Introduction to Security

CSS441: Security and Cryptography

Sirindhorn International Institute of Technology
Thammasat University

Prepared by Steven Gordon on 20 December 2015
css441y15s2l01, Steve/Courses/2015/s2/css441/lectures/introduction-to-security.tex, r4295

Contents

Computer Security Concepts

The OSI Security Architecture

Security Attacks

Security Services

Security Mechanisms

What Is Security?

Computer Security

> *The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources.*

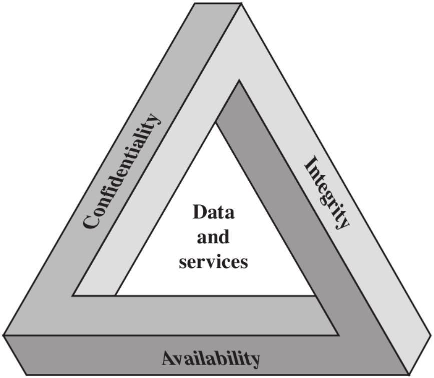
NIST Computer Security Handbook

Network and Internet Security

> *Measures to deter, prevent, detect, and correct security violations that involve transmission of information.*

Stallings, Cryptography and Network Security

Key Security Concepts



Others: Authenticity, Accountability

Credit: Figure 1.1 in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

Impact of Security Breaches

How do security breaches impact organisations?

- Effectiveness of primary operations are reduced
- Financial loss
- Damage to assets
- Harm to individuals

Different levels of impact. E.g. FIPS Publication 199 defines: Low/Minor, Moderate/Significant, High/Severe

Contents

Computer Security Concepts

The OSI Security Architecture

Security Attacks

Security Services

Security Mechanisms

ITU-T X.800 Security Architecture for OSI

- Systematic approach to define requirements for security and approaches to satisfying those requirements
- ITU-T Recommendation X.800, *Security Architecture for OSI*
- Provides abstract view of main issues of security
- Security aspects: Attacks, mechanisms and services
- Terminology:
  - Threat: potential violation of security
  - Attack: assault on system security derived from intelligent threat

Aspects of Security

Security Attack

Any action that attempts to compromise the security of information or facilities

- Threat: potential for violation of security of information or facilities

Security Mechanism

A method for preventing, detecting or recovering from an attack

Security Service

Uses security mechanisms to enhance the security of information or facilities in order to stop attacks

Contents

Computer Security Concepts

The OSI Security Architecture

Security Attacks

Security Services

Security Mechanisms

Types of Attacks

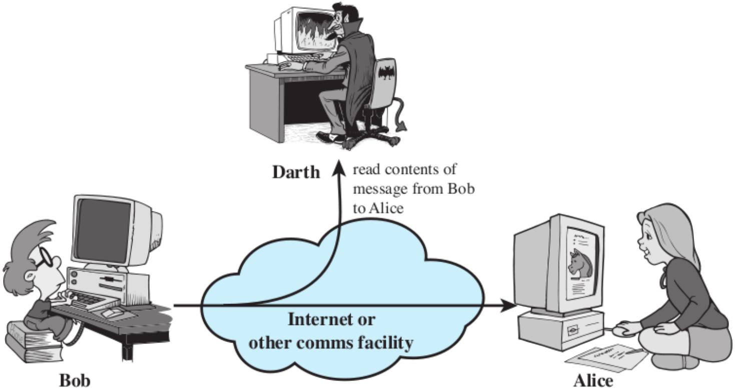
Passive Attack

- Make use of information, but not affect system resources, e.g.
  1. Release message contents
  2. Traffic analysis
- Relatively hard to detect, but easier to prevent

Active Attack

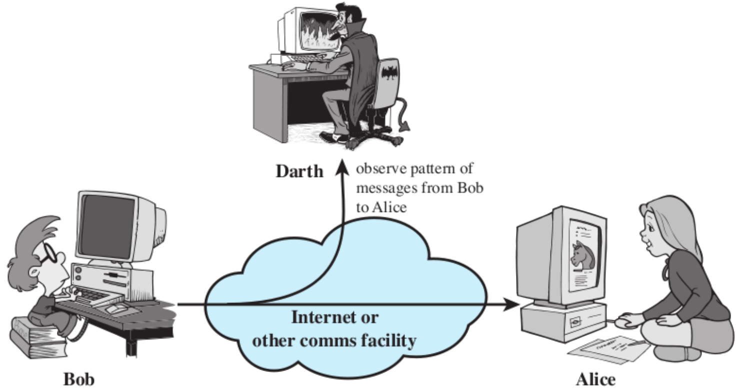
- Alter system resources or operation, e.g.
  1. Masquerade
  2. Replay
  3. Modification
  4. Denial of service
- Relatively hard to prevent, but easier to detect

Release Message Contents


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

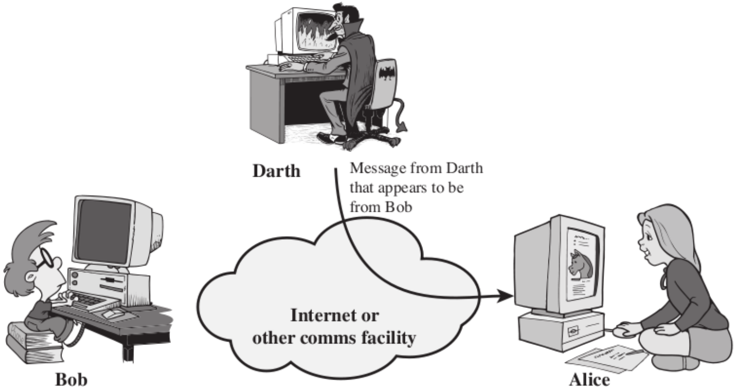
Credit: Figure 1.2(a) in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

Traffic Analysis


Darth
observe pattern of messages from Bob to Alice
Bob
Internet or other comms facility
Alice

Credit: Figure 1.2(b) in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

Masquerade Attack


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

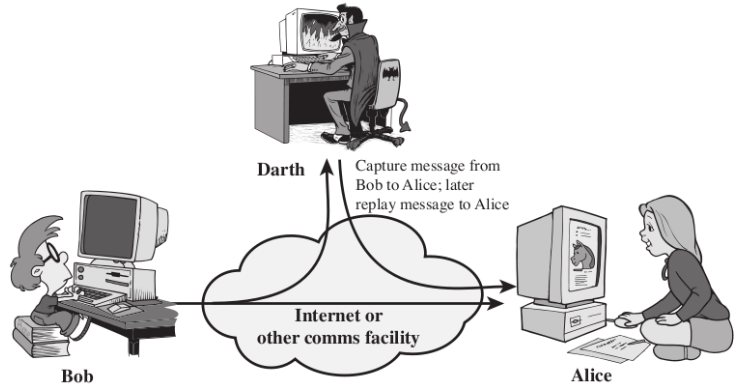
Credit: Figure 1.3(a) in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

“On the Internet, nobody knows you’re a dog”

"On the Internet, nobody knows you're a dog."

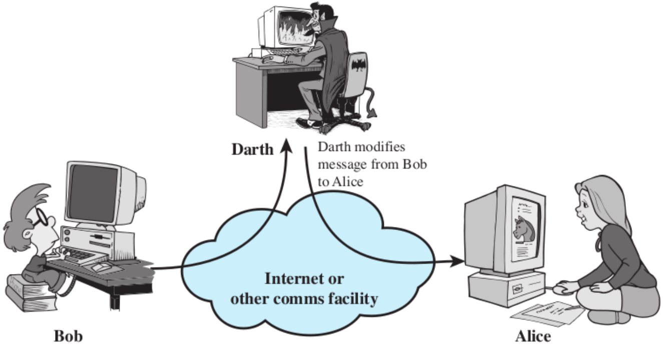
Credit: Peter Steiner, ©The New Yorker magazine

Replay Attack


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

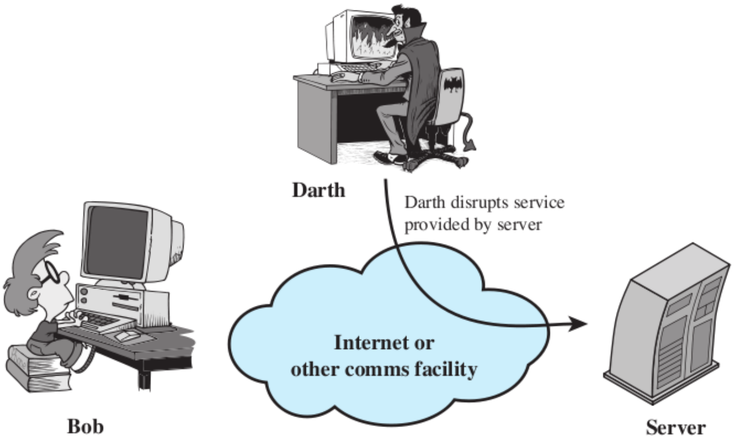
Credit: Figure 1.3(b) in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

Modification Attack


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Credit: Figure 1.3(c) in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

Denial of Service Attack


Darth
Darth disrupts service provided by server
Bob
Internet or other comms facility
Server

Credit: Figure 1.3(d) in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

Contents

Computer Security Concepts

The OSI Security Architecture

Security Attacks

Security Services

Security Mechanisms

Defining a Security Service

- ITU-T X.800: *service that is provided by a protocol layer of communicating systems and that ensures adequate security of the systems or of data transfers*
- IETF RFC 2828: *a processing or communication service that is provided by a system to give a specific kind of protection to system resources*
- Security services implement security policies and are implemented by security mechanisms

Security Services

1. Authentication Assure that the communicating entity is the one that it claims to be. (Peer entity and data origin authentication)
2. Access Control Prevent unauthorised use of a resource
3. Data Confidentiality Protect data from unauthorised disclosure
4. Data Integrity Assure data received are exactly as sent by authorised entity
5. Non-repudiation Protect against denial of one entity involved in communications of having participated in communications
6. Availability System is accessible and usable on demand by authorised users according to intended goal

Contents

Computer Security Concepts

The OSI Security Architecture

Security Attacks

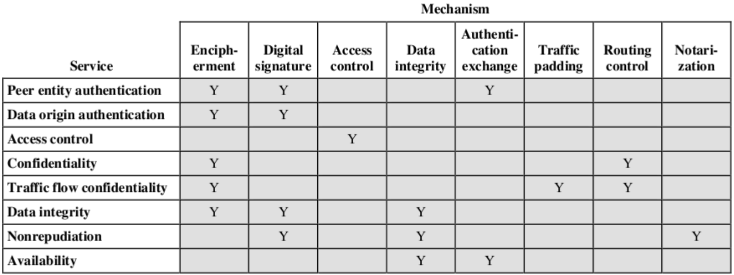
Security Services

Security Mechanisms

Security Mechanisms

- Techniques designed to prevent, detect or recover from attacks
- No single mechanism can provide all services
- Common in most mechanisms: cryptographic techniques
- Specific security mechanisms from ITU-T X.800: Encipherment, digital signature, access control, data integrity, authentication exchange, traffic padding, routing control, notarisation
- Pervasive security mechanisms from ITU-T X.800: Trusted functionality, security label, event detection, security audit trail, security recovery

Security Services and Mechanisms



	Mechanism							
Service	**Encipherment**	**Digital signature**	**Access control**	**Data integrity**	**Authentication exchange**	**Traffic padding**	**Routing control**	**Notarization**
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Credit: Table 1.4 in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011