Segurança física e de infraestrutura

Roberto Sadao Yokoyama

UTFPR-CP

Agosto, 2016

Aula de hoje: [1]

1. Visão geral
2. Ameaças à segurança física
3. Exemplos de ataques

[1] Slides baseados no material do livros: Goodrich [1] e Stallings [2]

Aula passada:

- Senhas
- Tecnologias de autenticação

Classificação

Três elementos da segurança de SI (Sistemas de Informação)

- **Segurança lógica**: protege dados computacionais contra ameaças baseadas em software e em meios de comunicação
- **Segurança física**: ou segurança de infraestrutura. Protege protegem SI que contêm dados e as pessoas que usam, operam e mantêm os sistemas
- **Segurança de dependência**: protege as pessoas e as propriedades dentro de uma área, e é usualmente exigida por lei, regulamentações e normas (ex. combate a incêndios).

Visão geral

Requisitos:

- **Prevenir danos à infraestrutura**: hardware (ex. recursos de armazenamento), instalações físicas (ex. edifícios), instalações de suporte (ex. energia elétrica) e pessoal
- **Impedir a utilização indevida da infraestrutura**: pode ser acidental ou maliciosa (ex. roubo de equipamentos, entrada não autorizada)

Ameaças à segurança física

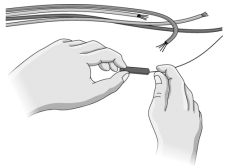
- **Ameaças ambientais**:
  - Desastres naturais: ex. tornado, furacão, inundação e terremoto
  - Temperatura e umidade inadequadas: baixas e altas temperaturas (<10°C ou >32°C). Alta umidade pode causar corrosão.
  - Outras: fogo e fumaça, dano provocado por água, pó e infestação (ex. roedores)
- **Ameaças técnicas**:
  - Energia elétrica: subtensão, sobretensão e interrupção do fornecimento
  - Interferência eletromagnética: ex. motores
- **Ameaças causadas por seres humanos**:
  - Acesso físico não autorizado
  - Roubo: roubo de equipamento e de dados por meio de cópia. Também inclui interceptação e grampo.
  - Vandalismo: destruição de equipamentos
  - Utilização indevida: uso impróprio de ativos por quem está autorizado a usá-los

"Espionagem"

- Técnicas simples de espionagem incluem:
  - Usar a engenharia social para permitir ao atacante ler/observar informações sobre o ombro da vítima
  - Instalação de pequenas câmeras para capturar as informações à medida que está sendo lido/observado
  - Usando binóculos para ver o monitor da vítima através de uma janela aberta
- Essas técnicas de observação direta são comumente conhecidas como *shoulder surfing*

Escutas

- Muitas redes de comunicação empregam o uso de fios de cobre, onde a informação é transmitida através de impulsos elétricos que viajam através dos fios
- Uma abordagem é desconectar brevemente o cabo *ethernet*, inserir um dispositivo passivo de derivação de cabo e reconectá-lo
- Estes ataques de escuta são passivos, pois não existe alteração do sinal sendo transferido, tornando-os extremamente difíceis de detectar



Keyloggers

- *Keylogger* é qualquer meio de gravar as teclas pressionadas pela vítima, normalmente usados para espionar senhas ou outras informações confidenciais.
- *Keyloggers* de *hardware* são tipicamente pequenos conectores instalados entre um teclado e um computador.
- Por exemplo, um *keylogger* USB é um dispositivo que contém conectores USB machos e fêmeas, que permitem que ele seja colocado entre uma porta USB em um computador e um cabo USB de um teclado.

"*Live CDs*"

- Um Live CD é um sistema operacional (SO), gravado no CD, que pode ser inicializado a partir de um meio externo, sem a necessidade da instalação. Além de CD, pode ser: DVD, pen-drive ou outra unidade removível.
- O atacante pode "montar"o disco rígido e depois ler e escrever dados, contornando os mecanismos de autenticação e controle de acesso do SO.

Sugestão de demonstração

Sugestão de demonstração para o seminário final da disciplina:

- Demonstração de computação forense[2]. Recuperar um arquivo deletado do *pen-drive* e verificar a informação do arquivo. Nesse *pen-drive* o arquivo recuperado é uma foto (tirada por *smartphone* com GPS). Implementar um programa para verificar os metadados do arquivo e extrair da imagem: data, horário, coordenada geográfica, etc. Localizar o endereço da coordenada geográfica usando uma ferramenta de mapa (ex. google maps). [nível: médio]

[2] computação forense é prática de obter informação contida em meios eletrônicos, como discos rígidos, para obter evidências a serem usadas em procedimentos legais [1]

Referências

[1] M. T. Goodrich and R. Tamassina. *Introdução à Segurança de Computadores*. Bookman, 2013.

[2] W. Stallings and L. Brown. *Segurança de computadores – princípios e práticas*. Elsevier, 2014.