UNIVERSITÀ DI PISA

Formal Methods for Secure Systems (9CFU)

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

Master Degree in Computer Engineering

Academic Year 2020-2021

Outline of the course

- Dependability (safety and security)
- Formal methods
- Formal methods applied to security issues
  - Languages
  - Verification techniques: static analysis, model checking, theorem proving
- Case studies
  - Data confidentiality
  - Malware analysis
  - Cyber-physical systems security
- Tools for (i) quantitative evaluation of dependability and (ii) formal verification
- Hands on activities

Outline of the course

References

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

Additional material provided by the teacher.

Website of the course: http://www.iet.unipi.it/c.bernardeschi/FMSS2020-21.html

Slides available @website; recorded lectures available @Microsoft Team

Exam: (ii) 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 functionality 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

Computer-based systems are vulnerable to cyber-security attacks (e.g., through wired or wireless connections)

Engineering a computer-based system that has to be dependable

Formal Methods (rigorous mathematical notations) provide engineers with tools and techniques for rigorously reasoning about the correctness of systems, and for proving safety and security properties