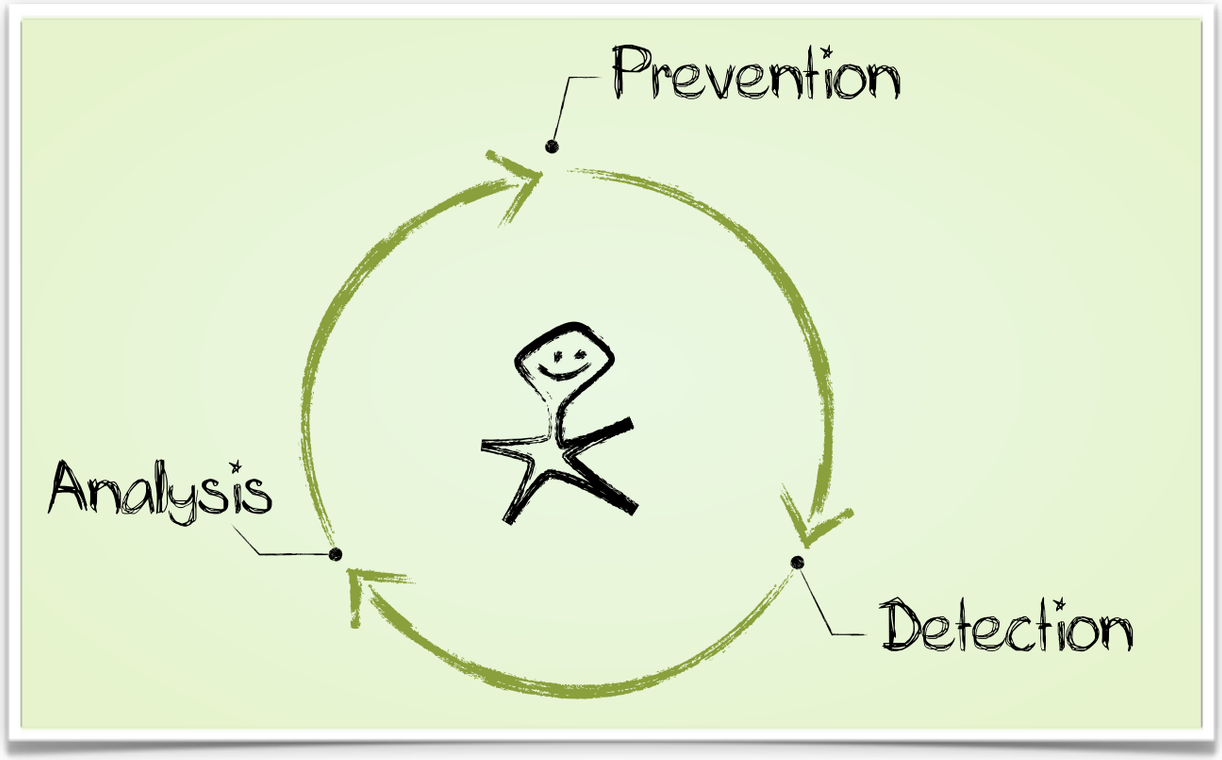
Computer Security and Machine Learning: Worst Enemies or Best Friends?

Konrad Rieck
Technische Universität Berlin
SYSSEC Workshop 2011

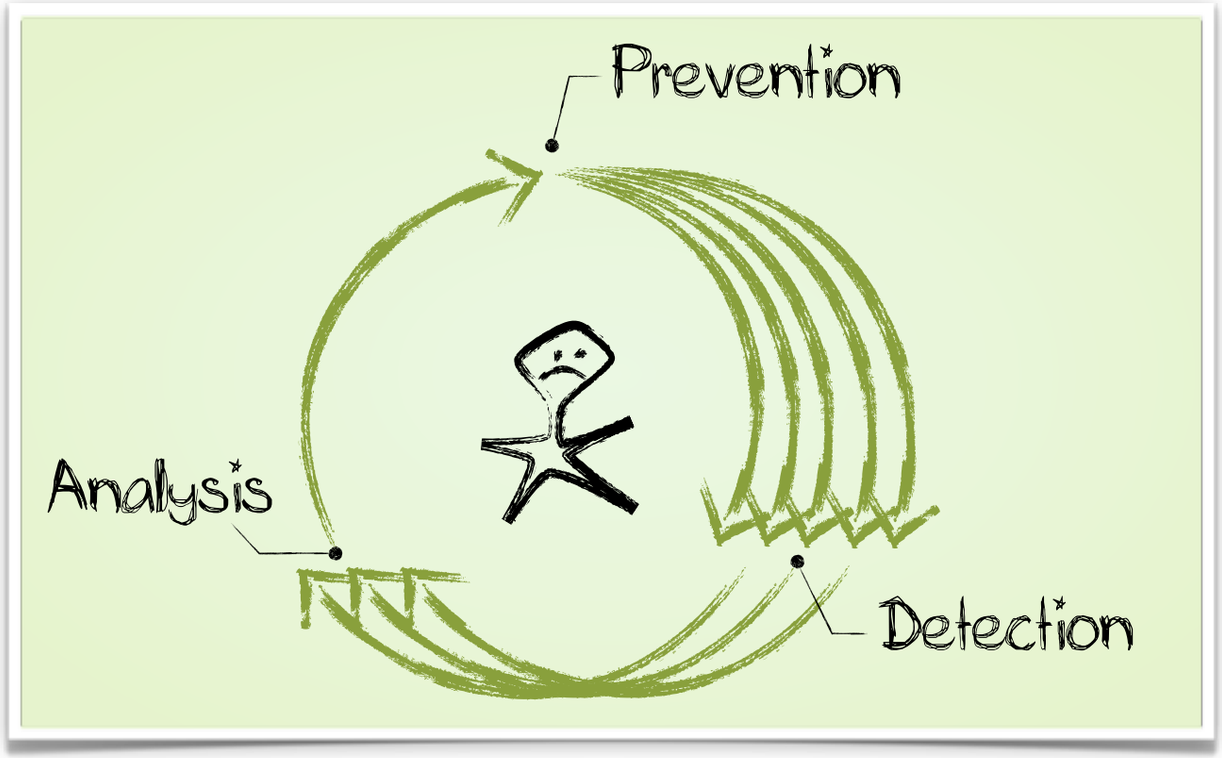
Technische Universität Berlin

Computer Security



- **The everlasting security cycle**
- **Central element:** *human researcher, analyst, operator, ...*

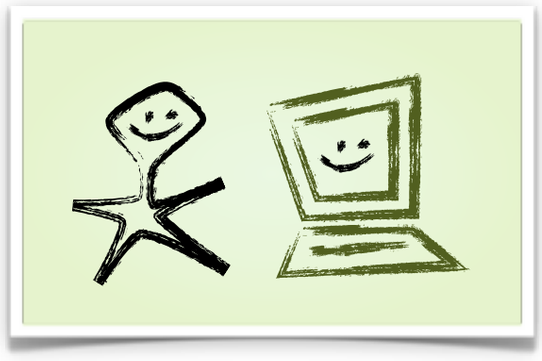
Computer Security



- **The everlasting security cycle**
- **Central element:** *human researcher, analyst, operator, ...*

- **Increasing imbalance of security cycle**
  - High amount and diversity of novel threats
  - Increasing automatization of attacks

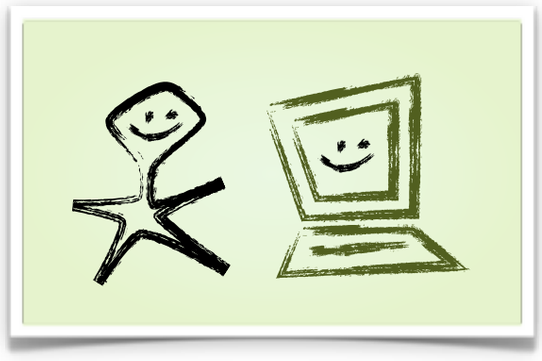
Intelligent Defense



Automatization of attacks

➠ Automatization of security?

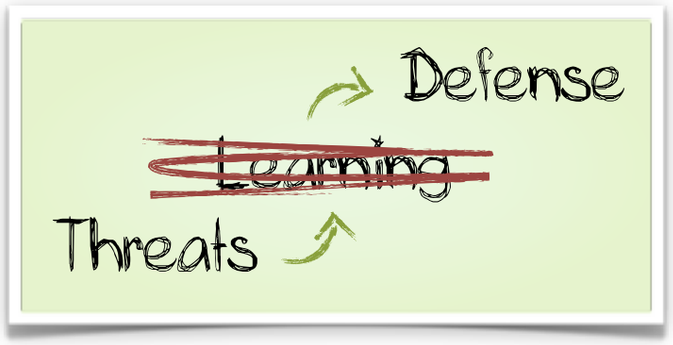
Intelligent Defense



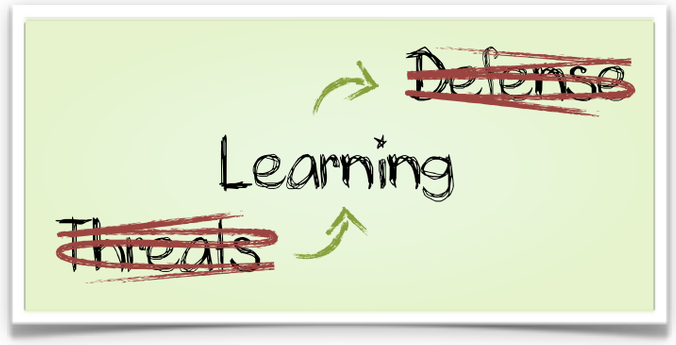
Automatization of attacks
➠ Automatization of security?

- **Need for intelligent and self-contained security systems**
  - Combination with techniques from machine learning
  - Assistance during prevention, detection and analysis
- **“This doesn't work!” vs. “That's already solved!”**
  - Large body of existing work and research
  - Almost not practical solutions and products

What's wrong?



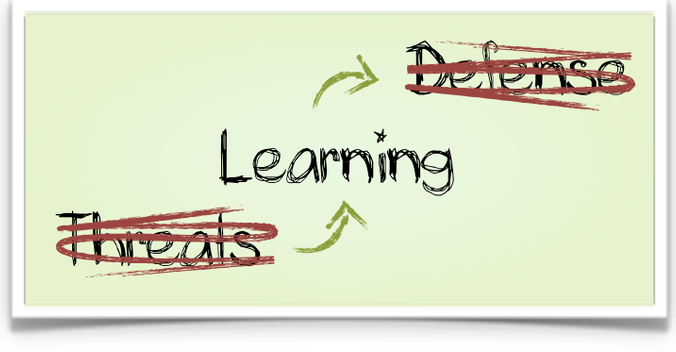
Security community



Learning community

What's wrong?

Security community



Learning community

- **Several factors in learning-based security systems**
  - Effectivity and efficiency
  - Transparency and controllability
  - Robustness against evasion
- **Need for interdisciplinary research in both domains!**

Perspectives

- **Research group**
  - Located at the University of Göttingen (soon)
  - Focus on computer security *and* machine learning
- **Research topics**
  - From honeypots to IDS and back again
  - Automatic analysis of malware data (static/dynamic)
  - Assisted discovery of security vulnerabilities
- **Contact**
  - Konrad Rieck (konrad.rieck@tu-berlin.de)