Technische Universität Braunschweig

Institut für Betriebssysteme und Rechnerverbund

Seminar Distributed Systems

Secure Trusted Execution for Resilient Distributed Systems

Nico Weichbrodt

October 19, 2016

Table of Contents

Organisational

- Course
  - Course held in German/English
  - HotCRP submissions and review management
    - `http://studentcloud015.scloud.etc.tu-bs.de/hotcrp`
- Language
  - Essay and presentation in either German or English
  - Can also be mixed
- Certificate Requirements
  - Essay (6 pages, double column)
  - Presentation of own topic (25min + discussion)
  - Active participation in discussions

Procedure

- Not a single meeting with all presentations

→ Two preseentations each meeting

- Every wednesday, starting November 16th, 3pm - 4:30pm

- The first two students have 4 weeks

Procedure

Procedure (4 Weeks)

Today	Topic selection
W 1-3	Read the paper[1]
W 1-3	Write essay and create presentation
W 3	Presentation dry-run, and peer's feedback
W 3	Peer review of essay
W 3-4	Incorporate comments
W 4	Presentation & Submission of slides
W 4	Submission of essay

[1] How to read a paper, `http://dl.acm.org/citation.cfm?id=1273458`

Requirements Presentation

- 25mins talks = approx. 25 slides
- Pictures $\gg$ text
- Presentation best-practices
  - Title, author, page numbers on each slide
  - Corporate design TU Braunschweig
- Structure of presentation (recommendation)
  - Introduction, Motivation
  - Problem
  - Approach
  - Evaluation, Conclusion (one slide summary!)
- Templates: `https://www.ibr.cs.tu-bs.de/kb/templates.html`
- LaTeX is preferred

Requirements Essay

- 6 pages (ACM Proceedings template)
- Structural components
  - Introduction & Motivation
  - Problem outline
  - Solutions, approaches tackling the problem
  - Evaluation
  - Conclusion, Discussion of results, Outlook
- Also look at your paper's related work!
- Templates:
  `https://www.acm.org/publications/proceedings-template`

Table of Contents

Topic Descriptions

David Goltzsche (English optional)

1. Intel Software Guard Extensions: Basics
   - Innovative Instructions and Software Model for Isolated Execution

     McKeen et al., Intel Corp., HASP 2013
   - Innovative Technology for CPU Based Attestation and Sealing

     Anati et al., Intel Corp., HASP 2013
2. SCONE: Secure Linux Containers with Intel SGX

   Arnautov et al., TU Dresden, OSDI 2016
3. VC3: Trustworthy Data Analytics in the Cloud using SGX

   Schuster et al., Microsoft Research, S&P 2015

Topic Descriptions

Stefan Brenner (English optional)

1. Fides: Selectively Hardening Software Application Components against Kernel-level or Process-level Malware

   Strackx et al., KU Leuven, CCS 2012

2. OASIS On Achieving a Sanctuary for Integrity and Secrecy on Untrusted Platforms

   Owusu et al., CyLab, CCS 2013

3. SecureKeeper: Confidential ZooKeeper using Intel SGX

   Brenner et al., TU Braunschweig, Middleware 2016

4. Ariadne: A Minimal Approach to State Continuity

   Strackx et al., KU Leuven, Usenix Security 2016

Topic Descriptions

Wenbu Xu (English preferred)

1. Efficient Byzantine fault Tolerance (MinBFT)

   Veronese et al., Stefanini IT Solutions, IEEE ToC 2011

2. Attested Append-Only Memory: Making Adversaries Stick to their Word

   Chun et al., UC Berkeley, SOSP 2007

Topic Descriptions

Bijun Li (English mandatory)

1. CheapBFT: Resource-efficient Byzantine Fault Tolerance

   Kapitza et al., TU Braunschweig, EuroSys 2012

2. Prophecy: Using History for High-Throughput Fault Tolerance

   Sen et al., Princeton University, NSDI 2010

Topic Descriptions

Nico Weichbrodt (English optional)

1. SecureBlue++: CPU Support for Secure Executables

   Boivie et al., IBM Research, Trust 2011

2. Shielding Applications from an Untrusted Cloud with Haven

   Baumann et al., Microsoft Research OSDI 2014

3. Controlled-Channel Attacks: Deterministic Side Channels for Untrusted Operating Systems

   Xu et al., University of Texas, S&P 2015

4. AsyncShock: Exploiting Synchronization Bugs in Intel SGX Enclaves

   Weichbrodt et al., TU Braunschweig, ESORICS 2016

Topics Overview

1. Intel SGX Basics (David) — Yannick
   (Innovative Instructions and Software Model for Isolated Execution)
2. Fides (Stefan) — Welf
   (Fides: Selectively Hardening Software Application Components against Kernel-level or Process-level Malware)
3. OASIS (Stefan) — Kay
   (OASIS On Achieving a Sanctuary for Integrity and Secrecy on Untrusted Platforms)
4. SecureBlue++ (Nico) — Stephan
   (SecureBlue++: CPU Support for Secure Executables)
5. Haven (Nico) — Björn
   (Shielding Applications from an Untrusted Cloud with Haven)
6. SCONE (David) — Silas
   (SCONE: Secure Linux Containers with Intel SGX)
7. VC3 (David) — Diorit
   (VC3: Trustworthy Data Analytics in the Cloud using SGX)
8. SecureKeeper (Stefan) — Florian
   (SecureKeeper: Confidential ZooKeeper using Intel SGX))

Topics Overview (2)

9. Ariadne (Stefan)
   (Ariadne: A Minimal Approach to State Continuity)
10. MinBFT (Wenbo) — Artur
    (Efficient Byzantine fault Tolerance (MinBFT))
11. CheapBFT (Bijun) — Juntao
    (CheapBFT: Resource-efficient Byzantine Fault Tolerance)
12. Prophecy (Bijun) — Tim
    (Prophecy: Using History for High-Throughput Fault Tolerance)
13. Append-Only Memory (Wenbo) — Manuel
    (Attested Append-Only Memory: Making Adversaries Stick to their Word)
14. AsyncShock (Nico) — Matthias
    (AsyncShock: Exploiting Synchronization Bugs in Intel SGX Enclaves)
15. Controlled-Channel Attacks (Nico) — Micha
    (Controlled-Channel Attacks: Deterministic Side Channels for Untrusted Operating Systems)