Chapter 0 – Reader’s Guide

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—*The Art of War*, Sun Tzu
Roadmap

- Cryptographic algorithms
  - symmetric ciphers
  - asymmetric encryption
  - hash functions
- Mutual Trust
- Network Security
- Computer Security
Standards Organizations

- National Institute of Standards & Technology (NIST)
- Internet Society (ISOC)
- International Telecommunication Union Telecommunication Standardization Sector (ITU-T)
- International Organization for Standardization (ISO)
The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter. Consequently, it is not easy to find a fixed point of departure..

— On War, Carl Von Clausewitz
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, firmware, information/data, and telecommunications).
Key Security Concepts
Levels of Impact

- can define 3 levels of impact from a security breach
  - Low
  - Moderate
  - High
Examples of Security Requirements

- confidentiality – student grades
- integrity – patient information
- availability – authentication service
Computer Security Challenges

1. not simple
2. must consider potential attacks
3. procedures used counter-intuitive
4. involve algorithms and secret info
5. must decide where to deploy mechanisms
6. battle of wits between attacker / admin
7. not perceived on benefit until fails
8. requires regular monitoring
9. too often an after-thought
10. regarded as impediment to using system
OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study
Aspects of Security

- consider 3 aspects of information security:
  - security attack
  - security mechanism
  - security service

- note terms
  - threat – a potential for violation of security
  - attack – an assault on system security, a deliberate attempt to evade security services
Passive Attacks

Darth reads the contents of the message from Bob to Alice on the Internet or other communications facility.
Active Attacks
Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed
Security Services

- **X.800:**
  “a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers”

- **RFC 2828:**
  “a processing or communication service provided by a system to give a specific kind of protection to system resources”
Security Services (X.800)

- **Authentication** - assurance that communicating entity is the one claimed
  - have both peer-entity & data origin authentication

- **Access Control** - prevention of the unauthorized use of a resource

- **Data Confidentiality** – protection of data from unauthorized disclosure

- **Data Integrity** - assurance that data received is as sent by an authorized entity

- **Non-Repudiation** - protection against denial by one of the parties in a communication

- **Availability** – resource accessible/usable
Security Mechanism

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - cryptographic techniques
- hence our focus on this topic
Security Mechanisms (X.800)

Specific security mechanisms:
- Encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization

Pervasive security mechanisms:
- Trusted functionality, security labels, event detection, security audit trails, security recovery
Model for Network Security

Sender

Security-related transformation

Message

Secret information

Secure message

Information Channel

Opponent

Trusted third party
(e.g., arbiter, distributor of secret information)

Recipient

Secure message

Security-related transformation

Message

Secret information
Model for Network Security

- using this model requires us to:
  1. design a suitable algorithm for the security transformation
  2. generate the secret information (keys) used by the algorithm
  3. develop methods to distribute and share the secret information
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service
Model for Network Access Security

Opponent
- Human (e.g., hacker)
- Software (e.g., virus, worm)

Access Channel

Gatekeeper function

Information System
- Computing resources (processor, memory, I/O)
- Data
- Processes
- Software
- Internal security controls
Model for Network Access Security

- using this model requires us to:
  1. select appropriate gatekeeper functions to identify users
  2. implement security controls to ensure only authorised users access designated information or resources
Summary

- topic roadmap & standards organizations
- security concepts:
  - confidentiality, integrity, availability
- X.800 security architecture
- security attacks, services, mechanisms
- models for network (access) security