



UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Sicurezza Informatica

2122-2-F1801Q123

Aims

- To be able to fruitfully follow the trends in computer security
- to correctly use crypto systems
- to be able to perform automatic static analysis of software
- to be able to use model checking tools to assess the security of computer systems

Contents

advanced tools and techniques to attack or protect computer systems

Detailed program

- 1 "Basic principles of computer security trends in computer security case studies from the news"
- 2 "Using cryptographic systems: symmetric and asymmetric implementations of crypto algorithms"

choosing crypto algorithms, their applicative contexts"

3 cryptography in wireless and cellular networks

4 "Static analysis for computer security: reasons, limits

abstract representations of specific aspects of execution

use case: static analysis to find buffer overflow vulnerabilities"

5 "Model checking: its origins and its role in computer security

formal representation of states

logics to describe properties, instances of security related properties"

6 "model checking tools

examples: model checking for network protocols and for software artifacts"

7 Practical and competitive hacking session against purposely vulnerable software ("Capture the Flag")

Prerequisites

Knowledge about Operating Systems, Networks, and Programming will be recalled

Teaching form

Usual frontal lecture, with personal study and support from online materials.

The course is taught in Italian.

Textbook and teaching resource

Educational and scientific papers available on Internet

helpful book: Pfleeger, Pfleeger - "Sicurezza in Informatica", Pearson

Semester

second Semester

Assessment method

Learning assessment includes a written exam (50% of final score) and an oral discussion on a short report (50% of final score):

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.

Office hours

The teacher is available for the students upon agreement through email, usually on tuesday morning.
