1 - Introduction

Jordi Nin

nin@ac.upc.edu

Department of Computer Architecture (DAC)
Universitat Politècnica de Catalunya (UPC)
Computer Security (SI)

Contents

Contents

Topics

1. Cryptography and PKI
   - Mathematical background
   - Private key vs. Public key
   - RSA and ElGamal
   - Digital Signatures
   - Public key infrastructure
2. Operating systems security
   - Access control
   - Virus and malware

Topics

3. Network security
   - Firewalls (perimetrical security)
   - Intrusion Detection Systems
   - Virtual Private Networks (IPSec)
4. Forensics
   - Evidence collection
   - .lnk files analysis

Grading criteria

General percentages

- Theory: 70% of the mark Laboratory: 25% of the mark
- Documentation Assignment: 5% of the mark

Laboratory lessons

- Session tests (50%) + Final exam (50%)

Theory lessons

- Theory Exams $\rightarrow$ TE_1=17/03/15, TE_2=28/04/15 and TE_3=2/06/15
- $TM = (TE_1 + TE_2 + TE_3)/3$ where TM and TE stand for Theory mark and Theory Exam

Laboratory sessions

Grading criteria

- Mini-tests (one per topic): 50% of the mark
- Final exam: 50% of the mark

- **OWASP-I**: 16-20/2/15
- **OWASP-II**: 23-27/2/15
- **Malware Detection**: 2-6/3/15
- **Certificates**: 9-13/3/15
- **WEP-Security**: 16-20/3/15
- **IPTables**: 23-27/3/15
- **Forensics**: 6-10/4/15
- **Final Exam**: 13-17/04/15

Documentation Assignment

Groups of two members. Each group will be assigned a project category and will prepare a document with the following contents:

- 5-10 good sources of information. Detail the reasons
- 5-10 bad sources of information Detail the reasons
- 10 formatted cites according to Mendeley
- A brief description (5 pages) of the project category.

The Documentation Assignment should be delivered before the last week of class.

Possible topics (open list)

- APT (Advanced Presisten threats)
- Deep web
- Mobile forensics
- iOS Security
- Android Security
- Cloud computing threats
- Fraud detection in crowdsourcing platforms

Basic Bibliography

- Cryptography → Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, Handbook of applied cryptography, ISBN: 0-8493-8523-7, CRC Press (free e-book available)
- Operating systems security → Avi Silberschatz, Peter Baer Galvin and Greg Gagne, Operating System Concepts, Eight Edition, John Wiley & Sons, Inc. 2008
- Public key infrastructure → Carlisle Adams, Steve Lloyd Understanding PKI : concepts, standards, and deployment considerations, Addison-Wesley, 2003
- Network security → Andrew S. Tanenbaum, Computer Networks, Fourth Edition, Prentice Hall Ed. Chapter 8, 2003 Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, Building Internet Firewalls, 2nd Edition, O'Reilly Media, 2000 Jay Beale, James C. Foster, Snort 2.0 Intrusion Detection, Syngress, 2003

Contents

Basic information security objectives

Confidentiality

Authenticity

Integrity

Non-repudiation

Basic information security objectives

Confidentiality

Keeping information secret from all but those who are authorized to see it

Authenticity

- Entity authentication or identification → corroboration of the identity of an entity (e.g., a person, a computer, etc.)
- Message authentication → corroborating the source of information; also known as data origin authentication

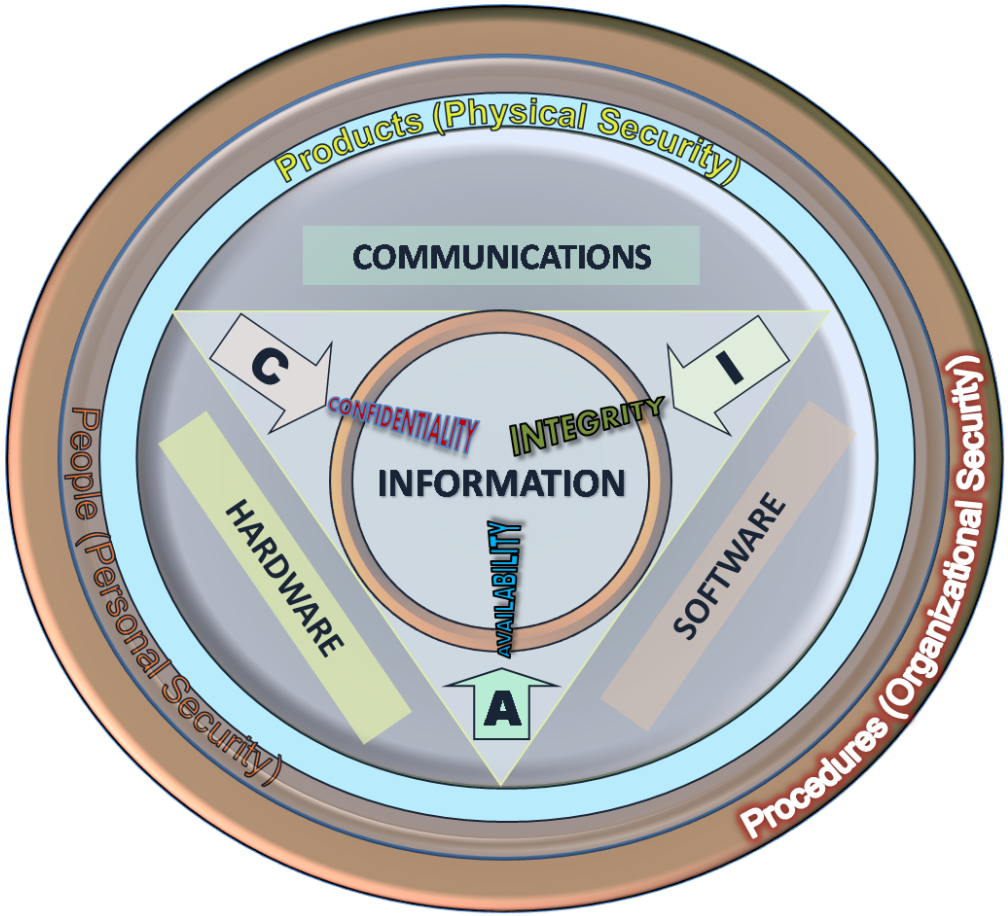
Integrity

Ensuring information has not been altered by unauthorized or unknown means (users)

Non-repudiation

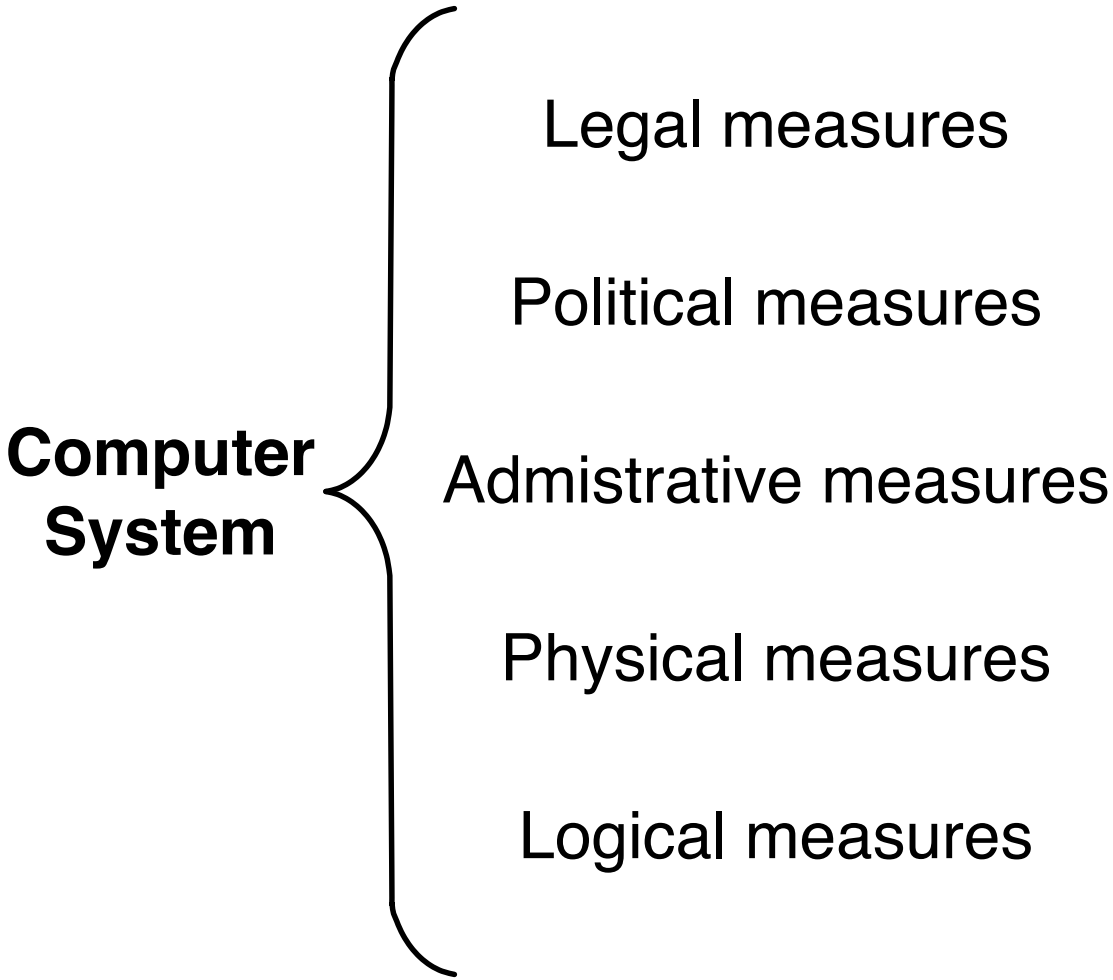
Preventing the denial of previous commitments or actions

Security taxonomy



Contents

Overview


Computer System
Legal measures
Political measures
Admistrative measures
Physical measures
Logical measures

Legal measures

From a legal point of view, it is possible to classify the measures in the following classes:

Example

- Laws about official (state) secrets
- Diplomatic cryptography
- Laws about security telecommunications
- Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (LOPD)
- ...

Political measures

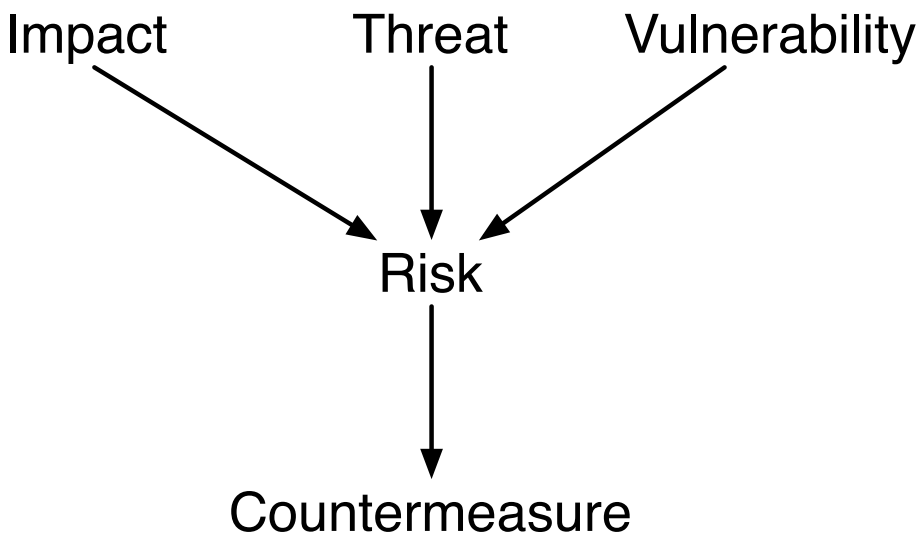
A security model implements a certain security police. e.g. An access control police can be implemented by an access matrix, or lattice multilevel, etc.

Example

- risk analysis police
- contingency plan
- data protection
- ...

Administrative measures

Develop a vulnerability study or risk analysis



Physical measures

Example

- measures against power outage
- data backups
- physical access control measures
- correct document destruction
- countermeasures against earthquakes, flooding, etc
- ...

Logical measures

Example

- cryptography
- antivirus
- firewalls
- ...

1 - Introduction

Jordi Nin

nin@ac.upc.edu

Department of Computer Architecture (DAC)
Universitat Politècnica de Catalunya (UPC)
Computer Security (SI)