Lecture 1
Introduction to Security

Dieter Gollmann
Microsoft Research
diego@microsoft.com

Introduction

- Security objectives
- Security strategies
- Distributed systems security = computer & communications security
- Aspects of computer security
- Fundamental design principles for computer security

Security objectives

- Confidentiality: prevent unauthorised disclosure of information
- Integrity: prevent unauthorised modification of information
- Availability: prevent unauthorised withholding of information or resources
- Other aspects: accountability, authenticity
- Definitions from ITSEC: European Information Technology Security Evaluation Criteria

Confidentiality

- Historically, security and secrecy were closely related; sometimes, security and confidentiality are used as synonyms
- Prevent unauthorised disclosure of information (prevent unauthorised reading)
- Privacy: protection of personal data
- Secrecy: protection of date belonging to an organisation

Integrity

- ITSEC: prevent unauthorised modification of information (prevent unauthorised writing)
- D.R. Clark, D.R. Wilson: A Comparison of Commercial and Military Computer Security Policies, 1987 IEEE Symposium on Security and Privacy, pp.184-194: No user of the system, even if authorized, may be permitted to modify data items in such a way that assets or accounting records of the company are lost or corrupted.

Integrity

- Orange Book (US Trusted Computer Systems Evaluation Criteria):

  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 (integrity synonymous for external consistency)
- In communications: detection and correction of intentional and accidental modifications of transmitted data

Availability

- IS 7498-2 (Basic Reference Model for Open Systems Interconnection (OSI) Part 2: Security Architecture): The property of being accessible and usable upon demand by an authorised entity
- Denial of Service (DoS): The prevention of authorised access of resources or the delaying of time-critical operations
- Distributed denial of service (DDoS) is receiving a lot of attention and systems are now designed to be more resilient against these attacks

A remark on terminology

- There is no single definition of security
- When reading a document, be careful not to confuse your own notion of security with that used in the document
- A lot of time is being spent - and wasted - trying to define an unambiguous notation for security
- Resources:
  - http://www.radium.ncsc.mil/tpep/process/faq.html
  - http://www.cesg.gov.uk/assurance/iacs/itsec/index.htm
  - ftp://ftp.cse-cst.gc.ca/pub/criteria/CTCPEC

Security strategies

- Prevention: take measures that prevent your assets from being damaged
- Detection: take measures so that you can detect when, how, and by whom an asset has been damaged
- Reaction: take measures so that you can recover your assets or to recover from a damage to your assets

Example 1 – Private Property

- Prevention: locks at doors, window bars, walls round the property
- Detection: stolen items are missing, burglar alarms, closed circuit TV
- Reaction: call the police, replace stolen items, make an insurance claim …
- Footnote: Parallels to the physical world can illustrate aspects of computer security but they can also be misleading

Example 2 – E-Commerce

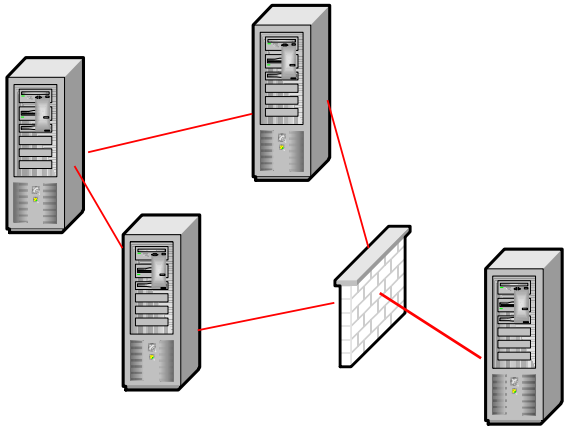
- Prevention: encrypt your orders, rely on the merchant to perform checks on the caller, don't use the Internet (?) …
- Detection: an unauthorized transaction appears on your credit card statement
- Reaction: complain, request new card number, etc.
- Footnote: your credit card number has not been stolen.

Security Policies

- Organisational security policy: Laws, rules, and practices that regulate how an organisation manages and protects resources to achieve its security policy objectives.
- Automated security policy: Restrictions and properties that specify how a computing system prevents violations of the organisational security policy.

- D. F. Sterne: On the Buzzword 'Security Policy', 1991 IEEE Symposium on Research in Security and Privacy, pages 219-230

Distributed systems



Distributed systems security

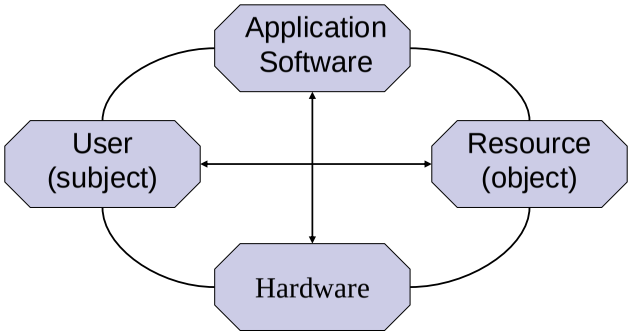
- Distributed systems: computer systems connected by a network
- Communications (network) security: deals with security aspects of the communications links
- Computer security: deals with security aspects related to the end systems; today, this is the difficult part
- Application security: relies on both to provide services securely to end users

Computer Security

- Access control (authorisation): prevention and detection of unauthorised actions by users of a computer system
  - How to design access control systems
  - How to support application security policies
- Secure software: software that can cope with malicious inputs (important paradigm shift from the PC world to the Internet)

Principles of Computer Security

The Dimensions of Computer Security



1st Fundamental Design Decision

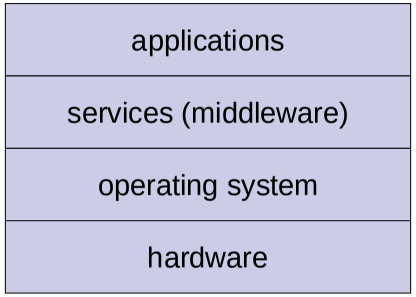
Where to focus security controls?

The focus may be on data – operations – users; e.g. integrity requirements may refer to rules on

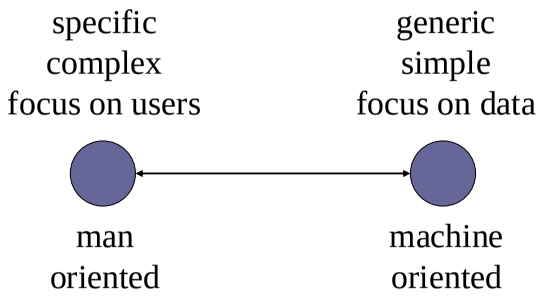
- Format and content of data items (internal consistency): account balance is an integer
- Operations that may be performed on a data item: credit, debit, transfer, …
- Users who are allowed to access a data item (authorised access): account holder and bank clerk have access to account

2nd Fundamental Design Decision

Where to place security controls?



A Man-Machine Scale



Lower layer mechanisms tend to be more generic, upper layer mechanisms are more likely to address individual user requirements

Data & Information

- Data are physical phenomena chosen by convention to represent certain aspects of our conceptual and real world. The meanings we assign to data are called information.
- Information and data lie on the two ends of the man-machine scale
- The distinction between data and information can be subtle but causes some of the more difficult problems in computer security

Data & Information

- Controlling access to information may be elusive and need to be replaced by controlling access to data
- If information and corresponding data are closely linked the two approaches give very similar results, but this is not always the case
- Covert channels: response time or memory usage may signal information
- Inference in statistical databases: combine statistical queries to get information on individual entries

3rd Fundamental Design Decision
Complexity or Assurance?

- The location of a security mechanism on the man-machine scale is often related to its complexity
- Generic mechanisms are simple, applications clamour for feature-rich security functions
- Do you prefer simplicity - and higher assurance - to a feature-rich security environment?

The Fundamental Dilemma of Computer Security

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

- Simple generic mechanisms may not match specific security requirements. To choose the right features from a rich menu, you have to be a security expert.
- Security unaware users are in a no-win situation

Security Evaluation

- To check whether a system delivers the security services promised, one has to state the function of the security system and the required degree of assurance (trust) in its security
- To gain high assurance, the security system has to be examined in close detail
- There is a trade-off between complexity and assurance. The higher an assurance level you aim for, the simpler your system ought to be.
- Feature-rich security and high assurance do not match easily

4th Fundamental Design Decision
Central or decentralized control?

- Within the domain of a security policy, the same rules should be enforced.
- With a single entity in charge of security, it is easy to achieve uniformity but this central entity may become a performance bottleneck. Distributed solutions may be more efficient but added care has to be taken to guarantee that different components enforce a consistent policy.
- Should the tasks of defining and enforcing security be given to a central entity or should they be left to individual components in a system?

5th Fundamental Design Decision
Blocking access to the layer below

- Every protection mechanism defines a security perimeter (boundary).
- The parts of the system that can disable the mechanism lie within the perimeter, the parts of the system that can malfunction without compromising the mechanism lie outside.
- Attackers try to bypass protection mechanisms; corollary to the second design decision: How do you stop an attacker from getting access to a layer below your protection mechanism?

The Layer Below - Examples

- Recovery tools like Norton Utilities recover data by reading memory directly and then restoring the file structure. Such a tool can be used to circumvent logical access control as it does not care for the logical memory structure
- Unix treats I/O devices and physical memory devices like files. If access permissions are defined badly, e.g. if read access is given to a disk containing read protected files, then an attacker can read the disk contents and reconstruct the files.

More examples

- Object reuse: in a single processor system, when a new process becomes active, it gets access to memory positions used by the previous process. You have to avoid storage residues, i.e. data left behind in the memory area allocated to the new process.
- Backup: whoever has access to a backup tape has access to all the data on it. Logical access control is of no help and backup tapes have to be locked away safely to protect the data.
- Core dumps: same story again

Summary

- Security terminology is ambiguous with many overloaded terms
- Distributed systems security builds on communications security and on computer security
- In computer security, two major challenges are the design of access control systems that fit the requirements of the Internet and the design of secure software
- In security, understanding the problem is more difficult than finding the solution

Books on Computer Security

- D. Gollmann: Computer Security, Wiley & Sons, 1999
- C.P. Pfleeger: Security in Computing, Prentice-Hall, 1997
- L. Gong: Inside Java 2 Platform Security, Addison Wesley, 1999
- John Viega & Gary McGraw: Building Secure Software: How to Avoid Security Problems the Right Way, Addison Wesley, 2001
- Michael Howard & David LeBlanc: Writing Secure Code, Microsoft Press, 2001
- J.S. Park: AS/400 Security in a Client/Server Environment, Wiley & Sons, 1995