Cryptography and Security

Bruno MARTIN

M1 Int'l
University Nice Sophia Antipolis

Motivation

- Increase of the exchanges over the Internet :
  - informations
  - commercial
- Changing work habits :
  - more communications
  - more mobility
  - more subcontractors.

Thus, less control on information

General Overview

Lecturer : B. Martin

5 lectures, 5 exercises / labs
Goal : understand the operation mode + use of security tools for :

- a machine
- a LAN
- accessing the Internet

And the basic knowledge for understanding the tools :

- cryptolography basics
- introduction to security

Networking «Environment»

- Yesterday :
  - centralized
  - paper exchange
  - no remote access
- Today :
  - distributed, either on different sites or locally
  - remote access
  - subcontractors increase

More and more computer-dependant : IS become crucial. 98% of the companies admit an addiction from moderate to severe.

Consequences

- communications increase, risks increase :
  - various frauds
  - hacking

Risk management

Consists of the realisation and keeping up to date :

- the **inventory** of the **assets**
- express the **security needs** of the assets
- risk analysis over the assets
- manage these risks to reduce them

Some methods : MEHARI or EBIOS (ISO 27001 related)
and educate staff (security letters, NDAs,...)

Network Threats

- message interception
  - passwords cracking
  - informations stealing
- systems intrusion
  - information stealing
  - viruses
  - malwares (mostly ransomwares)
  - embezzlement
- fake customers, fraud
- incidents

From the inside as well as from the outside

Assets

Include the goods of the organization and its human resources ;
3 kinds :

- assets managed through the IS (infos and business processes)
- technical assets constituting the IS (hardware, software, appliance,...)
- environmental assets (people and building)

Assets

Generally inventoried companies' assets :

- 96% physical assets (info/comm hardware)
- 93% software
- 82% information
- 57% info/comm services
- 41% staff and their knowledge
- 20% intangible value (reputation, image)

Cost of incidents

CLUSIF-APSAD (France) : statistics of incidents over 16 years :

	Loss (M€)		
Origin	1984	1994	2000
human Factor	309	280	177
Errors	269	426	338
Fraud	335	998	???

80% of losses are due to frauds from staff members.

Failures

- 58% design errors in the software or procedure
- 47% loss of essential service (energy, network,...)
- 46% usage errors
- 44% theft or disappearance
- 37% internal breakdown
- 36% viruses
- 8% natural disaster

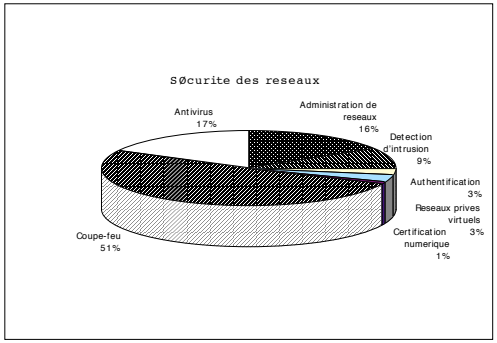
Some facts

Faults Frequency vs financial impact

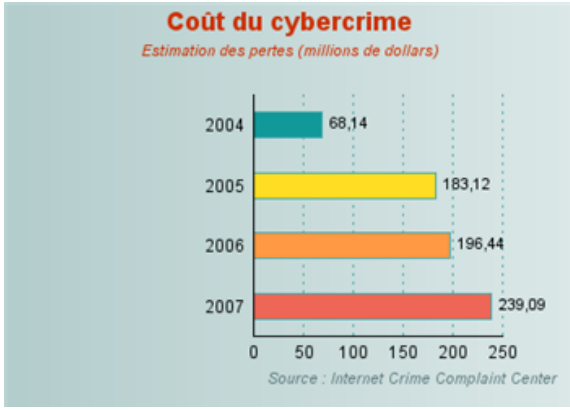
Origin	Frequency	Financial Impact
Human Errors	37%	29%
Faults	58%	21%
Fraud	5%	50%

Some facts

IT expenses in the US (Source : Goldman Sachs)

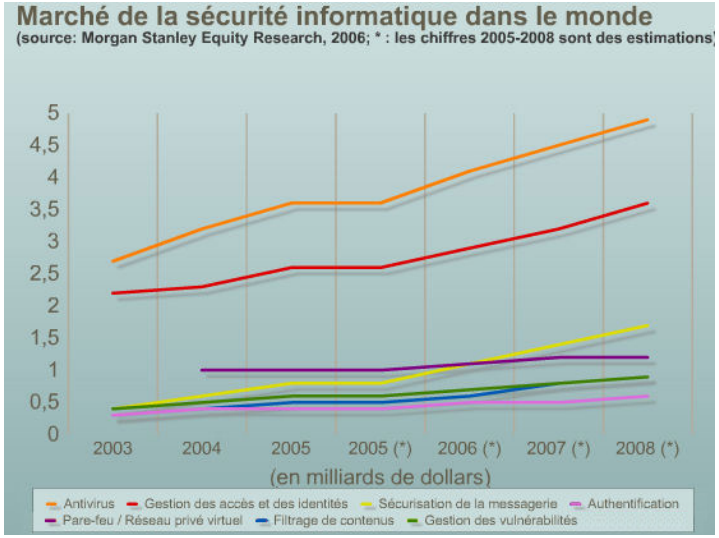


Some statistics



327 billion € in 2014

Some statistics



Goals of security

Increase the security in front of identified threats. Try to reach

- **disponibility :** the system is supposed to complete tasks within a certain time and with a certain QoS
- **integrity :** no information change by unauthorized people
- **confidentiality :** keep the information secret
- **authentication :** determine whether someone or something is, in fact, who or what it is declared to be

Two kinds of security

- **Data security :** concerns what is inside the computer (crypto+error correcting codes)
- **Network security :** concerns data when they are on the move between end systems.

Outline

1. **Introduction**
2. **General concepts**
3. **Security auditing**
4. **Crypto components**

OSI Standard (reminder)

Defines standards for data exchange

7	application layer
6	presentation layer
5	session layer
4	transport layer
3	network layer
2	data link layer
1	physical layer

1. Introduction

- What do we need to protect
  - data
  - resources
  - reputation
- against whom ?
- how can we protect ?
- why ?

Protect

- **Data :** informations kept inside the system ;
- **Ressources :** Systems (usually the computers) ;
- **Your reputation**

Protect the resources

Each resource has a cost (HD, printer, CPU time) which shouldn't be accessed by an intruder.
A sys-engineer doesn't wish to re-install OSes if the systems have been altered or corrupted or used to hack other computers or systems.

Data protection

5 main characteristics :

- **Confidentiality :** The information shouldn't be available to an unauthorized user nor a process
- **Integrity :** information should not be modified nor destroyed by an unauthorized user
- **authentication :** determine whether someone or something is, in fact, who or what it is declared to be
- **Disponibility :** information has to be available to authorized users
- **Provability :** usage of logs

Protect the reputation

Why ?
If your identity has been corrupted and the intruder commits evil actions under your name (legal problems. . .)
A site failure usually means that your organisation becomes untrusted.

1. Introduction

- What do we need to protect
  - data
  - resources
  - reputation
- against whom ?
- how can we protect ?
- why ?

Typology of attacks & risks

- **Intrusion :** any kind of (from the network, by a local terminal or by a program)
- **DOS :** attack against the availability of the systems. Classical consequence of viruses or *ping of death* like low orbit ion cannon
- **information theft :** it is not mandatory to penetrate a system to gain access to some information. A passive attack like sniffing may be sufficient (example : login).
- **ransoming :** a type of maltware designed to block access to a computer system until a sum of money is paid.

Typology of attacks

- **passive :**
  - unauthorized sniffing
  - unauthorized access to some information
- **active :**
  - unauthorized control of a computer
  - information change
  - acces to services
  - *DOS*

Who's sniffing or changing information ?

- governements :
  - NSA in the US
  - DGSE/DCRI in FR
- Mafia
- competitors
- hackers

Typology of attackers

- **Joyriders :** for fun
- **Vandales :** a will to damage by pleasure or for money
- **Score keepers :** intellectual challenge
- **Spies :** for the money (industrial secrets, economic intelligence)

Logical Attacks

- **Disguise :** take ownership of someone else identity
- **Mystification :** simulate the behavior of another machine, site to gather information like login, etc
- **Replay :** variant of disguise allowing the attacker to gain access to a system by replaying a legitimate connection sequence
- **Substitution :** intercept the disconnection sequence of a legitimate user and substitute the identities
- **Saturation :** against the availability of a resource (HD or data link). aka *ping of death* or *NT chargen*
- **Troyan :** program containing a hidden functionality
- **Trapdoor :** hidden access point in a software put in place by its developer

Physical attacks

Require a physical access to the installations (or close to)

- **interception :** gathering electromagnetic signal from a computer screen, sat or radio-frequencies listening
- **jamming :** DOS against the system.
- **sniffing :** gathering unencrypted information traveling in the network
- **scanning :** send a set of info to the system which provide a positive reply which is analyzed.
- **troyan :** the intruder attempts to introduce backdoors into the system.

1. Introduction

- What do we need to protect
  - data
  - resources
  - reputation
- against whom ?
- how can we protect ?
- why ?

How to protect ?

- **No protection** add nothing to the basic installation process
- **Security by obscurity** hiding the system's existence for a small server or home computer which shouldn't interest a hacker
- **Host security** securing host by host. Good for several computers. Not scalable.
- **Network security** access control to the end systems instead of securing host by host. Requires firewalls, authentication and crypto.

1. Introduction

- What do we need to protect
  - data
  - resources
  - reputation
- against whom ?
- how can we protect ?
- why ?

What to protect ?

Computer security covers

- **Physical aspect** : thefts, physical risks (electrical, fire, water...)
- **Logical aspect** : intrusions, logical bombs, viruses,...

avoid everything which provides a system failure or unavailability.

The system's security is as good as its weakest component

Why ?

- IS have a cost : the hardware and software cost (CPU, HD, net. appliances, net components, subscriptions,...)
- informations have a cost : confidentiality ; their lost also has a value (human time for data recovering or system reconstruction, when possible)
- a major failure is usually fatal for a business company.
- systems are not isolated anymore and LANs become wider and wider

2. Concepts

- Security policy
- Security models
- Services and mechanisms

Security policy

Goal : inform users, staff and officers of the conditions to fulfill to protect the technological assets of the company.
It defines the mechanisms to protect and to audit the system against the identified threats.
Usually starts with the sentence :

Everything which is not authorized is forbidden

For more details, one can read RFC2196

Security policy

Set of rules defining on what security applies

- define the importance of the information which is stored in the system, how it is protected and which resources have to be accessed
- one policy by organism
- a security policy can cover secrecy, integrity or both
- every policy is set up by an authority
- domain : set of informations and resources which is covered by the same policy (sometimes realm)

Who defines the security policy ?

All the staff must agree on the security policy for the security policy to become effective. It is more usually defined by

- the security officer
- the tech staff responsible
- the group in charge of auditing and security
- user representatives
- chief executive officer
- sometimes a lawyer

Characteristics of a security policy

1. it should be implementable
2. it should be improved by security measures and by sanctions
3. it must clearly state everyone's responsibility

Example of security policy

Secret data classification :

- every information has a security level
- everyone has a clearance level
- security level and clearance level consist in
  - a confidentiality level : (unclassified, confidential, secret, eyes only)
  - a set of domains (crypto, OTAN, NBC,...)
  - order relation :
    unclassified $<$ confidential $<$ secret $<$ eyes-only
    set of domain A **dominates** set of domain B if $B \subset A$.

Security policy contents

- purchasing policy for safety equipment
- a policy for respecting the individual rights (reading e-mails)
- access policy and data ownership with adequate error displays
- computer accounts management with audit
- authentication policy of the users
- define the resources availability, fault tolerance, OS and hardware updates and upgrades
- intrusions log

Example of security policy

- person X has the right to read document D if
  clearance(X) $\geq$ confidentiality(D) and
  set of domain(X)$\supseteq$ set of domain(D)

This policy doesn't cover information integrity.

2. Concepts

- Security policy
- Security models
- Services and mechanisms

Security models

Security models for the secrecy :

- access control models ; control the access of subjects to objects
- information flow models. control data transmission between objects

Very few models take integrity into account
None take availability into account

Security models

Formal expression (math) of the security policy
A security model contains :

- state variables (aka. subjects, objects, rights)
- transition functions

Goal : prove that every possible state of the system is coherent with a set of properties to fulfill.

Principles

- identity : is there a unique ID for each user, program, object or resource ?
- responsibility : are users responsible of their actions ?
- audit : is there a log of the user's actions ?
- authorizations : manage who has the right to do what.
- least privilege : what is the minimum necessary to complete a task ?
- sealing : different tasks should not interact
- redundancy : manage backups and redundancy, failure tolerance

Biba

The Biba Model (K.J. Biba, 1977), is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity.
Data and subjects are grouped into ordered levels of integrity.
The model is designed so that subjects may not corrupt objects in a level ranked higher than the subject, or be corrupted by objects from a lower level than the subject. Developed to circumvent a weakness in the Bell LaPadula model which only addresses data confidentiality.

Biba

Integrity level of an object is defined by measuring the integrity loss when the object is modified (like deleting an OS)
Integrity level of a subject is defined according to the principle of least privilege for completing a task.
Biba uses 5 different policies.

Biba

- S, set of subjects who can process information.
- O, set of objects storing informations
- I, set of integrity levels
- *il*, function defining the integrity level of a subject or an object
- *cl* function defining the corruption level of a subject or an object
- $\leq$, partial order on integrity levels
- min, function returning the greatest lower bound on a set of integrity levels
- o, capacity of a subject to observe an object
- m, capacity of a subject to modify an object
- i, capacity of a subject to call an object

Biba

1st specifies that the subject integrity level is not static but depends on its past behavior when accessing an object :

$$il'(s) = \min\{il(s), il(o)\}$$

Second plays is the same for objects

$$il'(o) = \min\{il(s), il(o)\}$$

Third measures the possible data corruption

$cl'(s) = \min\{cl(s), cl(o)\}$ for all accesses by s

$cl'(o) = \min\{cl(s), cl(o)\}$ for all modification by s

Biba

The 4th. defines a static integrity level for both subjects and objects :

$$s \mathbf{m} o \Rightarrow il(o) \leq il(s)$$

$$s \mathbf{i} o \Rightarrow il(o) \leq il(s)$$

Last, a subject cannot modify an object with a greater integrity level :

$$s \mathbf{o} o \Rightarrow il(o) \leq il(s)$$

New generalization

ACL allow a better access control to files.
Generalize UNIX UGO method
Exists with BSD/WIN/OSX
AC defines the actions that a **role** can execute on a **resource**.
Role : user or group
Permissions : actions like read or write
Resource : file or directory
classical UNIX if Bob wants to allow Alice to gain access to A SINGLE file... how to proceed ?

Access control by matrix (Bell-Lapaluda)

- **objects** : passive entities of the system
- **subjects** : active entities of the system which can access objects
- **access rights** : {owner, read, write, execute, join}
- **basic primitives** :
  - allow/deny a right
  - create/suppress a subject/object
- **transition rules** : if S_i has right D_j on O_k then primitive$_l$

Types permissions

- On the file system : delete, readattr, writeattr, readextattr, writeextattr, readsecurity, chown
- on files : read, write, append, execute
- on directories : list, search, add_file, add_subdirectory, delete_child

```
chmod +a ‘‘alice allow read’’ ./ressource.txt
```

ACL executed before UNIX rights as an ordered set of rules

2. Concepts

- Security policy
- Security models
- Services and mechanisms
  - Definitions
  - Security services
  - Security mechanisms

Security services

Defined in ISO 7498-2 :

1	Entity authentication
2	Access control
3	Data confidentiality with or without connection
4	Data integrity with or without recovery
5	non repudiation with proof of origin non répudiation with proof of delivery

Services and mechanisms

- Security policy is applied by means of security services
  provide a mean to implement the security policy
  Some services are useless for a given security policy :
  Example : advertising policy does not require secrecy.
- Each service fights again a particular set of threats
  Example : secrecy forbids unauthorized access to confidential data.
- Security services are implemented by security mechanisms
  some services may use the same mechanism
  Example : hash functions are used for both authentication and integrity.

Authentification

- Entity authentication provides checking of a claimed identity at a point in time.
- Typically used at start of a connection.
- Addresses masquerade and replay threats.
- Origin authentication provides verification of source of data.
- Does not protect against duplication or modification of data.
- GSM, web servers

Access control

- Provides protection against unauthorized use of resource, including :
  - use of a communications resource,
  - reading, writing or deletion of an information resource,
  - execution of a processing resource.
- Remote users

Data integrity

- Provides protection against active threats to the validity of data
- 5 types :
  - Connection integrity with recovery
  - Connection integrity without recovery
  - Selective field connection integrity
  - Connectionless integrity
  - Selective field connectionless integrity.
- MD5 hashes (SHA-3)

Data confidentiality

- Protection against unauthorized disclosure of information.
- four types
  - Connection confidentiality
  - Connectionless confidentiality
  - Selective field confidentiality
  - Traffic flow confidentiality
- Internet banking session
- Encrypting routers as part of Swift funds transfer network

Non-repudiation

- Protects against a sender of data denying that data was sent (non-repudiation of origin).
- Protects against a receiver of data denying that data was received (non-repudiation of delivery).
- Analogous to signing a letter and sending recorded delivery

Possible attribution of services by ISO layer

	1	2	3	4	5	6	7
Authentication		x	x	x			x
Access control Confidentiality	x	x	x	x		x	x
selective confidentiality						x	x
traffic secrecy	x		x				x
Integrity		x	x	x			x
Non-repudiation							x

Security mechanisms

Implement security services

- enciphering
- digital signatures
- access control
- data integrity
- authentication mechanisms
- traffic packaging
- routing control
- trusted third party

- security management (key management)
- audit
- intrusion detection

2. Concepts

- Security policy
- security models
- Services and mechanisms
  - Definitions
  - Security services
  - Security mechanisms

3. Criteria for security evaluation

- Different criteria
- Orange book

Different criteria

- *National Computer Security Center* (NCSC)
  - orange book : Trusted computer system evaluation criteria 1985
  - red book : Trusted network Interpretation of the TCSEC, 1987
- *European community*
  - Information Technology System Evaluation, 1991
  - comes from research on security models
  - important for the governments and defense
- *Bundesamt für Sicherheit in der Informationstechnik*
  - for firewalls
  - certification centers

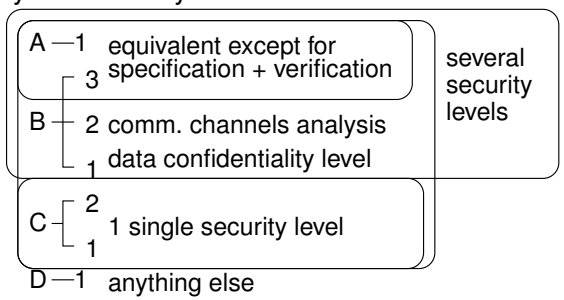
Orange Book

Based on Bell & Lapadula
hard and soft must satisfy some conditions for security policy, account management, insurance and documentation

- account management : identification, authentication, audit
- ensure that the system behaves accordingly to its specifications
- documentation on security functions, tests and design

Orange Book

Origine : command from DoD US
Utility : system security evaluation



	Description
A1	like B3 but better security management
B3	B2+ robustness against attacks
B2	B1+ security policy, security level management, bonne auth.
B1	C2+ manage security levels, data classification
C2	C1+ improved login, audit, resources isolation (memory)
C1	data protection based on the need to know. separation user/data
D	the rest

Orange Book

Proposes different security levels for the OSes with increasing security C1-C2-B1-B2-B3-A1
Example :

- A1 : SCOMP Honeywell
- B3 : Multics Honeywell, AIX IBM
- B2 : SunOS, AIX-IBM
- B1 : Solaris CMW, AIX IBM
- C2 : Solaris BSM, Solaris 2.3, IBM, DEC..