Formal Methods for Secure Systems

Prof. Cinzia Bernardeschi
Dipartimento di Ingegneria dell'Informazione
Università di Pisa

Academic Year 2021-2022

Outline of the course

Formal Methods for Secure Systems (9CFU)

SCHEDULE: 1-12 weeks: 8 hours

1. Dependability (6CFU)

- Basic concepts
- Building high reliable computer-based systems
- Quantitative evaluation of dependability
- Cyber-physical systems
- Hands on activities (Lab)

SCHEDULE:
1-3 weeks: 8 hours
4-12 weeks: 4 hours (Wednesday, Thrursday)

2. **Formal methods for security (3CFU)**

- Formal methods applied to security issues
- Case studies: Data confidentiality/Security protocols/ Cyber-physical systems security
- Hands on activities (Lab)

References

Dependablity

- A. Avizienis, J.C. Laprie, B. Randell, C. Landwehr.
  Basic Concepts and Taxonomy of Dependable and Secure Computing.
  IEEE Transactions on Dependable and Secure Computing, Vol. 1, N. 1, 2004.

- John Knight.
  Fundamentals of Dependable Computing for Software Engineers.
  Chapman & Hall, 2012

- M. Nicol, W.H. Sanders, K.S. Trivedi.
  Model-Based Evaluation: From Dependability to Security.
  IEEE Transactions on Dependable and Secure Computing, vol. 1 (1), 2004

- D.P. Siewiorek, R. S. Swarz.
  Reliable Computer Systems (Design and Evaluation) [Excerpts]
  Prentice Hall, 1998. On line version

References

Formal methods for security

- Flemming Nielson, Hanne Riis Nielson.
  Formal Methods, Springer, 2019

Additional material will be provided by the instructor.

Website of the course: http://www.iet.unipi.it/c.bernardeschi/FMSS.html

Exam: (i) presentation and discussion of a technical project and (ii) oral examination.

Computer-based systems

- Individual, organizations and society strongly depend on computer-based systems
- The set of services that computer-based systems help to provide is very diverse
- System dependability is the ability of the system to deliver the expected service during its operational life
- Dependability is important in safety-critical systems, systems whose failure or malfunction may result in death or serious injury to people, loss or serious damage of equipment, or environmental harm.
- For a computer-based safety-critical system, the safety of the system depends strongly on its computers.

Computer-based systems

Future safety-critical systems will be more automated and more dependent on computers than today's systems

Moreover, computer-based systems are vulnerable to cyber-security attacks (e.g., through wired or wireless connections). The system must be dependable also in presence of attacks.

The dependability of the system is as important as the functionality of the system, perhaps even more important.

Engineering a computer-based system that has to be dependable.

Formal Methods (based on rigorous mathematical notations) provide engineers with tools and techniques for rigorously reasoning about the correctness of systems, and for proving safety in presence of malfunctions or attacks.