

TAGESSPIEGEL
RERUM
COGNOSCERE CAUSAS

Digital
Edition

Future Energies

Science Match

2020



Marit Hansen

Landesbeauftragte für Datenschutz Schleswig-Holstein

Cybersicherheit und Datenschutz - vom Smart Meter bis zum Smart Home



SH_WLAN

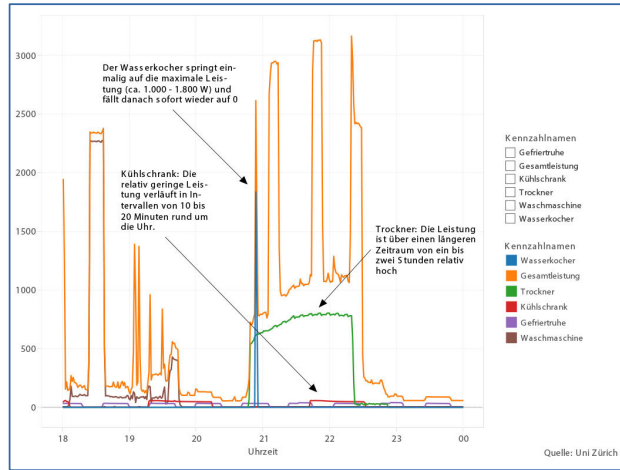


#sciencematch

Smart Meter – und der Datenschutz?

Datenschutzrisiken:

- Ausspähung des Haushalts via hochauflösender Verbrauchsmessung
- **Messwerte nicht genauer als viertelstündlich**
 - ▶ Immer noch sichtbar: Schlaf-/Wachzeiten, Kochverhalten, An-/Abwesenheiten, Veränderungen (Nachwuchs, Gäste)



<https://www.swr.de/swraktuell/smart-meter-datenschuetzer-warnen-der-spion-aus-der-steckdose/-/id=396/did=15941340/nid=396/1jgyd48/>

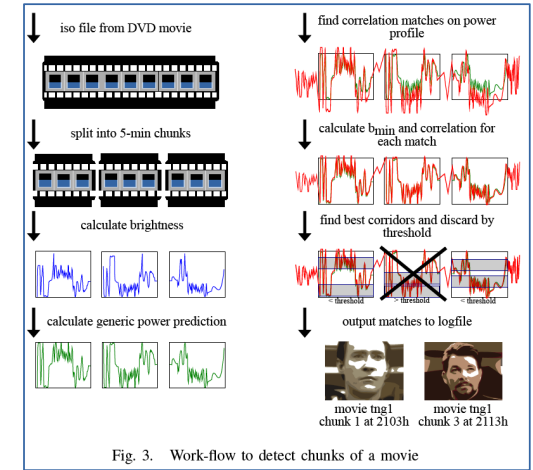


Fig. 3. Work-flow to detect chunks of a movie

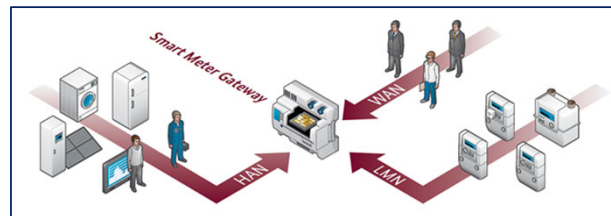
Quelle: Greveler, Ulrich, Benjamin Justus und Dennis Löhrl (2012). Forensic content detection through power consumption. In: IEEE International Workshop on Security and Forensics in Communication Systems, 6759-6763. Ottawa: IEEE Computer Society Press.

➤ Gesetz zur Digitalisierung der Energiewende

- ▶ U.a. klare Regelung, wer welche Daten zu welchem Zweck erhält; Löschfristen; Protokollierung der Datenübermittlungen; Pseudonymisierungen



<https://www.bfdi.bund.de/>



Quelle: Bundesamt für Sicherheit in der Informationstechnik

Sicherheitsrisiken:

- Unberechtigtes Fernauslesen
- **Sicherheit gemäß Schutzprofil und TR des BSI**
- Unberechtigtes Fernsteuern
- **Nicht via Smart Meter Gateway**

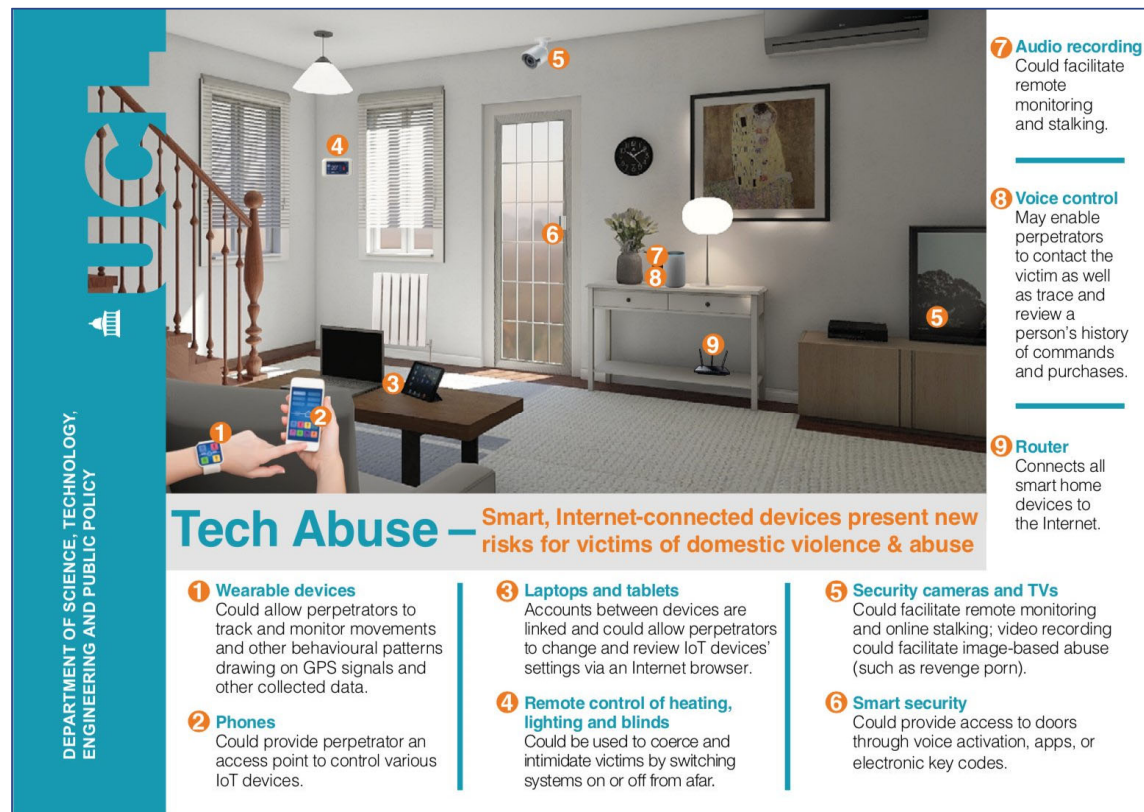
Herausforderung Smart Home

Smart Home:

- Immer wieder **neues Einfallstor** für Angriffe
- Z.B. „smarte **Glühlampe**“ als **Sprungbrett** bis hin zur Vollkontrolle
- Steuerung über „**Haus-Admin**“
- Risiken: Ausspähung, Vandalismus, Einbruch, Einsperren ...
- Auch neue Formen der häuslichen Gewalt

Fazit:

Mehr Datenschutz & Sicherheit by Design nötig



DEPARTMENT OF SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

Tech Abuse – Smart, Internet-connected devices present new risks for victims of domestic violence & abuse

- 1 Wearable devices**
Could allow perpetrators to track and monitor movements and other behavioural patterns drawing on GPS signals and other collected data.
- 2 Phones**
Could provide perpetrator an access point to control various IoT devices.
- 3 Laptops and tablets**
Accounts between devices are linked and could allow perpetrators to change and review IoT devices' settings via an Internet browser.
- 4 Remote control of heating, lighting and blinds**
Could be used to coerce and intimidate victims by switching systems on or off from afar.
- 5 Security cameras and TVs**
Could facilitate remote monitoring and online stalking; video recording could facilitate image-based abuse (such as revenge porn).
- 6 Smart security**
Could provide access to doors through voice activation, apps, or electronic key codes.
- 7 Audio recording**
Could facilitate remote monitoring and stalking.
- 8 Voice control**
May enable perpetrators to contact the victim as well as trace and review a person's history of commands and purchases.
- 9 Router**
Connects all smart home devices to the Internet.

<https://pbs.twimg.com/media/Ds7fJIPWsAA5t7G?format=jpg&name=large> (2019)
Leonie Tanczer, UCL, London - <http://www.csap.cam.ac.uk/network/leonie-tanczer/>

Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein

www.datenschutzzentrum.de