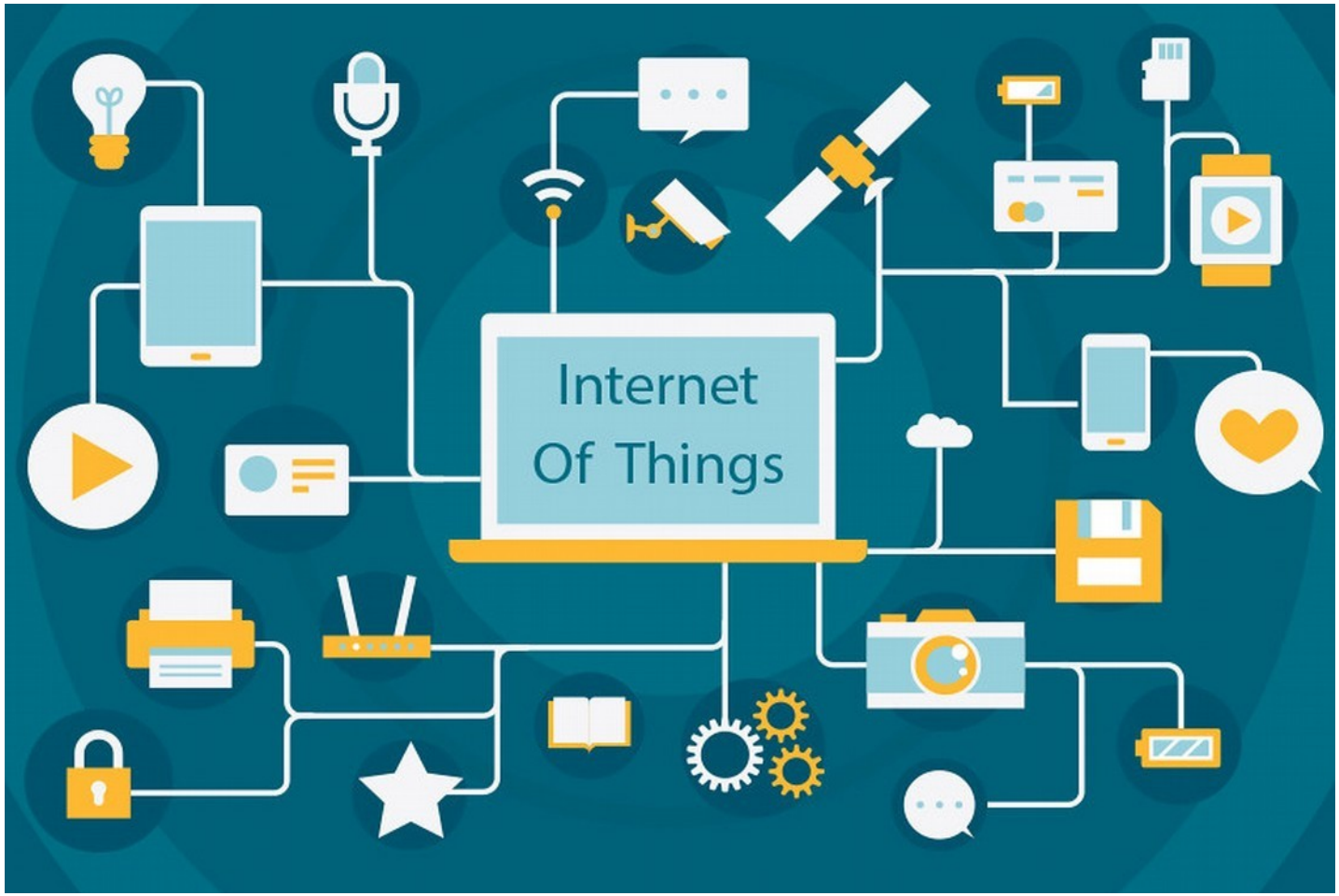
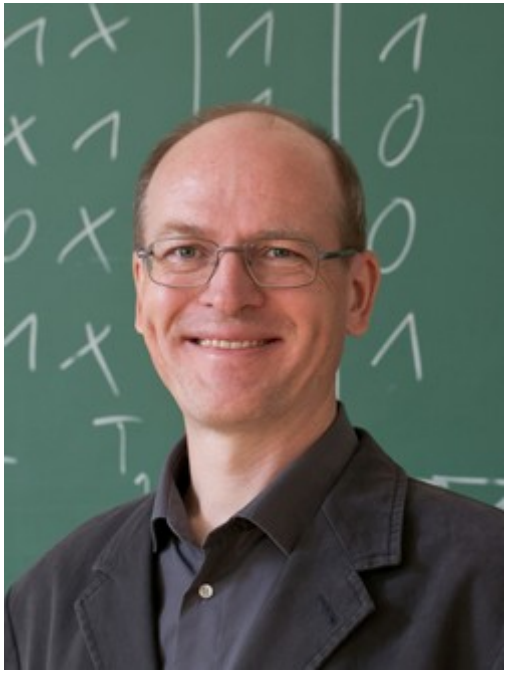
Tackling Privacy and Security Issues of the Internet of Things?

Erik Buchmann, Hochschule für Telekommunikation Leipzig, Germany



Prof. Erik Buchmann



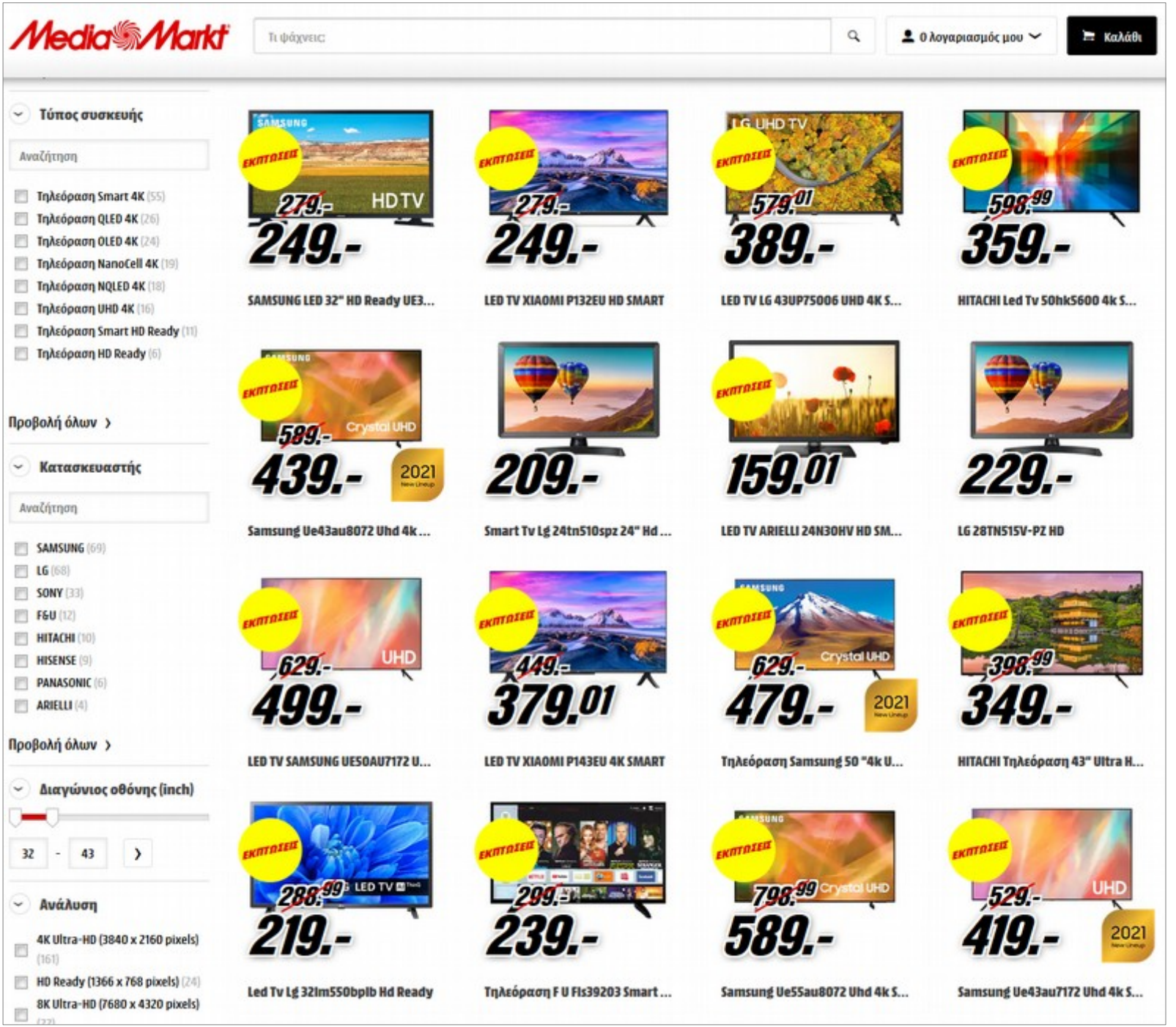
- 1996-2006 Studies and PhD
  at Technical University of Magdeburg, Germany
- 2007-2015 Head of the research group
  „Privacy Awareness in Information Systems“,
  Karlsruher Institut für Technologie
- 2013 Guest lecturer at TU Kaiserslautern
- 2015 Stand-in professor and visiting researcher at TU Saarbrücken
- 2016 Habilitation, Karlsruher Institut für Technologie
- Since march 2016: Full professor at Hochschule für
  Telekommunikation Leipzig, Chair for Data Privacy and Security

Outline of this Talk

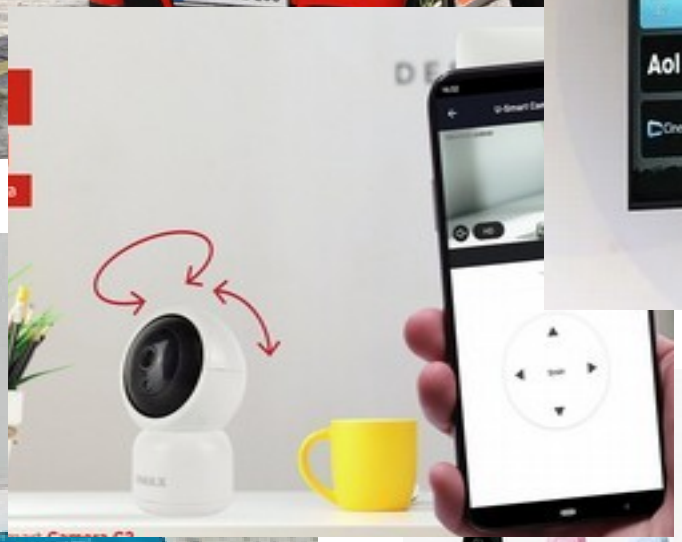
- **Motivation**
- Identifying the Risks
- Securing a Smart Home
- Anonymous IoT Devices
- Conclusion

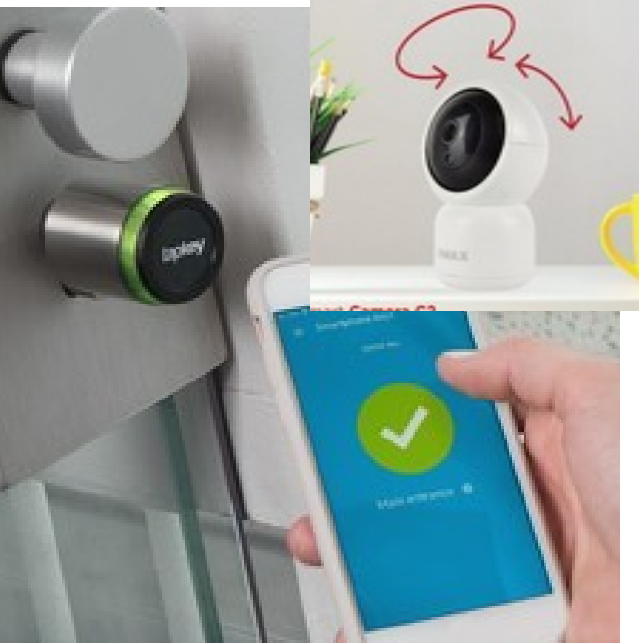
Internet of Things

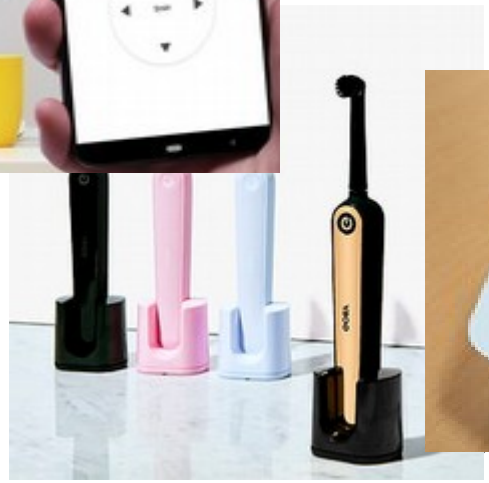
What do you think: How many of these TV sets do not have operating systems, apps, Internet access, etc.?



A Plethora of different IoT Devices exists

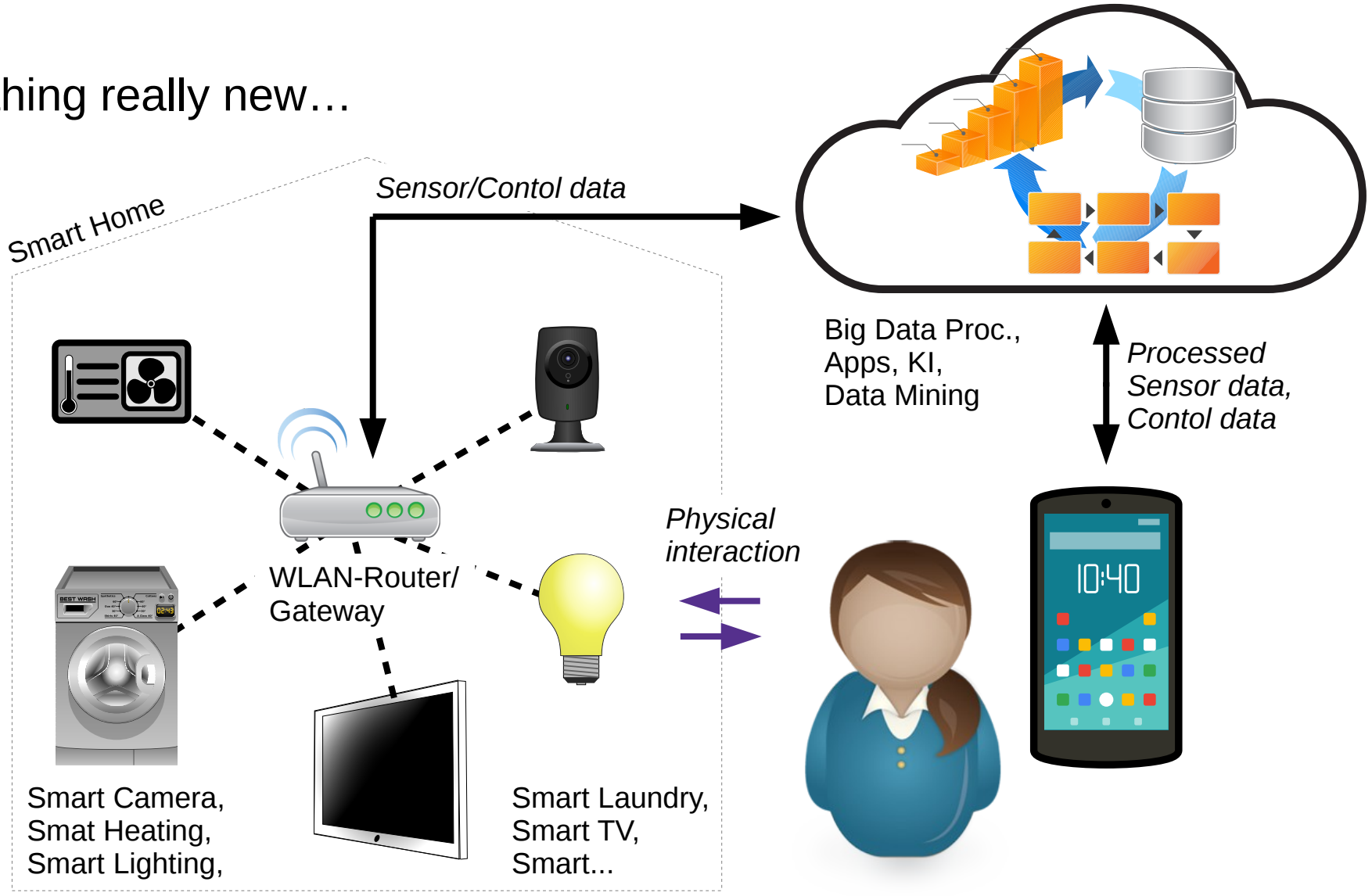






Technical Perspective

- Nothing really new…



Prospects of IoT

https://goingtothemovies.wordpress.com/, 2021

The Good: New Modes of Use

- *Internet access allows new services*
  - Smart car starts via smartphone app
  - Smart TV plays not only broadcasts, but also Netflix, Youtube, Amazon Prime, …
  - Some devices can be extended with new features per software
  - ...
- *Smart devices use sensors to observe user contexts*
  - Smart TV makes recommendations from user preferences
  - Smart heating learns when the user is at home, saves energy
  - Wearable calls emergency, when its (elder) user is becoming sick
  - ...

The Good: Enhanced Usability

- *Smart devices do a job better than its non-smart predecessors*
  - Smart toothbrush sensors tells which teeth need better care
  - Smart doorbell recognizes the persons ringing
  - Smart security camera distinguishes animals and burglars
  - …
- *Smart devices offer better user experience*
  - Controlling many smart devices with one central appliance – the user‘s smartphone
  - Remote maintainance, over-the-air updates for smart devices
  - Smart radio streams via NFC/Bluetooth without cable clutter
  - ...

The Bad: Incredible System Complexity

- *Dumb TV does not work if*
  - Electricity is off, hardware is broken, antenna is disconnected.
- *Smart TV does not work if*
  - Electricity is off, hardware is broken, Internet is disconnected or slowed down, digital rights management disallows it, media server/content-delivery network/cloud has failed, TLS certificates have been revoked, certificate authority has been hacked or certificate validity period expired, media server has changed its protocol, TV has been hacked or has been infected with a virus, TV installs a lengthy update, update has failed or brought new errors, terms and conditions of one of the services must be agreed to first, integrated Java-Script interpreter/software libraries are incompatible with new media types, media suscription has expired, authentication with the media server failed, content/network/cloud/service provider has discontinued its business, … *(to be continued infinitely)*

The Bad: Market Issues

- *Vendor lock-in*
  - Interoperability of smart devices from different manufacturers?
- *Unclear responsibilities*
  - Hardware, Sensors Operating system, apps, cloud, software libraries from different manufacturers: updates, troubleshooting?
- *Non-smart devices are no longer available*
  - cf. some time ago: cameras were banned on company premises, but all modern smartphones had cameras
- *Lifetime*
  - Software lifecycle is much shorter than hardware lifecycle
  - Without updates, device is at the end of its life time, even if hardware is in mint condition

F. Laforet, E. Buchmann, K. Böhm, „Individual privacy constraints on time-series data.“ Information Systems 54, 2015

The Ugly: Privacy

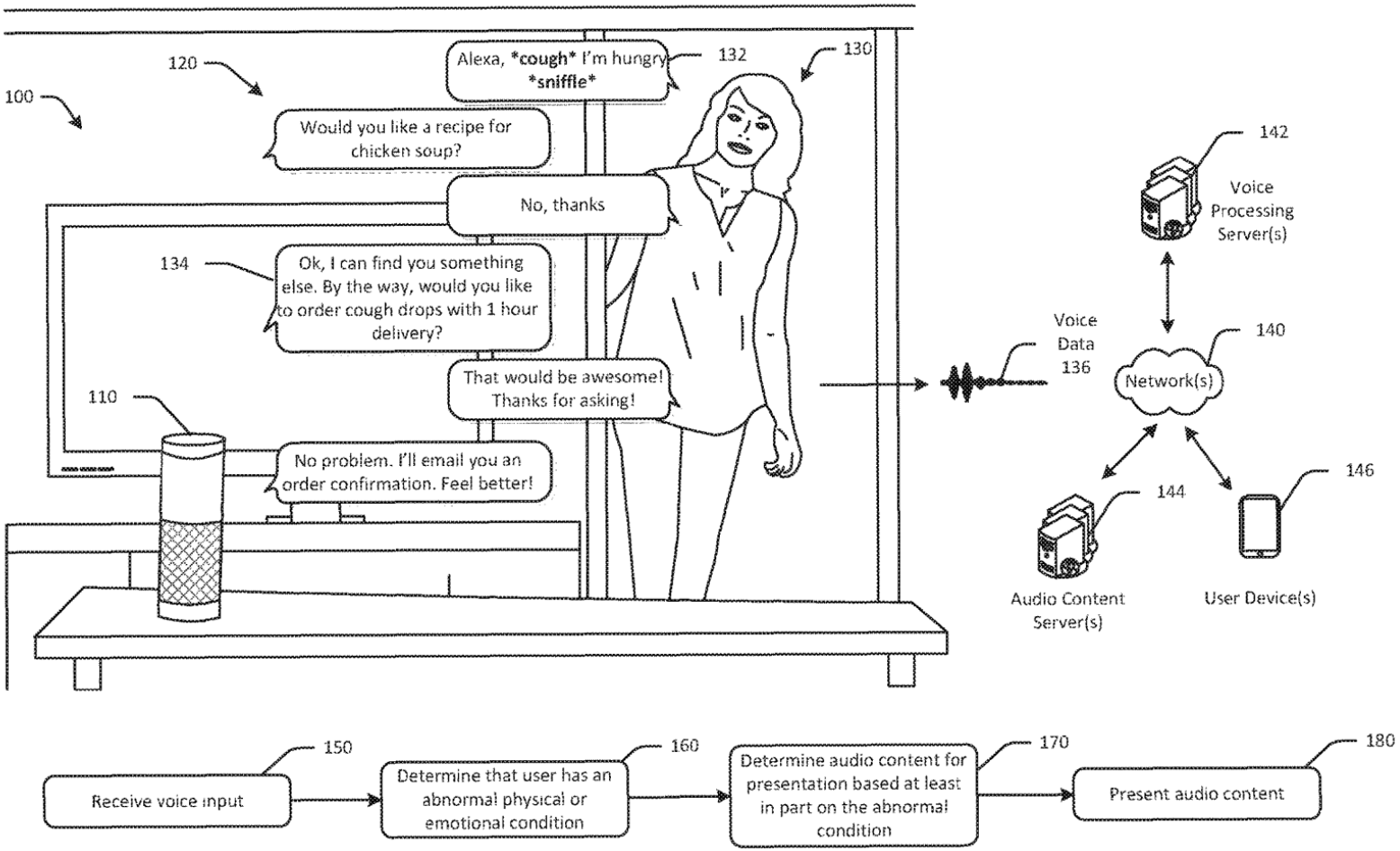
- Smart devices <u>need</u> sensors to observe the user, but might learn further private details as a coincidence

Voice-based determination of physical and emotional characteristics of users

United States Patent 10,096,319

October 9, 2018

Amazon Technologies, Inc.



The Ugly: Security

- Does a device store/transmit WLAN credentials in plain text, uses hardcoded admin accounts or has backdoors?

Mashable.com, 2018

- Security issues that are not known from experience with non-smart devices, e.g., heating can be attacked remotely, causing bursted pipes in winter

Wall Street Journal, 2021

The Ugly: Market Issues (again)

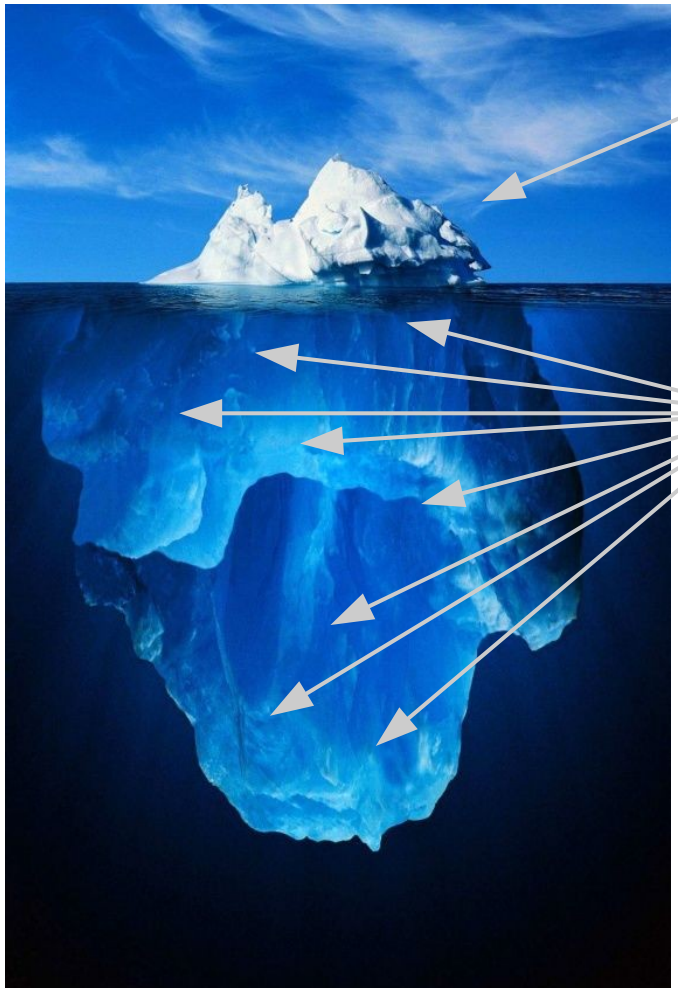
- Shifted liablities
  - If user does not accept an update and smart device blows up, it is the users fault
- Incentive to sell unfinished products
  - Over-the-air updates to fix issues after time of purchase
- Skills and expertise of the manufacturers?
  - Manufactuers, who are good with physical products, aren‘t necessarily good on the Internet.
  - Manufactuers, who are good on the Internet, aren‘t necessarily good with physical products.
- Immature regulatory environment
  - e.g., EU 2019/771 Regulation requires 2 years of security updates, starts 2023 (avg. lifespan of laundry machines: 11 years)

E. Buchmann. "Privacy-aware and Reliable Sensor-data Management." Habilitation Thesis, Karlsruhe Institute of Technology, 2016.

Intermediate Conclusion

- Technical perspective: No new challenges for privacy and security
  - IoT uses well-known protocols, system architectures, services, …

- However, IoT devices are used differently, and have a much higher system complexity, than its non-smart prede-cessors



User Interface/
User Expectations

Privacy and
Security Issues

Polarstern Luzern

Outline of this Talk

- Motivation
- **Identifying the Risks**
- Securing a Smart Home
- Anonymous IoT Devices
- Conclusion

E. Buchmann, A. Harmann. „Identifying Long-Term Risks of the Internet of Things“. UBICOMM 2020

We need a Risk Catalog!

- **Operational lifespan of traditional devices**
  - Depends (mostly) on hardware
- **Operational lifespan of smart devices**
  - Depends on hardware and IT ecosystem
  - Involves third parties for cloud services, updates, subscriptions, ...
  - Involves politics (cf. trade wars w. 5G suppliers, Brexit, GDPR, ...)
  - Might be surprisingly short due to high total system complexity

→ Without knowing **all** risks during the *entire* life cycle, it is impossible to build maturity models / make informed procurements / manage privacy issues / develop security strategies / ...

- *<u>Research problem:</u> Which specific risks for the continued long-term use of smart devices may materialize after purchase, but cannot be expected from a smart device's non-smart predecessor?*
  → Suitable **method**? Research **results**?

Research Method (1/4)

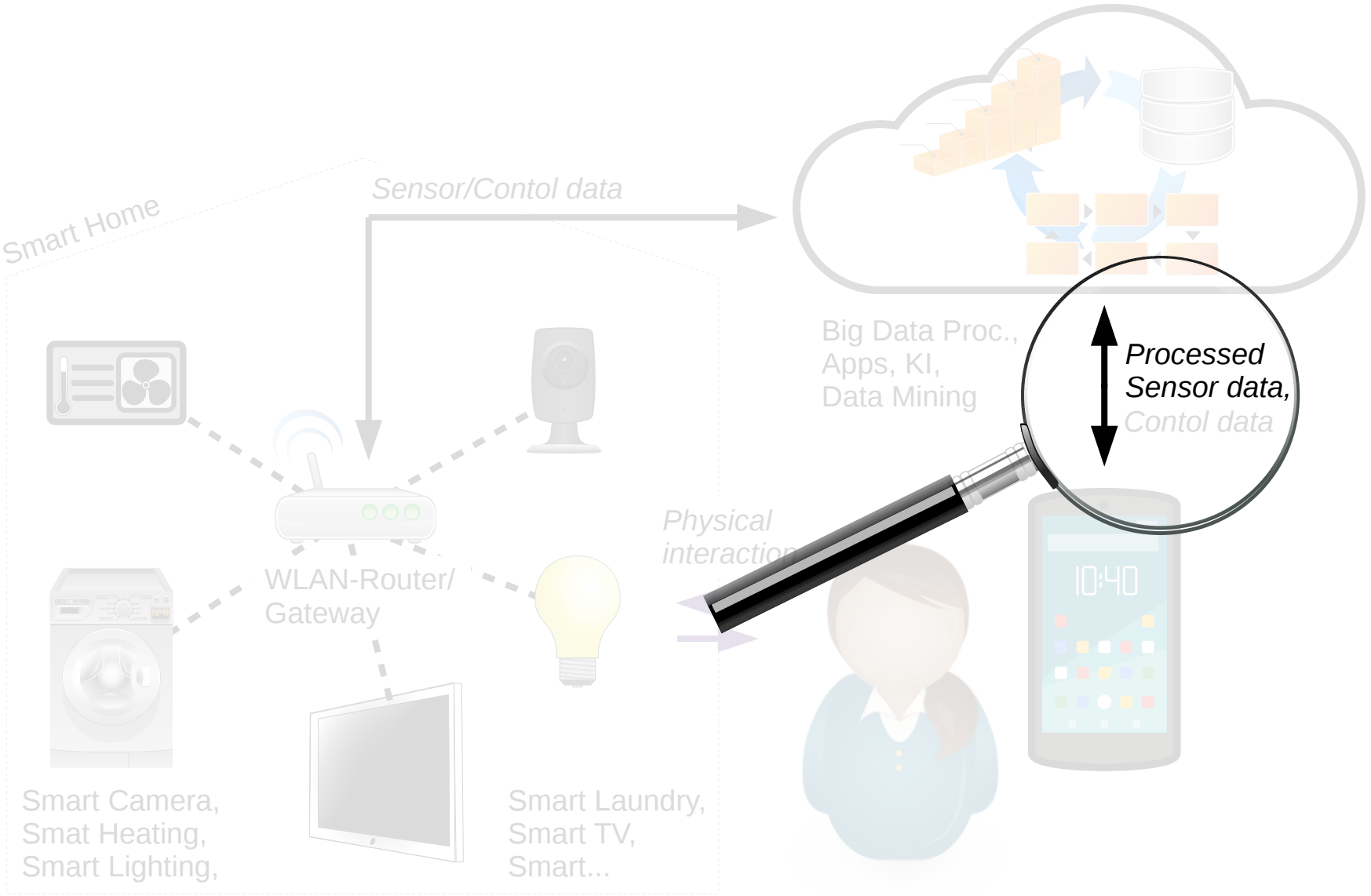
Running Example: A smart security camera, which connects to a cloud in UK via WLAN, the cloud service processes videos and sends burglar alerts to the user's mobile phone

- **Step 1:** Determine a number of relevant use cases. Model a generic IT infrastructure that fulfils the requirements for (a) a smart device and (b) its non-smart counterpart to operate as intended.

  Infrastructure Model:

  - Data*: Sensor data, operational data, meta-data, configuration*
  - Orga*: User, vendor, cloud service operator, network provider*
  - Processes*: Recording, processing, alerting, storing, updates*
  - Devices*: Camera, cloud, mobile phone*
  - Connections*: Camera-cloud, cloud-smartphone*

Running Example: Risks for Sensor-Data Connection between Cloud and external Device



Research Method (2/4)

- **Step 2**: Analyze each fragment in the infrastructure for the smart device in isolation. Determine under which conditions this fragment operates as intended at time of purchase.

  Example fragment: Connection cloud-smartphone

  - *Exchange of personal sensor data (videos of persons) with cloud service must be legally possible*
    - *Changes in future versions of the GDPR?*
    - *Which regulations apply if the cloud service is operated in UK/USA? (Privacy Shield, Brexit, …?)*
    - *What if a future trade war disallows data transfers to some parties? (see TikTok in the USA)*
  - *(...)*

BiliaST (Pixabay License)

Research Method (3/4)

- **Step 3**: Consider a condition a potential risk, if
  (i) the condition doesn't exist at time of purchase and
  (ii) doesn't materialize in the non-smart device's infrastructure.

  Example: Exchange of personal sensor data (videos of persons) with cloud service must be legally possible

  - *With current legislation, data transfers are possible if the camera is operated in private spaces, and/or the persons in the videos are informed and/or have agreed*

  - *A non-smart security camera does not need a data connection to a cloud service*

    → *We have identified one risk that is specific for a smart device using a cloud service*

Research Method (4/4)

- **Step 4**: Consolidate risks that are identical for multiple artefacts. Categorize similar risks and remove elementary ones.

- **Step 5**: Back up each individual risk by literature in order to evaluate the plausibility of the risks identified.

- **Step 6**: Repeat these steps with different use cases until no further risks are identified.

  Final result: A catalog of risks that is

  - *Specific for the smart devices considered*
  - *Comprehensive, as it regards all infrastructure components*
  - *New, compared to the risks of non-smart devices with the same functionality*

Long-term **compliance** risks

Sensor data connection between cloud service and external device

Risk	Description
Legislation	Changing legislation, new codes of conduct, new trade restrictions etc. impose limitations on the exchange of personal data with certain countries or parties.
Expiration	Disagreements to common compliance standards, expired certifications or approvals, non-renewed audits, etc., render the connection untrusted.
Concealment	Characteristics, that were hidden at roll-out, ban the connection by law, e.g., if it becomes known that personal information is sent to external parties without the customers consent.

Long-term **economic** risks

Risk	Description
Degradation	For economic reasons the service quality of the connection will be reduced, e.g., by applying bandwidth throttling in favor of other services.
Licensing	The revenue model might change. For example, the external party might switch to a pay-per-use model which makes external connections expensive.
Discontinuation	One of the parties involved discontinues its service or makes it uneconomic. Patents, licenses etc. disallow to continue the service with other parties.
Liabilities	One of the parties involved discontinues its business, and its contractual liabilities become void.

Long-term **operational** risks

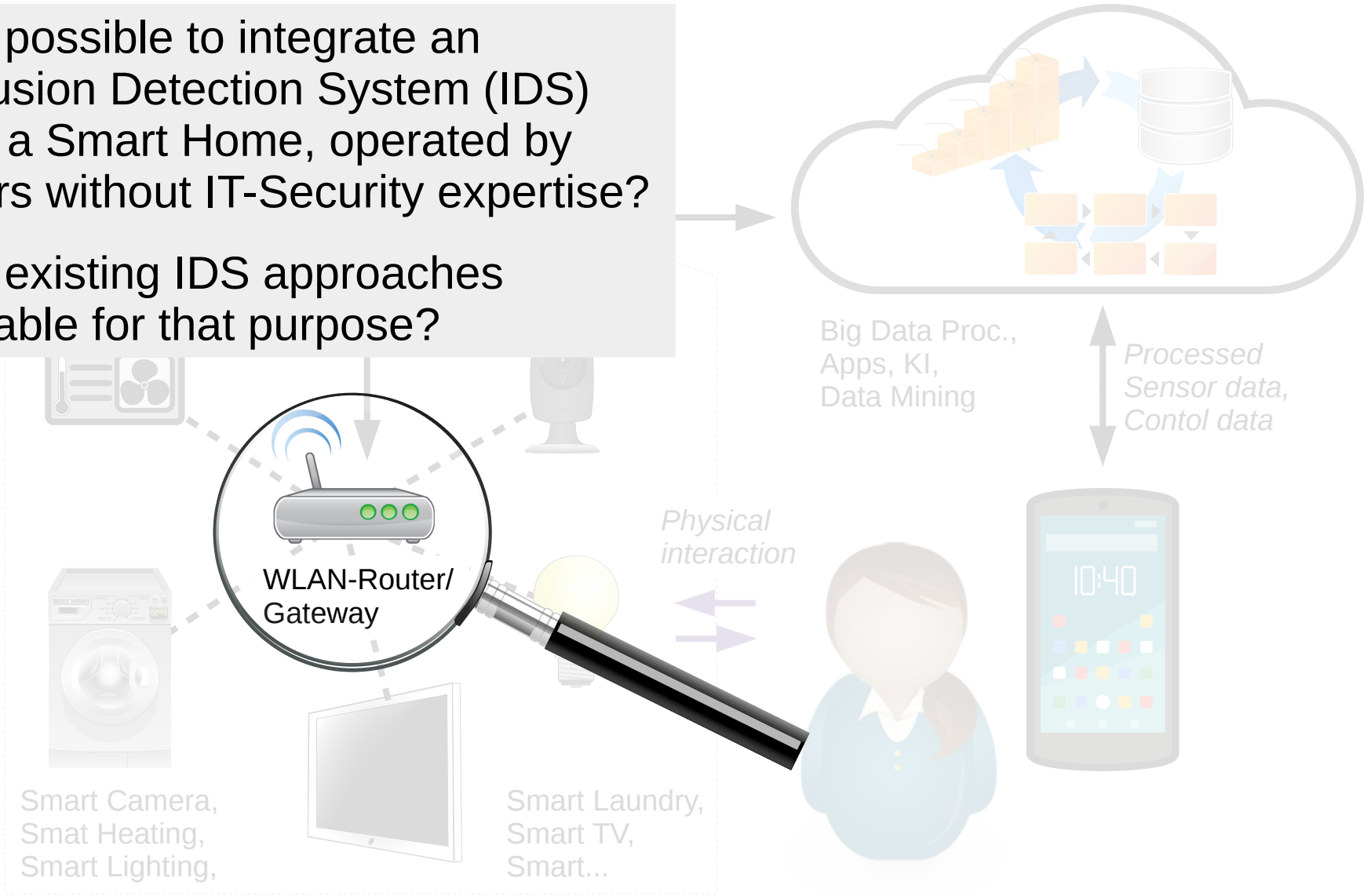
Risk	Description
Inflexibility	Without updates for new formats, protocols or interfaces, it becomes challenging to connect to more recent services or devices, or to adapt to new modes of service.
Unreliability	The service level in terms of reliability, throughput, etc. of the connection degrades, e.g., due to reduced support for end-of-lifetime products.
Unmaintainability	Due to the use of outdated formats, protocols or interfaces and closed-source components it becomes difficult to find experts or spare parts needed to that maintain the connection.
Insecurity	Without security updates and by using out-of-date security protocols, the connection does not meet the required level of security any more.
Defectiveness	Modernizations in the IT ecosystem make technical debts visible, e.g., if header fields reserved for future use in transmission protocols were not handled according to the standard.

Outline of this Talk

- Motivation
- Identifying the Risks
- **Securing a Smart Home**
- Anonymous IoT Devices
- Conclusion

Research Questions

1. Is it possible to integrate an Intrusion Detection System (IDS) into a Smart Home, operated by users without IT-Security expertise?
2. Are existing IDS approaches suitable for that purpose?



C. Haar and E. Buchmann, "FANE: A Firewall Appliance for the Smart Home," FedCSIS'19

Research Method

- Four levels are important for integration of IDS into smart homes:
  (IDS software can be left aside, because IoT bases on existing technology)

  1) Network Segmentation
  2) System Architecture
  3) IT-Security Process
  4) Contract Liabilities

Jordan Long

- Experiments with signature-based and anomaly-detecting (AI) IDS
  - Kitsune
  - Suricata

1) Network Segmentation

- A separate Segment for IoT devices
  - Simple solution from a technical perspective

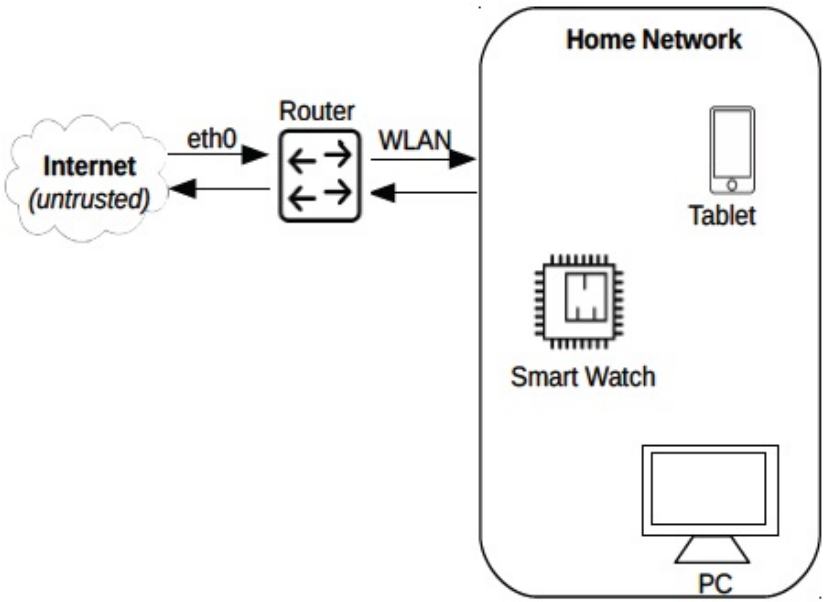


Figure 1: Typical Smart Home Architecture

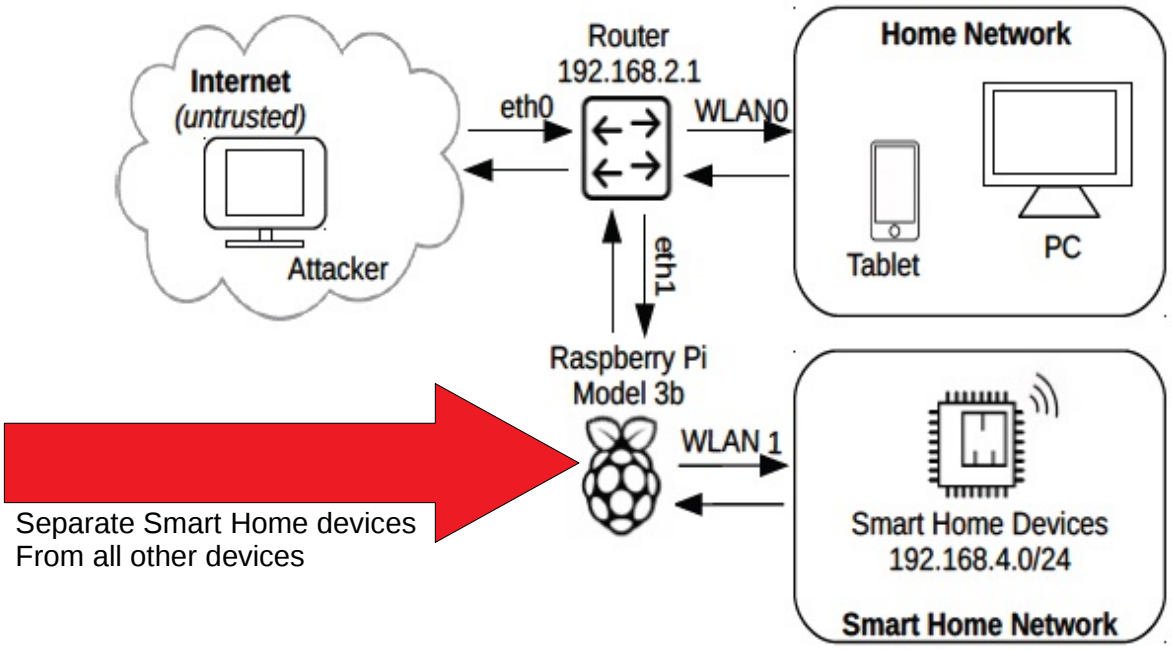


Figure 2: Experimental Smart Home Architecture

2) System Architecture

- IDS needs a reporting component that produces explainable reports
- If this is impossible, report must be sent to an expert (cf. next slide)

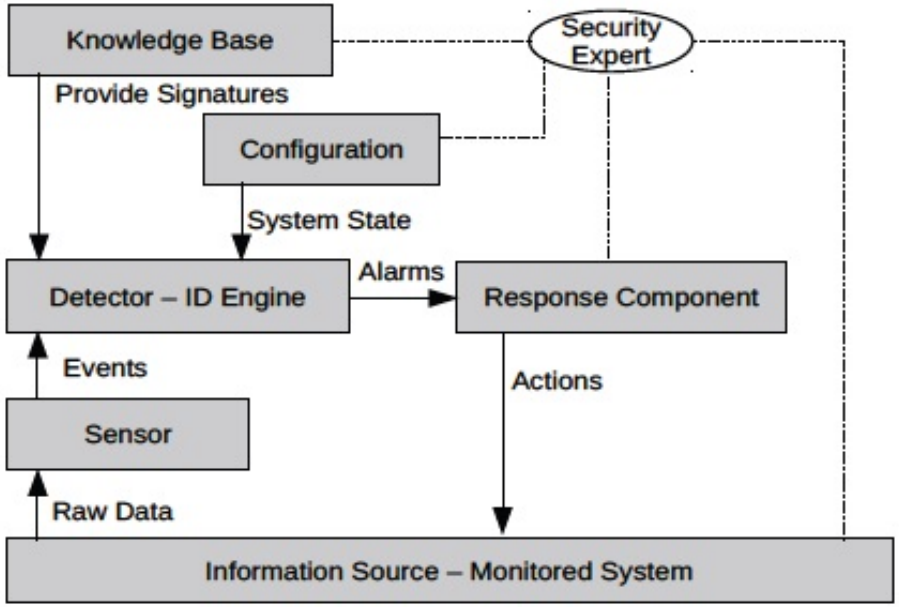


Figure 3: Existing IDS

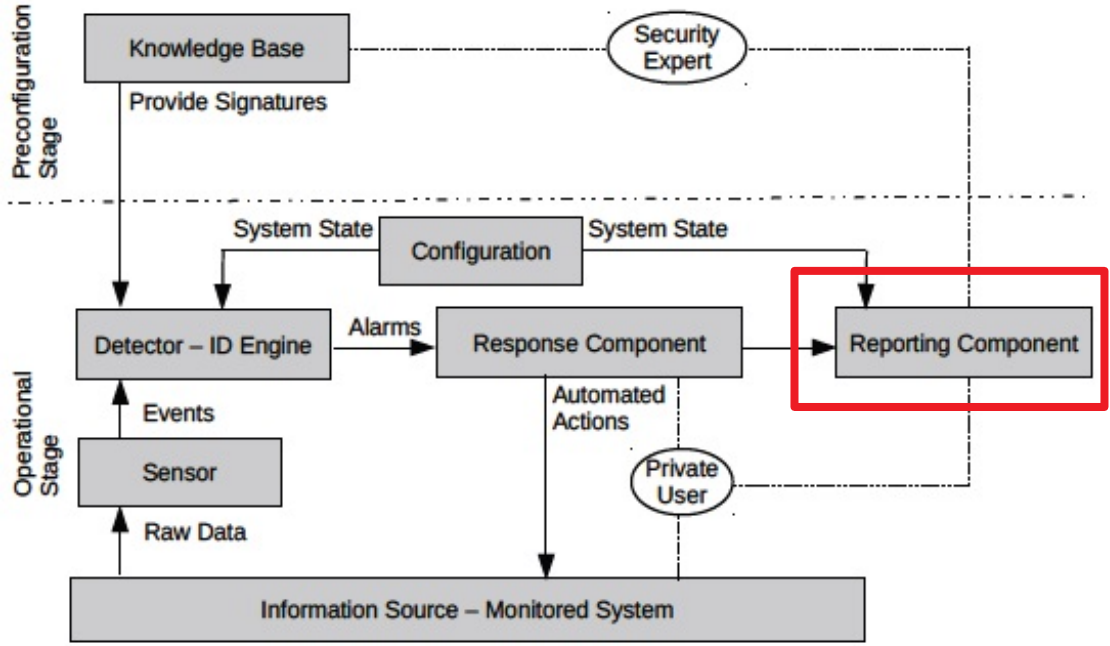


Figure 4: Smart Home IDS

3) IT-Security Process

- Responsibilities of the user
  - Install IDS, take (simple) countermeasures, otherwise call expert
- Responsibilities of a security expert
  - Pre-configure IDS, initiate non-automatic countermeasures

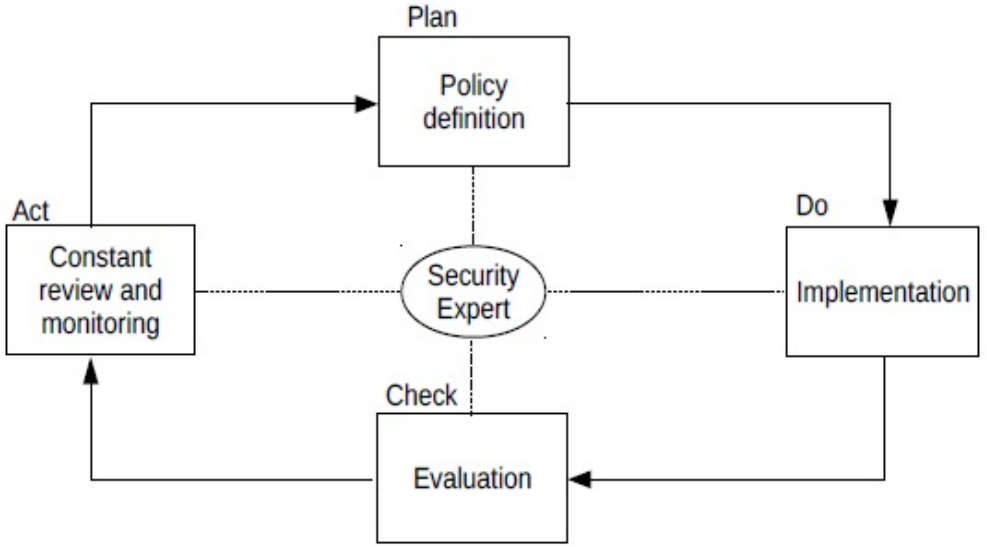


Figure 5: IT-Security Process

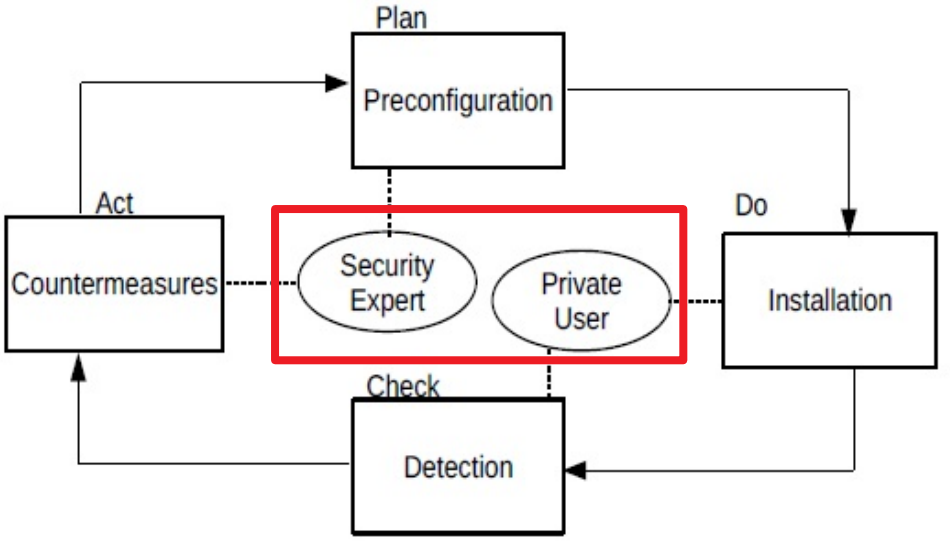


Figure 6: Adapted IT-Security Process

4) Contract Liabilities

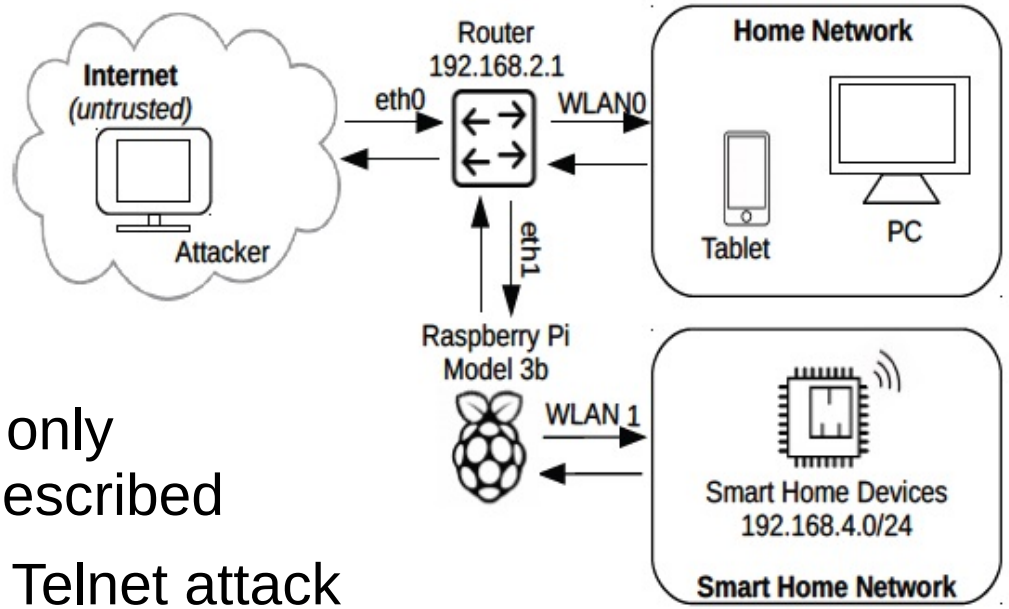
Traditional IDS

- Manufacturer is responsible for IDS software
- User is responsible for everything else

Our IDS Approach

- *Separation*: A Smart Home IDS must define a distinct service for all devices in the Smart Home network segment
- *Expertise*: IDS abilities must be specified without referring to certain transmission protocols, attacks, etc.
- *Understandability*: It must be clearly communicated to the user that an IDS does not offer a complete protection against any kinds of attack

Using existing IDS?



- IDS is installed on a Raspberry PI that spans a separate network for only IoT devices, security process as described
- Tests: Normal behavior, Portscan, Telnet attack
- Two different kinds of IDS:
  - Suricata:
    https://suricata.io
    - signature-based detection
    - implements state-of-the-art detection algorithms
    - starts with 27.000 preconfigured signatures and can be updated from a repository
  - Kitsune:
    https://github.com/ymirsky/Kitsune-py
    - anomaly detection
    - implements a number of neuronal networks
    - is installed with neuronal networks and a voting mechanism that are preconfigured

Test Results

- Amazon Dash button, Amazon Echo Dot, IoT temperature sensor, IP camera, each used for 60 minutes with and without attacks

(Signature-based) *(Anomaly detecting)*

- Normal use

		Suricata		**Kitsune**	
		Malicious	Benign	Malicious	Benign
Reality	Malicious	0	0	0	0
	Benign	0	112.602	43	112.559

- Portscan

		Suricata		**Kitsune**	
		Malicious	Benign	Malicious	Benign
Reality	Malicious	48	131.089	129.987	1.150
	Benign	0	106.472	178	106.294

- Telnet attack

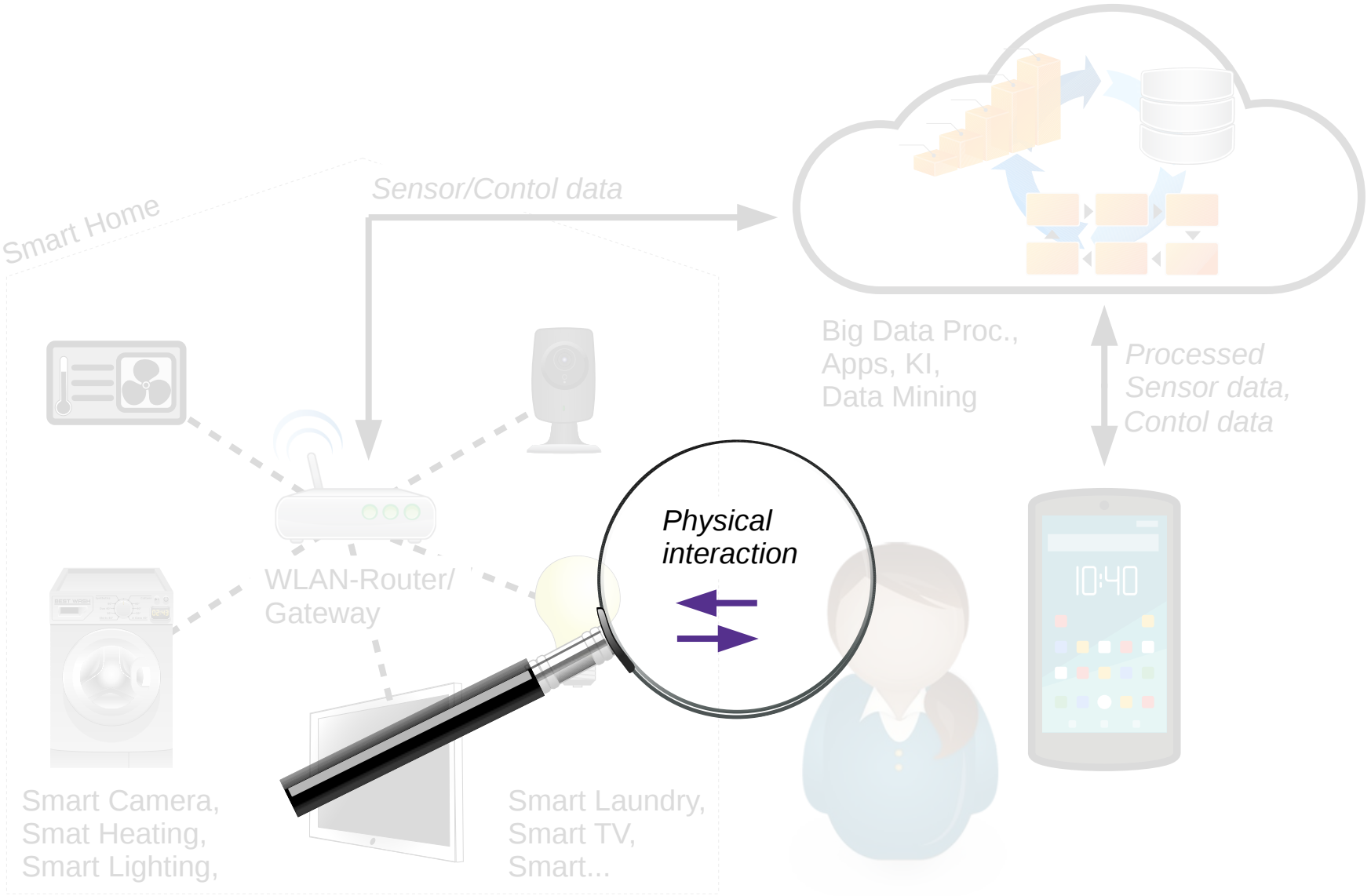
		Suricata		**Kitsune**	
		Malicious	Benign	Malicious	Benign
Reality	Malicious	1.117	0	0	1.117
	Benign	0	113.384	2.848	110.536

Our Conclusion: Signature-detecting IDS can be readily integrated into IoT setups, if an expert provides signatures in time.

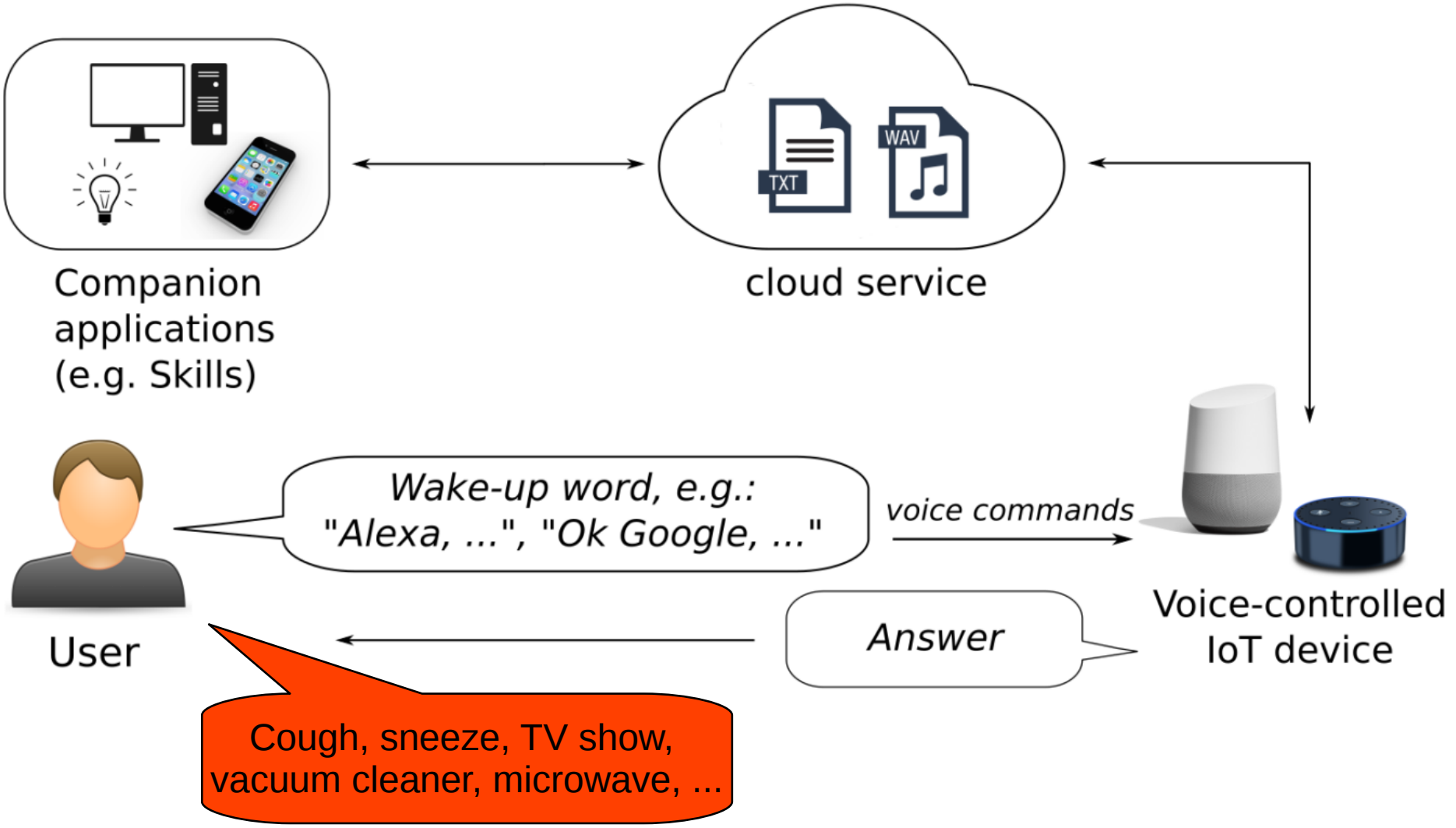
Outline of this Talk

- Motivation
- Identifying the Risks
- Securing a Smart Home
- **Anonymous IoT Devices**
- Conclusion

How much Privacy is Conceivable?



Example: Voice-controlled Smart Speakers



K. Winkler, E. Buchmann. "Dummy-based anonymization for voice-controlled IoT devices." UBICOMM 2018

Options to Anonymize Voice-Controlled Devices

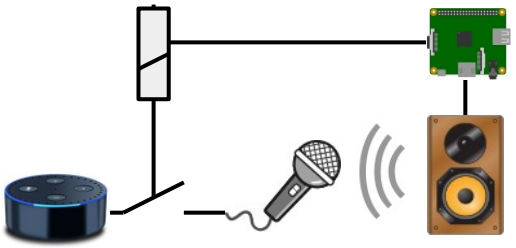
IoT device is closed source, any communication is encrypted

Option 1: **External anonymization** via speakers

- When the user is off the room, send spoken dummy commands by using an external speaker

Option 2: External **anonymization via relay**

- Disassemble IoT device, let an anonmization device turn on and off microphones and speaker
- Send spoken dummy commands via speaker

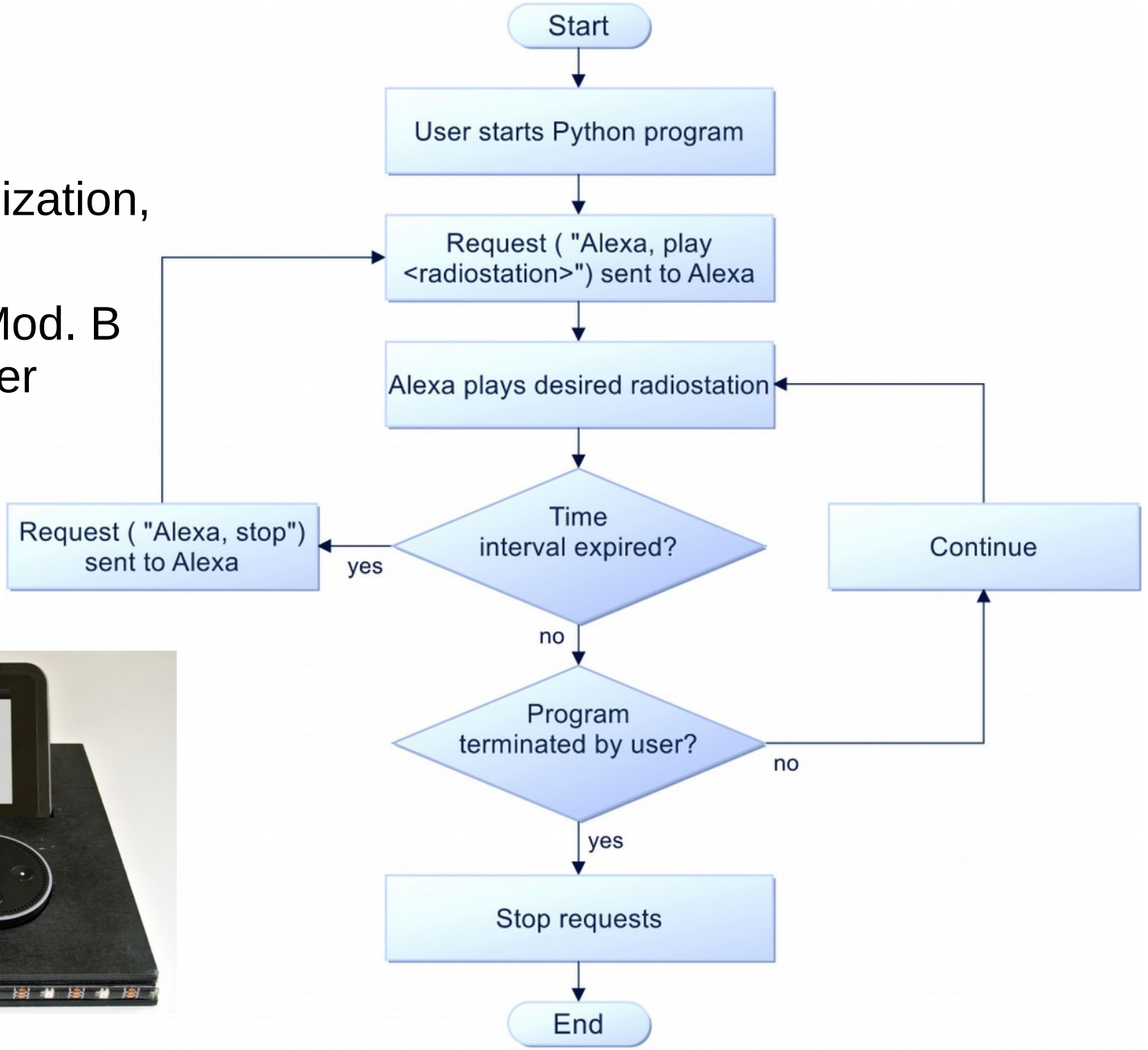


Option 3: **Re-wiring the IoT device**

- Directly connect all inputs and outputs of IoT device with the anonymization device, which synthesizes verbal commands

Our Prototype

- External anonymization, i.e., Option 1
- Raspberry Pi 3 Mod. B + external speaker (< 50 EUR)



Outline of this Talk

- Motivation
- Identifying the Risks
- Securing a Smart Home
- Anonymous IoT Devices
- **Conclusion**

Conclusion

Hochschule für Telekommunikation Leipzig
University of Applied Sciences

Prof. Erik Buchmann
Data Privacy and Security
buchmann@hft-leipzig.de

- IoT devices use well-known technology
  - Existing approaches usable to mitigate privacy and security issues,
- **BUT**: many aspects have a new/different *quantity*
  - System complexity, security and privacy risks, user expectations towards time of use, mode of use, usability, …
- Ideas to deal with this „**BUT“**?
  - Methods to obtain *comprehensive* risk catalogs
  - Security approaches that are *compatible* with IoT modes of use, i.e., can be applied by the persons using the device
  - Privacy approaches that *empower* the users of the device