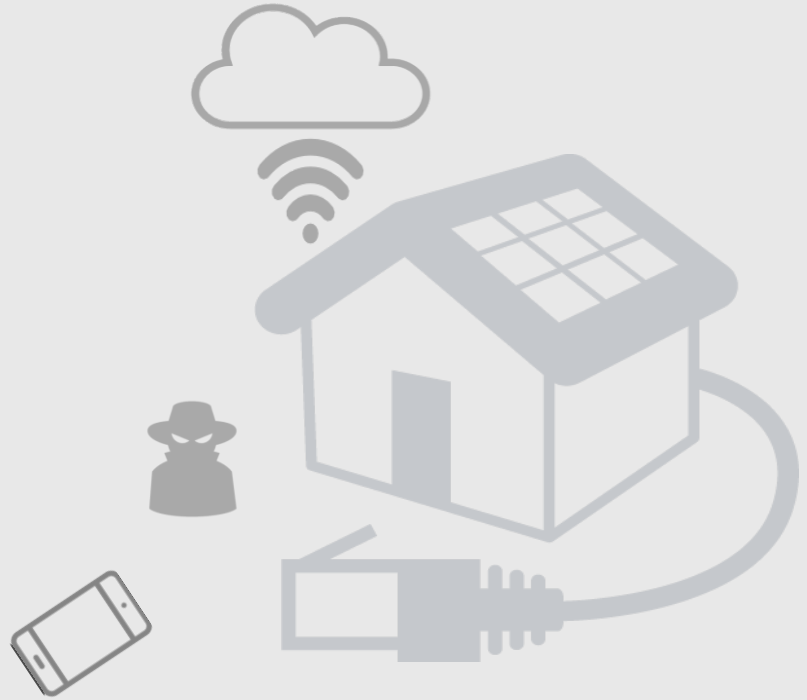
# On Privacy and Security Challenges in Smart Connected Homes

**Joseph Bugeja**

**Andreas Jacobsson**

**Paul Davidsson**



MALMÖ UNIVERSITY
INTERNET OF THINGS AND PEOPLE

KK-stiftelsen

verisure
ALARMS WITH IQ

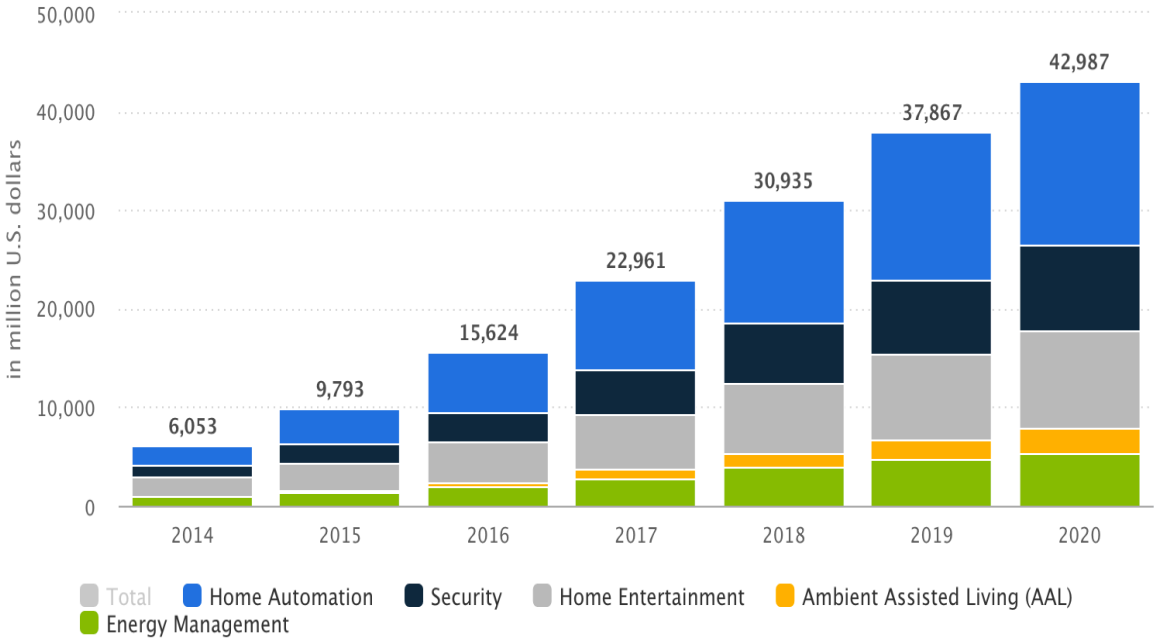
# AGENDA

1. Introduction
2. Challenges
3. State of the Art Mitigations
4. Research Directions
5. Final Remarks

# MOTIVATION

Why study smart homes? Why are privacy and security important considerations?

- Smart homes are technology-filled buildings and economically too important to ignore (Hindus, 1999)
- 43 billion USD in 2020 (Statista, 2015)





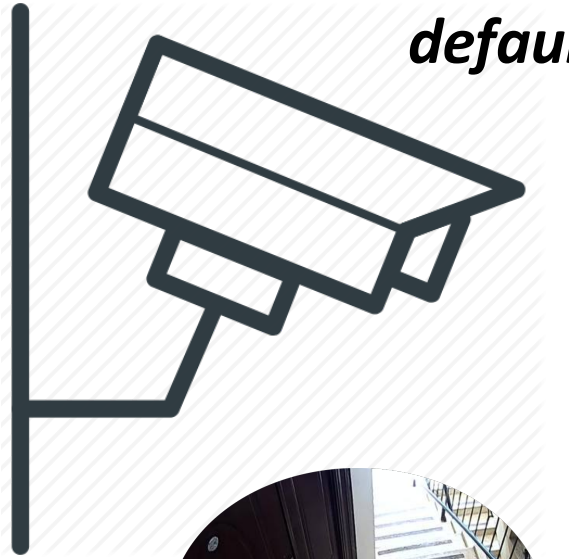
- US households with smart home technology is expected to double to 30 million households (August & XFINITY Home, 2016)

# SURVEILLANCE RISKS

Why study smart homes? Why are privacy and security important considerations?

- Your appliance might be silently watching or listening to your intimate conversations!

***"Peeping into 73,000 unsecured security cameras thanks to default passwords"***



***Shodan Images***


***Amazon Echo***

***"The TV Is Watching YOU"***

# PHYSICAL SECURITY RISKS

Why study smart homes? Why are privacy and security important considerations?

- Your appliance might cause life-threating risks to yourself, family members, and home!

## Wireless Insulin Pump

***"Insulin pump hack delivers fatal dosage over the air"***

http://goo.gl/rqv4r6

## Smart Thermostat

Ransomware PoC FTW!

#Defcon24 #wargames @IoTvillage

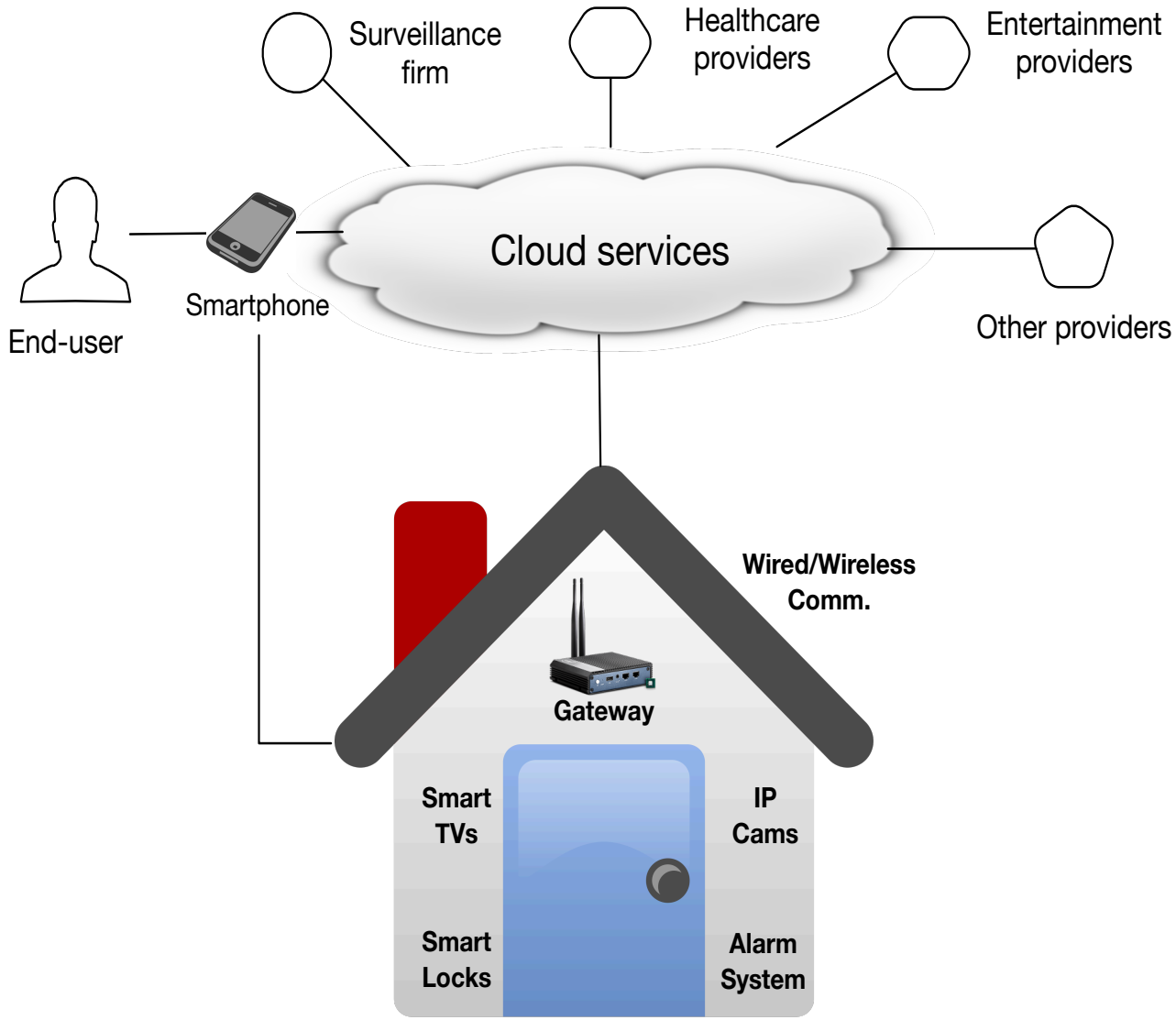

**Hackers demonstrated first ransomware for IoT thermostats at DEF CON**

Oh goody, a hacker could crank up the temperature of a smart thermostat to a sweltering 99 degrees and leave the IoT device like that until its owner pays a ransom to regain control.

http://goo.gl/gIMjP6

# SMART CONNECTED HOME OVERVIEW

What is a smart connected home?




- Residence incorporating ICT components that can be accessed, controlled and monitored remotely (e.g. over the Internet)
- Connectivity is the key enabler
- Smartphone is the house remote

# SMART CONNECTED HOME ARCHITECTURE

What is the technical composition of a smart connected home?

1. Sensors
(e.g. microphones)

2. Actuators
(e.g. motor)

DEVICE

3. Smart Objects
(e.g. smart lock)

4. Gateways
(e.g. 4G)

COMMUNICATION

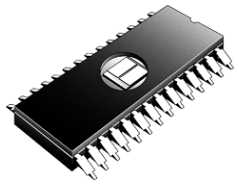
SERVICE

5. Network Channels
(e.g. Wi-Fi)

6. Software Apps.
(e.g. HA)

# DEVICE LEVEL CHALLENGES

What are the device level challenges?



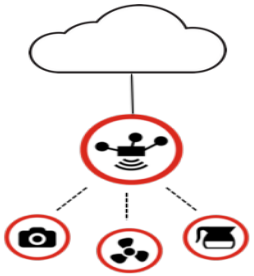
- Memory, computing, energy, storage, and throughput constraints

- Lack of keyboard, mouse, and tactile screen

- Easily accessible devices are prone to physical attacks

# COMMUNICATION & SERVICE LEVEL CHALLENGES

What are the communication and service level challenges?



- Use of bridges, hubs or gateways make the design of end-to-end security challenging

- Devices can join/leave the home networks anytime from anywhere


- Some devices are expected to operate for a long time without requiring maintenance

# STATE OF THE ART MITIGATIONS

What are the device, communication, and service level security approaches?

## DEVICE

- H/W enc, fail-secure design, and device authZ
- Enhanced algorithms, e.g. DTLS and ECSDA
- Platforms such as RERUM
- CC and EMVCo IC SE

## COMMUNICATION

- VPNs, firewalls, IDS, and IPS
- TOR-based systems
- Devices such as Cujo, Dojo, and Keezel
- ENISA, CSA, etc.

## SERVICE

- Security testing, secure design, and data masking
- Cryptographic schemes
- OWASP, Builditsecure.ly, I Am the Cavalry
- Sites such as BugCrowd

# OPEN SECURITY AND PRIVACY GAPS

Do the solutions leave any vulnerabilities?

| DEVICE | COMMUNICATION | SERVICE |
| --- | --- | --- |
| ▪ Resource Constraints | ▪ Encrypted Communication | ▪ Provider Reputation |
| ▪ Experimental Standards | ▪ Local Attacks | ▪ Personalization |

*…and more!*

# RESEARCH DIRECTIONS

What are the prominent areas where further investigation is required?

1 **IDENTITY MANAGEMENT**

- Secure Key Management Protocols
- Authentication Process Tuning

2 **RISK ASSESSMENT**

- Asset and Risk Evaluation
- Empirical Methods

3 **INFORMATION FLOW CONTROL**

- Intuitive UIs
- Control of Third-party Uses

4 **SECURITY MANAGEMENT**

- Patching Approaches
- Security and Privacy in Design

# FINAL REMARKS

- Home is the place where privacy is expected
- Smart connected home devices are being manufactured with invasive technologies and connection to manufacturers and providers
- Security and privacy threats are real and have been exploited repeatedly
- Different mitigations exist however we lack holistic solutions that cater for the different services, end-users, and architecture layers

# Thank you for your attention!



**joseph.bugeja@mah.se**


**@BugejaJoseph**


**https://www.mah.se/iotap**