Security Concepts
Threats, Attacks, Assets

CMSC 426 – Computer Security

Outline

- Standards Organizations
- Confidentiality, Integrity, Availability
- Computer Security Definitions
- Threats, Attacks, and Assets

Why Standards?

- The usual: interoperability, assurance of market share for compliant equipment, etc.
- *Even more important for security!*
  - Security is difficult.
  - Security is subtle.
  - Security should not be left to amateurs.

The Internet Organization

- Internet Architecture Board (IAB)
  - Broad architectural guidance
- Internet Engineering Steering Group (IESG)
  - Management of IETF and process
- Internet Engineering Task Force (IETF)
  - Internet Draft - possible standard
  - Request for Comment (RFC) - standard

RFCs

- http://www.ietf.org/rfc.html
- Examples:
  - 1883 IPv6 Specification
  - 2065 DNS Security Extensions
  - 3711 Secure Real-time Transport (SRTP)
  - 4250 - 4254 Secure Shell (SSH)

National Institute of Standards and Technology

- Federal Information Processing Standards (FIPS) and Special Publications
- Examples:
  - FIPS 186-4 Digital Signature Standard
  - FIPS 197 Advanced Encryption Standard
  - SP 800-90 Random Number Generation
  - SP 800-82 Industrial Control System Security

International Telecommunications Union

- "is responsible for studying technical, operating, and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis."
- Examples:
- X.509 Public Key Certificates
- X.800 Security Architecture for Open Systems

International Organization for Standardization

- Known as ISO, based on the Greek word for "equal"
- A wide variety of standards; known for Management Standards, e.g. ISO 9000 Quality Management
- ISO 27002 Code of Practice for Information Security Management
- You have to pay for the documents!

Security Concepts

- What do we need to protect?
- How are those assets threatened?
- What can be do to counter those threats?

Trust

- A matter of limiting and shifting trust
- In the early days of the Internet, all users were trusted - no need for real security
- Technical security solutions limit trust...to a vendor or an administrator
  - Example: telnet vs. ssh
- What if the vendor fails you?
  - RSA SecurID or MS Certificates and Flame
  - Risks are subtle!

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 (includes hardware, software, information/data, and telecommunications)."

  •NIST SP 800-12

CIA

- *Confidentiality*
- *Integrity*
- *Availability*
- That's it! Consistent with SP 800-12 and FIPS 199.

What Happened to NA?

- *Non-repudiation* is a specific integrity requirement.
- *Authenticity* is also an integrity requirement.
- Also, *accountability* (audit, etc.) is a countermeasure to deal with the imperfection of security mechanisms.

Levels of Impact

- *Low* - noticeable reduction in effectiveness of primary functions; minor damage to assets, financial loss, or harm to individuals.
- *Moderate* - significant reduction in effectiveness of primary functions; significant damage to assets, financial loss, or harm to individuals; no loss of life or life-threatening injuries.
- *High* - severe degradation or loss of mission such that primary functions can not be performed; major damage to assets, financial loss, or severe or catastrophic harm to individuals including loss of life or life-threatening injuries.

Exercise: PoS

- Consider a point-of-sale (PoS) terminal for a large retail chain.
- What are the requirements for confidentiality, integrity, and availability?
- What is the degree of importance of each requirement?

Exercise: SIM

- Consider the Subscriber Identity Module (SIM) in a mobile phone.
- What are the requirements for confidentiality, integrity, and availability?
- What is the degree of importance of each requirement?

Exercise: ICS

- Consider an Industrial Control System (ICS) for a chemical plant.
- What are the requirements for confidentiality, integrity, and availability?
- What is the degree of importance of each requirement?

Threats, Attacks, and Assets

Definitions

- *Threat* - a potential for violation of security; a possible danger that might exploit a vulnerability.
- *Attack* - an assault on system security that derives from an intelligent threat
- *Asset* - hardware, software, data, or communications facilities and networks

Vulnerabilities

- Three categories of vulnerabilities, corresponding to confidentiality, integrity, and availability:
  - System becomes *leaky*, exposing information to unauthorized users.
  - Can be *corrupted* to function improperly or produce incorrect answers.
  - May be *unavailable*; using the system or network becomes impossible or impractical.

- Systems have *vulnerabilities*.
- *Threats* are capable of exploiting vulnerabilities.
- An *attack* is a threat that is carried out.
- An attacker is also called an *adversary* or *threat agent*.
- A *countermeasure* is any means taken to prevent, detect, or recover from an attack.

Attacksonomy

	Active	*Passive*
Inside	Omega Engineering	Snowden
Outside	Phishing, worms, Flame	Packet sniffing, WLAN interception

Attacks and Consequences

- RFC 2828 defines *threat consequences*:
  - Unauthorized Disclosure
  - Deception
  - Disruption
  - Usurpation
- We'll go to RFC 2828 for details.

Exercise: Assets and Threats

For each asset and security requirement (C, I, A), identify one or more threats.

	Confidentiality	Integrity	Availability
Hardware			
Software			
Data			
Comms Lines			

Next time: Security Requirements