

CMPUT 299 (B1) Winter 2008

Security in a Networked World

Introductory Concepts

yannis@cs.ualberta.ca

Information Security Objectives (Definitions)

▶ Confidentiality

Yes, CIA !

- ▶ Assurance that (read) access to an information resource is allowed only to authorized users.

▶ Integrity

- ▶ Assurance that an information resource has not been modified by non-authorized users. (It is “as it was intended to be.”)

▶ Availability

- ▶ Assurance (within reason) that an information resource is accessible when needed.

[Information resource: its definition includes data, code *and* computation devices/systems as a whole.]

More Definitions

▶ Authentication

- ▶ Assurance that an entity is the one it claims to be. [In communication settings authentication is not always mutual.]

▶ Non-Repudiation

- ▶ Assurance that the originator of some information cannot deny being the originator of the information. [Non-repudiation extends to receiving as well.]

▶ Access Control

- ▶ Assurance that there exist precise mechanisms that allow granting and revoking access to an information item or execution of actions on behalf of a user.

Authorization: the act of approving particular access to particular resource.

Some Threats

- ▶ spoofing, fabrication (to Authentication)
- ▶ eavesdropping, interception (to Confidentiality)
- ▶ modification, replays (to Integrity)
- ▶ fraud (to Non-Repudiation)
- ▶ denial of service (DoS) (to Availability)
- ▶ unauthorized use (to Access Control)
- ▶ ...

Classification of Attacks in Networked Systems

- ▶ Passive attacks:
 - ▶ Determining message content
 - ▶ Traffic analysis (drawing inferences about content)
 - ▶ ...
- ▶ Active attacks:
 - ▶ Masquerade
 - ▶ Replay
 - ▶ Message modification
 - ▶ Denial of service
 - ▶ ...

Some of the “Tools” of Information Security

- ▶ Secret (private / symmetric) key crypto.
- ▶ Public key (asymmetric) crypto., certificates
- ▶ Cryptographic hashes, message digests
- ▶ (Pseudo-)random number generators
- ▶ ...

Some of the most potent attacks are those against the tools. Usually many of the security objectives in a system rely on the same set of tools, hence compromising the tools could result in violation of any number of the intended security objectives.

... and tools are not enough ...

Cryptography \neq Security

- ▶ Poor Cryptographic Designs
- ▶ Attacks Against Implementations
- ▶ Attacks Against Passwords
- ▶ Attacks Against Hardware
- ▶ Attacks Against Trust Models
- ▶ Attacks on the User
- ▶ Attacks Against Failure Recovery
- ▶ Attacks Against the Cryptography
- ▶ Lack of Attack Detection
- ▶ Lack of Foresight

<http://www.schneier.com/essay-028.html>

Elements of the Design Space

▶ Security *Policies*

▶ Trust *Models*

Security Policies

Security policies are processes/decisions/rules that define the stance of an organization on matters of security.

Inevitably, they are as diverse as organizations can be, e.g., public sector, non-profit, corporate, military, etc.

Key issues:

- ▶ What is to be protected?
- ▶ Who is a possible attacker?
- ▶ How much security can you afford?

Formal Definition of Security Policy

A security policy is a statement that partitions the states of the system into a set of *secure states* and a set of *nonsecure states*.

“Introduction to Computer Security” by Matt Bishop, 2005.

A *secure system* is a system that *starts* in a secure state, and *cannot* transition into an unauthorized state.

Well-formed policies describe exactly the secure/insecure partition and how the “*cannot*” is attained. Unfortunately policies are not always that precise, e.g., they assume the user is aware of an implied context (laws, other policies, etc.).

Important Forms of Access Control

▶ Discretionary (DAC)

- ▶ The object's owner can determine its access rules.
- ▶ The “owner” is whoever/whatever possesses the information (need *not* be the author/originator).
- ▶ The vast majority of computing platforms use DAC.

▶ Mandatory (MAC)

- ▶ Predetermined access rights, from specific entities to specific objects.
- ▶ Checks clearance level of user against sensitivity level of information resource.
- ▶ “Strong” form of enforcing constraints.

Formal Varieties of Policies

▶ Confidentiality Policies

▶ Bell-LaPadula Model

- ▶ Essentially military-style classification

- ▶ Uses *particular* mandatory & discretionary access rules.

▶ Integrity Policies

▶ Biba Model

- ▶ Defines levels of *integrity* for code/data. (Dual of Bell-LaPadula)

▶ Clark-Wilson Model

- ▶ Introduces the concept of *transactions*.

- ▶ Separates *constrained* and *non-constrained* data items.

- ▶ Introduces *integrity constraints* & *integrity verification* procedures (over constrained data items).

Formal Varieties of Policies (cont'd)

▶ Hybrid Policies

▶ Chinese Wall Model

- ▶ Geared at capturing *conflict of interest* situations.
- ▶ Constraints *accumulate* over time.

▶ Role-Based Access Control (RBAC) Model

- ▶ Introduces *roles* and access rights depend on roles.
- ▶ User can change roles but roles are fairly static.
- ▶ Better management of large scale systems.

▶ Originator Controlled Access Control Model

- ▶ Transfer of access rights only with *agreement of creator*.
- ▶ Remember: the owner is not the same as the creator.
- ▶ The owner cannot override the restrictions of the creator.

Trust Models

- ▶ Trust is a directional relationship.
- ▶ Trust usually has specific scope/domain.
- ▶ Trust is a human/subjective quality.
 - ▶ Trust is an assessment. [Denning93]
 - ▶ It depends on observations/reputation.
 - ▶ Problems: single observation, incorrect observation, etc.
 - ▶ The trusted party can be a machine.
 - ▶ Work has been done on *quantifying* degree of trust.
- ▶ Trust propagation.
 - ▶ Transitivity of trust is convenient.
 - ▶ Propagation can have unintended consequences.

Design Principles

“Introduction to Computer Security” by Matt Bishop, 2005.

- ▶ Principle of Least Privilege
 - ▶ Provide just the privileges necessary for the task.
- ▶ Principle of Fail-Safe Defaults
 - ▶ Deny access unless specifically allowed.
- ▶ Principle of Economy of Mechanism
 - ▶ Make security mechanisms as simple as possible.
- ▶ Principle of Complete Mediation
 - ▶ Every access should be checked if allowed.
- ▶ Principle of Open Design
 - ▶ Assume that the security mechanism is known to all.

Design Principles (cont'd)

“Introduction to Computer Security” by Matt Bishop, 2005.

- ▶ Principle of Separation of Privilege
 - ▶ Do not grant access based on only one condition.
- ▶ Principle of Least Common Mechanism
 - ▶ Do not share mechanisms used to access resources.
- ▶ Principle of Psychological Acceptability
 - ▶ Make secure access *acceptably* complex.

The Voice of Experience: Some Truisms

- ▶ There is no such thing as absolute security.
- ▶ Security is always a question of economics.
- ▶ Defenses should be of the same “height.”
- ▶ Attackers go around security, not through it.
- ▶ Programming is hard.
- ▶ Security should be included in the original design.
- ▶ If you don't run a program, it's not a danger.
- ▶ A chain is only as strong as its weakest link.
- ▶ Do not underestimate the value of your assets.

Preview: Strategies in Networked Environments

- ▶ Securing each host
- ▶ Securing the perimeter
 - ▶ Firewalls
 - ▶ All inbound/outbound traffic passes through the firewall.
 - ▶ Only authorized traffic is allowed to pass (based on policy).
 - ▶ Firewalls should be immune to penetration.

Characteristics & Uses of Firewalls

- ▶ Not a general purpose host.
- ▶ No user accounts.
- ▶ Targeted market products.
- ▶ Single (professional) administration.
- ▶ Advantages from being a “funnel” point.
- ▶ Can be used to implement multiple zones.
- ▶ One special zone can be a DMZ.