Fundamentos de Segurança Informática

2025/2026

T1 – Conceitos fundamentais

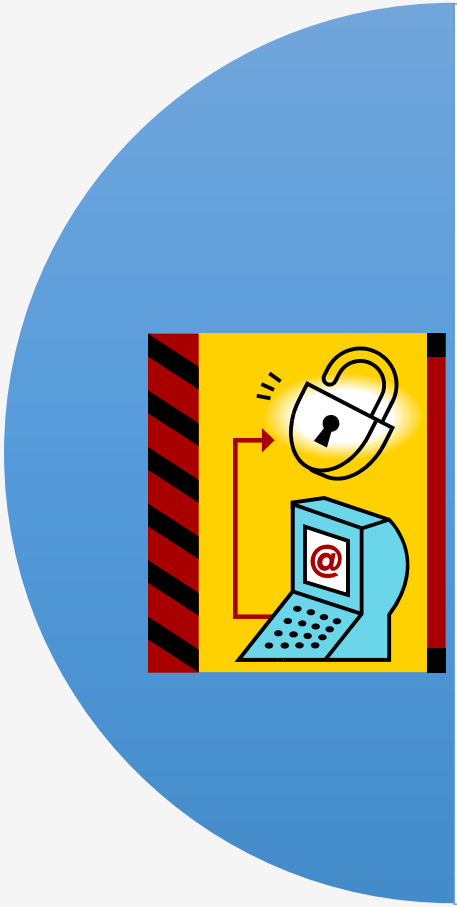
Conteúdo

- Conceitos de segurança informática
  - ✓ Definição
  - ✓ Exemplos
  - ✓ Desafios
- Ataques à segurança
  - ✓ Ataques passivos
  - ✓ Ataques ativos
- Serviços de segurança
  - ✓ Autenticação
  - ✓ Controlo de acessos
  - ✓ Confidencialidade dos dados
  - ✓ Integridade dos dados
  - ✓ Não repúdio
  - ✓ Serviço de disponibilidade
- Superfícies de ataque
- Modelos de segurança
  - Modelo de segurança de rede
  - Modelo de segurança de acesso à rede

Conteúdo

- Conceitos de segurança informática
  - ✓ Definição
  - ✓ Exemplos
  - ✓ Desafios
- Ataques de segurança
  - ✓ Ataques passivos
  - ✓ Ataques ativos
- Serviços de segurança
  - ✓ Autenticação
  - ✓ Controlo de acessos
  - ✓ Confidencialidade dos dados
  - ✓ Integridade dos dados
  - ✓ Não repúdio
  - ✓ Serviço de disponibilidade
- Superfícies de ataque
- Modelos de segurança
  - Modelo de segurança de rede
  - Modelo de segurança de acesso à rede

A área da segurança informática consiste em:



Mecanismos destinados a dissuadir, prevenir, detetar e corrigir violações à segurança da informação

Os algoritmos e protocolos criptográficos podem ser agrupados em quatro áreas principais:

Encriptação simétrica

- Utilizada para ocultar o conteúdo de blocos ou fluxos de dados **de qualquer dimensão**, incluindo mensagens, ficheiros, chaves de encriptação e palavras-passe

Encriptação assimétrica

- Utilizada para ocultar **pequenos** blocos de dados, tais como chaves de encriptação e valores de funções de hash, que são usados em assinaturas digitais

Algoritmos de integridade

- Utilizado para proteger blocos de dados, tais como mensagens, contra **alterações indevidas**

Protocolos de autenticação

- **Esquemas** baseados na utilização de algoritmos criptográficos, concebidos para autenticar a **identidade** de entidades

Objetivos da Segurança Informática

Confidencialidade

- **Confidencialidade dos dados**
  - Assegura que informação privada ou confidencial **não é disponibilizada nem divulgada** a indivíduos não autorizados
- **Privacidade**
  - Assegura que os indivíduos **controlam ou influenciam** que informação relacionada com eles pode ser **recolhida e armazenada**, por quem, e **a quem essa informação pode ser divulgada**

Integridade

- **Integridade dos dados**
  - Assegura que a informação e os programas **são alterados apenas de forma especificada e autorizada**
- **Integridade do sistema**
  - Assegura que um sistema **executa a sua função pretendida de forma íntegra**, livre de **manipulação não autorizada**, deliberada ou inadvertida

Disponibilidade

- Assegura que os sistemas **funcionam de forma atempada** e que o serviço **não é negado a utilizadores autorizados**

Requisitos de Segurança de Redes e Computadores

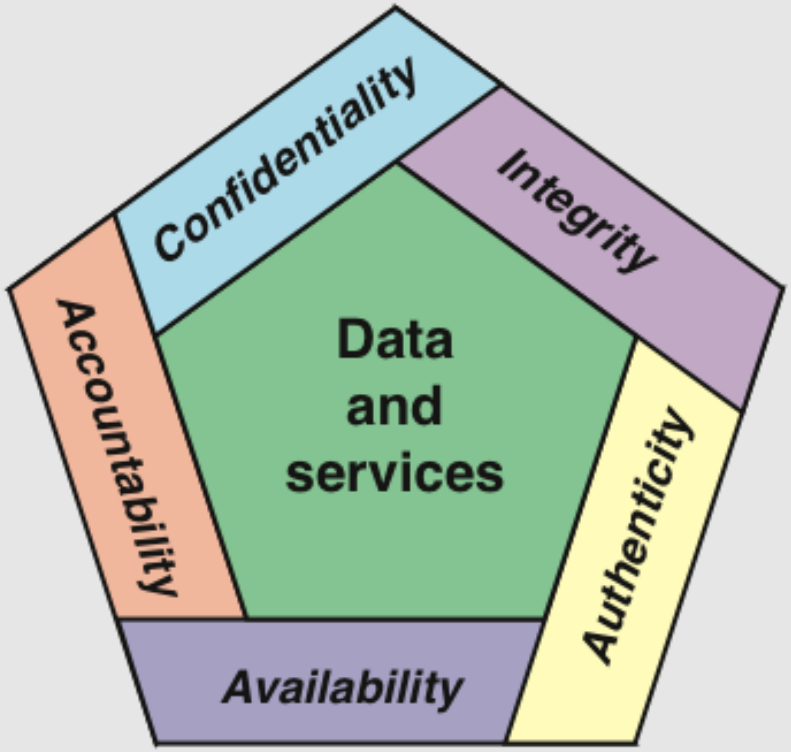


Figure 1.1 Essential Network and Computer Security Requirements

Ameaças e ataques (RFC 4949)

RFC 4949: "Internet Security Glossary, Version 2"

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Conteúdo

- Conceitos de segurança informática
  - ✓ Definição
  - ✓ Exemplos
  - ✓ Desafios
- Ataques à segurança
  - ✓ Ataques passivos
  - ✓ Ataques ativos
- Serviços de segurança
  - ✓ Autenticação
  - ✓ Controlo de acesso
  - ✓ Confidencialidade dos dados
  - ✓ Integridade dos dados
  - ✓ Não repúdio
  - ✓ Serviço de disponibilidade
- Superfícies de ataque
- Modelos de segurança
  - Modelo de segurança de rede
  - Modelo de segurança de acesso à rede

Ataques à Segurança

- Um critério para classificar ataques de segurança, utilizado tanto no X.800 (OSI Security Architecture) como no RFC 4949 (Internet Security Glassary), baseia-se na distinção entre ataques passivos e ataques ativos
- Um ataque passivo tenta obter ou utilizar informação do sistema, mas não afeta os recursos do sistema
- Um ataque ativo tenta alterar os recursos do sistema ou afetar o seu funcionamento

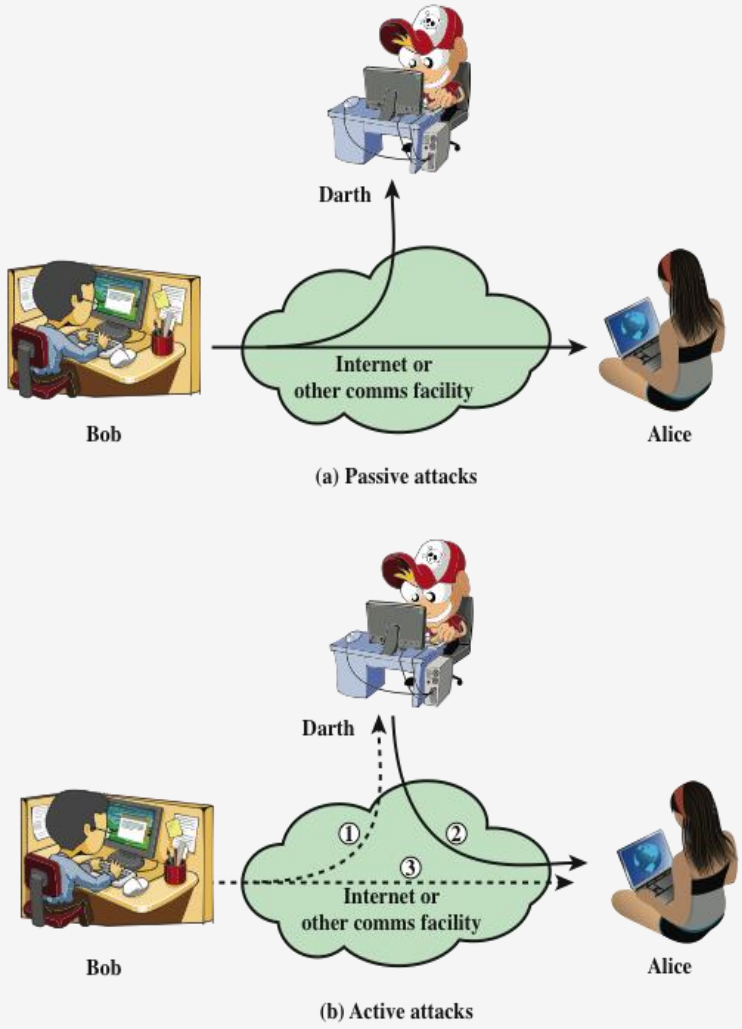


Figure 1.2 Security Attacks

X.800 vs. RFC 4949

X.800 (ITU-T)

- Define a arquitetura de segurança
- Serviços, ataques e mecanismos
- Responde: "O que é segurança da informação?"

RFC 4949 (IETF)

- Glossário de segurança da Internet
- Normaliza terminologia e conceitos
- Responde: "Como falamos corretamente sobre segurança?"

Ataques Passivos

- Consistem essencialmente na escuta ou monitorização das transmissões
- O objetivo do atacante é obter a informação que está a ser transmitida
- São muito difíceis de detetar, pelo que a ênfase é colocada na prevenção em vez da deteção

Exemplos:

- Leitura de emails transmitidos sem encriptação
- Interceção de chamadas VoIP sem encriptação
- Análise de tráfego (captura de pacotes numa rede Wi-Fi)

Ataques Ativos

- Envolvem alguma modificação do fluxo de dados ou a criação de um fluxo falso
- São difíceis de prevenir devido à grande variedade de vulnerabilidades físicas, de software e de rede que podem existir
- O objetivo é detetar os ataques e recuperar de quaisquer perturbações ou atrasos por eles causados

Repetição (Replay)	•Envolve a **captura passiva** de uma unidade de dados e a sua **retransmissão subsequente**, com o objetivo de produzir um **efeito não autorizado** •Exemplo: reutilização de tokens de sessão
Mascaramento (Masquerade)	•Ocorre quando uma entidade **se faz passar por outra entidade** •Normalmente inclui **uma das outras formas de ataque ativo** •Exemplo: IP spoofing
Modificação de mensagens	•**Uma parte de uma mensagem legítima é alterada**, ou as mensagens são **atrasadas ou reordenadas**, de modo a produzir um **efeito não autorizado** •Exemplos: ataque man-in-the-middle
Negação de serviço	•**Impede ou inibe** a utilização ou a **gestão normal das infraestruturas de comunicações** •Exemplo: ataque DoS (Denial of Service)

Conteúdo

- Conceitos de segurança informática
  - ✓ Definição
  - ✓ Exemplos
  - ✓ Desafios
- Ataques de segurança
  - ✓ Ataques passivos
  - ✓ Ataques ativos
- Serviços de segurança
  - ✓ Autenticação
  - ✓ Controlo de acesso
  - ✓ Confidencialidade dos dados
  - ✓ Integridade dos dados
  - ✓ Não repúdio
  - ✓ Serviço de disponibilidade
- Superfícies de ataque
- Modelos de segurança
  - Modelo de segurança de rede
  - Modelo de segurança de acesso à rede

Autenticação

- Autenticação diz respeito à garantia da identidade de uma entidade, seja ela um utilizador, sistema, dispositivo ou origem de uma comunicação
- No caso das comunicações com uma única mensagem, garante ao destinatário que a mensagem provém da fonte que afirma ser
- No caso de uma comunicação contínua, garante que as duas entidades são autênticas e que a ligação não é interferida de forma a permitir que uma terceira parte se faça passar por uma das duas partes legítimas
- São definidos dois serviços de autenticação no X.800:
  - Peer entity authentication (PEA): autentica a entidade numa sessão de comunicação, garante que o "peer" é quem diz ser
  - Data origin authentication (DOI): aplica-se aos dados, numa comunicação garante a origem dos dados/mensagem

Controlo de Acesso

- Controlo de acesso é a capacidade de limitar e regular o acesso a recursos de sistemas e aplicações, com base numa política de segurança
- Permite definir quem pode aceder a que recursos num sistema ou aplicação
- Requer a identificação e autenticação das entidades
- Permite a atribuição e aplicação de permissões de forma controlada

Confidencialidade dos Dados

- Permite proteger os dados transmitidos contra ataques passivos
- Pode abranger a proteção de todos os dados trocados entre duas entidades ao longo de um período de tempo
- Pode também aplicar-se de forma mais restrita, protegendo uma única mensagem ou apenas campos específicos dentro de uma mensagem
- A proteção do fluxo de tráfego assegura a confidencialidade de todas as mensagens numa sessão de comunicação, impedindo a observação da origem, destino, frequência, comprimento ou outras características do tráfego numa infraestrutura de comunicações

Integridade dos Dados

Pode aplicar-se a um fluxo de mensagens, a uma única mensagem ou a campos selecionados dentro de uma mensagem

A integridade orientada à ligação lida com um fluxo de mensagens, garante que as mensagens são recebidas tal como foram enviadas, sem duplicação, inserção, modificação, reordenação ou repetições

A integridade sem ser orientada à ligação lida com mensagens individuais sem considerar qualquer contexto mais alargado, fornece geralmente proteção apenas contra a modificação das mensagens

Não repudiação

- Impede que o emissor ou o recetor neguem uma mensagem transmitida
- A não repudiação assegura a existência de provas verificáveis da origem e da receção de uma mensagem
- Permite ao recetor demonstrar que o emissor enviou efetivamente a mensagem
- Permite ao emissor demonstrar que o recetor recebeu a mensagem

Disponibilidade

- Disponibilidade garante que sistemas, serviços e recursos estão acessíveis e operacionais quando necessários
- Assegura que utilizadores autorizados conseguem aceder aos recursos em tempo útil
- É afetada por falhas, ataques (ex.: DoS) ou manutenção inadequada
- É normalmente assegurada através de medidas ao nível da infraestrutura de suporte aos serviços: redundância, tolerância a falhas e mecanismos de recuperação

Conteúdo

- Conceitos de segurança informática
  - ✓ Definição
  - ✓ Exemplos
  - ✓ Desafios
- Ataques de segurança
  - ✓ Ataques passivos
  - ✓ Ataques ativos
- Serviços de segurança
  - ✓ Autenticação
  - ✓ Controlo de acesso
  - ✓ Confidencialidade dos dados
  - ✓ Integridade dos dados
  - ✓ Não repúdio
  - ✓ Serviço de disponibilidade
- Superfícies de ataque
- Modelos de segurança
  - Modelo de segurança de rede
  - Modelo de segurança de acesso à rede

Superfícies de Ataque

- Uma superfície de ataque consiste nas vulnerabilidades alcançáveis e exploráveis de um sistema

- Exemplos:
  - Portas abertas em servidores Web e outros servidores expostos ao exterior, bem como código a escutar nessas portas
  - Serviços disponíveis no interior de uma firewall
  - Código que processa dados de entrada, correio eletrónico, XML, documentos de escritório e formatos de troca de dados personalizados específicos da indústria
  - Interfaces, SQL e formulários Web
  - Um colaborador com acesso a informação sensível, vulnerável a um ataque de engenharia social

Conteúdo

- Conceitos de segurança informática
  - ✓ Definição
  - ✓ Exemplos
  - ✓ Desafios
- Ataques de segurança
  - ✓ Ataques passivos
  - ✓ Ataques ativos
- Serviços de segurança
  - ✓ Autenticação
  - ✓ Controlo de acesso
  - ✓ Confidencialidade dos dados
  - ✓ Integridade dos dados
  - ✓ Não repúdio
  - ✓ Serviço de disponibilidade
- Superfícies de ataque
- Modelos de segurança
  - Modelo de segurança de rede
  - Modelo de segurança de acesso à rede

Modelo de segurança de Rede

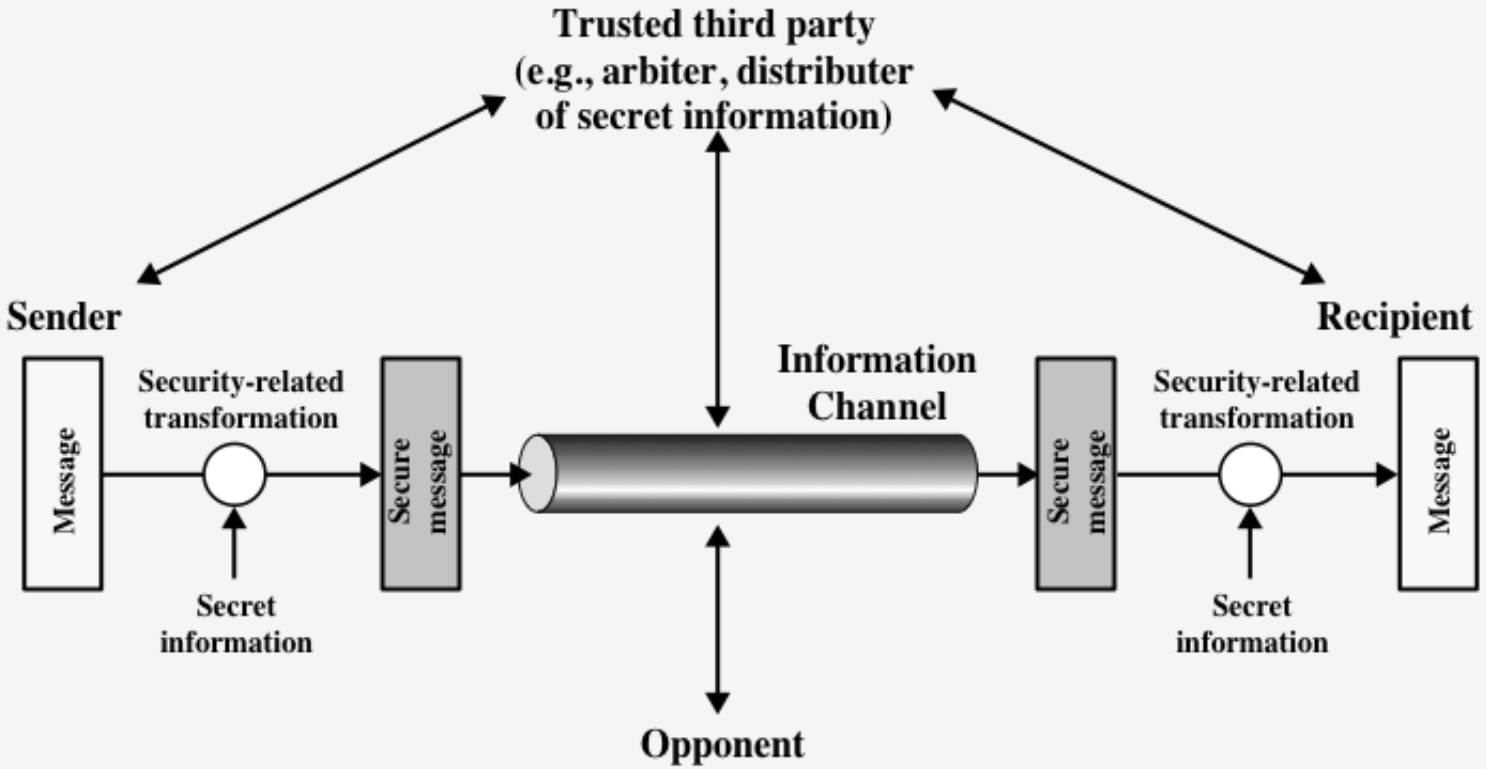


Figure 1.5 Model for Network Security

Modelo de segurança de acesso à Rede

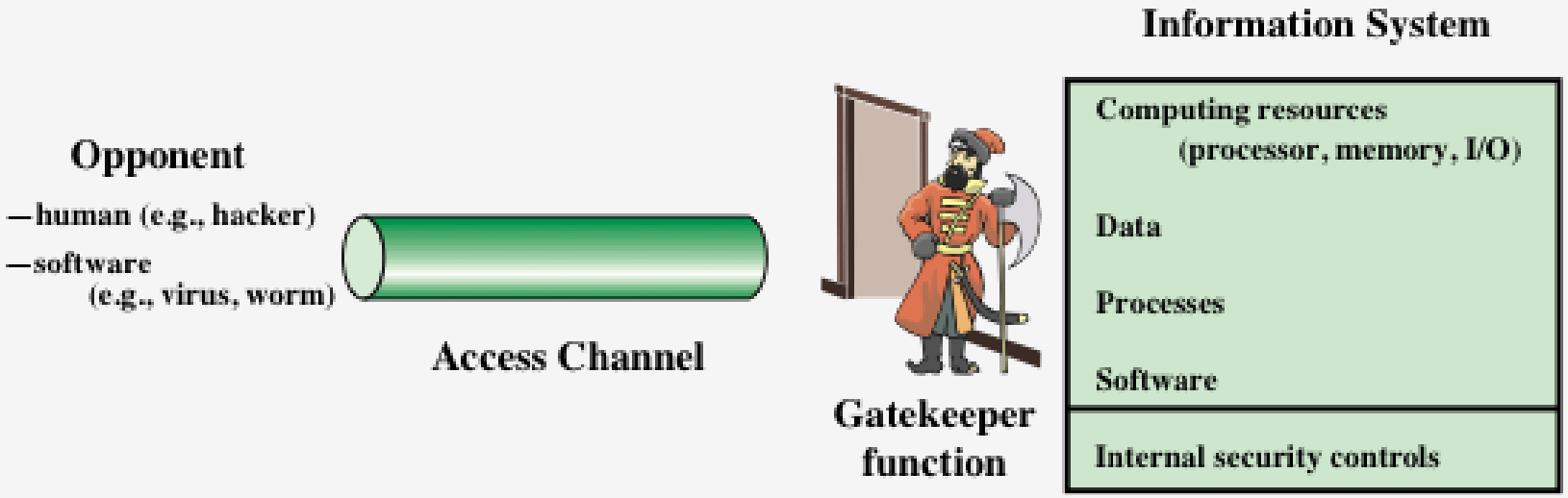


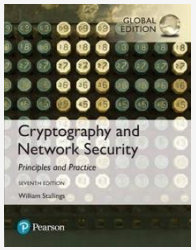
Figure 1.6 Network Access Security Model

Conteúdo

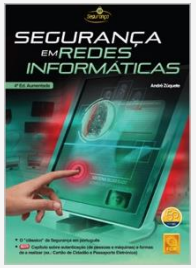
- Conceitos de segurança informática
  - ✓ Definição
  - ✓ Exemplos
  - ✓ Desafios
- Ataques de segurança
  - ✓ Ataques passivos
  - ✓ Ataques ativos
- Serviços de segurança
  - ✓ Autenticação
  - ✓ Controlo de acesso
  - ✓ Confidencialidade dos dados
  - ✓ Integridade dos dados
  - ✓ Não repúdio
  - ✓ Serviço de disponibilidade
- Superfícies de ataque
- Modelos de segurança
  - Modelo de segurança de rede
  - Modelo de segurança de acesso à rede

Bibliografia

Cryptography and network security, Stallings, Pearson, 2017, Chapter 1: Computer and Network Security Concepts



Segurança em Redes Informáticas, Capítulo 1: Introdução



Segurança Prática em Sistemas e Redes com Linux, Capítulo 1: Conceitos fundamentais