Foundations of Computer Security

Overview of Today's Lecture:

- Definitions
- Fundamental Dilemma
- Data vs. Information
- Principles of Computer Security
- The Layer Below
- Summary

Definitions:

- Security
- Computer Security
- Confidentiality
- Integrity
- Availability
- Accountability
- Nonrepudiation
- Reliability

Security:

- Security is about the protection of assets
- Knowledge of assets and their value is vital

Protection measures:

- Prevention – sometimes the only feasible measure
- Detection
- Reaction

Computer Security:

Traditional definition using the following:

- Confidentiality
- Integrity
- Availability

- Debatable !
- Priority ?
- Incomplete list ?

Confidentiality (Privacy, Secrecy):

- The prevention of unauthorised users *reading* sensitive information

- *Privacy* – protection of personal data
- *Secrecy* – protection of data of an organization

- Hide document's content ?
- Hide document's existence ? (Unlinkability and Anonymity)

Integrity

Informally

-Making sure everything is as it is supposed to be.

Formally

-Integrity deals with the prevention of unauthorised ***writing.***

Data Integrity

"The state that exists when computerised data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction."

Availability

"The property of being accessible and useable upon demand by an authorised entity."

-We want to prevent *denial of service*

Denial of service

"The prevention of authorised access to resources or the delaying of time-critical operations."

Accountability

- Users should be held responsible for their actions
- Thus system has to identify and authenticate users
- Audit trail has to be kept

"Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party"

Nonrepudiation

- Nonrepudiation provide un-forgeable evidence
- Evidence verifiable by a third party

- *Nonrepudiation of origin* – sender identification
  delivery – delivery confirmation

The concept of irrefutable evidence is alien to most legal systems !

Reliability

Reliability - (accidental) failures

Safety - impact of system failures on their environment

Security is an aspect of reliability and vice versa!

Dependability

"The property of a computer system such that reliance can justifiably be placed in the service it delivers"

Our Definition

Computer Security – What?

"Deals with the prevention and detection of unauthorised actions by users of a computer system"

Computer Security – Why?

"Concerned with the measures we can take to deal with intentional actions by parties behaving in some unwelcome fashion"

To Remember

- *No single definition of security exists*
- *When dealing with security material, do not confuse your notion of security with that used in the material*

The Fundamental Dilemma

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

Security evaluation - evaluates the function of a security service and its assurance of functionality

The Orange Book – guideline for evaluating security products (1985)

ITSEC - separates functionality and assurance
- introduces *Targets of Evaluation*

The Fundamental Dilemma cont.

In contrast conflict between security and ease of use:

- Engineering trade-off:
  - Security mechanisms need increased computational resources
  - Security interferes with working patterns of users
  - Managing security is work – thus better GUI wins

Data vs. Information

- Security is about controlling access to information and resources
- This can be difficult, thus controlling access to data is more viable

Data – represents information

Information – (subjective) interpretation of data

- Problem of inference

Principles of Computer Security

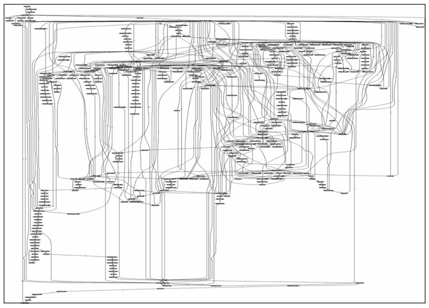
Computer security is NOT rocket science if:

- approached in a systematic, disciplined & well planned manner, from the birth of a developed / designed system

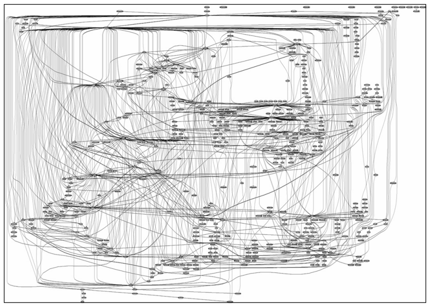
However:

- if added as an afterthought to an existing complex system -> TROUBLE!

Linux with **Apache** – serving a website



Windows with **IIS** – serving a website



Principles of Computer Security

Fundamental Design parameters:

- Focus of Control
- The Man-Machine Scale
- Complexity vs. Assurance
- Centralised or Decentralised Controls
- The Layer Below

Focus of Control

1st Design Decision

In a given application, should the protection mechanisms in a computer system focus on:

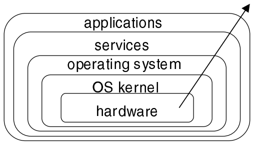
- *Data*
- *Operations*
- *Or users?*

The Man-Machine Scale

2nd Design Decision

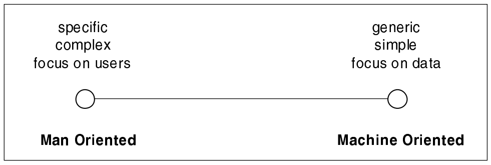
In which layer of the computer system should a security mechanism be placed?

applications
services
operating system
OS kernel
hardware



The Man-Machine Scale

Combining previous two design decisions:



specific
complex
focus on users — generic
simple
focus on data

Man Oriented — **Machine Oriented**

Related to the distinction between data (machine oriented) and information (man oriented)

Complexity vs. Assurance

3rd Design Decision

Do you prefer simplicity- and higher assurance- to a feature-rich security environment?

This decision is linked to the fundamental dilemma!

Feature-rich security systems and high assurance do not match easily

Centralised or Decentralised Controls

4th Design Decision

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?

Central entity – could mean a bottleneck

Distributed solution – more efficient but harder to manage

The Layer Below

Every protection mechanism defines a *security perimeter*

Security perimeter – parts of a system that can be used to disable the protection mechanism

5th Design Decision

How can you prevent an attacker getting access to a layer below the protection mechanism?

The Layer Below

To watch out for -

- Recovery Tools
- Unix Devices
- Object Reuse (Release of Memory)
- Buffer Overruns
- Backup
- Core Dumps

Summary

- Definitions
- Fundamental Dilemma
- Data vs. Information
- Principles of Computer Security
- The Layer Below

Next Lecture

Identification and Authentication

End