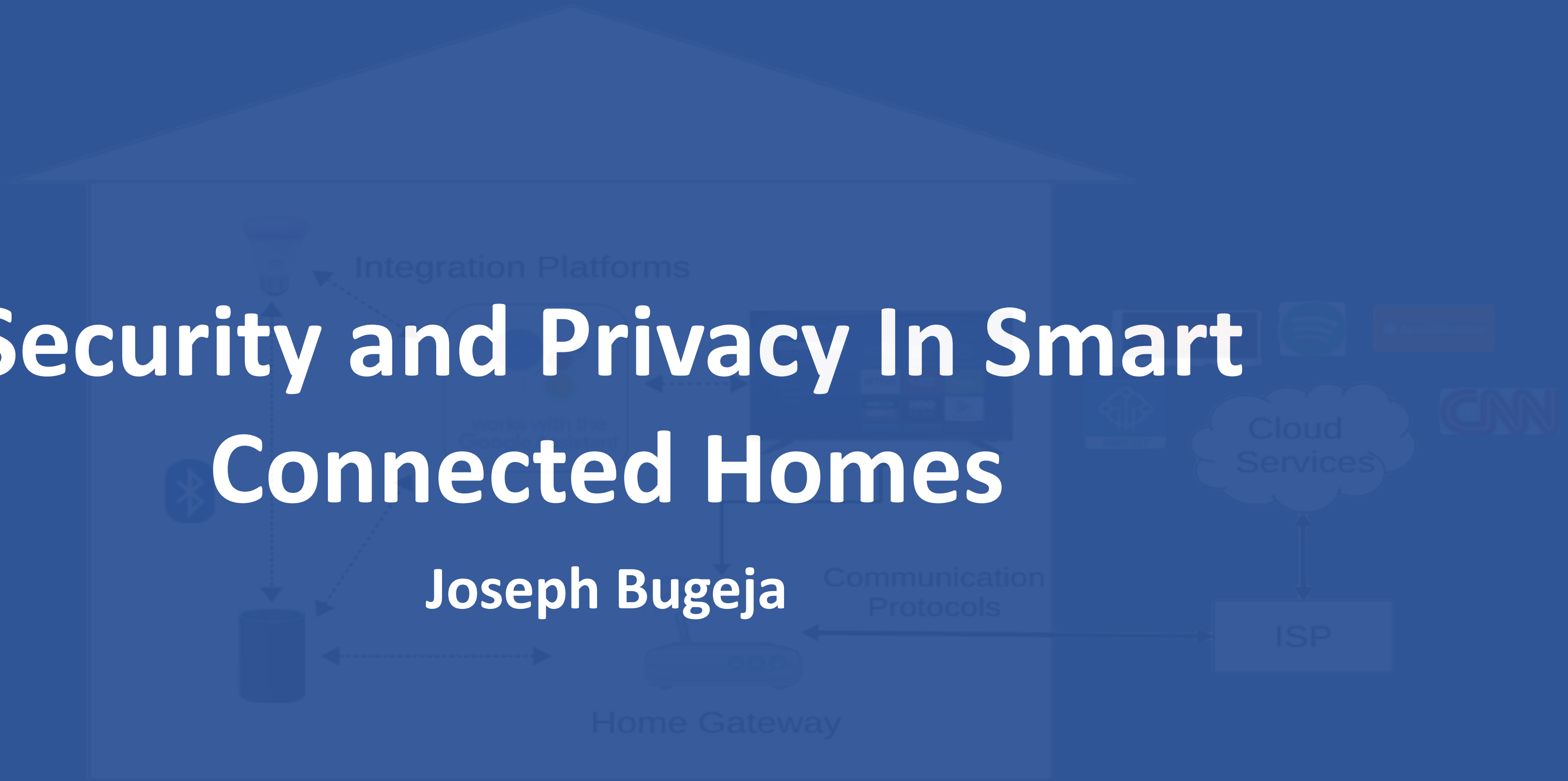
04-Mar-2020



Security and Privacy In Smart Connected Homes

Joseph Bugeja

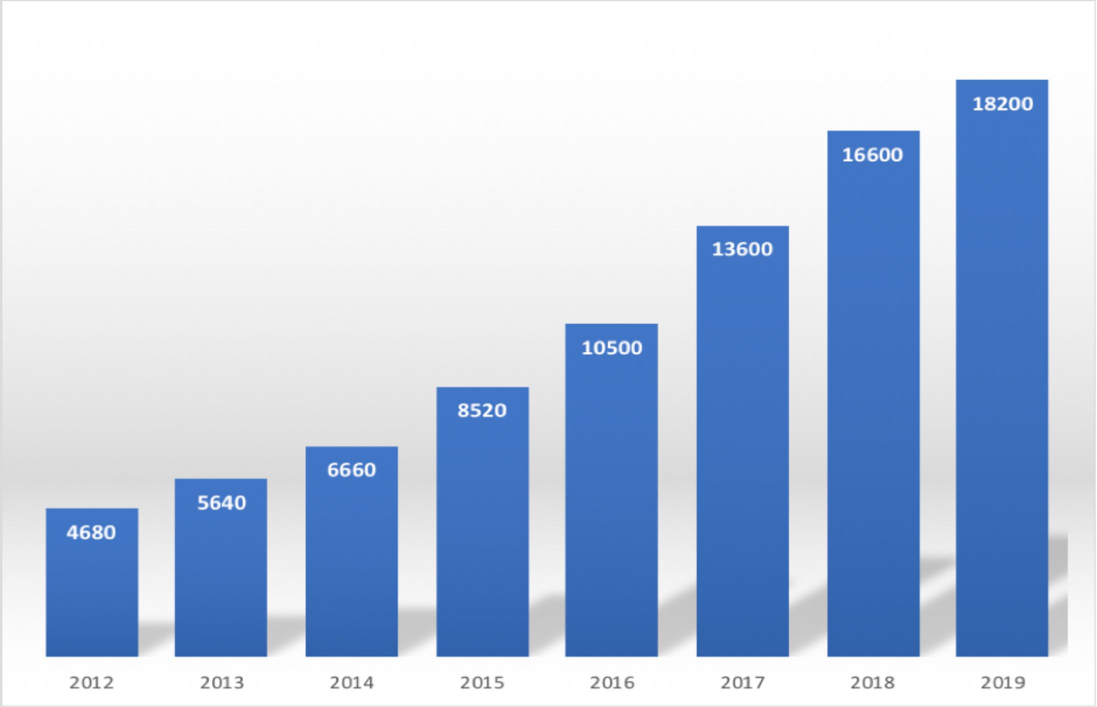
MALMÖ UNIVERSITY
INTERNET OF THINGS AND
PEOPLE RESEARCH CENTER

KK·stiftelsen

INTRODUCTION

- Smart home IoT device shipments are expected to grow to 1.6 billion shipped devices in 2023 (*IDC*, 2019)

- Total number of publications appearing in *Google Scholar* for the term “Smart Home”

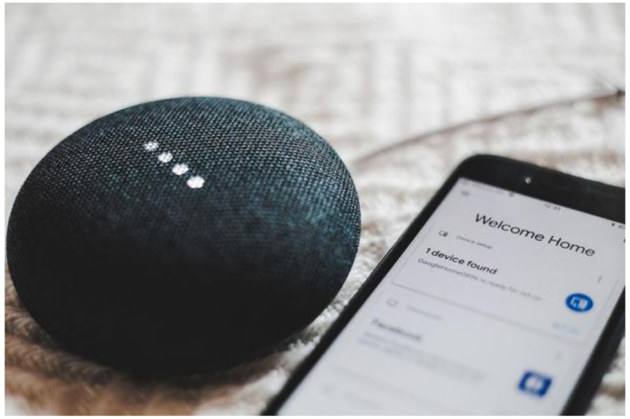


- The proliferation of smart devices has brought about many security and privacy concerns

SOME RECENT SECURITY AND PRIVACY RISKS

Internet of Things (IoT) under fire: Kaspersky detects more than 100 million attacks on smart devices in H1 2019

"This figure is around seven times more than the number found in H1 2018…" – Kaspersky 2019



Cybersecurity risk with smart bulbs and other home devices

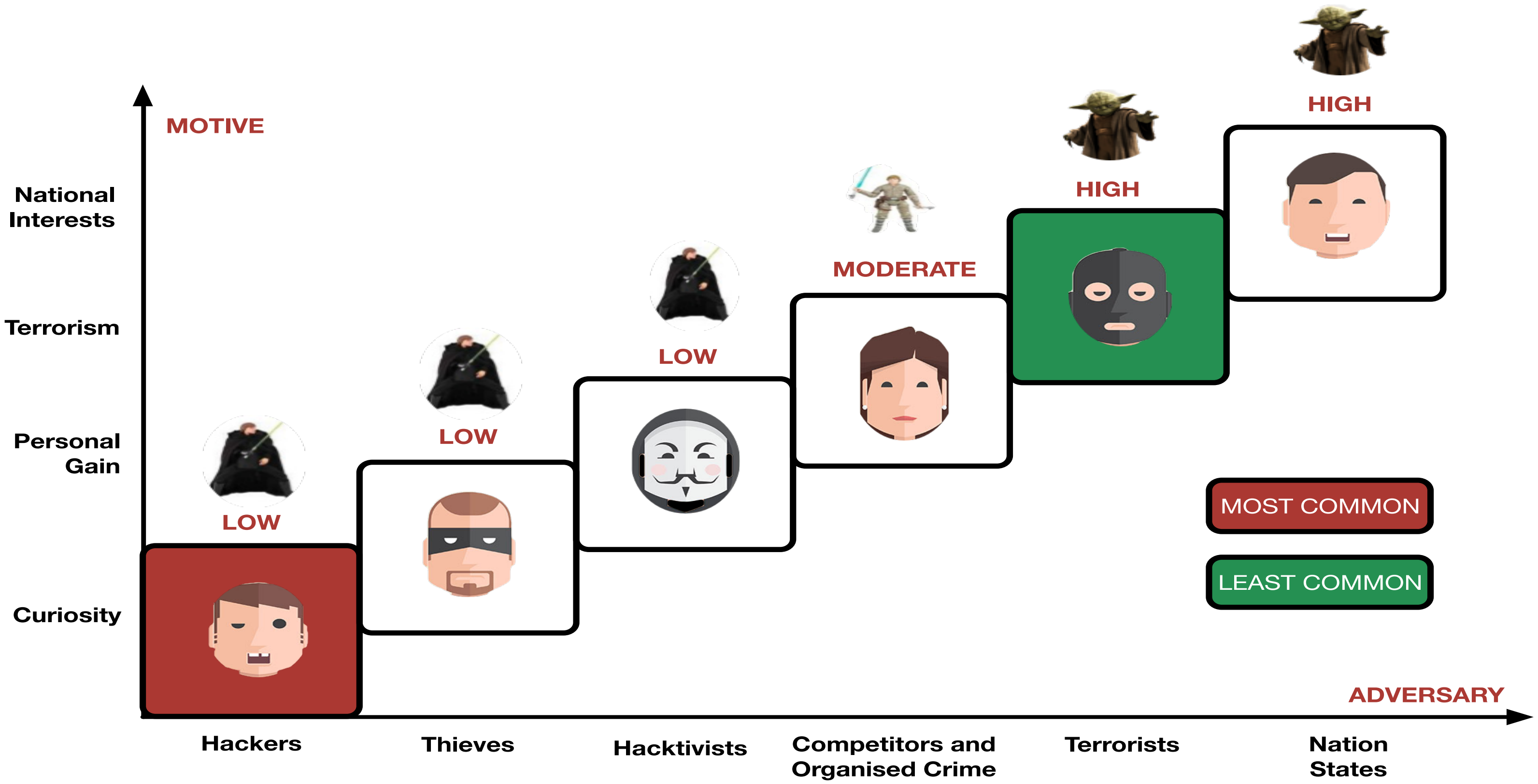
"a threat actor can infiltrate a home …, spreading ransomware or spyware, by using nothing but a laptop and an antenna …" – Check Point, 2019

Smart devices are sharing personal data with third parties

72/81 IoT devices shared data with 3rd parties that were completely unrelated to the original manufacturer[1]

[1] Ren, Jingjing, et al. "Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach." *Proceedings of the Internet Measurement Conference*. 2019.

SELECTED RESEARCH CONTRIBUTIONS



MOTIVE

National Interests

Terrorism

Personal Gain

Curiosity

ADVERSARY

Hackers — LOW

Thieves — LOW

Hacktivists — LOW

Competitors and Organised Crime — MODERATE

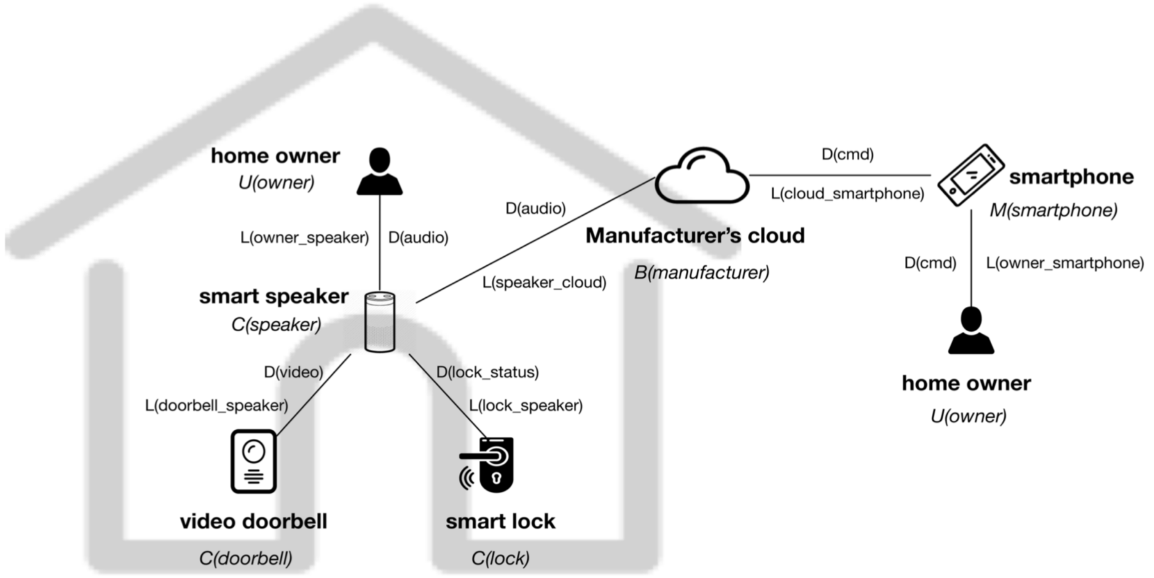
Terrorists — HIGH

Nation States — HIGH

🟥 MOST COMMON

🟩 LEAST COMMON

SELECTED RESEARCH CONTRIBUTIONS



Nodes, $N = \{doorbell, lock, speaker, manufacturer, smartphone\}$

$C(speaker).capabilities =$
$\{gateway, storage, processing, interaction\}$
$B(manufacturer) = cloud$

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

Identification

Localization and Tracking

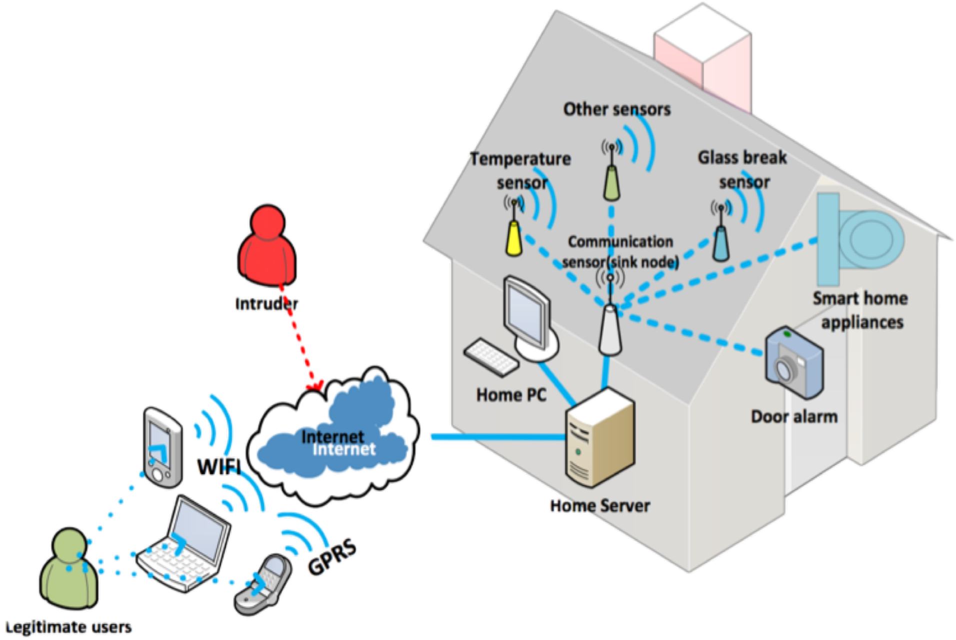
Profiling

○ **Threat does not exist**

◐ **Threat is a potential future threat**

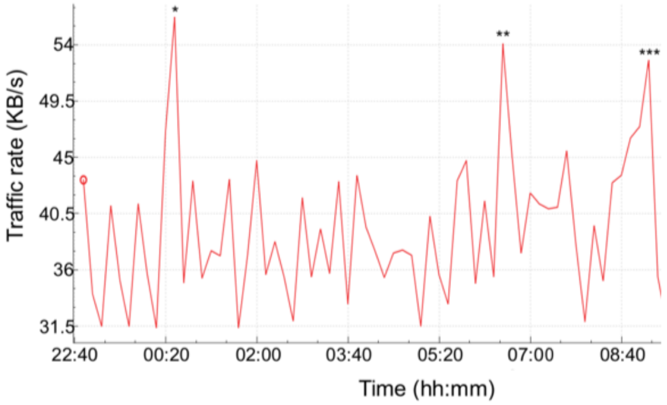
● **Threat is present**

NEXT STEPS

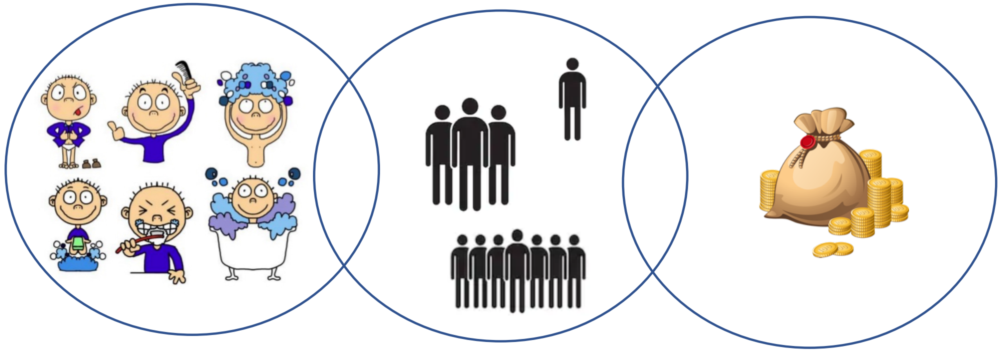


Smart connected home

Network traffic



Profiling users



FINAL REMARKS

- ✓ IoT has transformed the brick-and-mortar home into a digital trove of personal data that can be remotely accessed
- ✓ We contributed to the understanding of the smart connected home and its risks from a scientific perspective
- ✓ Several open issues need to be addressed requiring a close-knit collaboration between academia and industry

THANK YOU FOR *YOUR* ATTENTION !

joseph.bugeja@mau.se

bugejajoseph.com