Foundations of Security

Daniel Bosk

Department of Information and Communication Systems (ICS),
Mid Sweden University, SE-851 70 Sundsvall.

foundations.tex 1963 2014-09-05 09:54:41Z danbos

Overview

1. Definitions
   - Security Strategies
   - Data and Information
   - Security Objectives
2. Dilemmas of Security
   - The Fundamental Dilemma of Security
   - Another Dilemma of Security
3. Principles of Security
   - Dimensions of Security
   - Fundamental Design Decisions
   - Focus and Placement of Control
   - Complexity or Assurance
   - Centralised or Decentralised Controls
   - The Layer Below

Overview

1. Definitions
   - Security Strategies
   - Data and Information
   - Security Objectives
2. Dilemmas of Security
   - The Fundamental Dilemma of Security
   - Another Dilemma of Security
3. Principles of Security
   - Dimensions of Security
   - Fundamental Design Decisions
   - Focus and Placement of Control
   - Complexity or Assurance
   - Centralised or Decentralised Controls
   - The Layer Below

Security Strategies

- The main purpose of security is to protect assets.
- In our *(security) policy* we define what is to be accomplished, the goals, e.g. who may access what asset and how.
- We then have *mechanisms* to help us enforce our policy, e.g. cryptography.
- Each of our mechanisms we can say is more or less *trustworthy*. A trustworthy mechanism will not break our security policy.
- Generally we look at failures of systems, these can be divided into unintentional and intentional.
  - *Unintensional failures* are *reliability issues*.
  - *Intentional failures* are *security issues*.
- But note that unintensional failures can be exploited for breaking our security policy – and hence are security issues, or *threats*.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Security Strategies

- Our protection strategies can be divided into the following:
  - Prevention, taking measures that prevent your assets from being damaged.
  - Detection, taking measures that allow detection of when, how, and by who an asset has been damaged.
  - Reaction, taking measures that allow to recover assets or recover from damage to assets.

Security Strategies

Example (Private property)

Prevention	Locks on doors, window bars, surrounding walls, ...
Detection	Stolen items are missing, burglar alarms, video surveillance, ...
Reaction	Call the police, replace stolen items (insurance?), ...

Example (E-commerce)

Prevention	Encrypt orders, rely on merchants checking identities, ...
Detection	An unauthorised transaction appears on your bank statement, ...
Reaction	Complain to bank, ask for new card, ...

Data and Information

Definition (Data and information [Han73])

Physical phenomena chosen by convention to represent certain aspects of of our conceptual and real world. The meanings 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.

Security Objectives

Confidentiality Concerns unauthorised disclosure of information.

Integrity Concerns unauthorised modification.

Availability Concerns unauthorised withholding of information or resources.

Authenticity Concerns the identity of principals in systems.

Accountability (non-repudiation) Concerns proof that some principal was involved in some event.

Security Objectives
Confidentiality

- Prevent unauthorised *reading*.
- *Confidentiality* involves the obligation to protect someone else's information if you know them.
- By *secrecy* we mean the effect of protection of data belonging to someone.
- Think about what to hide: the content of a document, or the document's existence?

Security Objectives
Privacy

- Privacy is different, this concerns protection of personal data.
- The users should be in control of their data and of the information about their activities.
- Also the right to be left alone.

Security Objectives

Integrity

- Prevent unauthorised *writing*.
- Data integrity: "The state that exists when computerized data is the same as that in the source document and has not been exposed to accidental or malicious alteration or destruction."
- Concerns detection and correction of intentional and unintensional modifications of data.

Security Objectives

Integrity

- Clark and Wilson: "No user of the system, even if authorized, may be permitted to modify data in such a way that assets or accounting records of the company are lost or corrupted."
- I.e. make sure that everything is as it is supposed to.
- Integrity is a prerequisite to many other security services.

Security Objectives
Availability

- This is the property of being available and usable upon demand by an authorised principal.
- Denial of Service (DoS) is an attack on availability which prevents authorised access to resources or the delaying of time-critical operations.
- A very important part of security, unfortunately not many methods for accomplishing this are available.
- Distributed Denial of Service (DDoS) gets much attention, this can also be seen as a reliability problem (unintential).

Security Objectives
Availability

Example (Smurf attack)

- Attacker sends ICMP echo request to a broadcast address with the victim's address as the spoofed sender address.
- The echo request is distributed to all nodes in the broadcast range.
- All nodes replies to the echo request, and the replies are sent to the victim – the victim is flooded.
- Depending on the size of the broadcast range, there is a considerable amplification.

Security Objectives
Accountability

- Within the system, audit logs can be kept for *accountability*.
- Should record security relevant events and associated user identities.
- This requires a connection between the user and user identity.
- Distributed systems can use cryptographic *non-repudiation* to achieve the same goal.

Security Objectives
Non-Repudiation

- *Non-repudiation* concerns unforgeable evidence that a specific action has occured.
- *Non-repudiation of origin*: protects against a sender of data denying data was sent.
- *Non-repudiation of delivery*: protects against a receiver denying data was received.
- Note: what is meant my received? E.g. a mail delivered to your mailbox.
- Also note that a simple audit log doesn't necessarily give non-repudiation, it might have been forged by the system administrator.
- It's usually accomplished by using crypto.

Security Objectives
Non-Repudiation

- A commonly found definition: "Non-repudiation provides irrefutable evidence about some event."
- Is anything ever irrefutable?
- Non-repudiation generates mathematical evidence.
- This does not necessarily mean it is accepted, e.g. in court of law.
- In Sweden, this is regulated in law SFS 2000:832 (among others).

Security Objectives

Security and Reliability

- Reliability addresses the consequences of unintensional errors.
- On a PC (offline), you are in control of the software components sending input to each other.
- Once online, hostile adversaries provide input.
- To make software more reliable, it is tested against typical usage patterns.
- To make software more secure, it has to be tested against non-typical usage patterns.
- In fact, you can never be sure the software is secure by just testing – you need to prove it secure.

Overview

1. Definitions
   - Security Strategies
   - Data and Information
   - Security Objectives
2. Dilemmas of Security
   - The Fundamental Dilemma of Security
   - Another Dilemma of Security
3. Principles of Security
   - Dimensions of Security
   - Fundamental Design Decisions
   - Focus and Placement of Control
   - Complexity or Assurance
   - Centralised or Decentralised Controls
   - The Layer Below

The Fundamental Dilemma of Security

Situation

Security-unaware users have specific security requirements but no security expertise.

Dilemma

- If you provide them with a standard ("best-practice") solution it might not meet their requirements.
- If you want to tailor your solution to the users' needs, they may be unable to tell you what they require.

Another Dilemma of Security

- The other dilemma is the conflict between security and usability.
- Security mechanisms may need additional computational resources.
- Security interfers with the ordinary working pattern which users are accustomed to.
- Effort has to be put into managing security.

Overview

1. Definitions
   - Security Strategies
   - Data and Information
   - Security Objectives
2. Dilemmas of Security
   - The Fundamental Dilemma of Security
   - Another Dilemma of Security
3. Principles of Security
   - Dimensions of Security
   - Fundamental Design Decisions
   - Focus and Placement of Control
   - Complexity or Assurance
   - Centralised or Decentralised Controls
   - The Layer Below

Dimensions of Security

- On the horizontal axis we have user (subject) in one end and resource (object) in the other.
- On the vertical axis we have hardware in the bottom and application software in the top.

Fundamental Design Decisions

1. Where to focus security controls?
2. Where to place security controls?
3. Complexity or assurance?
4. Centralised or decentralised control?
5. Blocking access to the layer below?

Focus and Placement of Control

- Focus of control may be on data, operations, or users.
- If we look at the control of integrity, its requirements may refer to rules on:
  - Format and content of data items, e.g. account balance must be integer.
  - Operations that may be performed on a data item, e.g. credit, debit and transfer.
  - Users who are allowed access to a data item, e.g. account holder and bank clerk.

Focus and Placement of Control

Man–Machine Scale

- Applications (focus on users, information)
- Services (middleware)
- Operating system
- Operating system kernel
- Hardware (focus on data, generic)

Complexity or Assurance

- Often the location of a security mechanism in the man–machine scale correlates with its complexity.
- Generic mechanisms are simple, applications are usually feature rich.
- Back to the fundamental dilemma:
  - Simple generic mechanisms may not match specific security requirements.
  - To choose the right features from a rich selection, you need to be a security expert.
  - Security-unaware users are at a loss.

Centralised or Decentralised Controls

- Within the domain of a security policy, the same controls should be enforced everywhere.
- Having a centralised entity to do this makes it easy to achieve uniformity, however, this entity may become a bottleneck.
- A distributed solution might be more efficient, however, then you must ensure they all enforce consistently with each other.

The Layer Below

- Every security mechanism defines a *security perimeter*.
- The parts of a system which can malfunction without breaking the mechanism are said to be outside the perimeter.
- The parts of the system that can disable the mechanism are within the perimeter.

The Layer Below

- Attackers will try to bypass security mechanisms.
- How do you ensure an attacker cannot get access to the layer below the security mechanism?

The Layer Below

- Recovery tools, read the sectors directly from the disk; logical access control is implemented in the operating system.
- Buffer overruns, a value assigned to a variable is too large for the memory buffer allocated; memory allocated for other variables may be overwritten.
- Side-channel analysis, look at the time different operations take to perform, look at power consumption.
- Javascript to perform security checks? The client can use a Web page without Javascript enabled.

Referenser I

[Han73] Per Brinch Hansen. *Operating system principles*. Prentice-Hall, Inc., 1973.