Kraftwerke am Internet: IT-Sicherheit und Industrie 4.0

Michael Hohmuth, Kernkonzept GmbH

Tim Lackorzynski, TU Dresden

MICROKERNEL MADE IN GERMANY

Inhalt

IT-Sicherheit und Industrie 4.0?

Unser Ansatz: Komplexität / Angriffsfläche minimieren

Digitalisierung in der Industrie?

Prozessanalyse

Predictive Maintenance

Losgröße 1

Dezentralisierung

Vernetzung

…

(Bild: BitKom)

Datenerhebung/-austausch/-verarbeitung …

… übers Internet

Die Versäumnisse von gestern …

IT-Infrastruktur ohne Sicherheit

Folge:

Viren

Würmer

Spam

Neueste Beispiele:

Erpressungstrojaner à la Locky, Petya, TeslaCrypt

(Bild: Sophos)

(Bild: heise Security)

… und die Fehler von heute …

Vernetzung von Geräten, die nicht vernetzt werden sollten:

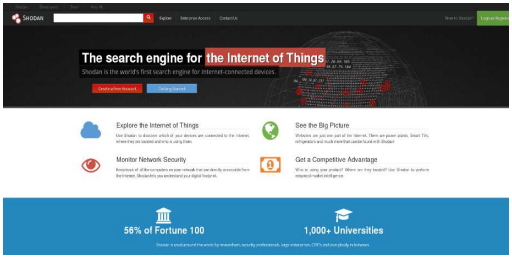
SCADA, Krankenhausinfrastruktur, Hochöfen …

IoT?

Industrie 4.0?

Smart Grids?

Kraftwerke?



(www.shodan.io)

(Spiegel Online)

… führen zu den Problemen von morgen

Stuxnet

Hochprofessionelles Umfeld

Staaten:

- USA: NSA, TAO...
- Israel: Unit 8200
- China: PLA Unit 61398…
- Nordkorea: Bureau 121
- Syrien: Syrian Electronic Army
- …

(Bild: Ralph Langner)

… führen zu den Problemen von morgen

McAfee:

„Cybercrime is a growth industry.”,

„The combination of high value, low risk, and low ‘work factor’ […] makes cybercrime a winning proposition.”

Allianz rechnet mit 10x-Wachstum bei Versicherungen gegen Cybercrime

Das Internet ist Spielwiese für unterschiedlichste Interessen:

Militärische – politische – monetäre

Fazit

Industrie 4.0 heißt: Sie betreiben ein IT-System

Daten sind Teil ihrer Wertschöpfung

Paradigmen aus der IT-Welt müssen umgesetzt werden:

Verschlüsselung, Authentifizierung

SW-Update-Zyklen, SW-Management-Prozesse

(BSI-)Zertifizierungen für kritische Infrastrukturen

Mit „normaler Software“ und Hardware aus dem Laden nicht zu leisten

Die Bundesregierung empfiehlt

Regierung ruft die Bevölkerung zu Hamsterkäufen auf

Individueller Vorrat an Lebensmitteln für zehn Tage

Je zwei Liter Wasser pro Person und Tag

Bitte halten Sie eine Taschenlampe bereit

Angriffe erkennen / verhindern

Erkennung / Mitigation

Löblich

Kommt zu spät!

Prevention

Angriffsfläche minimieren

Kleine Trusted Computing Base

Das Problem

Vertrauensverlust

in die Betriebssysteme unserer IT

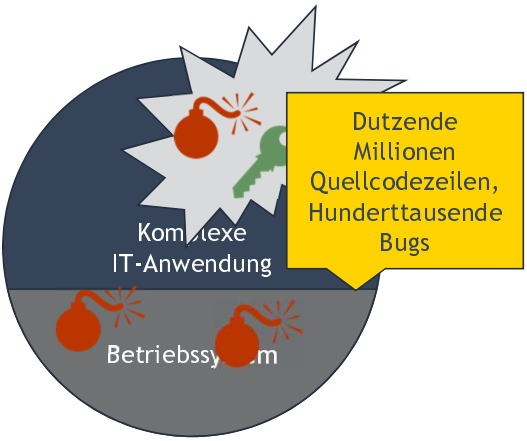
Zu hohe Komplexität

Zu viele Bugs

Große Angriffsfläche

Patch auf Patch auf Patch

Es bleiben immer Fehler übrig …



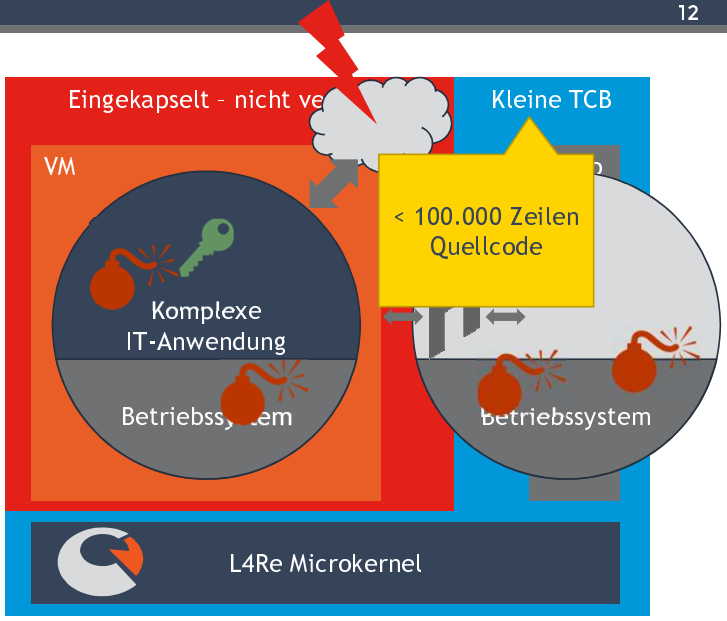
Die Lösung

Isolation

Kleine Trusted Computing Base (TCB)

Sichere Kommunikation

L4Re Microkernel



L4Re Betriebssysteme-Technologie

x86, ARM, MIPS

- 32 / 64 Bit

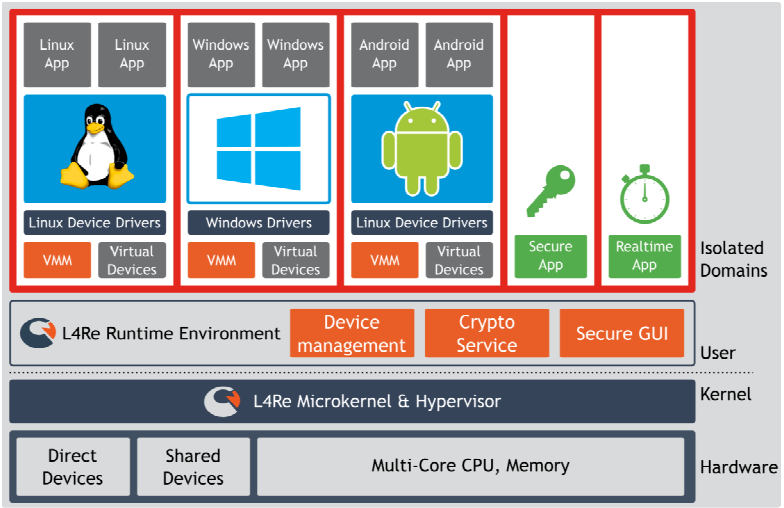
µApps mit kleiner TCB

Raum-/Zeit-Isolation

Virtualisierung

- Para- und HW-Virt.
- Mit untrusted VMMs

Gereift seit 1997



KERNKONZEPT

Vielen Dank!

www.kernkonzept.com

zwanzig20
PARTNERSCHAFT FÜR INNOVATION

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

MICROKERNEL MADE IN GERMANY

Backup

www.kernkonzept.com

Vergleich / Alleinstellungsmerkmale

Vs. „gehärtete“, herkömmliche Systeme

- Trusted Computing Base mind. 2 Größenordnungen kleiner

Vs. Separation Kernel

- Offene Systeme mit dynamischem Start/Stopp von Komponenten

Vs. formal verifizierte Mikrokerne

- „It works“ — breite Unterstützung verfügbarer Hardwareplattformen

Vs. andere Mikrokerne

- Sichere Mikrokernschnittstelle — 20 Jahre Forschung
- Vertrauen durch Open Source

Kernkonzept: Mission

Das L4Re Betriebssystem:

Sicher — vertrauenswürdig — offen

Entwickeln — vermarkten — supporten

Von klein bis groß

- IoT, Industrie 4.0, Infrastruktur, PC / Mobile, Server, Cloud
- Konsumenten, Industrie, Verwaltung, VS-Bedarfsträger

Kernkonzept — Dienstleistungen

Consulting

Wir helfen Kunden, das L4Re-System in eigenen Produkten und Lösungen einzusetzen

Auftragsentwicklung / Wartung

Entwicklung und Wartung von L4Re-basierter Software

Lizenzierung

Open-Source- und kommerzielle L4Re-Lizenzen

Vertrauenswürdig durch Open Source

“Nothing up our sleeves”

Keine Backdoors, keine Malware — nachprüfbar

Maximale Transparenz und Qualität, minimale Angriffsfläche

Sichere Systemplattform für jeden Industriezweig

Kostengünstig

Kein Hersteller-Lock-In

Kooperatives Entwicklungsmodell

Kunden und Anwendungen

Sichere Netzwerkinfrastruktur

Laptop

Mobile Endgeräte

CPU-Verifikation

Auto-Armaturenbrett

Smart Meter Gateway

genua
Soviel ist sicher.

Imagination

Ziele — L4Re-System in fünf Jahren

Industrieplattform mit Open-Source-Community

Nachhaltige Finanzierung für Infrastruktur und Entwicklung

Qualität

Testsuite auch für Kunden verfügbar

Einsatz formaler Methoden

Vertrauenswürdigkeit

Zertifizierung für wichtige Anwendungsfelder, z. B. CC / EAL

Neue Anwendungsfelder erschlossen

Industrie 4.0, Internet of Things, Cloud

fastVPN - Überblick

Projektpartner	Typ	Kernkompetenzen
Teleconnect GmbH Dresden Verbundkoordinator	KMU	Systemdesign, 25 Jahre Erfahrung in Software- und Hardware-Entwicklung insbesondere im Bereich Kommunikation, Schaltkreisentwicklung, Projektmanagement;
Kernkonzept GmbH	KMU	Software-Entwicklung (Betriebssystem, Virtualisierung) und Sicherheit
TU Dresden, Lehrstuhl Datenschutz und Datensicherheit (DuD)	UNI	Datenschutz & Datensicherheit in und durch verteilte Systeme
TU Dresden, Interactive Media Lab (IML)	UNI	Mensch-Computer-Interaktion, Benutzungsschnittstellen, interaktive Informationsvisualisierungen
Vattenfall Europe Netcom (assoziierter Partner)	IND	realistische Industrieanforderungen/Testumgebung, Erfahrungen mit Sicherheitslösungen und -konzepten im industriellen Umfeld

fastVPN - Überblick

- Echtzeitfähige, breitbandige und leicht erweiterbare Datenübertragungs-infrastruktur:
  - auf vorhandener Infrastruktur zeitgleich mit bestehenden Systemen
  - transparent für höhere Schichten, realisiert als fastvpn-Nodes
  - Basistechnologie: ITU-T G.9960 (G.hn), IEEE 802.3 (Ethernet)
  - Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit unabhängig vom Anwendungsprotokoll
- Kryptographische Absicherung der Datenübertragung
- Mikrokern-basierte Software-Architektur mit Virtualisierung