POLITECNICO DI MILANO

Systems Security Research at POLIMI

Federico Maggi

Stefano Zanero

Who we are

- POLIMI is Italy's largest school of engineering, with 38.000 students and 1500 full term faculty
- DEI (our department) is a very large and complex research environment, with more than 180 full term faculty, several hundreds of PhD students and post-docs, and thousands of students
- Security research is carried on in different directions by different work groups
  - Network security protocols
  - **Systems security: malware analysis, virology, intrusion detection**
  - Cryptography and hardware design
  - Information systems and database security
- In the following slides, we will introduce shortly the key current and previous projects of our research group, which focuses on Systems Security

Research team and lab

- The team is in the larger Systems Architecture group, led by prof. Donatella Sciuto, within the Performance Evaluation Lab, led by prof. Giuseppe Serazzi
- Systems Security research team:
  - Stefano Zanero (Asst. Prof.)
  - Federico Maggi (Post-doc)
  - Alessio Antonini (PhD student)
  - Claudio Criscione (PhD student)
  - Alessandro Frossi (R.A.)
  - Alberto Volpatto (R.A.)

Research background: our origins

- Intrusion detection and prevention
  - In particular, application of statistical methods and unsupervised learning to IDS
- ULISSE (one of the first NADS which analyzed packet payloads)
- SSAADE (a HIDS based on system call sequence and arguments)
- Masibty (a WAF based on learning)
- Additional contributions on aggregation, retraining, ...
- Core contributions:
  - Using multiple layers of algorithms to analyze complex interactions
  - Conversely, aggregating multiple models and facets of a phenomenon into one coherent outcome

Research topics: our current targets

- Virology
  - Propagation modelling of worms
  - Propagation (or non-propagation...) of Bluetooth and wifi viruses
- Malware analysis
  - Joint work with TUV and UCSB on *Reanimator*, an hybrid dynamic-static analysis tool for discovering dormant behavior in large databases of malware (Oakland 2010)
- Attack vectors and threat analysis
  - Short URL usage and abuse (submitted)
  - BURN (Baring Unknown Rogue Networks), a visualization and exploration tool for the FIRE database (VizSec 2011)

Research vision: our next targets

- Cloud security
- Cyber-Physical systems
- Underground economy and cybercrime threats
- Thanks for your attention! Contact us:
  - zanero@elet.polimi.it
  - maggi@elet.polimi.it
- Website: http://vplab.elet.polimi.it