

Patterns and Anti-Patterns of Secure Systems

Back to the Roots!

Prof. Walter Kriha

Computer Science and Media
Faculty, HDM Stuttgart

kriha@hdm-stuttgart.de

April 5, 2016

!!! IMPORTANT INFORMATION !!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

More information about the RSA and AES can be found here:

<http://en.wikipedia.org/wiki/ElGamal Encryption System>

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

"Die Sicherheitslücke wird erst geschlossen sein, wenn die Verantwortlichen im Gefängnis sitzen." Carsten Meywirth, Head of Cyber Crime Dep., BKA. Talk at CEBIT 2016

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.

To receive your private key, follow one of the links:

1. <http://6dbxggam4crv6rr6.tor2web.org/>

2. <http://6dbxggam4crv6rr6.onion.to/DF7>

3. <http://6dbxggam4crv6rr6.onion.cab/DF>

4. <http://6dbxggam4crv6rr6.onion.link/DF>

Well, Mr. Meywirth, you've got yourself a little problem at hand here...

If all of this addresses are not available, follow these steps:

1. Download and install Tor browser: <https://www.torproject.org/download/download-easy.html>

2. After a successful installation, run the browser and wait for initialization.

3. Type in the address bar: 6dbxggam4crv6rr6.onion.to/DF7

4. Follow the instructions on the site.

Image: <http://www.heise.de/security/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html>

!!! Your personal identification ID: 

Who IS responsible ?????

- The hackers, educated by states for the „cyber war“?
- The regular companies for spreading malware through advertising?
- The politicians who want even more backdoors and block liability?
- The software companies using outdated operating systems and architectures?
- The software developers which use inferior computer languages prone for malware attacks?
- The IT-Security „experts“ for not protecting us?
- The user, too dumb for IT?

Image: <http://www.heise.de/ct/news/2013/01/01/Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html>

And the Answer is: 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.

„Verhaltensweisen“ in Case of Locky, Petya et.al.

- Use backups frequently, automatically. But don't overwrite good files with damaged ones.
- Don't use directly attached drives or remotes or at least attach them only for a short time. Use ftp etc.
- Don't rely on time machine on MACs: code to destroy your versions has been found in malware (KeRanger)
- If you are a company: use Windows advanced access guidelines and tie your system down completely
- Try to prevent the removal of shadow copies – should ask you actually before, but Locky can prevent this
- Hope for an old version of the trojan. If so, get acquainted with de-cryption, keys, headers of files etc.
- Don't visit questionable sites like The New York Times, the BBC, MSN, and AOL. They spread malware through ads
- Don't reboot after phase 1 of Petya: remove disk and save the data.
- Learn to buy Bitcoins and use Tor....



2016: No Secure Nothing

No privacy (data loss, thanks to companies, states, criminals),
No safe routers, home equipment etc.
No safe cars (high-jacking, theft, MIM-attacks, privacy),
No safe mobile or desktop computation (blackmail)
No safe infrastructure (electricity, grids)
No safe services (identity theft, communication chan. etc.)
No safe production (SCADA, dinosaurs,

=> Let's take a look at several branches and how they stumble into the future.

=> Then we will take a look at IT-Security and its role

=> And finally, we will define building blocks for resilient and secure systems.



Stumbling into the Future....

From PC to the Web: A role model?

Internet Services

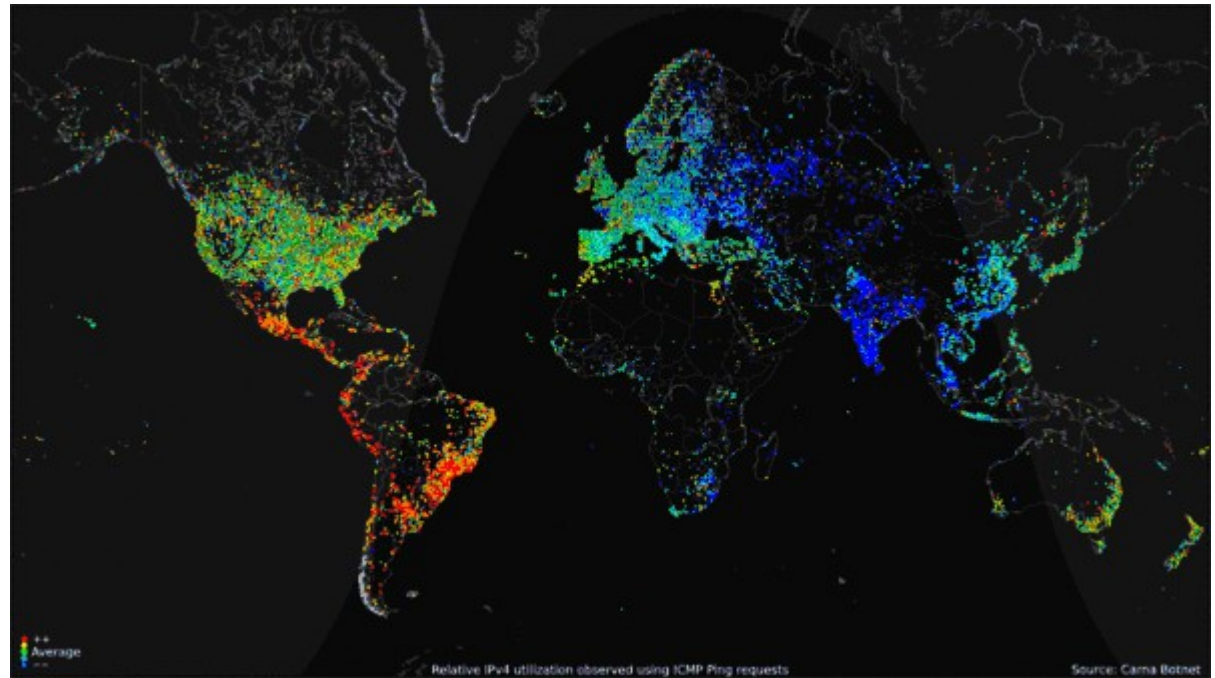
Smart Cars

IoT and Smart Homes

Production and Industry 4.0

Critical Infrastructures

From PC to the (mobile) Web: A role model?



"Internet Census 2012: Port scanning /0 using insecure embedded devices", Carna Botnet, 2012

Regular people started to use computers and the internet. Systems had no notion of security, users, transport, fault-tolerance or attacks.

Early Software Anti-Patterns

- A fast programming language is more important than type and memory safety
- Buffer-overflows are caused by dumb developers and will disappear over time
- Frequent updates fix software quality problems
- Mobile systems can be built like desktops
- New Features dominate safety and security economically

Early Security Anti-Patterns

- Authentication is the first miracle-cure of security
- Updates are the second miracle-cure of security
- Firewalls tame sudden connectivity
- Software is not affected by changes in location, connectivity or user types (see mobile disaster)
- Always start with very weak protocols with respect to integrity and confidentiality
- Trust establishment can be outsourced to commercial Certificate Authorities
- „Real“ security needs expensive admin personel („Richtlinien“)
- Hackers are far and few and do it for fun

Based on those patterns, we started to build worldwide business services, infrastructures, the IoT and much more....

Internet Business and Services



Credits: M.Mozart

2016: The „year of the lost data“. Almost every retail store had major losses of credit card information. The US Government did not want to stay apart and lost critical employee information...

Data Security Anti-Patterns

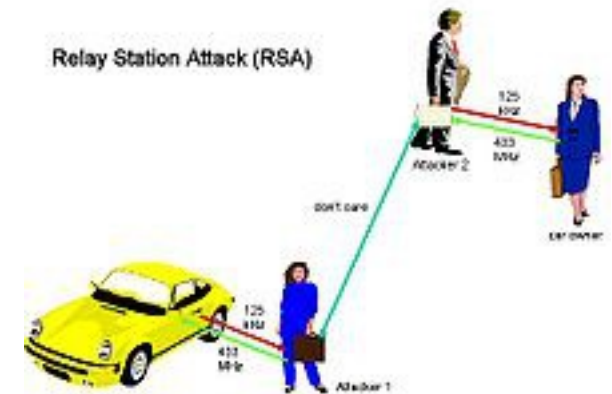
- Traditional client-server computing works in principle
- A media strategy is more important than a security strategy (home depot was fined \$19 Mio)
- Every break needs to be seen as an exception, not the rule.
- Pushing the risks closer to customers is beneficial (pins etc.)
- Blame the users: look what they are doing on Facebook!
- The bad guys are on the outside

Ein neues Bewusstsein für IT-Sicherheit muss also her. Auch im privaten Umfeld: "Auf der einen Seite beschweren wir uns über die NSA", so DFS-Experte Broecker. "Auf der anderen Seite veröffentlichen wir private Daten bei Facebook oder kaufen Spielzeug, das in die Cloud funkt."
CEBIT 2016

Cars: from „closed shop“ to „open house“ in 8y.



http://www.mitsubishicars.com/MMNA/jsp/outlandersport/12/index.do?flash=gallery#/?page=interior_gallery



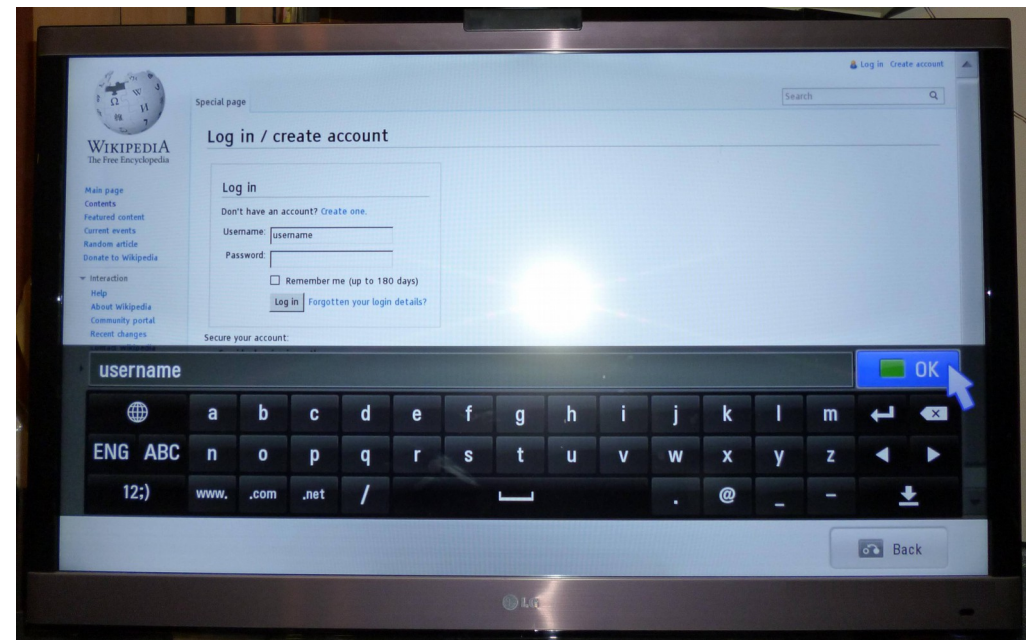
<http://en.wikipedia.org/wiki/User:Techie2>

Cars used to be static and closed environments. Today, they allow download, connect media-systems to infrastructure buses, update assisted driving over-the-air, open doors and start with a mobile device, check tire pressures wireless and so on...

Car Security Anti-Patterns

- Cars are different and well-known attacks like MIM or malware do not apply.
- It is no problem to connect C-based embedded software to the Internet
- Unique parts communicating over wireless channels need neither integrity nor privacy protection (sensors)
- One bus-system is better than two (read: cheaper..)
- The industry needs to follow success patterns from mobile and desktop computing, e.g. with respect to development speed, languages used etc. The car production process now includes customer time.

IoT and Smart Home Security



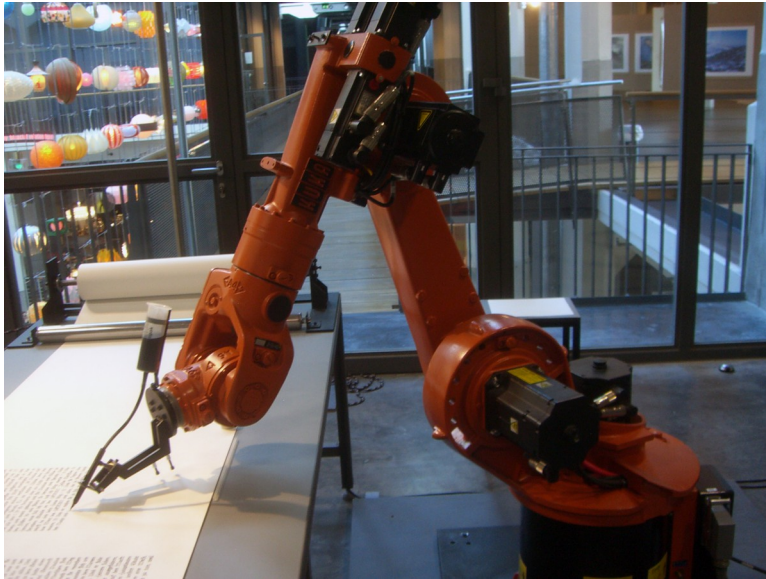
IP-cams open to the public, smart TVs sending user data (audio and video) into the cloud. Vulnerable smart-meters and routers. Un-usable peering procedures for guest-devices.

IoT and Smart Home Anti-Patterns learned

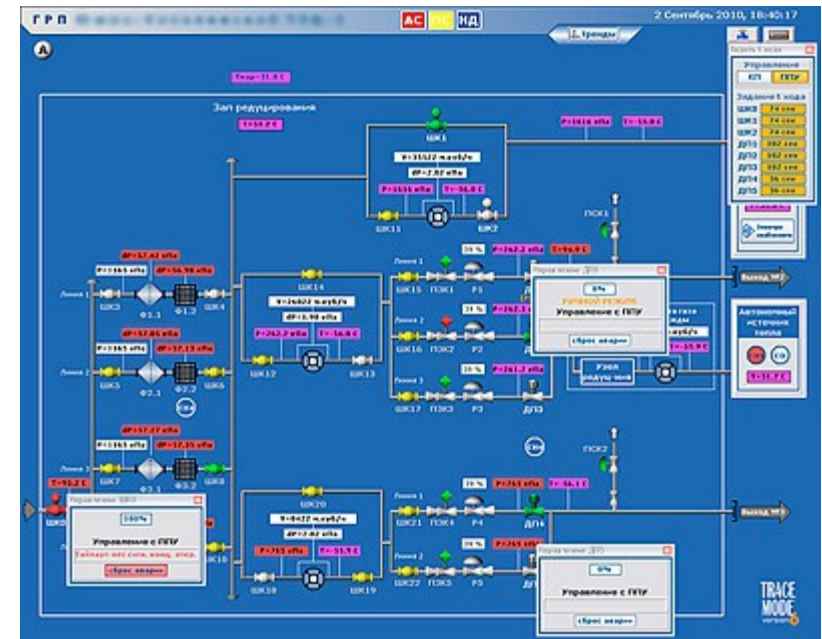
- There is somebody with advanced security administration know-how at home.
- Upload of user data into the cloud is no problem
- Open devices on the internet are OK
- Default and few hard-coded keys are all that is needed in embedded control
- Heterogeneous devices in a home create no security problem
- Calling home is OK
- Features first

The „lost user syndrome“ from the PC-area is now replicated endlessly across embedded devices

Production and Industry 4.0



Source: M.T.Schäfer



„Stark vereinfacht könnte man sagen, dass Industrie 4.0 eine IP-Adresse für jedes noch so kleine Element in der Fertigungsstraße, bis hinunter zu 24 Volt Stromversorgung auf der Hutschiene, nach sich zieht. Die Unternehmen der Automobilindustrie mit mehr als 500 Mitarbeitern gelten als Industrie 4.0-Pioniere“. Martin Schindler, CEBIT 2016

Production today shows aging, non-maintainable systems connected to the Internet. Systems which cannot be protected with traditional methods (e.g. because losing a byte make the robot stop). Networks are not separated.

Production and Industry 4.0 Anti-Patterns

- Office IT-Security is a good role model
- Traditional IT-Security advice is useful in production too
- Use flexible and re-programmable devices everywhere

The difference to the previous cases lies in the possible loss of life and reputation!

Critical Infrastructures

© National Nuclear Security Administration



Such infrastructures are e.g. energy grids, water supplies, health centers, financial systems etc. Like production environments, they show a much larger potential for damages and catastrophic events. Is the non-nuclear zone of a nuclear power plant less critical?

CI Anti-Patterns

- CI-Systems can use regular IT and IT-Security methods and technologies
- CI-Systems benefit from remote control options in IT
- CI-Systems can separate control and material flow without problems
- Risk assessment is the same as in other branches

The truth is, that many concepts from office-oriented IT-Sec do not apply here. Attackers are less important than the consequences of failures. Individual failure of components cannot compromise the whole system. Damage reduction is the goal, not prevention. Security is in the architecture, not the components alone!



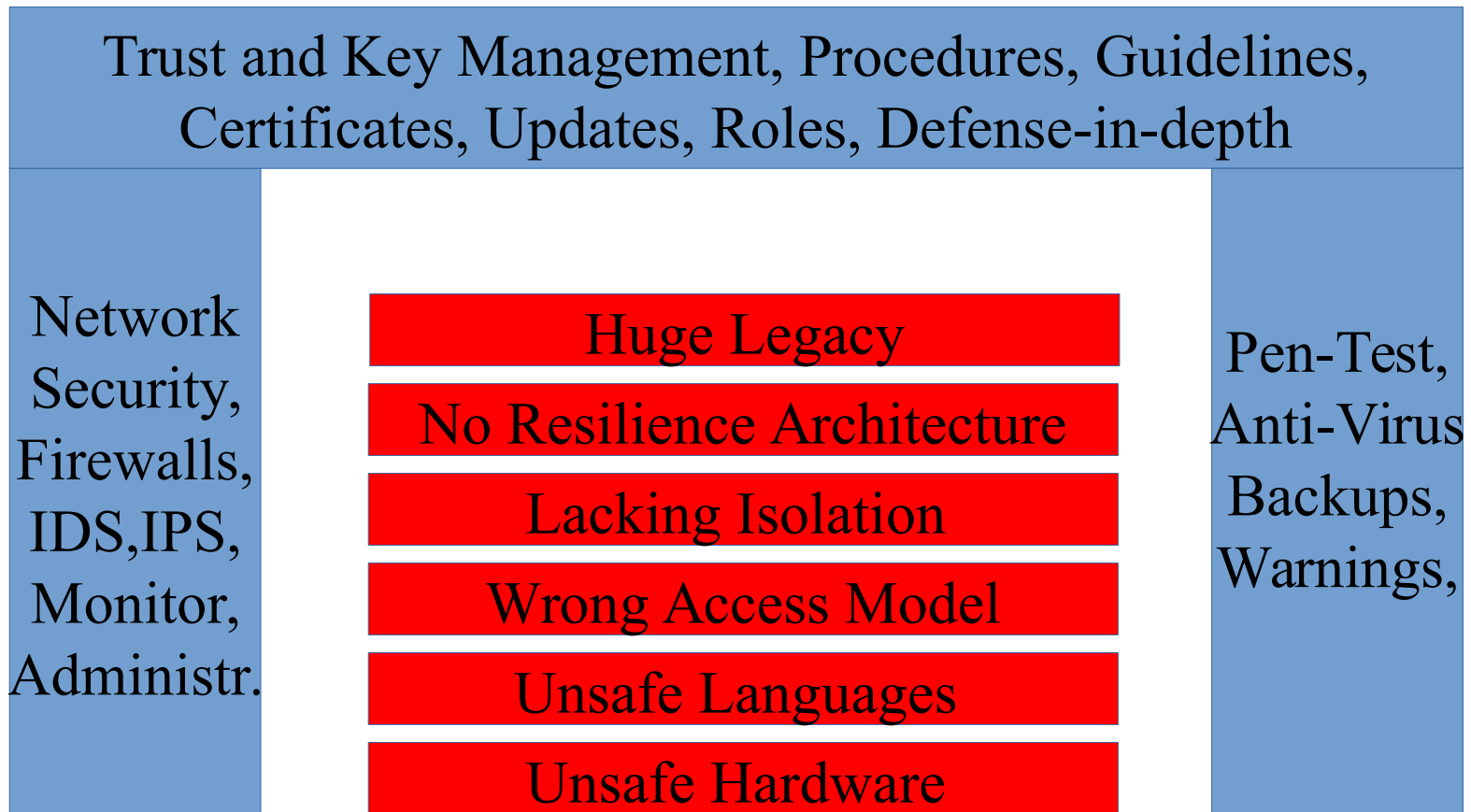
What went wrong?

The Crisis of IT-Security

How to protect a dog-pile of hardware/software technology?

Part of the solution or part of the problem? The Security-Industrial Complex

How to protect a dog-pile of technology?



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

Solution or Part of the Problem?

- IT-Security measures keeps weak software technology alive (e.g. virus checking)
- States start putting security measures in laws („kritis“), thereby creating enormous costs and opportunities
- The IT-Security community benefits financially from weak software

„Cyber war“, terrorism and regular malware have created a security-industrial complex where public, private and criminal elements mix. (see HBGary)

There is something fundamentally wrong...


For more than 50 years, all computer security has been based on the separation between the trusted portion and the untrusted portion of the system. Once it was "kernel" (or "supervisor") versus "user" mode, on a single computer. The Orange Book recognized that the concept had to be broader, since there were all sorts of files executed or relied on by privileged portions of the system. Their newer, larger category was dubbed the "Trusted Computing Base" (TCB). When networking came along, we adopted firewalls; the TCB still existed on single computers, but we trusted "inside" computers and networks more than external ones.

There was a danger sign there, though few people recognized it: our networked systems depended on other systems for critical files....

The National Academies report Trust in Cyberspace recognized that the old TCB concept no longer made sense. (Disclaimer: I was on the committee.) Too many threats, such as Word macro viruses, lived purely at user level. Obviously, one could have arbitrarily classified word processors, spreadsheets, etc., as part of the TCB, but that would have been worse than useless; these things were too large and had no need for privileges. In the 15+ years since then, no satisfactory replacement for the TCB model has been proposed.

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.



Damage Reducing (Resilient) Systems

Building Blocks for Secure Systems

- Secure Hardware
- Type- and Memory-safe Languages
- Secure Delegation with (Object) Capabilities
- Compartmentization
- Robust Architectures



Hardware

Secure Hardware

- Absolutely no backdoors
- Support for Compartmentalization
- Open Source Hardware?

CHERI: Hybrid Capability Hardware

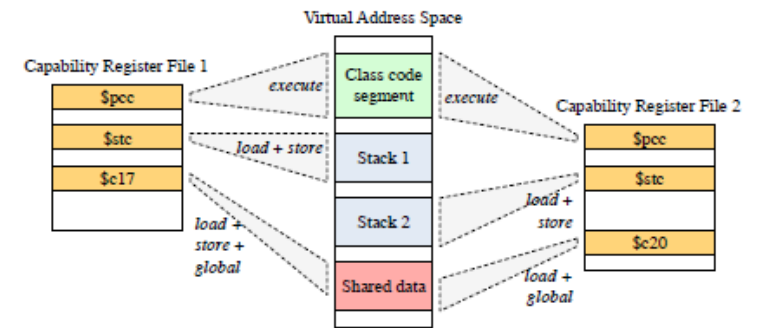
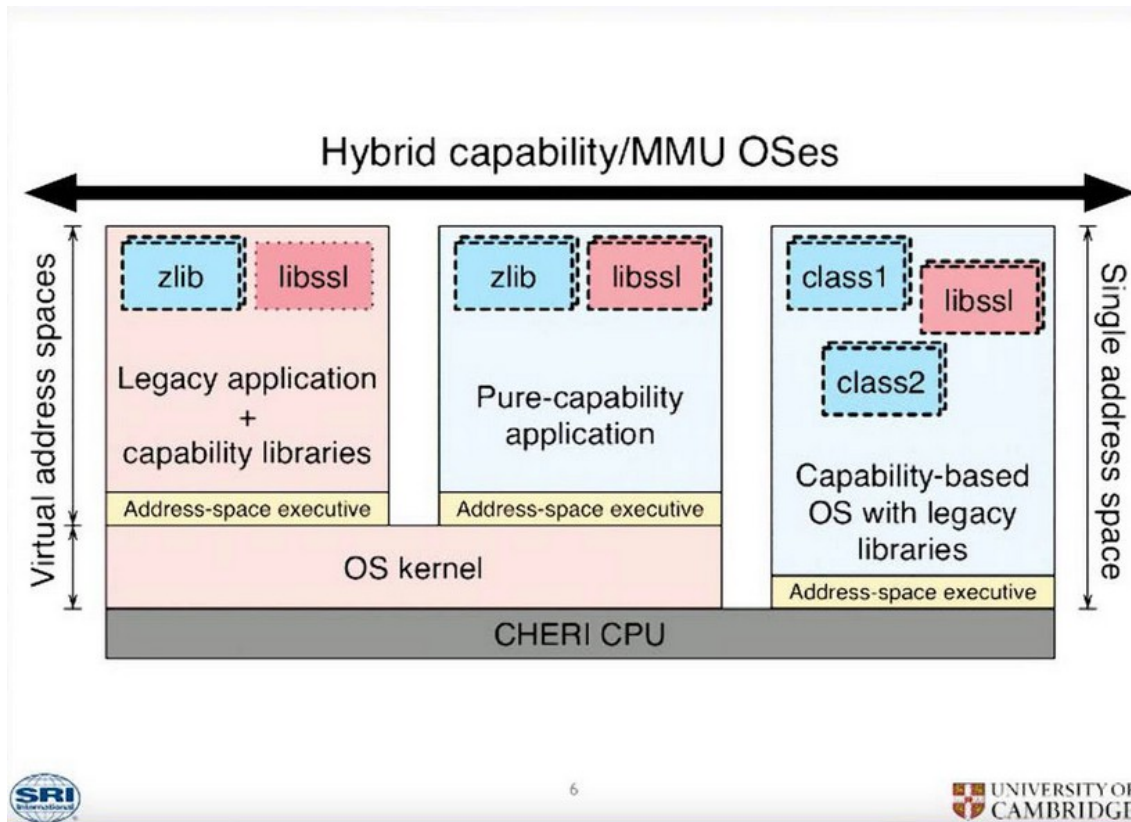


Fig. 8. Capability register files describe the rights of a user thread, and can be used to implement both isolation and controlled memory sharing.

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

Buffer/Integer Overflows, Memory Corruption

```
Exception: STATUS_ACCESS_VIOLATION at eip=61616161
eax=00000012 ebx=00000004 ecx=610E3038 edx=00000000 esi=004010AE
edi=610E21A0
ebp=61616161 esp=0022EF08
program=D:\kriha\security\bufferoverflow\over.exe, pid 720, thread main
cs=001B ds=0023 es=0023 fs=003B gs=0000 ss=0023
Stack trace:
Frame  Function  Args
 90087 [main] over 720 handle_exceptions: Exception:
STATUS_ACCESS_VIOLATION
104452 [main] over 720 handle_exceptions: Error while dumping state
(probably corrupted stack)
```

A program crash is a way into the system! But the real quality problem is much deeper: Stick a finger in some code and figure out what you can do from there. **What functions can you reach from any point in code? Who's failure is that?**

Still responsible for the most critical attacks!

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; ❶

    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()); ❷
    buffer.extend(p[3..3+payload].iter().cloned()); ❸

    let mut rng = rand::thread_rng(); ❹
    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!



Secure Delegation of Authority

Object Capabilities

- Root Causes: ACLs
- OCAP Principles
- Use Case: IoC Confinement

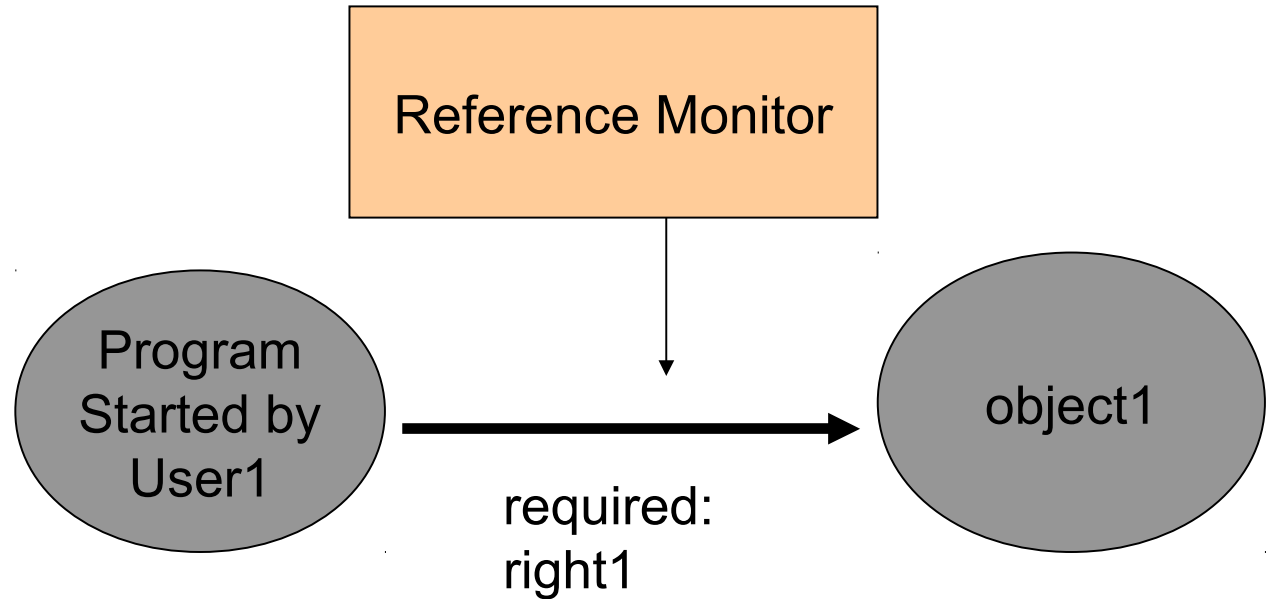
Root Causes: Ambient Authority Everywhere!

Access Control Matrix:

	Object1	Object2
Static Rights	User1	Right2
	Right1	
	User2	Right3
		Right1

Uses all possible rights from User1

Access Control Point:



Root Causes: Designation vs. Authority

Open (char* filename, int mode)

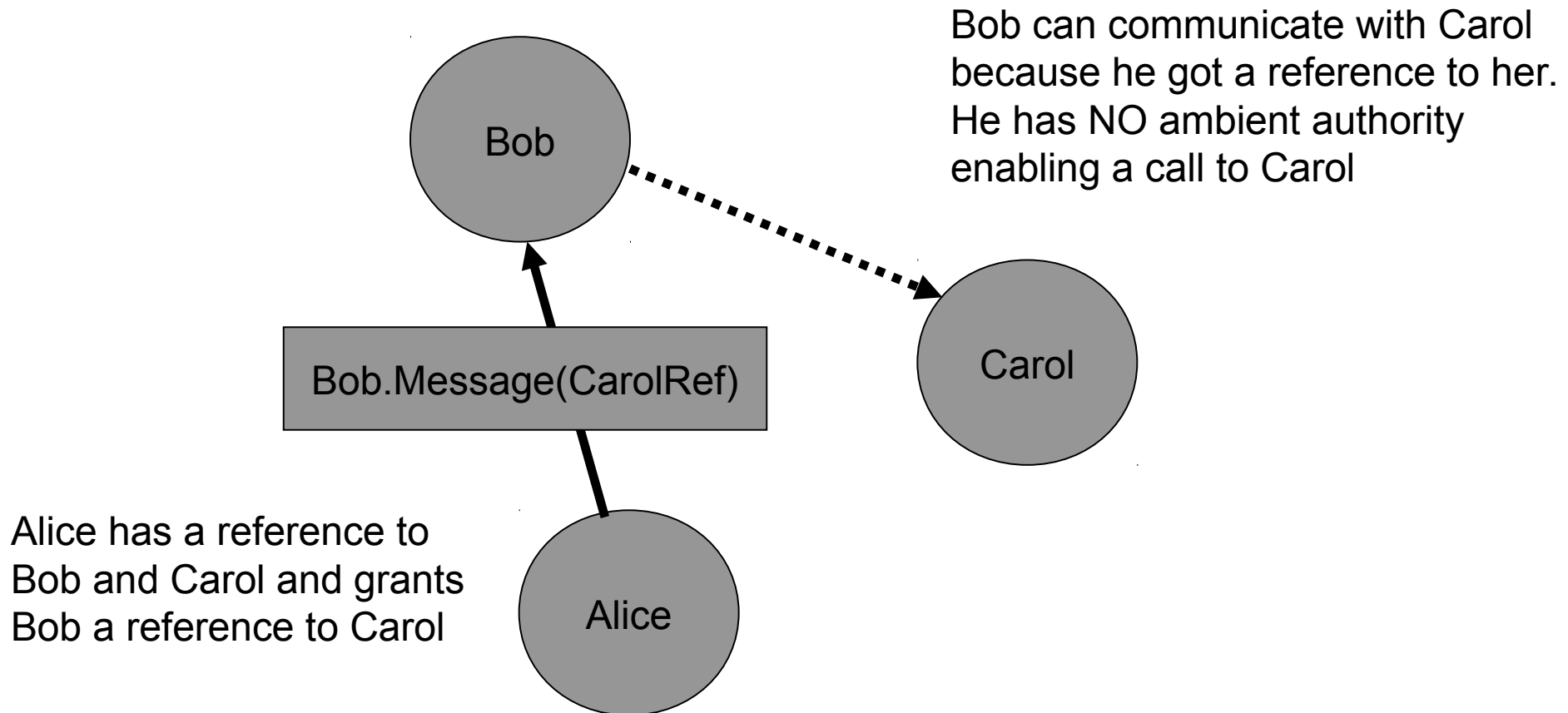
// application needs to transform the symbolic filename into a resource

Open (Filedescriptor fd)

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

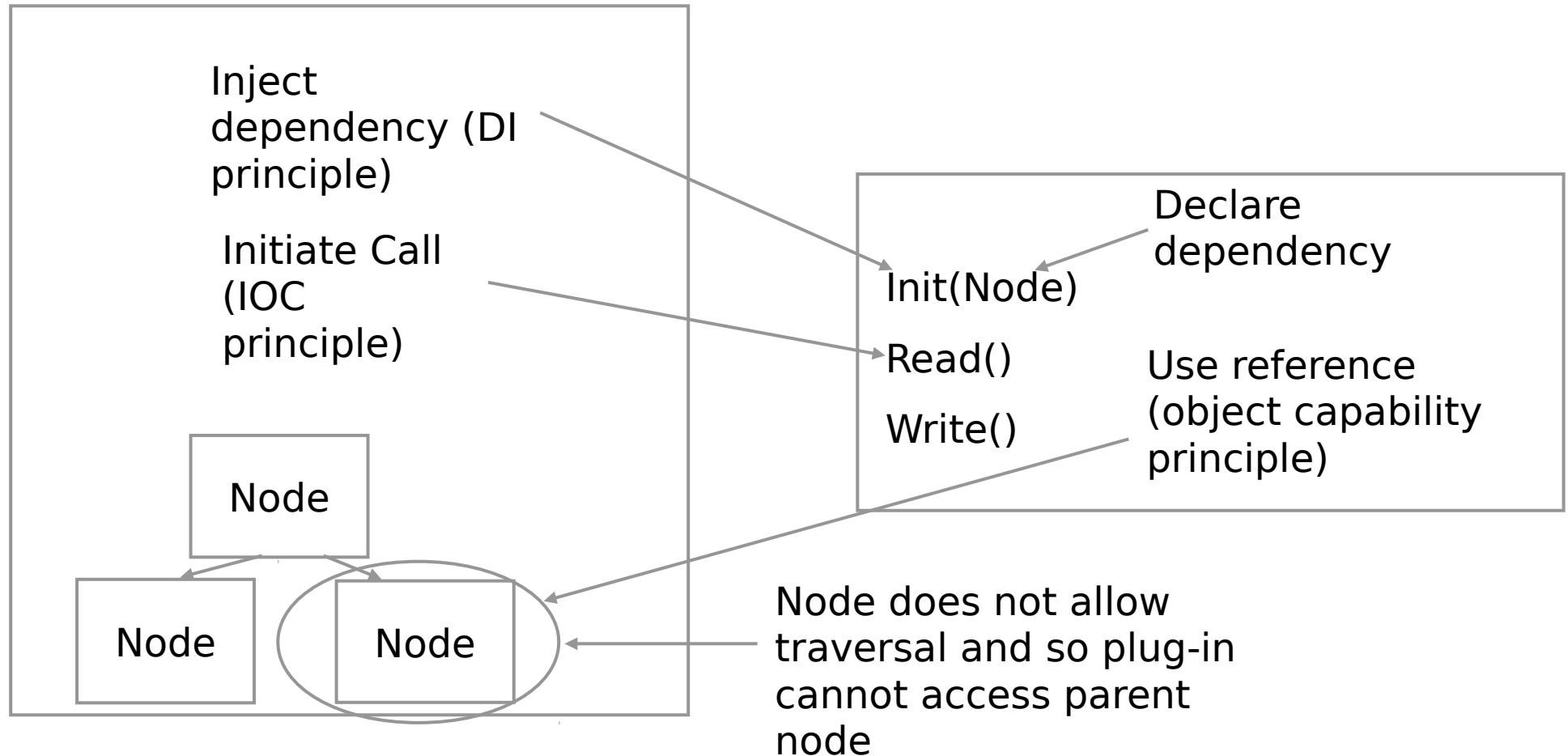
An API like this forces the transfer of all authority from the user to the application because it is unclear what file will be opened at runtime. This is even more dangerous, if the application is privileged. Wrong arguments checking can lead to privilege elevation. The second API does NOT require ambient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

Solutions: Object Capabilities



Object Capabilities reduce authority in a system: no access without a reference. And references combine access right and access method (designation and authority). They are a superior way to CONSTRAIN effects and are easier to analyze than external permissions. The diagram is called „Granovetter-Diagram“ after the well known sociologist Granovetter).

Solution: 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

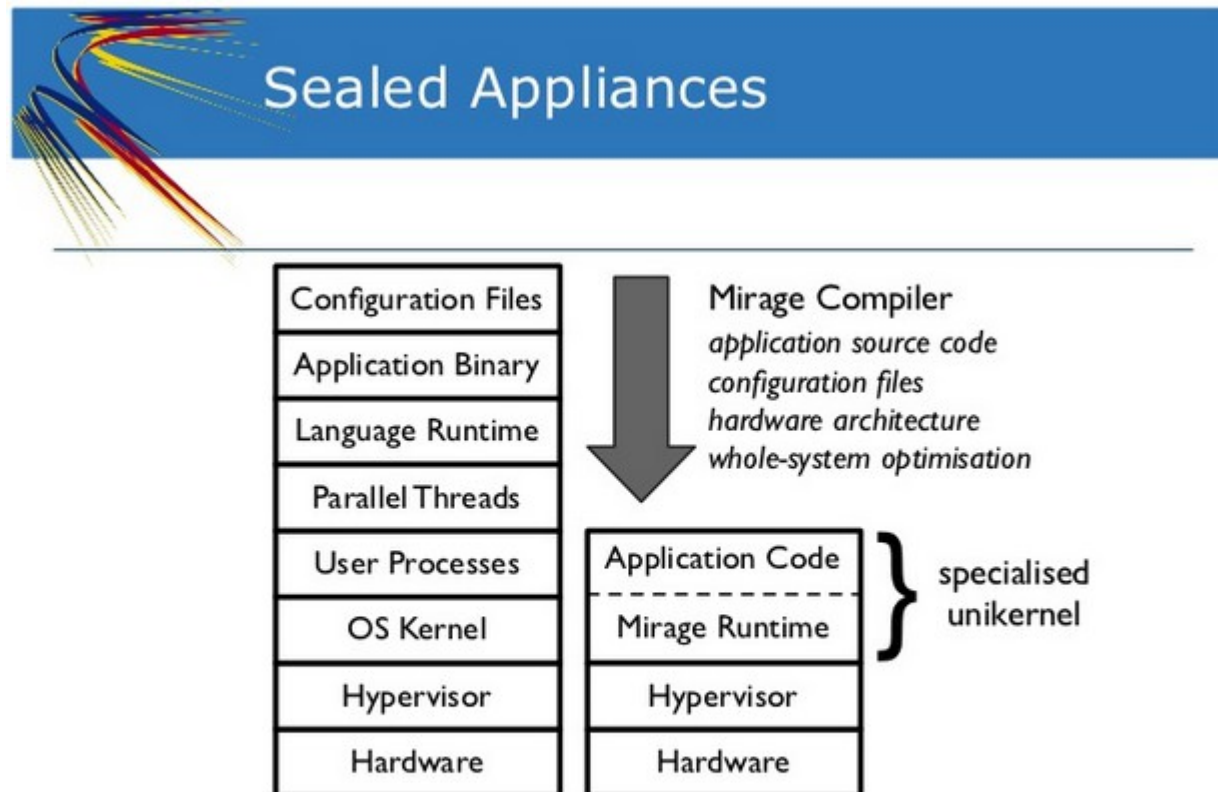


Isolation

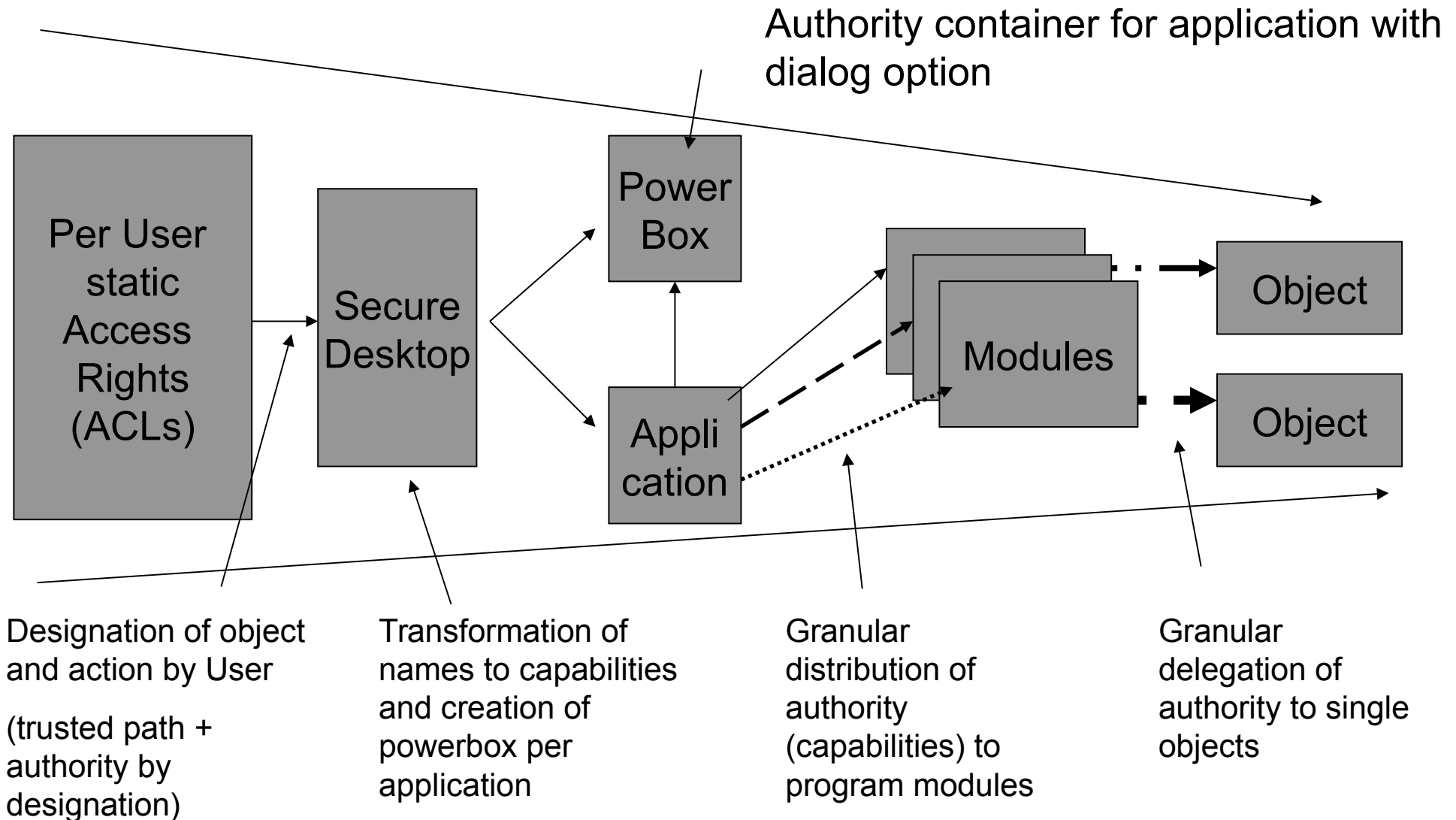
Application Compartmentalization

- Unikernels
- Power Box Concepts

Compartmentization: Unikernels/Mirage OS



Solutions: Authority Reduction Architecture



We need to narrow authority down from the global rights matrix (ACLs or Access Control Matrix) of a users rights to the minimum authority necessary to execute a function. Test: try to find how many rights you REALLY need to copy a file!



Beyond Robust Components

Robustness by Architecture

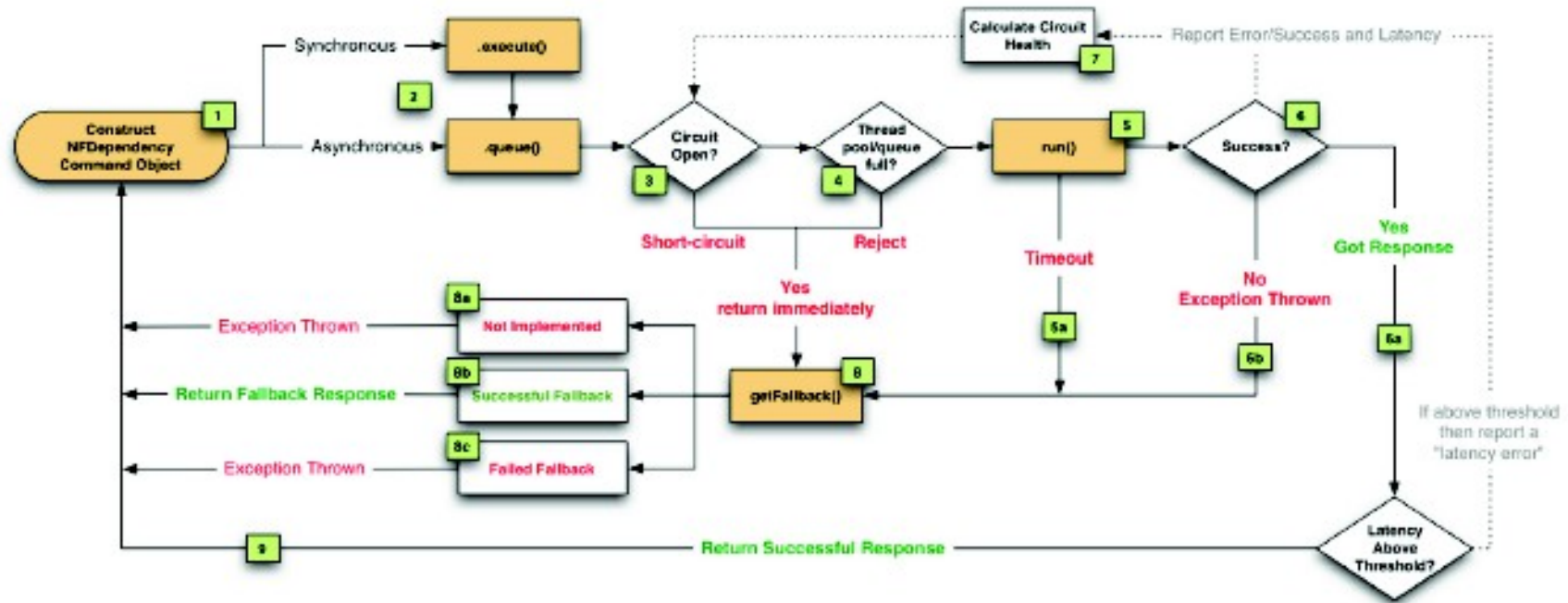
- What makes systems resilient/robust?
- Examples for critical infrastructures

Why is the Internet robust?

- **Many IXPs (exchange points) available because there is an incentive for large providers to connect with small endpoint providers**
- **Many different providers are prohibiting intra-provider failures from becoming global ones**
- **Sudden capacity changes are not financial threats through 5% rule (providers do not have to pay for 5% overcapacity in one month. This prevents panic actions)**
- **Considerable amounts of spare capacity are available (overprovisioning), even though CDNs threaten both distribution of flow as well as capacity reserves.**
- **Routers do not provide alternative traffic information (why do I believe that this is a good thing?). No map of internet traffic routes and capacity exists.**
- **BGP does not influence routers in other networks**
- **Specialists take care of problems on a daily base, SLAs are not cross-network**
- **There is no global or centralized control of individual machine behavior**
- **TCP adjusts service to available capacity (large range of what is called „best effort“)**

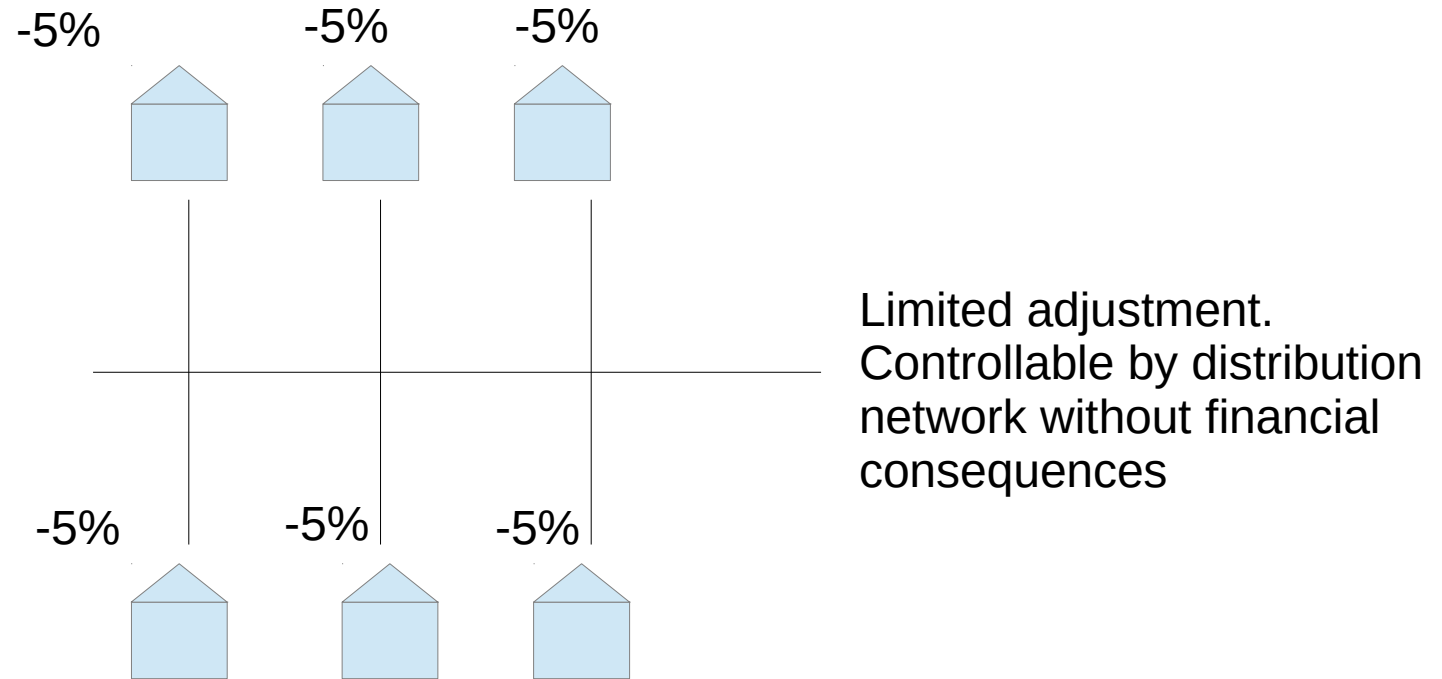
Enisa Inter-X: Resilience of the Internet Interconnection Ecosystem. There is no global authority which senses the state of the Internet and performs remote control of routers!

Self-Regulated Fault-Tolerance



Source: A.Cockcroft, Netflix

3. Semi-autonomous Components



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.

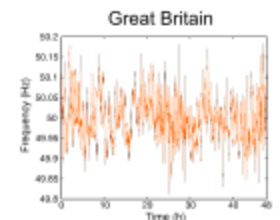
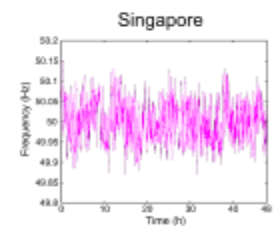
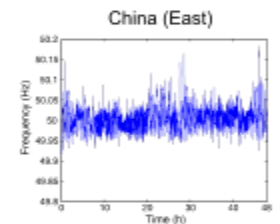
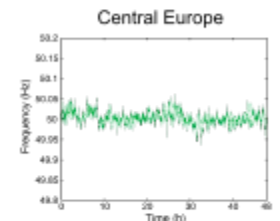
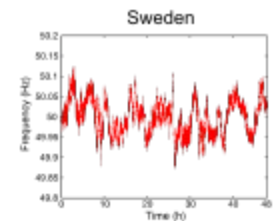
Randomness: The 50.2 Hz Problem

Automatic shut-down of PVSs brings down power grids

Solution: stochastic distribution of shutdown levels across systems

**Forum Netztechnik/Netzbetrieb im VDE (FNN),
März 2011**

Randomness in distributed systems avoids digital level jumps or thrashing

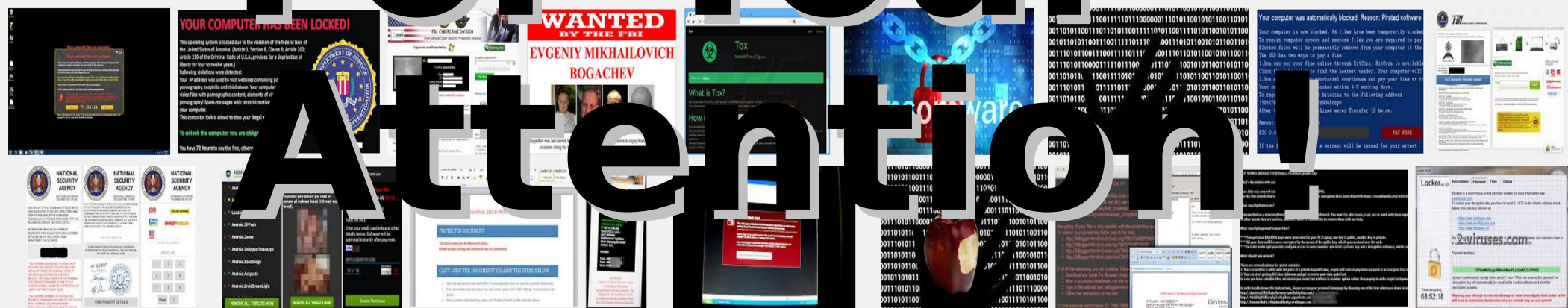
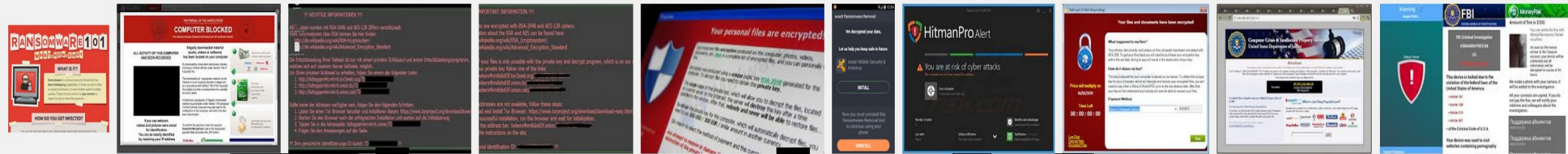
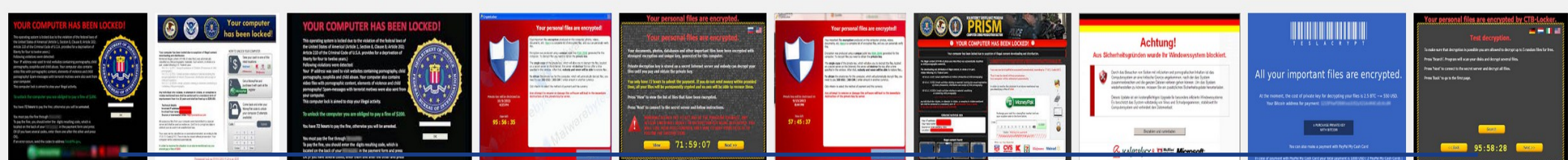


Technological modesty lessons from Ukraine

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?



Thank You for Your Attention!

Resources

- **Ben Hayes, NeoConOpticon**
- **World Threat Assessment,**
http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf
- **W.Kriha, Secure System Slides on www.kriha.org**
- **Butler Lampson, Perspectives on Protection and Security, SOSP15 History Day, <http://dl.acm.org/citation.cfm?doid=2830903.2830905>**
- **Margo Seltzer, Mark Miller, David Mazières, Yuanyuan Zhou, Is Achieving Security a Hopeless Quest, SOSP15 History Day**
- **Schneier on Equation Group: <http://www.lawfareblog.com/2015/02/the-equation-groups-sophisticated-hacking-and-exploitation-tools/>**
- **W. Kriha, R.Schmitz, Sichere Systeme, Springer Verlag**
- **Cap-talk mailing list**
- **<http://www.shareable.net/blog/towards-a-resilience-pattern-language>**
- **Lewis J. Perelman, Shifting Security Paradigms: Toward Resilience.**
- **Matej Kosik, Jiri Safarik, A Contribution to Techniques for Building Dependable Software Systems**
- **Glenn Greenwald,**
http://www.salon.com/2012/08/15/the_sham_terrorism_expert_industry/
- **Sicherheitslücken bei Software. FBI warnt vor Hackerangriffen auf Autos. NZZ.ch 18.3.2016**

Resources

1. **Top ten Windows Vulnerabilities 2014**
2. **ENISA Study IoT and Smart Home Security December 2015**
3. **Carsten Meywirth, BKA, „The threat is global - Current trends of Cyber Crime“ CEBIT 2016**
4. **Sony Pictures breach: <https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/>
<http://www.theatlantic.com/international/archive/2014/12/did-north-korea-really-attack-sony/383973/> or <http://tinyurl.com/po3wxhy>**
5. **Links on resilience from Bruce Schneier:
<https://www.schneier.com/crypto-gram/archives/2015/0315.html>**
6. **Honeytrain and IT-Security Business Expectations:
http://www.n-tv.de/technik/Hacker-lassen-Zug-entgleisen-article14728321.html?google_editors_picks=true**
7. **IT-Security Gesetz BRD (Entwurf)
<https://netzpolitik.org/wp-upload/141104-Schreiben-Einleitung-L%C3%A4nderbeteiligung-IT-Sicherheitsgesetz-final.pdf>**
8. **Ukraine Power Plant attacks,
<http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/>**

Resources

1. **Verschlüsselte OSGP-Kommunikation von Smart Metern leicht belauschbar, heise.de, 12.05.2015 Dennis Schirmmacher**
2. **Big-name sites hit by rash of malicious ads spreading crypto ransomware, by Dan Goodin - Mar 15, 2016 <http://arstechnica.com/security/2016/03/big-name-sites-hit-by-rash-of-malicious-ads-spreading-crypto-ransomware/>**
3. **Feb 2nd 2016, Security Now 545, Three Dumb Routers, Steve Gibsons guide to using multiple routers for a secure network.
<https://twit.tv/shows/security-now/episodes/545?autostart=false>**
4. **Unikernel joining Docker,
<http://highscalability.com/blog/2016/1/21/why-does-unikernel-systems-joining-docker-make-a-lot-of-sens.html>**
5. **Mirage OS,
http://www.slideshare.net/xen_com_mgr/mirage-extreme-specialisation-of-virtual-appliances?qid=f23caf3c-5292-4399-8b35-146f7bbd607a&v=&b=&from_search=4**
6. **Capability Hardware Enhanced RISC Instructions: CHERI Instruction-set architecture Robert N.M. Watson, Peter G. Neumann, Jonathan Woodruff, Jonathan Anderson, David Chisnall, Brooks Davis, Ben Laurie, Simon W. Moore, Steven J. Murdoch, Michael Roe April 2014 Technical Report Number 850 Computer Laboratory UCAM-CL-TR-850 ISSN 1476-2986
<https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-850.pdf>
Video: <https://www.youtube.com/watch?v=4a1FcOReJRI>**
7. **Steve Klabnik,
<https://www.codementor.io/rust/tutorial/steve-klabnik-rust-vs-c-go-ocaml-erlang>**
8. **Jens Getreu,
<http://www.getreu.net/public/downloads/doc/Enhance%20Embedded%20System%20Security%20With%20Rust/>**