computing
conference 2020

On the Analysis of Semantic Denial-of-Service Attacks Affecting Smart Living Devices

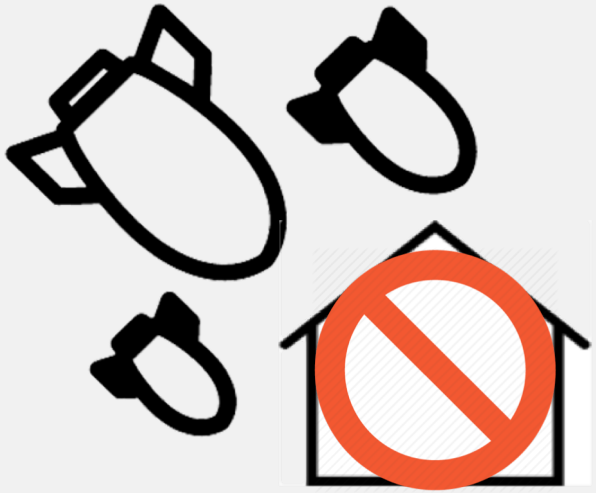
Presenter: Joseph Bugeja

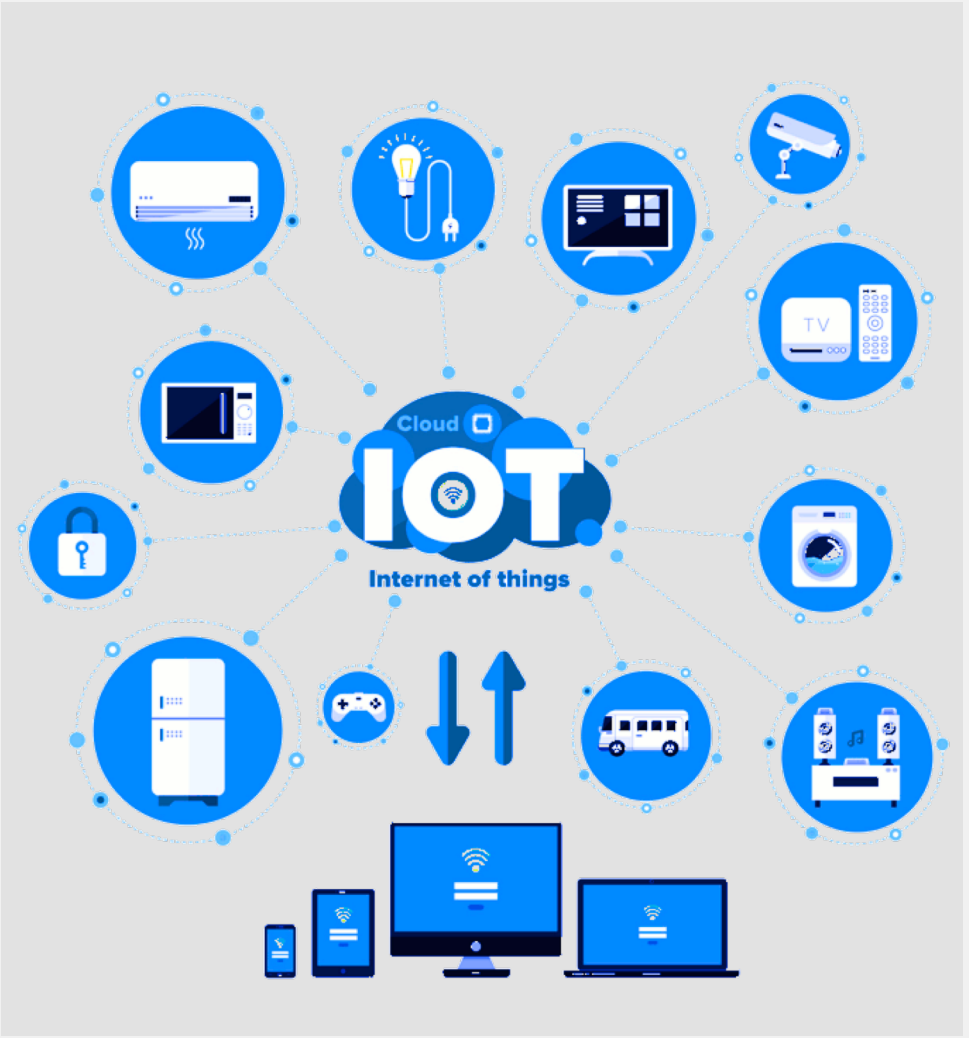
MALMÖ UNIVERSITY
INTERNET OF THINGS AND PEOPLE RESEARCH CENTER

KK-stiftelsen

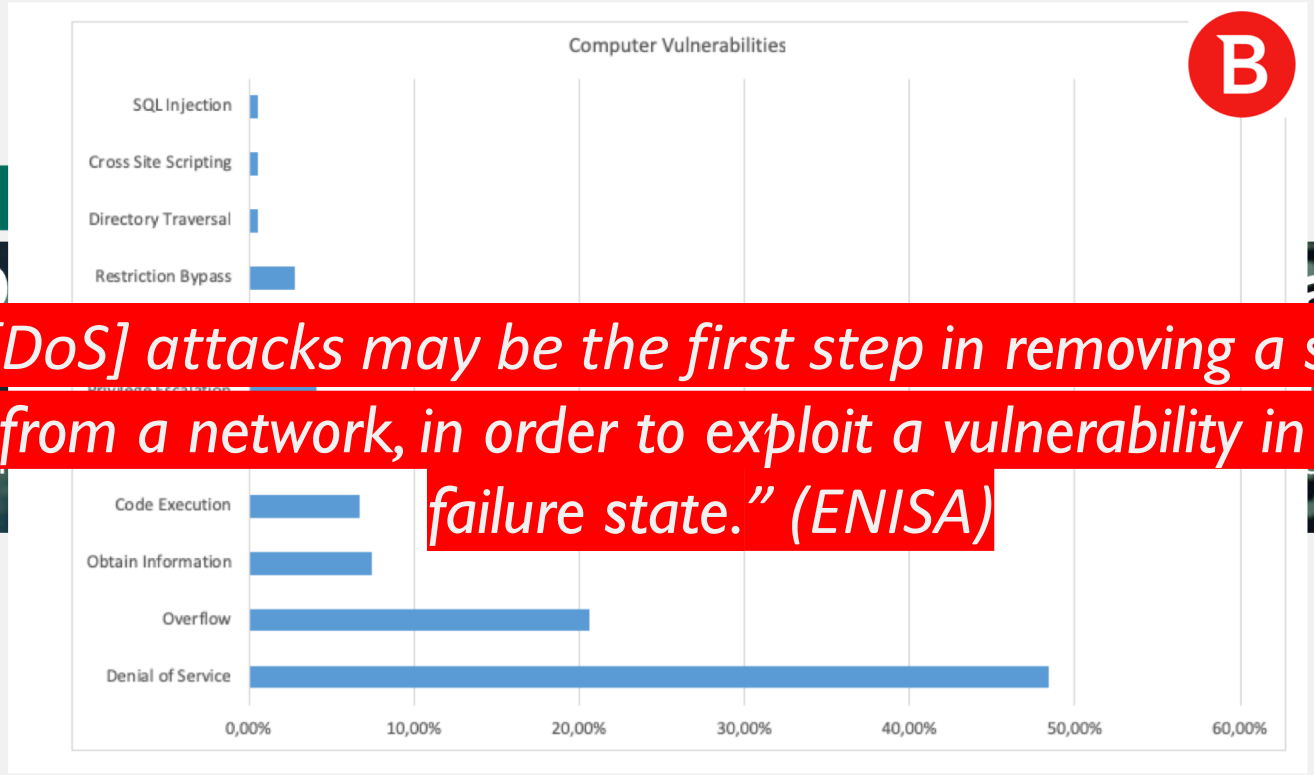
Introduction

- More than 75 billion connected devices by 2025 (*Statista*)
- Many benefits, but bolstering security is a top priority
- Resilience against Denial-of-service (DoS) attacks is important





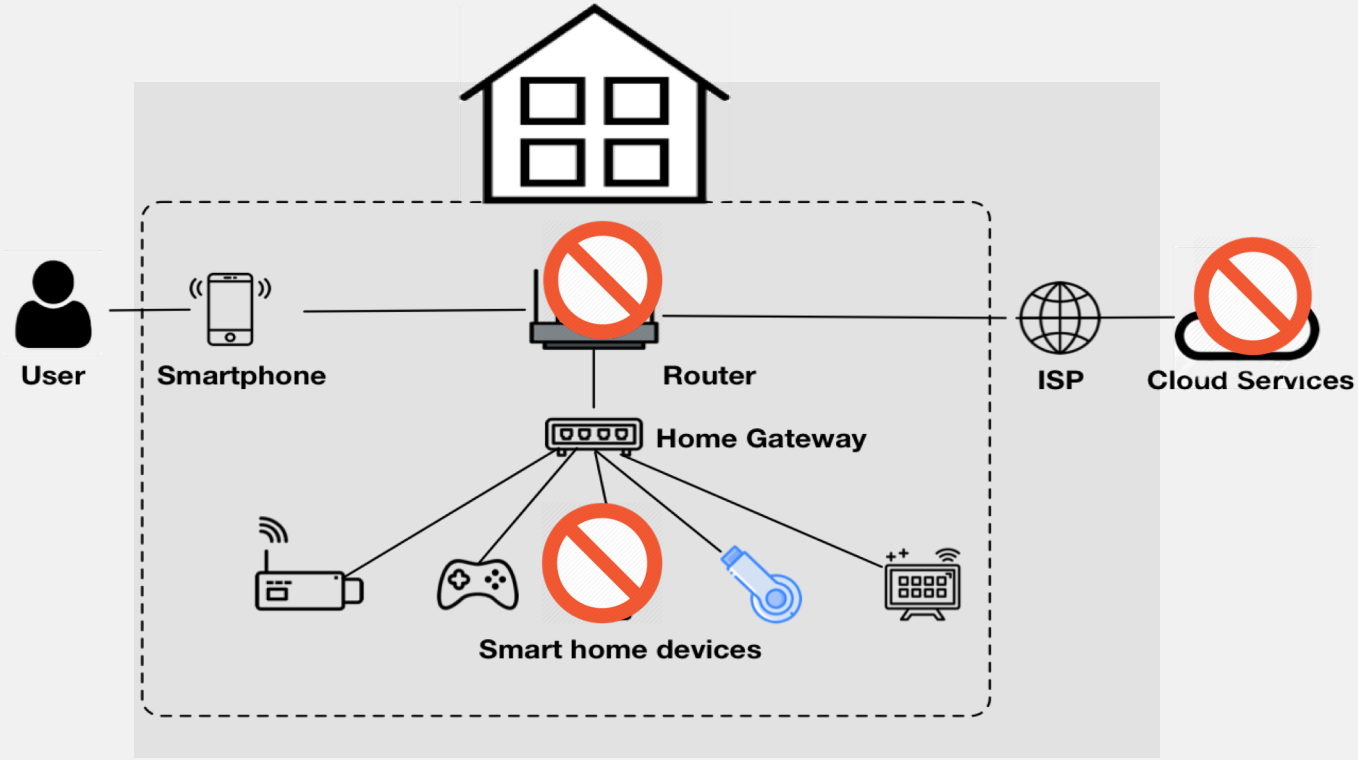
Introduction



"Such [DoS] attacks may be the first step in removing a smart home component from a network, in order to exploit a vulnerability in its disconnected failure state." (ENISA)

DoS Attacks

- Goal: DoS attacks attempt to exhaust or disable access to resources at the victim, e.g., by draining the battery of a device
- In the home, DoS can target cloud end-points, the home router, and the IoT devices
- Two broad categories of DoS attacks: semantic and flooding attacks
- We focus on **semantic attacks** and attacks targeting directly the **smart home devices**



Definition: *A smart connected home is a residence that uses IoT technologies, such as sensors, smart devices, and communication protocols, allowing for remote access, control, and management, typically via the Internet.*

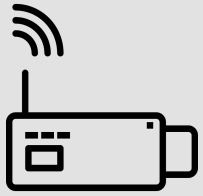
Experiment Design

- 5 commercial devices connected to an Internet router, over Wi-Fi
- Devices were updated to their latest firmware
- All devices were connected to the same network
- OpenVAS vulnerability scanner was used for testing against DoS attacks

OpenVAS
Open Vulnerability Assessment System

KALI
BY OFFENSIVE SECURITY

Devices used for testing



IP camera

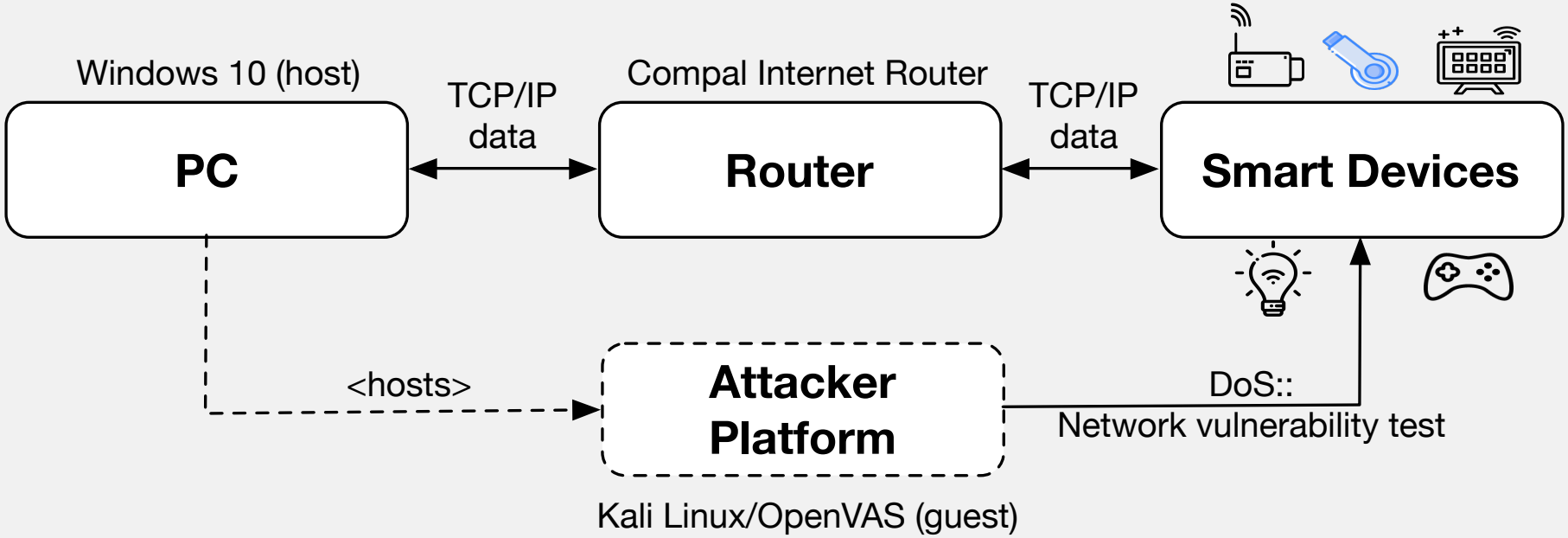
Gaming console

Lighting system

Media player

Connected TV

Experiment Design



- Test cases were executed over OpenVAS web interface
- Host scanning was performed across all TCP ports and the top 100 UDP ports
- 1,384 network tests for DoS were executed
- For each successful attack the attack payload was inspected

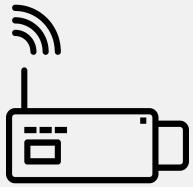
Results

Gaming console

(2) Critical

(1) High

(6) Medium



IP camera

(1) Critical

(1) High

Connected TV

(1) Critical

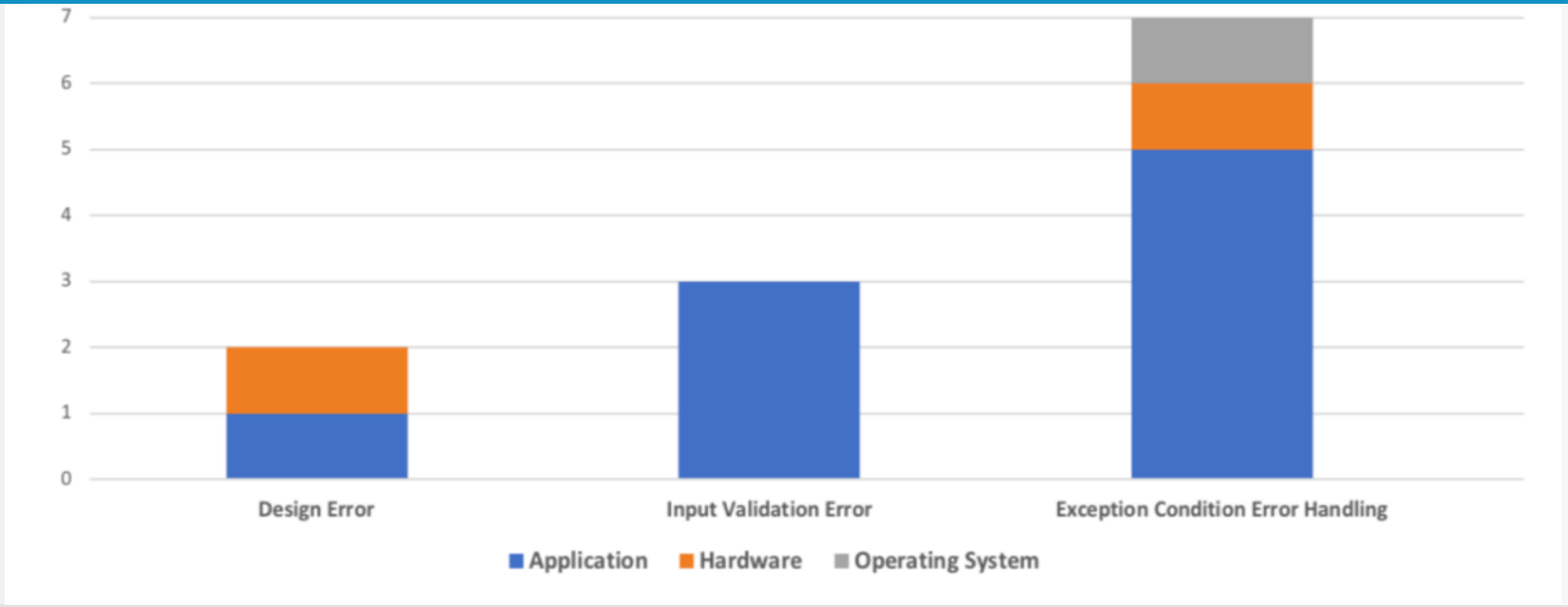
(1) Medium

Media player

Lighting system

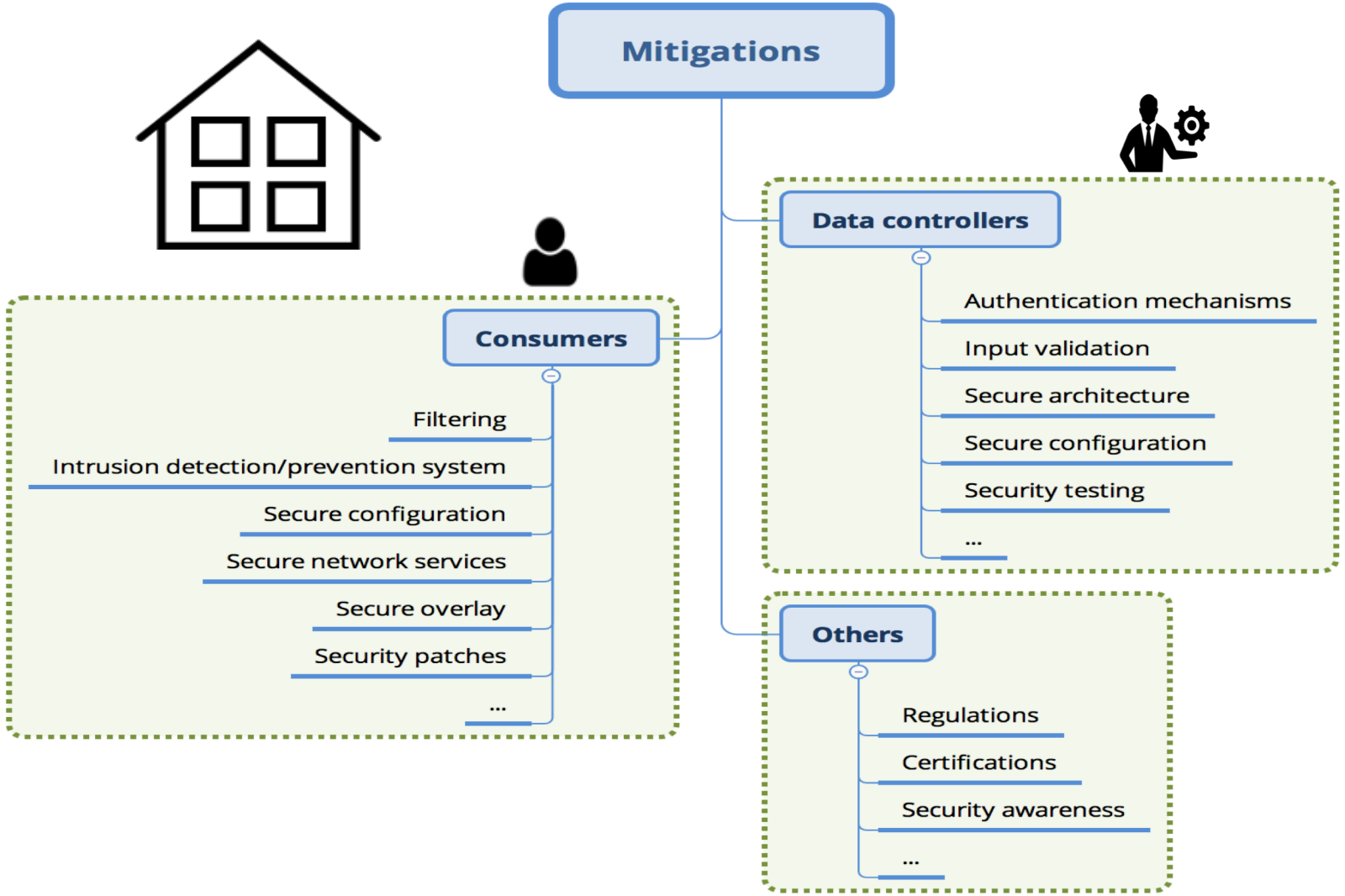
- Gaming console from an established manufacturer was the most prone to semantic DoS attacks
- All discovered vulnerabilities did not require the attacker to authenticate to the host and were remotely exploitable
- 2/3 device types had vulnerabilities resulting in complete shutdown of the device
- Some vulnerabilities are shared across different device types

Results



- Most of the successful DoS attacks target the high-level application
- The majority of the attacks arise due to a failure in the code to respond to unexpected data/conditions
- We observe the prevalence of HTTP GET DoS attacks where the application layer protocol HTTP is exploited
- Exploit code is readily available on the Internet

Some Mitigations

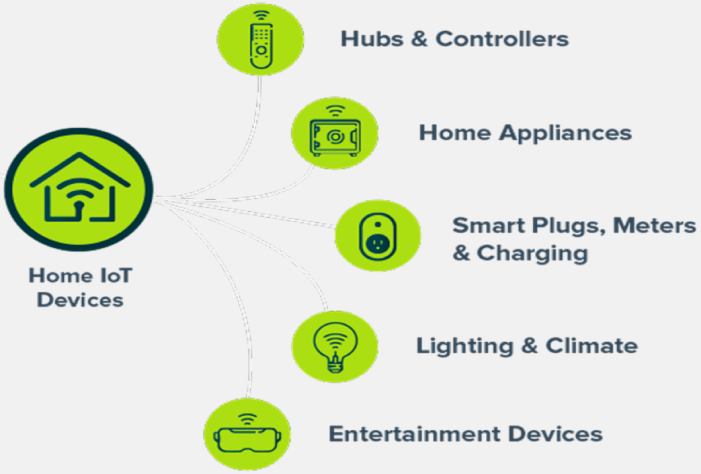


Concluding Remarks

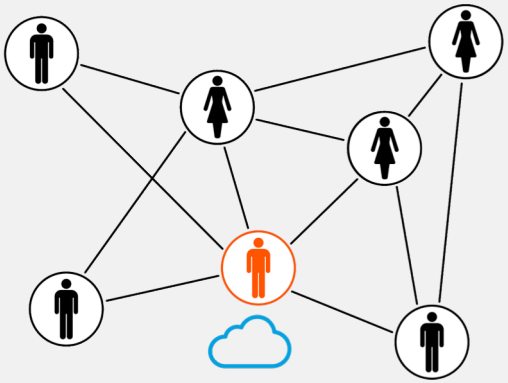
- The growth of connected devices in particular inside homes raises the importance of an assessment of their resilience
- We conducted a vulnerability assessment that tested the resilience of 5 commercial Internet-connected devices against out-of-the-box semantic DoS attack test cases
- Our attack analysis indicated that the root causes of the exploited vulnerabilities are a failure to handle unexpected data/conditions in code
- Semantic DoS attacks are prevalent in commercial devices, and is easy to exploit possibly causing a total shutdown of a device (or the entire home) with simple HTTP header manipulation

Future Work

- Broader selection of devices

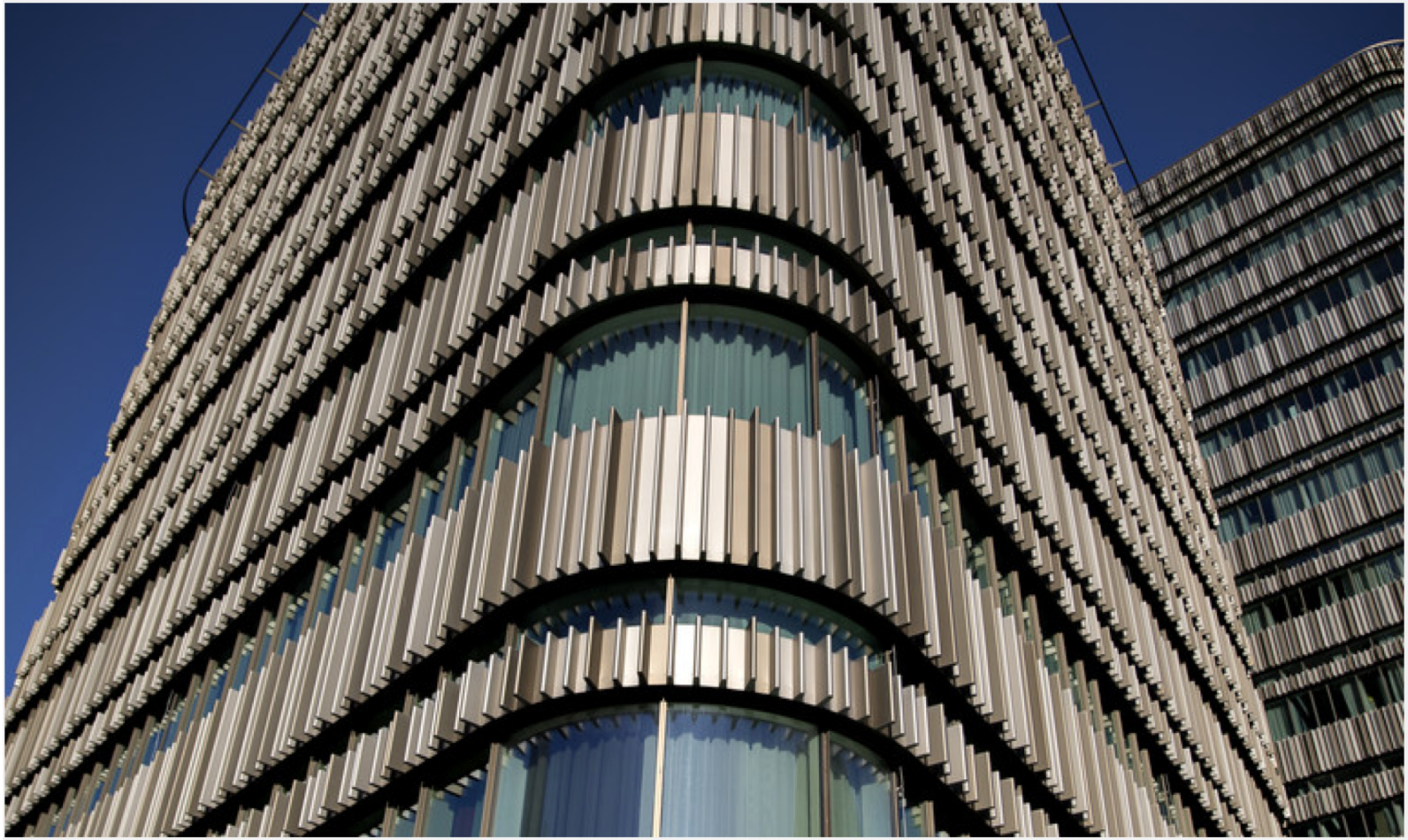


- More sophisticated attack models



- Proactive detection of DoS attacks

Thank you for your attention!



Source: mau.se

Joseph Bugeja
joseph.bugeja@mau.se

Andreas Jacobsson
andreas.jacobsson@mau.se

Romina Spalazzese
romina.spalazzese@mau.se