Fail = First Attempt In Learning
Internet of Things

- Why do I talk about that topic?
- Background: IT-Journalist since more than 12 years
- Refrigerator that sent out spam mails (2014)
Structure of my #34C3 talk

- IoT numbers and examples
- Where is the problem?
- IoT examples of fails in terms of: security & privacy
- Solutions in terms of regulation, consumers, it-security and developers
## Internet of Things

<table>
<thead>
<tr>
<th>Category</th>
<th>2016</th>
<th>2017</th>
<th>2018</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consumer</strong></td>
<td>3,963.0*</td>
<td>5,244.3</td>
<td>7,035.3</td>
<td>12,863.0</td>
</tr>
<tr>
<td><strong>Business (cross industry)</strong></td>
<td>1,102.1</td>
<td>1,501.0</td>
<td>2,132.6</td>
<td>4,381.4</td>
</tr>
<tr>
<td><strong>Business (vertical specific)</strong></td>
<td>1,316.6</td>
<td>1,635.4</td>
<td>2,027.7</td>
<td>3,181.0</td>
</tr>
<tr>
<td><strong>Grand-Total</strong></td>
<td>6,381.8</td>
<td>8,380.6</td>
<td>11,196.6</td>
<td>20,415.4</td>
</tr>
</tbody>
</table>

Source: Gartner (January 2017) *MILLIONS
Internet of Things

International Data Corp. (IDC)
- DATA FROM JUNE 2017 -

Spending on IoT in 2017: grow 17% compared with the previous year, reaching more than $800 billion.

By 2021 global IoT spending is expected to reach about $1.4 trillion.
What is the Internet of Things?

Connected Everything:
- Toys, Sex Toys
- Home Automation like
- Light bulbs, surveillance cameras,
  thermostats
- Digital Assistants, Wearables
Internet of Things

* Smart Coffee Maker
  - can connect with other things like fitness & sleeping trackers via IFTTT
  - e.g. little sleep – strong coffee
Internet of Shit

* Toilet IoT Sensor

By an Israeli Start-up named OutSense

Stool analysis

data sent to the cloud
Internet of Shit

@internetofshit

whatever, put a chip in it. say hello: internetofshit@gmail.com

In your stuff

facebook.com/internetofshit

Beigetreten Juli 2015

Tweet an Internet of Shit

Internet of Shit @internetofshit · 6 Std.
Antwort an @internetofshit

hi device makers

feel free to use the cloud

but pls, store the encryption keys on device

so customers can use shit if the internet breaks

Original (Englisch) übersetzen
Where is the problem?

Before vendors started to „connect everything“ they were creating „manually operated“ devices without connectivity.

They had lots of knowledge in terms of materials, ergonomics, and mechanical engineering, but almost zero in the fields of IT-security.
Where is the problem?

Result: they are making the same sorts of security errors than the high-tech industry was dealing with 15 years ago.
The early 2000s web security called and they want their lack of security back.

Rick Holland, Digital Shadows
Where is the problem?

- Hard-coded passwords
- Unsecure Bluetooth
- Permanent cloud server connection
Where is the problem?

Unsecured Devices $\longrightarrow$ Botnet $\longrightarrow$ DDoS Attacks $\longrightarrow$ Internet Outage
Botnet =

a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam.
Botnet owners can control the network of infected computers by issuing commands to perform malicious activities like DDoS attacks.
DDoS

Distributed Denial of Service Attacks are an attempt to stop legitimate visitors from accessing the data normally available on the website. This can lead to completely shutting down a service.
Mirai

* Mirai was responsible for one of the biggest internet outages in history.

* Knocking Twitter, Reddit, Spotify, PayPal and several other major services offline in 2016, because an integral Internet infrastructure provider (Dyn) was attacked via DDoS - by "zombie" IoT devices.
Mirai botnets of 50k devices have been seen. This allows huge attacks, generating obscene amounts of traffic. Even a year after its initial release, Mirai botnet infections are still widespread.
Botnet of 100,000 routers could unleash cyberattack at any moment

BY JAMES WALKER 1 HOUR AGO IN TECHNOLOGY

A botnet of 100,000 home broadband routers is lying dormant and could be activated at any time, according to a security researcher. A new strain of the virulent IoT malware Mirai is being used to amass devices, perhaps in preparation for a major attack.
DDoS attacks increased 91% in 2017 thanks to IoT

In Q3 2017, organizations faced an average of 237 DDoS attack attempts per month. And with DDoS-for-hire services, criminals can now attack and attempt to take down a company for less than $100.

By Alison DeNisco Rayome | November 20, 2017, 5:45 AM PST

35 per cent increase in monthly attack attempts from Q2 to Q3,
91 per cent increase from Q1/2017
(Coreo Network Security Report)
University attacked by its own vending machines, smart light bulbs & 5,000 IoT devices

A university, attacked by its own malware-laced soda machines and other botnet-controlled IoT devices, was locked out of 5,000 systems.

Source: 2017 Data Breach Digest scenario report by Verizon
Innovations

How a fish tank helped hack a casino

By Alex Schiffer  July 21
Woman films her internet-connected camera whispering ‘Hola señorita’
IP-based camera

“It’s like in a movie scene. With this flaw cybercriminals can exchange the images. The camera will show pictures from the same, empty room while the bank is actually just getting robbed.”

Camera as security = useless
German „Stiftung Warentest“: The people testing the toys ranked three out of seven connected toys extremely critical, the other ones as critical.

Among them: Teddy bears, robot dogs and dolls.
Unsecure Bluetooth

Three out of the tested toys did not need a password or pin-code for their bluetooth-connection. Which means: Every smartphone-user close enough could connect with the toy to listen to the children, ask questions or threaten them.
Data-collecting Apps

Apps, that belong to and control the toys, record the device-ID and data of the users to third-party companies or put trackers to control the online-behaviour of the parents.
Advice

„A not-connectable „dumb“ teddy might be the smarter choice in the future.“

(Stiftung Warentest)
Smart doll „Cayla“ got forbidden in Germany by law. It is judged as a „prohibited broadcasting station“. Parents who do not destroy it will be fined.
Cayla visited @Europarl_EN today - the goal, you ask? for herself to be the last #IoT device without proper security. #toyfail #IoTfail
Children's messages in CloudPets data breach

An open database containing links to more than 2 million voice messages recorded on cuddly toys has been discovered, cybersecurity researcher Troy Hunt has revealed.
#toyfail

List of institutions with warnings:

- UK consumer group Which?
- Germany Stiftung Warentest
  - Austrian VKI
- Norwegian consumer council
  - FBI
  (to be continued)
Advice

Consider if you really need a connected toy for your child - (( Or yourself..... ))
Coming up next... 

SEX TOYS
Internet-connected vibrator with built-in webcam fails penetration testing

Please, if you're going to make a connected intimate device, secure it properly.

SEBASTIAN ANTHONY - 4/6/2017, 12:06 PM
Smart Dildo

A high-tech vibrator (Siime Eye, costs $250) with a built-in Web-connected endoscope has been penetration tested by a UK security outfit and found to be massively insecure.
Smart Dildo

The device’s default password is 88888888. If you forget to change it, a few more players than expected might be watching your newest video about your private sex adventure.
Sex toy company admits to recording users' remote sex sessions, calls it a 'minor bug'
Vibrator & App

A vibrator-controlling app that records all your sex sounds and stores them on your phone without your knowledge.
Vibrator & App

Lovense says:

No information or data was sent to the company's servers, and that this audio file exists only temporarily. An update issued fixed the bug.
Internet of Dongs

The Internet Of Dongs Project
Hacking Sex Toys For Security And Privacy
Internet of Dongs

(c) Eddie Mize
Internet of Dongs

* Project Hacks
Sex Toys to Keep
Your Intimate Life
Private

https://internetofdons.gs/
Privacy dangers

„Amazon Echo can learn a lot about their users, their habits and their personalities.“

Daniel Nesbitt, Big Brother Watch, UK.
“The data that’s collected about you is an incredibly valuable asset for the companies that collect this information. And they turn around and use it, or sell it in various ways to monetize that information.”

Cyber Security Expert Sean Laws at KSL.com
What happens with the data?

All digital assistants send all voice controls that are made after „Ok Google“ or „Alexa“ to their servers.

The data will be saved there.
Privacy dangers

"It is not easy for users to understand how, to what extent and where the information collected is processed. Also, it is not clear how long the data will be stored."

German data privacy delegate, Andrea Voßhoff.
Counter Measures

* Google Home and Amazon Echo both have a "Mute Button"

* Check the "Settings" to control or delete the data that is collected
Yes, but...

Although Amazon and Google claim not to listen to conversations before the voice commands ...

Both devices already got hacked.
WHAT CAN WE DO?

#tuwat against #iotfails
Status Quo

—> Information asymmetry between vendor & customer

Currently manufacturers do not need to provide essential information about the security of a device such as for how long it will receive security updates.
What we need

* A security star rating system for IoT products

* Vendors should be forced to close security holes instead of ignoring them

* Vendors should provide us at least with an e-mail-address where we can easily report security flaws
What we need

* Mandatory offline-mode for electronical devices
* an airbag and seatbelt for the digital age
* product liability & clear update policy
Law: GDPR

Coming up in May 2018:

General Data Protection Regulation (GDPR)

with

* Privacy by Design
* Privacy by Default
* More possibilities for law enforcement
Max Schrems

“With every new technology we do experience a phase of craze. Everything that goes, will be done. If vendors won’t observe the law, we have to remind to do it.”
Max Schrems
What can consumers do?

„As a customer we can ask for a compensation when data breaches occur or any other violations of data privacy. If four million people sue a company, and ask for 1000 euro compensation, that could be ‘a bit expensive‘."

Max Schrems
What can consumers do?

Support organizations that help you with fighting for your rights

(E.G. NOYB - noyb.eu)
What can customers do?

* Ask: Does this product really need an internet connection?
* Is it possible to turn it off - and is that product still working after that?
What can customers do?
* Read everything you can find on the product before buying it.
* If the vendor does not offer an option that you are happy with: don’t buy it!
* Write to the vendor to get more information.
What can customers do?

* Clicktivism sometimes helps to stop vendors making stupid decisions

* Online participation
What can customers do?

Follow the basics in IT-security
Updates, Updates, Updates
Separated network for IoT
Safe Passwords
What can customers do?

* Support open hardware and open software
* Products where the data is stored locally are always a better option in terms of privacy
* Start building your own tools
What can developers do?

* Support privacy by design
* Support security by design
* Think about it from the beginning of your product development
* You can change things - take your responsibility
What can IT-Security do?

* Point the vendors to the problems
* Make help IoT Security stronger
* Keep reporting security flaws
* Publish your research (Open Science)
* Help develop IoT standards, labels and seatbeats
* Support each others work to get a stronger voice
How many must be killed in the Internet of Deadly Things train wrecks?

History tells us that technology doesn’t get regulated properly until people start to die. Why will IoT be any different?

By Stilgherrian for The Full Tilt | November 20, 2017 -- 04:37 GMT (04:37 GMT) | Topic: Security
Internet of Fails

„The great age of railway construction was likewise riddled with decades of disasters before the introduction of effective signalling and fail-safe brakes.“

Phil Kernick, founder of information security consultancy CQR.
Internet of Fails

Automotive Industry:
the mandatory fitting of seat belts, designing the bodies of cars to reduce injury to pedestrians, airbag and measures to reduce air pollution.
Internet of Fails

So do we need to kill a few people first?
"Unfortunately that's what will happen."

Safety and security standards for the Internet of Things (IoT) can't come soon enough.
Your ideas?
Your input?
Thank you for your attention,
dear #34c3 crowd!
Now.... Let’s #tuwat!

Contact:
Twitter: @shroombab
shroombab@gmail.com