Formal Methods for Security

**FMS**

- II sem, 6 CFU (4 hours a week)
- oral + written exam
- no prerequisites

Why?

Chiara Bodei
chiara.bodei@unipi.it
Everyone wants to feel safe, but ...

Google Cracks Key Security Code, Calls for New Standard

Internet, falla in OpenSSL: 'Heartbleed' mette a rischio password e carte di credito in due terzi dei siti web

Cybersecurity, allarme Copasir: "In Italia piattaforme-colabrodo"

Allarme Ransomware, l'Italia il Paese più colpito in Europa

Cyber-sécurité : des hackers spécialisés aident les entreprises à mieux se protéger

Security has become everyone’s concern
How?

• Acquire a security-aware way of thinking to systems
• System design should be security-oriented from the very beginning
• **Formal methods** can improve system security

  - Delimit systems and their environments
  - Characterize and model the systems’ behavior
  - Define the desired security properties
  - Formally prove properties
• we provide a broad overview of security in networking systems and software applications.
• we explore the theoretical foundations of security, the formal methodologies used to design, analyse and verify secure systems and applications.

- Language based security
- Design principles for security protocols
- Information flow security
- Java security
  - Stack inspection
  - Access Control
- Web-application security

Formal methodologies
  - Logics for protocols
  - Theorem proving
  - Static Analysis

• experimental aspects are addressed, too.
Theses

- Security of protocols
- Security by static analysis
- Secure services
- Context-aware Security
- Security issues in IoT
- ....