Introduction to Security

ITS335: IT Security

Sirindhorn International Institute of Technology
Thammasat University

Prepared by Steven Gordon on 20 December 2015
its335y15s2l01, Steve/Courses/2015/s2/its335/lectures/intro.tex, r4287

Contents

Computer Security Concepts

Threats, Attacks and Assets

Architecture for Communications Security

Computer Security Strategy

Summary

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

Key Security Objectives

Confidentiality

- Data confidentiality: assure confidential information not made available to unauthorized individuals
- Privacy: assure individuals can control what information related to them is collected, stored, distributed

Integrity

- Data integrity: assure information and programs are changed only in a authorized manner
- System integrity: assure system performs intended function

Availability

- Assure that systems work promptly and service is not denied to authorized users

Other Security Objectives

Authenticity

- Users and system inputs are genuine and can be verified and trusted
  - Data authentication
  - Source authentication

Accountability

- Actions of an entity can be traced uniquely to that entity
- Supports: non-repudiation, deterrence, fault isolation, intrusion detection and prevention, after-action recovery and legal action

Computer Security Challenges

- computer security is not as simple as it might first appear to the novice
- potential attacks on the security features must be considered
- procedures used to provide particular services are often counter-intuitive
- physical and logical placement needs to be determined
- additional algorithms or protocols may be involved
- attackers only need to find a single weakness, the developer needs to find all weaknesses
- users and system managers tend to not see the benefits of security until a failure occurs
- security requires regular and constant monitoring
- is often an afterthought to be incorporated into a system after the design is complete
- thought of as an impediment to efficient and user-friendly operation

Computer Security Concepts

Assets

- System resources that the users/owners wish to protect
- Hardware, software, data, communication lines

Vulnerabilities

- Weakness in system implementation or operation
- Can make asset: corrupted, leaky, unavailable

Security Policy

- Set of rules and practices that specifies how a system provides security services to protect assets

Threats

- Potential violation of security policy by exploiting a vulnerability

Computer Security Concepts

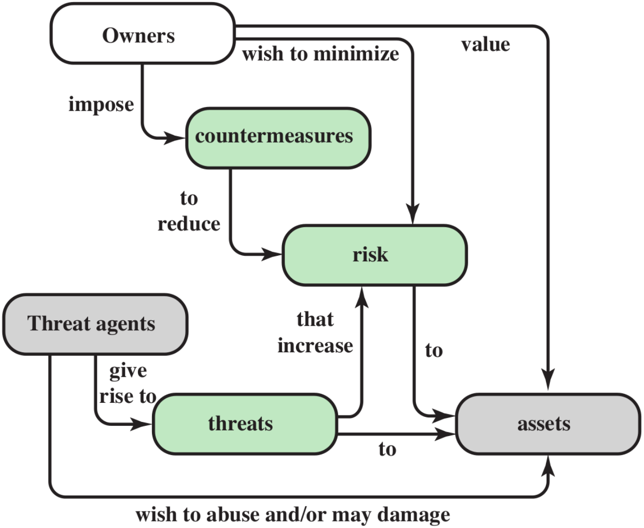
Attack

- A threat that is carried out; a successful attack leads to violation of security policy
  - Active attack: attempt to alter system resources or operation
  - Passive attack: attempt to learn information that does not affect system resources
  - Inside attack: initiated by entity with authorized access to system
  - Outside attack: initiated by unauthorized user of system

Countermeasure

- Means to deal with an attack
  - Prevent, detect, respond, recover
- Even with countermeasures, vulnerabilities may exist, leading to risk to the assets
- Aim to minimize the risks

Computer Security Concepts



Credit: Figure 1.2 in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

Contents

Computer Security Concepts

Threats, Attacks and Assets

Architecture for Communications Security

Computer Security Strategy

Summary

Threat Consequences and Attacks

Threat Action An attack

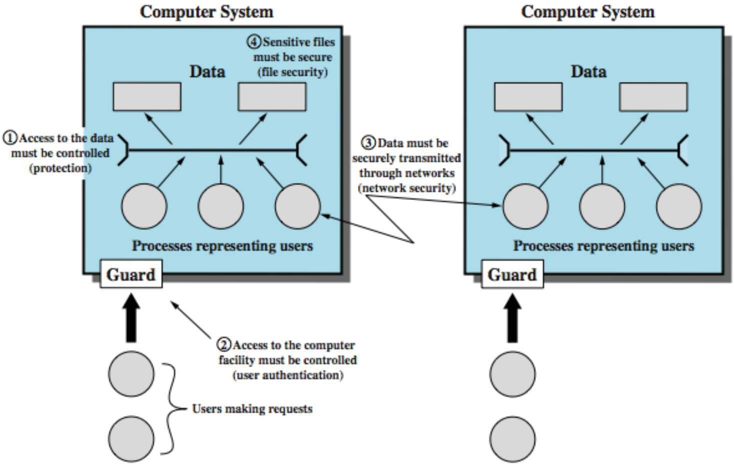
Threat Agent Entity that attacks, or is threat to system (adversary, attacker, malicious user)

Threat Consequence A security violation that results from a threat action

- Unauthorized Disclosure: exposure, interception, inference, intrusion
- Deception: masquerade, falsification, repudiation
- Disruption: incapacitation, corruption, obstruction
- Usurpation: misappropriation, misuse

See: R. Shirey, Internet Security Glossary, IETF RFC 2828, May 2000. `http://www.ietf.org/rfc/rfc2828.txt` (or version 2 in RFC 4949).

Scope of Computer Security


Computer System
Data
④Sensitive files must be secure (file security)
①Access to the data must be controlled (protection)
Processes representing users
Guard
②Access to the computer facility must be controlled (user authentication)
Users making requests
③Data must be securely transmitted through networks (network security)
Computer System
Data
Processes representing users
Guard

Credit: Figure 1.3 in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

Assets and Examples of Threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Credit: Table 1.3 in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

Contents

Computer Security Concepts

Threats, Attacks and Assets

Architecture for Communications Security

Computer Security Strategy

Summary

Architecture for Communications Security

- 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
- Focuses on security of networks and communications systems
- Concepts also apply to computer security

Aspects of Security

Security Attack

Any action that attempts to compromise the 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

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

Attacks on Communication Lines

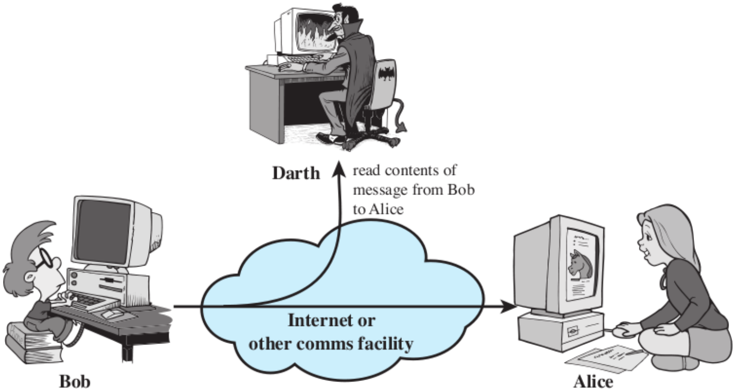
Passive Attack

- 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

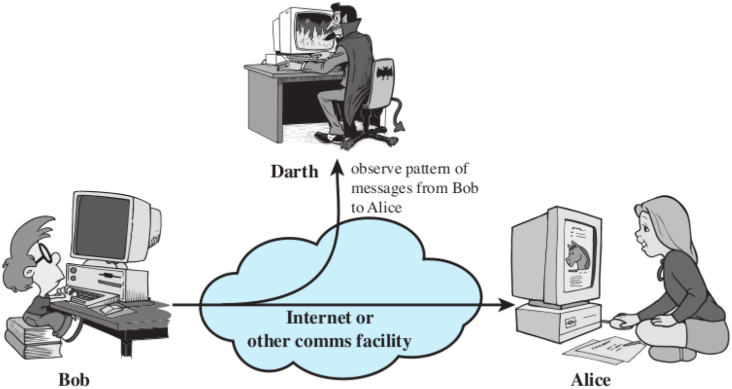
- Alter system resources or operation, e.g.
  1. Masquerade
  2. Replay
  3. Modification
  4. Denial of service
- Relatively hard to prevent, but easier to detect

Release Message Contents


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

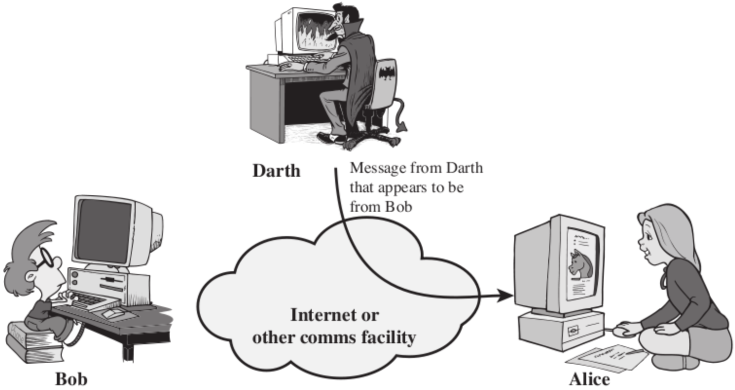
Credit: Figure 1.2(a) in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

Traffic Analysis


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

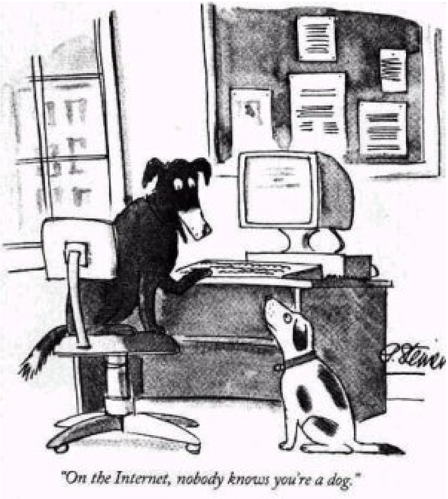
Credit: Figure 1.2(b) in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

Masquerade Attack


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

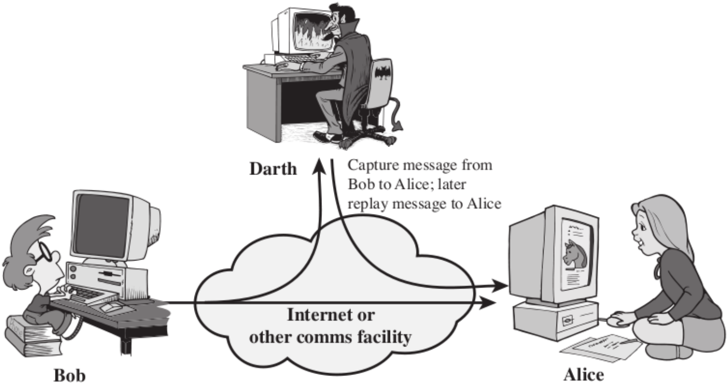
Credit: Figure 1.3(a) in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

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



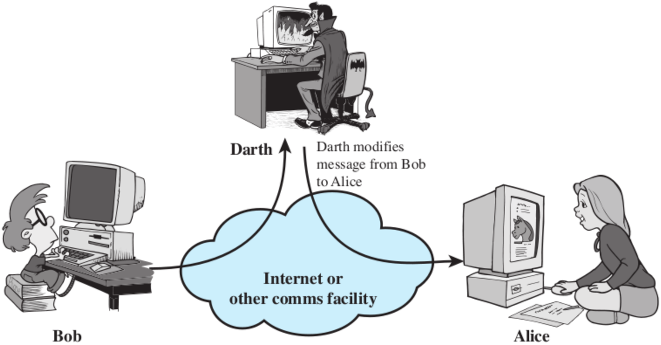
Credit: Peter Steiner, ©The New Yorker magazine

Replay Attack


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

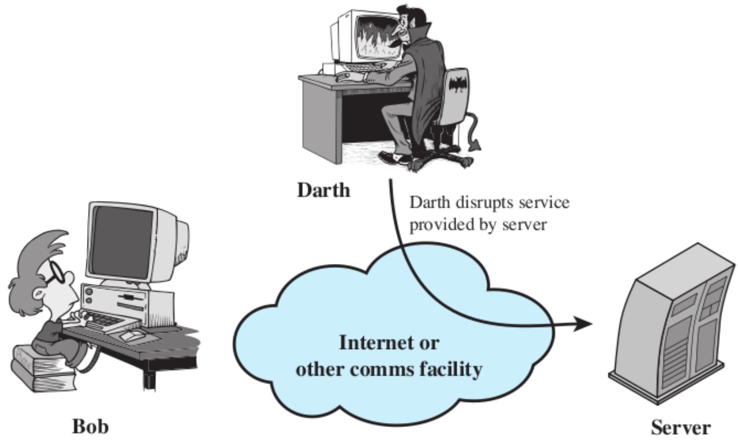
Credit: Figure 1.3(b) in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

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

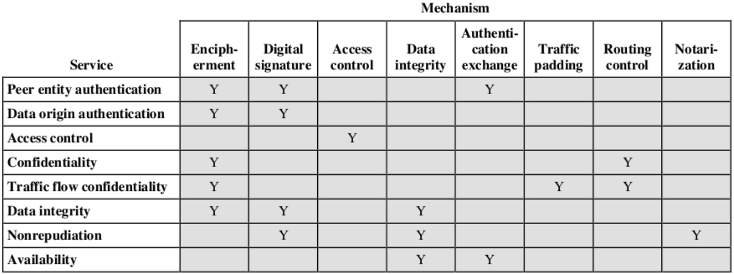

Darth
Darth disrupts service provided by server
Bob
Internet or other comms facility
Server

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

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, notarization
- 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

Contents

Computer Security Concepts

Threats, Attacks and Assets

Architecture for Communications Security

Computer Security Strategy

Summary

Computer Security Strategy and Principles

Policy What is the security scheme supposed to do?

- Informal description or formal set of rules of desired system behaviour
- Consider: assets value; vulnerabilities; potential threats and probability of attacks
- Trade-offs: Ease of use vs security; cost of security vs cost of failure and recovery

Implementation How does it do it?

- Prevention, detection, response, recovery

Assurance Does it really work?

- Assurance: degree of confidence that security measures work as intended
- Evaluation: process of evaluating system with respect to certain criteria

Information Security Principles

NIST Guide to General Server Security

- Simplicity
- Fail-safe
- Complete Mediation
- Open Design
- Separation of Privilege
- Least Privilege
- Psychological Acceptability
- Least Common Mechanism
- Defense-in-Depth
- Work Factor
- Compromise Recording

Contents

Key Points

- Objectives: confidentiality, integrity, availability
- Protect assets: hardware, software, data, comms
- Attacks:
  - Passive: release message, traffic analysis
  - Active: masquerade, replay, modification, DoS
  - Inside or outside
- Countermeasures, Security mechanisms: techniques to prevent, detect, recover from attacks; often use cryptographic techniques

Areas To Explore

Standards and procedures for computer security

- ISO/ITU, NIST FIPS, IETF, IEEE, . . .

Monitoring and trends in threats and attacks

- CERT, CVE, NVD . . .

Certification and professional associations

- SANS, CISSP, CCSP, GIAC, CompTIA, . . .