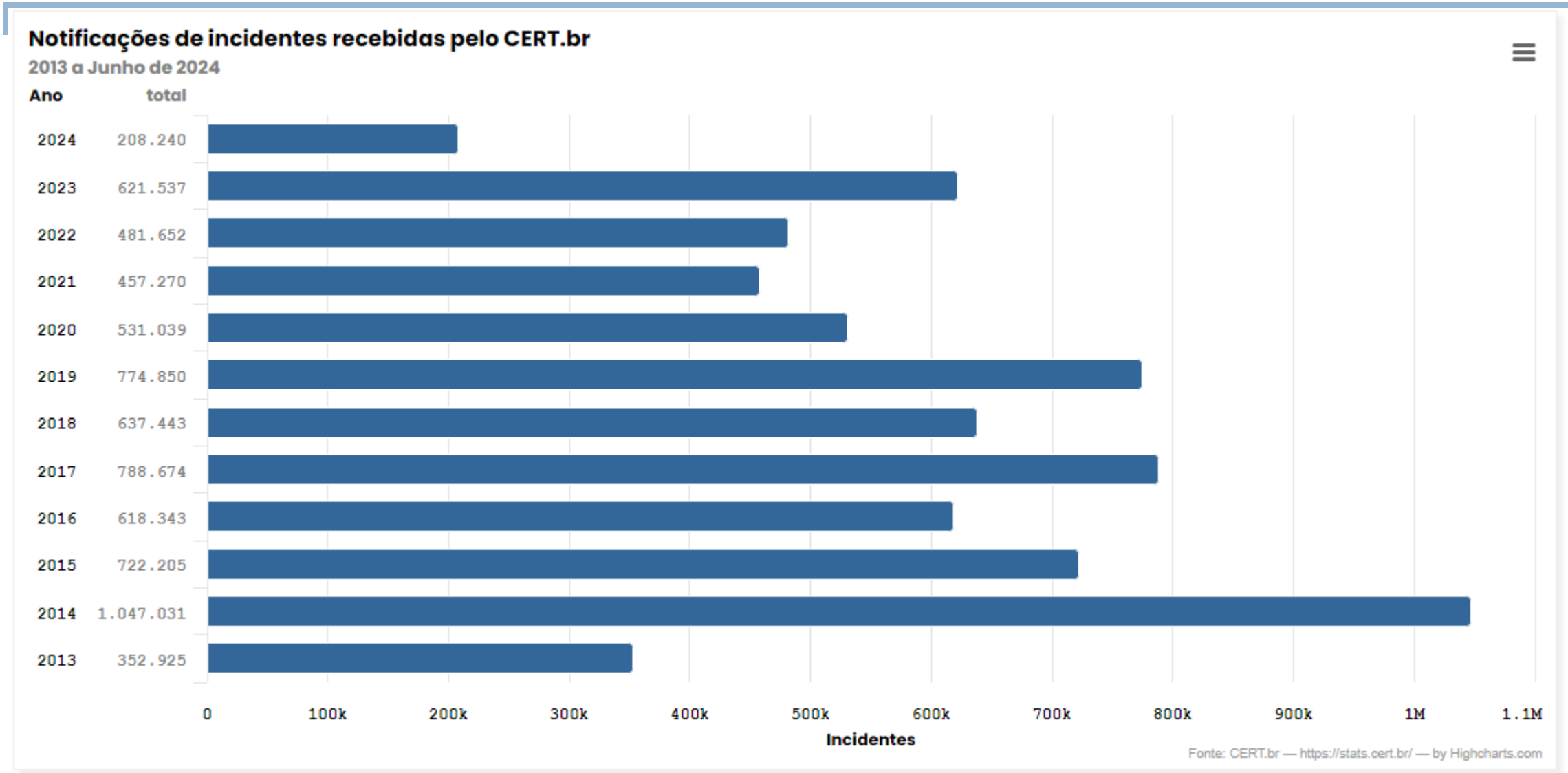
- Tendo projetado diversos mecanismos de segurança, é preciso decidir onde usá-los, ou seja, onde os mecanismos devem ser colocados. Isso é verdadeiro tanto em termos de posicionamento físico:
  - em que pontos de uma rede certos mecanismos de segurança
- Quanto em um sentido lógico
  - Em que camada ou camadas de uma arquitetura como TCP/IP - Transmission Control Protocol/Internet Protocol.

Introdução

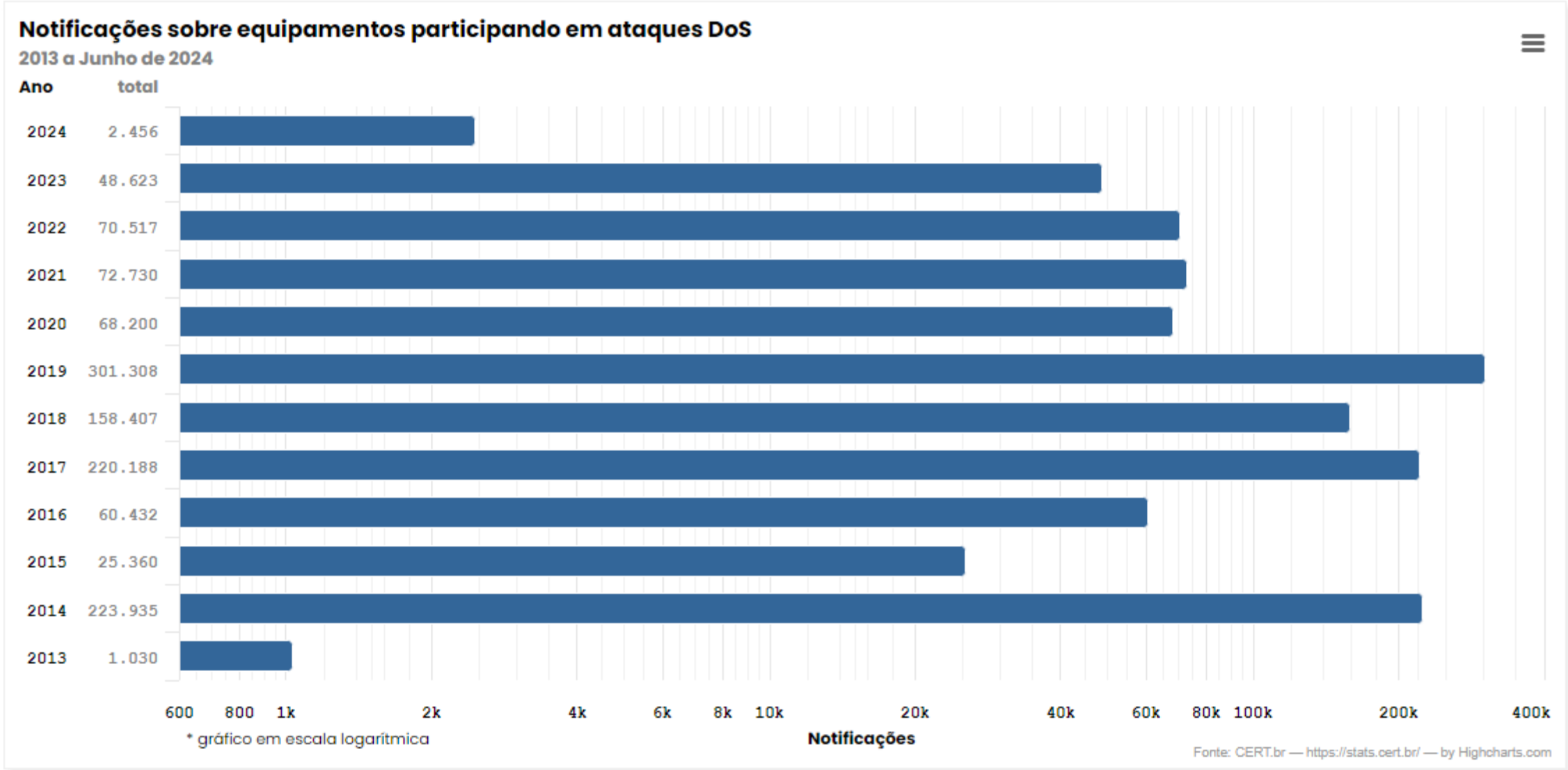
- Mecanismos de segurança normalmente envolvem mais do que um algoritmo ou protocolo específico. Eles geralmente também exigem que os participantes possuam alguma **informação secreta**, que levanta questões sobre a criação, distribuição e proteção dessa **informação secreta**.
  - Por exemplo, uma chave de **criptografia**.

1.1 TENDÊNCIAS DE SEGURANÇA

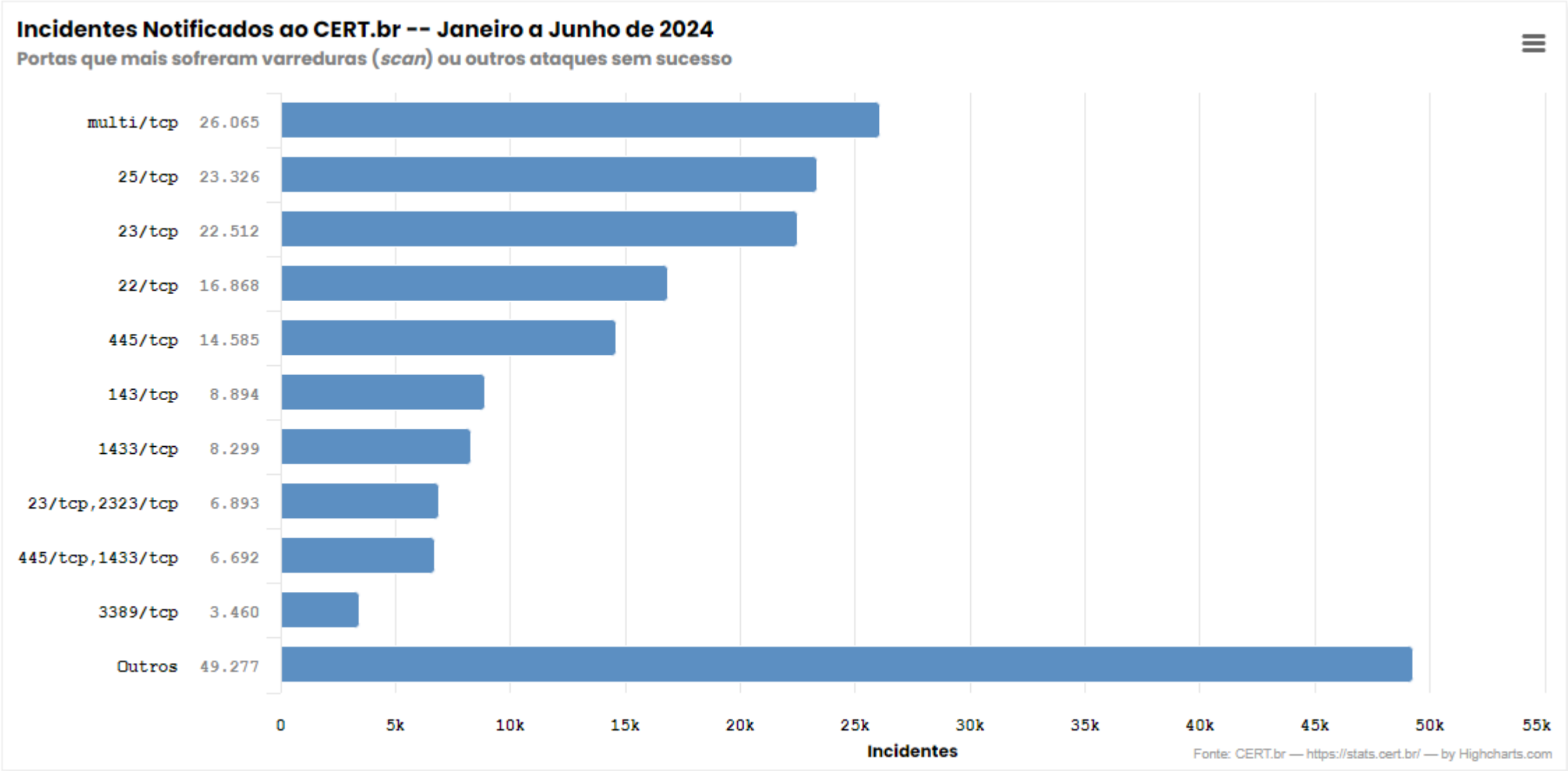
1.1 TENDÊNCIAS DE SEGURANÇA



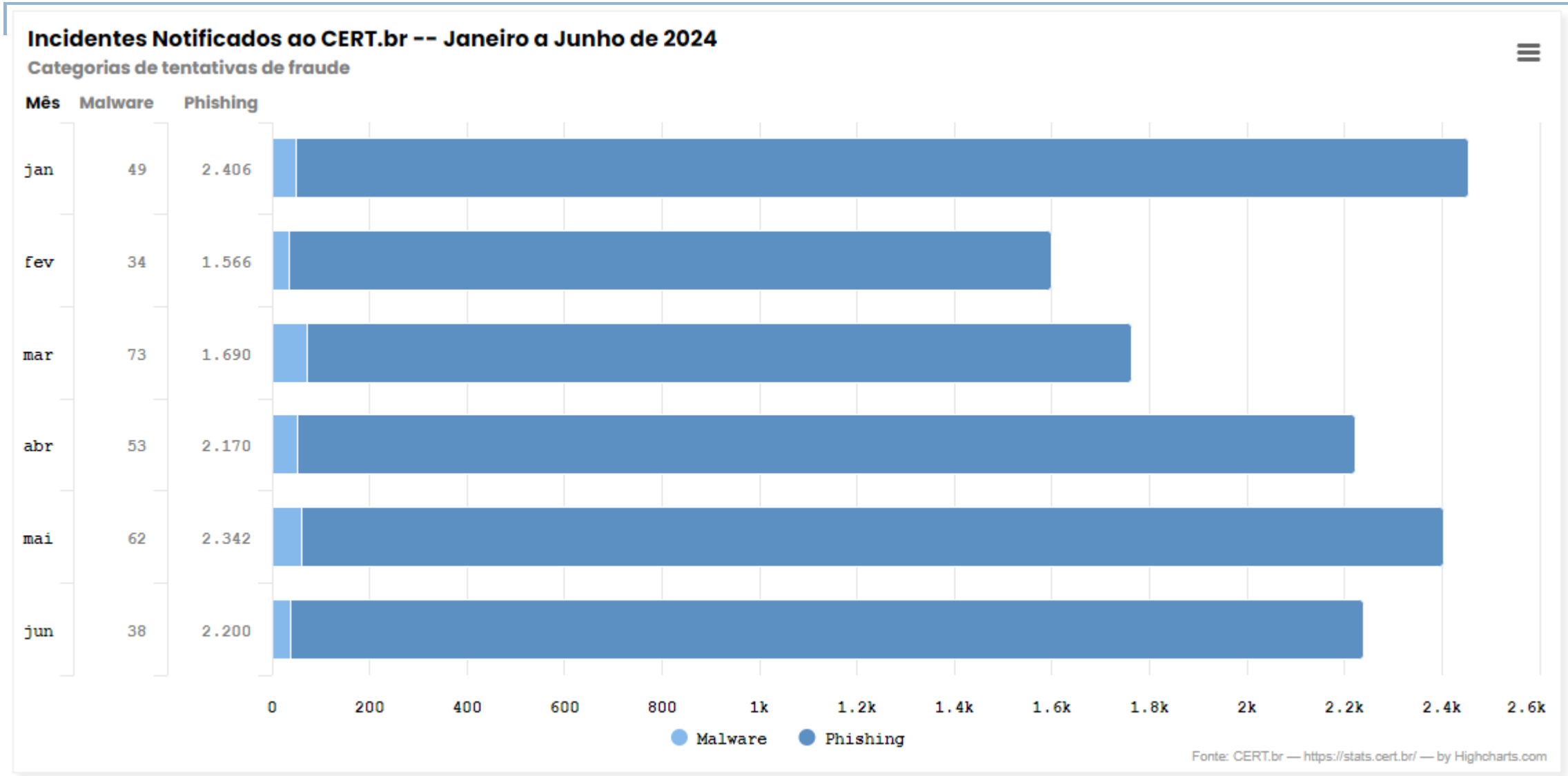
1.1 TENDÊNCIAS DE SEGURANÇA



1.1 TENDÊNCIAS DE SEGURANÇA



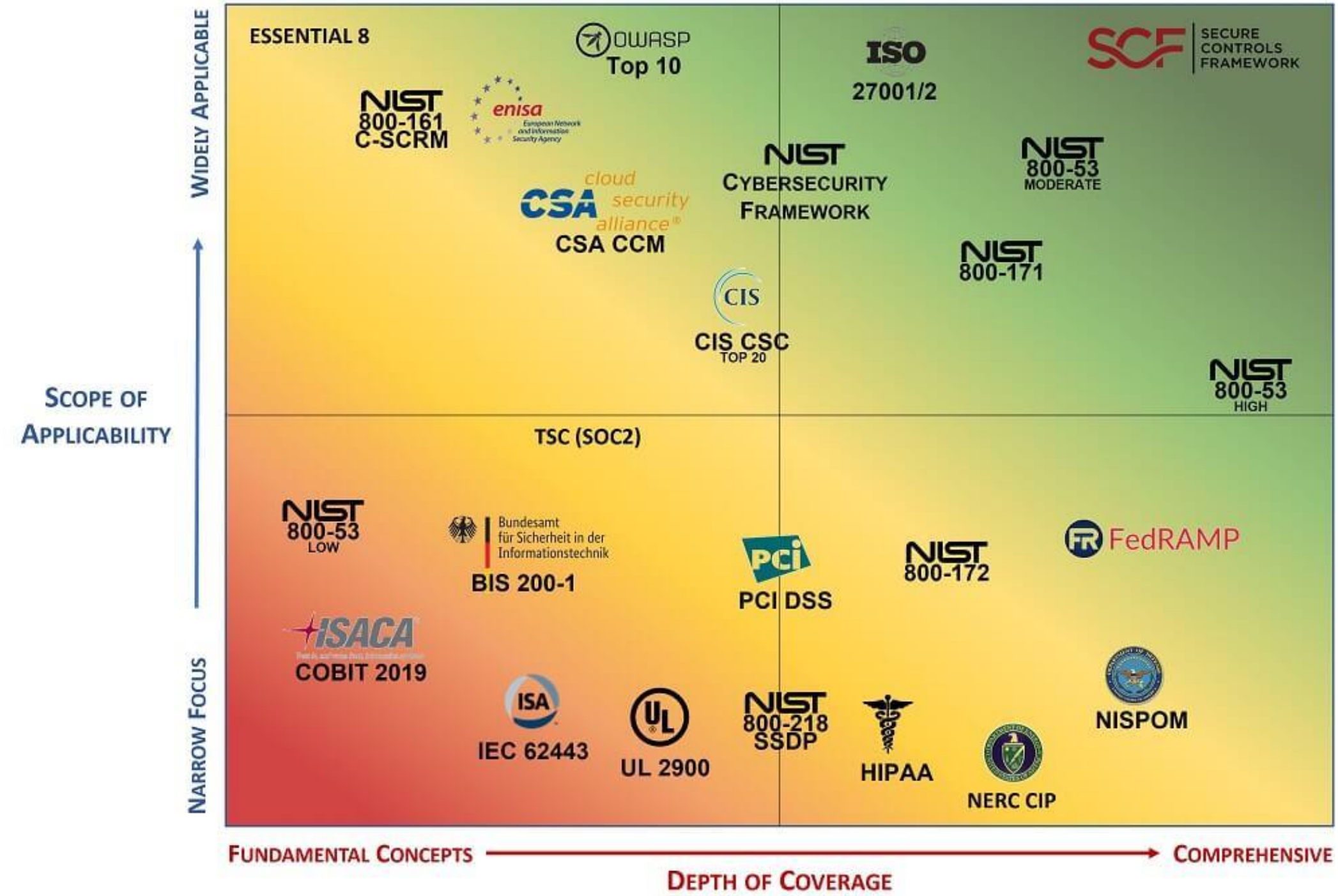
1.1 TENDÊNCIAS DE SEGURANÇA



1.2 A ARQUITETURA DE SEGURANÇA OSI

- Para avaliar efetivamente as necessidades de segurança de uma organização e avaliar e escolher diversos produtos e políticas de segurança, o gerente responsável precisa de algum meio sistemático de definir os requisitos de segurança e caracterizar as técnicas para satisfazer esses requisitos.
- A recomendação X.800 da ITU-T[2] Security architecture for OSI, define tal técnica sistemática.
- A arquitetura de segurança OSI[3] é útil para os gerentes como um meio de organizar a tarefa de prover segurança

2. International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) é uma agência patrocinada pelas Nações Unidas que desenvolve padrões, chamados de 'recomendações', relacionados a telecomunicações e à Open Systems Interconnection (OSI).
3. A arquitetura de segurança OSI foi desenvolvida no contexto da arquitetura de protocolo OSI. Porém, para nossos propósitos neste capítulo, um conhecimento da arquitetura de protocolos OSI não é obrigatório.


ESSENTIAL 8
OWASP Top 10
ISO 27001/2
SECURE CONTROLS FRAMEWORK
NIST 800-161 C-SCRM
enisa
NIST CYBERSECURITY FRAMEWORK
NIST 800-53 MODERATE
cloud security alliance
CSA CCM
NIST 800-171
CIS
CIS CSC TOP 20
NIST 800-53 HIGH
TSC (SOC2)
NIST 800-53 LOW
Bundesamt für Sicherheit in der Informationstechnik
BIS 200-1
PCI DSS
NIST 800-172
FedRAMP
ISACA
COBIT 2019
ISA
IEC 62443
UL 2900
NIST 800-218 SSDP
HIPAA
NERC CIP
NISPOM
WIDELY APPLICABLE
NARROW FOCUS
SCOPE OF APPLICABILITY
FUNDAMENTAL CONCEPTS
COMPREHENSIVE
DEPTH OF COVERAGE

CIS Controls™

V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

ISO 27001 COMPLIANCE STEPS

1.2 A ARQUITETURA DE SEGURANÇA OSI

- A arquitetura de segurança OSI enfoca ataques, mecanismos e serviços de segurança. Estes podem ser definidos resumidamente da seguinte forma:
  - **Ataque à segurança**: Qualquer ação que comprometa a segurança da informação pertencente a uma organização.
  - **Mecanismo de segurança**: Um processo (ou um dispositivo incorporando tal processo) que é projetado para detectar, impedir ou permitir a recuperação de um ataque à segurança.
  - **Serviço de segurança**: Um serviço de processamento ou comunicação que aumenta a segurança dos sistemas de processamento de dados e as transferências de informação de uma organização. Os serviços servem para frustrar ataques à segurança e utiliza um ou mais mecanismos de segurança para prover o serviço.

1.2 A ARQUITETURA DE SEGURANÇA OSI

- **Ameaça**
  - Potencial para violação da segurança quando há uma circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos. Ou seja, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade.
- **Ataque**
  - Um ataque à segurança do sistema, derivado de uma ameaça inteligente, ou seja, um ato inteligente que é uma tentativa deliberada (especialmente no sentido de um método ou técnica) de burlar os serviços de segurança e violar apolítica de segurança de um sistema.

Para ilustrar...


(AGENTE DE AMEAÇA)
EXPLORA
AMEAÇA
VULNERABILIDADE
=
UMA PORTA ABERTA
(OU DESTRANCADA... OU FÁCIL DE ABRIR!)
PODE RESULTAR EM...
=
PODENDO RESULTAR EM...
INCIDENTE!
RISCO = PROBABILIDADE
(QUAIS AS CHANCES DE UMA AMEAÇA EXPLORAR UM RISCO?)
404
DANOS
GISELE KAUER, - 2020

AMEAÇAS PODEM SER...

-POR GISELE KAUER, 2020-

• NATURAIS:

DECORRENTES DA NATUREZA, COMO TSUNAMIS, TORNADOS, TERREMOTOS, INCÊNDIOS (DE ORIGEM NATURAL).

• INTENCIONAIS:

COMO POSSÍVEIS ROUBOS, INVASÕES, FRAUDES -PROPOSITAIS!-

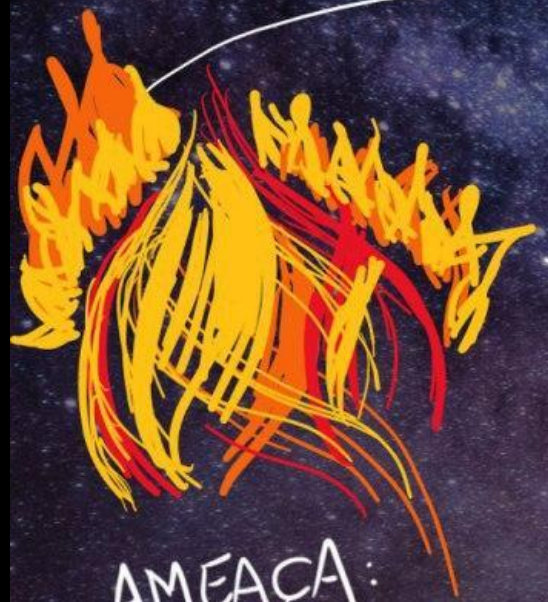
• INVOLUNTÁRIAS:

ERROS POR DESCONHECIMENTO, DESCUIDO, DESATENÇÃO; COMO FUNCIONÁRIOS SEM TREINAMENTO ADEQUADO, QUE PODEM SER VÍTIMAS DE PHISHING.

INTERNAS X EXTERNAS

INTERNAS	EXTERNAS
EX.: -FUNCIONÁRIOS	EX.: -CRACKERS -DESASTRES NATURAIS

EXEMPLO (1)



AMEAÇA:
incêndio

VULNERABILIDADE:
servidor com backup no mesmo local físico

GISELE KAVER, 2020

INCIDENTE:
incêndio na sala de servidores

RISCO: A PROBABILIDADE DE UM INCÊNDIO ATINGIR O SERVIDOR E SEU BACKUP.

EXEMPLO (2)

AMEAÇA:
ataque - cracker
(através de malware, engenharia social, ou combinando as duas coisas.)

VULNERABILIDADE:
sistema operacional desatualizado (e, consequentemente, vulnerável a certas falhas de segurança.)

INCIDENTE:
"contaminação" do sistema/empresa/PC/servidor/etc
(POR VÍRUS OU OUTRO TIPO DE MALWARE, COMO RANSOMWARE, WORM, BOTNET, ETC.)

RISCO: QUAL A PROBABILIDADE DE UM CRACKER SE APROVEITAR DA FALHA DE SEGURANÇA PRESENTE NAS VERSÕES ANTERIORES À ATUALIZAÇÃO XX.12-345 PARA REALIZAR ATAQUE?

—GISELE KAUER, 2020—

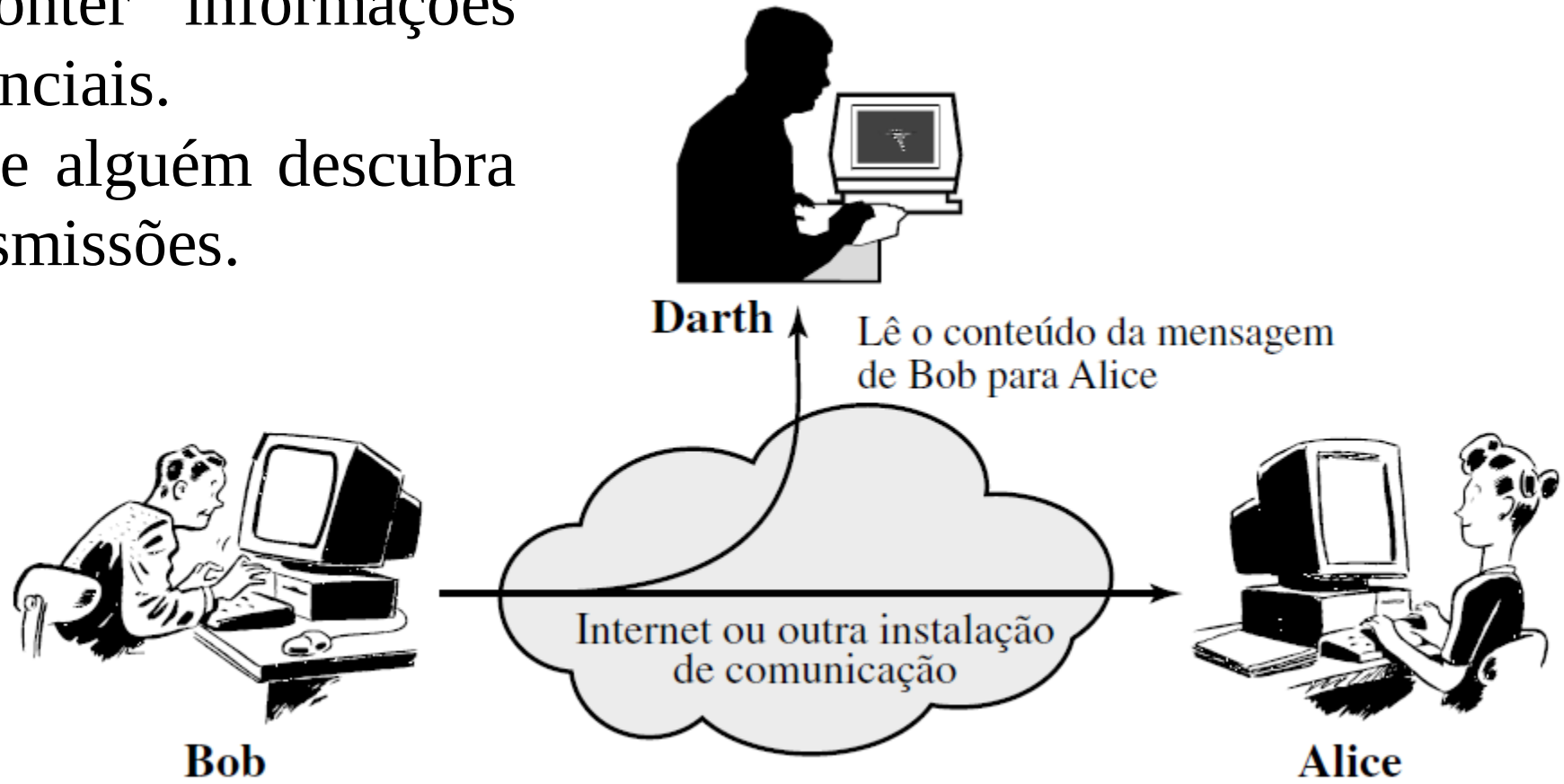
1.3 ATAQUES À SEGURANÇA

- Uma maneira útil de classificar os ataques à segurança, usada tanto na X.800 quanto na RFC 2828, é em termos de ataques passivos e ataques ativos.
- Ataques passivos
  - Os ataques passivos possuem a natureza de bisbilhotar ou monitorar transmissões. O objetivo é obter informações que estão sendo transmitidas. Dois tipos de ataques passivos são liberação do conteúdo da mensagem e análise de tráfego.

Liberação do conteúdo da mensagem

A **liberação do conteúdo da mensagem** é facilmente compreendida (Figura a). Uma conversa telefônica, uma mensagem de correio eletrônico e um arquivo transferido podem conter informações importantes ou confidenciais.

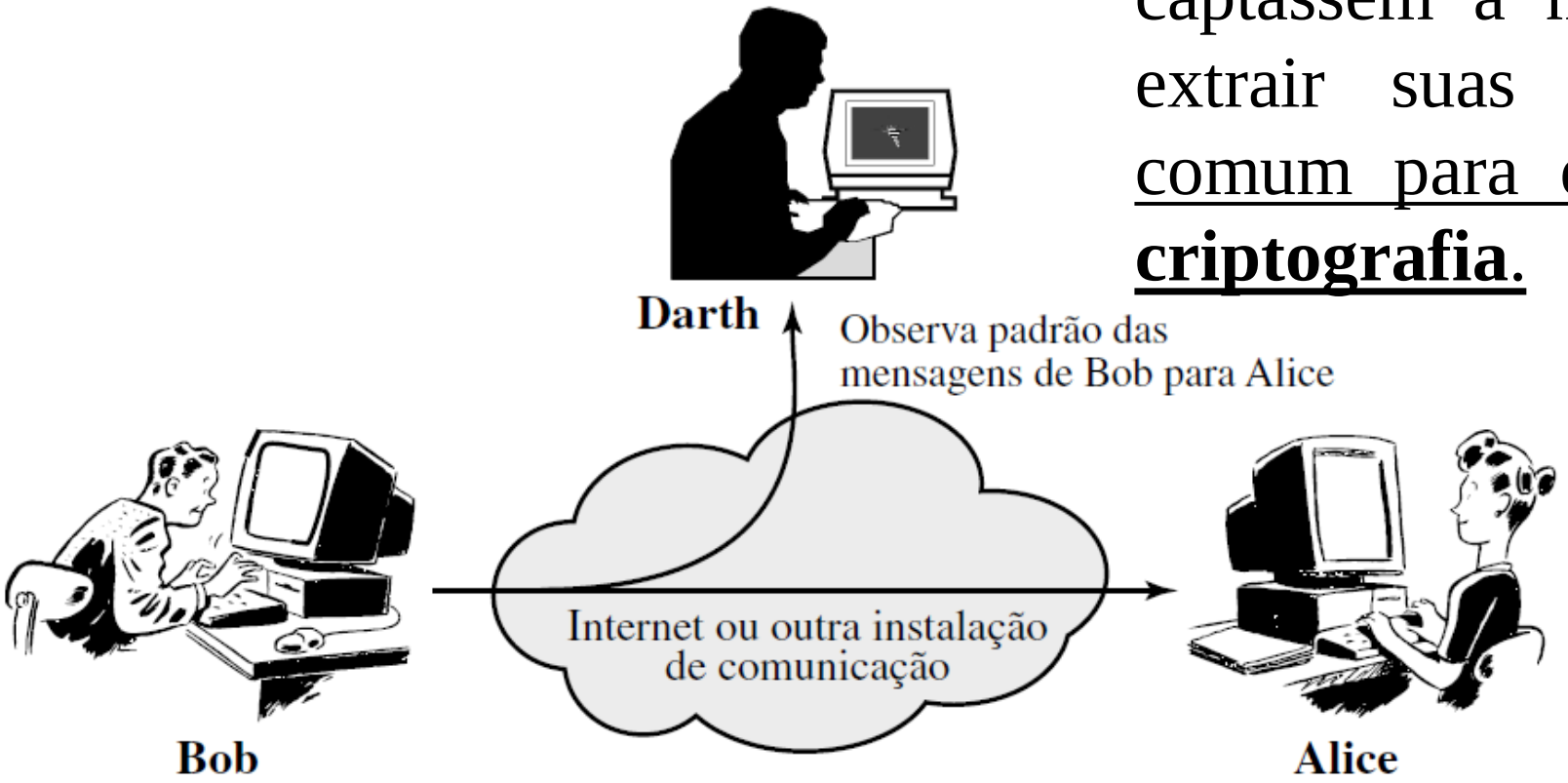
Desejamos impedir que alguém descubra o conteúdo dessas transmissões.



(a) Liberação de conteúdo da mensagem

Análise de Tráfego

Um segundo tipo de ataque passivo, a **análise de tráfego**, é mais sutil (Figura b). Suponha que tivéssemos uma maneira de disfarçar o conteúdo das mensagens ou de outro tráfego de informações de modo que os oponentes, mesmo que captassem a mensagem, não pudessem extrair suas informações. A técnica comum para disfarçar o conteúdo é a **criptografia**.

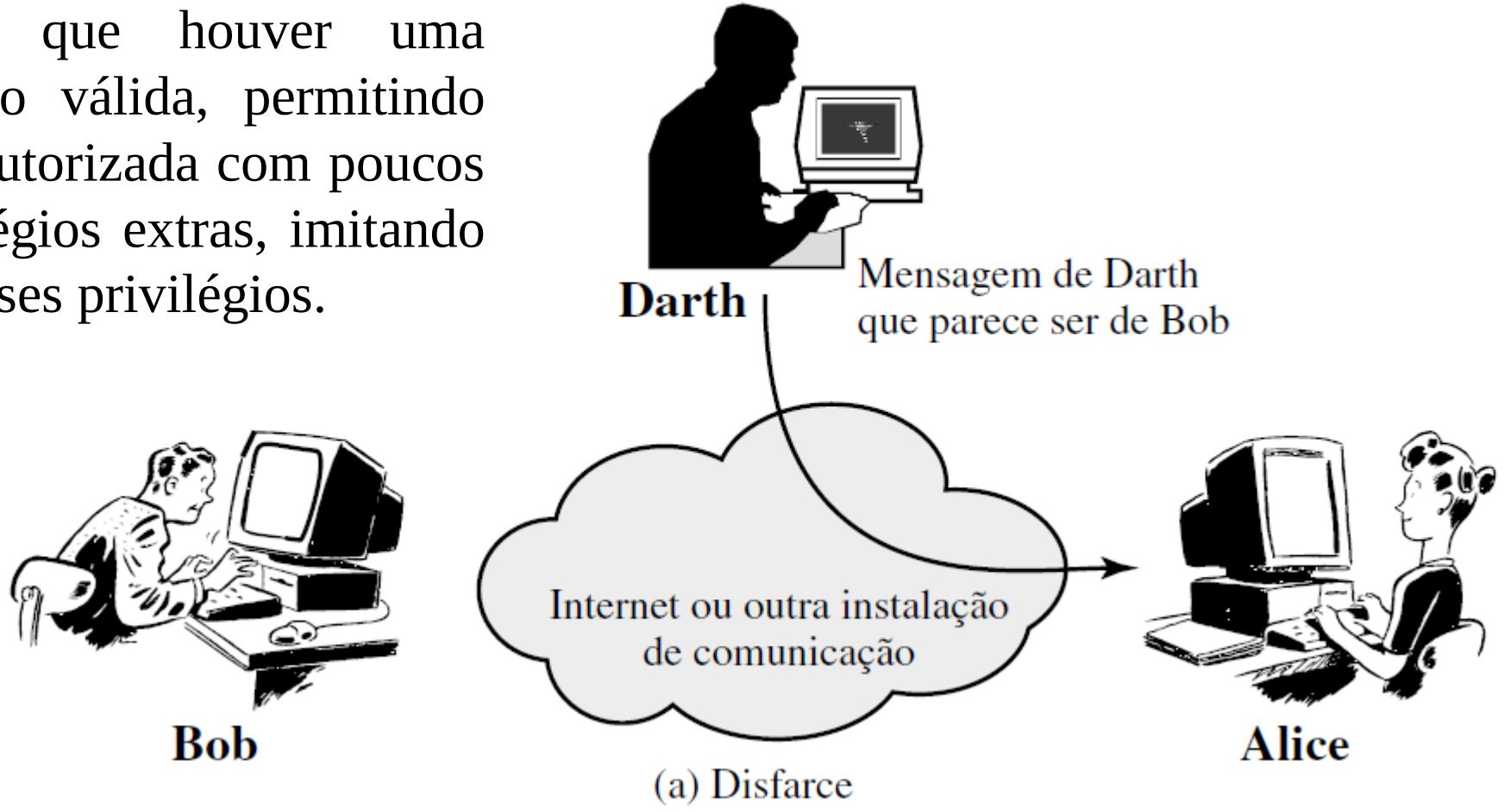


1.3 ATAQUES À SEGURANÇA

- Ataques ativos
  - Ataques ativos envolvem alguma modificação do fluxo de dados ou a criação de um fluxo falso e podem ser subdivididos em quatro categorias: disfarce, repetição, modificação de mensagens e negação de serviço.

Disfarce

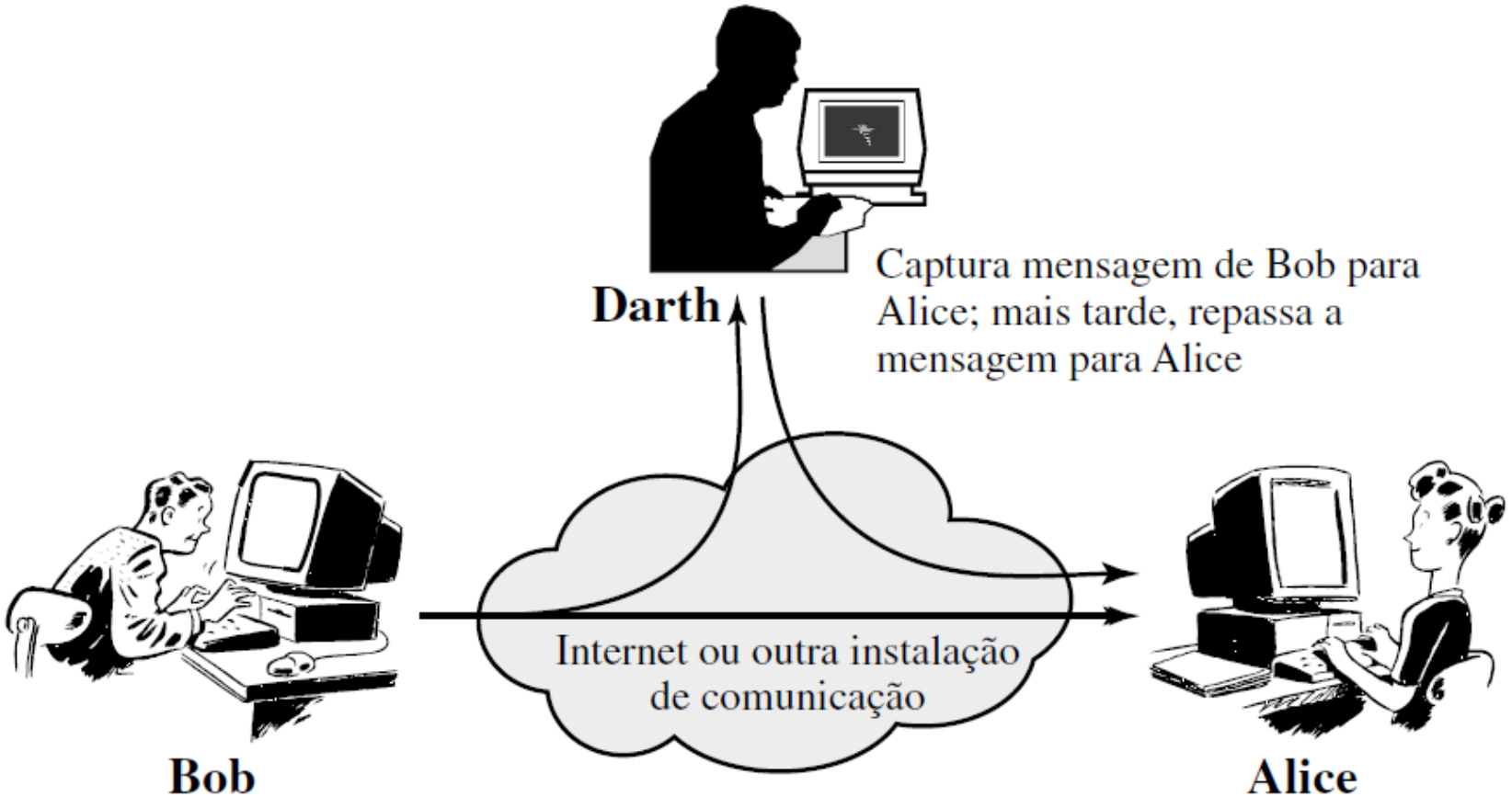
Um **disfarce** ocorre quando uma entidade finge ser uma entidade diferente (Figura a). Um ataque de disfarce normalmente inclui uma das outras formas de ataque ativo. Por exemplo, sequências de autenticação podem ser captadas e reproduzidas depois que houver uma sequência de autenticação válida, permitindo assim que uma entidade autorizada com poucos privilégios obtenha privilégios extras, imitando uma entidade que tenha esses privilégios.



(a) Disfarce

Repasse

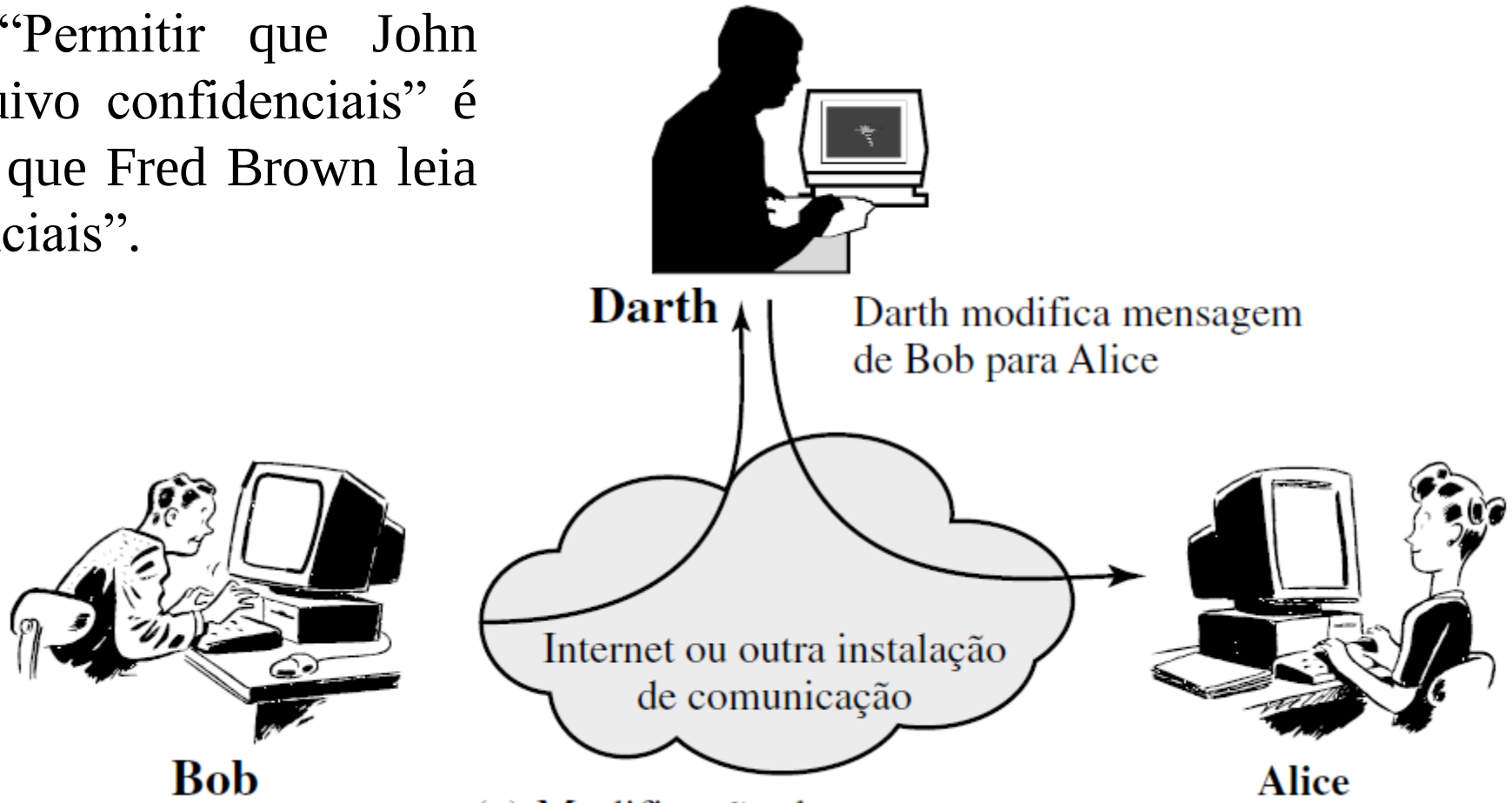
O **repasse** envolve a captura passiva de uma unidade de dados e sua subsequente retransmissão para produzir um efeito não autorizado (Figura b).



(b) Repasse

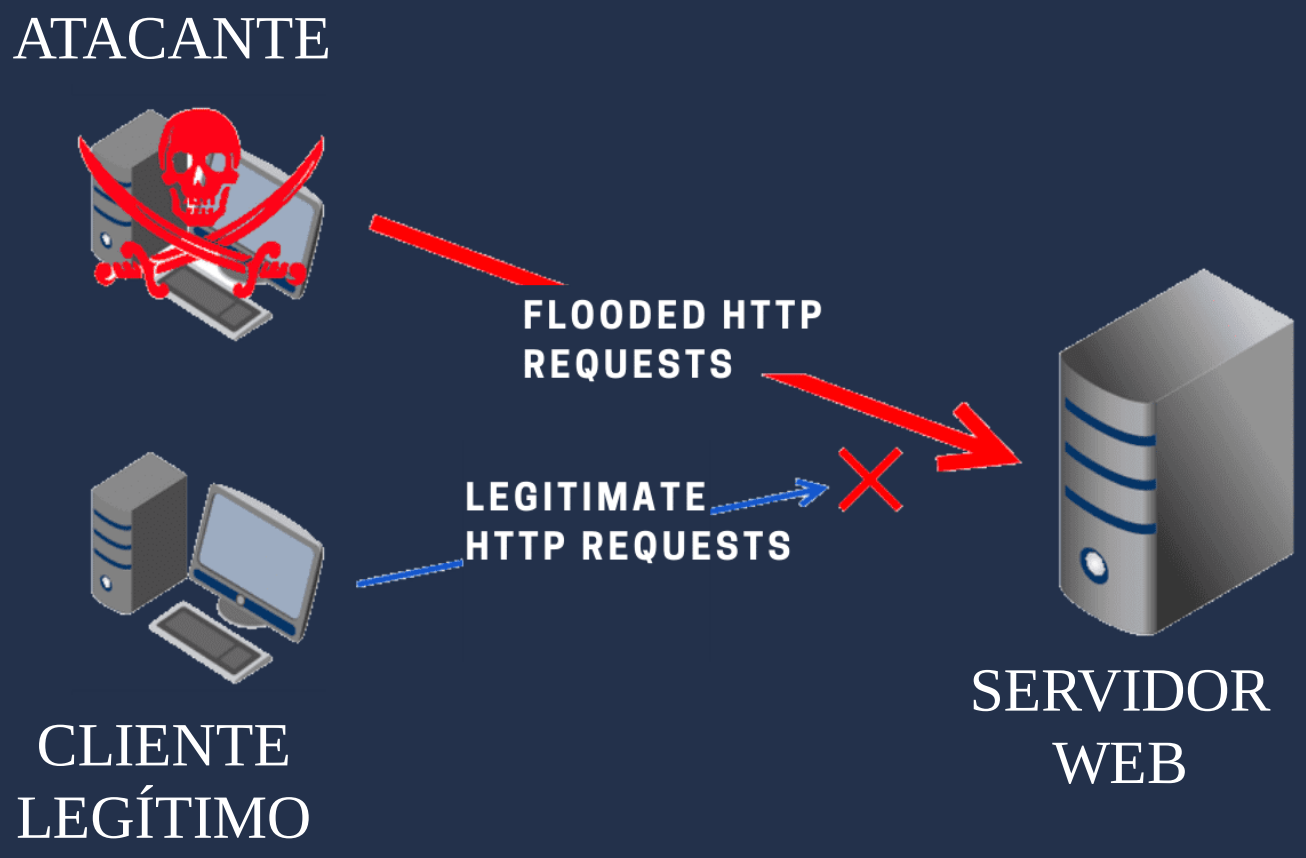
Modificação de mensagens

A **modificação de mensagens** simplesmente significa que alguma parte de uma mensagem legítima foi alterada ou que as mensagens foram adiadas ou reordenadas para produzir um efeito não autorizado (Figura c). Por exemplo, uma mensagem significando "Permitir que John Smith leia *contas* de arquivo confidenciais" é modificada para "Permitir que Fred Brown leia *contas* de arquivo confidenciais".



(c) Modificação de mensagens

DENIAL OF SERVICE ATTACKS



A **negação de serviço** impede ou inibe o uso ou gerenciamento normal das instalações de comunicação. Esse ataque pode ter um alvo específico; por exemplo, uma entidade pode suprimir todas as mensagens dirigidas a determinado destino (por exemplo, o serviço de auditoria de segurança). Outra forma de negação de serviço é a interrupção de uma rede inteira, seja desativando a rede ou sobrecarregando-a com mensagens, a fim de prejudicar o desempenho.

1.4 SERVIÇOS DE SEGURANÇA

- **SERVIÇO DE SEGURANÇA É** Um serviço de processamento ou comunicação que é fornecido por um sistema para prover um tipo específico de proteção aos recursos do sistema; os serviços de segurança implementam políticas (ou diretrizes) de segurança e são implementados por mecanismos de segurança.

1.4 SERVIÇOS DE SEGURANÇA

- **SERVIÇO DE SEGURANÇA**
  - Autenticação
  - Controle de acesso
  - Confidencialidade dos dados
  - Integridade de dados
  - Irretratabilidade
  - Disponibilidade

AUTENTICAÇÃO

- O serviço de autenticação refere-se à garantia de que uma comunicação é autêntica. No caso de uma única mensagem, a função do serviço de autenticação é garantir ao destinatário que a mensagem é proveniente de onde ela afirma ter vindo.
- No caso de uma interação de saída, como a conexão de um terminal com um hospedeiro, dois aspectos estão envolvidos.
  - Primeiro, no momento do início da conexão, o serviço garante que as duas entidades são autênticas.
  - Segundo, o serviço precisa garantir que a conexão não sofra interferência de modo que um terceiro possa fingir ser uma das duas partes legítimas, para fins de transmissão ou recepção não autorizada.

AUTENTICAÇÃO

- Dois serviços de autenticação específicos são definidos na X.800:

Autenticação da entidade par:

- Provê a confirmação da identidade de uma entidade par de uma associação. O serviço é fornecido para uso no estabelecimento de uma conexão ou, às vezes, durante a fase de transferência de dados. Ele tem a intenção de garantir que uma entidade não está disfarçada ou realizando uma repetição não autorizada de uma conexão anterior.

AUTENTICAÇÃO

Autenticação da origem de dados:

- Provê a confirmação da origem de uma unidade de dados. Não oferece proteção contra a duplicação ou a modificação das unidades de dados. Esse tipo de serviço dá suporte a aplicações como correio eletrônico, nas quais não existem interações anteriores entre as entidades que se comunicam.

CONTROLE DE ACESSO

- No contexto da segurança de redes, o controle de acesso é a capacidade de limitar e controlar o acesso aos sistemas e aplicações hospedeiras por meio de enlaces de comunicação. Para conseguir isso, cada entidade precisa ser identificada antes de obter acesso, ou autenticada, de modo que os direitos de acesso possam ser ajustados ao indivíduo.

CONFIDENCIALIDADE DE DADOS

- Confidencialidade é a proteção dos dados transmitidos contra ataques passivos. Com relação ao conteúdo de uma transmissão de dados, vários níveis de proteção podem ser identificados. O serviço mais amplo protege todos os dados transmitidos entre dois usuários por um período de tempo.
  - Por exemplo, quando uma conexão TCP é estabelecida entre dois sistemas, essa ampla proteção impede a divulgação de quaisquer dados do usuário transmitidos pela conexão TCP.

INTEGRIDADE DE DADOS

- A integridade pode se aplicar a um fluxo de mensagens, a uma única mensagem ou a campos selecionados dentro de uma mensagem. Novamente, a técnica mais útil e direta é a proteção total do fluxo.

INTEGRIDADE DE DADOS

- Um serviço de integridade orientado à conexão, que lida com um fluxo de mensagens, garante que elas sejam recebidas conforme enviadas, sem duplicação, inserção, modificação, reordenação ou repasses.
- A destruição dos dados também está coberta sob esse serviço. Assim, o serviço de integridade orientada à conexão relaciona-se tanto à modificação do fluxo de mensagem quanto à negação de serviço. Por outro lado, um serviço de integridade sem conexão, que lida com mensagens individuais sem considerar qualquer contexto maior, geralmente oferece proteção apenas contra modificação da mensagem.

IRRETRATABILIDADE (NÃO RETRATAÇÃO)

- A irretratabilidade impede que o emissor ou o receptor neguem uma mensagem transmitida. Assim, quando uma mensagem é enviada, o receptor pode provar que o emissor alegado de fato a transmitiu. De modo semelhante, quando uma mensagem é recebida, o emissor pode provar que o receptor alegado de fato a obteve.

SERVIÇO DE DISPONIBILIDADE

- Tanto X.800 quanto RFC 4949 definem a disponibilidade como a propriedade de um sistema ou de um recurso do sistema de ser acessível e utilizável sob demanda por uma entidade autorizada, de acordo com especificações de desempenho
  - Um sistema está disponível se oferecer serviços de acordo com a sua arquitetura sempre que for solicitado pelos usuários.

SERVIÇO DE DISPONIBILIDADE

- Diversos ataques podem resultar na perda ou na redução da disponibilidade. Alguns deles são favoráveis a contramedidas automatizadas, como autenticação e **encriptação**, enquanto outros exigem algum tipo de ação física para impedir ou recuperar-se da perda de disponibilidade dos elementos de um sistema distribuído.

1.5 MECANISMOS DE SEGURANÇA

- Os mecanismos são divididos entre aqueles implementados em uma camada de protocolo específica, como TCP ou protocolo da camada de aplicação, e aqueles que não são específicos a camadas de protocolo ou serviços de segurança em particular.
  - MECANISMOS DE SEGURANÇA ESPECÍFICOS
  - MECANISMOS DE SEGURANÇA DIFUSOS

MECANISMOS DE SEGURANÇA ESPECÍFICOS

- Codificação.
- Assinatura digital.
- Controle de acesso.
- Integridade de dados.
- Troca de autenticação.
- Preenchimento de tráfego.
- Controle de roteamento.
- Notarização.

MECANISMOS DE SEGURANÇA ESPECÍFICOS

- **Codificação**
  - O uso de algoritmos matemáticos para transformar os dados para um formato que não seja prontamente inteligível. a transformação e subsequente recuperação dos dados depende de um algoritmo e zero ou mais chaves de **encriptação**.
- **Assinatura digital**
  - Dados anexados a (ou uma transformação criptográfica de) uma unidade de dados que permite que um destinatário dela prove sua origem e integridade e a proteja contra falsificação (por exemplo, pelo destinatário).

MECANISMOS DE SEGURANÇA ESPECÍFICOS

- **Controle de acesso**
  - Uma série de mecanismos que impõem direitos de acesso os recursos.
- **Integridade de dados**
  - Uma série de mecanismos utilizados para garantir a integridade de uma unidade de dados ou fluxo de unidades de dados.
- **Troca de autenticação**
  - Um mecanismo intencionado a garantir a identidade de uma entidade por meio da troca de informações.

MECANISMOS DE SEGURANÇA ESPECÍFICOS

- **preenchimento de tráfego**
  - A inserção de bits nas lacunas de um fluxo de dados para frustrar as tentativas de análise de tráfego.
- **Controle de roteamento**
  - Permite a seleção de determinadas rotas fisicamente seguras para certos dados e mudanças de roteamento, sobretudo quando uma brecha de segurança é suspeitada.
- **Notarização**
  - O uso de um terceiro confiável para garantir certas propriedades de uma troca de dados.

MECANISMOS DE SEGURANÇA DIFUSOS

- Funcionalidade confiada.
- Rótulo de segurança.
- Detecção de evento.
- Trilha de auditoria de segurança.
- Recuperação de segurança.

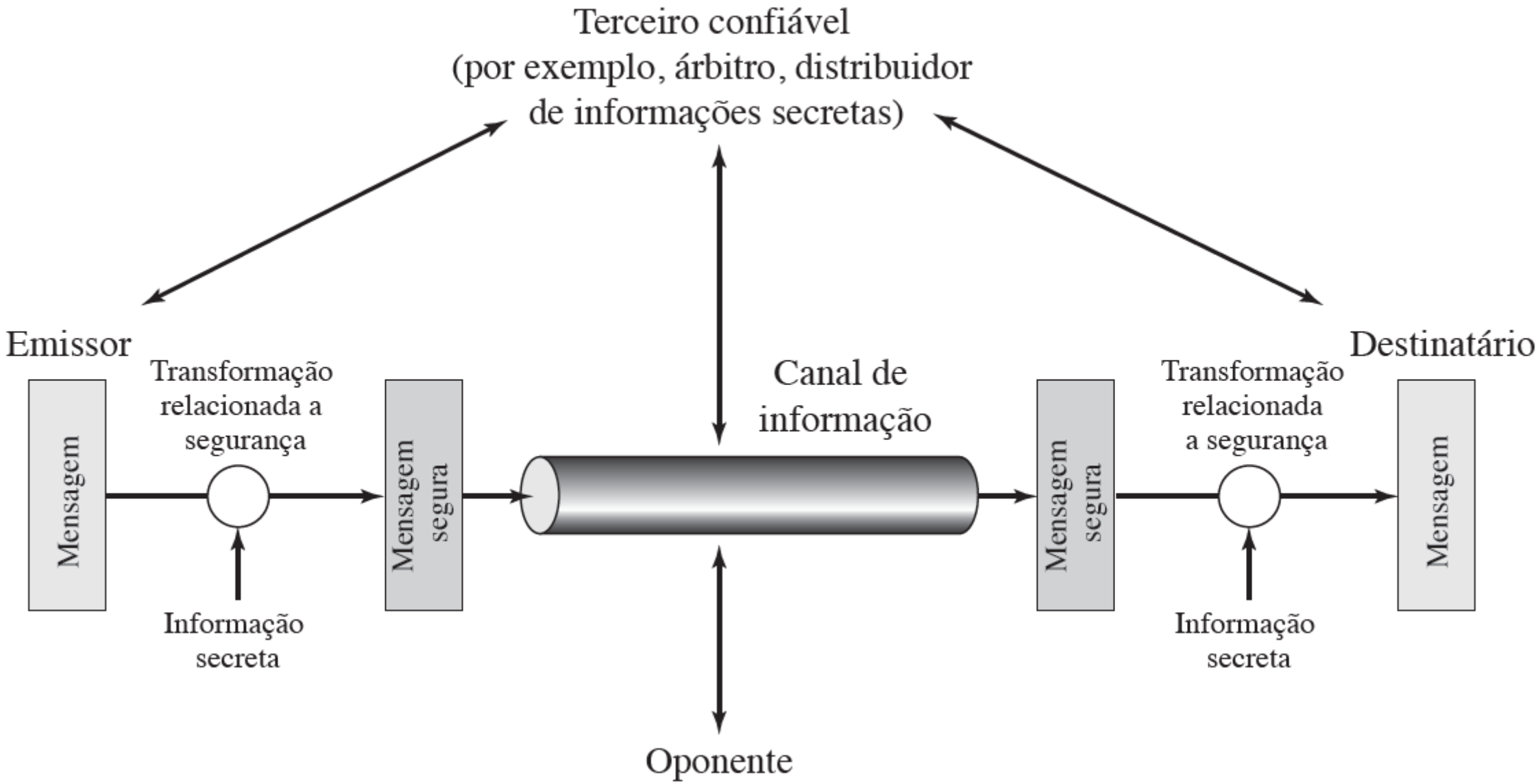
MECANISMOS DE SEGURANÇA DIFUSOS

- **Funcionalidade confiada**
  - Aquilo que é percebido como sendo correto com relação a alguns critérios (por exemplo, conforme estabelecido por uma política de segurança).
- **Rótulo de segurança**
  - A marcação vinculada a um recurso (que pode ser uma unidade de dados) que nomeia ou designa os atributos de segurança desse recurso.
- **Detecção de evento**
  - Detecção de eventos relevantes à segurança.
- **Trilha de auditoria de segurança**
  - Dados coletados e potencialmente utilizados para facilitar uma auditoria de segurança, que é uma revisão e exame independentes dos registros e das atividades do sistema.
- **Recuperação de segurança**
  - Lida com solicitações de mecanismos, como funções de tratamento e gerenciamento de eventos, e toma medidas de recuperação.

Relacionamento entre serviços e mecanismos de segurança.

SERVIÇO \ MECANISMO	Codificação	Assinatura digital	Controle de acesso	Integridade de dados	Troca de autenticação	Preenchimento de tráfego	Controle de roteamento	Notarização
Autenticação de entidade pareada	S	S			S			
Autenticação da origem de dados	S	S						
Controle de acesso			S					
Confidencialidade	S						S	
Confidencialidade do fluxo de tráfego	S					S	S	
Integridade de dados	S	S		S				
Responsabilização		S		S				S
Disponibilidade				S	S			

UM MODELO PARA SEGURANÇA DE REDE



MECANISMOS DE SEGURANÇA DIFUSOS

- Os aspectos de segurança entram em cena quando é necessário ou desejável proteger a transmissão de informações de um oponente que pode apresentar uma ameaça à confidencialidade, autenticidade, e assim por diante. As técnicas para oferecer segurança possuem dois componentes:
  - Uma transformação relacionada à segurança sobre a informação a ser enviada. Alguns exemplos incluem a encriptação da mensagem, que a "embaralha" de modo que fique ilegível pelo oponente, e o acréscimo de um código com base no conteúdo da mensagem, que pode ser usado para verificar a identidade do emissor.
  - Alguma informação secreta compartilhada pelos dois principais e, espera-se, ser desconhecida do oponente. Um exemplo é uma chave de encriptação usada com a transformação para embaralhar a mensagem antes da transmissão e desembaralhá-la no recebimento.

UM MODELO DE SEGURANÇA DE ACESSO À REDE


BREAK
TIME!!!

- FIM