

Security Pitfalls

A review of recurring failures

Dr. Dominik Herrmann

Download slides at

<https://dhgo.to/pitfalls>



Research on security, privacy, online tracking, forensics.

Postdoc researcher University of Hamburg

Temporary professor University of Siegen

Junior Fellow German Informatics Society



Media reports about security revolve around fear, uncertainty, and doubt.

Cyber Crime Still on the Rise, Using Nine Basic Attack Methods



/ SECURITY

grapegeek/iStockphoto



By Arik Hesseldahl

| [Twitter](#) @ahess247 | [EMAIL](#) | [ETHICS](#)

April 13, 2015, 9:01 PM PDT



THE FISCAL TIMES ☰

POLICY + POLITICS

How Terrorists Could Hijack the Internet of Things



© George Frey / Reuters

By Patrick Tucker, Defense One [f Like](#) 21

September 10, 2016

By 2020, there will be anywhere from 20 billion to 50 billion internet-connected devices, including about one in five cars and or trucks, according to industry forecasts. That's big business for outfits that sell data

Cyber Armageddon: The Threat To Modern Civilisation

Rajinder Tumber



Nuclear weapons are known to be the most dangerous weapons on Earth. Just one of these has the capability to destroy an entire city, potentially killing millions of humans and other life. Yet, while the United Nations,

Many vulnerabilities could be avoided, if vendors followed best practices and security management standards.



Cyber Security and Resilience of Intelligent Public Transport

Good practices and recommendations

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/intelligent-public-transport/good-practices-recommendations/at_download/fullReport

Problem: Best practices are often abstract and of organizational nature.

OPERATORS

integrate cybersecurity in corporate **governance**

implement a **strategy** addressing holistically cyber security & safety risks

implement risk mgmt. for cybersecurity in multi-stakeholder environments incl. contractors and dependencies

clearly and routinely **specify** their cyber security **requirements**

annually review cybersecurity processes, practices and infrastructures

MANUFACTURERS

create **products/solutions** that **match** the cybersecurity **requirements** of end-users

collaborate in the development of IPT-specific **standards** and apply them to IPT solutions

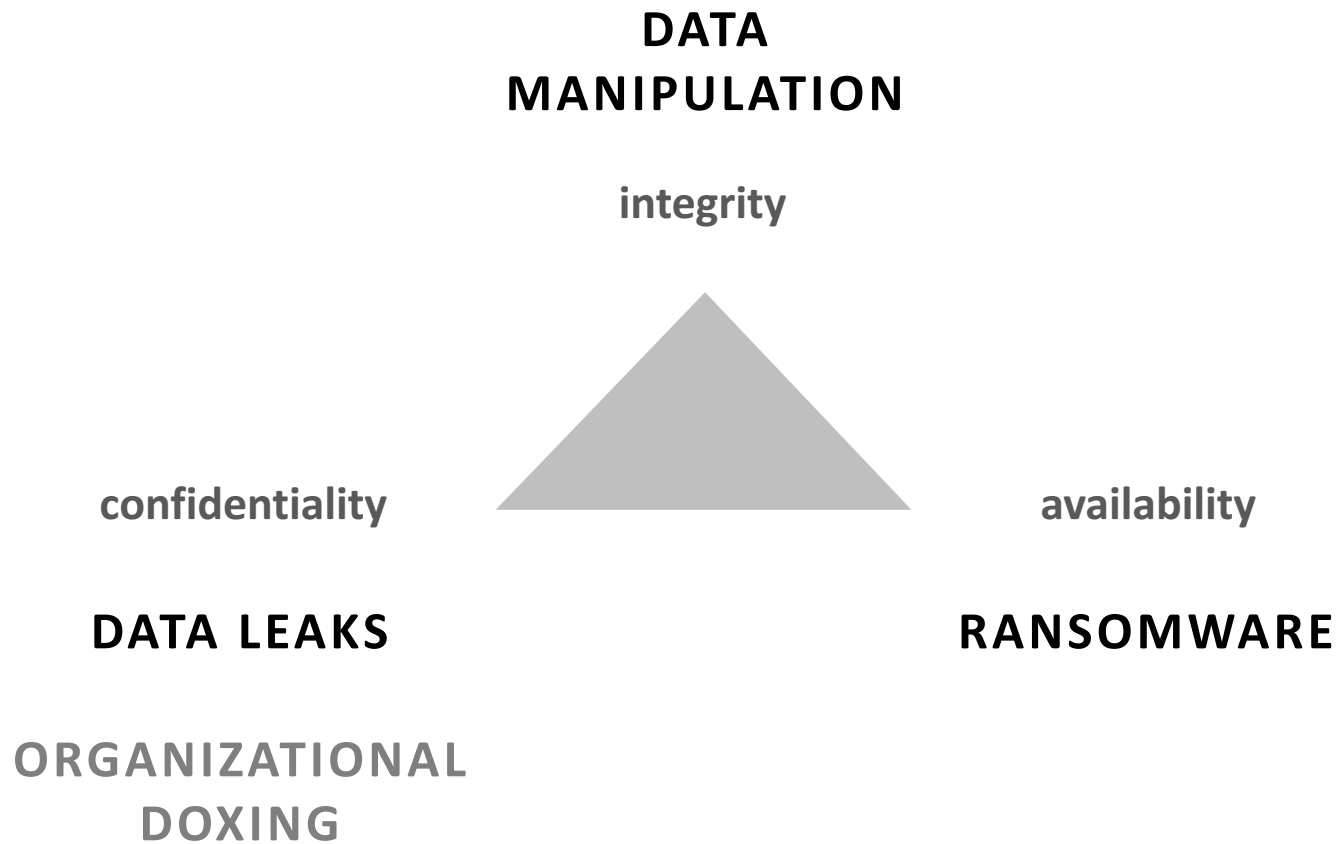
develop a trusted **information sharing platform** on risks and vulnerabilities

provide **security guidance** for systems, products and solutions

Good practices and recommendations

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/intelligent-public-transport/good-practices-recommendations/at_download/fullReport

As more and more data is stored and processed, securing data against attacks becomes more important.



The Classical Engineering Perspective

PROACTIVE SECURITY




Weakness 1: Out of sight, out of mind

Exploiting known vulnerabilities is still a very successful attack vector. Vendors and users fail to patch their software in a timely manner.

The security flaws at the heart of the Panama Papers

PANAMA PAPERS / 06 APRIL 16 /
by JAMES TEMPERTON AND MATT BURGESS



Mossack Fonseca ran old Outlook Web Access (2009), Drupal (2013, 25 vulns)

SHODAN

Devices vulnerable to Heartbleed

Search for `vuln:cve-2014-0160` returned 128,017 results on 14-09-2016

Top Countries

1. United States	28,637
2. Germany	9,444
3. China	9,169
4. Korea, Republic of	6,549
5. France	6,329
6. United Kingdom	4,703
7. Russian Federation	4,496
8. India	4,387
9. Brazil	3,225
10. Japan	3,123

Heartbleed (2014)
128k vulnerable devices in 9/2016



UltraReset attack on MiFare Ultralight (New Jersey & San Francisco, 2012)
... still works in 2016 (Vancouver)



Weakness 2: Fools with tools ... don't know their trade

Due to unawareness, carelessness, and haste, vendors ship products with embarrassing security holes, for instance in user authentication.

**ABUS, Blaupunkt, Lupus
alarm systems (2016):**

insecure default passwords
can be disabled without the PIN

also:

Loxone Smart Home (2016)



The image is a screenshot of a web article from the magazine 'c't magazin für computer technik'. The article title is 'Home security systems hacked with 1234 password UPDATE'. The main image shows a shield behind a chain-link fence with a crescent moon in the background. Below the image is a yellow banner with the text 'TRENDS & NEWS | C'T DECKT AUF'. The article is by Sven Hansen and Ronald Eikenberg, dated 29.06.2016. The tags include 'Abus, alert systems, Climax, connected devices, Egardia, Lupus Electronics, Secvest'. The article text states: 'Many smart home security systems come with standard passwords. Potential intruders can deactivate them online and use them to spy on homes - the affected systems are in use in'.

Many industries are currently learning how to do security properly.

Vaillant heatings (2015):

authentication and password check performed by a Java applet in the user's browser

Vulnerability in Vaillant Heating Systems Allows Unauthorized Access

A critical security vulnerability in the heating and power systems of German company Vaillant allows unauthorized people access the systems, turn them off and damage them at will.

Vaillant has sent all its customers a warning, recommending they manually disconnect the vulnerable devices, namely ecoPower 1.0, from the network and wait for one of their employees to fix the systems on site.





Weakness 3: Underestimating the adversary

Insecure designs result from software developers making poor decisions because of wrong assumptions.

BMW ConnectedDrive (2015)

- all cars used the same cryptographic key
- communication with BMW servers was not protected

Impact: car doors could be unlocked by sending a faked SMS to the car

BMW Update Kills Bug In 2.2 Million Cars That Left Doors Wide Open To Hackers

FEB 2, 2015 @ 08:45 AM

7,535 VIEWS



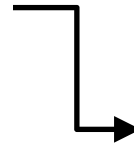
BMW Connected Drive

German car manufacturer BMW has issued a security patch over the air to its **vehicles**, after the emergence of a **vulnerability that would have allowed**

Insecure designs result from software developers making poor decisions because of wrong assumptions.

BMW ConnectedDrive (2015)

- all cars used the same cryptographic key
- communication with BMW servers was not protected



“No one is able to ...”

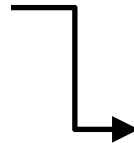
- reverse engineer the hardware where the key is stored
- set up a fake GSM network to send an SMS to the car

Impact: car doors could be unlocked by sending a faked SMS to the car

Insecure designs result from software developers making poor decisions because of wrong assumptions.

BMW ConnectedDrive (2015)

- all cars used the same cryptographic key
- communication with BMW servers was not protected



Researchers just did it.

- reverse engineer the hardware where the key is stored
- set up a fake GSM network to send an SMS to the car

Impact: car doors could be unlocked by sending a faked SMS to the car

Insecure designs result from software developers making poor decisions because of wrong assumptions.

Security Experts Warn Millions of Car Owners Should Stop Using Remote Keys

by David Meyer AUGUST 11, 2016, 10:55 AM EDT





**Weakness 4: Outsourcing security to vendors ...
... can get out of hand quickly**

The RFID tickets used for public transport in Berlin stored the last 10 waypoints, which could be used to create personal location profiles of commuters.

VBB-FAHRCARD

Berlins elektronische Fahrkarte speichert Bewegungsprofile

Mit der überwiegend in Berlin, aber auch in Brandenburg eingesetzten VBB-Fahrcard können laut VBB keine Bewegungsprofile gespeichert werden. Wie sich nun herausgestellt hat, stimmt das nicht. Lesegeräte in [BVG-Bussen](#) [speichern](#) Bewegungsprofile auf der Fahrcard.

Wie der Fahrgastverband IGEB herausgefunden hat, lässt die VBB-Fahrcard entgegen den Aussagen der Herausgeber die



Die VBB-Fahrcard kann Bewegungspunkte speichern, obwohl dies laut VBB technisch unmöglich sein soll. (Bild: Andreas Sebayang/Golem.de)

Datum: 29.12.2015, 11:35

Autor: [Andreas Sebayang](#)

Themen: [BVG](#), [Bundesregierung](#), [Cookies](#), [Datenschutz](#), [E-Ticket](#), [VBB](#),

- operators denied the leak until proven wrong
- claimed that tracking was enabled by vendor without their knowledge



Weakness 5: Social Engineering

High-profile frauds heavily rely on social engineering.



Austrian Firm Fires CEO After \$56-million Cyber Scam

Austrian aircraft parts maker FACC said Wednesday that it has fired its chief executive of 17 years after cyber criminals stole some 50 million euros (\$56 million) in a so-called "fake president" scam.

FACC, whose customers include Airbus, Boeing, and Rolls-Royce, said that its supervisory board fired Walter Stephan with immediate effect after he "severely violated his duties".

“Fake President Fraud”

also: “Spear Phishing”

LEONI



16 Aug 2016 [Ad-hoc announcement] [Company] Back to overview

Leoni targeted by criminals

Nuremberg: Leoni AG (ISIN DE 0005408884 / WKN 540888) realised on Friday 12 August 2016 that it had become the victim of fraudulent activity with the help of falsified documents and identities and the use of electronic communication channels. As a result, company funds were transferred to accounts abroad. The Management Board immediately launched an investigation into the events and is currently assessing claims for damages and insurance claims. It has also reported the matter to the police criminal investigators. The damage amounts to an outflow of liquidity totalling around EUR 40 million. The criminal activities have not affected the IT infrastructure or data security.

Consumers have privacy rights, e.g. to access and delete their personal data. Handling requests is very frustrating for consumers and vendors.

We conducted a field study with 150 apps and 120 websites.

Even after the second mail **only 1 in 2** vendors complied.

1 in 4 website owners could be tricked into sending the data **to a different** e-mail address.

Most vendors deleted our accounts **without prior confirmation**.

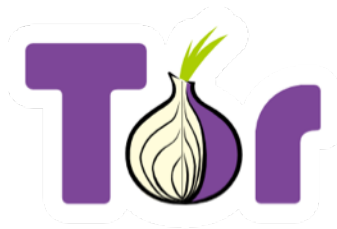
The Classical Engineering Perspective

PROACTIVE SECURITY

A More Recent Approach

▶ **REACTIVE SECURITY**

It is difficult to track down proficient adversaries.



*anonymized
communications*



*cryptographic
currencies*

**intrusion
detection**

find anomalies
(logging & audits)

**emergency
protocols**

operations and
communications

**not all hackers
are equal**

blackhats vs.
whitehats

3 CONSIDERATIONS FOR REACTIVE SECURITY

Vendors often miss the opportunity to collaborate with security researchers.

Scientists Banned from Revealing Details of Car-Security Hack

The UK has banned researchers from revealing details of security vulnerabilities in car locks. In 2008, Phillips brought a similar suit against researchers who broke the Mifare chip. That time, they lost. This time, Volkswagen sued and won.

This is bad news for security researchers. (Remember back in 2001 when security researcher Ed Felten sued the RIAA in the US to be able to publish his research results?) We're not going to improve security unless we're allowed to publish our results. And we can't start suppressing scientific results, just because a big corporation doesn't like what it does to their reputation.

Vendors often miss the opportunity to collaborate with security researchers.

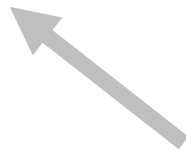
Judge orders halt to Defcon speech on subway card hacking

Federal judge grants the state of Massachusetts' request to prevent three MIT students from giving a presentation about hacking smartcards used in the Boston subway system.

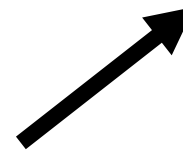
opportunity for vendors
bugs uncovered by the
security community

**As a result there is a flourishing black market for security vulnerabilities.
In response, the software industry has started to set up bug bounty programs.**

black market
for zero-day exploits



white market
bug bounty programs



opportunity for vendors
bugs uncovered by the
security community

Security Pitfalls

TAKE-AWAY MESSAGES

1

Consider attacks on confidentiality, integrity, and availability of your (customers') data.

2

Learn from attacks on others and avoid common mistakes in proactive measures.

3

Prepare to react to security incidents and collaborate with the security community.

Dr. Dominik Herrmann

dh@exomail.to

Slides: <https://dhgo.to/pitfalls>

