IT-Security – Solution or Problem?

A Critical Industry Overview

5. Security Day HdM Stuttgart

Prof. Walter Kriha
Computer Science and Media
HdM Stuttgart
walter@kriha.de

Agenda

- Some History
- Industries
  - Finance
  - Automotive
  - Public Water Supply
  - Industry 4.0
  - Retail
  - Digital Platform Economies
- Consumer Products
  - Cars
  - Smart Home
- Summary
- IT-Security – Problem or Solution?
- Building Blocks for Secure Systems
  - Compartments
  - Safety by Architecture

History I

- 2001 met secure language “E” and capabilities via cap-talk mailing list
- 2002-2010 IT-Security course at HdM, books on internet security and secure systems with Roland Schmitz. “Sichere Systeme” had a focus on damage reduction technologies in software (capabilities, language security, robustness)
- 2011 HBGary – a sign of what was to come: state sponsored hacking, cyber warfare
- 2012 Giving up IT-Sec. Moving to secure systems, a mixture of technical, social and political research on security related topics (NeoConOptiCon, usability and security, damage reduction technologies)
- 2013 Research on critical infrastructures (smart energy grids etc.)

History II

- 5/2013, talk at Smart Grid Week Salzburg
  - IT fundamentally unsafe
- 11/2013 Blackout – Smart Energy Grids, HdM Stuttgart
- 12/2014, IT-Sicherheit – Bedrohungen und Schutzmechanismen für elektrische Netze, Wien
  - Resilient Architecture, Patterns for Damage Control
- 4/2016, Automatisierungstreff VDE, Böblingen
  - Robust Systems vs. Security-Industrial Complex
- 11/2016, WIENER NETZSERVICE FORUM
  - IT-Security in times of industrialized hacking

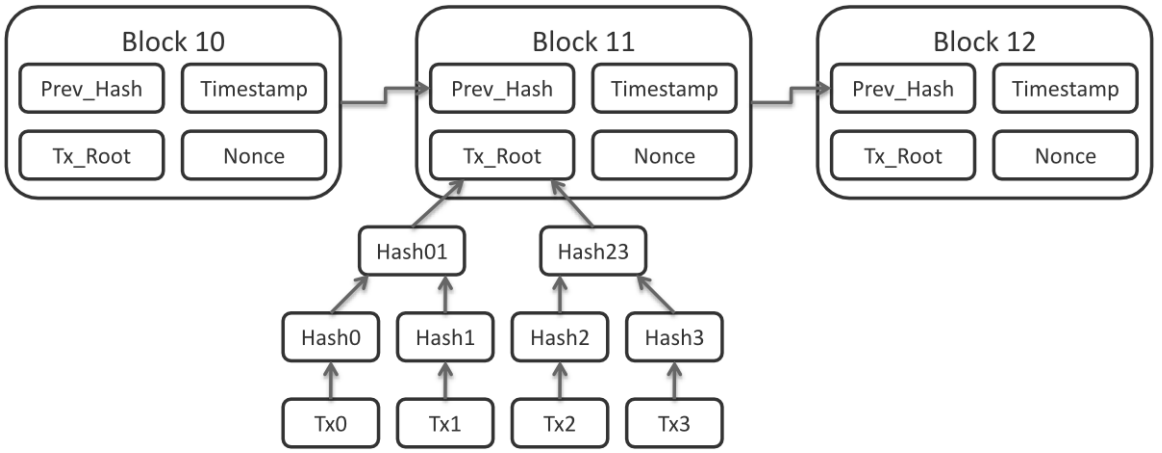
Industries

Finance::Challenges

- Expensive IT-Sec Infrastructure to maintain (Seasoned ATMs, new mobile clients like TWINT, data-leaks etc.)
- Disruption: >12000 Fintechs (block-chain etc.)
- Increasingly sophisticated attacks on high levels (SWIFT etc.)
- Financial pressure from 0-interest policy
- Extreme forms of risk-taking by interested parties (investment banking

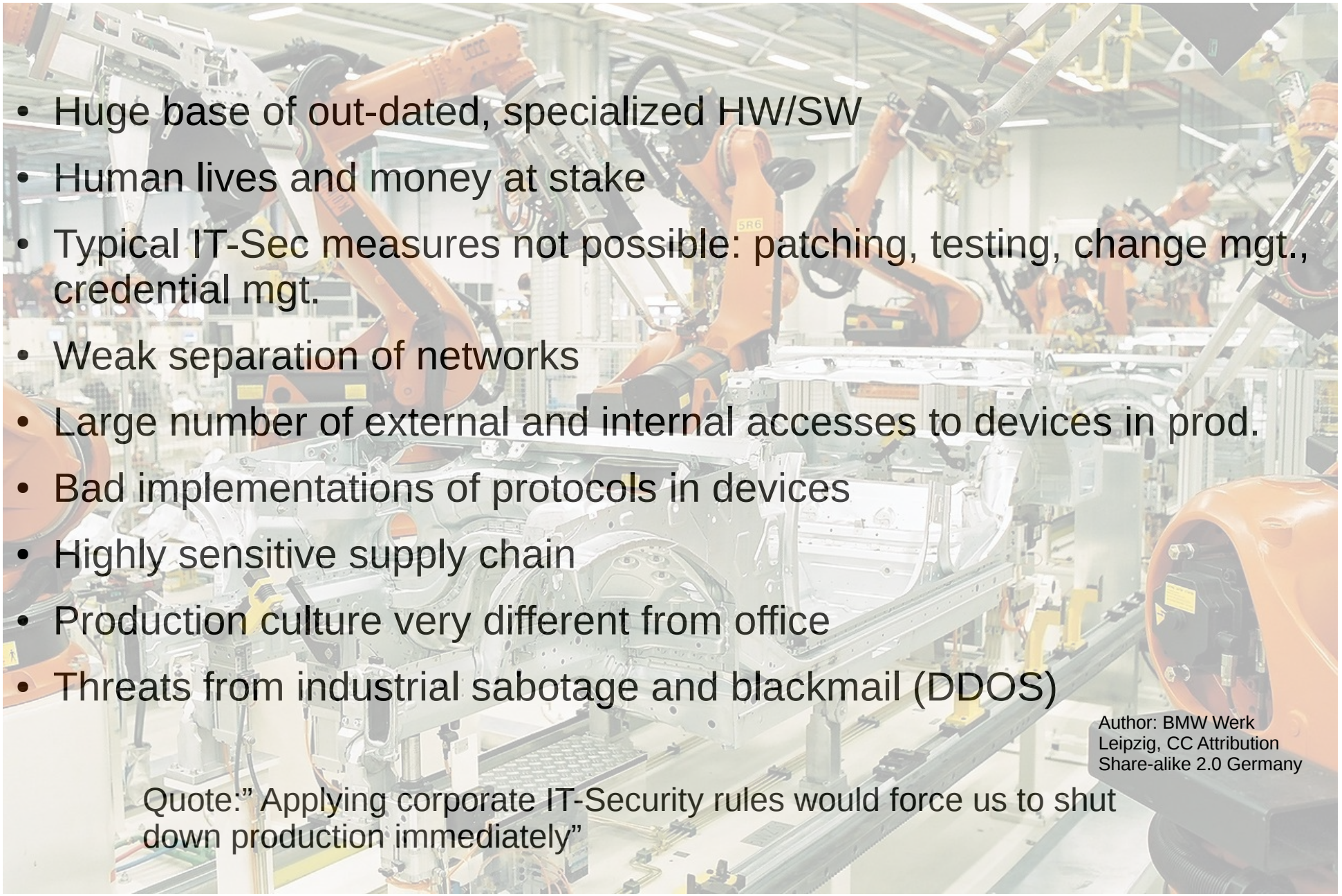
Is there still a need for centralized money management? Will banks be able to afford excellent IT-Security in the future?

Finance::Solutions



- Classic IT-Sec: Security Architecture designed around compartments, data-classification, need-to-know/need to do, no uncontrolled DevOps, HSM based key management, Mainframes, backend security via secure delegation
- Data-loss prevention (dumb terminals, closed interfaces) OSINT (Media/Darkweb monitoring) to pro-actively detect attacks and trends
- Fix-the-employee (web based trainings, videos and others)
- Block-chain technology for smart contracts, anonymous money transfers, crypto-currency key stores etc.

Automotive Production::Challenges



- Huge base of out-dated, specialized HW/SW
- Human lives and money at stake
- Typical IT-Sec measures not possible: patching, testing, change mgt., credential mgt.
- Weak separation of networks
- Large number of external and internal accesses to devices in prod.
- Bad implementations of protocols in devices
- Highly sensitive supply chain
- Production culture very different from office
- Threats from industrial sabotage and blackmail (DDOS)

Quote:" Applying corporate IT-Security rules would force us to shut down production immediately"

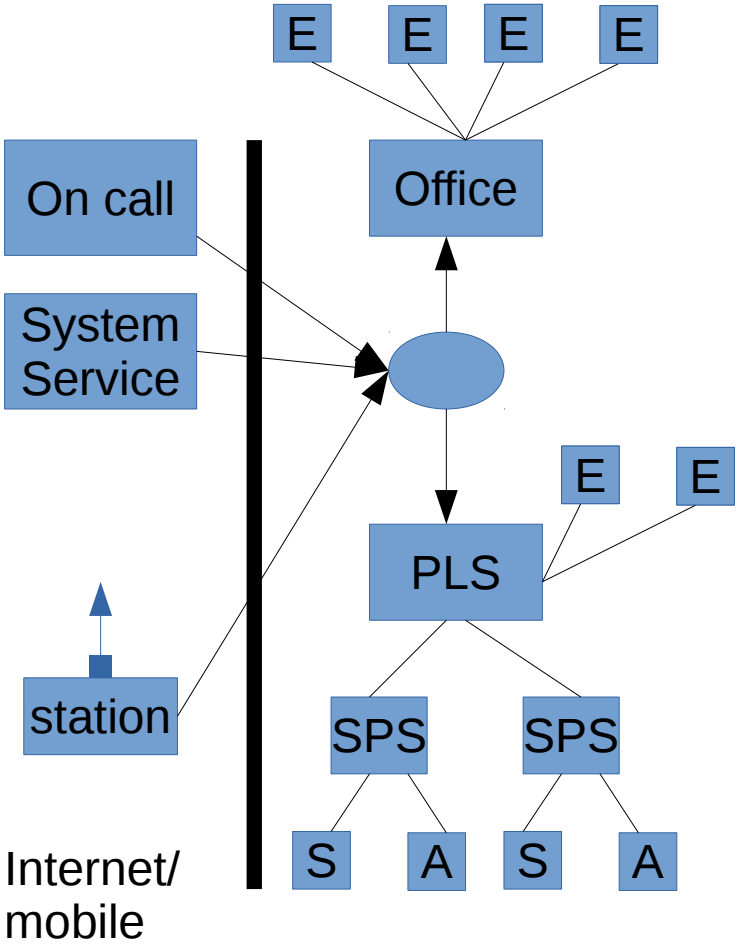
Automotive Production::Solutions

- Create network/admin compartments
- Dedicated filtering equipment for prod. sections
- Control and record admin access
- Disallow direct access from outside
- Force suppliers into update strategy
- Influence supplier technology (robust protocols)
- Risk-management that fits to production
- Create automated verification strategy against sabotage

Clearly a long-term strategy is needed to prevent disruption. This will include things mentioned under “Industry 4.0” later, but hopefully also a concept for a resilient architecture.

Public Water Supply::Challenges

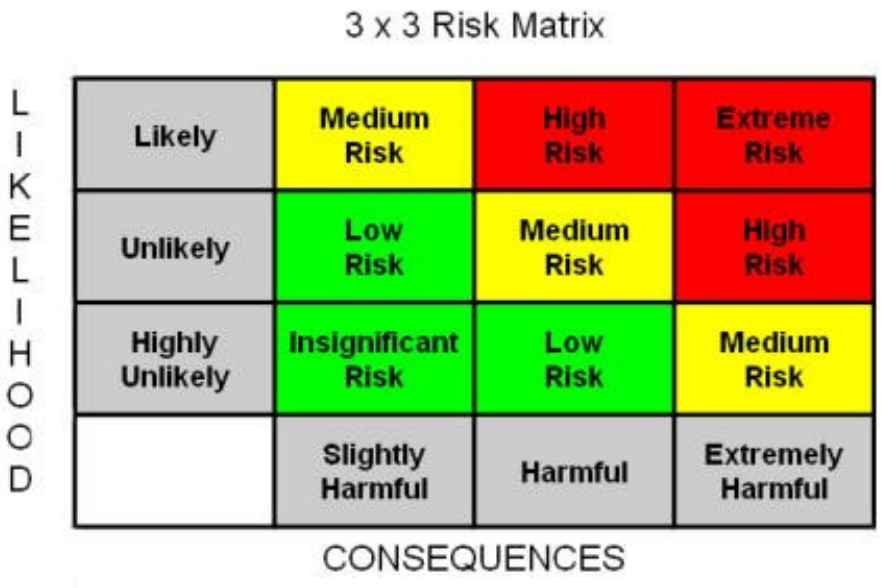
- Highly distributed, stand-alone infrastructure with proprietary protocols and heterogeneous hardware
- Systems operating unsupervised in remote areas
- Availability key
- Subject to critical infrastructure laws
- Remote control of stations
- Long life-cycles of equipment
- Low-latency, real-time requirements
- Critical physical systems
- Blackmail more likely than APT



Public Water Supply::Solutions

- Classic risk-analysis (DoS, malware, sniffing, physical threats etc.)
- Compartments, (subnets, operation vs. admin)
- Encryption, filtering, detection, white-listing applications
- Hardening of devices and software, cleansing, anti-virus.
- Logging and monitoring of data flow
- State-of-the-Art protection, reporting interface to BSI, ISMS
- Restricted access (time, rights)
- Install SOC, audits, regulations, strategy, credential mgt.

- Signing of sensor data, anomaly detection with deep learning,
- Splitting system in independent parts
- Increasing water reserves



Is a classic risk analysis REALLY the right approach for critical infrastructures?

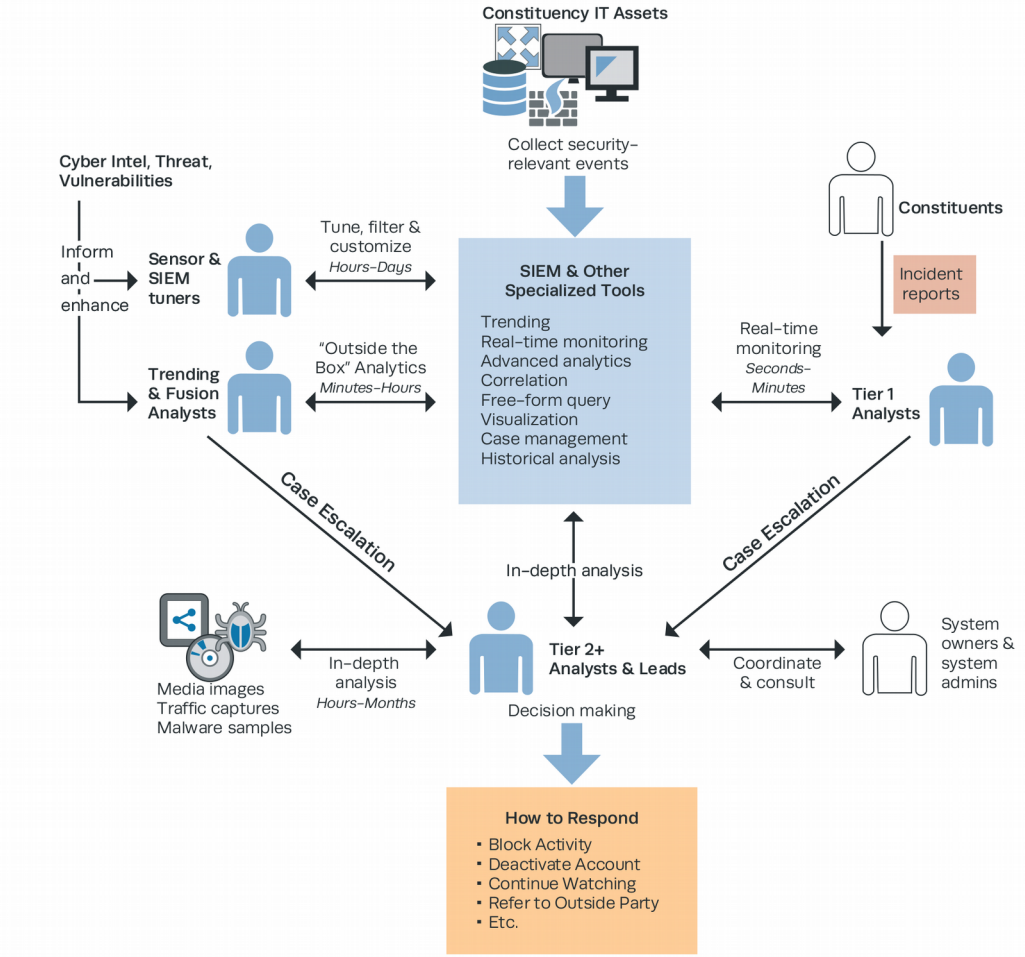
Industry 4.0::Challenges

- Highly targeted, complicated (ATP) attacks
- Intelligent, re-programmable devices
- Centralized remote control of production
- Sensitive and valuable data
- Insider threats

Targeted attacks makes commercial malware protection useless as these signatures are never seen outside of the company under attack

Industry 4.0::Solutions

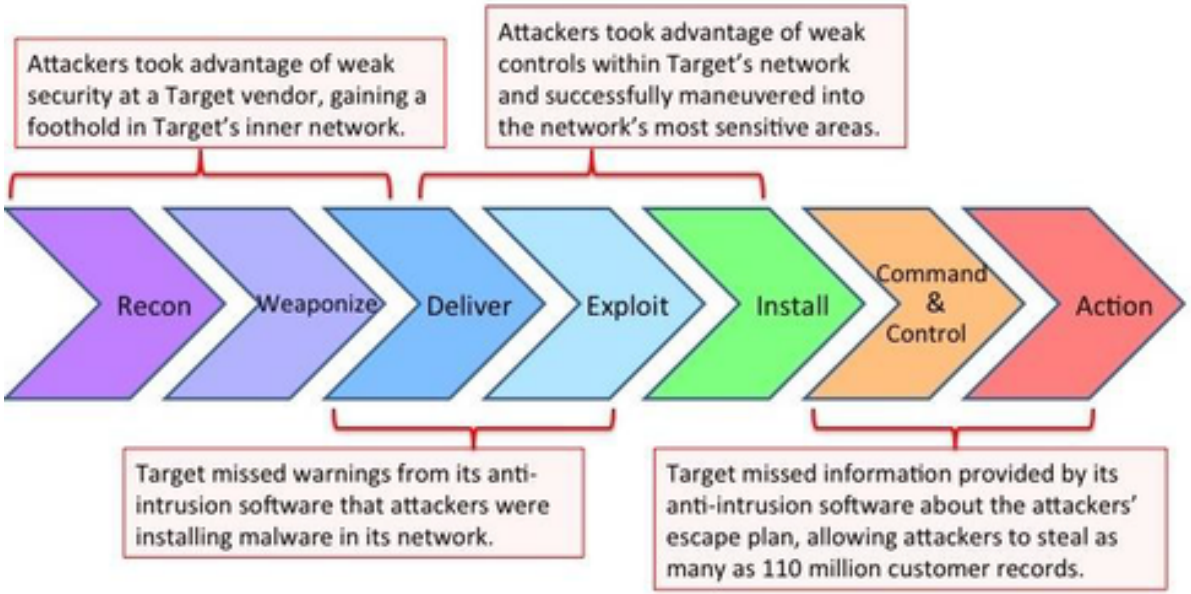
- Shift from prevention to detection and response
- Incident Response: “Kill-Chain reverse”
- “Threat Intel(ligence)”
- Security Operation Centers
- In-source virus/malware detection and handling
- Full monitoring of all data input/output
- OSINT, monitoring of malware sites
- Internal honey-traps, IDS etc., protect “golden nuggets”
- (P)en-test aaS



Mitre, 10 Steps to world-class COC

It takes huge human and financial resources to follow every incident back to the attacker. Privacy is collateral damage.

Retail::Challenges



"A 'Kill Chain' Analysis of the 2013 Target Data Breach," March 26, 2014; US Senate Committee on Commerce, Science, and Transportation

- 2015, practically all US retailers lost user data
- 2016, massive black-mailing with DDOS
- Public sites essential for business
- Low profit margins compared to other industries
- Many small companies
- DarkWeb sells DDOS 3 month for €5000.-

Retail::Solutions (???)

- DDOS: host site on google or amazon
- Data: spend much more money on security or
- Use PaaS in the Cloud

Sec = f($)

The situation in retail raises some fundamental questions: do we need state-intervention against DDOS attacks due to the fact, that neither owners nor producers of IoT and Smart Home devices care about those attacks?

Can we defend a typical intranet (Active Directory etc.) or web-site with small money?

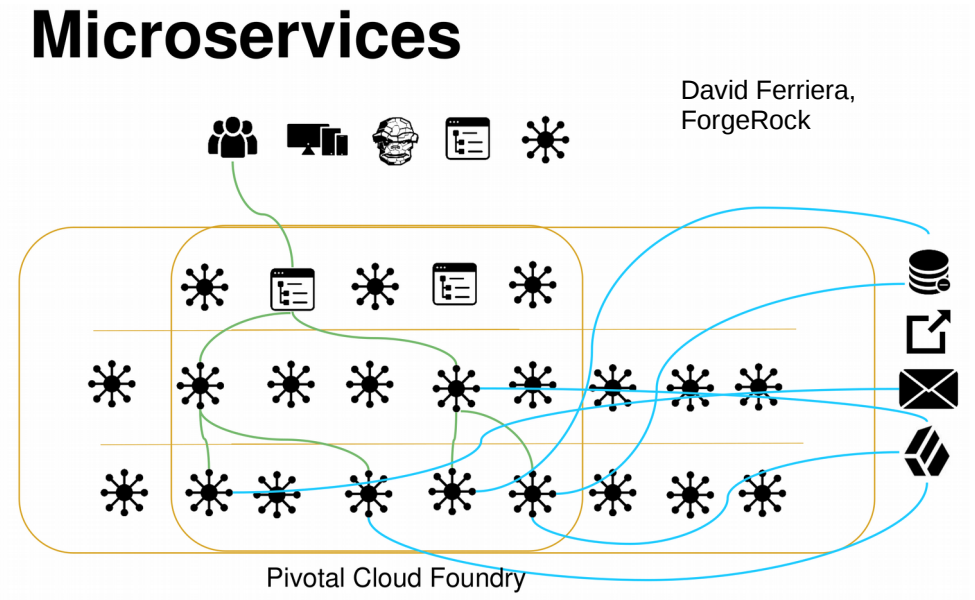
Does IT-Sec REALLY cost so much or is something seriously wrong in IT?

Digital Platforms::Challenges

- Winner-takes-all markets (network effects)
- Extreme Growth in a short time (Uber engineering: 200-2000 emp. In 1.5 years)
- Extreme request numbers and spikes
- Global data and services

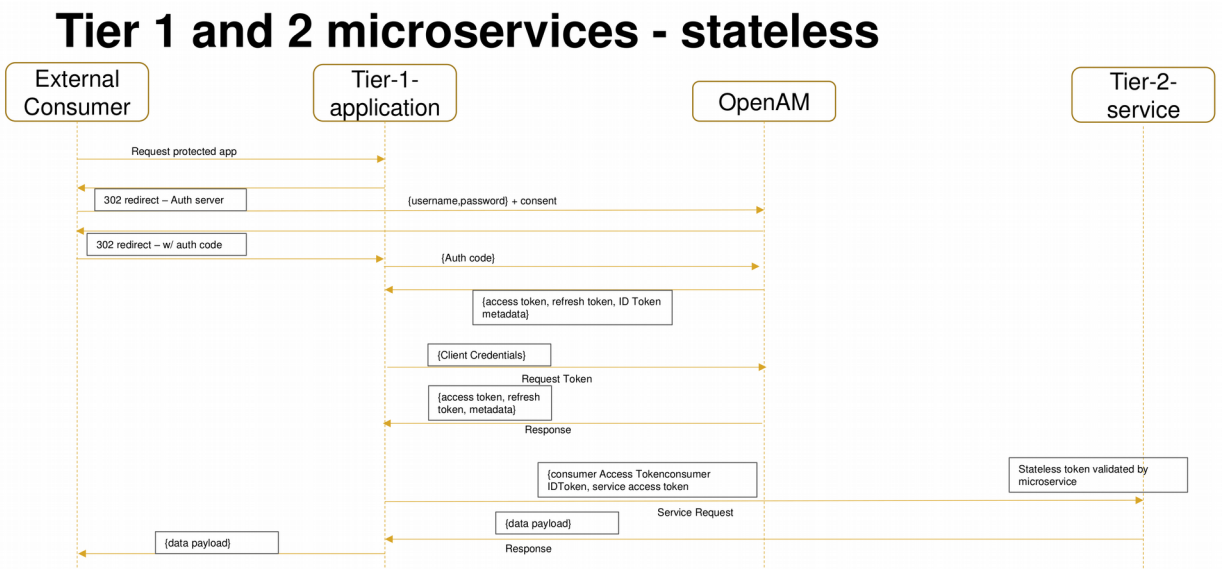
- Weak isolation in VMs (XEN) and (Docker) Containers, dynamic east/west traffic,
- IAGO attacks (malicious kernel/vm)
- Endpoint proliferation, dynamic job scheduling, SDNs
- Credential management and bearer tokens (RAM scraping)
- Secure Software Devel./Deploy (DevOps vs. Isolation, credential security)
- Cross-cutting concerns: transactions, security

Accenture Technology Vision 2016 survey]



Digital Platforms::Solutions

- Use SAAS for all office stuff
- Use P/IAAS for runtime
- Develop core software internally (Microservices)



From: David Ferriera, ForgeRock

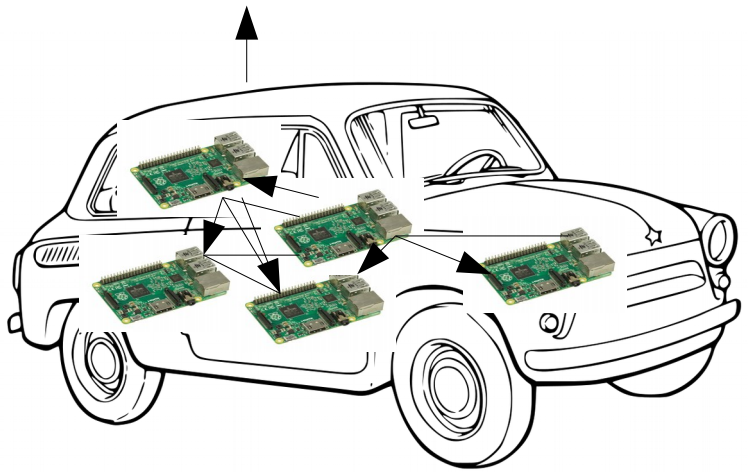
- Credential mgt. tools, HSM
- Pervasive , automatic monitoring (e.g. Dapper, ELK)
- Deep learning based IDS
- “repair, repave, rotate”
-
- Service isolation and segmentation, Unikernel approach, VMs
- Fine-grained backend security via secure delegation (like finance..)

There is a fundamental tension between defining and running jobs dynamically (including network re-configuration) and a static security configuration!

There is another fundamental tension between performance and security!

Products

Cars::Challenges

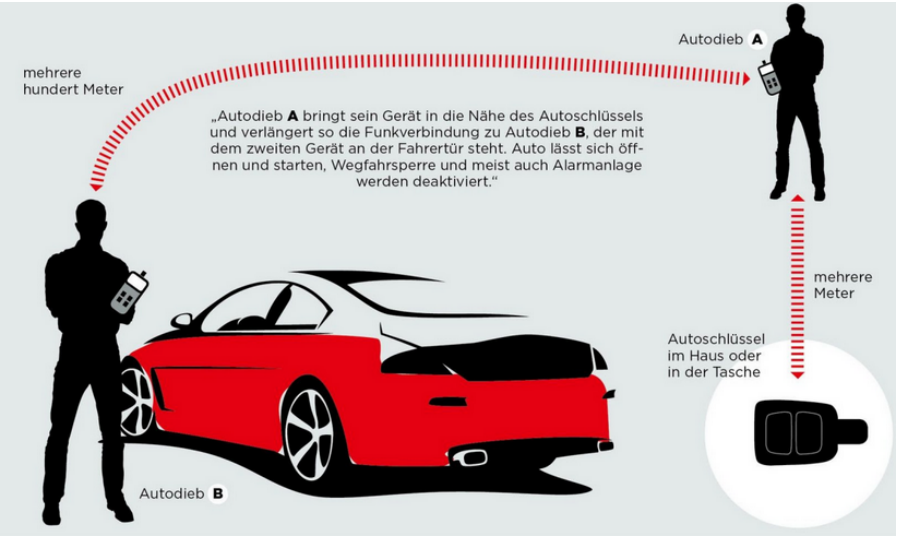


20-400 computers, wireless connectivity, several networks

- Suddenly open systems
- Cars are distributed computer systems with wheels
- Worldwide maintenance req.
- Change of parts req.
- Crypto-HW expensive at scale
- (CAN)Bus systems outdated
- Problematic programming languages used

Within 10 years cars changed from a closed system to an open, distributed environment. The global markets favor features over security. The situation mirrors the time when PCs with MS-Windows were connected to the Internet. But then we did not know many security problems of open systems. Now we do and the weak security of cars was done on purpose!

Keyless GO(NE)



Most security problems detected 5 years ago are still valid (tire pressure sensors, Man-in-the-Middle problems, unprotected interfaces, problematic ties between Entertainment systems and basic car control etc.
ADAC: cars from ALL makers show this problem! No reaction from Car-Industry.

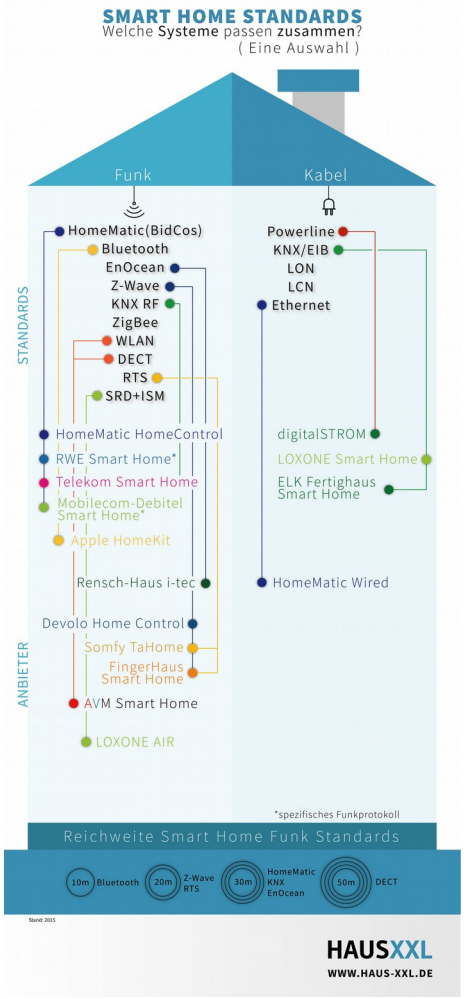
Cars::Solutions

- Respect Distributed Systems Knowledge
- Create affordable and secure CIA/crypto components and key mgt. solutions
- Create resilient and damage-reducing bus architectures (DOS detection, byzantine protocols)
- Use safe programming languages
- IDS?

Let us at least apply things which are known to WORK! The committee-driven style of the automotive industry might work in the long run.

Smart Home::Challenges

- Traditional IT-Sec does not fit (VLANs, update-logic, administration by specialists)
- Devices made by small companies with limited SW skills and budget
- Strong push to market, no incentive for secure solutions
- Bad usability
- Weak programming languages and systems used



Linux will no longer profit from being “a little bit better and not well known”!

Smart Home::Solutions

- Make memory and type safe languages with good performance and small footprint mandatory (Rust?)
- Learn to create extensible but secure gateways
- Connect “wimpy” devices securely
- Separate security updates from new features
- Make security updates automatic and mandatory
- Think about updates vs. send-in and a new definition of legal borders between sellers and buyers
- Randomize systems sold at scale
- Provide a secure base-SW for small companies (BSI?)
- Punish companies with unsafe defaults (The recent DDOS attacks from IoT/SH devices on digital platforms in the US might cause a change in politics.)

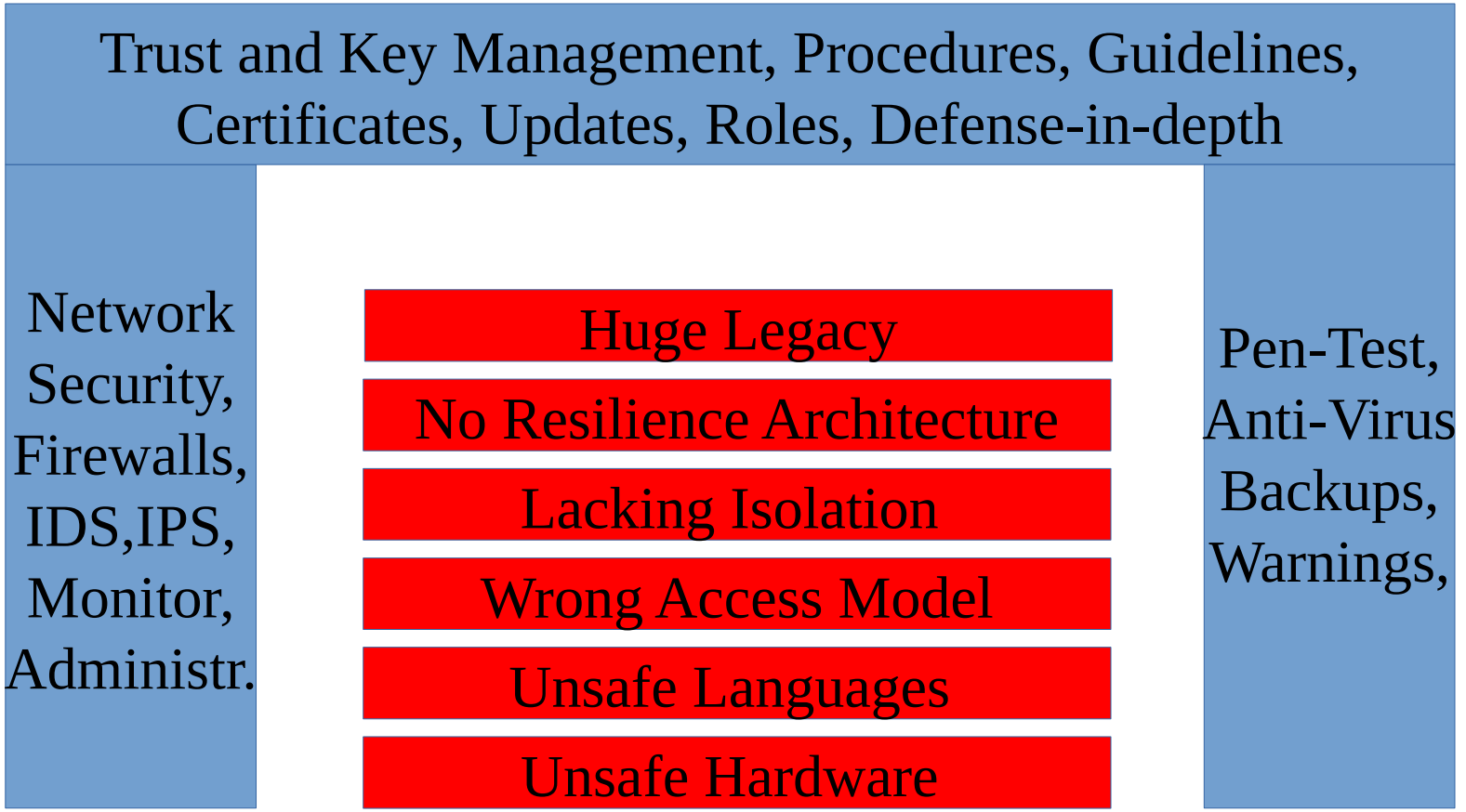
Don’t let us apply things which are known to NOT WORK!

A Summary

- We have reached the phase of “industrial hacking” (thanks to cyber warfare)
- Preventive measures in our intranets do not protect us anymore (but they still cost us dearly)
- Incident response is fun and costs even more (KMUs won’t be able to do this)
- Constant monitoring with big data is required (at the price of privacy)
- Pen-testing is NO SOLUTION, because it cannot achieve better security/safety (a lesson learned in 40 years of SW-development)
- Fixing the user does not work! (learning about social engineering is OK)
- “Security Fatigue” is getting more common among users
- Few people are interested in solving fundamental problems (most make too much money from the current situation)
- IT-Security costs can be considered a tax on top of everything

IT-Security: Problem or Solution?

How IT-Sec is currently used



This is an extremely expensive and at least in the case of regular users extremely useless approach.

There is something fundamentally wrong...

We have a serious computer security problem. Everything depends on everything else, and security vulnerabilities in anything affects the security of everything. We simply don't have the ability to maintain security in a world where we can't trust the hardware and software we use.

Bruce Schneier quoting Steve Bellovin.

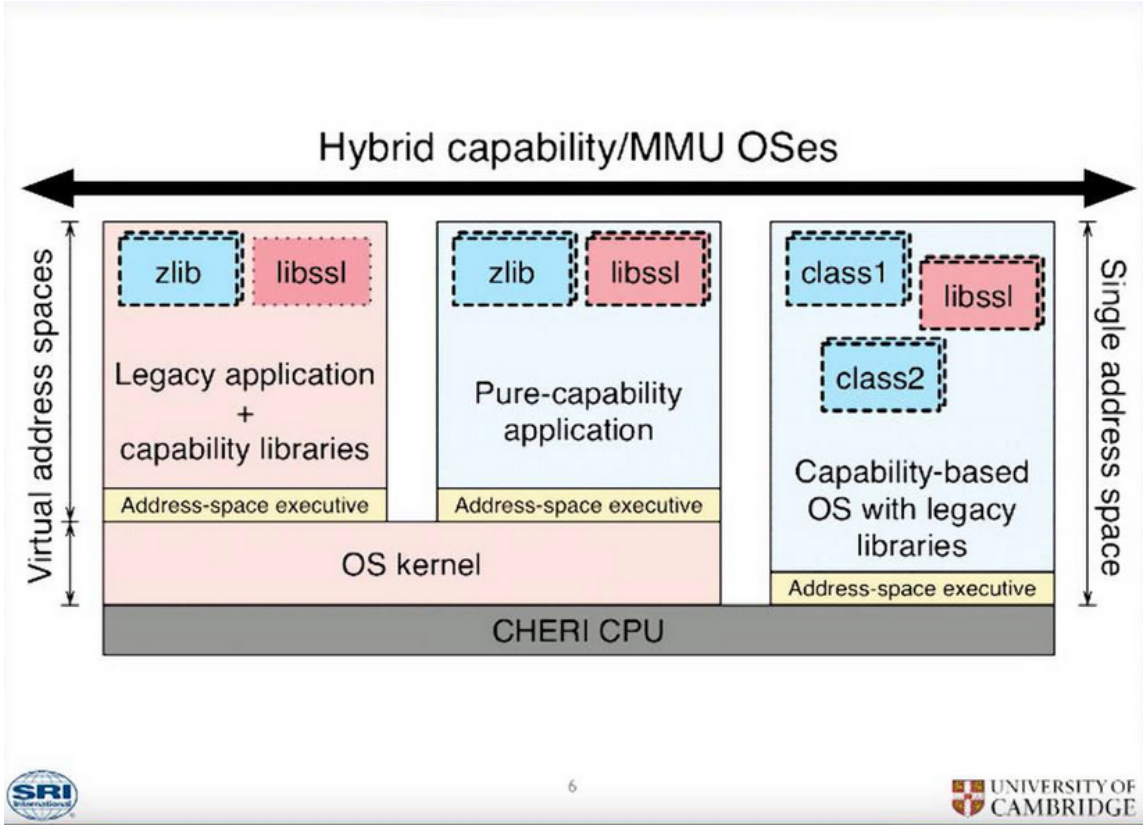
Safety vs. Security

- Do not confuse Security and Safety! Many problems are fundamentally safety problems which can also be exploited
- Hackers are the excuse for software companies to continue bad practices
- Industrialized hacking only makes the brittleness of our systems much more visible
- Stop using IT-Security for things which are not in its domain (like buffer overflows, malware etc.)
- Do not put bad technology into certificates and compliance laws (like anti-virus products)

The recent Amazon crash: does it make a difference if it was caused by hackers instead of an admin mistake?

Building Blocks for Secure Systems

Secure Hardware: Hybrid Capability Hardware



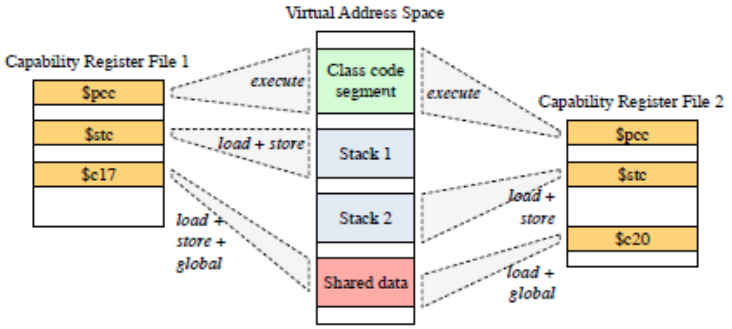


Fig. 8. Capability register files describe the rights of a user thread, and can be used to implement both isolation and controlled memory sharing.

CHERI provides protection of capabilities (both memory and object) even for C-based languages and legacy code.

Type- and Memory-safe Languages: Rust

```
fn tls1_process_heartbeat (s: Ssl) -> Result<(), isize> {
    const PADDING: usize = 16;

    let p = s.s3.rrec;
    let hbtype:u8 = p[0];
    let payload:usize = ((p[1] as usize) << 8) + p[2] as usize; (1)

    let mut buffer: Vec<u8> = Vec::with_capacity(1+2+payload+PADDING);
    buffer.push(TLS1_HB_RESPONSE);
    buffer.extend(p[1..1+2].iter().cloned());                    (2)
    buffer.extend(p[3..3+payload].iter().cloned());              (3)

    let mut rng = rand::thread_rng();                            (4)
    buffer.extend( (0..PADDING).map(|_|rng.gen::<u8>())
                        .collect::<Vec<u8>>() );

    if hbtype == TLS1_HB_REQUEST {
        let r = ssl3_write_bytes(s, TLS1_RT_HEARTBEAT, &*buffer);
        return r
    }
    Ok(())
}
```

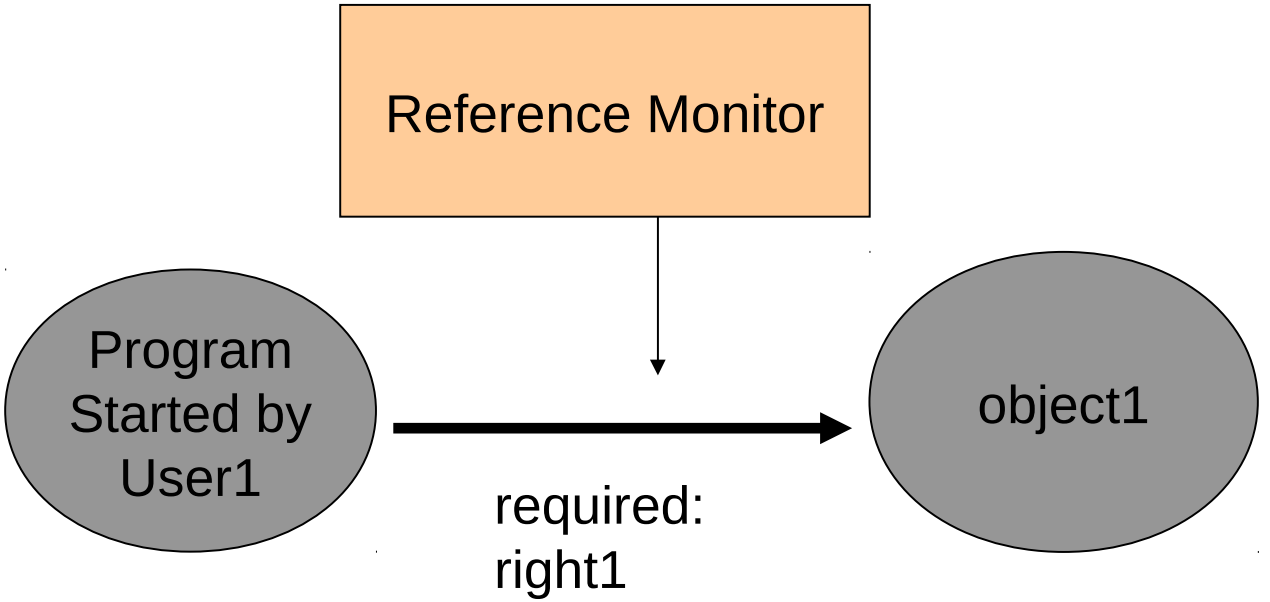
No use of uninitialized Values. No buffer-overread etc. Sharing mutable state across a concurrency boundary without a mutex is a compile-time error. No GC, no-cost abstraction. (Example: Jens Getreu). Ocaml is another option. Secure Ecma Script looks promising too, so does Elixir. Watch out for shared state multithreading!!

Object Caps against Ambient Authority

Access Control Matrix:

Static Rights	Object1	Object2
User1	Right1	Right2
User2	Right3	Right1

Uses all possible rights from User1



Access Control Point:

Safe APIs: Designation vs. Authority

Open (char* filename, int mode)

// application needs to transform the symbolic filename into a resource

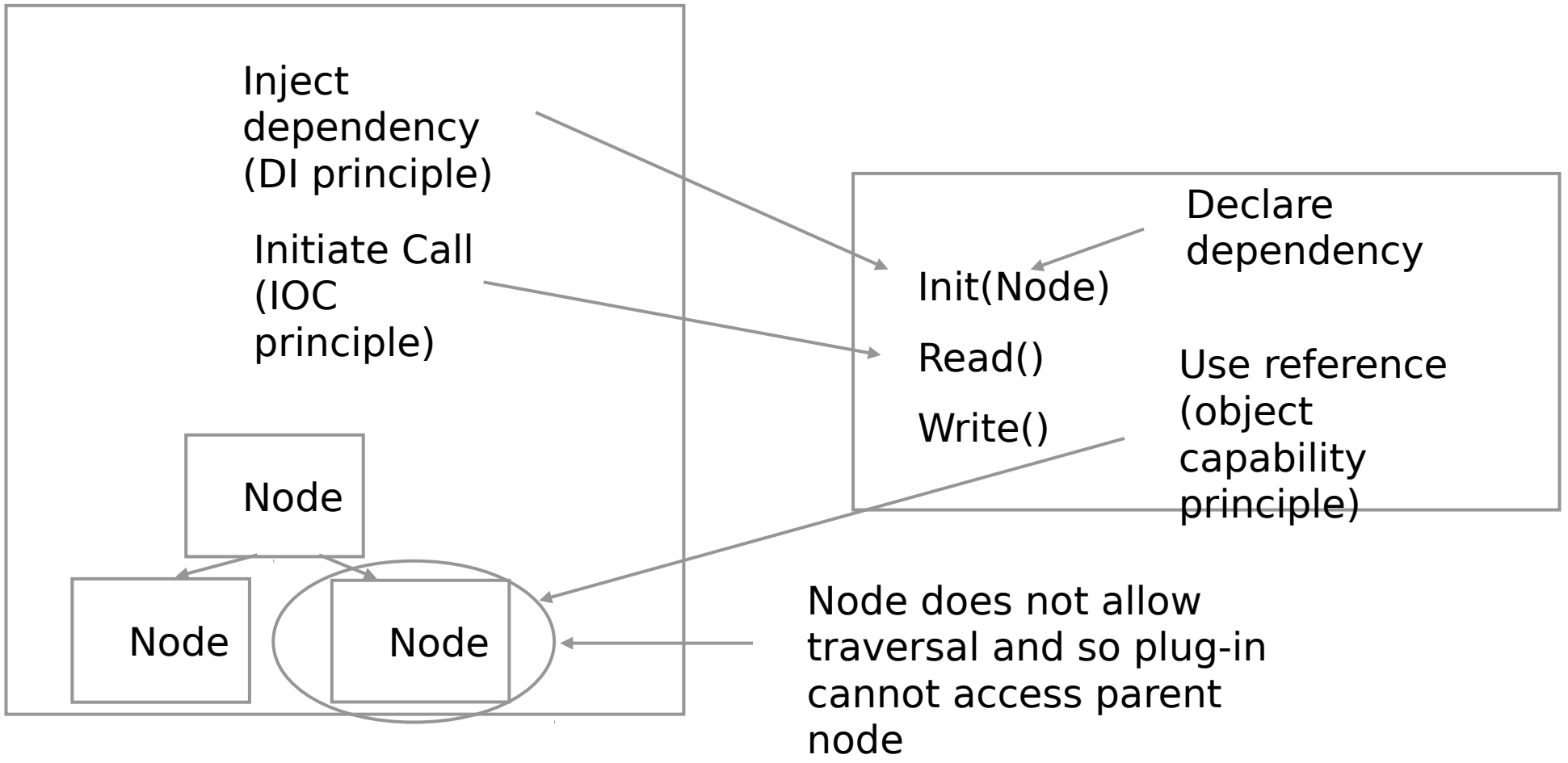
Open (Filedescriptor fd)

// application receives an open resource without the need to perform any rights-related operations

An API like this forces the transfer of all authority from the user to the application because it is unclear what file will be opened at runtime. This is even more dangerous, if the application is privileged. Wrong arguments checking can lead to privilege elevation. The second API does NOT require ambient authority!

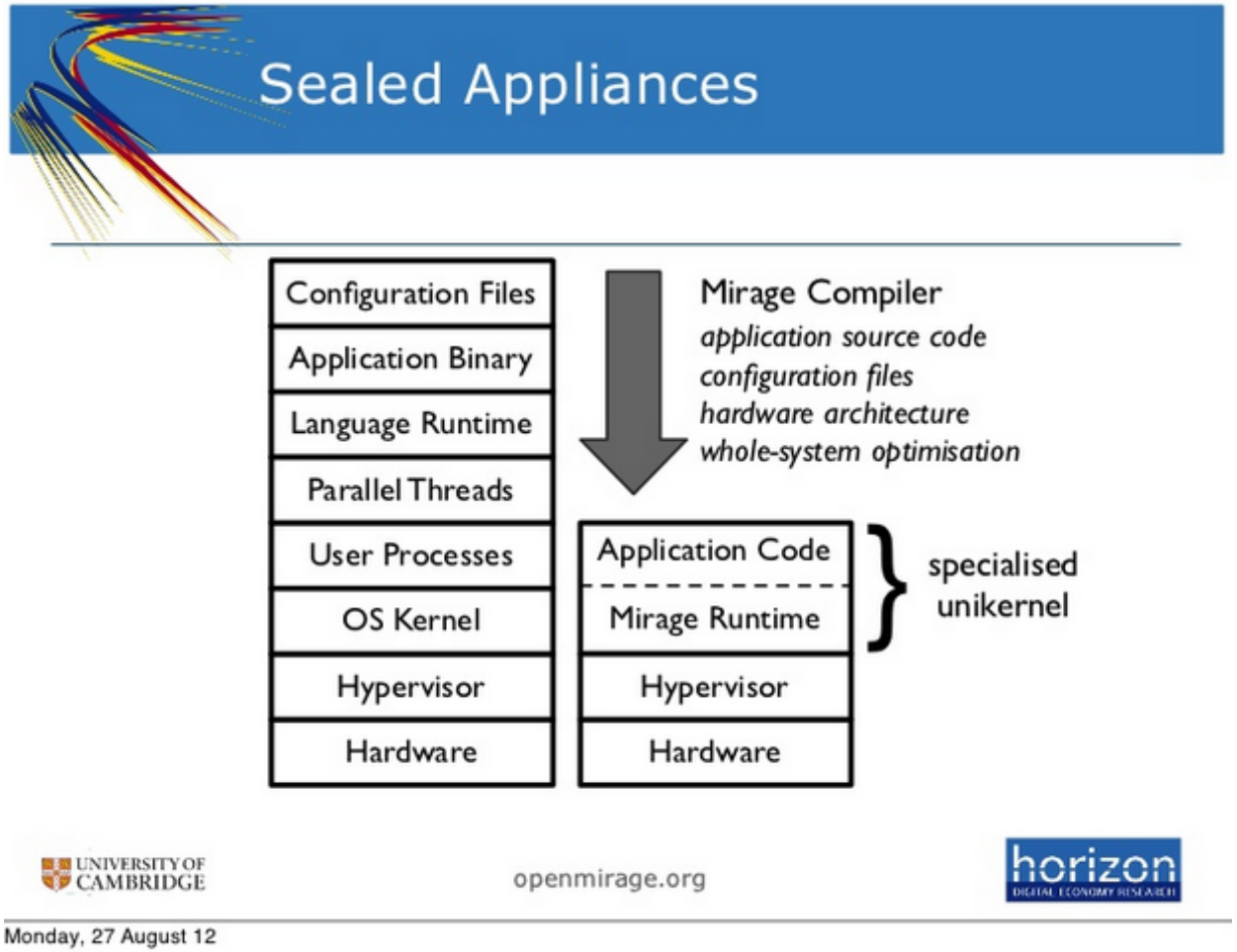
Compartments

Safe Extensions by Inversion of Control

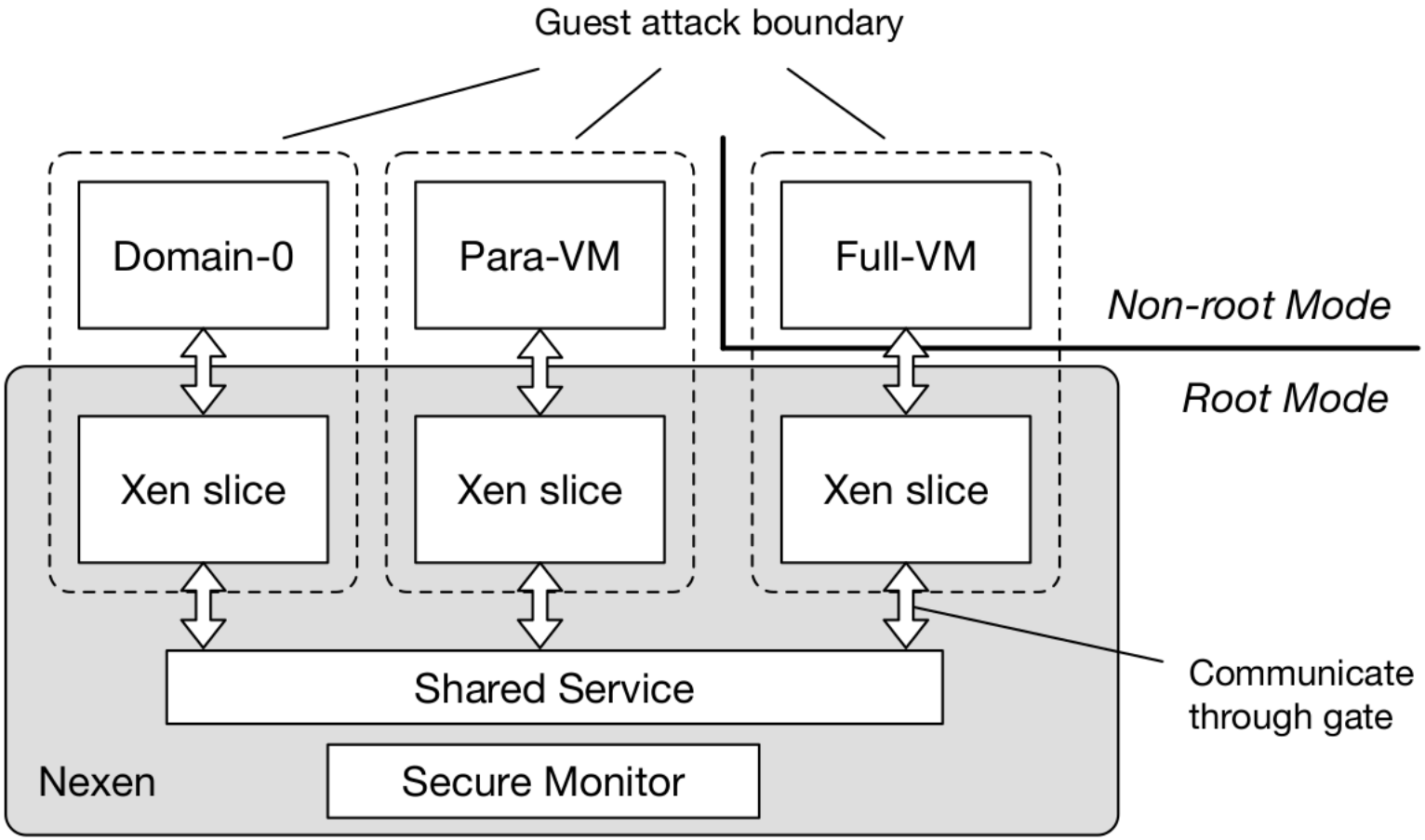


How do we make extensions safe? How do we achieve complicated business requirements like multi-tenant abilities? The answer is in Inversion-Of-Control architectures combined with strict control over references (no global crap for „flexibility“ reasons…) which effectively virtualizes the plug-in runtime environment

Compartmentization: Unikernels/Mirage OS



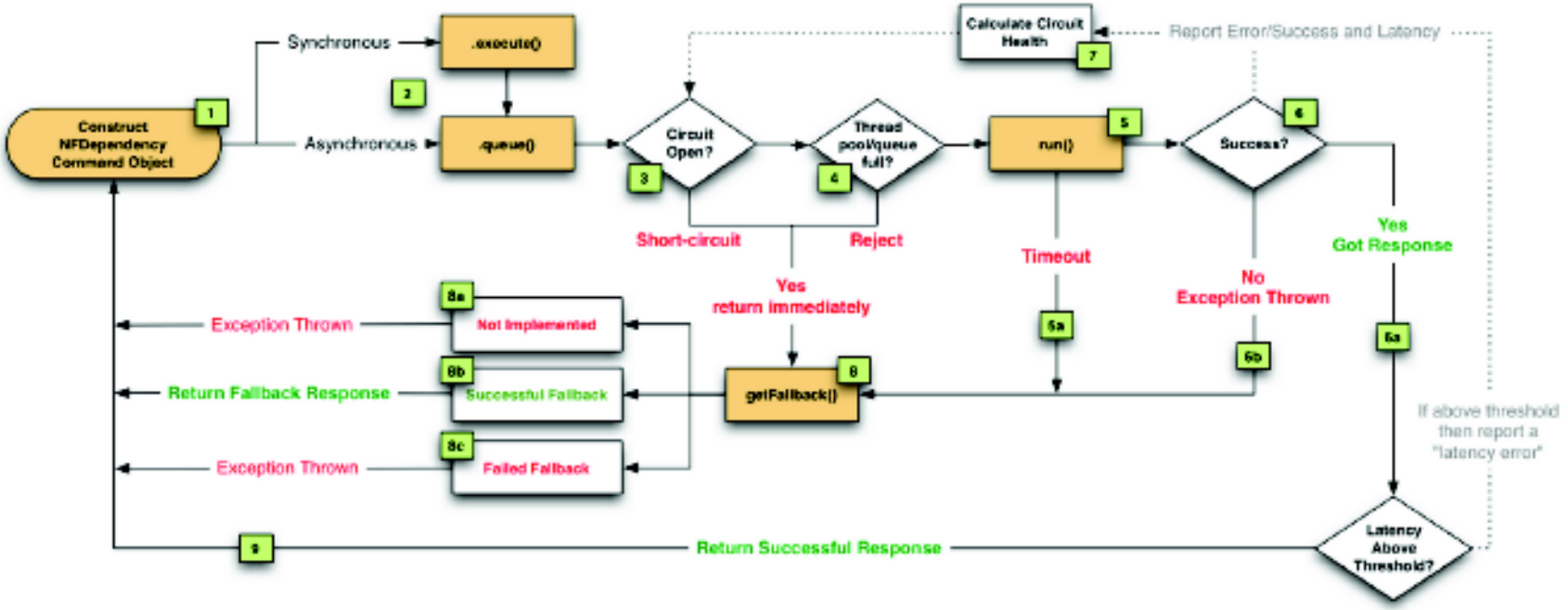
Deconstructed VM:Nexen



XEN, a 270kloc monolith running at full privilege level. Nexen does least-privilege separation on same level. See also Intel Guard technology and IAGO attacks.

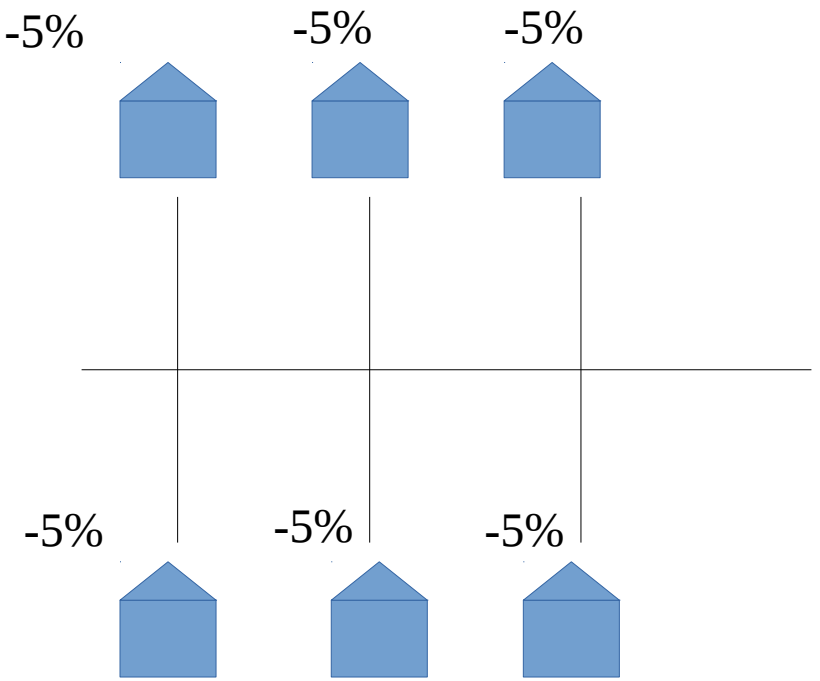
Safety by Architecture

Self-Regulated Fault-Tolerance



Source: A.Cockcroft, Netflix

Semi-autonomous Components



Limited adjustment. Controllable by distribution network without financial consequences

This pattern relies on semi-autonomous components which prevent remote control beyond a certain level. It is robust, as it prevents a remote access from turning off everything or causing huge level changes.

Technological modesty lessons from Ukraine’s power loss

The downtimes would have been much longer without additional MANUAL breaker switches

Do we need re-programmable interfaces (e.g. serial to ethernet) everywhere? They got flushed/destroyed.

What if the attackers had flushed/ re-programmed the SCADA systems?

Resources 1::General

- The rise of the digital customer, Rino Borini, Adnovum Notitia 29/2016, Zürich
- https://blog.mi.hdm-stuttgart.de/index.php/2016/09/08/secure-systems-2016-an-overview-walter-kriha/
- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller & Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction
- Cyber-Sicherheitsstrategie für Deutschland, Herausgegeben vom Bundesministerium des Innern

Resources 2::Incident Response

On SOCs, Threat Intelligence, Resilience Engineering:
https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907
https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf
https://attack.mitre.org/wiki/Main_Page
https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907
On the “decade of incident response” https://www.schneier.com/blog/archives/2014/11/the_future_of_i.html
Excellent attack szenarios: https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
SANS Critical Security Controls:
https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

Thread Intelligence:
https://www.heise.de/security/artikel/Threat-Intelligence-IT-Sicherheit-zum-Selbermachen-3453595.html

Resources 3::Software

- Kymberlee Price, 2016, Security Vulnerabilities in 3rd Party Code: FIX ALL THE THINGS
- Dustin Collins, Securing the Modern Software Delivery Lifecycle 02/16
- Justin Smith, Cloud Native Key Management, Pivotal, 10/16
- Justin Smith, 2016, Cloud Native Security: Rotate, Repair, Repave
- Ranga Rajagopalan, Rethinking Application Security With Microservices Architectures, Darkreading.com 2016
- David Ferriera, Director – Cloud Technology, Forgerock, An Authentication and Authorization Architecture for a Microservices World
- Ken Fromm, Serverless Security, https://read.acloud.guru/thinking-serverless-addressing-security-issues-a8490e73cbea

Resources 3::Software

- Kymberlee Price, 2016, Security Vulnerabilities in 3rd Party Code: FIX ALL THE THINGS
- Dustin Collins, Securing the Modern Software Delivery Lifecycle 02/16
- Justin Smith, Cloud Native Key Management, Pivotal, 10/16
- Justin Smith, 2016, Cloud Native Security: Rotate, Repair, Repave
- Ranga Rajagopalan, Rethinking Application Security With Microservices Architectures, Darkreading.com 2016
- Deconstructing Xen, Lei Shi et.al. Key Laboratory of Scalable Computing and Systems, Shanghai Jiao Tong University
- Iago Attacks: Why the System Call API is a Bad Untrusted RPC Interface, Stephen Checkoway, Hovav Shacham

Resources 4::Industries

- Antonia Böttinger, Andreas Gold, Keyless GO(NE)
- Olaf Carlson-Wee , Banking from the Future: Cryptocurrency Key Storage, Coinbase
- IoT Goes Nuclear: Creating a ZigBee Chain Reaction, Eyal Ronen(B), Colin OFlynny, Adi Shamir and Achi-Or Weingarten, PRELIMINARY DRAFT, VERSION 0.91 Weizmann Institute of Science, Rehovot, Israel
- https://www.heise.de/security/meldung/Finnland-DDoS-Attacke-auf-Heizungssteuerung-3459730.html

Supplemental Slides

Don’t fix the User!

Die Gefahr sei dabei, so Roger Strukhoff vom IKT-Forschungsinstitut Tau, dass wir zu viel regulieren. Nicht jedes Gerät müsse mit höchsten Sicherheitsmaßnahmen geschützt werden. Wichtiger sei, die Ressourcen sinnvoll einzusetzen. "Wie sich IT-Security lösen lässt, ist vielleicht zu 20 Prozent eine Frage der Technik. Der Rest sind Verhaltensweisen", sagte der Forscher. (Discussion at DatacenterDynamics Converged, CEBIT 2016)

> You can't have privacy without security, and I think we have glaring failures in computer security in problems that we've been working on for 40 years. You really should not live in fear of opening an attachment to a message. It ought to be confined; your computer ought to be able to handle it. And the fact that we have persisted for decades without solving these problems is partly because they're very difficult, but partly because there are lots of people who want you to be secure against everyone but them. And that includes all of the major computer manufacturers who, roughly speaking, want to manage your computer for you. The trouble is, I'm not sure of any practical alternative. Whitfield Diffie, quote taken from Bruce Schneiers cryptogram March 2015

For more depressing insights: Butler Lampson @SOSP15: Perspectives on Protection and Security.

IT-Security::The Dome

For decades, we have confused security with safety. And used IT-Security against safety deficits. And by doing so, we have allowed IT to hide behind attackers!

“Kritis”::Law on Critical Infrastructures

- Establishing “defense measures”
- Many optional requirements
- Mostly preventive, nothing with respect to incident response
- And absolutely no demands against the IT-Industry and its way of software and system production! (Zero liability)

This establishes the legal base for a “tax on the honest”, in other words: the security-industrial complex can now legally acquire significant parts of the GNP

Don’t fix the User!

Die Gefahr sei dabei, so Roger Strukhoff vom IKT-Forschungsinstitut Tau, dass wir zu viel regulieren. Nicht jedes Gerät müsse mit höchsten Sicherheitsmaßnahmen geschützt werden. Wichtiger sei, die Ressourcen sinnvoll einzusetzen. "Wie sich IT-Security lösen lässt, ist vielleicht zu 20 Prozent eine Frage der Technik. Der Rest sind Verhaltensweisen", sagte der Forscher. (Discussion at DatacenterDynamics Converged, CEBIT 2016)

> You can't have privacy without security, and I think we have glaring failures in computer security in problems that we've been working on for 40 years. You really should not live in fear of opening an attachment to a message. It ought to be confined; your computer ought to be able to handle it. And the fact that we have persisted for decades without solving these problems is partly because they're very difficult, but partly because there are lots of people who want you to be secure against everyone but them. And that includes all of the major computer manufacturers who, roughly speaking, want to manage your computer for you. The trouble is, I'm not sure of any practical alternative. Whitfield Diffie, quote taken from Bruce Schneiers cryptogram March 2015

For more depressing insights: Butler Lampson @SOSP15: Perspectives on Protection and Security.

Things Learned

- We can’t protect Intranets and its keys
- Only crypto can help: Multi-party compute/smart contracts
- Need to weigh ops against sec ans your risk tolerance
- Decentralization is key (autonomous, self-healing)