Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Proaktive Sicherheitssysteme
→ Wo kommen wir her, wo geht es hin?

Andreas Speier

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
https://www.internet-sicherheit.de

if(is) internet-sicherheit.

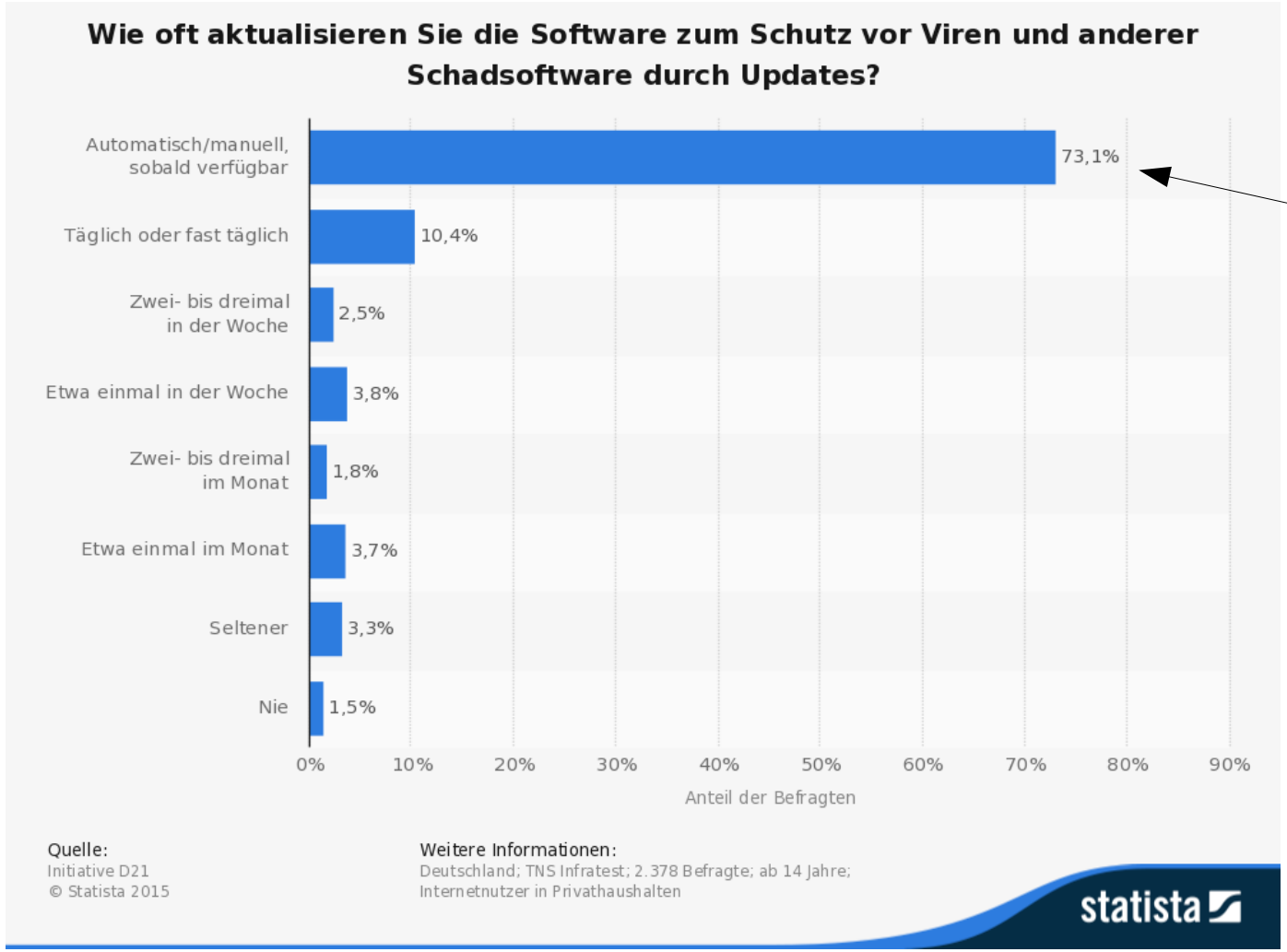
Problem Systemsicherheit

- "*Gängige*" Problembeseitigung bei Schwachstellen:

- Problem:
  - Verbessert nicht wesentlich die Sicherheitslage, da
  - Kern des Problems bleibt bestehen:
    - *Zu große Systeme*
    - *Keine Isolierung der Komponenten*
    - *Schlechte / schlecht getestete Software*
    - *Oft zu lange Update-Zyklen*

© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule

Problem Systemsicherheit
→ Updates



z.B. Windows: ~ 1 / Monat
→ Patchday

© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule

Problem Systemsicherheit
→ Fehler

- **Lines of Code (LoC)**
  - **Statistische Fehleranzahl** in Systemen
    - Ø Industrie: **15 – 20** Fehler auf 1000 LoC [1]
    - Ø MS Anwendungen: **10 – 20** Fehler auf 1000 LoC [1]
  - Je mehr Code, desto wahrscheinlicher sind Fehler
    - Beispiel: OS ↔ LoC (Mio.)
    - Tendenz steigend

Windows 2000	*4-5*
Windows XP	*40*
Windows Server 2003	*50*
Mac OS X 10.4	*86*
Linux Kernel 2.6.32	*12,6*
Linux Kernel 3.6	*15,9*

[1] - "Code Complete: A Practical Handbook of Software Construction", Second Edition, *Steve McConnell*, 2014

© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule

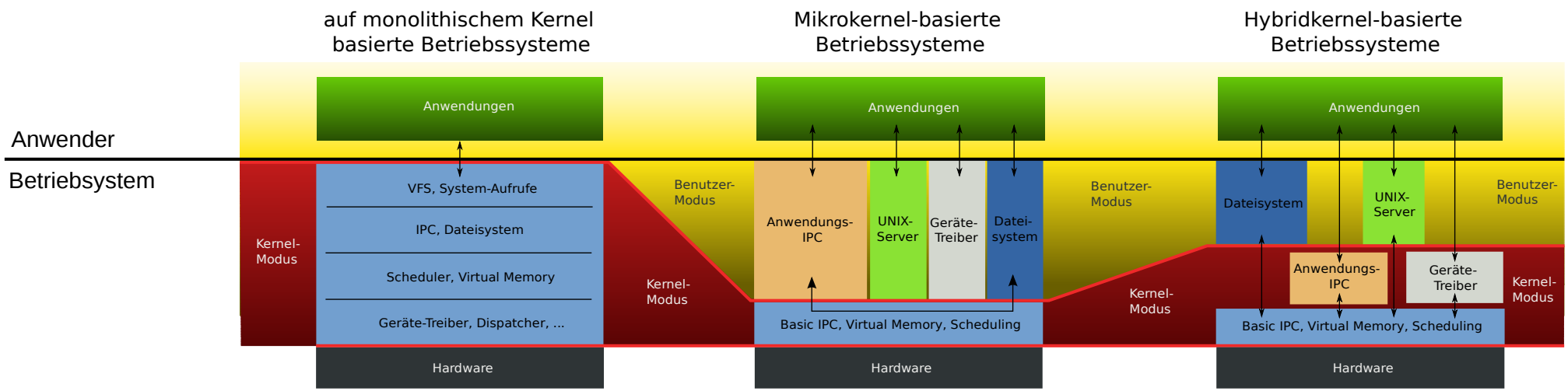
Problem Systemsicherheit
→ Fehler → Konsequenz

- **Überprüfbarkeit**
  - Geringe #LoC → leichter zu prüfen; u.U. formal verifizierbar
  - Hohe #LoC → (fast) unmöglich vollständig zu prüfen

© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Grundlagen
→ Kernel-Architekturen

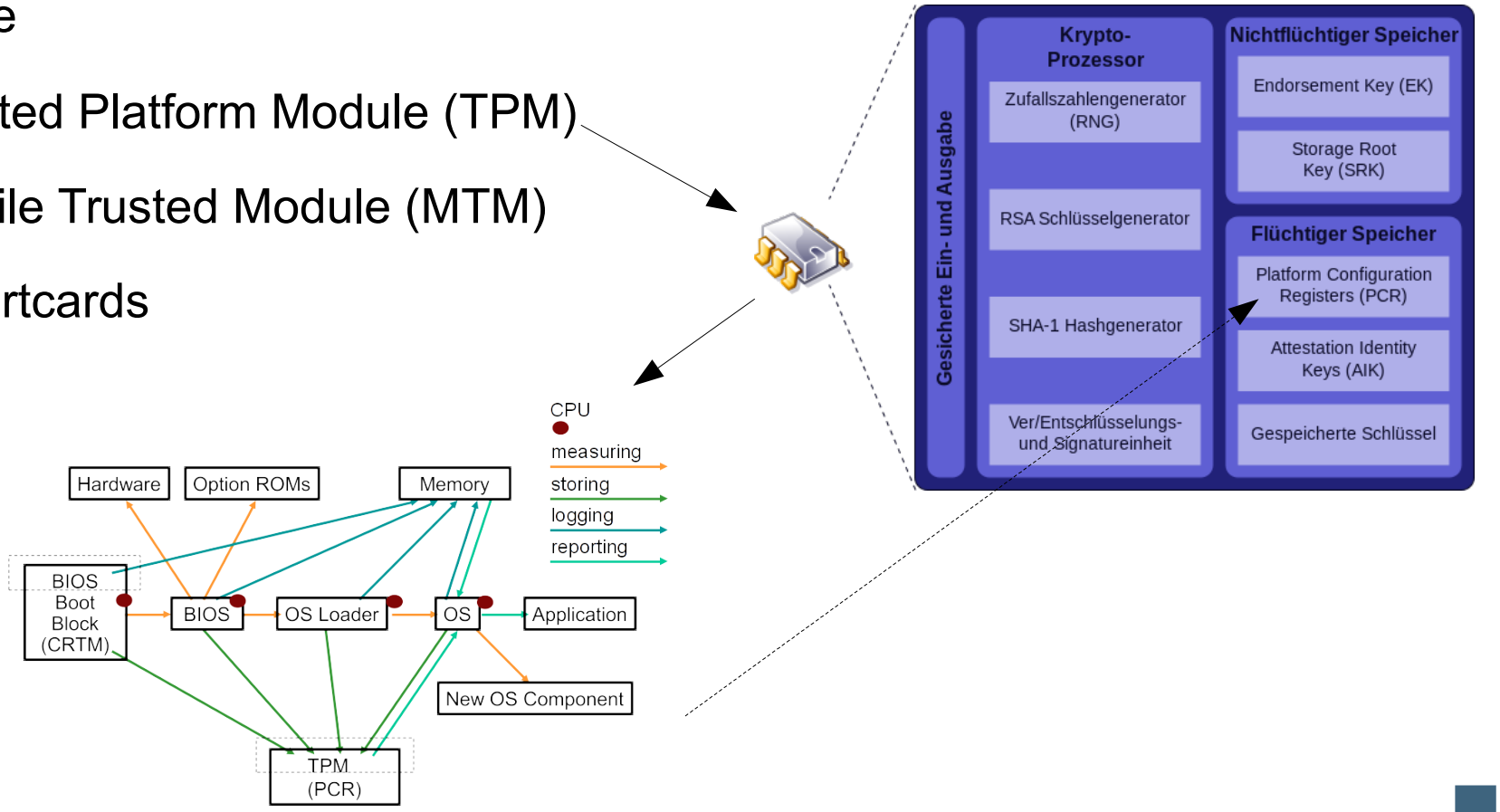
- **Beispiele unterschiedlicher Kernelarchitekturen:**
  - **Monolitische Kernel**
  - **µkernel**
  - **Hybride Kernel**



© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule

Sicherheitsarchitekturen
→ Grundlagen

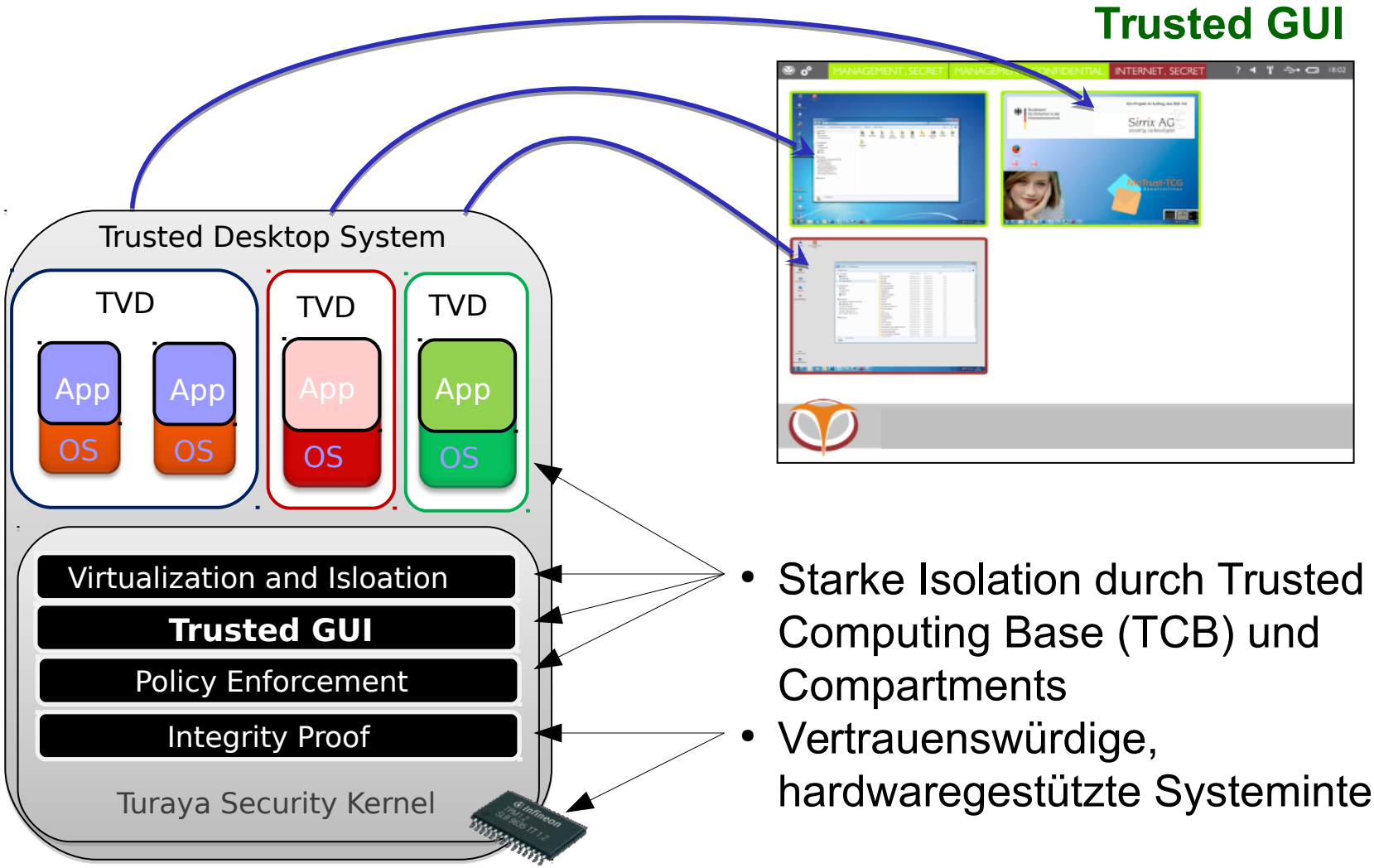
- Software alleine bietet keinen ausreichenden Schutz
- Sicherheit muss bereits in der Hardware beginnen → zum Schutz der Software
  - Trusted Platform Module (TPM)
  - Mobile Trusted Module (MTM)
  - Smartcards



CRTM = Core Root of Trust Measurement, PCR = Platform Configuration Register

© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule

Sicherheitsarchitekturen
→ Grundlagen

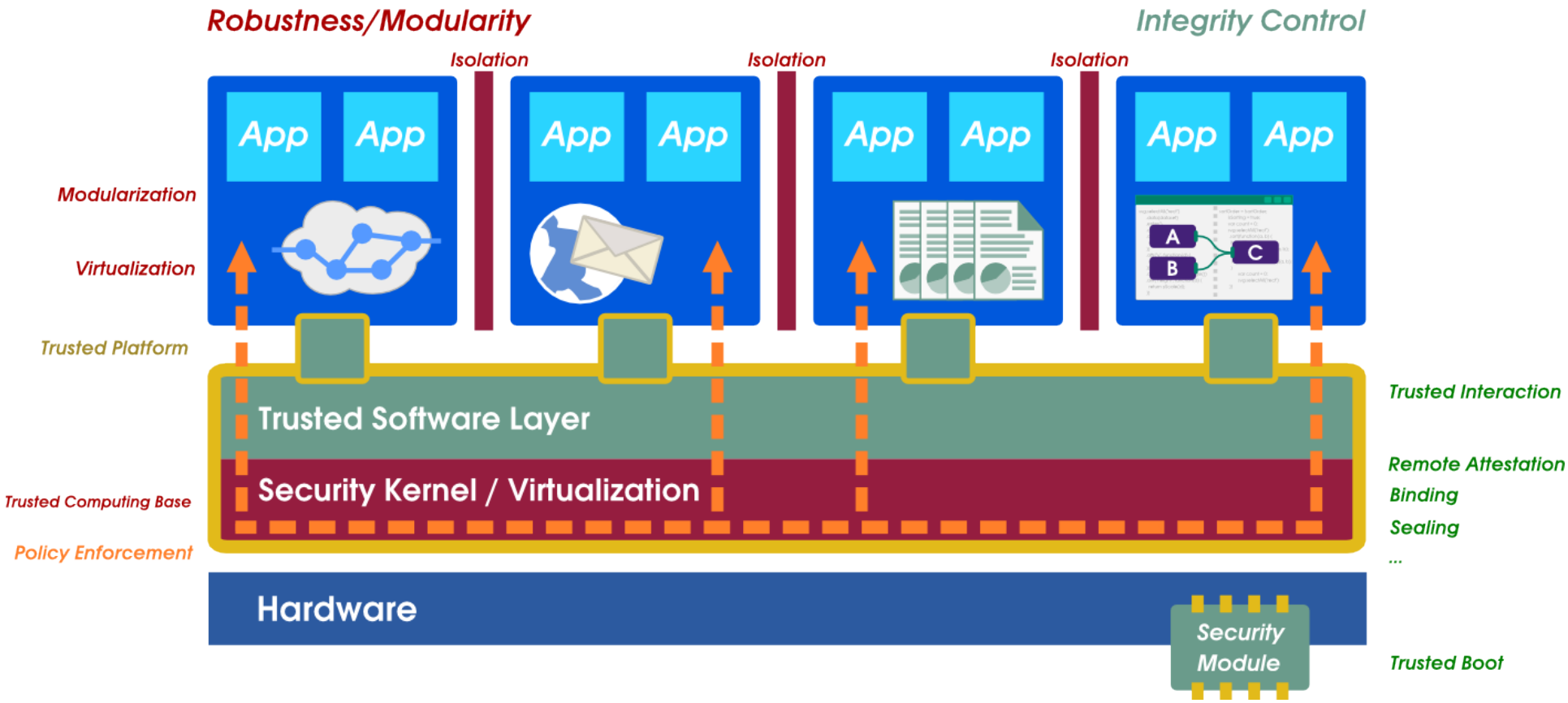


- Starke Isolation durch Trusted Computing Base (TCB) und Compartments
- Vertrauenswürdige, hardwaregestützte Systemintegrität

TVD = Trusted Virtual Domains

© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule

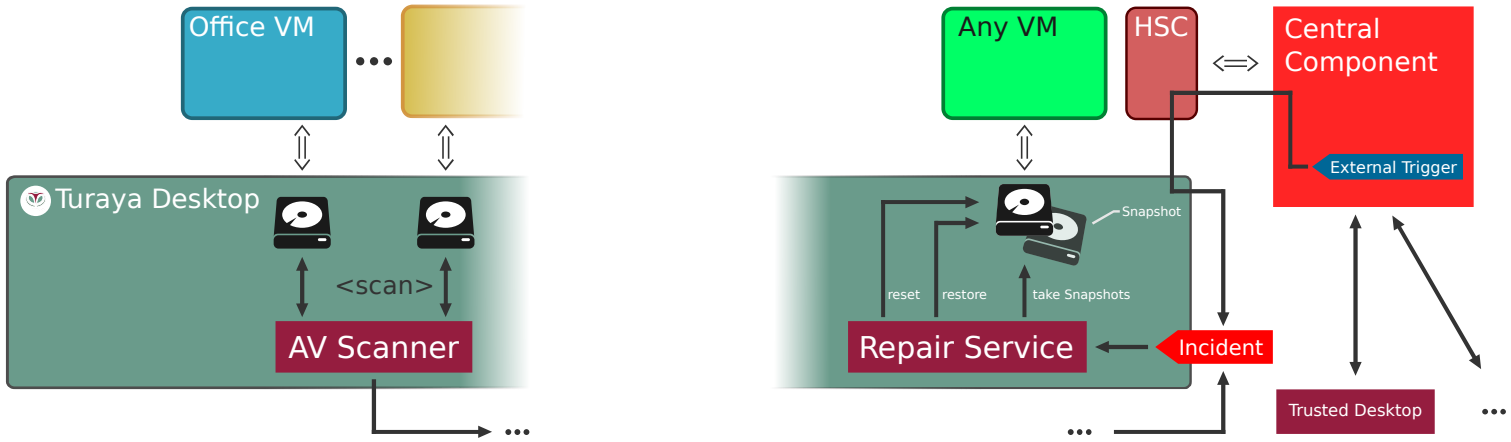
Sicherheitsarchitekturen
→ Grundlagen



© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule

Sicherheitsarchitekturen
→ Sicherheitsanwendungen

- Auslagerung von Sicherheitskomponenten
  - Schutz von Softwaresensoren → nicht angreifbar durch Schadsoftware in den Compartments
  - Systemüberwachung “von außen”
- Beispiel: *Externer AV-Scanner* (*Ergebnisse des iTES Projektes* [2])

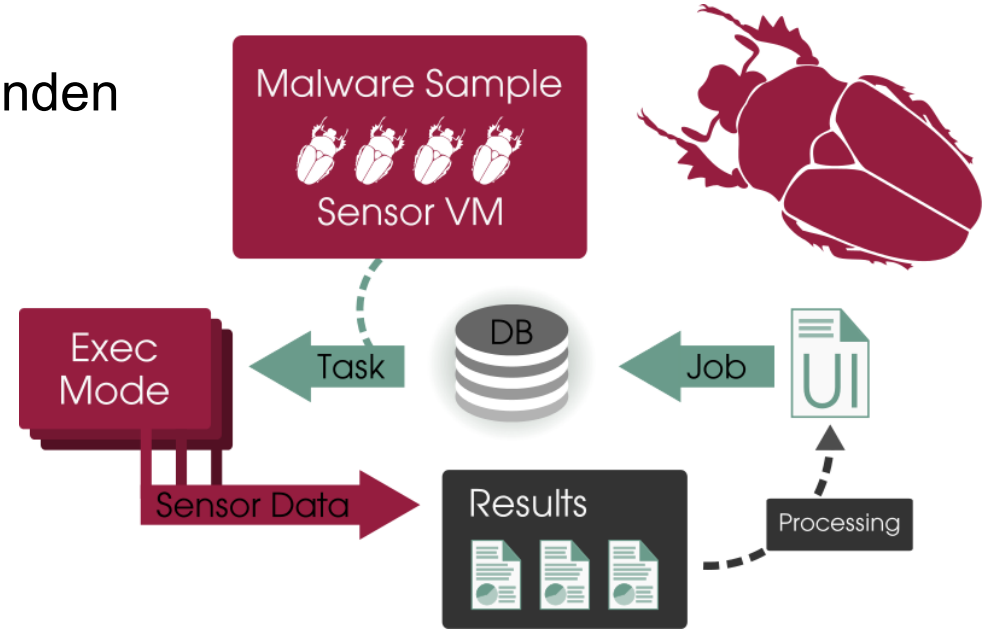


[2] https://ites-project.org

© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule

Kenne den Feind

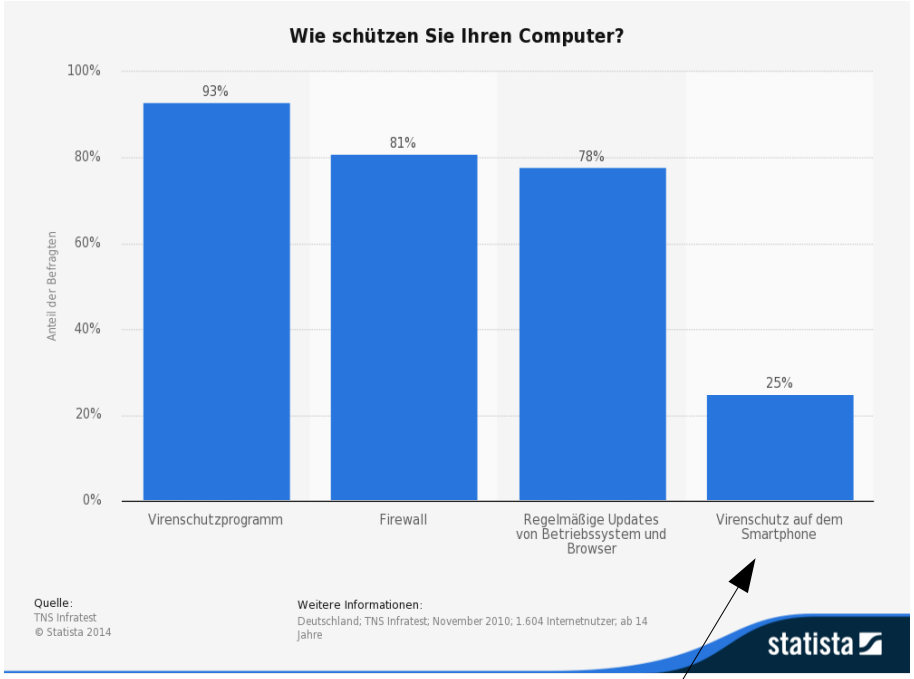
- **Schadsoftware-Forschung**
  - Was ist “anders” an Schadsoftware?
  - Gibt es ein eindeutiges Verhalten von Schadsoftware?
  - Wie lässt sich dieses zuverlässig erkennen?
- Analysieren von Schadsoftware
- Geeignete Gegenmaßnahmen finden



© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule

Mobile Systemsicherheit

- **Smartphones / Tabletts sind kleine Computer!**
- Sie leiden unter den selben Sicherheitsproblemen



Ziel: Übertagen von proaktiven Sicherheitstechnologien auf mobile Geräte

Meist ist es sogar noch schlimmer!

© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule

Mobile Systemsicherheit

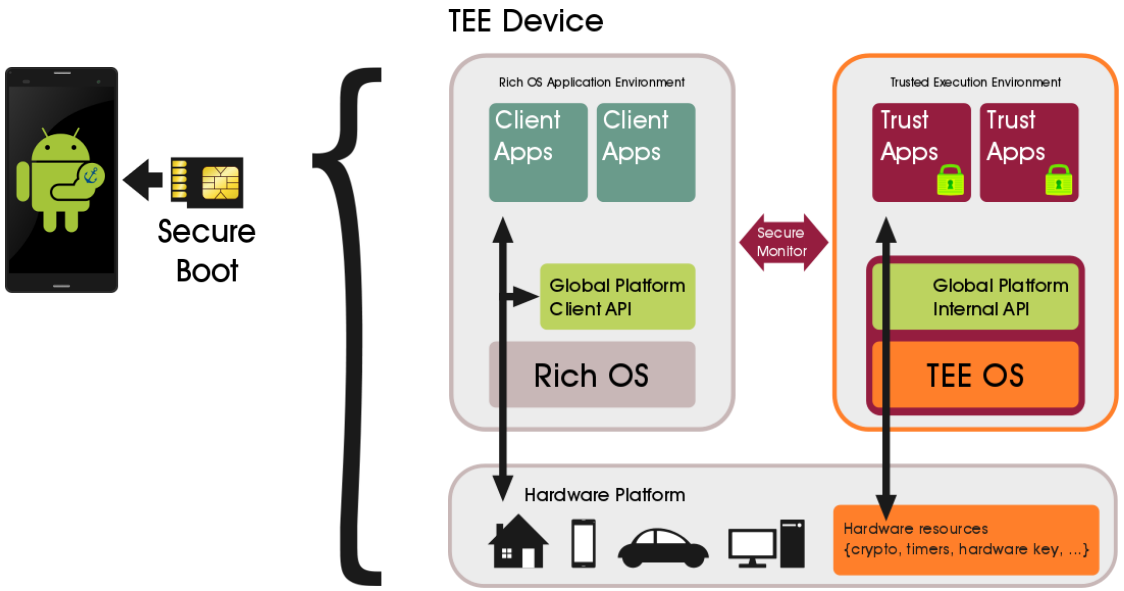
- **Schutz der Systeme bereits in der Hardware**
  - Mobile Trusted Module → Verfügbarkeit ???
  - Trusted Platform Moduel → für PC Plattformen entwickelt → ???
  - Alternativen → Smartcards !
- **Smartcards**
  - Geringere Möglichkeiten gegenüber TPM / MTM
  - Nicht so tief im System (Hardware) verankert
  - **NACHRÜSTBAR !**
- **Aktuelles Projekt:**
  - „Smartcard-basierte Sicherheitsanker für Android“ (SmaSA)

© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule

Projekt SmaSA

- **Wie lassen sich Sicherheitstechnologien auf mobilen Plattformen verwenden und bieten diese einen vergleichbaren Schutz zu Sicherheitssystemen auf PC Basis?**

- Verfügbare, hardware-gestützte Technologien nutzen:
  - Smartcards
  - Trusted Execution Environment (TEE) → *TrustZone bei ARM*



© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule

Kurzer Rückblick der Technologieentwicklung

EMSCB Turaya
- L4 µKernel
- µHypervisor
- L4-Linux

TrustedDesktop
- Hardened Linux Kernel
- VirtualBox / KVM VMs

BizzTrust
- Type Enforcement
- Security Extensions

TUD:OS
- L4 µKernel
- µHypervisor
- L4-Linux

QubesOS
- Hardened Xen
- Xen Hypervisor
- Xen Domains

grsecurity
Linux Kernel Patch Set

...

Forschung | *"Markt"*

© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule

Ausblick

- **Gehärtete Systeme**
  - Flexibel einsetzbar, daher geeignet für
    - Arbeitsplatzrechner
    - Server

- **µKernel Systeme**
  - Vergleichsweise unflexibel, aber klein, schnell und sicherer, daher geeignet für
    - Spezielle Systeme → industrielle Steueranlagen
    - Komponenten kritischer Infrastrukturen

- ***Die Entwicklung muss in beide Richtungen weiter gehen!***
- ***Es müssen immer wieder neue Ansätze entwickelt und getestet werden!***

© Andreas Speier, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Proaktive Sicherheitssysteme
→ Wo kommen wir her, wo geht es hin?

FRAGEN?

Andreas Speier

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
https://www.internet-sicherheit.de

if(is) internet-sicherheit.