

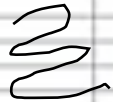
Security Methods and Verification

SMV

II sem, 6 CFU
(4 hours a week)

oral + written
exam

no prerequisites



Metodi per
La Sicurezza e
La
verifica

Why?

Chiara Bodei

chiara.bodei@unipi.it

Everyone wants to feel safe, but ...

Google Cracks Key Security Code,
Calls for New Standard

Attaccati i server di Yahoo! Ma non è il baco Shellshock

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

*Il capo della sicurezza informatica del motore di Sunnyvale assicura:
"Al momento non abbiamo trovato prove di danni ad altri sistemi o
della violazione di account di utenti. E' stata una falla specifica e
relativa a un limitato numero di macchine ed è stata sistemata"*

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

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

*Per due anni un 'bug' ha reso vulnerabile il software di sicurezza usato
da milioni di siti per criptare le comunicazioni più delicate. Il furto dei
dati per la sottile
coinvolto*

LE FIGARO · fr

THE TIMES

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

**Millions hit
as hackers
empty bank
accounts**

Talk Talk ignored warning over online security

Cyberangriff:


**ThyssenKrupp von
Hackern angegriffen**

DIE ZEIT

**Security has become
everyone's concern**

How?

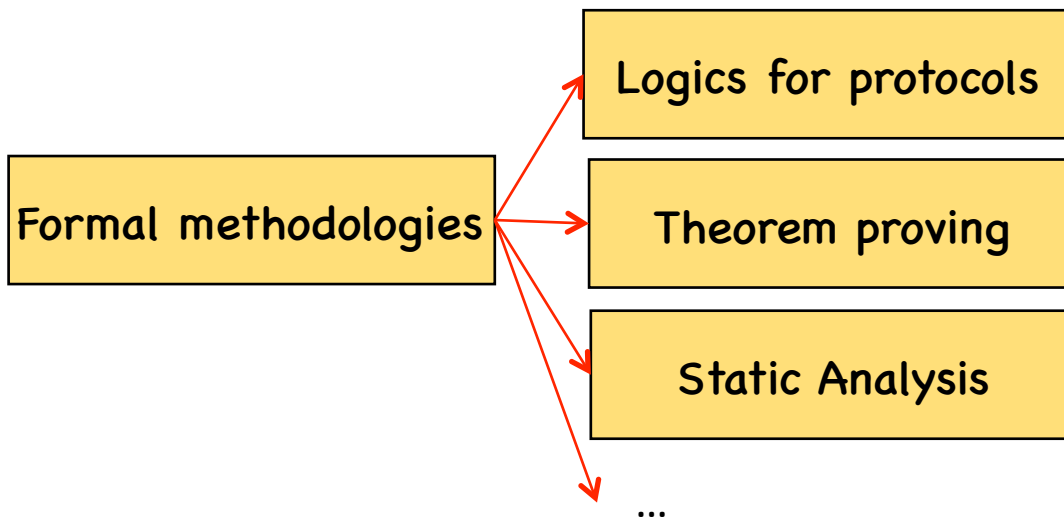
- Acquire a security-aware way of thinking to systems
- System design should be security-oriented from the very beginning
- **Formal methods** can improve system security



Delimit systems and their environments
Characterize and model the systems' behavior
Define the desired security properties
Formally prove properties

What?

- 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.



- experimental aspects are addressed, too.

Language based security

Design principles for security protocols

Information flow security

Java security
Stack inspection
Access Control

Web-application security

Theses on

```
graph TD; A[Theses on] --> B[Security of protocols]; A --> C[Security by static analysis]; A --> D[Secure services]; A --> E[Context-aware Security]; A --> F[Security issues in IoT]; A --> G[....];
```

Security of protocols

Security by static analysis

Secure services

Context-aware Security

Security issues in IoT

....