THE DOCTORAL DISSERTATION

JOSEPH BUGEJA

ON PRIVACY AND SECURITY
IN SMART CONNECTED
HOMES

MALMÖ UNIVERSITY

10 peer-reviewed publications

- On Privacy and Security Challenges in Smart Connected Homes
- An Analysis of Malicious Threat Agents for the Smart Connected Home
- Smart Connected Homes
- An Investigation of Vulnerabilities in Smart Connected Cameras
- Functional Classification and Quantitative Analysis of Smart Connected Home Devices
- An Empirical Analysis of Smart Connected Home Data
- On the Design of a Privacy-Centered Data Lifecycle for Smart Living Spaces
- Is Your Home Becoming a Spy? A Data-Centered Analysis and Classification of Smart Connected Home Systems
- A Privacy-Centered System Model for Smart Connected Homes
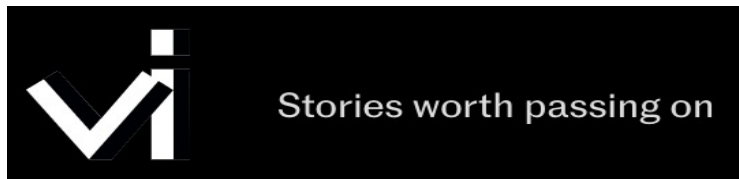- PRASH: A Framework for Privacy Risk Analysis of Smart Homes

MEDIA ATTENTION

dagens arena

ETC

NYHETER 24

EPOCH TIMES

Vi — Stories worth passing on

Förvaltarforum

Är ditt smarta hem säkert?

2021-04-29

Under det senaste decenniet har sakernas internet, eller Internet of Things (IoT), förändrat vår värld på många sätt, inte minst våra hem och fastigheter. Enligt den senaste prognosen kommer det att år 2025 finnas över 482 miljoner så kallade "smarta hem" världen över och antalet uppkopplade enheter kommer att överstiga 200 miljarder år 2030.

Detta beror delvis på de många fördelar som dessa tekniker erbjuder sina användare, som till exempel ökad bekvämlighet, energieffektivitet, trygghet och säkerhet.

Source: https://forvaltarforum.se

THE HOME IS WHERE THE HEART IS

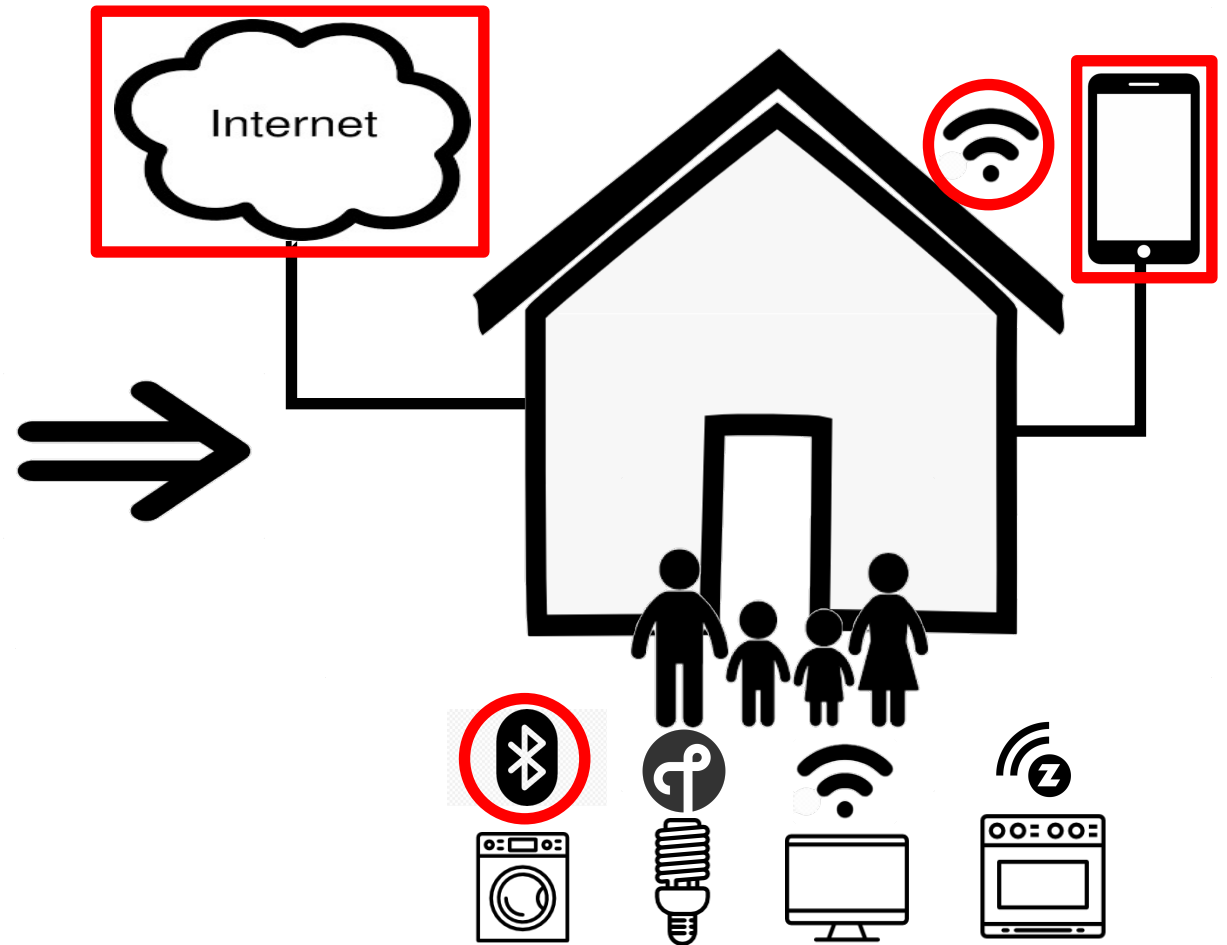The home is *the most powerful sign of the self of the inhabitant who dwells within*[1]

[1] Csikszentmihalyi M. & Halton. E., 1981. *The Meaning of Things: Domestic Symbols and the Self.*

EVOLUTION OF THE HOME

Traditional Home
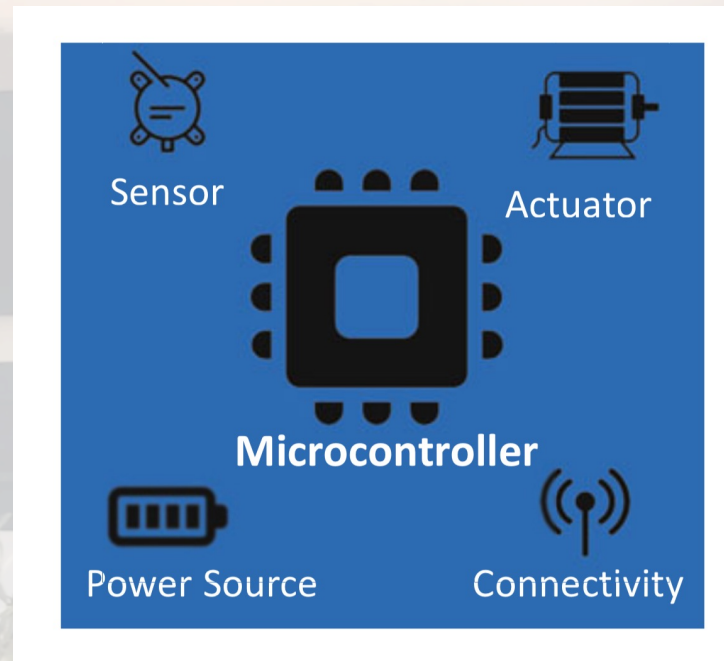
Smart Connected Home

Internet

THE SMART CONNECTED HOME

THE SMART CONNECTED HOME

The home appliances and hardware have become computers

PRIVACY AND SECURITY THREATS

- A smart TV might watch us back

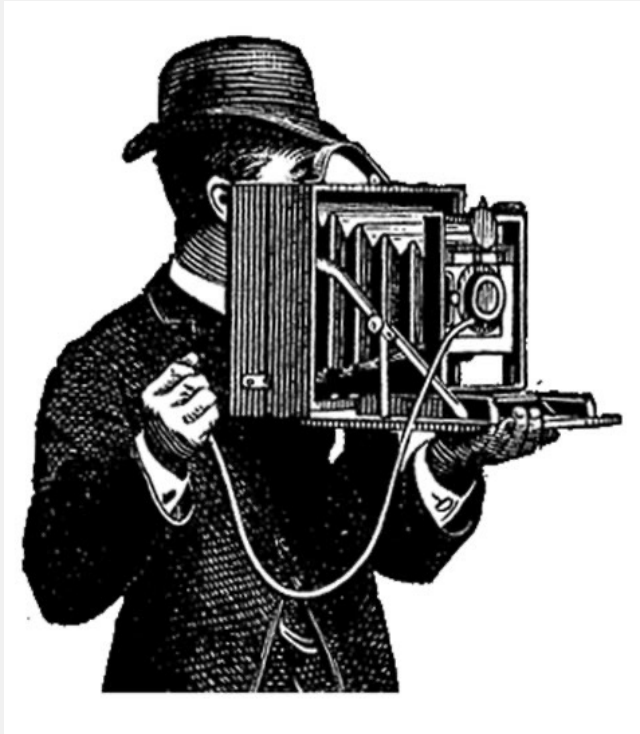- A smart speaker might listen to our intimate and sensitive conversations

- A smart thermostat might detect our behaviors and activities

#SOTEU

If everything is connected, everything can be hacked.

European Commission President Ursula von der Leyen delivers 'State of the European Union' speech at the European Parliament in Strasbourg, France, 15 Sep 2021

PRIVACY

PRIVACY AND SECURITY

PRIVACY AND SECURITY

Art. 32 GDPR "Security of processing." This requires that personal data must be processed securely using appropriate technical and organisational measures.

How has the nature of privacy and security been transformed as the home got connected to the Internet?

TAXONOMY AND ANALYSIS
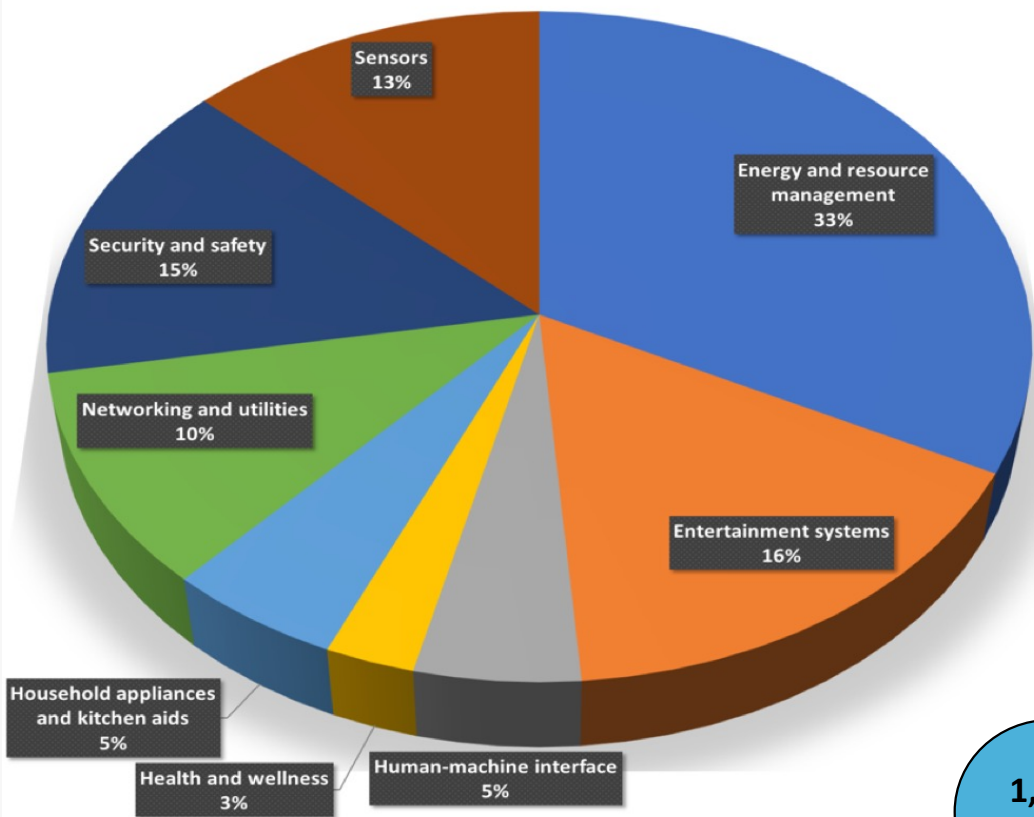
1,193 devices
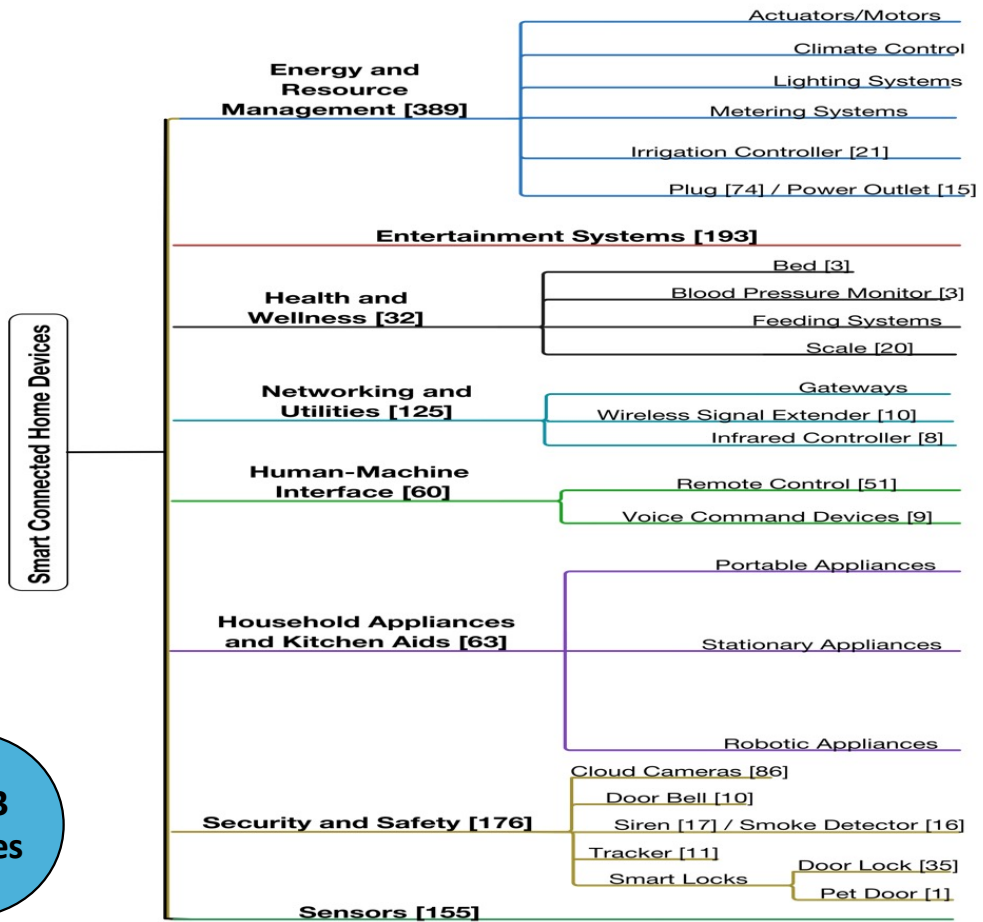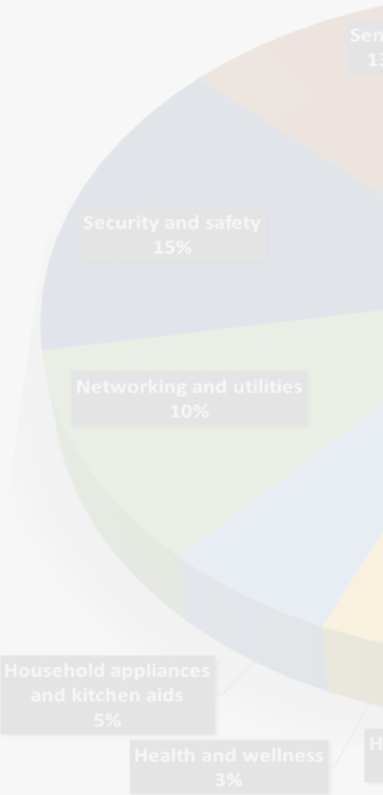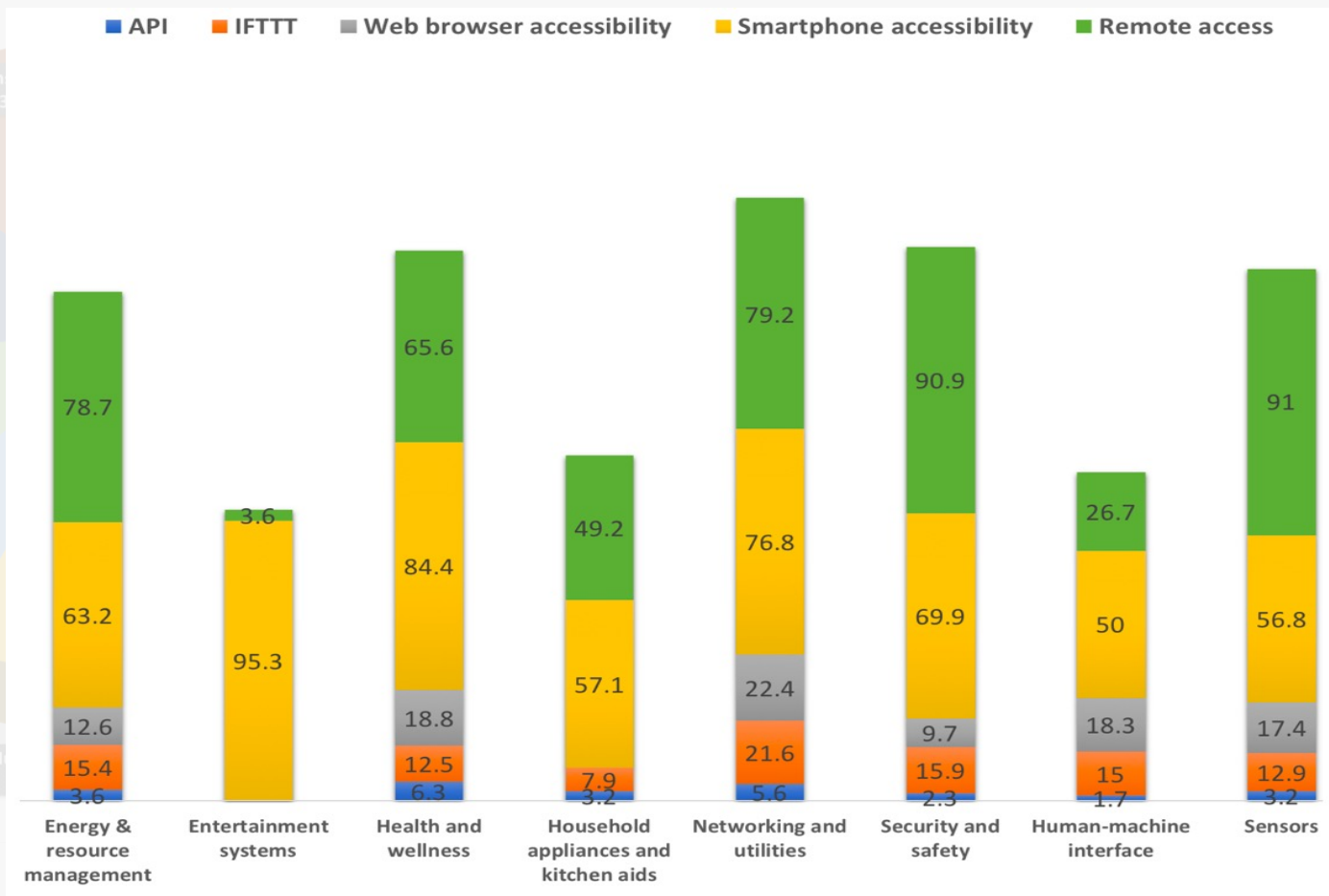
Bugeja, J., Davidsson, P., Jacobsson, A. (2018). Functional Classification and Quantitative Analysis of Smart Connected Home Devices (pp. 1–6). In: *Proceedings of the Global IoT Summit (GloTS 2018)*. IEEE.

TAXONOMY AND ANALYSIS

Bugeja, J., Davidsson, P., Jacobsson, A. (2018). Functional Classification and Quantitative Analysis of Smart Connected Home Devices (pp. 1–6). In: *Proceedings of the Global IoT Summit (GIoTS 2018)*. IEEE.

CLASSIFICATION OF SYSTEMS

81 systems

Energy and resource management

Entertainment systems

Health and wellness

House appliances and kitchen aids

Human-machine interface

Security and safety

App-based accessors Watchers Location harvesters Listeners

Optimal number of clusters

Gap statistic (k) vs Number of clusters k

Bugeja, J., Jacobsson, A., Davidsson, P. (2020). Is Your Home Becoming a Spy? A Data-Centered Analysis and Classification of Smart Connected Home Systems. In: *Proceedings of the 10th International Conference on the Internet of Things (IOT 2020)*. ACM.

DATA CATEGORIZATION

Login ids, Passwords, Body metrics, … — **Personal and Account Details**

Contact Information — Email, Phone, Address, …

Feedback, Demographic data, Comments, … — **User-Generated Content**

Configuration Settings — Operating schedules, Language preferences, Contact preferences, …

Card numbers, Expiration dates, Security codes, … — **Financial Information**

User Activity Data — Voice commands, Features accessed, Activity duration, …

Room location, User location, GPS, … — **Location Information**

Offline Data — CCTV footage, Phone conversation, Offline interaction, …

MAC address, Network related, Software versions, … — **Device Information**

Environmental Data — Motion, Humidity, Ambient light, …
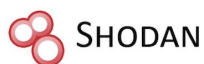
Bugeja, J., Jacobsson, A., Davidsson, P. (2018). An Empirical Analysis of Smart Connected Home Data (pp. 134–149). In: *Proceedings of the Internet of Things (ICIOT 2018). Lecture Notes in Computer Science,* vol 10972. Springer.

VULNERABILITIES IN CONNECTED CAMERAS

SHODAN

{Threat Agent :: Hacker}

National Interests

Terrorism

Personal Gain

Curiosity

Property Name	Value
area_code	null
asn	AS6830
city	Gelsenkirchen
country_code	DE
country_code3	DEU
country_name	Germany
data.0._shodan.crawler	264b5a9d15a64f96a4768e9d8081b
data.0._shodan.id	null
data.0._shodan.module	rtsp-tcp
data.0.data	RTSP/1.0 200 OK CSeq: 1 Server: Hipcam RealServer/V1.0 Public: OPTIONS,DESCRIBE,SETUP,TEARDOWN,PLAY,SET_PARAMETER,GET_PARAMETER
data.0.domains	['unitymediagroup.de']

62.

ip	104
ip_str	62.
isp	Unitymedia
last_update	2018-03-20T19:29:37.676273
latitude	51.5221
longitude	7.0575
org	Unitymedia
os	null
ports	[554]
postal_code	
region_code	07

High
CVE-2007-5213

Medium
CVE-2011-5261

Critical
CVE-2015-2887

Hackers   Thieves   Hacktivists   Competitors and Organized Crime   Terrorists   Nation States

An Investigation of Vulnerabilities in Smart Connected Cameras (pp. 537–542). In: *Proceedings of the International Conference on Pervasive Computing and Communications Conference (PerCom Workshops 2018).* IEEE.

PRIVACY-CENTERED *SYSTEM MODEL*
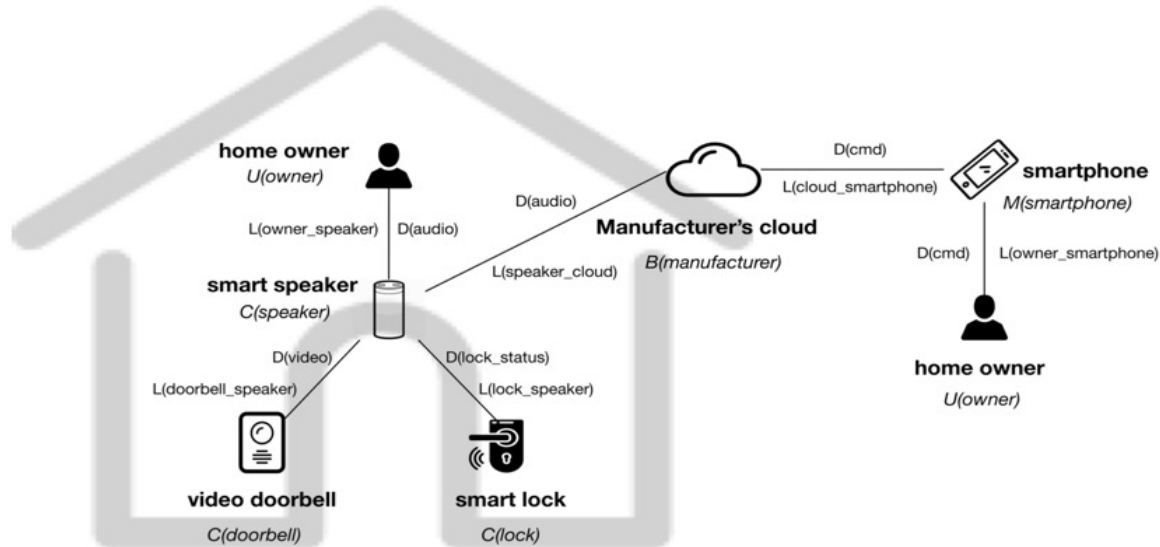
Nodes, $N = \{doorbell, lock, speaker, manufacturer, smartphone\}$
$C(speaker).capabilities =$
$\{gateway, storage, processing, interaction\}$
$B(manufacturer) = cloud$

Policy, $P =$
$\{(doorbell\_speaker, \{(video, \{read\})\}, doorbell, speaker, \emptyset),$
$(lock\_speaker, \{(lock\_status, \{read\})\}, lock, speaker, \emptyset),$
$(speaker\_cloud, \{(audio, \{read\})\}, speaker, manufacturer,$
$\quad Time = \{8:00 - 24:00\} \wedge Location = \{house\}),$
$(cloud\_smartphone, \{(cmd, \{read\})\}, smartphone,$
$\quad manufacturer, \emptyset),$
$(owner\_smartphone, \{(cmd, \{read\})\}, owner, smartphone, \emptyset),$
$(owner\_speaker, \{(audio, \{read\})\}, owner, speaker, \emptyset)\}$

Identification

Localization and Tracking

Profiling

○ **Threat does not exist**

◑ **Threat is a potential future threat**

● **Threat is present**

Bugeja, J., Jacobsson, A., Davidsson, P. (2020). A Privacy-Centered System Model for Smart Connected Homes (pp. 1–4). In: *Proceedings of the International Conference on Pervasive Computing and Communications Conference (PerCom Workshops 2020).* IEEE.

PRIVACY RISK ANALYSIS OF SMART HOMES

Bugeja, J., Jacobsson, A., Davidsson, P. (2020). PRASH: A Framework for Privacy Risk Analysis of Smart Homes. Sensors 2021, 21(19), 6399.
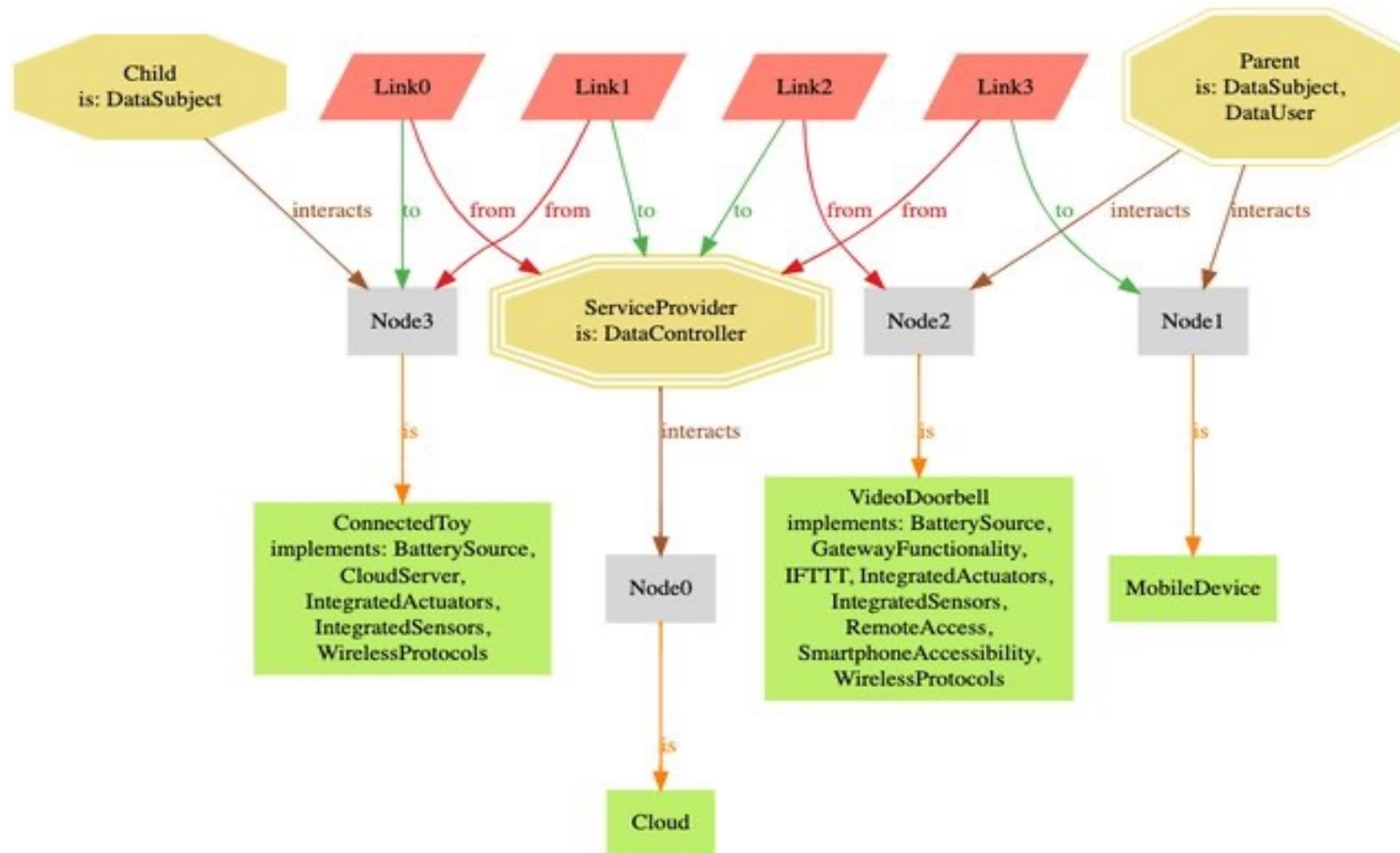
PRIVACY RISK ANALYSIS OF SMART HOMES
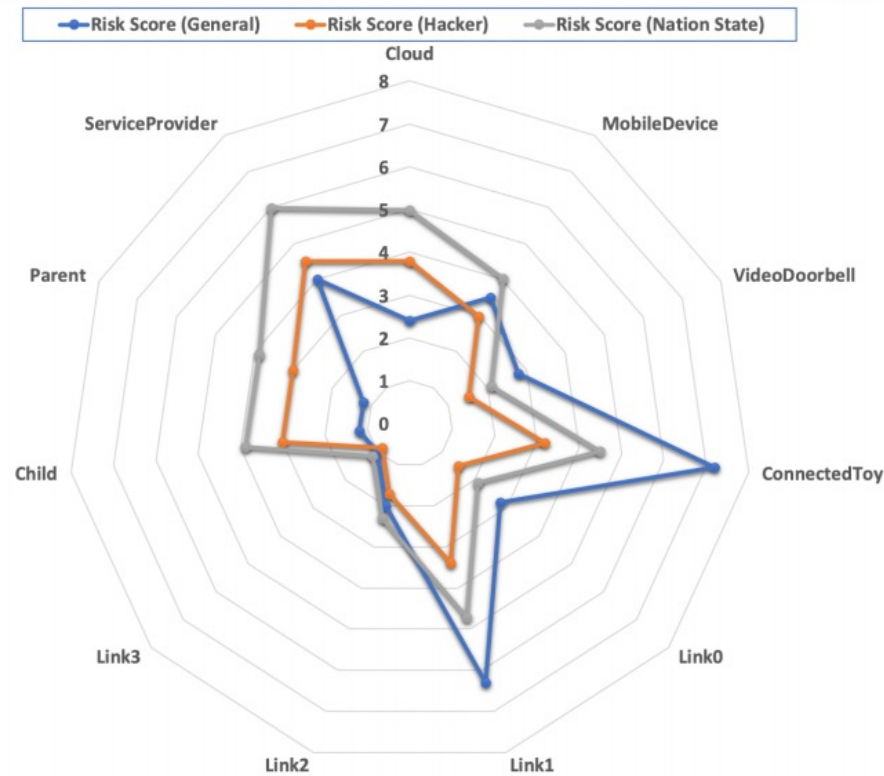
$$\alpha_l = \begin{cases} \prod_{i=1}^{n} \alpha_{l.i}, & \text{if } AND \text{ node} \\ max(\alpha_{l.i}), i = 1 \ldots n, & \text{if } OR \text{ node} \end{cases}$$

$$\alpha_{l.ta} = \frac{e^{ta_p - \alpha_l}}{1 + e^{ta_p - \alpha_l}}$$

$$\alpha_i = max(\alpha_{i.i}), i = 1 \ldots n, \text{ for both } AND \text{ or } OR \text{ node}$$

$$r_\mu = \alpha_{l.\mu} \times \alpha_{i.\mu}, \mu = 1 \ldots n$$

Bugeja, J., Jacobsson, A., Davidsson, P. (2020). PRASH: A Framework for Privacy Risk Analysis of Smart Homes. Sensors 2021, 21(19), 6399.

PRIVACY-CENTERED DATA LIFECYCLE

Information privacy threats	Protection goals	Data generation	Data collection	Data processing	Data disclosure
Identification	Unlinkability	◐	◐	●	○
Localization and tracking	Unlinkability	◐	◐	●	○
Profiling	Unlinkability	○	◐	◐	●
Linkage	Unlinkability	○	◐	◐	●
Privacy-violating interaction and presentation	Confidentiality	●	○	○	●
Inventory attacks	Detectability	○	●	○	○
Lifecycle transitions	Transparency	○	●	○	○

Bugeja, J., Jacobsson A. (2020). On the Design of a Privacy-Centered Data Lifecycle for Smart Living Spaces (pp. 126-141). In: *Friedewald M., Önen M., Lievens E., Krenn S., Fricker S. (eds) Privacy and Identity Management. Data for Better Living: AI and Privacy. Privacy and Identity 2019. IFIP Advances in Information and Communication Technology*, vol 576. Springer.

PRIVACY-CENTERED DATA LIFECYCLE

Bugeja, J., Jacobsson A. (2020). On the Design of a Privacy-Centered Data Lifecycle for Smart Living Spaces (pp. 126-141). In: *Friedewald M., Önen M., Lievens E., Krenn S., Fricker S. (eds) Privacy and Identity Management. Data for Better Living: AI and Privacy. Privacy and Identity 2019. IFIP Advances in Information and Communication Technology*, vol 576. Springer.
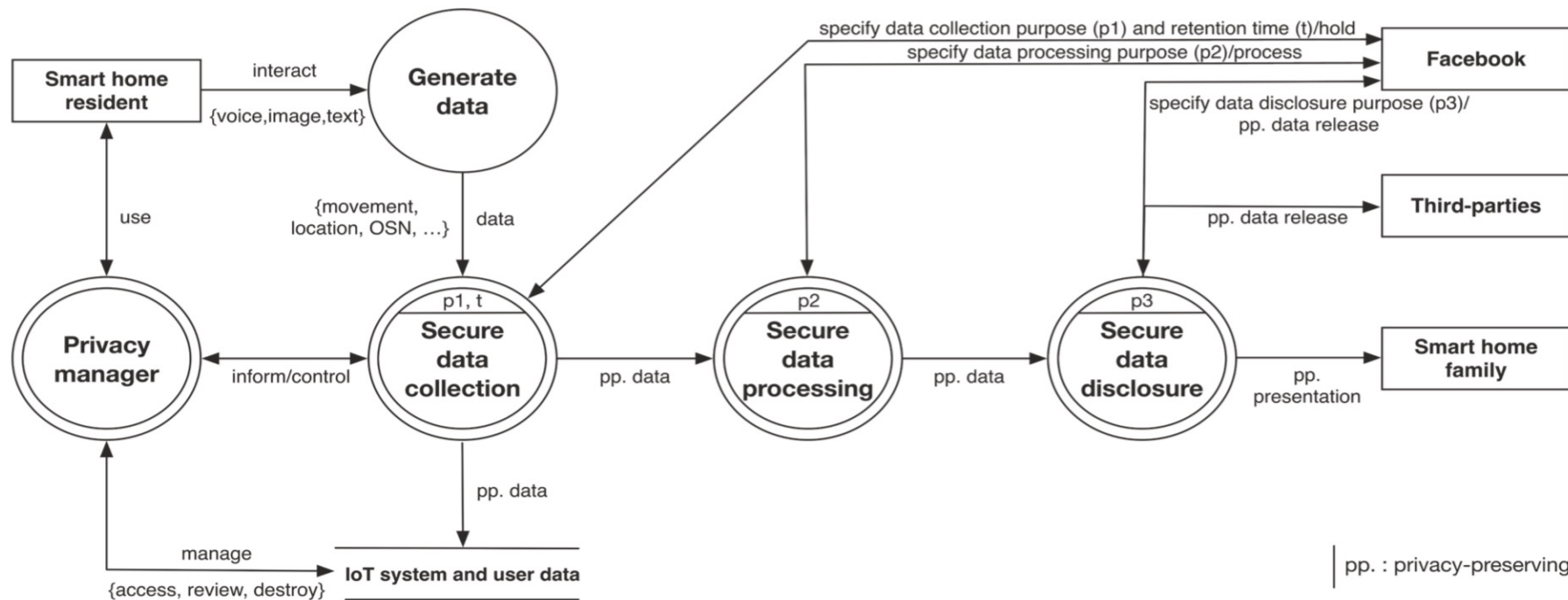
CONCLUSIONS

- Threat agents are finding ways to learn how to tap into the smart connected home and looking for new ways to attack in-home technologies

- In the dissertation, we presented contributions that enable early identification of threats, better planning for risks, and enable informed decisions about mitigations of potential impacts

- The presented contributions provide a foundation that helps deepen the understanding of privacy and security in smart connected homes

·PRIVATE·

NEXT STEPS

- Using Machine Learning techniques to automatically detect attacks on smart homes

- Creation of tools and mechanisms to support the implementation of more secure and privacy-preserving smart home technologies

- Offering guidelines for developers and policy makers to build smart home technologies that prioritize human values

Thanks!

MALMÖ UNIVERSITY
INTERNET OF THINGS AND PEOPLE