UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

COURSE SYLLABUS

Cybersecurity for Data Science

2627-2-F9202P022

Aims

Knowledge and understanding:

- structural elements which are the most vulnerable in a computer system
- main attack methods for ICT systems, and of their possible impact and relevance in business world
- techniques aimed at reducing risks in computer systems, networks and software
- tools to search for and protect from vulnerabilities, for instance firewalls and antivirus

Applying knowledge and understanding:

- analyzing which parts of a given ICT system introduce threats and risks
- evaluating the actual cost-benefit tradeoff of main available defenses in computer systems, for several application domains
- using common software while avoiding pitfalls, and to configure and use some open source computer security tools

Contents

The domain of cybersecurity: technologies where we apply the discipline, and goals: basic terminology in the area (e.g. vulnerability VS exploit, etc.); unifying principle: tecnologies introduce possibilities of the being used improperly. Protection of data: cryptography, filtering network traffic, detection of threats. Improving security without technology: awareness and best practices. Case studies: data management frameworks, and where they can be hardened against security threats.

Detailed program

1-Introduction to cybersecurity:
a.founding principle, specifical problems arising in computer science
b.actors involved: software developers, attackers, system admin, analysts
c.goals: confidentiality, integrity, availability
d.some real incidents

2-Vulnerabilities and attacks:
a.errors in software, the "buffer overflow"
b.flaws in the networks, sniffing and spoofing
c.social engineering
d.exfiltrating critical information
e.denial of service

3-Defenses:
a.maintenance of software
b.filtering and monitoring on networks
c.best practices

4-Cryptography:
a.methods (symmetric key, public key)
b.some tools (PGP, TLS)
c.vulnerable applications of cryptography: bad implementations or usage

5-Security specifically in big data sets, frameworks and defenses

6-Case studies, incidents and some open source tools

Prerequisites

.

Teaching form

- 10~12 frontal lessons of 2 hours each held by the teacher in presence;
- 2~4 frontal lessons of 2 hours each held by the teacher remotely in asynchronous mode;
- 6 interactive laboratory lessons of 3 hours each held by the teacher in presence;

Textbook and teaching resource

Charles. Pfleeger - S. Pfleeger, "Security in Computing", Pearson, 2015

Semester

first Semester

Assessment method

Learning assessment includes a written exam and an oral discussion on a short report:

the written exam covers a subset of the topics presented during lectures (and defined when starting the course),

the report concerns experimental activity related to one of the topics of the course, chosen by the student.

The final score is the average of scores of written and oral tests.

Office hours

The teacher is available for the students upon agreement through email.

Sustainable Development Goals