Politecnico di Milano
Dip. Elettronica e Informazione
Milano, Italy

Computer Security
Introductory notes

Useful information

- **Stefano Zanero**
  tel. 4017 - zanero@elet.polimi.it
- **Federico Maggi**
  tel. 4009 - fmaggi@elet.polimi.it
- Materials
  - Slides **+ lesson notes** (slides alone do not tell the whole story; actually, they may lead you to miss the message and learn the details)
  - R. Anderson, “Security Engineering”, Wiley (pdf freely available on the course website)
  - OR: Gollman, “Computer Security”, Wiley
  - C. Anley, J. Heasman, F. Linder, G. Richarte, “The Shellcoder's Handbook”, Wiley, 2007
  - Howard, LeBlanc, “Writing Secure Code”, Microsoft

Lecture topics

- We will try to have an holistic approach to *systems security.* We will study both what happens on hosts, and what happens on network, with an eye to the impact of policies and procedures... as well as the impact of humans!
  - Application access control, and access control models
  - Secure programming
  - What is an "exploit" and how common vulnerabilities are exploited
  - Network security, firewalling, intrusion detection
  - Cryptography and secure protocols (an overview)
  - Malicious code (viruses, worms, bots...)
  - Digital forensics
- Practical approach but with theoretical foundation

The key objectives of information security

- The so-called CIA paradigm for information security states three objectives:
  - **Confidentiality**: secured information can be accessed only by the entities who are authorized to access it
  - **Integrity**: secured information can be modified only by authorized entities, and only in the way such entities are entitled to modify it
  - **Availability**: secured information must be available to all the parties who have a right to access it, within specified time constraints
- This is **not easy**, as the third requirement directly conflicts with solutions of the first two requirements
  - Security is a typical **engineering problem**

Typical implementation

- A typical security system implements security controls as a relationship between:
  - Authorized **subjects**
  - Protected **objects**
- How do we specify **authorizations** at the application and system levels?
- How do we **authenticate** subjects?
- How do we **audit** that everything is working correctly?
- **Authentication, Authorization, Auditing** is the so called "AAA" paradigm
- … but I know, this is the boring part

Vulnerability, Exploit

- A **vulnerability** is a defect in information protection which allows to violate one of the constraints of the CIA paradigm
- An **exploit** is a specific way to use one or more vulnerabilities to accomplish a specific objective which violates the constraints
  - E.g., letting an unauthorized person access one of the protected objects, or making it impossible for an authorized person to do so
- Identifying vulnerabilities and developing exploits is an **essential** part of the skillset of an information security professional

Incident, Attack and Attackers

- An **incident** is an instance in which a violation of the CIA paradigm occurs, because of a vulnerability
  - An incident may be just an **accident** (e.g. power loss?) or a **disaster** (e.g. earthquake or huge black out)
  - An incident may be caused by a willing agent, in which case it is usually called an **attack**
- A **threat** is whatever/whoever might cause an **incident** to occur
- Someone who violates (or attempts to) an information security system is called an **attacker**
  - Not a **hacker**, though: hacking is an attitude to experiment with things, occasionally breaking them, and has (almost) nothing to do with violating information security systems

Security is all about managing risk

- **Risk** is a statistical and economical evaluation of the exposure to **damage** that occurs because of the presence of **vulnerabilities** and **threats**
- Since **threats** are quite an independent variable, the reduction of **vulnerabilities** and the creation of suitable arrangements to contain **damage** are the tools to **manage risk** and reduce it
- Once again, security is a **typical engineering task** of reducing risk while balancing the cost of vulnerability reduction and damage containment against the advantages

Costs?

- Security has a cost
  - A high cost, do you really want to work for free? :-)
- Security has not just a cost in terms of expenses
  - Reduction of usability
  - Performance hit due to security controls
  - Privacy violations
  - Impairment vs. empowerment of users
- Balancing these costs against risk reduction is paramount
  - Simply throwing money at security does not really work
  - "Doing something" is not always better than "nothing"
    - Political examples are overabundant in this area