Information Security

Information security
- All measures taken to prevent unauthorized use of electronic data
  - unauthorized use includes disclosure, alteration, substitution, or destruction of the data concerned
- Provision of the following three services
  - Confidentiality
    - concealment of data from unauthorized parties
  - Integrity
    - assurance that data is genuine
  - Availability
    - system still functions efficiently after security provisions are in place
- No single measure can ensure complete security

Why is information security important?
- Governments, commercial businesses, and individuals are all storing information electronically
  - compact, instantaneous transfer, easy access
- Ability to use information more efficiently has resulted in a rapid increase in the value of information
- Information stored electronically faces new and potentially more damaging security threats
  - can potentially be stolen from a remote location
  - much easier to intercept and alter electronic communication than its paper-based predecessors

Completing the security process
- Confidentiality + integrity → system security
- However, it is not enough for system to be secure
- System must also be available
  - must allow guaranteed, efficient and continuous use of information
  - security measures should not prohibitively slow down or crash system or make it difficult to use
    - what good is a secure system if you can’t use it?
- Cryptographic systems
  - high level of security and flexibility
  - can potentially provide all objectives of information security: confidentiality, integrity, and availability

Building blocks of a secure system
- Confidentiality: concealment from unauthorized parties
  - identification – unique identifiers for all users
  - authentication
    - user: assurance that the parties involved in a real-time transaction are who they say they are
    - data: assurance of message source
  - authorization - allowing users who have been identified and authenticated to use certain resources
- Integrity: assurance the data is has not been modified by unauthorized parties
  - non-repudiation
    - proof of integrity and origin of data which can be verified by any third party at any time

Symmetric and public key cryptosystems

Symmetric-key cryptosystem
- same key is used for encryption and decryption
- system with 1000 users requires 499,500 keys
  - each pair of users requires a different key

Public-key cryptosystem
- separate keys for encryption and decryption
- system with 1000 users requires 2000 keys
  - each individual user has exactly two keys
Public-key encryption: confidentiality

- Alice wants to send message $M$ to Bob
  - uses Bob's public key to encrypt $M$
- Bob uses his private key to decrypt $M$
  - only Bob has key
  - no one else can decrypt $M$

**Identification provided by public key encryption**

But ... anyone can send message to Bob using his public key
- how are we sure the message came from Alice?

Digital signatures

- Electronic equivalent of handwritten signatures
- Handwritten signatures are hard to forge
- Electronic information is easy to duplicate
- Digital signatures using public key encryption
  - Idea:
    - Bob uses his private key to "sign" a message
    - Alice verifies signature using Bob's public key
  - Data authentication provided by digital signatures

Signed challenges

- Alice wants assurance of real-time communication
- Bob tries to provide assurance by digital signature
- Alice is assured message originated from Bob
  - digital signatures provide data origin authentication
  - But ... Eve can intercept signature and use it to authenticate herself as Bob at any later time
- Signed challenge
  - Alice sends random number (a challenge) to Bob
  - Bob replies with challenge encrypted with signature
- **User authentication provided by signed challenges**
  - combination of digital signature and unpredictability of Alice's random number challenge

Certification authority

- A third party trusted by all users that creates, distributes, revokes, & manages certificates
- Certificates bind users to their public keys
- For example, if Alice wants to obtain Bob's public key
  - she retrieves Bob's certificate from a public directory
  - she verifies the CA's signature on the certificate itself
  - if signature verifies correctly, she has assurance from the trusted CA this really is Bob's public key
  - she can use Bob's public key to send confidential information to Bob or to verify Bob's signatures, protected by the assurance of the certificate
- **Integrity is provided by the certification authority**

Attacks

- Compromise systems in ways that affect services of information security
  - attack on confidentiality:
    - unauthorized disclosure of information
  - attack on integrity:
    - destruction or corruption of information
  - attack on availability:
    - disruption or denial of services

**Prevention, detection, response**

- proper planning reduces risk of attack and increases capabilities of detection and response if an attack does occur

Prevention

- Establishment of policy and access control
  - who: identification, authentication, authorization
  - what: granted on "need-to-know" basis
- Implementation of hardware, software, and services
  - users cannot override, unalterable (attackers cannot defeat security mechanisms by changing them)
  - examples of preventative mechanisms
    - passwords - prevent unauthorized system access
    - firewalls - prevent unauthorized network access
    - encryption - prevents breaches of confidentiality
    - physical security devices - prevent theft
- Maintenance
Prevention is not enough!

Prevention systems are never perfect.

No bank ever says: “Our safe is so good, we don’t need an alarm system.”

No museum ever says: “Our door and window locks are so good, we don’t need night watchmen.”

Detection and response are how we get security in the real world, and they’re the only way we can possibly get security in the cyberspace world.

Bruce Schneier, Counterpane Internet Security, Inc.

Detection

- Determine that either an attack is underway or has occurred and report it
- Real-time monitoring
  - or, as close as possible
  - monitor attacks to provide data about their nature, severity, and results
- Intrusion verification and notification
  - intrusion detection systems (IDS)
    - typical detection systems monitor various aspects of the system, looking for actions or information indicating an attack
    - example: denial of access to a system when user repeatedly enters incorrect password

Response

- Stop/contain an attack
  - must be timely!
    - incident response plan developed in advance
- Assess and repair any damage
- Resumption of correct operation
- Evidence collection and preservation
  - very important
    - identifies vulnerabilities
    - strengthens future security measures

Exercises

Classify each of the following as an attack on confidentiality, integrity, and/or availability (more than one may apply). Justify your answers.

1. John copies Mary’s homework
2. Paul crashes Linda’s system
3. Carol changes the amount of Angelo’s check from $100 to $1,000
4. Gina forges Roger’s signature on a deed
5. Rhonda registers the domain name “AddisonWesley.com” and refuses to let the publishing house buy or use that domain name
6. Jonah obtains Peter’s credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number
7. Henry spoofs Julie’s IP address to gain access to her computer

References

Introduction to Information Security
ECC white paper, March 1997
http://www.certicom.com

The Information Security Process: Prevention, Detection and Response
James LaPedra
GIAC practical repository, SANS Institute
http://www.giac.org/practical/gseo

InformIT Reference Guides
http://www.informit.com/isapi/articles/index.asp