

Tales of Insecurity

A campfire is burning brightly in the center-right of the frame, casting a warm orange glow. The background is dark, showing the silhouettes of trees and a tent on the left. The overall scene is a nighttime outdoor setting.

Evergreens, developments, and insights
for integrators and service providers

Dr. Dominik Herrmann

University of Hamburg

University of Siegen

Download slides at

<https://dhgo.to/tales>

research on security, privacy, online tracking, forensics

PhD and Postdoc @ University of Hamburg

Temporary professorship @ University of Siegen

Junior Fellow of German Informatics Society



Dr. Dominik Herrmann



DAILY NEWS: THE GENIE IS OUT OF THE BOTTLE – WE ARE DOOMED

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



/ SECURITY

grapegeek/iStockphoto



By Arik Hesseldahl

|  @ahess247 | EMAIL | ETHICS

April 13, 2015, 9:01 PM PDT



WIRED

SUBSCRIBE

KIM ZETTER SECURITY 07.08.15

1:33 PM

IS CYBER-ARMAGEDDON UPON US? 3 GLITCHES TODAY HAVE SOME SAYING YES

A TRIO OF cyber incidents this morning had some people seeing cyberarmageddon. We're looking at you, Senator Bill Nelson (D-Florida).

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,

**Cloud
Services**

**Big
Data**

**Mobile
Apps**

**NEW
OPPORTUNITIES**

**Attacks on
Critical Infrastructure**



**Data
Leaks**

**Ransomware
and Fraud**

**NEW + OLD
THREATS**

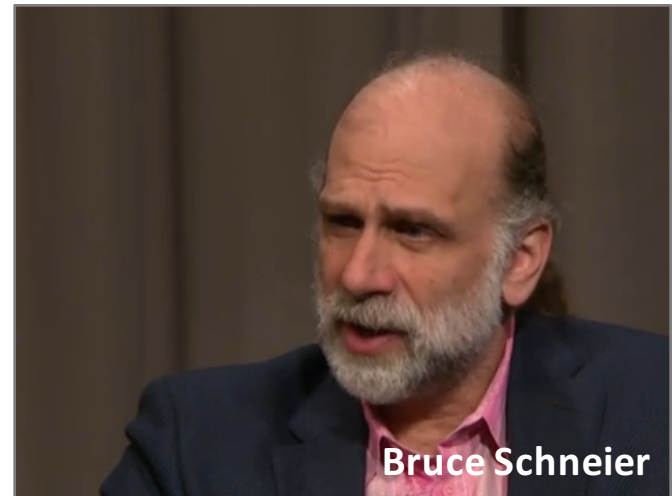
**data will become
the oil of the 21st century**

**Big
Data**



**data has become
a toxic asset, a liability**

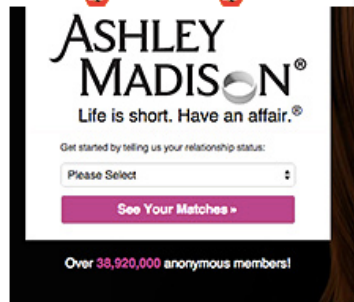
**Data
Leaks**



Data leaks have an interesting property: collateral damage that affects (1) citizens and (2) contractors of the victim.

Ashley Madison Hacked, Cheaters Site Users Revealed

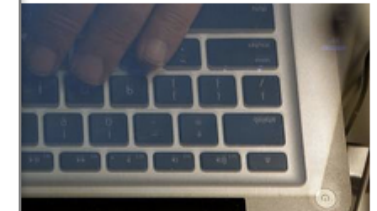
CELEBRITY NEWS AUG. 19, 2015 AT 10:39AM BY RACHEL TORGERSON



TECH

Hacking Team, the Surveillance Tech Firm, Gets Hacked

... surveillance tools to dozens of
ed files



Datenleck: 20.000 Wiener-Linien-Kunden betroffen

Letztes Update am 15.10.2015, 14:09

Die persönlichen Daten von 20.000 Wiener-Linien-Kunden sind im Netz gelandet. Die Informationen wurden nach derzeitigem Stand bei einer Zulieferfirma in Deutschland entwendet.

Collateral damage allows data leaks to be monetized.

2015



“for the lulz”



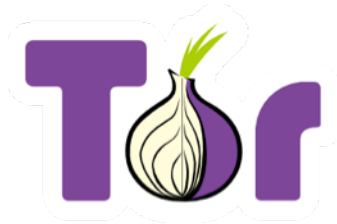
for profit

THEN ————— HACKING ————— NOW

Two recent developments help adversaries get away with their demands.



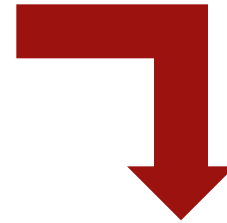
*crypto-
currencies*



*anonymized
communications*

**collateral
damage**

leverage



for profit

How did the genie get out the bottle?

FIVE WEAKNESSES




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)

Devices Vulnerable to Heartbleed

Search for `vuln:cve-2014-0160` returned 237,539 results on 26-03-2016



Top Countries

1. United States	57,598
2. China	17,455
3. Germany	17,273



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.

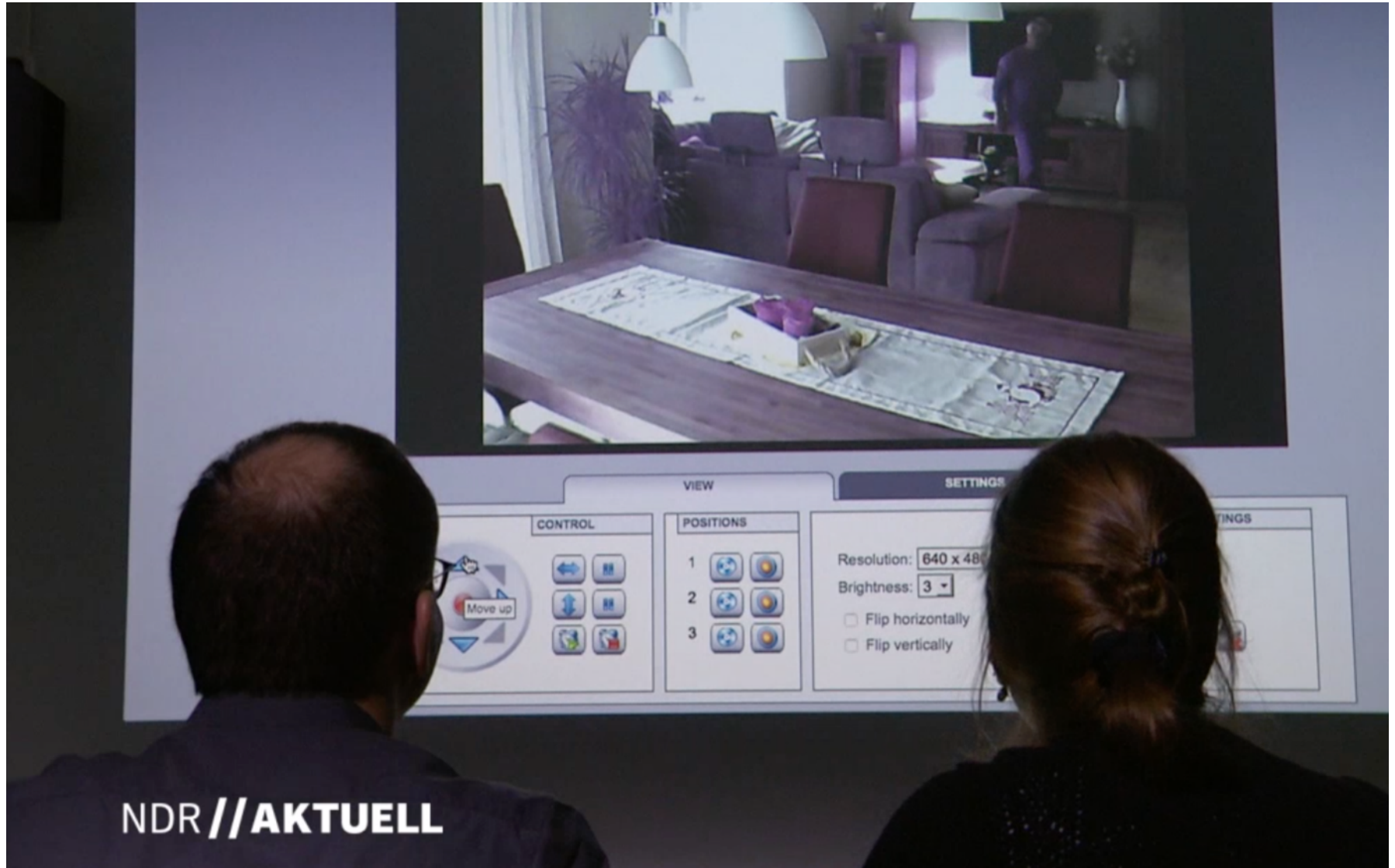
Maginon webcams (2015)

1. bypasses firewall of DSL router via UPnP
2. comes with empty default password

thousands of cameras sold at ALDI and Hofer



Insecure devices can now be discovered by everyone within short time by querying specialized search engines like *shodan.io*.



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



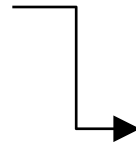
BMW Connected Drive

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 ...”

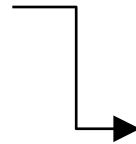
- reverse engineer the hardware where the key is stored
- set up a fake GSM network to send an SMS to the car

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

GCHQ intervenes to prevent catastrophically insecure UK smart meter plan

BY **GRAEME BURTON** | SECURITY | 21 MARCH 2016



GCHQ demands more encryption to prevent smart meter disaster

INTELLIGENCE AGENCY GCHQ has intervened in the rollout of smart meters to

proposal to use same cryptographic key on 53 mn. devices

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

New app-based TAN system for online banking less secure than previous systems, say FAU researchers



Bild: FAU/Luisa Gerlitz
📅 November 3, 2015

Several German banks, including Hypovereinsbank, Sparkasse, DKB and VR-Bank, are introducing a new system of mobile banking for smartphones. However, IT security researchers Vincent Hauptert and Tilo Müller from FAU have shown through a hacker attack that the new app-based TAN system

**proposal to run banking app
and TAN app on the same phone**

GCHQ intervenes to prevent catastrophically insecure UK smart meter plan

BY **GRAEME BURTON** | SECURITY | 21 MARCH 2016



GCHQ demands more encryption to prevent smart meter disaster
INTELLIGENCE AGENCY GCHQ has
intervened in the rollout of smart meters to

proposal to use same cryptographic key on 53 mn. devices



Weakness 4: Relying on software libraries ...

... can get out of hand quickly

Vulnerabilities in software libraries are concerning due to (1) their large impact and (2) the fact that it takes longer until the patch reaches end users.

1,500 iPhone apps have a serious flaw that hackers can easily exploit



By [Chris Smith](#)

Tuesday April 21, 2015, 10:20 AM

While security companies usually detail vulnerabilities in Android [that hackers can use for malicious purposes](#), analytics service SourceDNA [uncovered](#) an encryption flaw that may affect as many as 1,500 applications, [Ars Technica reports](#).

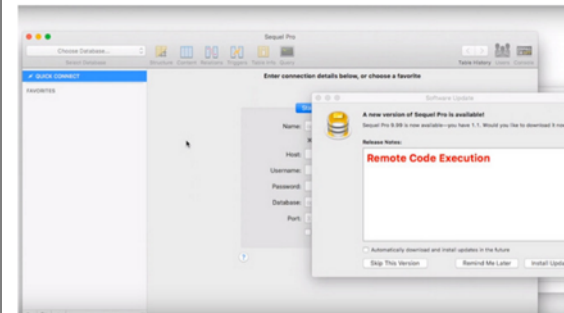
AFNetworking
(2015)

Sparkle software updater leaves 'huge' number of Mac apps open to attack

By: [Mikey Campbell](#)

Tuesday, February 9, 2016 5:50 PM

A "huge" number of third-party Mac apps are under threat of man-in-the-middle attacks due to a recently discovered vulnerability in Sparkle, an open source framework used to facilitate software updates.



Proof-of-concept video showing remote code

Sparkle Updater
(2016)



Weakness 5: With big data comes big responsibility

Problem 1: 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**.

Problem 1: 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.

Compliance will become important with upcoming **EU General Data Protection Regulation** (high fees)

Opportunity: operators could **delegate** the process of handling privacy-related requests **to (cloud) service providers** in the future.

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**.

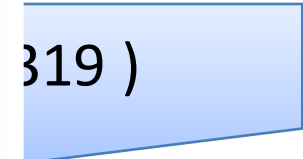
Problem 2: Misconceptions about the effectiveness of anonymization and pseudonymization results in inadvertent disclosure of sensitive personal data.



Pseudonymiz



(not effective)

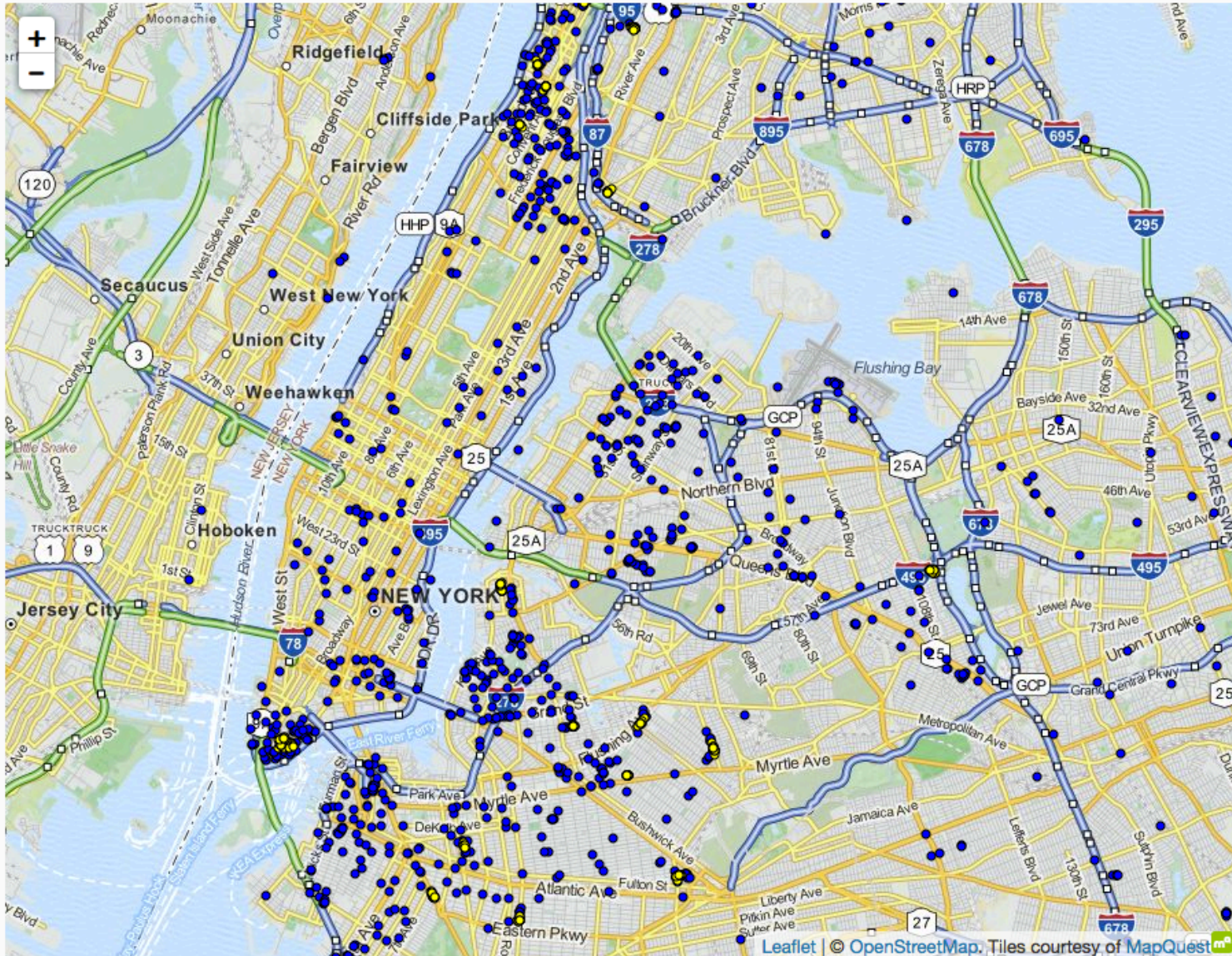


71B9C3F3EE5EFB81CA05E9B90C91C88F, 98C2B1AEB8D40FF826C6F1580A600853,
 VTS, 5, , 2013-12-03 15:46:00, 2013-12-03 16:47:00, 1, 3660, 22.71,
 -73.813927, 40.698135,
 -74.093307, 40.829346

GPS coords

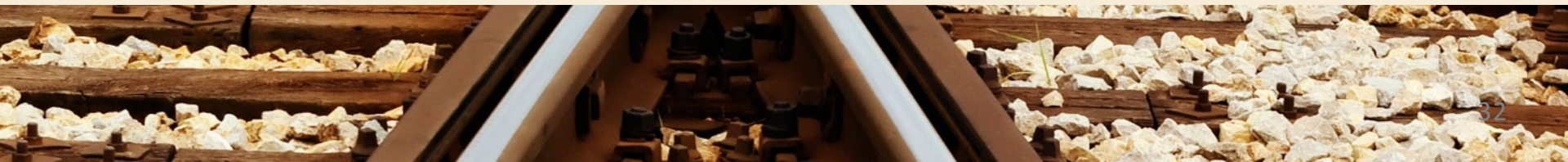


Problem 2: Anonymization and pseudonymization are difficult and may result in inadvertent disclosure of sensitive personal data.





Implications for vendors and integrators



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

Furthermore, it is challenging to determine which security measures to implement with what priority. The utility of measures is difficult to assess.

Popular metric:

Return on Security Investment (ROSI)

Calculation relies on **good estimates** for

- annual loss expectancy
- mitigation ratio

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

In too much discourse, truth is lost: Statistics, organizational measures and paper audits distract from the source of vulnerabilities: the source code.

opportunity for vendors
bugs uncovered by the
security community

internal code reviews ————— expensive and
limited coverage ————— penetration testing

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.

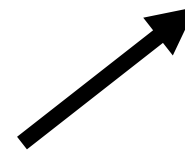
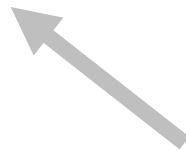
opportunity for vendors
bugs uncovered by the
security community

internal code reviews ————— expensive and limited coverage ————— penetration testing

**As a result there is a flourishing black market for security vulnerabilities.
In response vendors in the software industry have 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

internal code reviews

expensive and
limited coverage

penetration testing

Tales of Insecurity

TAKE-AWAY MESSAGES

1

Cloud computing, mobile apps, and big data increase the impact of attacks

2

We will see more high-profile attacks until industry takes security seriously.

3

Vendors should accept the help of the security community.

Dr. Dominik Herrmann

dh@exomail.to

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