Computer Science Security
Introduction

Pierre.Paradinas@cnam.fr

le cnam

Les cours

- Introduction et définitions
- Matrice d'accès
- Politique de sécurité
- Sécurité et assurances
  - Critères communs
- Contrôle d'accès
- Information flow
- Sécurité physiques des composants

- Exposés le 20 novembre
- Visites au salon CARTES à Villepinte semaine du 18 novembre

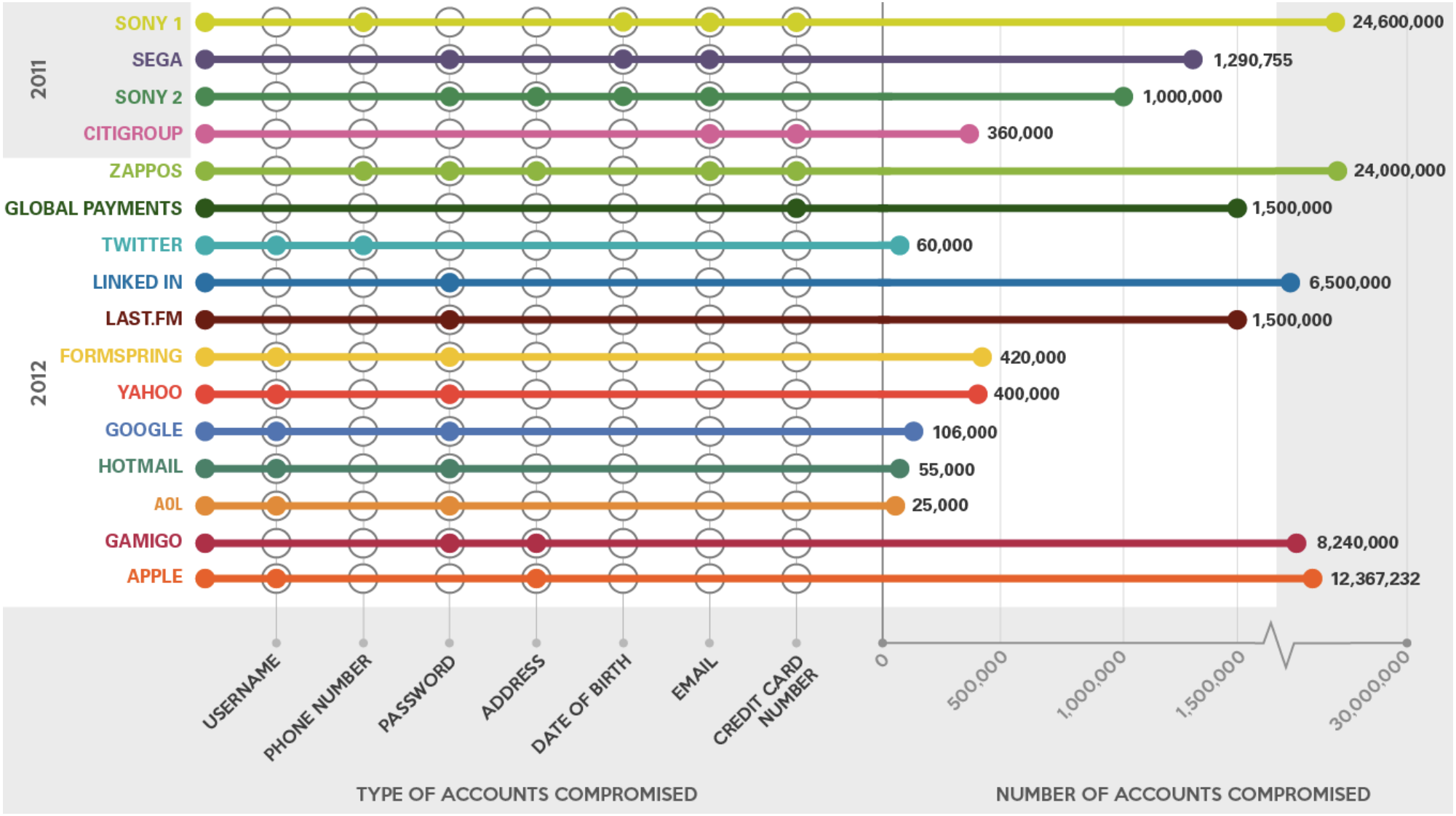
Sujet des exposés

- 1 à 2 personnes par groupe
- Sujet ouvert : proposition à faire valider
- Sujets proposés :
  - BYOD : les solutions Bull/Thales de téléphone mobile
  - Sécurité dans la JVM (state of the art et statut actuel dans les naviagteurs)
  - La sécurité des compteurs électriques et la protection de la vie privée
  - Un point précis sur la polémique PRISM (quels outils mis en oeuvre par les agences… quelle parade possible…)
  - Mozilla Social API For Firefox, Facebook Messenger Firs...
    - (tcrn.ch/WDxYtZ)
  - Automotive security (http://autosec.org)
  - La DO178-C & ARINC 653

Computer Security

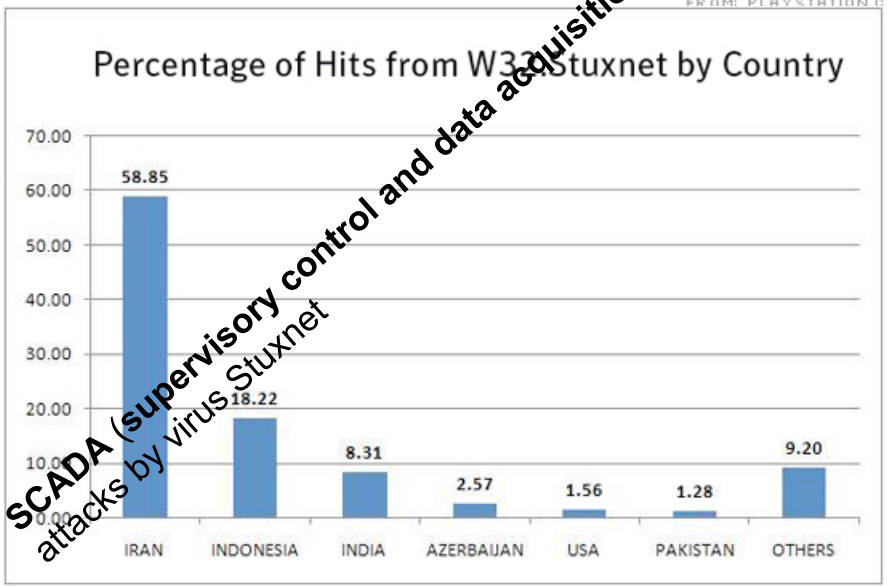
- **Introduction** & definitions
- (Secure) Design Principles
- Modern issues in security
- Bibliography

Every day there is security issue !



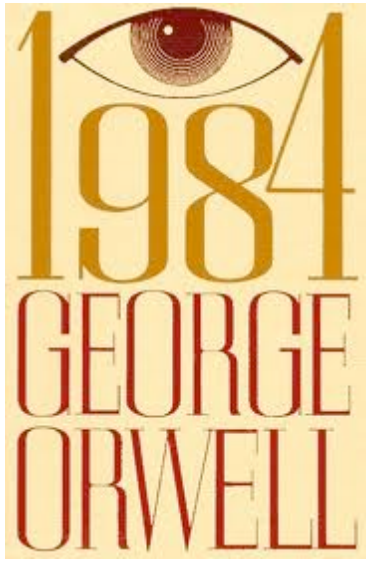
le cnam

Security a key issue



SCADA (supervisory control and data acquisition)
attacks by virus Stuxnet

facebook
Privacy issues



The New York Times

Attack on Estonia

APRIL 26-27 First data-flooding attacks on Estonia's computer networks, coinciding with the government's decision to relocate a Soviet-era World War II memorial. Web sites of Parliament, the president and the prime minister are hit.

APRIL 30 After the Web sites of several daily newspapers are brought down by cyberattacks, Estonian officials convene an emergency meeting of computer experts from Internet service providers, banks, government agencies and law enforcement. A plan is set to protect vital services, like online banking.

MAY 2 Internet service providers around the world help to block the malicious data. The flow of incoming data begins to trail off as groups of Internet addresses are blocked.

MAY 5 Police arrest a 19-year-old Estonian man of Russian descent, suspected of helping organize the attacks. He is later released. The government of Estonia says the attacks originated in Russia.

MAY 8 Estonian officials prepare for an attack expected to coincide with Victory Day, a Russian holiday on May 9. European Internet experts meeting in Tallinn volunteer to help.

MAY 9-10 Attackers invisibly take control of computers around the world to coordinate larger attacks. A huge spike in data traffic forces Hansabank, Estonia's biggest bank, to shut down its online banking network.

MAY 18 Last major wave of attacks, though some assaults continue.

le cnam

Exigences critiques sur les SEs

Secteur	Criticités			Contraintes temps-réel	Gestion de panne catas.	Exigence de certification	Normes processus de développement
	Sûreté	Sécurité	Sécur. Info				
Automobile	■	■		Dures	Oui	Moyenne en croissance (ISO 26262)	Moyens
Ferroviaire	■	■		Dures	Oui	Forte	Moyens
Aéronautique	■	■		Dures	Oui	Forte	Objectifs
Espace	■	■		Dures pour les lanceurs, faibles pour les satellites	Selon les applications, alarmes au minimum	Forte	Objectifs, mais avec préconisation de moyens
Nucléaire	■	■		Dures	Oui	Forte	Objectifs
Énergie (production, distribution, utilisation)	■	■		Dures	Alarmes	Variable	
Production industrielle	■	■		Selon le procédé	Selon le danger	Variable	
Instrumentation médicale	■	■	■	Moyennes	Alarmes	Forte	Objectifs
Bâtiment (domotique)	■		■	Selon l'application	Alarmes	Faible	
Télécoms	■		■	Selon l'application	Alarmes	Variable selon les réseaux	Moyens
Électronique grand public			■	Faibles	Non	Faible	
Logistique			■	Faibles	Non	Faible	
Infrastructures urbaines			■	Faibles	Alarmes	Faible	
Sécurité	■	■	■	Moyennes à fortes	Alarmes	Croissante	Moyens
Transaction électronique	■	■	■	Moyennes	Non	Forte	Moyens

La qualité de services dans les SEs (1/2)

Secteur	Fonctions principales						Limitations principales	Interactions entre fonctions critiques et fonctions à qualité de service
	Mesure et comm.	IHM	Optim. Confort	Optim. Process	Optim. Énergie	Qualité de service		
Automobile							Coût des composants et du logiciel	Aujourd'hui : réseaux et processeurs indépendants. Intérêt à fusionner demain ?
Ferroviaire							Nécessité d'assurer ces fonctions sans compromettre la sécurité	Il faut démontrer l'indépendance entre les fonctions S (critique) et NS (Non-critique) ⇒ ségrégation ou développement des fonctions NS avec le niveau de sécurité le plus élevé
Aéronautique							Cout, durée de vie, consommation énergétique et poids	Il faut démontrer l'indépendance entre les fonctions S (critique) et NS (Non-critique) ⇒ ségrégation ou développement des fonctions NS avec le niveau de sécurité le plus élevé
Espace							Poids et blindage des systèmes ⇒ impact sur les processeurs et la mémoire disponible	Prédominance des fonctions les plus critiques (« safety ») assurée par le hardware
Nucléaire							Cout et durée de vie (gestion de l'obsolescence)	
Énergie (production, distribution, utilisation)							Coût (production et installation), taille, alimentation et consommation énergétique	Limitées aujourd'hui, mais la capacité d'intégrer des fonctions de protection, mesure et optimisation, sans perte de confiance vis-à-vis des fonctions critiques, est un sujet important pour le futur

Secteur	Fonctions principales						Limitations principales	Interactions entre fonctions critiques et fonctions à qualité de service
	Mesure et comm.	IHM	Optim. Confort	Optim. Process	Optim. Énergie	Qualité de service		
Production industrielle	■	■		■	■	■		
Instrumentation médicale	■	■					Cout, durée de vie, consommation énergétique	
Bâtiment (domotique)	■	■	■		■		Coût (production et installation), taille, alim. et consommation énergétique	
Télécoms	■	■				■	Coûts, performances, alim. énergétique dans les pays émergents	Sécurité info pour toutes fonctions
Électronique grand public	■	■				■	Coûts	Sécurité info pour toutes fonctions
Logistique	■	■				■		Sécurité info pour toutes fonctions
Infrastructures urbaines	■	■			■	■		Sécurité info pour toutes fonctions
Sécurité					■	■		Sécurité info pour toutes fonctions
Transaction électronique			■			■		Sécurité info pour toutes fonctions, gestion de la confiance

Computer Security

- Introduction & **Definitions**
- (Secure) Design Principles
- Modern issues in security
- Bibliography

Computer Science Security Definitions

- Basics and definitions about confidentiality, integrity and availability
- About threats
- Policy and mechanisms
- Assumptions and trust
- Assurance
- From specifications to the program

Basics

- A system provides features. The **threats** may corrupt the system
- Security protects the system against threats
- Security is based on policies and mechanisms
- System security analyzing improves security
- Security is also related to trust
- Human beings are part of the system and generally the weakest link !

Basic security properties

- Confidentiality
- Integrity
- Availability

  - These properties are different and related to the system context

Basic security properties: confidentiality

- Confidentiality is the feature of information where it have to be keep “secret” and not to be “revealed”
- Examples:
  - secret key involved in a cryptographic protocol
  - information “reserved” to a group of person
  - password
  - ...

Basic security properties: integrity

- Integrity is a feature of information where there is trust on the data (or resources) in term of alterations/modifications (data integrity) and on data origin (origin integrity some time call authentication)
- Examples:
  - In a operating system, “user management” must be based on integrity. Only “user” authorized may change the rules and authorization attached to a user
  - In a fund transfer integrity is on the amount, origin and destination
- Integrity Mechanisms:
  - Prevention (how to protect)
  - Detection (how to detect if an information was altered)

Basic security properties: availability

- Availability refers to the possibility to use data or resources of a system
- Availability is part of the security issues as if some one establish conditions where the data or resources of a system are no longer available for a normal use it causes a "deny of access"
- Examples:
  - DOS on Internet are well known
  - If a bank network is not available the day before Christmas then many commercial transactions will be impossible or done without "confirmation" from the bank
- The system design (statical, expected pattern, parameters,...) defines a usage model, if it fails we enter in DOS
- DOS detection is very complex task

Threats/Attacks

- A **threat** is a potential violation of security. When the violation occurs, it is an **attack**. The attacks are performed by attackers
- A system must be prepared to prevent attacks and executes countermeasures
- 4 large classes of threat:
  - Disclosure (non authorized information are revealed)
  - Deception (acceptance of false data)
  - Disruption (interruption of operation)
  - Usurpation (non authorized control of the system)

Different threats

- Snooping (wiretapping, passive wiretapping)
- Modification
- Masquerade
- Delegation
- Repudiation of origin
- Denial of receipt
- DOS

Policy and mechanism

- Definition: A security policy is a statement of what is, and what is not allowed
  - A security policy specifies “secure” and “non secure” states and actions
- Definition: A security mechanism is a method, tool, or procedure for enforcing a security policy
- A security policy can (must) be defined by mathematical and formal technics
- Example:
  - Change its password is allowed for an entity
  - Request a proof of an identity before to accept to change a password is a security mechanism

Goals of policy and mechanism

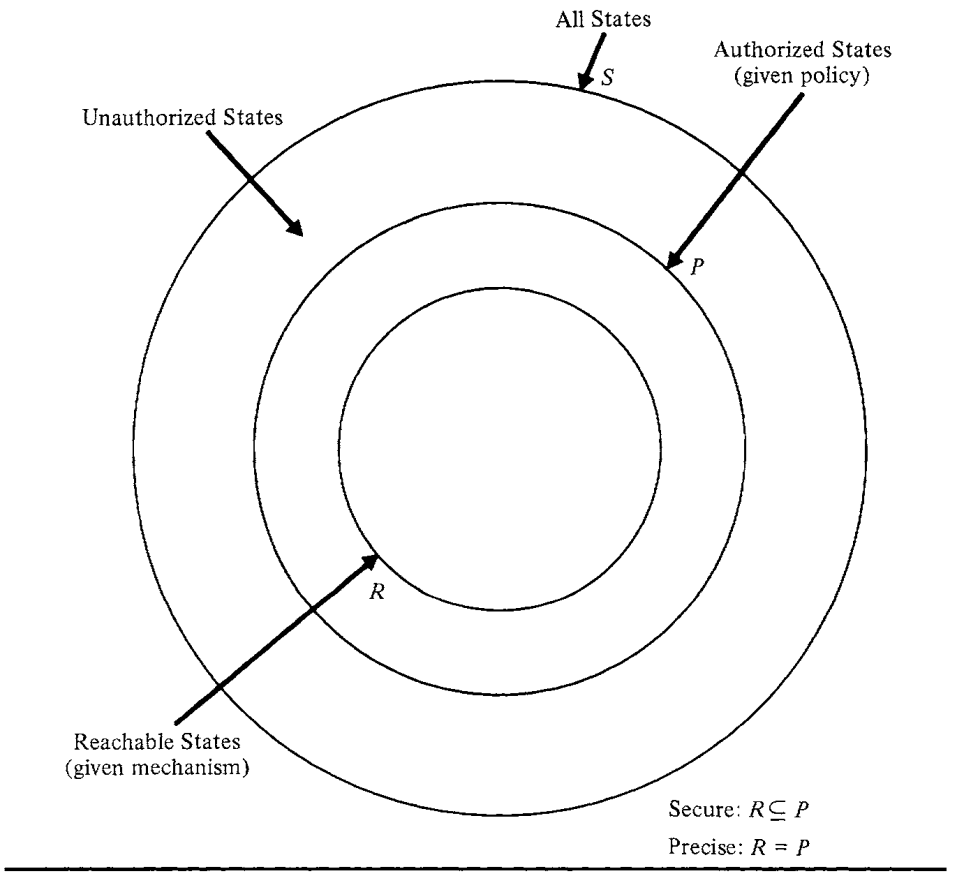
- For a given security policy security mechanisms can:
  - Prevent
    - In this case attacks fail, attacks are not efficient,
  - Detect
    - The mechanism is able to detect that attacks are performed, detected and have to be reported
  - Recovery
    - Is the set of actions necessary to put in place to reach and establish a new "secure state" of the system

Assumptions and Trust

- Security is based on assumptions:
  - Policy splits system states in two part with no ambiguity: “secure” and “non-secure”
  - Mechanism prevent to move from “secure” state to “non secure” state
- If one of these assumptions are false **then** the system is non secure
- Let P the set of system states. Let Q the set of system secure state. Let R the set of reduced system states by the mechanisms ($R \leq P$).
  - A security mechanism is secure if $R \leq Q$
  - A security mechanism is precise if $R = Q$
  - A security mechanism is broad if there are state $r \in R$ et $r \notin Q$

Security and Precision (R=P)

FIGURE 4.4 Security and precision.



Assumptions and Trust

- In real word, mechanisms are broad
- Trust in mechanisms requires assumptions:
  - Each mechanism implement one or more part of the security policy
  - The union of mechanisms implements the all policy
  - The mechanism are correctly implemented, installed and managed during the life cycle of the system

Insurance

- Trust is difficult to evaluate ? How much you trust a system ?
- How you develop your system provides an assurance level of the trust in the system
- A system is said to **satisfy** a specification if the specification correctly states how the system will work.

Specification

- Specifications are a precise statement of the system behaviors
  - It describe what the system is allow to do (and not to do)
- The specification may be formal (based on mathematical or formal language) or informal (set of phrases) description
- The level of description may be different (low or high level language description)
- The specification are not only relevant to security function but on the system itself
  - Use the same formalism is challenging and benefit for the system
- Security is a non functional property

Design and implementation

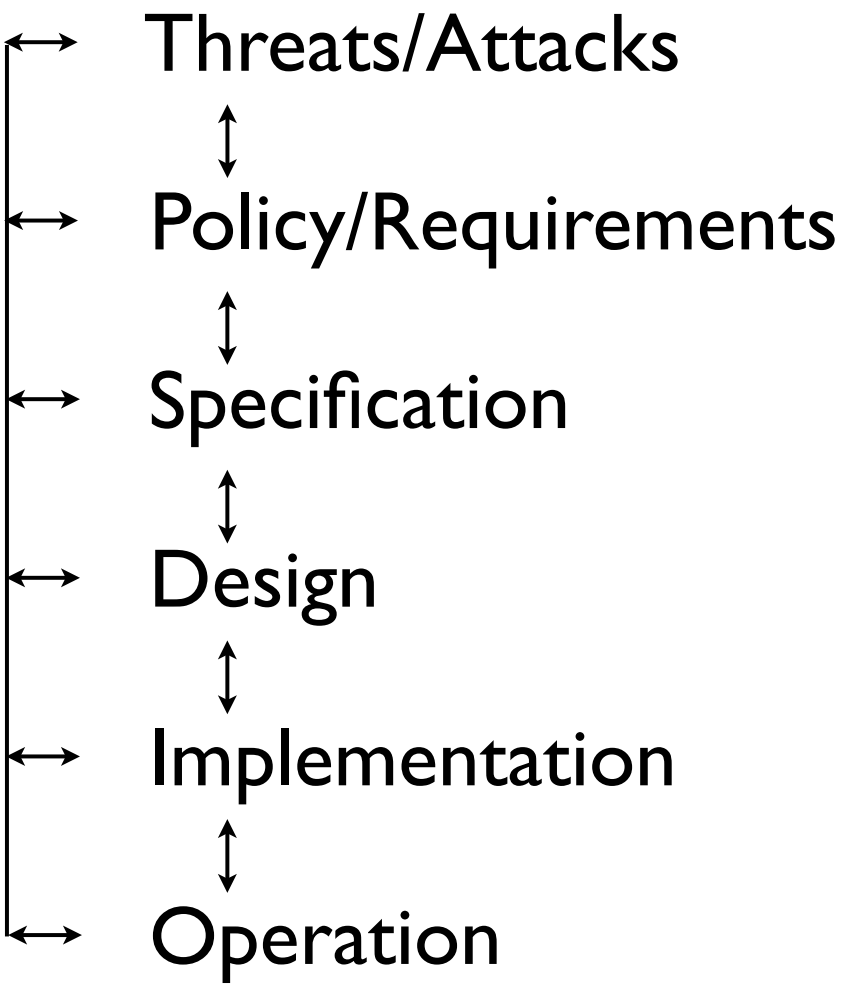
- The **design** of a system transforms the specification into a component that will implement them
  - The design is said to satisfy the specifications, in any cases, the design will not permit the system to violate the specification
- The design **implementation** realizes the functions (execute the "system functions")
  - On CS it is a program executable on an engine
  - By transitivity an implementation satisfy a system specification
  - A **program** is correct if it implementation performs as specified
    - Proof of program is very complex and difficult to do !
  - As correctness is a big issue, a posteriori technics like verification of the system by **testing** are performed

Operational issues and others points

- Cost benefit analysis
- Risk analysis
- Laws and customs (cryptography)
- Certifications
- Organizational problems
- People problems
  - inside and outside

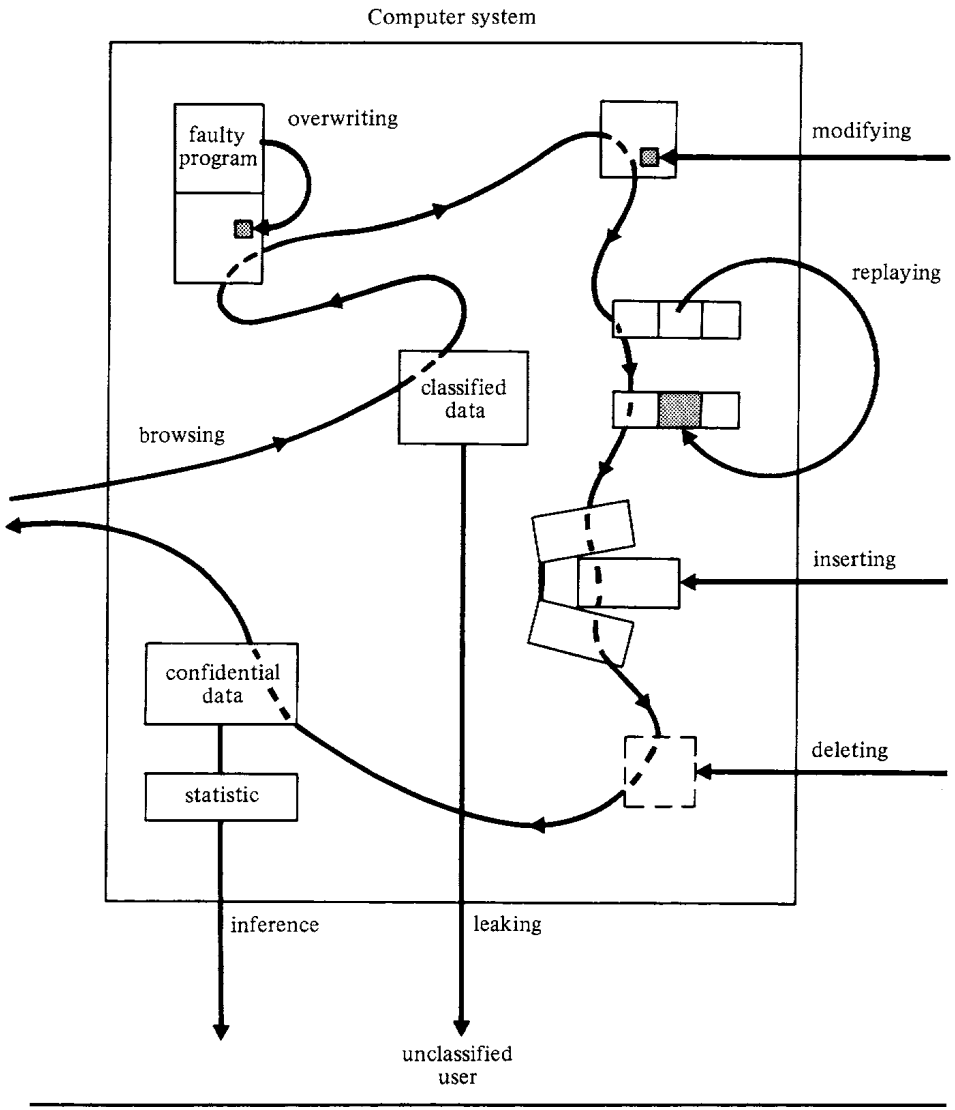
Not so simple

- The different notions are "interleaved" and nested
- System is in "real word" and the word changes !
- The cost of security have to be compared with the system (and threats) costs



From D. Denning books

FIGURE 1.4 Threats to data stored in computer systems.



Computer Security

- Introduction & Definitions
- **(Secure) Design Principles**
- Modern issues in security
- Bibliography

Design principles

- As in all system design phase is essential
- In security, following principles avoid some classical mistakes, errors, ... the principles are not an insurance but may help !
- The principles
  - The principle of **Least Privilege** states that a subject should be given only those privileges that it needs in order to complete its task
    - Program or process have only access to their data. A wrong program will not be able to modify data of an other program or process
    - The principle of **Fail-Safe Defaults** states that, unless a subject is given explicit access to an object, it should be denied access to that object
  - If we come back to privilege modes, there is a contradiction with this principle. In a super mode all access are allowed and its more large than the restriction on the objets

Design Principle (Cont'd)

- The principle of **Economy Mechanism** states that the security should be as simple as possible
  - Doesn't build a "gaze factory"

Design Principle (Cont'd)

- The principle of **Complete Mediation** requires that all accesses to object be checked to ensure that they are allowed
  - Let a subject request to read a file F. If it is allowed to read the file and the file is read in different step. After some step if the status of the file change (i.e. the right granted is remove) the subject may continue to read the file

Design Principle (Cont'd)

- The principle of **Open Design** states that the security of a system is not based on secrecy of its design and implementation
  - It is not true to think that secret design or implementation increase the security...
  - In cryptography publication of algorithms and protocols improve the security because the community is able to see the design and to evaluate the strength of it

Design Principle (Cont'd)

- The principe of **Separation of Privilege** states that a system should not grant permission based on a single condition
- Example:
  - in organization some decisions or actions require the agreement of different person
  - during a count creation on information system is necessary to get authorization of HR services and from IT department
  - in Unix to switch on root mode needs the root password and be part of the group with GID 0 in Berkley based Unix

Design Principle (Cont'd)

- The principe of **Least Common Mechanism** states that mechanisms used to access resources should not be shared
- Rationale:
  - In a system where resources are shared by different users may provide information through "information channels". To avoid these issues isolation and confinement are established by OS

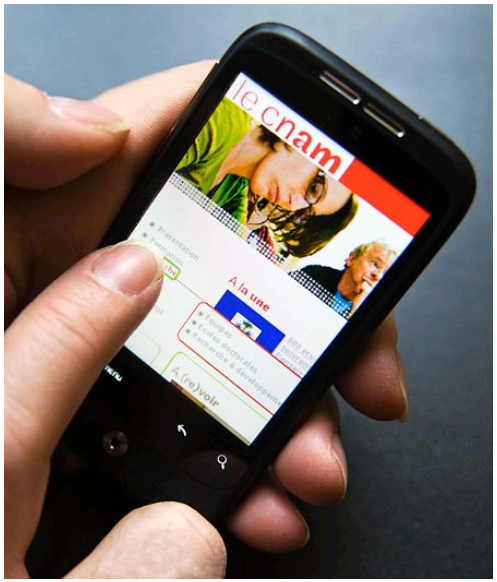
Design Principle (Cont'd)

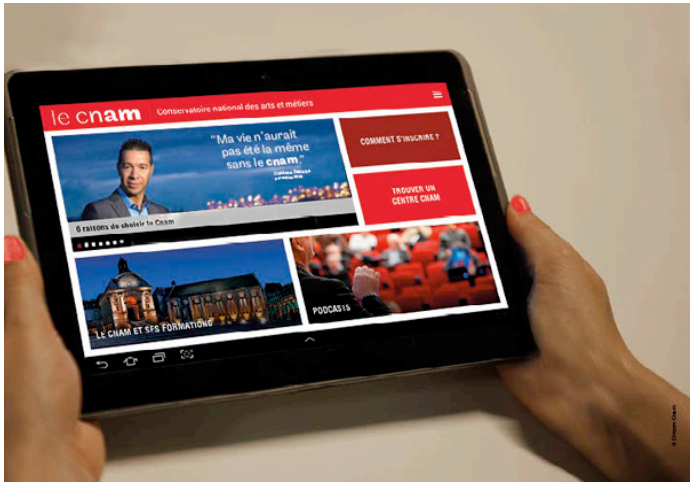
- The principle of **Psychological Acceptability** states that:
  - the mechanism must be easy and completely to use (i.e. acceptable and no bypass)
  - the mechanism should not increase the conditions to access information

Computer Security

- Introduction & Definitions
- (Secure) Design Principles
- **Modern issues in security**
- Bibliography

Mobile devices...





Mobile phone security

- What it is important to protect ?
- What are the threats
  - Data (calendar, contact, access code...)
    - privacy
  - Identity of the phone owner
    - ID & pwd
  - Availability
- Who are the attacker (same as IT)
  - Professional, thieves and hackers
- Consequences
  - ...

Mobile phone security

- Consequences
  - Data deletion, loss, stolen,...
  - Record conversations between the users
  - Decrease HS performances (battery)
  - Phone calls perform on number taxed
  - Use as a zombie machine
  - …

What are the technics

- Attacks on:
  - Attack based on SMS & MMS
  - Attacks based on communication networks
    - GSM
    - Wi-Fi, Buetooth
  - Physical attacks and reverse engineering
  - and on software...

What are the technics (cont'd)

- Attacks based on vulnerabilities in software
  - OS
  - Web and App
  - Malicious Software (Malware)
    - Viruses and Trojans
    - Spyware
      - Long list on the wikipedia article

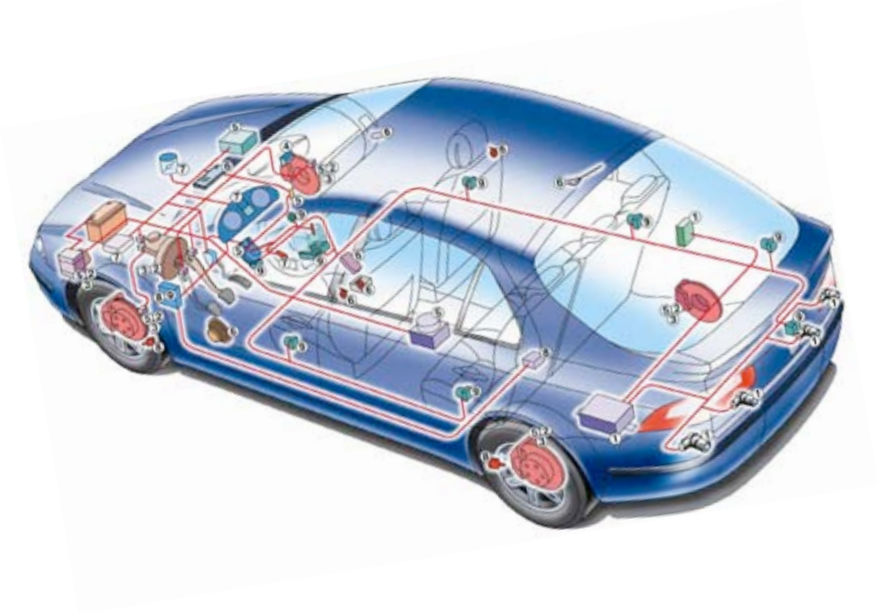
Contermeasure

- Hardware
- Firmware, bootloader
- Operating System
  - With isolation, rights,…
  - Memory protection and sand box mechanisms
  - VM, hyperviser
- Applications distribution model
- Access control (where are the protections)
    - Pin Code, or advanced biometrics device like on iPhone 5S
- But also…

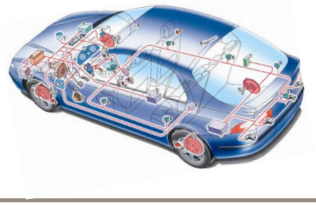
Contermeasure (cont'd)

- Completed by
  - Resource Monitoring in the smartphone
  - Network audit and surveillance
  - Manufacturer's audit and surveillance
  - User awareness (!)

Automotive



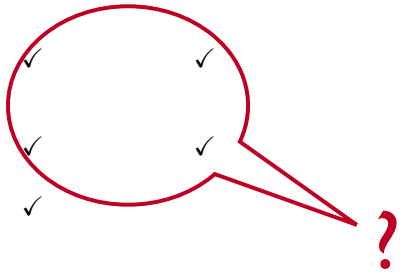
Automotive



- More and more ECU in a car
- A CAN bus (Controller Area Network)

Component	Functionality	Low-Speed Comm. Bus	High-Speed Comm. Bus
ECM	*Engine Control Module* Controls the engine using information from sensors to determine the amount of fuel, ignition timing, and other engine parameters.		✓
EBCM	*Electronic Brake Control Module* Controls the Antilock Brake System (ABS) pump motor and valves, preventing brakes from locking up and skidding by regulating hydraulic pressure.		✓
TCM	*Transmission Control Module* Controls electronic transmission using data from sensors and from the ECM to determine when and how to change gears.		✓
BCM	*Body Control Module* Controls various vehicle functions, provides information to occupants, and acts as a firewall between the two subnets.	✓	✓
Telematics	*Telematics Module* Enables remote data communication with the vehicle via cellular link.	✓	✓
RCDLR	*Remote Control Door Lock Receiver* Receives the signal from the car's key fob to lock/unlock the doors and the trunk. It also receives data wirelessly from the Tire Pressure Monitoring System sensors.	✓	
HVAC	*Heating, Ventilation, Air Conditioning* Controls cabin environment.	✓	
SDM	*Inflatable Restraint Sensing and Diagnostic Module* Controls airbags and seat belt pretensioners.	✓	
IPC/DIC	*Instrument Panel Cluster/Driver Information Center* Displays information to the driver about speed, fuel level, and various alerts about the car's status.	✓	
Radio	*Radio* In addition to regular radio functions, funnels and generates most of the in-cabin sounds (beeps, buzzes, chimes).	✓	
TDM	*Theft Deterrent Module* Prevents vehicle from starting without a legitimate key.	✓	

Table I. Key Electronic Control Units (ECUs) within our cars, their roles, and which CAN buses they are on.



Security/safety

- Part of the bus is dedicated to critic systems
- Part of the bus is dedicated infotainement systems
- New scenario is:
  - The control is taken by external entity on the car
  - Control may be used to corrupt car function
- Security issues on the CAN bus
  - Broadcast Nature
  - Fragility to DoS
  - No Authenticator Fields
  - Weak Access Control

Other domains

- Airplane
  - DO178B & DO178C
  - & ARINC 653
  - …
- Smart grid and privacy
  - Your electric consumption is related to what TV program you watch !s

Bibliograhy

- Books:
  - Computer Security - Art and Science, Matt Bishop, Addison Wesley, 2003
  - Security Engineering, Ross Anderson, Addison Wesley
  - Cryptography and Data Security - Addison Wesley, Dorothy Denning, 1982
    - Available on the web
- Web
  - http://www.schneier.com/
  - http://www.autosec.org
  - Rapport Pottier
  - Identity Theft Resource Center (Dashable.com)

Computer Science Security
(Secure) Design Principles

P. Paradinas - 2013

le cnam