CYBERSICHERHEIT IN DER HARDWAREENTWICKLUNG

RISIKEN, CHANCEN UND LÖSUNGEN

WARUM HARDWARE-SICHERHEIT?

- Angriffe auf Software sind bekannt, aber: Hardware wird zunehmend Ziel
- Beispiele: Spectre, Meltdown, Rowhammer
- Komplexe Systeme = viele potenzielle Angriffsflächen
- Sicherheitslücken in Hardware sind oft langlebig und schwer behebbar

VALUTIS TECHNOLOGIES

Unterschiede Hard- und Software-Entwicklung

Merkmal	Software	Hardware
Änderbarkeit	Hoch (Patches, Updates)	Sehr begrenzt, oft nicht nachträglich
Entwicklungsdauer	Schneller, agile Methoden	Monate bis Jahre, aufwendig
Fehlertoleranz	Hoch – Korrektur jederzeit möglich	Gering – Fehler schwer behebbar
Sicherheitsplanung	Häufig reaktiv	Frühzeitig notwendig
Testbarkeit	Automatisierte Tests verbreitet	Hardwaretests aufwändig, teuer

Unterschiede Hard- und Software-Entwicklung

Merkmal	Software	Hardware
Änderbarkeit	**Hoch (Patches, Updates)**	**Sehr begrenzt, oft nicht nachträglich**
Entwicklungsdauer	Schneller, agile Methoden	Monate bis Jahre, aufwendig
Fehlertoleranz	Hoch – Korrektur jederzeit möglich	Gering – Fehler schwer behebbar
Sicherheitsplanung	Häufig reaktiv	Frühzeitig notwendig
Testbarkeit	Automatisierte Tests verbreitet	Hardwaretests aufwändig, teuer

Unterschiede Hard- und Software-Entwicklung

Merkmal	Software	Hardware
Änderbarkeit	**Hoch (Patches, Updates)**	**Sehr begrenzt, oft nicht nachträglich**
Entwicklungsdauer	Schneller, agile Methoden	Monate bis Jahre, aufwendig
Fehlertoleranz	Hoch – Korrektur jederzeit möglich	Gering – Fehler schwer behebbar
Sicherheitsplanung	**Häufig reaktiv**	**Frühzeitig notwendig**
Testbarkeit	Automatisierte Tests verbreitet	Hardwaretests aufwändig, teuer

SECURE BY DESIGN IN DER HARDWARE

- Sicherheitsziele müssen Teil des Architekturentwurfs sein
- Vermeidung unnötiger Funktionalität (Reduktion der Angriffsfläche)
- Isolation und physische Trennung als Designprinzip
- Beispiel: Datenfluss nur in eine Richtung (Dioden)

VALUTIS TECHNOLOGIES

BEISPIEL 1 – TRUSTED PLATFORM MODULE (TPM)

Problem: Schlüssel können durch Schadsoftware oder Speicheranalyse ausgelesen werden („Cold Boot Attacks“)

Hardwarelösung für z. B. BitLocker, Secure Boot:

- Eigenständiger Sicherheitschip auf dem Mainboard
- Speichert kryptografische Schlüssel
- Die Schlüssel verlassen niemals das TPM

VALUTIS TECHNOLOGIES

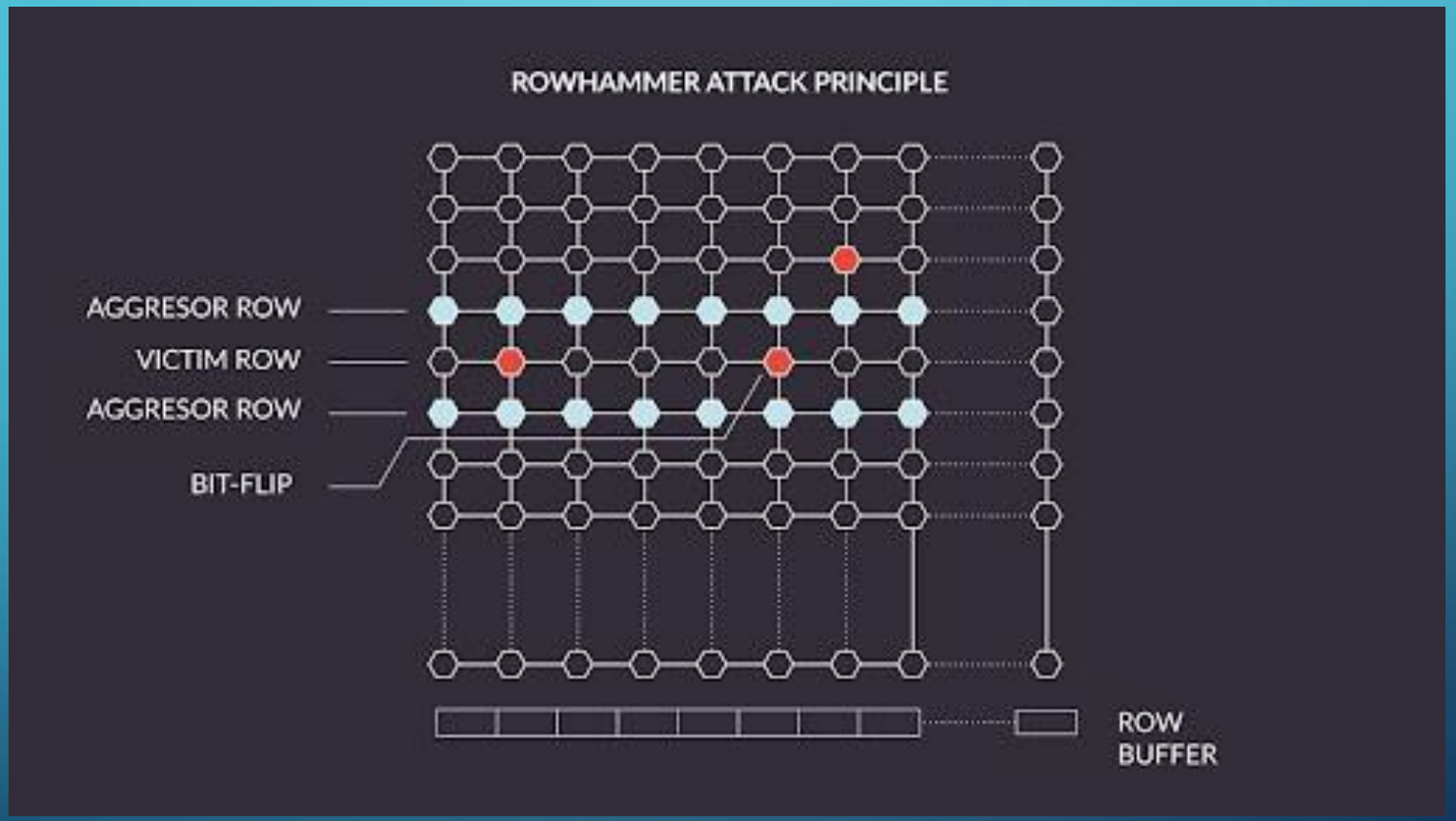
BEISPIEL 2 – MEMORY MANAGEMENT UNIT (MMU)

Problem: Ohne harte Speichertrennung können Programme versehentlich oder absichtlich auf fremde Speicherbereiche zugreifen.

Hardwarelösung:

- MMU ist ein Bestandteil der CPU
- Übersetzt logische Adressen in physikalische und prüft Zugriffsrechte
- Prozesse erhalten isolierte Speicherbereiche ("virtueller Speicher")

NEGATIVBEISPIEL – ROWHAMMER-ANGRIFF



https://opensource.googleblog.com/2021/11/Open%20source%20DDR%20controller%20framework%20for%20mitigating%20Rowhammer.html

VALUTIS TECHNOLOGIES

FAZIT – HARDWARE IST UNVERZICHTBAR

- Höhere Resilienz gegen Angriffe
- Geringere Angriffsfläche bei gutem Design
- Kaum manipulierbar

VALUTIS TECHNOLOGIES

Ransomwaresicheres Backup - V^{t}-Cyberstorage

Gemeinsam die Ära der Ransomware beenden.

VALUTIS TECHNOLOGIES

Alexander Haunhorst

01525 4253126

ah@valutistech.com

LinkedIn