Berlin Institute of Technology
FG Security in Telecommunications

“Learning from Rootkits”

– Safe Place to stand for a Runtime Monitoring/Attestation System –

SPRING 5: SIDAR Graduierten-Workshop über Reaktive Sicherheit

Patrick Stewin, 7. July 2010, Bonn, Germany
patrickx@sec.t-labs.tu-berlin.de

Agenda

- Introduction
- Motivation
- Challenges
- Analysis x86 Platform
- Challenges for Attackers/Rootskits
- Important Related Work
- Conclusion and Further Research

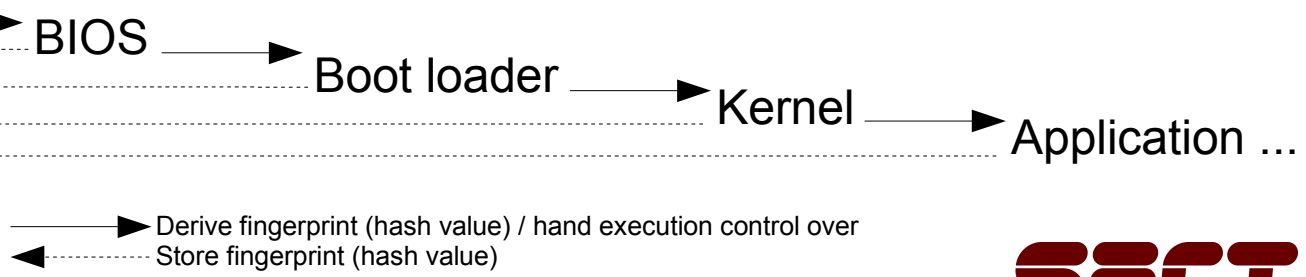
Introduction

- Rootkit evaluation:
  - Originally placed in user space with root privileges to hide it
  - Rootkits moved from user space to kernel space and beyond!
  - Goal: somehow isolate rootkit from host platform using platform's stealth capabilities
- Stealth – Isolation
- Can we use stealth/isolation capabilities of x86 platforms to improve security properties?

Motivation

- Why to improve computer platform security properties?
- Example: Time-Of-Check-Time-Of-Use (TOCTOU) problem
  - Cf. Trusted Computing Group (TCG) attestation model
    - Chain of Trust starting at Root of Trust for Measurement (RTM)
      - Derives and stores fingerprint of software before software gets execution control
      - TOC: once, just before execution
      - No statement about runtime behavior (cf., e.g., buffer overflow attacks)

(STMicroelectronics)



Goals

- Understand isolated execution environments to:

  i. Develop countermeasures against powerful and stealthy rootkits

  ii. Use them to enhance platform's security properties

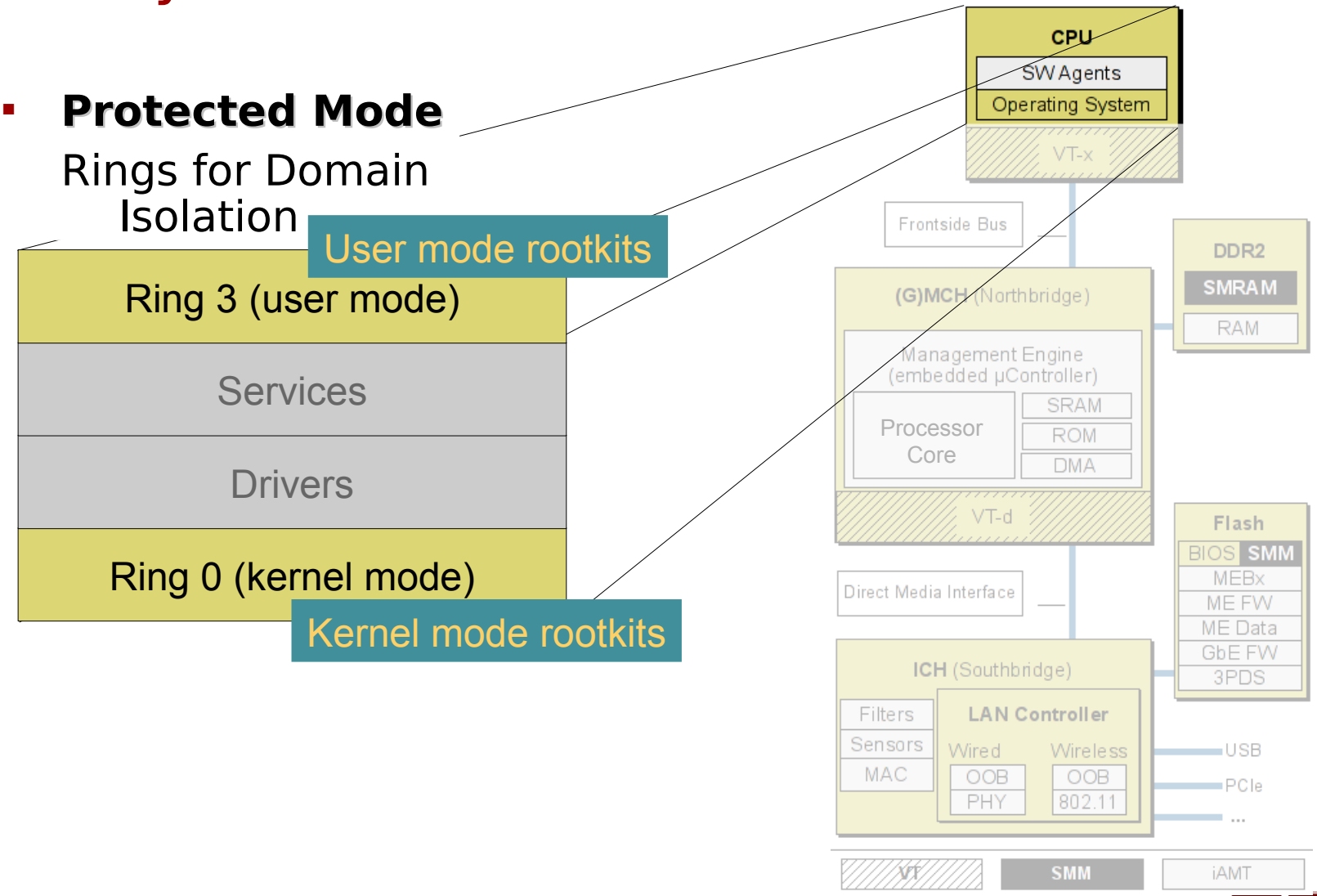
Challenges

- Research mainly done on rootkits
- Monitor needs safe place to stand: “Learning from Rootkits”
  - Understand properties of rootkit environments
  - Related to Trusted Computing Base
- Monitor environment must be *bullet proof*
  - Rootkit environments are not!
- Measurement strategy
  - How, when and what to measure?

Analysis of x86 Platform

- **Protected Mode**

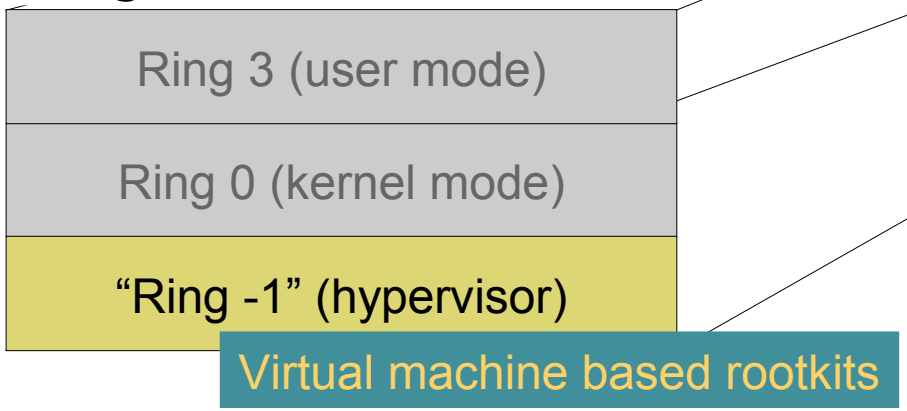
  Rings for Domain Isolation

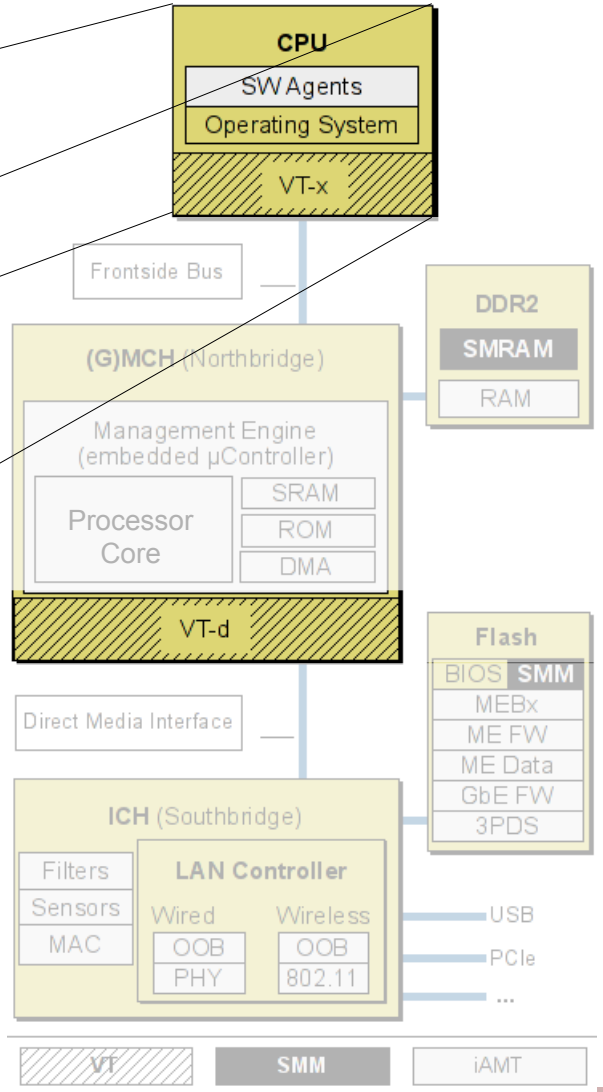


Analysis of x86 Platform

- **HW Virtualization Extensions:**

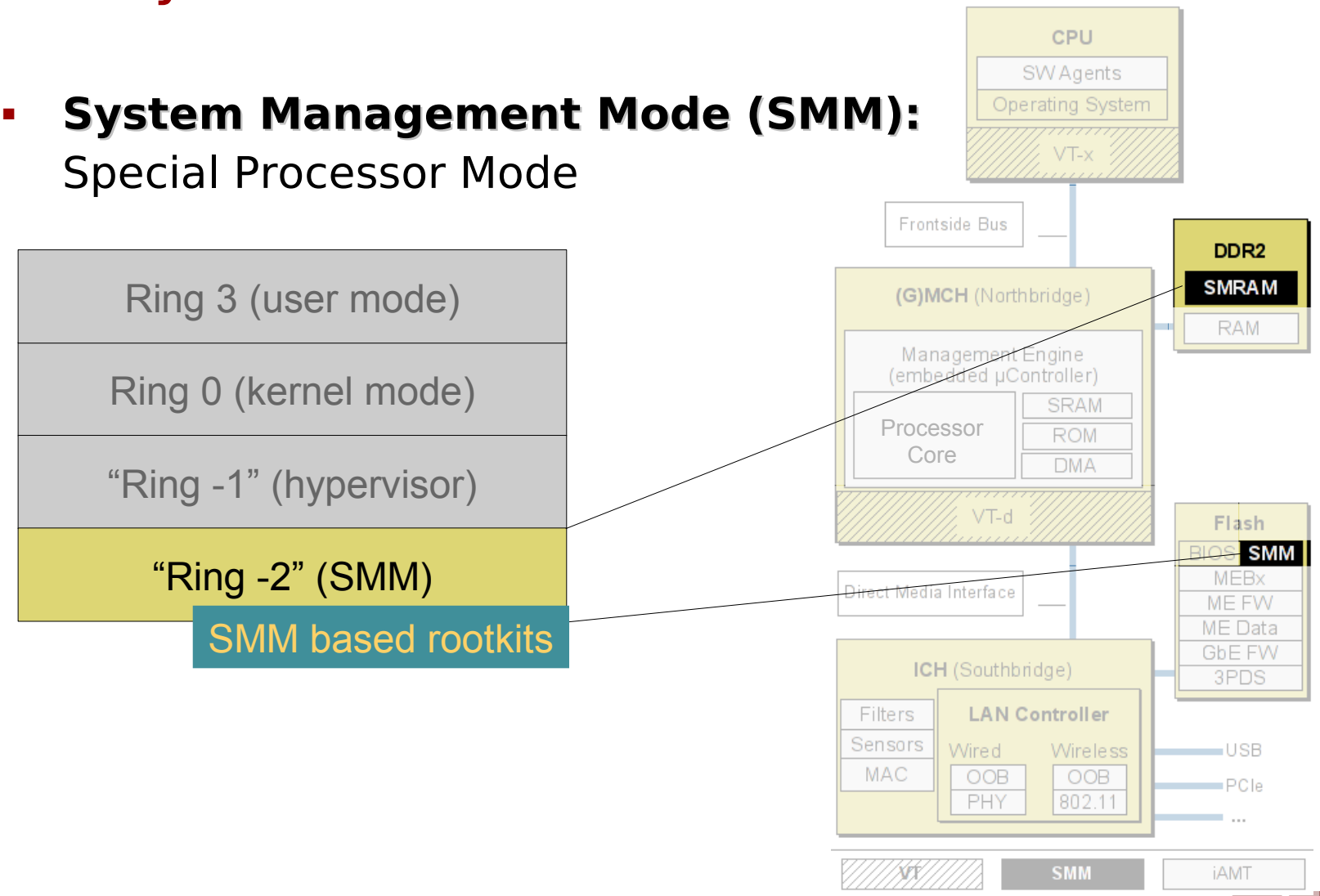
  E.g. OS Isolation





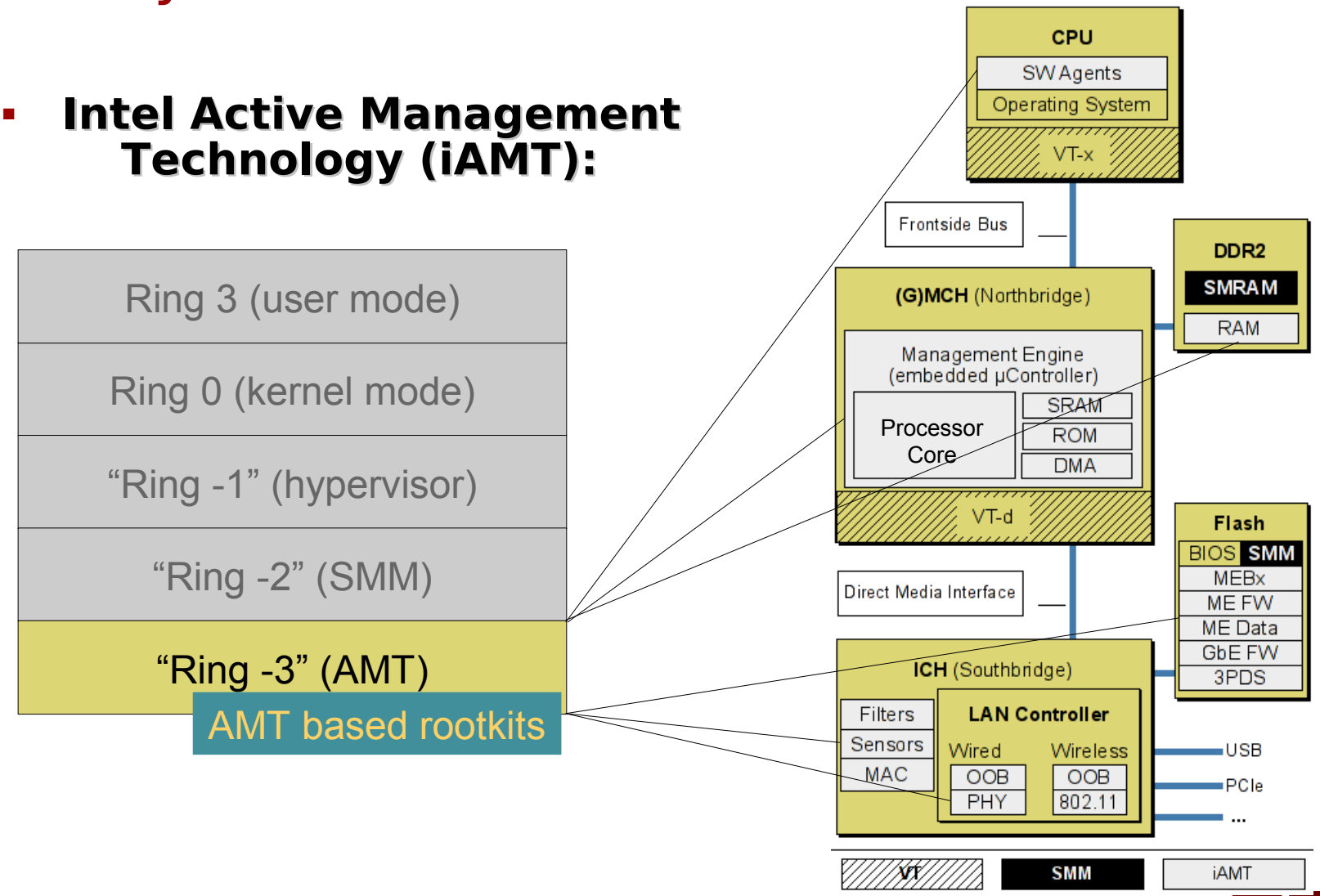
Analysis of x86 Platform

- **System Management Mode (SMM):**
  Special Processor Mode

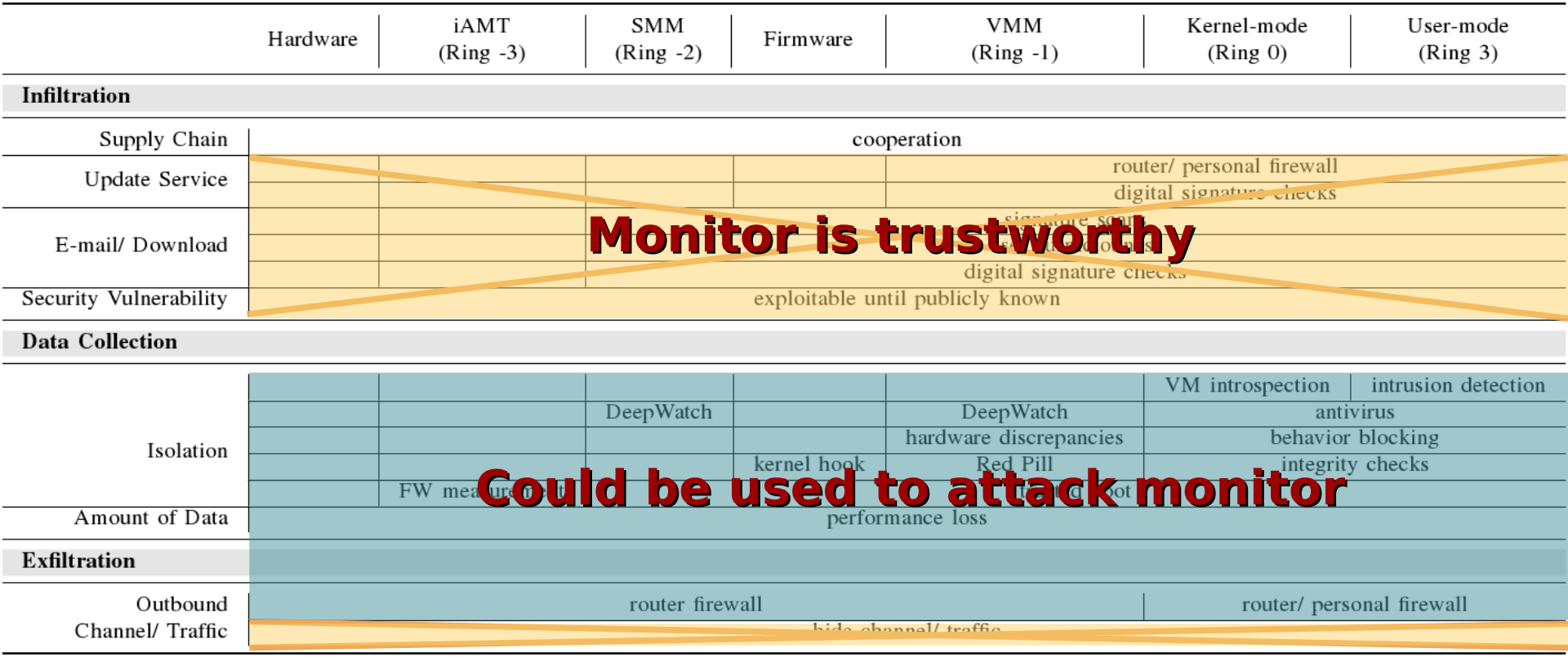


Analysis of x86 Platform

- **Intel Active Management Technology (iAMT):**



Challenges for Attackers/Rootkits



Important Related Work

- S. Embleton, S. Sparks, and C. Zou, *"Smm rootkits: a new breed of os independent malware,"* in SecureComm '08: Proceedings of the 4th international conference on Security and privacy in communication networks. New York, NY, USA: ACM, 2008, pp. 1–12.
- J. Rutkowska, *"Subverting Vista kernel for fun and profit,"* Black Hat USA, Aug. 2006. [Online]. Available: `http://blackhat.com/presentations/bh-usa-06/BH-US-06-Rutkowska.pdf`
- A. Tereshkin and R. Wojtczuk, *"Introducing Ring -3 Rootkits,"* Black Hat USA, Jul. 2009. [Online]. Available: `http://www.blackhat.com/presentations/bh-usa-09/TERESHKIN/BHUSA09-Tereshkin-Ring3Rootkit-SLIDES.pdf`

Conclusion and Further Research

- Modern x86 platforms have very powerful stealth capabilities (stealthier than root in user mode)
  - Cf. kernel mode, VMBR, SMM, iAMT
- ➢ Basis for monitor environment

- **Further Research:**
  - Countermeasures against rootkits (e.g., ring -3 rootkits)
  - Measurement strategy (cf. TOCTOU example)
    - When and what to measure?
      - Depends on use cases!
    - Which “ring”?
  - Develop runtime monitoring/attestation system according to measurement strategy

Questions?

Thank you!