

Segurança

CST em Análise e Desenvolvimento de Sistemas

Prof. Emerson Ribeiro de Mello

mello@ifsc.edu.br

Licenciamento



Slides licenciados sob [Creative Commons “Atribuição 4.0 Internacional”](#)

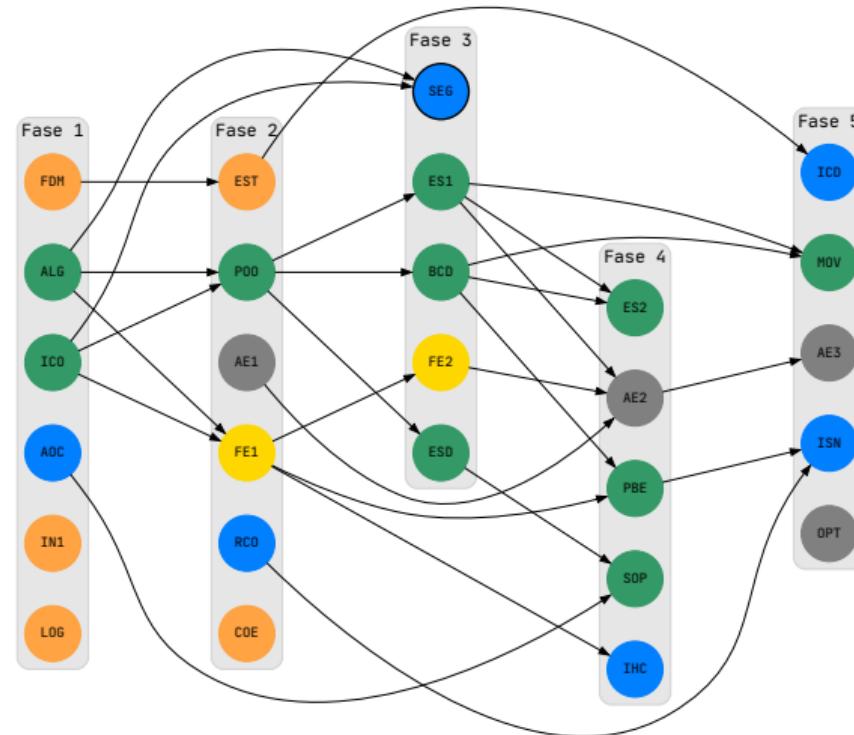
Sumário

- 1 Apresentação da disciplina
- 2 Ferramentas para essa disciplina
- 3 Introdução à segurança

Apresentação da disciplina

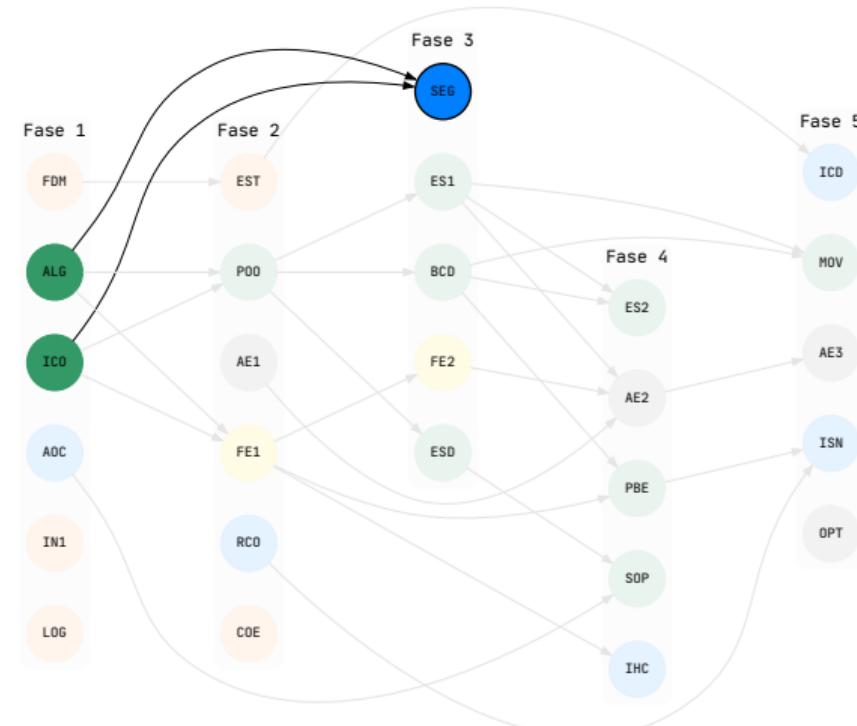
Relação com outras unidades curriculares

<https://sigaa.ifsc.edu.br/sigaa/link/public/curso/curriculo/54017903>



Relação com outras unidades curriculares

<https://sigaa.ifsc.edu.br/sigaa/link/public/curso/curriculo/54017903>



Pré-requisitos dessa disciplina

Introdução à computação (ICO)

- 1 Saber instalar e configurar programas no Linux
- 2 Saber utilizar o terminal e os comandos básicos do Linux
- 3 Saber lidar com arquivos, diretórios, caminhos e variáveis de ambiente
- 4 Saber utilizar o Git no terminal (*init, add, commit, branch, merge, checkout*)
- 5 Saber utilizar o GitHub (*push, pull, clone*) e autenticação via PAT
- 6 Saber navegar na Internet pelo computador e usar email de forma efetiva
- 7 Saber usar o SIGAA

Pré-requisitos dessa disciplina

Pensamento computacional e algoritmos (ALG)

- 1 Saber criar algoritmos utilizando fluxogramas e pseudocódigo
- 2 Saber realizar teste de mesa
- 3 Saber criar algoritmos utilizando a linguagem de programação Java
 - estruturas de decisão e repetição
 - vetores e matrizes
 - leitura de dados do teclado e escrita em tela

Ementa

Propriedades básicas de segurança; Ameaças, ataques e vulnerabilidades; Principais técnicas de ataque e softwares maliciosos; Modelos de gestão de identidade e de acesso. Mecanismos de segurança para autenticação, autorização e controle de acesso; Técnicas e algoritmos de criptografia simétrica e assimétrica; Privacidade e usabilidade; Legislação e padrões na área de segurança da informação. Desenvolvimento de aplicações que façam uso de mecanismos de segurança.

Objetivos da disciplina

- Compreender as propriedades básicas de segurança
- Conhecer os principais tipos de ataques e os diferentes tipos de softwares maliciosos
- Conhecer leis e normas relacionadas a segurança
- Aplicar técnicas e algoritmos de criptografia
- Implementar mecanismos de segurança em sistemas de informação

Metodologia

- Aulas expositivas-dialogadas e práticas em laboratório sob a supervisão do professor
- Metodologia de aprendizado baseado em projetos, em que desafios são lançados e o docente orienta os estudantes em suas soluções

Horários

■ Aulas: Laboratório de Redes



- 20:40 – 22:30 - terça-feira
- 20:40 – 22:30 - quinta-feira

■ Atendimento extraclasse: Sala de Professores de Tele I



- 13:30 – 15:30 - terça-feira



Interações do professor com a turma será por meio do SIGAA ou email

Instrumentos de avaliação

Atividade	Quantidade	Sigla	Tipo	Peso
Avaliação escrita	2	<i>a</i>	individual	80%
Seminário	1	<i>s</i>	grupo	10%
Participação	-	<i>p</i>	individual	10%

$$\text{Conceito Final} = \left[\left(\frac{\sum_{i=1}^2 a_i \times w_i}{\sum_{i=1}^2 w_i} \right) \times 0,8 + s \times 0,1 + p \times 0,1 \right] \quad (1)$$

- Pesos das avaliações: $W = \{w_1, w_2\} = \{3, 2\}$

Sobre a recuperação de estudos

- Para aqueles com frequência igual ou superior a 75% e que realizaram¹ as avaliações escritas, mas que não atingiram a nota mínima (6)
 - O conteúdo da avaliação de recuperação abrangerá todo o conteúdo referente a avaliação que o discente não obteve a nota mínima
 - A nota da avaliação de recuperação substituirá a nota da avaliação que está sendo recuperada
- Não haverá recuperação para o seminário e participação, pois são avaliados de forma contínua e o discente tem a oportunidade de melhorar sua nota ao longo do semestre

¹ Salvo os casos previstos no artigo 162 do Regulamento Didático-Pedagógico (RDP) do IFSC, no RDP não está previsto a segunda chamada, situação que ocorre quando o discente não faz a atividade avaliativa na data estabelecida.

Fraude no processo avaliativo

- O **plágio é estritamente proibido**, seja ao copiar trabalhos de colegas, de repositórios *online* ou ao utilizar ferramentas de Inteligência Artificial (e.g. Copilot, ChatGPT etc) para obter a solução completa ou parcial de atividades avaliativas.
- **Caso seja identificado plágio ou fraude, o discente receberá nota 0** na atividade em questão, sem direito à recuperação. Além disso, o caso será encaminhado à coordenação do curso para registro no histórico escolar do discente e aplicação das medidas disciplinares cabíveis.

Bibliografia básica

-  SANTOS BARRETO, Jeanine dos et al. **Fundamentos de Segurança da Informação.** 1. ed. Porto Alegre: Sagah, 2018. ISBN 9788595025875.
Disponível em: <<https://app.minhabiblioteca.com.br/#/books/9788595025875>>.
-  STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e Práticas.** 4. ed. São Paulo: Pearson Prentice Hall, 2007. Tradução da 4^a edição norte-americana. ISBN 9788576050673.

Bibliografia complementar

-  FOROUZAN, Behrouz A.; MOSHARRAF, Firouz. **Redes de Computadores: Uma Abordagem Top-Down**. 5. ed. Porto Alegre: AMGH, 2013. ISBN 9788580551693. Disponível em:
[<https://app.minhabiblioteca.com.br/reader/books/9788580551693>](https://app.minhabiblioteca.com.br/reader/books/9788580551693).
-  HORSTMANN, Cay S.; CORNELL, Gary. **Core Java – Volume I – Fundamentos**. 8. ed.: Pearson, 2010.
-  SILBERSCHATZ, Abraham; GALVIN, Peter Baer; GAGNE, Greg. **Fundamentos de Sistemas Operacionais**. 9. ed. Porto Alegre: AMGH, 2015. ISBN 9788521630012. Disponível em:
[<https://integrada.minhabiblioteca.com.br/#/books/978-85-216-3001-2>](https://integrada.minhabiblioteca.com.br/#/books/978-85-216-3001-2).

Ferramentas para essa disciplina

Ferramentas para essa disciplina

- **Sistema operacional:** Linux
- **Linguagem de programação:** Java
- **Ferramenta de automatização de projetos:** Gradle
- **Repositório de código:** GitHub



Desejável que tenha cursado as disciplinas de POO, RCO e FE1

Introdução à segurança

Segurança computacional, cibersegurança ou segurança cibernética

Consiste em proteger sistemas de computadores, redes de computadores e dados contra ataques, danos ou acessos não autorizados de forma a garantir a confidencialidade, integridade e disponibilidade dos sistemas e dados

- Como evitar que uma pessoa, com acesso físico ao telefone, possa fazer ligações?



Fonte: Google Images

- Como evitar que uma pessoa, com acesso físico ao telefone, possa fazer ligações?
- **Resposta:** Adicione um cadeado ao telefone!



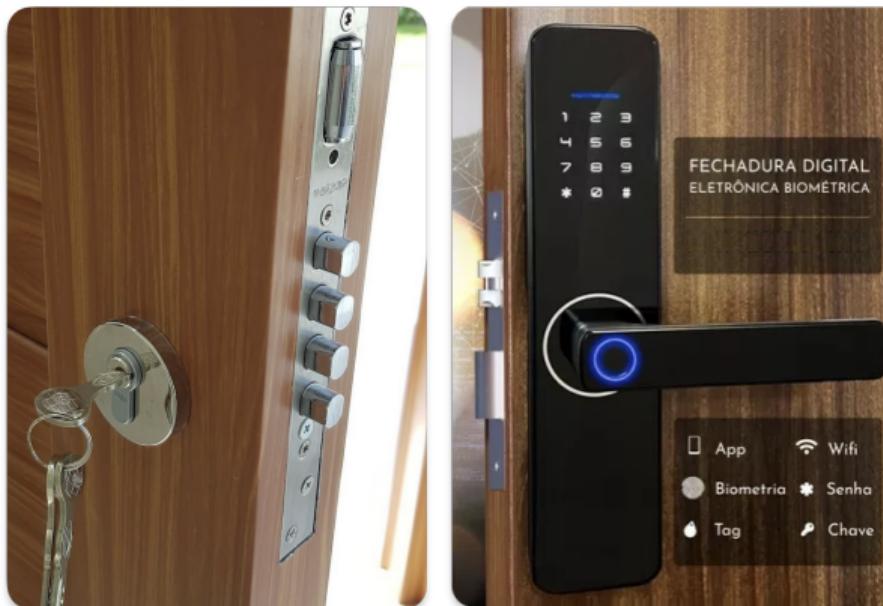
Fonte: Google Images

- Como evitar que uma pessoa, com acesso físico ao telefone, possa fazer ligações?
- **Resposta:** Adicione um cadeado ao telefone!
- Resolveu o problema ou apenas limitou o acesso de pessoas com menos habilidades?



Fonte: Google Images

Qual das duas fechaduras é menos suscetível de ser aberta por uma pessoa não autorizada?



Fonte: Google Images

Fonte: Google Images

Qual das duas fechaduras é menos suscetível de ser aberta por uma pessoa não autorizada?

- É possível ser aberta por pessoas com habilidade, ferramentas, tempo e acesso físico ao local



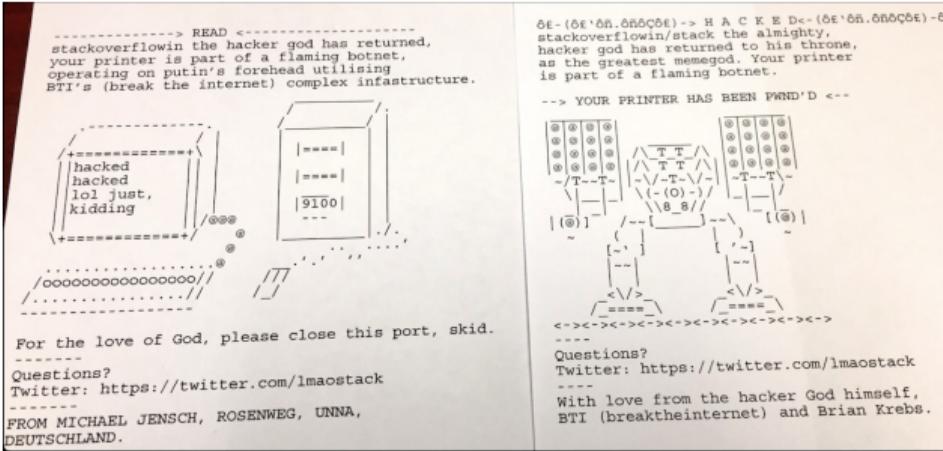
Fonte: Google Images



Fonte: Google Images

- É possível ser aberta por pessoas com habilidade, ferramentas, tempo e NÃO precisa ter acesso físico ao local

Alguns casos relacionados à cibersegurança



Fonte: <https://twitter.com/StephSanchezPhD/status/828670493377040385>

- 2017 um hacker invadiu 160 mil impressoras conectadas à Internet e fez com que elas imprimissem arte ASCII e um aviso para fecharem as portas²

²https://www.theregister.com/2017/02/06/hacker_160000_printers/

Alguns casos relacionados à cibersegurança

- Em 2015 pesquisadores mostraram que era possível hackear um carro Jeep Cherokee e controlar remotamente o sistema de freios, motor e outros sistemas
- Carros antigos sem conexão à Internet não são vulneráveis a esse tipo de ataque, porém atualmente a maioria dos carros novos possuem conexão à Internet



Fonte: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway>

Você pode participar de um ataque sem saber

- Em 2013, Corporação Target teve dados de 70 milhões de clientes e de 40 milhões de cartões de crédito roubados.
 - Criminosos roubaram credenciais de acesso de um fornecedor de equipamentos de ar-condicionado da empresa.
- Em 2016, hackers recrutaram milhões de dispositivos IoT para uma *botnet* massiva chamada Mirai, usando-a para lançar um ataque DDoS contra o provedor de nome de domínio Dyn
- Em 2017, hackers invadiram a rede de um cassino por um aquário conectado à Internet e roubaram dados

Nexx Smart Wi-Fi Garage Door

<https://www.cisa.gov/news-events/ics-advisories/icsa-23-094-01>

- Todos dispositivos compartilham a mesma credencial de acesso aos servidores MQTT da Nexx
- Dados pessoais do cliente, ID do dispositivo e comandos para abrir ou fechar o portão são enviados sem qualquer criptografia
- 04/jan/2023 – pesquisador entrou em contato com a empresa³
- Mais de 4 meses sem resposta



³<https://medium.com/@samsabetan/>

[the-uninvited-guest-idors-garage-doors-and-stolen-secrets-e4b49e02dad](https://medium.com/@samsabetan/the-uninvited-guest-idors-garage-doors-and-stolen-secrets-e4b49e02dad)

Qualidade de *software* e segurança

- Já usou algum *software* que travou ou que apresentou um comportamento errôneo?
 - Aprendemos a compensar esses problemas. Por exemplo, salvando o trabalho frequentemente
- Softwares estão repletos de *bugs*, sendo alguns deles inerentes à complexidade do *software*, relacionados a dependências externas (bibliotecas) e à falta de qualidade

Qualidade de *software* e segurança

- Já usou algum *software* que travou ou que apresentou um comportamento errôneo?
 - Aprendemos a compensar esses problemas. Por exemplo, salvando o trabalho frequentemente
- Softwares estão repletos de *bugs*, sendo alguns deles inerentes à complexidade do *software*, relacionados a dependências externas (bibliotecas) e à falta de qualidade

A maioria dos softwares é desenvolvida sem a preocupação com a segurança e a qualidade do *software* é frequentemente sacrificada em detrimento do prazo de entrega

Qualidade de *software* e segurança

- **Qualidade de *software*** é a conformidade com os requisitos funcionais e de desempenho, padrões de desenvolvimento e características implícitas que são esperadas de todo *software* desenvolvido profissionalmente
- **Segurança de *software*** é a conformidade com os requisitos de segurança de todo *software* desenvolvido profissionalmente

Segurança é sempre uma troca (SCHNEIER, 2020)

- Segurança vs funcionalidades
- Segurança vs conveniência (usabilidade)
- Segurança vs desempenho
- Segurança vs custo

Internet das coisas (IoT) e implicações de segurança

- Assistentes de voz, termostatos, câmeras de segurança, lâmpadas, geladeiras, máquinas de lavar roupa, ar condicionado, brinquedos, etc.
- Economia de mercado fará com que a maioria dos dispositivos eletrônicos tenham conexão à Internet
- E se houver uma vulnerabilidade de segurança em um desses dispositivos? Como seria possível corrigir? E se o fabricante não mais existir?



Fonte: <https://www.samsung.com.br/>

Internet das coisas (IoT) e implicações de segurança

*"Qualquer coisa conectada à Internet pode ser hackeada; Tudo está sendo conectado à Internet; Portanto, tudo está tornando-se vulnerável, Rod Beckstrom
(SCHNEIER, 2020)"*

A Internet foi projetada para ser robusta, não segura

- Foi projetada para ser
 - Aberta – qualquer dispositivo pode conectar
 - Robusta – roteamento mesmo diante de falhas em dispositivos
 - Escalável – crescer sem necessidade de reestruturar

A Internet foi projetada para ser robusta, não segura

- Foi projetada para ser
 - Aberta – qualquer dispositivo pode conectar
 - Robusta – roteamento mesmo diante de falhas em dispositivos
 - Escalável – crescer sem necessidade de reestruturar

Border Gateway Protocol (BGP)

- 2010, China anunciou rotas para 15% do tráfego da Internet por 18 minutos
- 2017, Rússia fez anúncios para 7% do tráfego da Internet por 8 minutos
- Graças a Edward Snowden, sabemos que a NSA abusa da insegurança da rede para interceptar tráfego

A Internet foi projetada para ser robusta, não segura

- Quando os protocolos foram propostos, a segurança não era uma preocupação, pois a rede era pequena e confiável
- No final da década de 1990, a IETF indicava que a segurança seria responsabilidade dos usuários finais e não da rede
 - Modelo de segurança fim-a-fim
- IETF apresentou propostas para melhorar segurança do BGP e outros protocolos
 - Muitos não foram amplamente adotados pelos provedores de Internet
 - Ser pioneiro é custoso e não traz retorno financeiro, uma vez que o restante da rede não adotou

Vulnerabilidade

Vulnerabilidade

Fraqueza do sistema que pode ser em termos de procedimentos, configuração ou implementação e que pode ser explorada por um atacante para violar a segurança do sistema

- Vulnerabilidades existem em *software* e *hardware*
 - Algumas podem ser descobertas facilmente e outras podem demorar anos para serem descobertas
 - Algumas podem ser corrigidas facilmente e outras podem ser impossíveis de corrigir

Catálogos de vulnerabilidades (CVE) e fraquezas (CWE)

- *Common Vulnerabilities and Exposures (CVE)*⁴ é um programa para identificar, definir e catalogar vulnerabilidades em cibersegurança que são conhecidas publicamente
 - Toda vulnerabilidade tem um identificador único (ex: CVE-2023-12345)
- *Common Weakness Enumeration (CWE)*⁵ é um catálogo de fraquezas que podem se tornar vulnerabilidades
 - Em 2023 as principais fraquezas ainda estão relacionadas com linguagens que lidam com memória de forma insegura⁶, como C e C++

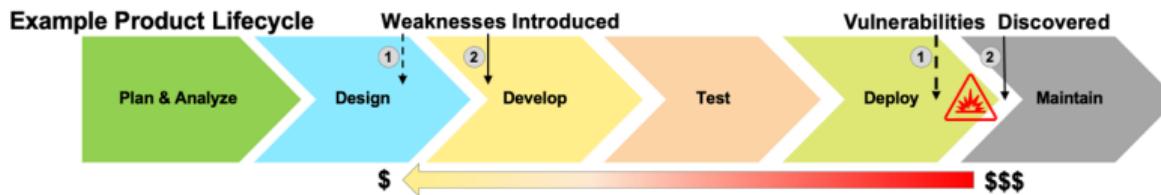
⁴<https://www.cve.org>

⁵<https://cwe.mitre.org/about/>

⁶<https://www.memoriesafety.org/docs/memory-safety>

Catálogo de fraquezas que podem se tornar vulnerabilidades

Common Weakness Enumeration (CWE)



Fonte: <https://cwe.mitre.org/about/>

"Conhecer as fraquezas de um software/hardware permite que desenvolvedores possam tomar medidas para mitigá-las antes da implantação, quando é mais barato e mais fácil"

- As 25 fraquezas mais perigosas de 2023⁷
 - Escrita fora dos limites de um *buffer* (CWE-787)
 - Validação de entrada incorreta em páginas web – Cross-site Scripting (CWE-79)
 - Validação de entrada incorreta em comandos SQL – SQL Injection (CWE-89)

⁷<https://cwe.mitre.org/data/definitions/1425.html>

Exemplo de vulnerabilidade em *hardware*

Spectre (CVE-2017-5753, CVE-2017-5715) e Meltdown (CVE-2017-5754)^{8,9}

- Falha de projeto de processadores da Intel x86 produzidos depois de 1995, mas alguns processadores AMD e ARM também são afetados
 - Demoraram dez anos para serem descobertas (2017) e afeta a maioria dos dispositivos eletrônicos
- Permite que um processo malicioso leia a memória de outros processos
 - Não explora qualquer vulnerabilidade de *software*
- Correções contra o Meltdown foram lançadas para Linux, Windows e macOS, mas impactam no desempenho (até 30%)
- Correções para o Spectre são mais difíceis de serem aplicadas e podem não ser eficazes

⁸<https://meltdownattack.com>

⁹<https://www.youtube.com/watch?v=RbHbFkh6eeE>

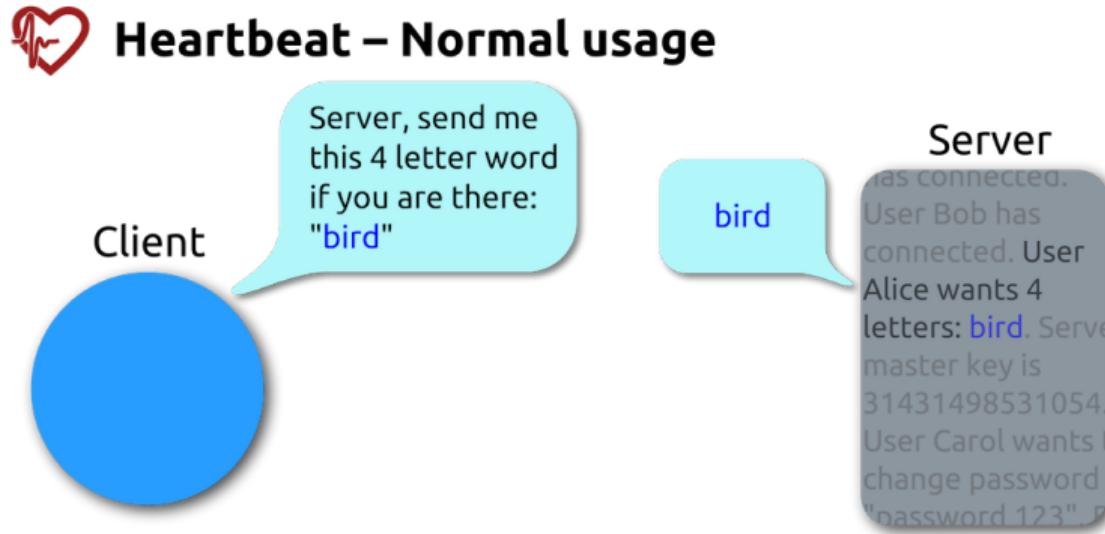
Exemplo de vulnerabilidade em *software*

Heartbleed (CVE-2014-0160)

- Vulnerabilidade introduzida em 2012 na biblioteca de criptografia de código aberto OpenSSL
 - Ficou oculta por mais de dois anos e foi **descoberta por dois pesquisadores independentes** como um intervalo de pouco dias entre as descobertas
- Um cliente malicioso (ex: cliente HTTP) poderia montar consultas de forma a ler além dos limites de um *buffer* e obter informações sensíveis da memória do servidor

Exemplo de vulnerabilidade em *software*

Heartbleed (CVE-2014-0160)



Fonte: <https://en.wikipedia.org/wiki/Heartbleed>

Exemplo de vulnerabilidade em *software*

Heartbleed (CVE-2014-0160)



Heartbeat – Malicious usage

Client

Server, send me
this 500 letter
word if you are
there: "bird"

bird. Server
master key is
31431498531054.
User Carol wants
to change
password to
"password 123"...

Server

was connected.
User Bob has
connected. User
Mallory wants 500
letters: bird. Serve
master key is
31431498531054.
User Carol wants to
change password
"password 123". P

Fonte: <https://en.wikipedia.org/wiki/Heartbleed>

Descoberta de vulnerabilidades

Como descobrir se o seu *software* possui vulnerabilidades?

- Existem técnicas manuais e automáticas para descobrir vulnerabilidades
 - Ex: *Fuzzing*, análise estática, análise dinâmica, revisão de código, teste de invasão, análise de *logs*, análise de tráfego, etc
- Existem ferramentas automáticas que ajudam a descobrir e corrigir vulnerabilidades no seu código
 - Ex: GitHub Dependabot, Snyk, mend.io, SonarQube, etc

Vulnerabilidade de dia zero

Zero-day vulnerability

- Vulnerabilidade que ainda não é conhecida pelo fabricante do *software* ou *hardware* ou que ainda não foi corrigida por esse
 - São as mais críticas e perigosas, pois os usuários não têm como se proteger
 - São descobertas por pesquisadores de segurança, *hackers* ou agências de inteligência
 - São vendidas e podem ser usadas em ataques direcionados
- **Google Project Zero**¹⁰ é um time de pesquisadores de segurança que buscam por vulnerabilidades de dia zero em *hardwares* e *softwares* dos quais usuários do mundo todo dependem
 - Participaram da descoberta das vulnerabilidades Spectre e Meltdown

¹⁰<https://googleprojectzero.blogspot.com>

Programa de recompensa por vulnerabilidades

Bug bounty

- **Bug bounty** é um programa de recompensa para pesquisadores que descobrem e relatam vulnerabilidades
 - <https://security.apple.com/bounty/>
 - <https://pt-br.facebook.com/whitehat/>
 - <https://www.google.com/about/appsecurity/reward-program/>
 - <https://www.microsoft.com/en-us/msrc/bounty>

Programa de recompensa por vulnerabilidades

Exemplo de recompensas do Bug bounty da Apple - 2024

Network attack without user interaction	Zero-click radio to kernel with physical proximity	\$5,000 – \$500,000
	Zero-click unauthorized access to sensitive data	\$5,000 – \$500,000
	Zero-click kernel code execution with persistence and kernel PAC bypass	\$100,000 – \$1,000,000

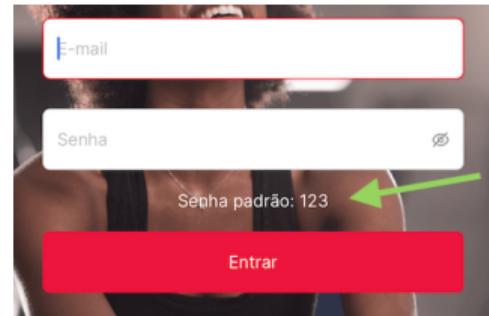
Fonte: <https://security.apple.com/bounty/categories/>

Segurança desde a concepção

Security by Design

- **Security by Design** é uma abordagem que visa a segurança desde o início do ciclo de vida do *software*
- Produtos de *software* que são seguros por padrão, sem a necessidade de configurações adicionais pelos usuários ou administradores
- Algumas publicações
 - <https://www.cisa.gov/resources-tools/resources/secure-by-design>
 - <https://research.google/pubs/secure-by-design-at-google/>

Insecure design



Março de 2024. Fonte: omitida

- Senha padrão para todos os novos usuários
- Senha apresentada na página de *login*

Exemplo de fraqueza: não autenticar para funções críticas

CWE-306: Missing Authentication for Critical Function - <https://cwe.mitre.org/data/definitions/306.html>

```
// Exemplo de código que não autentica para funções críticas
public class ManutencaoDeContas{

    public Conta criarConta(String numero, String nome, double saldo){
        Conta c = new Conta(numero, nome, saldo);
        return c;
    }

}
```

- O código acima não autentica o usuário antes de criar uma nova conta

Exemplo de fraqueza: não autenticar para funções críticas

CWE-306: Missing Authentication for Critical Function - <https://cwe.mitre.org/data/definitions/306.html>

```
// Exemplo de código que autentica para funções críticas
public class ManutencaoDeContas{

    private boolean autenticado = false;

    public void autenticar(String usuario, String senha){
        // código para autenticar
    }

    public Conta criarConta(String numero, String nome, double saldo){
        if (!autenticado){
            throw new SecurityException("Usuário não autenticado");
        }
        Conta c = new Conta(numero, nome, saldo);
        return c;
    }
}
```

Tempo entre a descoberta e a aplicação da correção

- Em 2017, o ataque WannaCry explorou uma vulnerabilidade que já havia sido corrigida pela Microsoft
- Muitos administradores não aplicam as correções imediatamente, pois temem que a correção possa quebrar o sistema
 - Julho de 2024 uma falha na atualização do software de segurança CrowdStrike¹¹ fez com que sistemas Windows ficassem inoperantes
- Muitos usuários não aplicam as correções imediatamente, pois não sabem da existência da correção

¹¹https://en.wikipedia.org/wiki/2024_CrowdStrike_incident

Ameaça

Qualquer evento, ação, pessoa ou entidade que tem o potencial de causar danos a um sistema ou organização

- Ameaças podem ser intencionais (usuários maliciosos) ou não intencionais (desastre natural, erro humano etc)

Ataque

Concretização de uma ameaça, explorando uma vulnerabilidade para causar danos a um sistema ou organização

- Ataques podem ser direcionados ou indiscriminados
- Ataques podem ser de curto ou longo prazo

Ataques estão ficando mais fáceis, baratos e eficazes

Padrão de criptografia DES

- 1975 – DES (*Data Encryption Standard*) é proposto
- 1976 – Especialistas estimaram que seria necessário US\$ 20 milhões para quebrá-lo
- 1997 – DES foi quebrado por menos de US\$ 250 mil
- 2012 – Pesquisadores quebraram o DES em 2 dias usando uma máquina de US\$ 10 mil
- Hoje – É possível quebrar o DES em minutos usando um computador pessoal

Ataques estão ficando mais fáceis, baratos e eficazes

Telefonia celular

- 1990 – Telefones celulares foram projetados para confiar em qualquer torre de celular
 - Era complexo para o telefone verificar se a torre era legítima
 - Era caro implantar torres falsas
- 1995 – FBI e CIA dispunham de torres falsas em seus carros¹²
- 2000 – Implantar torres falsas era tão fácil e barato que isso era demonstrado em conferências de segurança

¹²2024 – Tem carro com ERB falsa rodando por SP – <https://g1.globo.com/sp/sao-paulo/noticia/2024/07/25/carro-do-golpe-policia-investiga-quadrilha-que-usa-veiculo-com-antena-e-computador-para-rastrear-celulares-e-aplicar-golpes-em-sp.ghtml>

Ataques estão ficando mais fáceis, baratos e eficazes

Senhas de computador

- A velocidade dos computadores está aumentando de maneira exponencial, tornando-os mais rápidos para quebrar senhas e criptografias por **força bruta**
 - Método de ataque que tenta todas as combinações possíveis de uma senha
- A nossa capacidade em memorizar senhas longas e complexas não está aumentando na mesma velocidade
 - Senhas longas e complexas são difíceis de serem lembradas
 - Senhas curtas e simples são fáceis de serem quebradas (data de nascimento, nome do cachorro, placa do carro, etc)
- Senhas que poderiam ser seguras dez anos atrás, hoje não são mais
 - 5Wij247C, Mu1t0D1f1c11, f0nt3H4ck3r, P@ssw0rd!

Cibersegurança

Envolve **pessoas, processos e tecnologia** para **proteger** a informação de **ameaças e garantir a continuidade** do negócio

"Segurança é um processo contínuo e não um produto"

Bruce Schneier

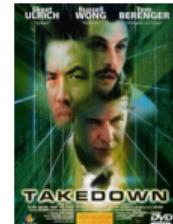
Pessoas

Não importa o quanto robusto seja um controle técnico de segurança, se critérios não técnicos afetarem sua implementação ou uso, então a segurança pode ficar fragilizada



- Repetição de padrões nas mensagens transmitidas pela Enigma
- <http://www.imdb.com/title/tt2084970>

- Kevin Mitnick, um dos hackers mais famosos, disse que a engenharia social é a forma mais eficaz de invasão
- <http://www.imdb.com/title/tt0159784>



Política de segurança

- **Diretrizes** indicam o que usuários ou processos podem ou não fazer
- **Normas** indicam como deverá ser feito
- **Procedimentos** que devem ser tomados em cada estado do sistema

- **Normas ISO/IEC/NBR 27000** são um conjunto de normas internacionais que fornecem diretrizes e práticas para a gestão da segurança da informação
 - Guia de boas práticas
 - Gestão de risco
 - Gestão de incidentes

Tecnologia

■ Proteção física

- Cadeado, cofre, câmera de segurança, leitor biométrico

■ Proteção no dispositivo do usuário e na rede de computadores

- Antivírus, firewall, IDS, IPS

■ Proteção de dados

- Criptografia
- Cópia de segurança (*backup*)

■ Autenticação e autorização

- LDAP, Microsoft Entra ID, Keycloak
- OAuth, SAML, OpenID Connect, SSO, MFA
- ACL, RBAC

Propriedades básicas de segurança

Confidentiality, Integrity, Availability (CIA triad)



Fonte: Operational Technology

Cybersecurity for Energy Systems

■ Confidencialidade

- A informação só deve ser revelada para usuários autorizados

■ Integridade

- A informação não deve ser alterada, destruída ou perdida, de maneira não autorizada ou acidental

■ Disponibilidade

- A informação deve estar disponível quando necessário

É necessário garantir as três propriedades para que a informação seja considerada segura

Confidencialidade

- Confidencialidade deve ser garantida durante a transmissão, processamento e armazenamento da informação
- A confidencialidade pode ser garantida por meio de mecanismos como criptografia e controle de acesso
- **Se a confidencialidade não for garantida**, então tem-se uma revelação não autorizada de informação

Confidencialidade

- Confidencialidade deve ser garantida durante a transmissão, processamento e armazenamento da informação
- A confidencialidade pode ser garantida por meio de mecanismos como criptografia e controle de acesso
- **Se a confidencialidade não for garantida**, então tem-se uma revelação não autorizada de informação



Privacidade é um aspecto da confidencialidade, mas não é a mesma coisa. Privacidade é a capacidade de controlar a informação sobre si mesmo. A confidencialidade é a capacidade de controlar a informação de forma geral

Integridade

- Somente partes autorizadas podem alterar a informação
 - Também garante o não repúdio e a autenticidade da informação
- A integridade pode ser verificada por meio de mecanismos como *checksum* e assinaturas digitais
 - Tais mecanismos não impedem a alteração, mas permitem detectá-la
- **Se a integridade não for garantida**, então tem-se uma alteração não autorizada ou destruição da informação

Disponibilidade

- A informação deve estar disponível quando necessário
- Pode-se garantir a disponibilidade por meio de redundância, backups, sistemas de energia ininterrupta, etc
- **Se a disponibilidade não for garantida**, então tem-se uma disruptão no acesso ou no uso da informação

Outras propriedades de segurança

Além da *CIA triad*

■ Autenticidade (*Authenticity*)

- Autenticidade de uma informação consiste em garantir que é proveniente de quem diz ser, ou seja, garantir a autoria da informação
- Também garante a autenticidade de uma entidade, garantindo que ela é quem diz ser

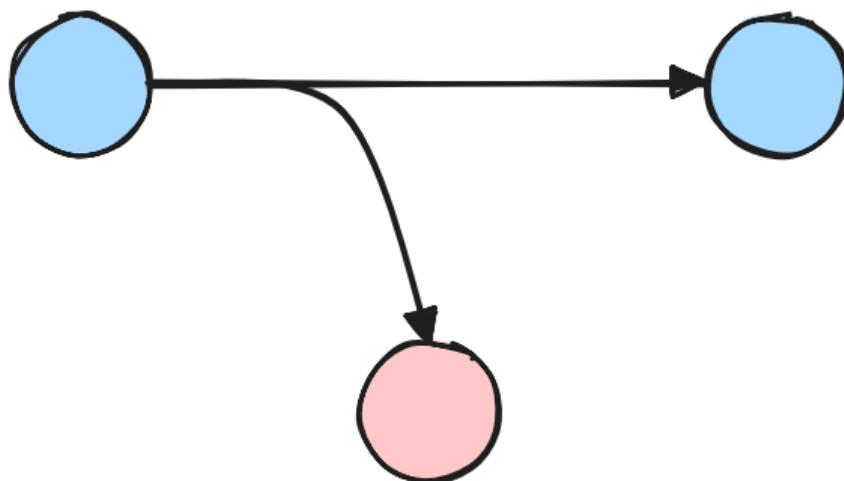
■ Responsabilidade (*Accountability*)

- Capacidade de rastrear ações até um indivíduo ou processo
- Em conjunto com a integridade e autenticidade, dá suporte ao **não repúdio**

Classificação de ataques

Interceptação

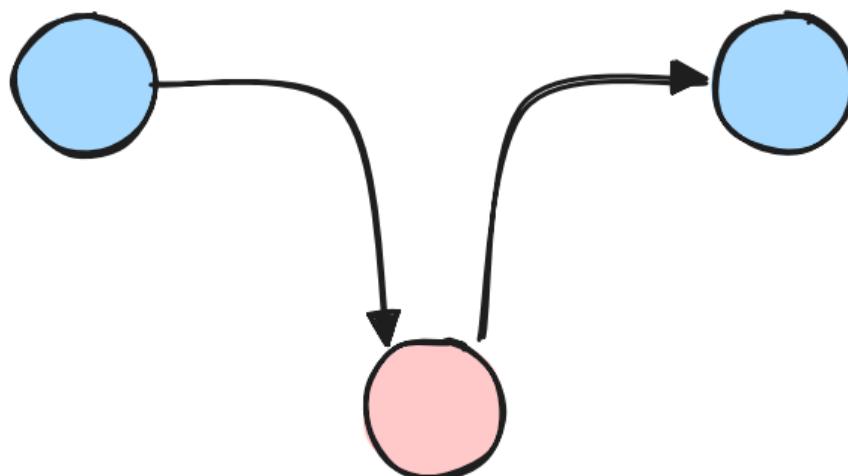
Parte não autorizada obtém acesso a uma informação



Classificação de ataques

Modificação

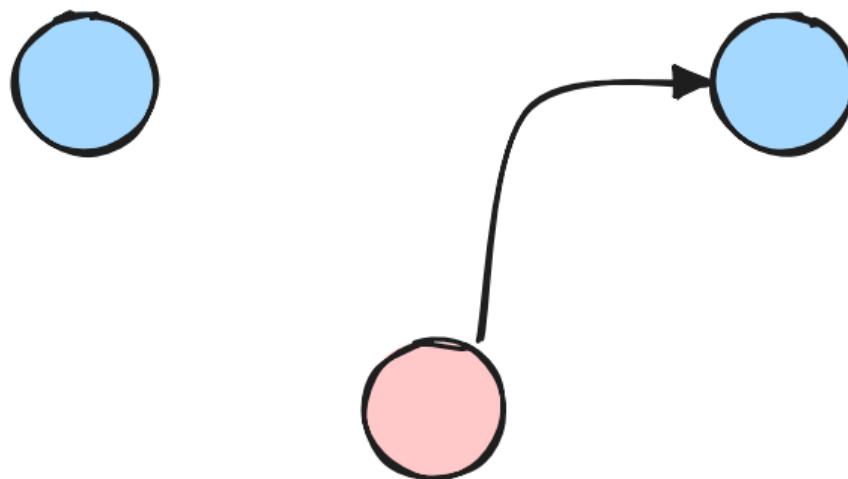
Parte não autorizada altera uma informação e a envia para o destinatário



Classificação de ataques

Personificação

Parte não autorizada envia uma informação como se fosse uma parte legítima



Classificação de ataques

Interrupção

Parte não autorizada interrompe a comunicação entre duas partes legítimas



Incidentes de segurança

Evento que compromete a confidencialidade, integridade ou disponibilidade de um sistema ou organização

- **Vazamento de dados** é um incidente de segurança que compromete a confidencialidade
- **Perda de dados** é um incidente de segurança que compromete a integridade
- **Indisponibilidade** é um incidente de segurança que compromete a disponibilidade

Incidentes de segurança

Exemplos

- 1 As notas de um estudante são alteradas no sistema acadêmico por uma pessoa não autorizada (ex. um aluno, um professor ou um técnico)
- 2 Em um hospital, um ataque de *ransomware* criptografa os prontuários dos pacientes
- 3 Um *hacker* obtém acesso a um banco de dados de uma empresa e rouba informações de cartões de crédito
- 4 Os votos de uma eleição são alterados por um ataque cibernético

Incidentes de segurança

Exemplos

- 1 As notas de um estudante são alteradas no sistema acadêmico por uma pessoa não autorizada (ex. um aluno, um professor ou um técnico)
 - Como garantir a integridade das notas?
- 2 Em um hospital, um ataque de *ransomware* criptografa os prontuários dos pacientes
- 3 Um *hacker* obtém acesso a um banco de dados de uma empresa e rouba informações de cartões de crédito
- 4 Os votos de uma eleição são alterados por um ataque cibernético

Incidentes de segurança

Exemplos

- 1 As notas de um estudante são alteradas no sistema acadêmico por uma pessoa não autorizada (ex. um aluno, um professor ou um técnico)
- 2 Em um hospital, um ataque de *ransomware* criptografa os prontuários dos pacientes
 - Como garantir a disponibilidade dos prontuários?
- 3 Um *hacker* obtém acesso a um banco de dados de uma empresa e rouba informações de cartões de crédito
- 4 Os votos de uma eleição são alterados por um ataque cibernético

Incidentes de segurança

Exemplos

- 1 As notas de um estudante são alteradas no sistema acadêmico por uma pessoa não autorizada (ex. um aluno, um professor ou um técnico)
- 2 Em um hospital, um ataque de *ransomware* criptografa os prontuários dos pacientes
- 3 Um *hacker* obtém acesso a um banco de dados de uma empresa e rouba informações de cartões de crédito
 - Como garantir a confidencialidade das informações?
- 4 Os votos de uma eleição são alterados por um ataque cibernético

Incidentes de segurança

Exemplos

- 1 As notas de um estudante são alteradas no sistema acadêmico por uma pessoa não autorizada (ex. um aluno, um professor ou um técnico)
- 2 Em um hospital, um ataque de *ransomware* criptografa os prontuários dos pacientes
- 3 Um *hacker* obtém acesso a um banco de dados de uma empresa e rouba informações de cartões de crédito
- 4 Os votos de uma eleição são alterados por um ataque cibernético
 - Como garantir a integridade dos votos ao mesmo tempo que se garante o sigilo do voto?

Resumo

- **Vulnerabilidade** é uma fraqueza do sistema que pode ser explorada por um atacante para violar a segurança do sistema
- **Ameaça** é qualquer evento, ação, pessoa ou entidade que tem o potencial de causar danos a um sistema
- **Ataque** é a concretização de uma ameaça, explorando uma vulnerabilidade para causar danos a um sistema ou organização
- **Propriedades básicas de segurança** são confidencialidade, integridade e disponibilidade
- **Cibersegurança** envolve pessoas, processos e tecnologia para proteger a informação de ameaças e garantir a continuidade do negócio

Aula baseada em

-  NIELES, Michael; DEMPSEY, Kelley; PILLITTERI, Victoria. An Introduction to Information Security. **NIST Special Publication 800-12 Rev. 1**, jun. 2017. Disponível em: <<https://csrc.nist.gov/pubs/sp/800/12/r1/final>>.
-  SCHNEIER, Bruce. **Clique aqui para matar todo mundo**. 2020. Disponível em: <<https://app.minhabiblioteca.com.br/reader/books/9788550808871>>.
-  SHIREY, R. **Internet Security Glossary, Version 2**. Ago. 2007. Disponível em: <<http://www.rfc-editor.org/rfc/rfc4949.txt>>.
-  STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e Práticas**. 4. ed. São Paulo: Pearson Prentice Hall, 2007. Tradução da 4^a edição norte-americana. ISBN 9788576050673.