SoSe 2017
Master Seminar
Intrusion Detection and Forensic Analysis

Mohsen Ahmadvand
Alei Salem

Chair for Software Engineering (I22)
Prof. Dr. Alexander Pretschner

Introduction

- Cyber attacks are imminent
- 100% Security = simply unattainable
- Systems will eventually be compromised
- Defense in depth tactics

Introduction (cont'd)

- Defense in depth tactics:
  - (Preventive): Secure Coding + Security software e.g. firewalls
  - (Detective): Intrusion detection e.g. runtime integrity checking
  - (Post-mortem): Forensic analysis

Introduction (cont'd)

- Defense in depth tactics:
  - (Preventive): Secure Coding + Security software e.g. firewalls
  - **(Detective): Intrusion detection e.g. runtime integrity checking**
  - **(Post-mortem): Forensic analysis**

Content

- Research Topics (Integrity checking + intrusion detection):

  - An analysis of attacks that lead to integrity violation,
  - System and process monitoring techniques,
  - Application integrity checking via runtime self-monitoring techniques,
  - Integrity protection techniques for *Docker* containers,
  - Hypervisor-based integrity protection techniques,
  - Security metrics for integrity protection techniques,
  - Cost analysis of integrity protection techniques.

Content

- Research Topics (Forensic Analysis):
  - Reconstruction of system state from logging data,
  - Visualization of logs and system states (e.g. graphs),
  - Mining logs for traces of malicious behavior(s), and
  - Classification of logs/system states as malicious benign (using machine learning)

Roadmap

I. Topic selection

II. Literature review

III. First submission

IV. Peer review (20%)

V. Final submission (50%)

VI. Talks/Presentation (30%)

Administrative

- Rules and policies here
- Master Seminar
- Maximum participants: 10
- Registration
  - Via matching.in.tum.de
  - From February 3rd – 8th

Thank you

Questions?