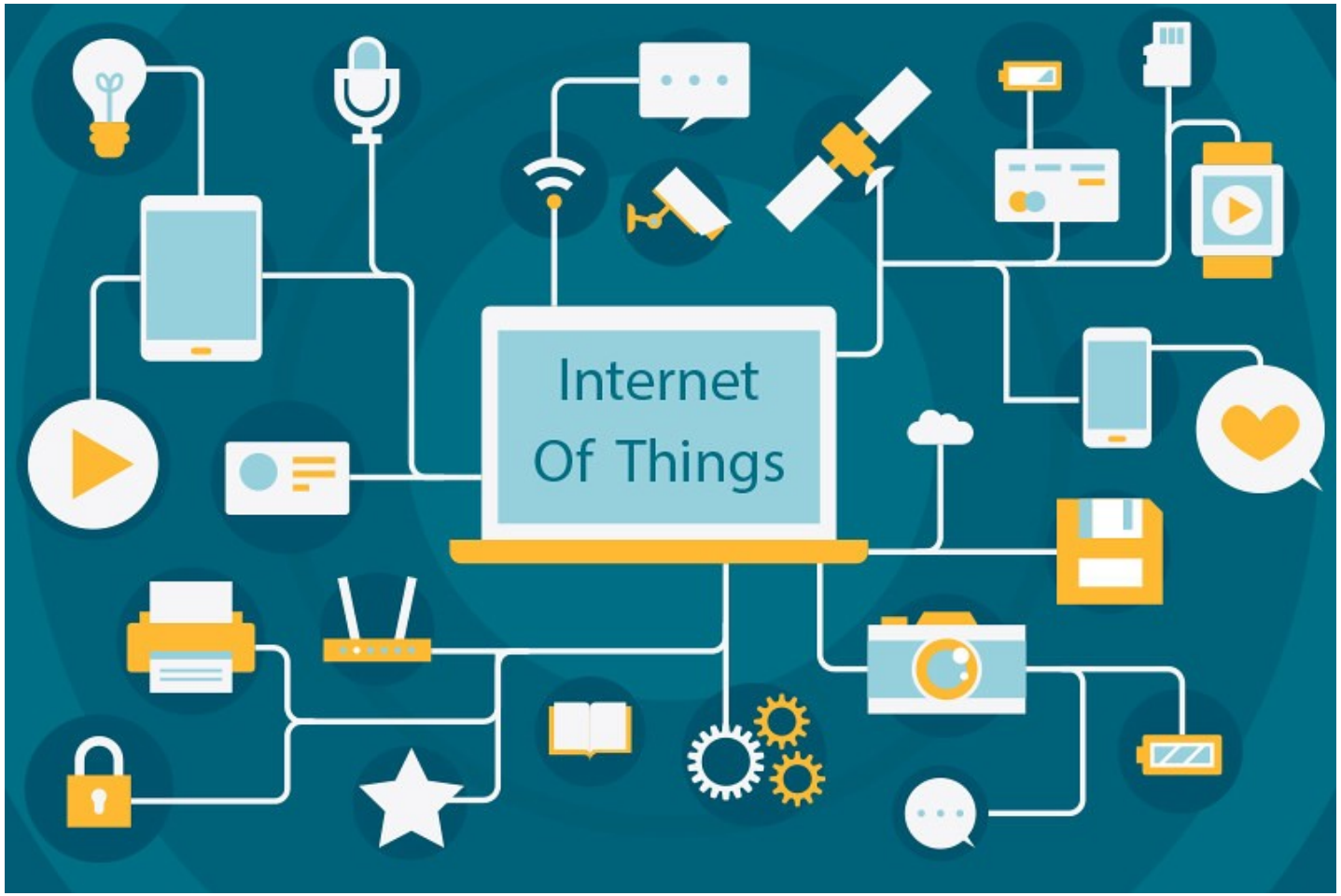
IDENTIFYING LONG-TERM RISKS OF THE INTERNET OF THINGS

Erik Buchmann, Andreas Hartmann (buchmann|hartmann@hft-leipzig.de)



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 in Information Systems

OUTLINE OF THIS TALK

- Motivation
- Problem Definition
- Research Method
- First results
- Conclusion

OBSERVATION

- Classical TV

makamuki0 (Pixabay License)

- *Primary function: show live TV*
- Operates ~15 years with
  - Power, antenna, TV mechanic, mostly standard spare parts

- Smart TV

Samsung (CC BY-NC-SA 2.0)

- *Primary function: show live TV*
- Operates ??? years with
  - Power, Internet, Netflix subscription, subscription support, model support, custom spare parts, cloud services, operating system updates, security updates, functional updates, …?

NUMEROUS SIMILAR EXAMPLES

- *Smart fridges, smart toothbrushs, smart security cameras, smart doorbells, smart vacuum cleaners, smart toys for children, smart thermostats, smart shutters, smart radios, smart lightbulbs, e-cars, smart electricity meters, smart watches, smart fitness gadgets, smartphone-controlled e-bikes/e-scooters, …*

- **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

OUR RESEARCH OBJECTIVE

A systematic research method to answer this question:

- ***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?***

  - Smart device: A device containing computational capabilities and data links not needed for the primary function of its non-smart prececessor
  - Long-term: The operational lifespan that can be expected from the device's hardware
  - Risk: A circumstance that makes the further use of the device impossible for technical, economic or regulatory reasons

RESEARCH METHOD (1/4)

<u>Running Example:</u> 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 smart device and its non-smart counterpart to operate as intended.

  Generic 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-mobile phone*

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 camera-cloud

  - *Transfer of personal sensor data (videos of persons) to the 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 the condition doesn't exist at time of purchase and doesn't materialize in the non-smart device's infrastructure.

  Example: Transfer of personal sensor data (videos of persons) to the 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

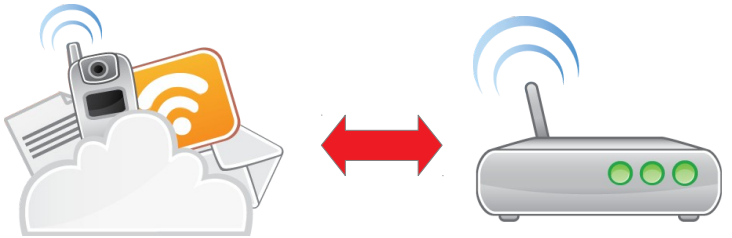
  - *Specific for the smart devices considered*
  - *Comprehensive, as it regards all infrastructure components*
  - *New, compared to the risks of non-smart devices with the same functionality*

PRELMINIARY RESULTS

- Our set of devices:
  1) Smart TV (Philips Ambilight 32PFS6402),
  2) Smart security camera (Reolink RLC-410)
  3) Smart speaker (Amazon Echo) with voice assistant.

- Infrastructure Model
  - 5 categories of data, 4 categories of organizations, 5 categories of processes, 3 categories of devices, 2 categories of connections

- Our focus for the moment
  - ***Bidirectional connection between cloud service and external device***



→ *Three categories of long-term risks* (see next slides)

(1) LONG-TERM *COMPLIANCE* RISKS

Bidirectional 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.

(2) LONG-TERM *ECONOMIC* RISKS

Bidirectional connection between cloud service and external device

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.

(3) LONG-TERM *OPERATIONAL* RISKS

Bidirectional connection between cloud service and external device

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.

DISCUSSION

- Our research method allows to identify *comprehensive* sets of risk for long-term operation of smart devices

- Recall that the risks shown in the last slides stem from only
  - three devices and
  - one fragment of the infrastructure model (connection between cloud service and external device)

  → *More is yet to come when continuing the research process for all fragments of the model and more devices*

CONCLUSION

Hochschule für Telekommunikation Leipzig
University of Applied Sciences

Prof. Erik Buchmann

Data Privacy and Security

buchmann@hft-leipzig.de

- The IT components of a smart device might impact the lifetime of the device
- To make a decision for a smart device, a comprehensive catalog of risks for the use of the device is needed
- Our contributions
  1) A research method to identify long-term risks
  2) Preliminary results for a fragment of a smart devices infrastucture
- Future work
  - Complete the risk catalog for all infrastructure fragments identified
  - Consider other smart devices to identify new fragments