OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

# A Security-, Privacy- and Usability- Scoring System for IoT Devices

Sebastian Fischer (OTH Regensburg)


CLOUD COMPUTING 2022 - April 24, 2022 to April 28, 2022 - Barcelona, Spain

OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

# Sebastian Fischer

| | |
|---|---|
| *2021 - present* | Lecturer at OTH Regensburg, Germany |
| *2015 - present* | PhD candiate at FU Berlin, Germany |
| *2018 - 2021* | Research Associate at Fraunhofer AISEC, Germany |
| *2015 - 2018* | Research Associate at OTH Regensburg, Germany |
| *2015* | M. Sc. Applied Research in Computer Science, OTH Regensburg |
| *2013* | B. Sc. Computer Science, OTH Regensburg |

sebastian.fischer@oth-regensburg.de

# Research topics

- Internet of Things Security
  - Security Standards
  - Device identification
  - Device Security
- Cybersecurity with the help of AI

# Cybersecurity Issues with IoT

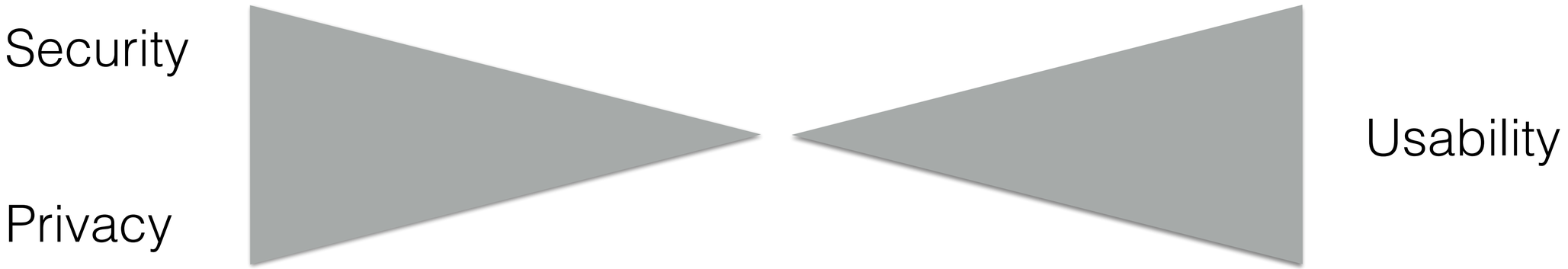
- A lot of security incidents in the last years with IoT devices [1]
- By outsourcing to the cloud, data is particularly at risk [2]
- The constant connection increases the attack surface area
- Botnets are the consequences [3] [4] [5]

# Security, Privacy and Usability

- The important points for the development of IoT and Cloud Applications are
  - **Security** - protection of data
  - **Privacy** - protection of private data
  - **Usability** - easy to use and understand

# Security, Privacy and Usability

- Security and privacy are not the same, but can often be combined
  - The less data is stored and forwarded (to the cloud), the more privacy and security you have
- Usability usually contrasts with security
  - e.g., the easier a login is, the less secure it usually is (not in every case)

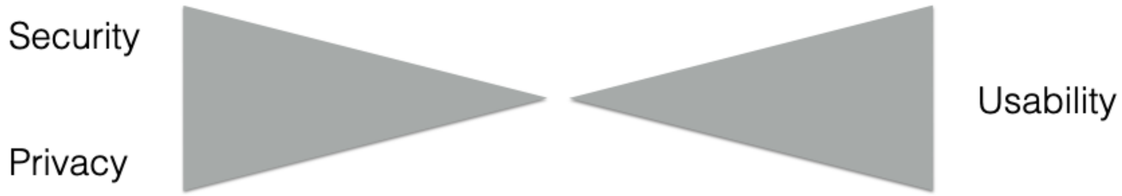


# Scoring System

- A Security-, Privacy- and Usability- Scoring System for IoT Devices is under development
- It should help the manufacturers to define the **requirements**
- Depending on the amount and type of data (e.g., private, personal), the score changes
- The individual scores enable a targeted focus

# Scoring System - Details

- Individual scores for: Security, Privacy, Usability
- Score Range: 0.00 to 1.00 (two decimals)
- The scoring changes with the different kind of application and data
- As a requirement, all scores can be high, but in practice not everything can be realized:



# Categories and Characteristics

Consumer IoT

Enterprise IoT

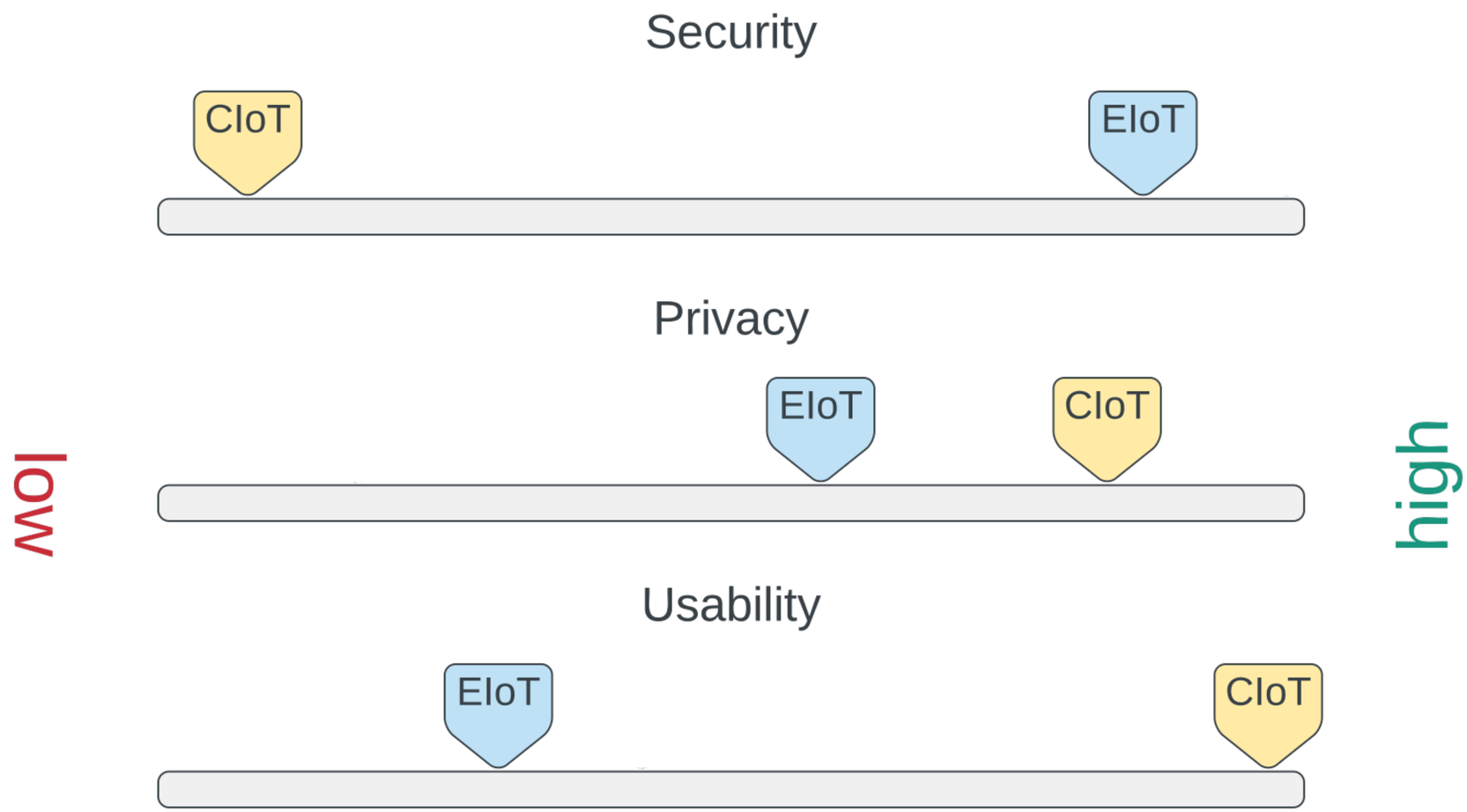
Industrial IoT

- **Characteristics:**
  - CI - Critical Infrastructure
  - PD - Private Data
  - SD - Sensitive Data
  - SY - Safety

# Example

- As Example, a networked baking oven is used
- The oven can be a Consumer or Enterprise product
- Depending on the application, the requirements in the areas of security, privacy and usability are different
- A device for a company can be more difficult to set up, as it is done by a professional. However, the requirements for security are higher, because if the device is attacked, it can cause more damage.

# Example


Security
CIoT
EIoT
Privacy
EIoT
CIoT
low
high
Usability
EIoT
CIoT

# Mapping Standards

- Depending on the score (requirement), different standards can be used
  - Consumer or Enterprise standard
  - Baseline requirements or advanced standard
- e.g., ETSI EN 303 645 - baseline requirement for consumer products (68 requirements) [6]
- e.g., IEC 62443 series - for industrial communication networks (263 requirements) [7] [8]

# Summary

- The scoring system …
  - is currently **work in progress**
  - should help to **select standards**
  - recalls the **importance** of **Security, Privacy** and **Usability**
  - is developed to show the **requirements**
- => Please give Feedback to help the research!

# References


- [1] Bundesamt fu¨r Sicherheit in der Informationstechnik (BSI), “Bericht zum Digitalen Verbraucherschutz 2020,” 2021, accessed on: 5- March-2022. [Online]. Available: https://www.bsi.bund.de/DE/Service- Navi/Publikationen/DVS-Bericht/dvs-bericht node.html
- [2] Luo, Xiangyang, L. Yang, Dai Hao, Fenlin Liu and Daoshun Wang. “On Data and Virtualization Security Risks and Solutions of Cloud Computing.” J. Networks 9 (2014): 571-581.
- [3] O. von Westernhagen, “Hide’n Seek: IoT-Botnetz mit Spionage-Skills,” 2018, accessed on: 24-January-2022. [Online]. Available: https://www.heise.de/security/meldung/Hide-n-Seek-IoT- Botnetz-mit-Spionage-Skills-3950938.html
- [4] D. Schirrmacher, “OMG-Botnet macht aus IoT-Ger¨aten Proxys,” 2018, accessed on: 24-January-2022. [Online]. Available: https://www.heise.de/security/meldung/OMG-Botnet-macht- aus-IoT-Geraeten-Proxys-3982037.html
- [5] M. Tremmel, “TORII - Neues IoT-Botnetzwerk ist gekommen, um zu bleiben,” 2018, accessed on: 24-January-2022. [Online]. Available: https://www.golem.de/news/torii-neues-iot-botnetzwerk- ist-gekommen-um-zu-bleiben-1809-136860.html?utm source=nl.2018- 10-01.html&utm medium=e-mail&utm campaign=golem.de-newsletter
- [6] European Telekommunikations Standards Institute (ETSI), “EN 303 645 - Cyber Security for Consumer Internet of Things: Baseline Require- ments,” European Standard, vol. 2.1.0, 2020.
- [7] International Electrotechnical Commission (IEC), “IEC 62443-4- 1,” Jan. 2018, accessed on: 5-March-2022. [Online]. Avail- able: https://www.vde-verlag.de/normen/0800517/din-en-iec-62443- 4-1-vde-0802-4-1-2018-10.html
- [8] K. Greuter, “Evaluating the quality of the international consumer IoT Cyber Security Standard,” June 2020, accessed on: 5-March-2022. [Online]. Available: http://essay.utwente.nl/82092/