Conceitos Básicos de Segurança

Segurança e Auditoria em Sistemas

Profa. Natássya Barlate Floro da Silva

Universidade Tecnológica Federal do Paraná — Câmpus Cornélio Procópio

03 de Março de 2020

Roteiro

Motivação

- Computadores são mais úteis ligados em redes:
  - Compartilhamento de recursos e informações;
  - Interoperabilidade e intercâmbio de informações;
  - Mobilidade de acesso e gerenciamento remoto;
  - Sistemas de processamento distribuído.
- Aumento da extensão das redes e dos acessos: maior necessidade de cuidado e controle.
- 1971: primeiro *worm* que mostrava a mensagem "I'm the creeper: catch me if you can".
- 1989: primeiro ataque DoS (*Denial of Service*) causando lentidão na Internet e com sequelas durando dias.

Segurança

- Segurança de rede e de Internet consiste de medidas para desviar, prevenir, detectar e corrigir violações de segurança:
  - Um usuário malicioso intercepta uma comunicação e tem acesso a um conteúdo confidencial.
  - Um usuário malicioso intercepta uma comunicação e altera o conteúdo, incluindo privilégios ao seu usuário.
  - Um usuário malicioso cria sua própria mensagem se passando por um usuário válido.
  - Um empregado demitido intercepta a mensagem que contém a retirada dos seus privilégios e a adia para conseguir acesso a informações confidenciais.
  - Um usuário envia instruções para a realização de transações financeiras e posteriormente nega tê-las enviado.

Segurança

- Segurança de um sistema, aplicação ou protocolo está relacionada a:
  - Garantir um conjunto de propriedades desejadas;
  - Prevenção contra um adversário com capacidades específicas.
- Exemplo: acesso físico permite o *boot* a uma máquina a partir de um *live* USB ou CD e acesso aos seus arquivos com permissões padrões.

Propriedades de Segurança

- Propriedades ou objetivos de segurança:
  - **Confidencialidade**: assegura que informações privadas e confidenciais não sejam acessadas por usuários não autorizados. Relacionada também à privacidade.
  - **Integridade**: garantia de que não há modificação ou destruição de informações ou das funcionalidades de um sistema.
  - **Disponibilidade**: assegura que os sistemas operem prontamente e seus serviços não fiquem indisponíveis para usuários autorizados.
  - **Autenticidade**: garantia de ser genuíno, capaz de ser verificado com confiança, podendo ser para uma transmissão, mensagem ou para sua origem.
  - **Responsabilização**: também relacionada a não-repúdio, assegura que ações de uma entidade sejam atribuídas exclusivamente a ela, provendo irretratabilidade.

Propriedades de Segurança

- Propriedades ou objetivos de segurança:
  - **Confidencialidade**: assegura que informações privadas e confidenciais não sejam acessadas por usuários não autorizados. Relacionada também à privacidade.
  - **Integridade**: garantia de que não há modificação ou destruição de informações ou das funcionalidades de um sistema.
  - **Disponibilidade**: assegura que os sistemas operem prontamente e seus serviços não fiquem indisponíveis para usuários autorizados.
  - **Autenticidade**: garantia de ser genuíno, capaz de ser verificado com confiança, podendo ser para uma transmissão, mensagem ou para sua origem.
  - **Responsabilização**: também relacionada a não-repúdio, assegura que ações de uma entidade sejam atribuídas exclusivamente a ela, provendo irretratabilidade.

Propriedades de Segurança

- Propriedades ou objetivos de segurança:
  - **Confidencialidade**: assegura que informações privadas e confidenciais não sejam acessadas por usuários não autorizados. Relacionada também à privacidade.
  - **Integridade**: garantia de que não há modificação ou destruição de informações ou das funcionalidades de um sistema.
  - **Disponibilidade**: assegura que os sistemas operem prontamente e seus serviços não fiquem indisponíveis para usuários autorizados.
  - **Autenticidade**: garantia de ser genuíno, capaz de ser verificado com confiança, podendo ser para uma transmissão, mensagem ou para sua origem.
  - **Responsabilização**: também relacionada a não-repúdio, assegura que ações de uma entidade sejam atribuídas exclusivamente a ela, provendo irretratabilidade.

Propriedades de Segurança

- Propriedades ou objetivos de segurança:

Tríade CIA

- **Confidencialidade**: assegura que informações privadas e confidenciais não sejam acessadas por usuários não autorizados. Relacionada também à privacidade.
- **Integridade**: garantia de que não há modificação ou destruição de informações ou das funcionalidades de um sistema.
- **Disponibilidade**: assegura que os sistemas operem prontamente e seus serviços não fiquem indisponíveis para usuários autorizados.
- **Autenticidade**: garantia de ser genuíno, capaz de ser verificado com confiança, podendo ser para uma transmissão, mensagem ou para sua origem.
- **Responsabilização**: também relacionada a não-repúdio, assegura que ações de uma entidade sejam atribuídas exclusivamente a ela, provendo irretratabilidade.

Propriedades de Segurança

- Propriedades ou objetivos de segurança:
  - **Confidencialidade**: assegura que informações privadas e confidenciais não sejam acessadas por usuários não autorizados. Relacionada também à privacidade.
  - **Integridade**: garantia de que não há modificação ou destruição de informações ou das funcionalidades de um sistema.
  - **Disponibilidade**: assegura que os sistemas operem prontamente e seus serviços não fiquem indisponíveis para usuários autorizados.
  - **Autenticidade**: garantia de ser genuíno, capaz de ser verificado com confiança, podendo ser para uma transmissão, mensagem ou para sua origem.
  - **Responsabilização**: também relacionada a não-repúdio, assegura que ações de uma entidade sejam atribuídas exclusivamente a ela, provendo irretratabilidade.

Propriedades de Segurança

- Propriedades ou objetivos de segurança:
  - **Confidencialidade**: assegura que informações privadas e confidenciais não sejam acessadas por usuários não autorizados. Relacionada também à privacidade.
  - **Integridade**: garantia de que não há modificação ou destruição de informações ou das funcionalidades de um sistema.
  - **Disponibilidade**: assegura que os sistemas operem prontamente e seus serviços não fiquem indisponíveis para usuários autorizados.
  - **Autenticidade**: garantia de ser genuíno, capaz de ser verificado com confiança, podendo ser para uma transmissão, mensagem ou para sua origem.
  - **Responsabilização**: também relacionada a não-repúdio, assegura que ações de uma entidade sejam atribuídas exclusivamente a ela, provendo irretratabilidade.

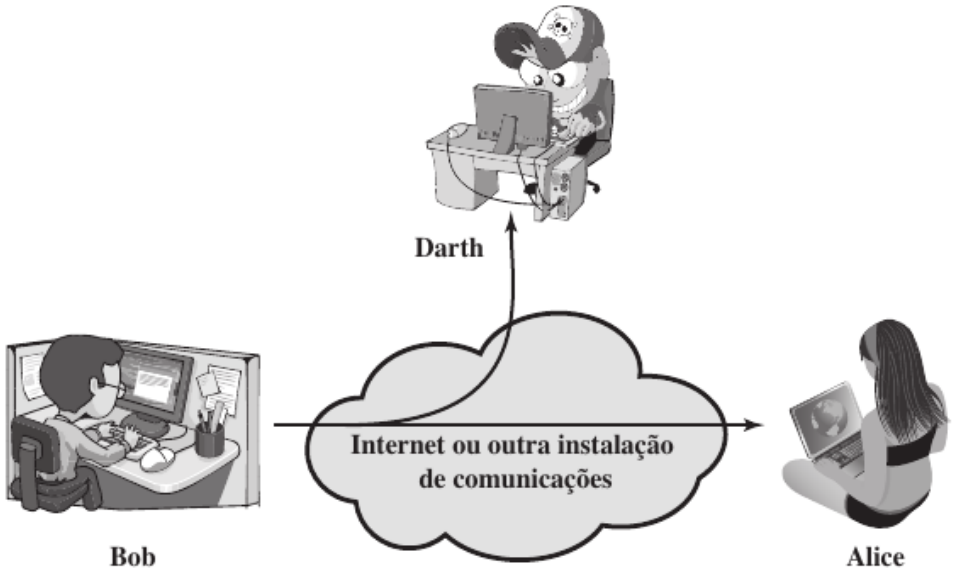
Políticas de Segurança

- Objetivos mais específicos do sistema.
- Relaciona:
  - Riscos ao patrimônio;
  - Acesso dos usuários;
  - Uso de canais de comunicação;
  - Presença de sistemas redundantes e tolerantes a falhas;
- Em geral, definem regras para o acesso, controle e transmissão de informações em um sistema.
- Exemplo: apenas o aluno A pode observar as notas do seu boletim.

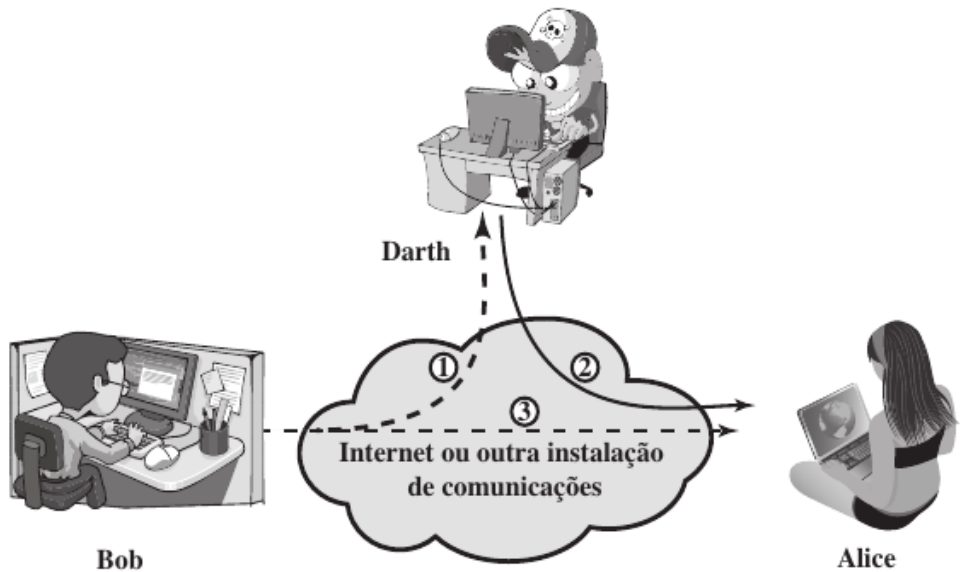
Ameaças e Ataques

- Ameaça: uma chance de violação da segurança que poderia quebrar a segurança e causar danos. Pode ser uma ação ou evento.
- Ataque: ato inteligente e deliberado de violar a política de segurança de um sistema.

Tipos de Ataques



- Passivo: tentativa de descobrir informações.



- Ativo: tentativa de alterar recursos do sistema ou afetar sua operação.

Tipos de ataques

- Passivo:
  - Vazamento de conteúdo da mensagem;
  - Análise de tráfego.
  - Muito difíceis de serem detectados.
- Ativos:
  - Disfarce: usuário se passa por outro;
  - Repasse: retransmissão para produzir efeito não autorizado;
  - Modificação de mensagens;
  - Negação de Serviço, também conhecido por DoS (*Denial of Service*).

Mecanismos de Segurança

- Ferramentas e características do sistema que permite manter as propriedades e políticas de segurança desejadas e detectar, impedir e se recuperar de ataques.
- Codificação:
  - Reversíveis: permitem criptografar e decriptografar dados.
  - Irreversíveis: algoritmos de *hash* e códigos de autenticação de mensagem.
- Assinatura Digital: garante autenticidade e integridade.

Mecanismos de Segurança

- Uso de uma entidade certificadora.
- Controle de acesso.
- Preenchimento de tráfego: adição de tráfego para frustrar sua análise.
- *Firewalls*.
- IDS (*Intrusion Detection System*) – Sistema de Detecção de Intrusão.

Desafios de Segurança

- Propriedades são claras, mas os mecanismos para obtê-las costumam ser complexos.
- No desenvolvimento de uma solução de segurança, é importante considerar potenciais ataques a essas funcionalidades. Em geral, os ataques são realizados explorando uma fraqueza inesperada.
- Muitas vezes só faz sentido elaborar mecanismos de segurança quando vários aspectos de ameaças são considerados, resultando em um aumento da complexidade.

Desafios de Segurança

- Existe uma tendência natural de não se investir em segurança até que uma falha nela ocorra.
- A segurança requer monitoramento regular.
- Segurança costuma ser incorporada nos sistemas após os projetos estarem prontos.

Implantações dos Mecanismos de Segurança

- Dependem sempre de um balanceamento para o sistema:
  - Segurança x Desempenho.
  - Custo da segurança x Valor do patrimônio.

Falha em Políticas: Caso Sarah Palin[1]

- A candidata a vice-presidência dos Estados Unidos pelo partido Republicano Sarah Palin teve a sua conta de e-mail do Yahoo! hackeada por David Kernell.
- A falha ocorreu na política de recuperação de senhas dos e-mail da Yahoo!.
- Baseado em informações bibliográficas, como data de nascimento e onde estudou no ensino médio, disponíveis na página da Wikipedia, foi possível recuperar a senha de Sarah Palin.
- Segundo Kernell, levou apenas "15 segundos" para recuperar a senha.

[1] Baseado nas notas de aula do professor Lucas Sampaio.
Fonte: https://en.wikipedia.org/wiki/Sarah_Palin_email_hack

Falha em Políticas: Caso Mat Honan[2]

- Mat Honan é um jornalista americano que teve sua vida digital apagada em 3 de agosto de 2012.
- Na época, era possível realizar compras na Amazon sem logar em sua conta. Hackers realizaram uma compra adicionando um novo número de cartão de crédito na conta de Mat Honan.
- Com a informação dos últimos 4 dígitos do cartão de crédito, foi possível resetar a senha do Amazon e ter acesso aos últimos 4 dígitos de todos os cartões cadastrados.

[2] Baseado nas notas de aula do professor Lucas Sampaio.

Fonte: https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Falha em Políticas: Caso Mat Honan[2]

- Usando os últimos 4 dígitos do cartão de crédito real de Mat Honan e o seu endereço de cobrança (obtido pela Internet por estar vinculado a um domínio), foi possível resetar a senha do seu e-mail na Apple.
- Como o e-mail da Apple era o *backup* para o seu e-mail do Gmail, também foi possível resetar a sua senha do Gmail e posteriormente obter o acesso da sua conta do Twitter.
- Todo o trabalho de Mat Honan, que estava hospedado na nuvem da Apple e do Google, foi perdido nesse processo.

[2] Baseado nas notas de aula do professor Lucas Sampaio.

Fonte: https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Ameaças e Ataques: Poder computacional muda com o tempo[3]

- Zachary Harris, um matemático, recebeu um e-mail com uma oferta de emprego da Google.
- Ao notar que a chave usada para autenticação de e-mails era de 512 bits, quando o recomendado seria de 1024 bits, Zachary achou que seria um teste para a vaga de emprego.
- Então, Zachary quebrou a chave e a usou para enviar um e-mail entre os fundadores do Google, Brin e Page, indicando um site mantido por ele mesmo.

[3] Baseado nas notas de aula do professor Lucas Sampaio.

Fonte: https://www.wired.com/2012/10/dkim-vulnerability-widespread/

Ameaças e Ataques: Poder computacional muda com o tempo[3]

- Dois dias depois, as chaves usadas pelos servidores da Google passaram a ser de 2048 bits e Zachary nunca obteve uma resposta.
- O mesmo problema foi detectado na época para servidores do PayPal, Yahoo, Amazon, eBay, Apple, Dell, LinkedIn, Twitter, SBCGlobal, US Bank, HP, Match.com and HSBC.
- Esse ataque é conhecido como *email spoofing*, quando um usuário se passa por outro usuário de e-mail.

[3] Baseado nas notas de aula do professor Lucas Sampaio.

Fonte: https://www.wired.com/2012/10/dkim-vulnerability-widespread/

Ameaças e Ataques: Vulnerabilidades Meltdown e Spectre[4]

- As vulnerabilidades Meltdown e Spectre são falhas de CPU, indicando que nem mesmo hardwares são confiáveis.
- Nos dois casos, instruções são executadas pela CPU e os dados relativos são colocados na sua cache, mesmo se forem dados confidenciais. Depois dessa execução, os dados podem ser lidos dos registradores por outros programas.
- O problema foi encontrado em todos os hardwares das grandes produtoras de processadores do mundo: Intel, AMD, Qualcomm, Mediatek e Samsung.

[4] Baseado nas notas de aula do professor Lucas Sampaio.

Fonte: https://www.kaspersky.com.br/blog/35c3-spectre-meltdown-2019/11289/

Falha em Mecanismos: Vulnerabilidades na geração de números aleatórios para carteiras Bitcoin[5]

- Os aplicativos para Android que utilizavam a função secureRandom() do Java para criar carteiras do Bitcoin eram vulneráveis, já que a função não gerava uma semente válida para a criação de suas chaves.
- A semente usada era geralmente a mesma, resultando em chaves muito fracas para as carteiras. Logo, ao adivinhar as chaves, atacantes poderiam transferir *bitcoins* dos usuários.

[5] Baseado nas notas de aula do professor Lucas Sampaio.
Fonte: https://android-developers.googleblog.com/2013/08/some-securerandom-thoughts.html

Falha em Mecanismos: Sessões na Web[6]

- Atacantes tiveram acesso aos dados financeiros de diversos clientes do Citibank apenas alterando a URL do site.
- O site exigia que fosse utilizado um login e uma senha para visualizar informações das contas no banco.
- Porém, após a verificação, os usuários eram redirecionados para uma nova URL que não verificava se o usuário logado era o dono da conta.

[6] Baseado nas notas de aula do professor Lucas Sampaio.

Fonte: https://www.nytimes.com/2011/06/14/technology/14security.html

Exercício

Exercício

Considere um caixa eletrônico de banco no qual os usuários fornecem um cartão e uma senha. Dê exemplos de requisitos de confidencialidade, integridade e disponibilidade associados com esse sistema e, em cada caso, indique o grau de importância desses requisitos.