Information and System Security

based on slides by

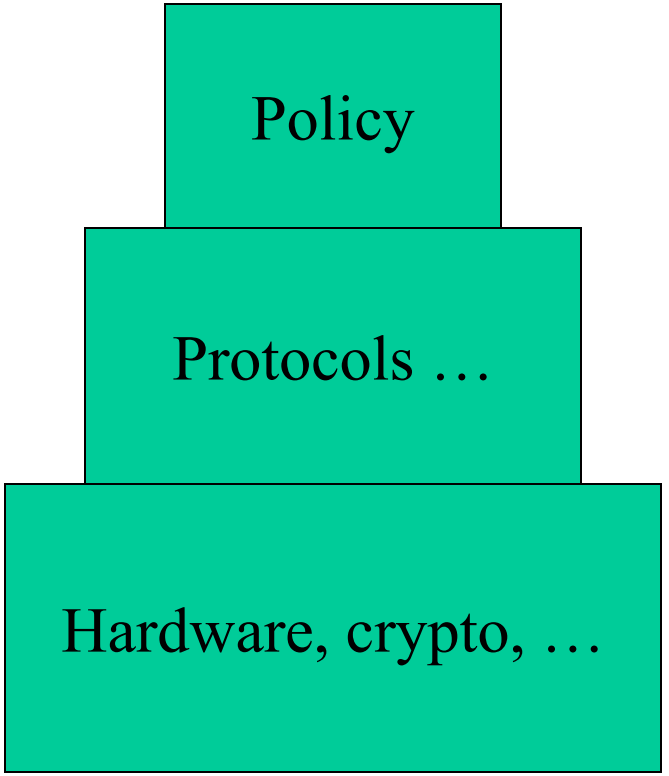
Elisa Bertino
CERIAS and Purdue University
and
Ross Anderson
Cambridge University

What is Security Engineering?

Security engineering is about building systems to remain dependable in the face of malice, error and mischance. As a discipline, it focuses on the tools, processes and methods needed to design, implement and test complete systems, and to adapt existing systems as their environment evolves.

Design Hierarchy

- What are we trying to do?
- How?
- With what?



Security vs Dependability

- Dependability = reliability + security
- Reliability and security are often strongly correlated in practice
- But malice is different from error!
  - Reliability: "Bob will be able to read this file"
  - Security: "The Chinese Government won't be able to read this file"

Methodology

- Sometimes you do a top-down development. In that case you need to get the security spec right in the early stages of the project
- More often it's iterative. Then the problem is that the security requirements get detached
- In the safety-critical systems world there are methodologies for maintaining the safety case
- In security engineering, the big problem is often maintaining the security requirements, especially as the system – and the environment – evolve
- Role of human beings…

Clarifying terminology

- *A system* can be:
  - a product or component (PC, smartcard,…)
  - some products plus O/S, comms and infrastructure
  - the above plus applications
  - the above plus internal staff
  - the above plus customers / external users
- Common failing: policy drawn too narrowly

Clarifying terminology (2)

- *A subject* is a physical person
- *A person* can also be a legal person (firm)
- A principal can be
  - a person
  - equipment (PC, smartcard)
  - a role (the officer of the watch)
  - a complex role (Alice or Bob, Bob deputising for Alice)
- The level of precision is variable – sometimes you need to distinguish 'Bob's smartcard representing Bob who's standing in for Alice' from 'Bob using Alice's card in her absence'. Sometimes you don't

Clarifying terminology (3)

- *Secrecy* limits the number of principals who can access information
- *Privacy* means control of your own secrets
- *Confidentiality* is an obligation to protect someone else's secrets
- Thus your medical privacy is protected by your doctors' obligation of confidentiality

Clarifying terminology (4)

- *Anonymity* is about restricting access to metadata. It has various flavours, from not being able to identify subjects to not being able to link their actions
- An object's *integrity* lies in its not having been altered since the last authorised modification
- *Authenticity* has two common meanings –
  - an object has integrity plus freshness
  - you're speaking to the right principal

Clarifying Terminology (5)

- *Trust* is the hard one! It has several meanings:
  1. a warm fuzzy feeling
  2. a trusted system or component is one that can break my security policy
  3. a trusted system is one I can insure
  4. a trusted system won't get me fired when it breaks
- Our definition: Number 2: NSA definition
- E.g. an NSA man selling key material to the Chinese is trusted but not trustworthy (assuming his action unauthorised)

Clarifying Terminology (6)

- *A security policy* is a succinct statement of protection goals – typically less than a page of normal language
- *A protection profile* is a detailed statement of protection goals – typically dozens of pages of semi-formal language
- *A security target* is a detailed statement of protection goals applied to a particular system – and may be hundreds of pages of specification for both functionality and testing

What often passes as 'Policy'

1. This policy is approved by Management.
2. All staff shall obey this security policy.
3. Data shall be available only to those with a 'need-to-know'.
4. All breaches of this policy shall be reported at once to Security.

Vague and imprecise

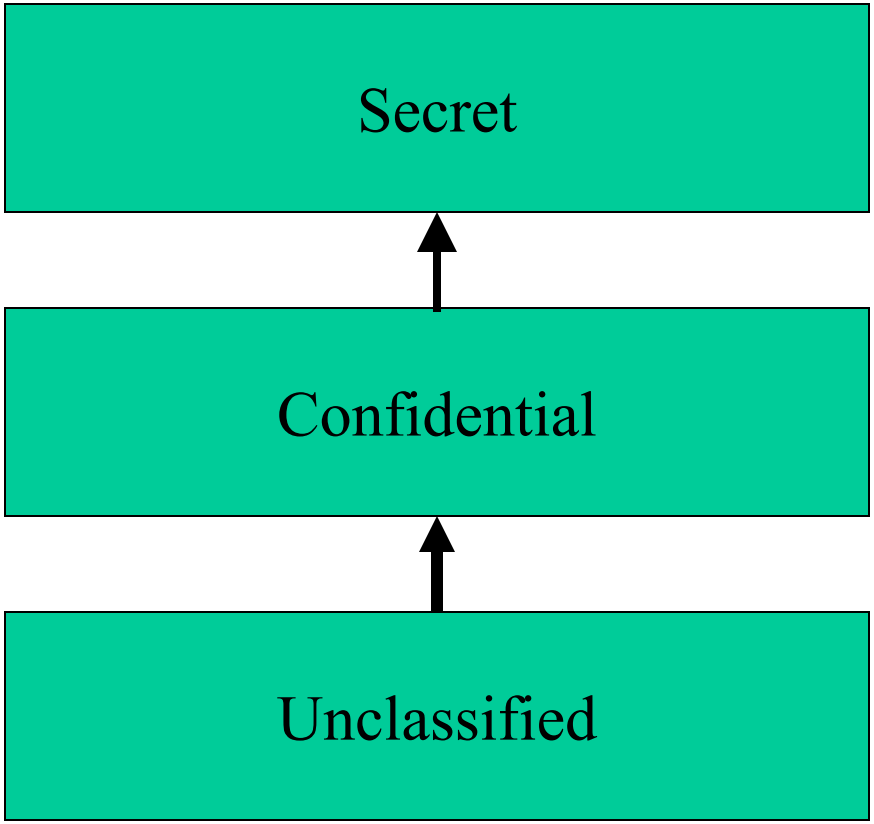
Policy Example – MLS

- Multilevel Secure (MLS) systems are widely used in government
- Basic idea: a clerk with 'Secret' clearance can read documents at 'Confidential' and 'Secret' but not at 'Top Secret'
- 60s/70s: problems with early mainframes
- First security policy to be worked out in detail following Anderson report (1973) for USAF which recommended keeping security policy and enforcement simple

Levels of Information

- Levels include:
  - Top Secret: compromise could cost many lives or do exceptionally grave damage to operations. E.g. intelligence sources and methods
  - Secret: compromise could threaten life directly. E.g. weapon system performance
  - Confidential: compromise could damage operations
  - Restricted: compromise might embarrass?
- Resources have classifications, people (principals) have clearances. Information flows upwards only

Information Flows

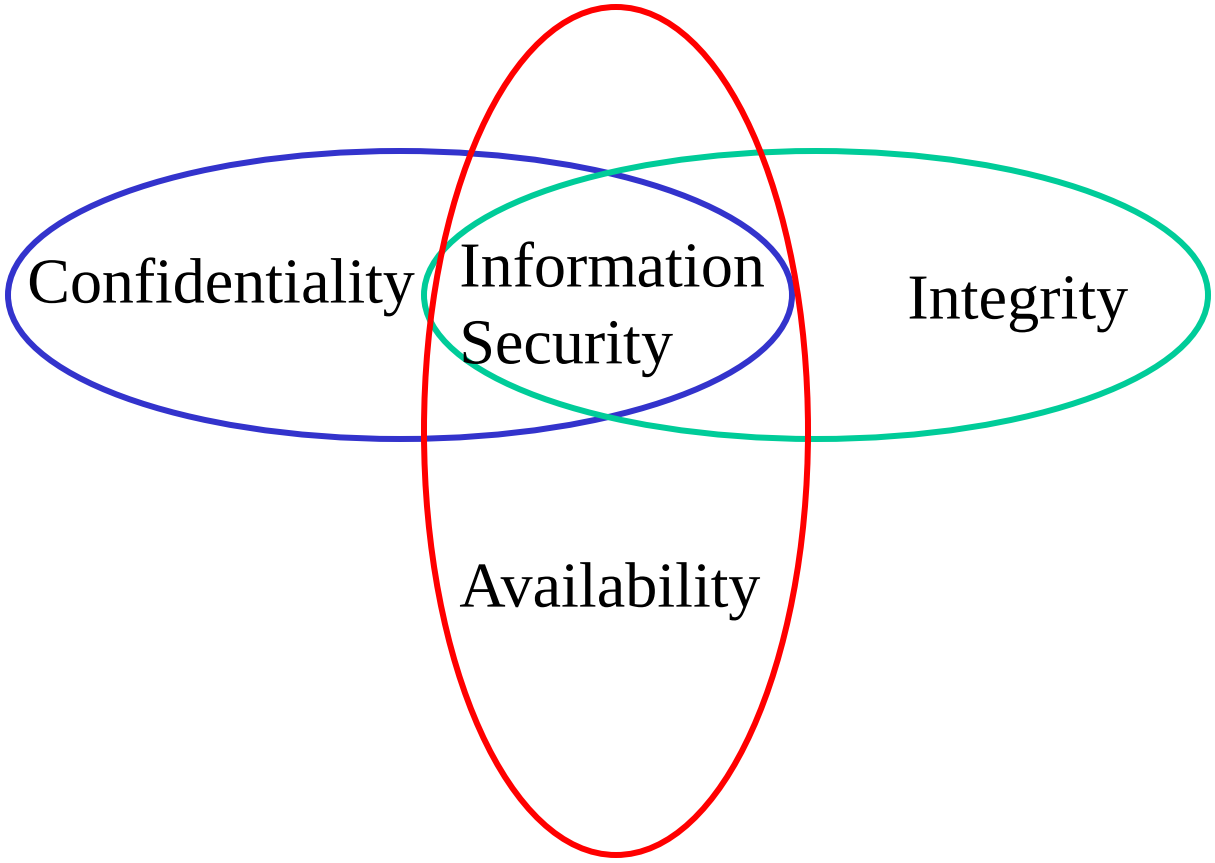


FOCUS: Information Protection

Why Information protection?

- Information are an important strategic and operational asset for any organization
- Damages and misuses of information affect not only a single user or an application; they may have disastrous consequences on the entire organization
- Additionally, the advent of the Internet as well as networking capabilities has made the access to information much easier

Information Security: Main Requirements



Information Security: Examples

- Consider a payroll database in a corporation, it must be ensured that:
  - salaries of individual employees are not disclosed to arbitrary users of the database
  - salaries are modified by only those individuals that are properly authorized
  - paychecks are printed on time at the end of each pay period

Information Security: Examples

- In a military environment, it is important that:
  - the target of a missile is not given to an unauthorized user
  - the target is not arbitrarily modified
  - the missile is launched when it is fired

Information Security - main requirements

- **Confidentiality** – it refers to information protection from unauthorized read operations
  - the term privacy is often used when data to be protected refer to individuals
- **Integrity** – it refers to information protection from modifications; it involves several goals:
  - Assuring the integrity of information with respect to the original information (relevant especially in web environment) – often referred to as authenticity
  - Protecting information from unauthorized modifications
  - Protecting information from incorrect modifications – referred to as semantic integrity
- **Availability** – it ensures that access to information is not denied to authorized subjects

Goals of Security

- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers' violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds (intrusion tolerant- difficult to achieve)
- We focus on Prevention

Information Security – How?

- Information must be protected at various levels:
  - The operating system
  - The network
  - The data management system
  - Physical protection is also important

Information Security – Mechanisms

- Confidentiality is enforced by the access control mechanism
- Integrity is enforced by the access control mechanism and by the semantic integrity constraints
- Availability is enforced by the recovery mechanism and by detection techniques for DoS attacks – an example of which is query flood

Information Security – How? Additional mechanisms

- *User authentication* - to verify the identity of subjects wishing to access the information
- *Information authentication* - to ensure information authenticity - it is supported by signature mechanisms
- *Encryption* - to protect information when being transmitted across systems and when being stored on secondary storage
- *Intrusion detection* – to protect against impersonation of legitimate users and also against insider threats

Data vs Information

- Computer security is about controlling access to information and resources
- Controlling access to information can sometimes be quite elusive and it is often replaced by the more straightforward goal of controlling access to data
- The distinction between data and information is subtle but it is also the root of some of the more difficult problems in computer security
- *Data* represents information. *Information* is the (subjective) interpretation of data

Data vs Information

Data Physical phenomena chosen by convention to represent certain aspects of our conceptual and real world. The meaning we assign to data are called information. Data is used to transmit and store information and to derive new information by manipulating the data according to formal rules.

from:

P.Brinch Hansen. *Operating Systems Principles*. Prentice-Hall, 1973.

Data vs Information

- Protecting information means to protect not only the data directly representing the information
- Information must be protected also against transmissions through:
  - Covert channels
  - Inference
    - It is typical of database systems
    - It refers to the derivation of sensitive information from non-sensitive data

Inference - Example

Name	Sex	Programme	Units	Grade Ave
Alma	F	MBA	8	63
Bill	M	CS	15	58
Carol	F	CS	16	70
Don	M	MIS	22	75
Errol	M	CS	8	66
Flora	F	MIS	16	81
Gala	F	MBA	23	68
Homer	M	CS	7	50
Igor	M	MIS	21	70

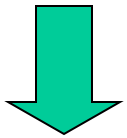
Inference - Example

- Assume that there is a policy stating that the average grade of a single student cannot be disclosed; however statistical summaries can be disclosed
- Suppose that an attacker knows that Carol is a female CS student
- By combining the results of the following legitimate queries:
  - Q1: SELECT Count (*) FROM Students WHERE Sex ='F' AND Programme = 'CS'
  - Q2: SELECT Avg (Grade Ave) FROM Students WHERE Sex ='F' AND Programme = 'CS'

  The attacker learns from Q1 that there is only one female student so the value 70 returned by Q2 is precisely her average grade

Information Security

- It consists of:
  - first defining a *security policy*
  - then choosing some *mechanism* to enforce the policy
  - finally providing *assurance* that both the mechanism and the policy are sound



SECURITY LIFE-CYCLE

Policies and Mechanisms

- Policy says what is, and is not, allowed
  - This defines "security" for the information
- Mechanisms enforce policies
- Composition of policies
  - If policies conflict, discrepancies may create security vulnerabilities

Policies

Policy: may be expressed in

- natural language, which is usually imprecise but easy to understand;
- mathematics, which is usually precise but hard to understand;
- policy languages, which look like some form of programming language and try to balance precision with ease of understanding

Mechanisms

Mechanisms: may be

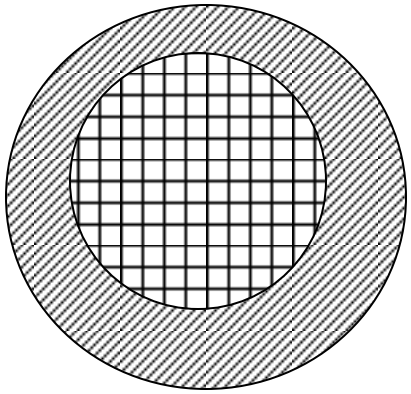
- technical, in which controls in the computer enforce the policy; for example, the requirement that a user supply a password to authenticate herself before using the computer
- procedural, in which controls outside the system enforce the policy; for example, firing someone for ringing in a disk containing a game program obtained from an untrusted source

Composition

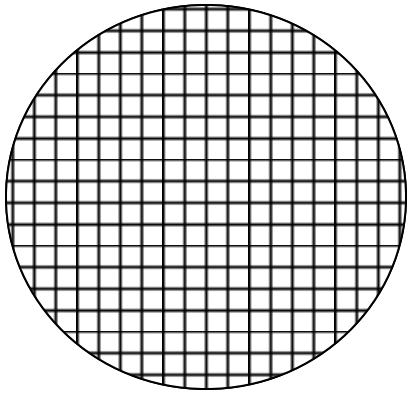
The composition problem requires checking for inconsistencies among policies.

If, for example, one policy allows students and faculty access to all data, and the other allows only faculty access to all the data, then they must be resolved (e.g., partition the data so that students and faculty can access some data, and only faculty access the other data).

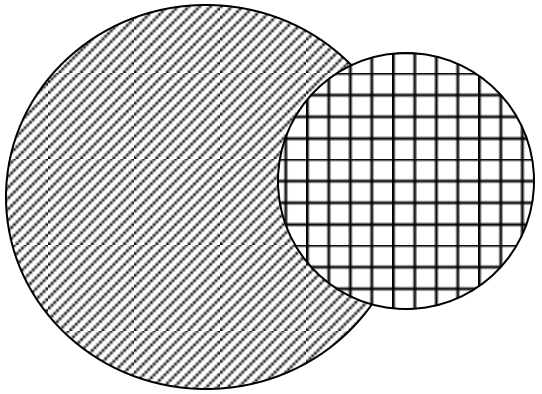
Types of Mechanisms



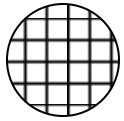
Secure



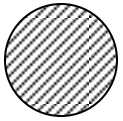
Precise
and
secure



Broad
not secure



set of reachable states



set of secure states

Assurance

- Specification
  - Requirements analysis
  - Statement of desired functionality
- Design
  - How system will meet specification
- Implementation
  - Programs/systems that carry out design

Management and Legal Issues

- Cost-Benefit Analysis
  - Is it more cost-effective to prevent or recover?
- Risk Analysis
  - Should we protect some information?
  - How much should we protect this information?
- Laws and Customs
  - Are desired security measures illegal?
  - Will people adopt them?

Human Factor Issues

- Organizational Problems
  - Power and responsibility
  - Financial benefits
- People problems
  - Outsiders and insiders
  - Social engineering

Key Points

- Policies define security, and mechanisms enforce security
  - Confidentiality
  - Integrity
  - Availability
- Importance of assurance
- The human factor

Privacy: Motivations

- Privacy is an important issue today
  - Individuals feel
    - Uncomfortable: ownership of information
    - Unsafe: information can be misused
    - (e.g., identity thefts)
  - Enterprises need to
    - Keep their customers feel safe
    - Maintain good reputations
    - Protect themselves from any legal dispute
    - Obey legal regulations

Definition

- **Privacy** is the ability of a person to control the availability of information about and exposure of him- or herself. It is related to being able to function in society anonymously (including pseudonymous or blind credential identification).
- **Types of privacy** giving raise to special concerns:
  - Political privacy
  - Consumer privacy
  - Medical privacy
  - *Information technology end-user privacy; also called data privacy*
  - Private property

Data Privacy

- Data Privacy problems exist *wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise.* Improper or non-existent disclosure control can be the root cause for privacy issues.

- The most common sources of data that are affected by data privacy issues are:
  - Health information
  - Criminal justice
  - Financial information
  - Genetic information

Data Privacy

- The challenge in data privacy is to share data while protecting the personally identifiable information.
  - Consider the example of health data which are collected from hospitals in a district; it is standard practice to share this only in aggregate form
  - The idea of sharing the data in aggregate form is to ensure that only non-identifiable data are shared.
- The legal protection of the right to privacy in general and of data privacy in particular varies greatly around the world.