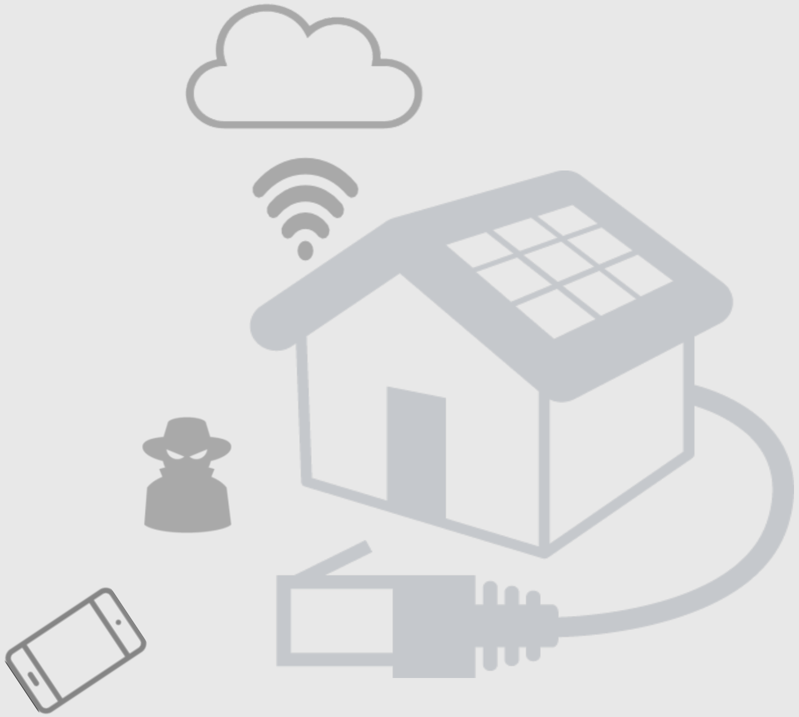
An Analysis of Malicious Threat Agents for the Smart Connected Home



Joseph Bugeja

Andreas Jacobsson

Paul Davidsson

MALMÖ UNIVERSITY
INTERNET OF THINGS AND PEOPLE

KK·stiftelsen

verisure
ALARMS WITH IQ

AGENDA

1 Introduction

2 Threat Agents

3 Research Method

4 Threat Model

5 Reflections

6 Closing Remarks & Future Work

HISTORY

“He who defends *everything*, defends nothing”

- Fredrick the Great

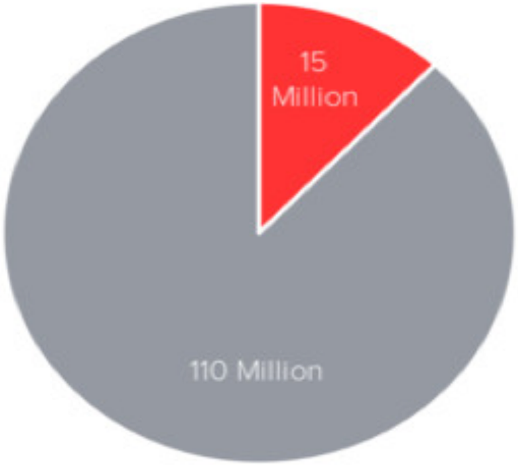
VULNERABILITY BASED STRATEGIES

What are the challenges with vulnerability based strategies?

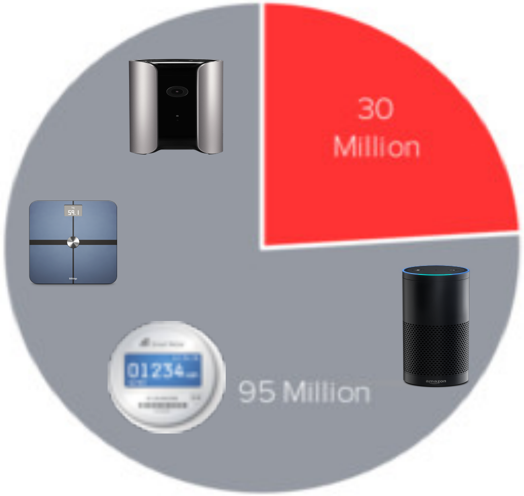
Hard Challenges

- Identify ALL vulnerabilities
- Close them before they are exploited
- Do it continuously, forever
- For all technology and users

- 2016



- 2017



HISTORY

"*Know your enemy* and know yourself and you can fight a thousand battles without disaster"

- Sun Tzu

THREAT AGENTS

What are threat agent archetypes?

- *Threat agent archetypes* are collective descriptions of attacks, representing similar risk profiles

- Intelligent attackers whose motivations drive their objectives

- Attributes such as skills, access, and resources define their most likely methods

Hacker

Low

Motivation: Curiosity

Objectives: Try things out
Cause confusion

Methods: Malware
Attack a network or device

TRADITIONAL HOME

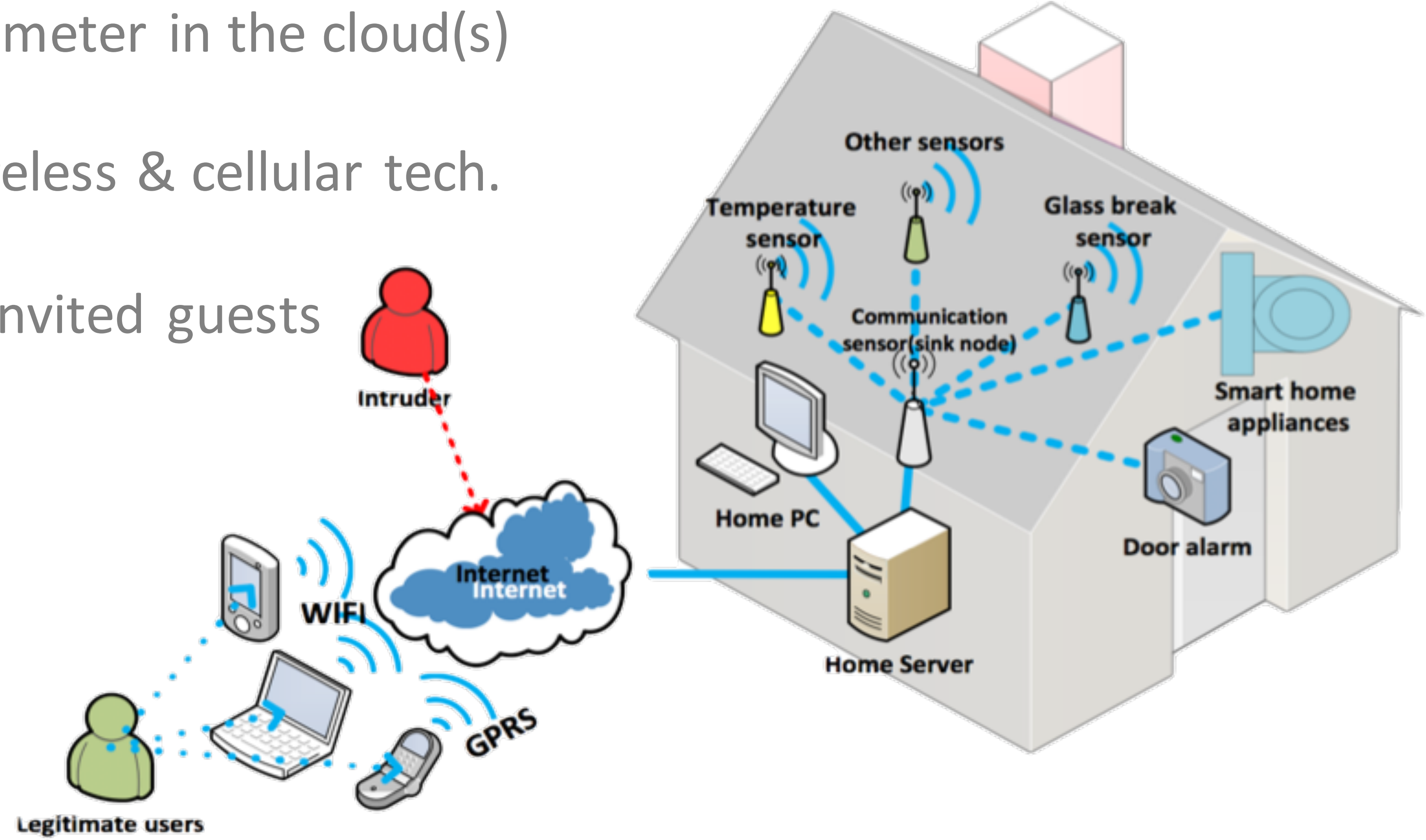
What are the characteristics of a traditional home?

- Well-defined perimeter
- Wired technologies
- Concise access list

SMART CONNECTED HOME

What are the characteristics of a smart connected home?

- Perimeter in the cloud(s)
- Wireless & cellular tech.
- Uninvited guests



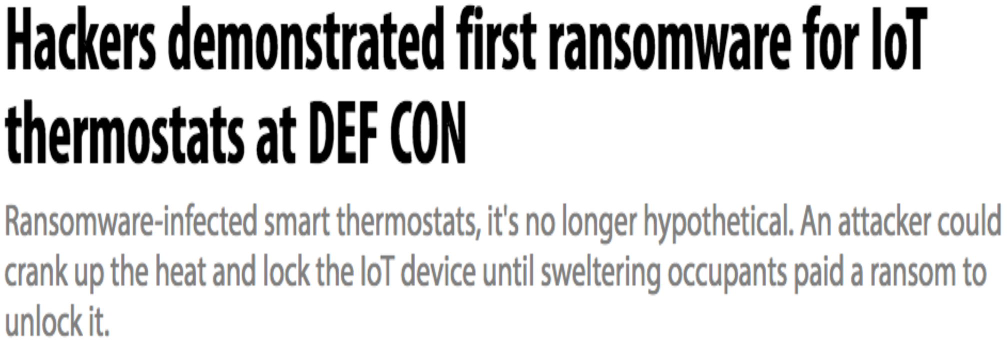
- Many benefits but …

SECURITY AND PRIVACY THREATS

Are information security and privacy threats in smart home real?

- Your smart appliance might be *watching* or *listening* to your intimate conversations; and may cause *life-threating* risks to yourself, family members, and home

New – Turn on the lamp
Will it rain tomorrow?
New – Play a Pop station on Pandora
Set an alarm for eight a.m.
New – How is traffic?
New – When do the Phoenix Suns play next?



Hackers demonstrated first ransomware for IoT thermostats at DEF CON

Ransomware-infected smart thermostats, it's no longer hypothetical. An attacker could crank up the heat and lock the IoT device until sweltering occupants paid a ransom to unlock it.

PROBLEM DEFINITION

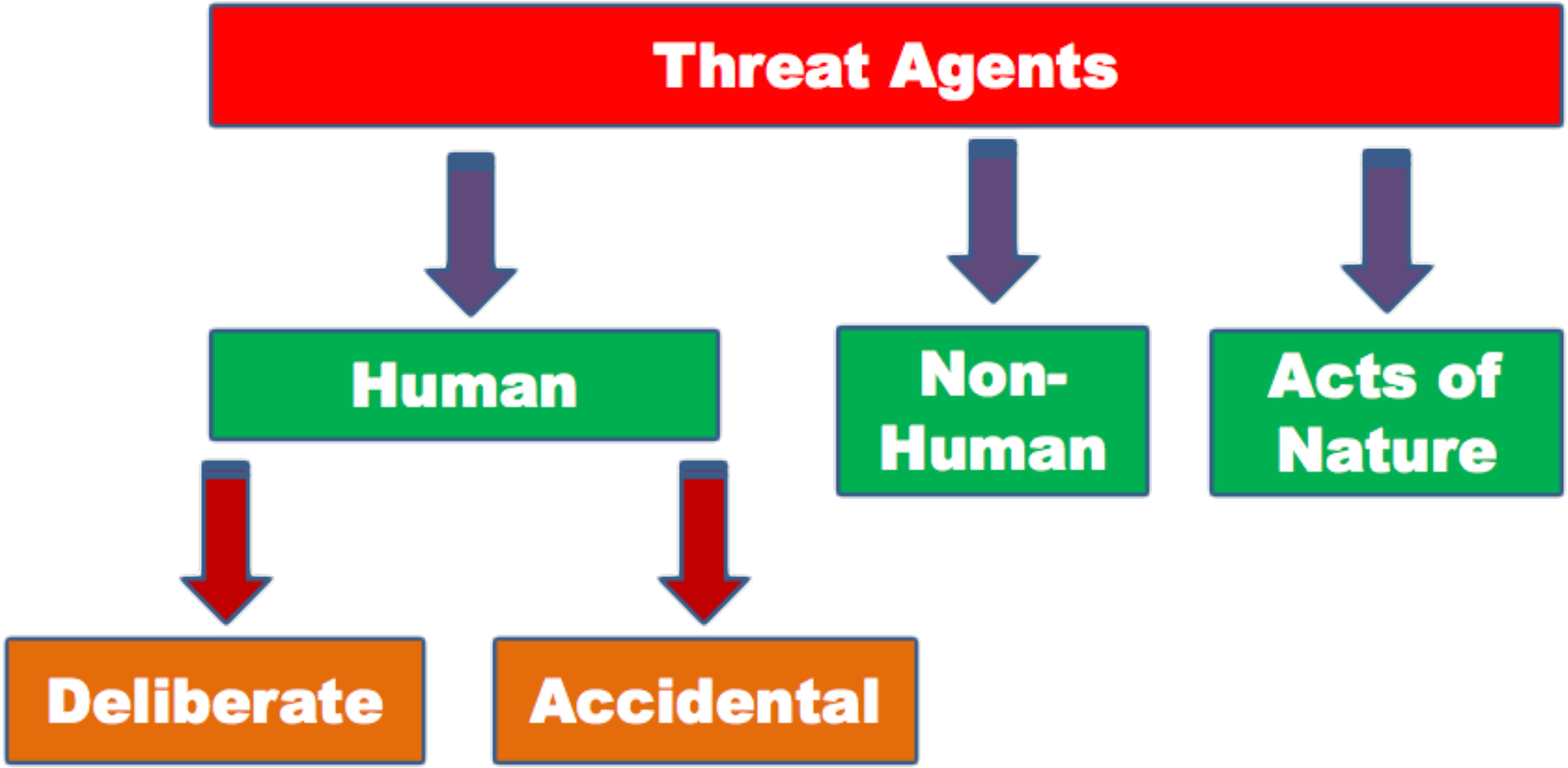
What is the problem being studied?

- *Who* are the threat agents?

THREAT AGENTS

What are the sources for threat agents?

Threats can come from anywhere, but generally fall under three categories Human, Non-human, and Nature. Threats can also be deliberate or accidental.



Threat Agents

Human

Non-Human

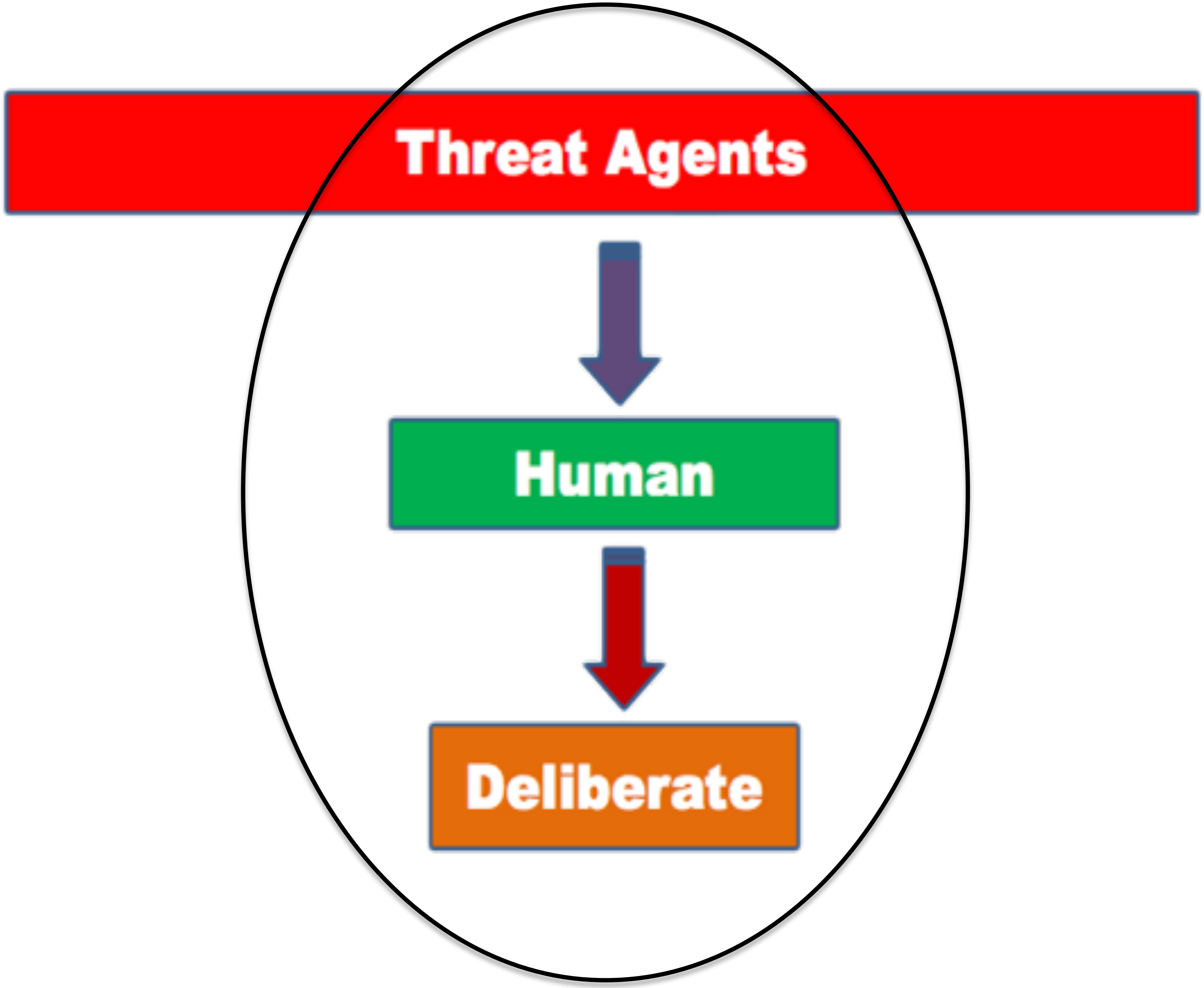
Acts of Nature

Deliberate

Accidental

THREAT AGENTS

What type of threat agents does this research look at?



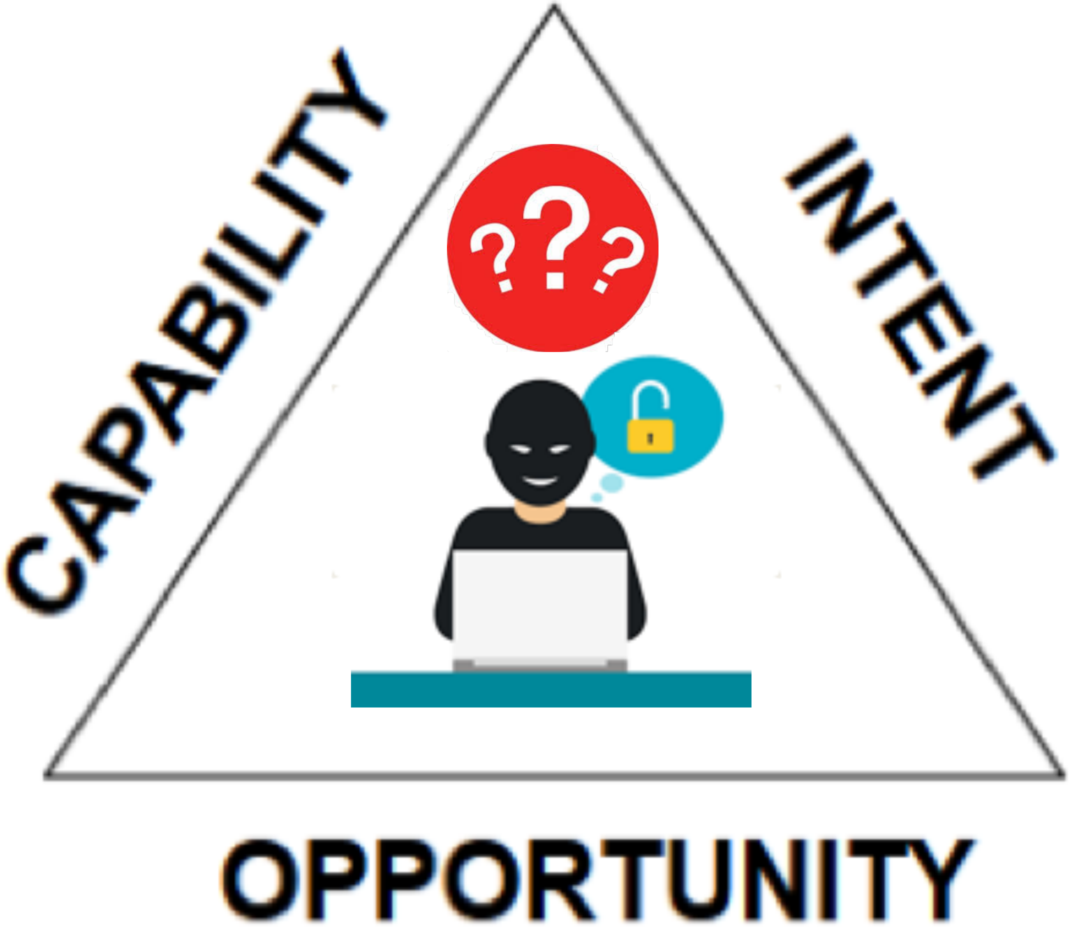
Threat Agents

Human

Deliberate

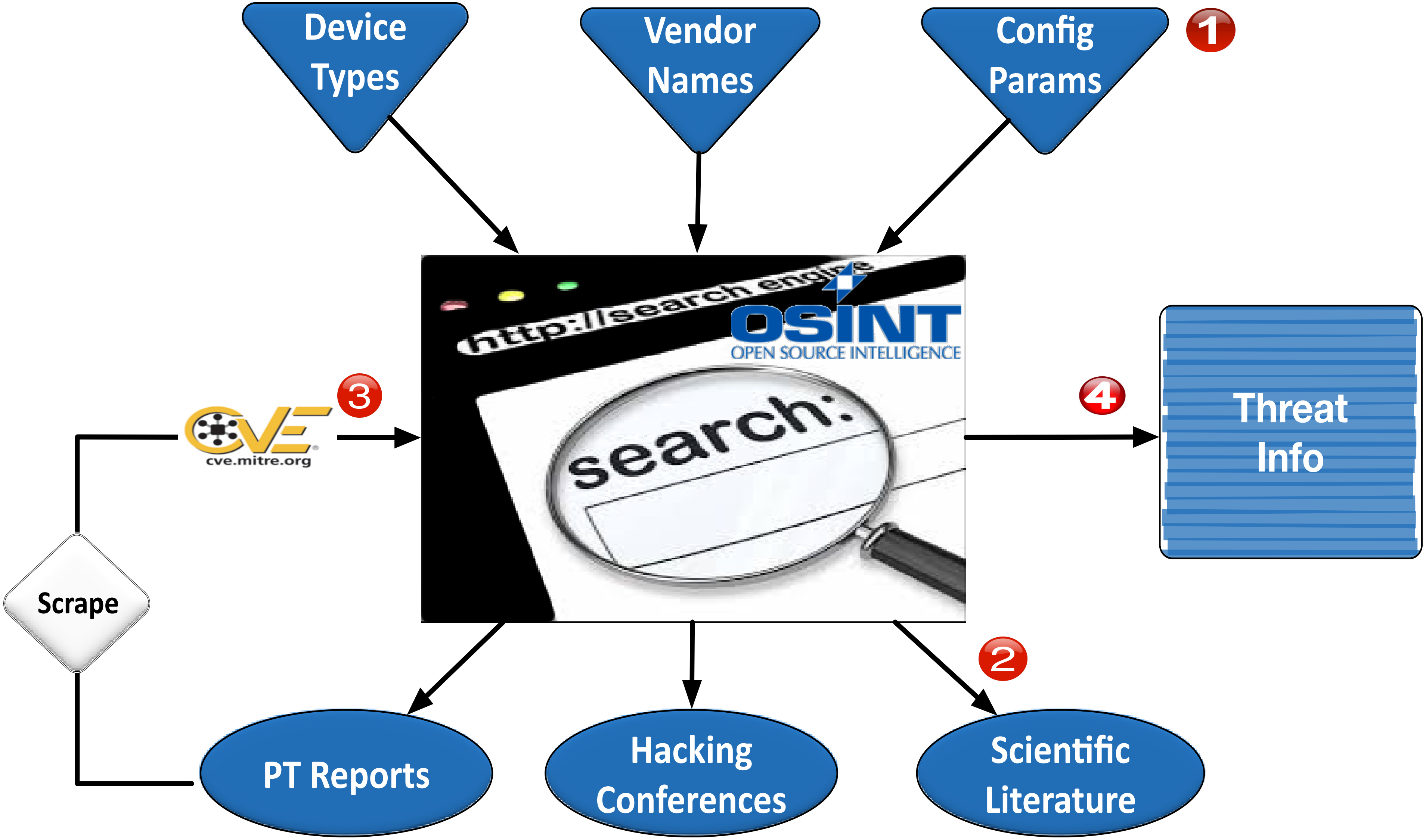
RESEARCH QUESTIONS

What are the research questions being studied?



RESEARCH METHOD

What research approach was adopted to answer the research questions?



THREAT AGENT CLASSIFICATION

What are the existing approaches for identifying threat agents?

Sandia National Laboratories

intel

ICS-CERT

OTA

- Identifies and measures cybersecurity threats
- No threat agent identification
- Emphasis on technical role

TARA

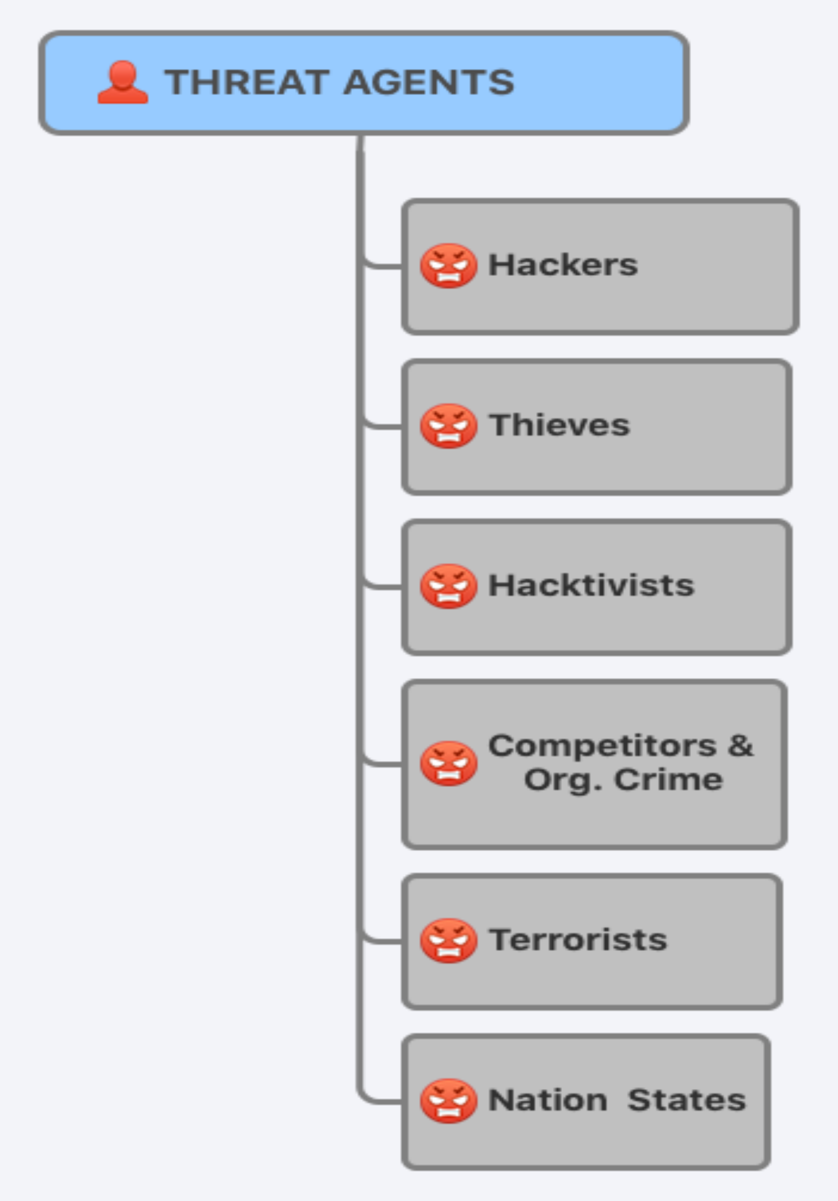
- Captures 22 threat archetypes and 8 characteristics
- Database is not disclosed to public
- Similar looking profiles

ICS-CERT

- Identifies 5 external threat agents
- Extensive database
- Used by other agent typologies

THREAT AGENTS

Who are the threat agents for the smart connected home?



THREAT AGENTS

- Hackers
- Thieves
- Hacktivists
- Competitors & Org. Crime
- Terrorists
- Nation States

HACKERS

Who are hackers? What methods they typically use? What is their primary motivation?

- Individuals (“hobby hackers”) that include malicious persons, script kiddies, and nosy employees of an organization

SHODAN
Computer Search Engine

- Viruses, worms, phishing

- Primarily motivated by curiosity

- Skill-level: Apprentice

Low

THIEVES

Who are thieves? What methods they typically use? What is their primary motivation?

- Opportunistic individuals that are associated with stealing mostly for personal financial gain

- System/physical intrusion, DoS, spoofing

- Main motive is monetary gain

- Skill-level: Apprentice

Low

HACKTIVISTS

Who are hacktivists? What methods they typically use? What is their primary motivation?

- Individuals or members of a larger group that pursue a political or social agenda

- DoS, fraud, and identity theft

- Primarily aim to promote and publicize their cause

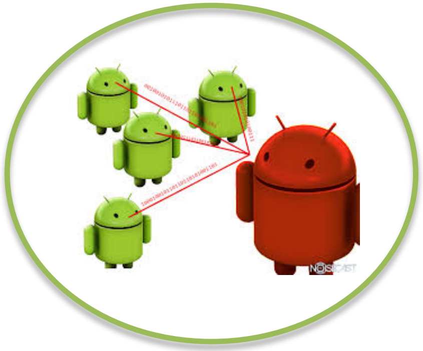
- Skill-level: Apprentice

Low

COMPETITORS AND ORGANIZED CRIME

Who are competitors & org. crime? What are their typical methods primary motivation?

- Commercial competitors that compete for revenues or resources, and private criminal organizations



- Botnets, ransomware, and inside information

- Competitive advantage, CI, and monetization

- Skill-level: Journeyman

Moderate

TERRORISTS

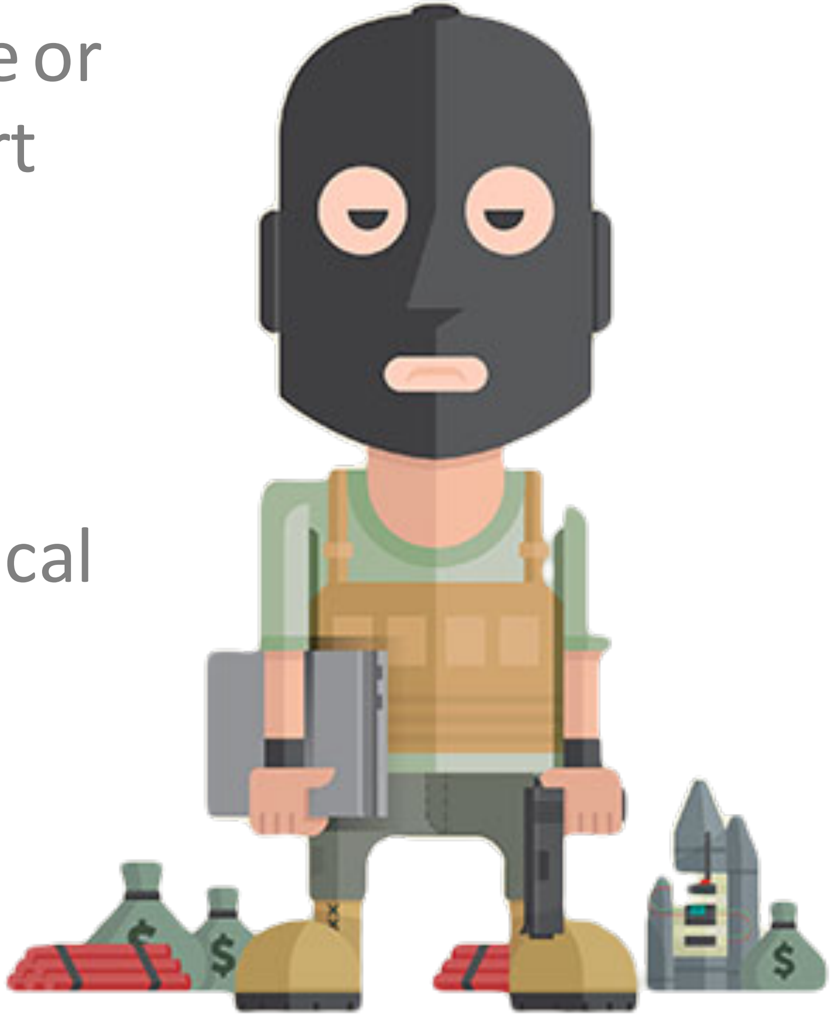
Who are terrorists? What methods they typically use? What is their primary motivation?

- Individuals that rely on violence or fear-related behavior to support personal socio-political agenda

- Damage/loss, outages, and physical attacks

- Terrorism

- Skill-level: Master



High

NATION STATES

Who are nation states? What methods they typically use? What is their primary motivation?

- Highly sophisticated individuals that are funded by governments and associated with a military unit

ADVANCED PERSISTENT THREAT

- Customized malware, spear phishing attacks, and zero-day attacks

- Cyber warfare, (counter-)intelligence

- Skill-level: Master

High

THREAT AGENT SKILL LEVELS

What are the skill levels for the smart connected home threat actors?

Low

- Minimal technical skills
- Largest number of attackers
- Easiest to defend against

Medium

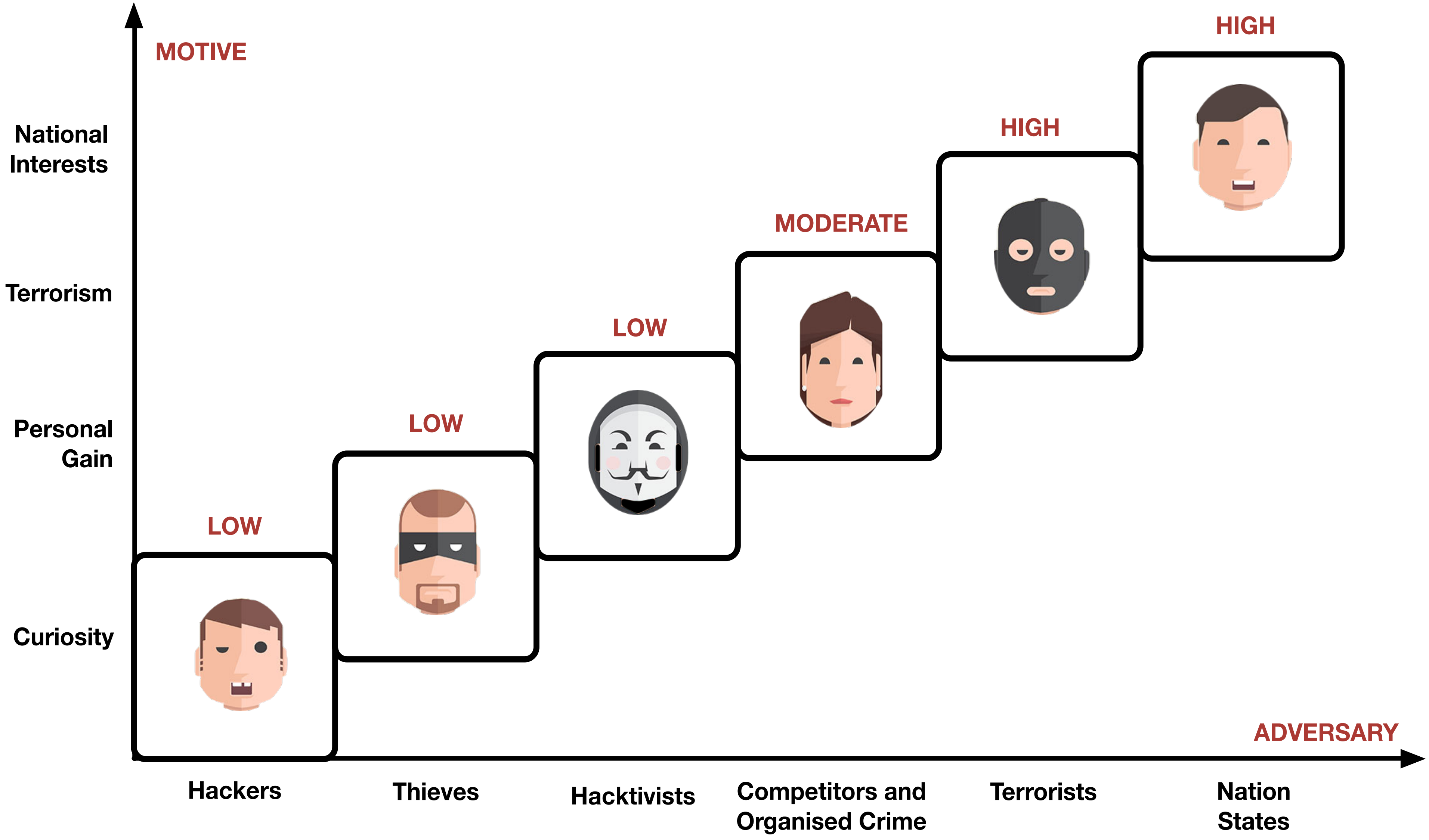
- Sufficient technical skills
- Locate new vulnerabilities
- Threat agents with such skills are likely found in all classes

High

- High-level technical skills
- Write new powerful attack toolkits
- Hardest to defend against

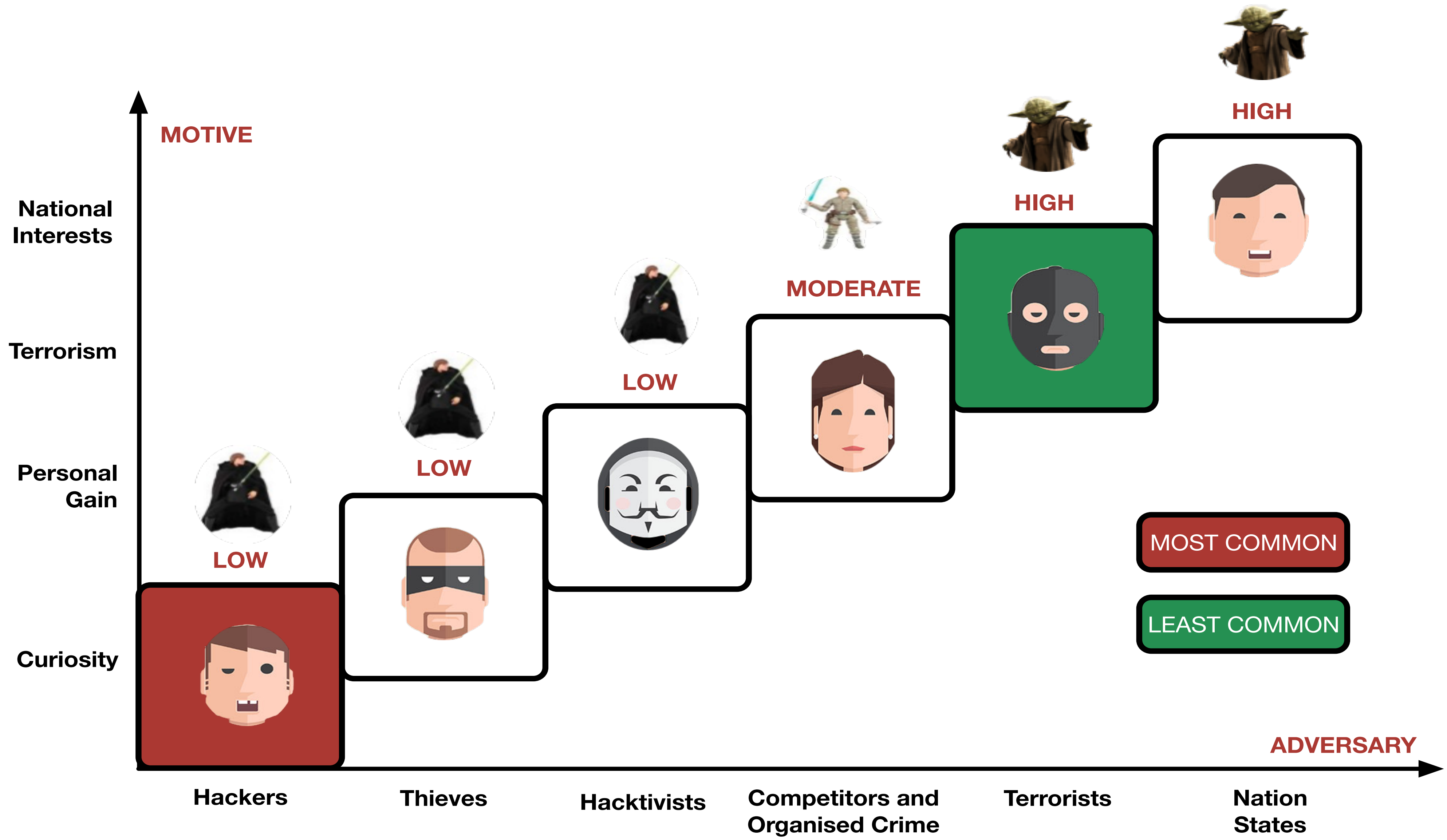
THREAT MODEL

What is a threat model that identifies the different threat agent profiles?



THREAT MODEL

What is a threat model that identifies the different threat agent profiles?



MOTIVE

National Interests

Terrorism

Personal Gain

Curiosity

LOW

LOW

LOW

MODERATE

HIGH

HIGH

MOST COMMON

LEAST COMMON

ADVERSARY

Hackers

Thieves

Hacktivists

Competitors and Organised Crime

Terrorists

Nation States

SOME REFLECTIONS

What are the prominent areas where further investigation and effort is required?

1 OPEN DATA

- Lack of IoT dedicated databases
- Absence of first-hand data

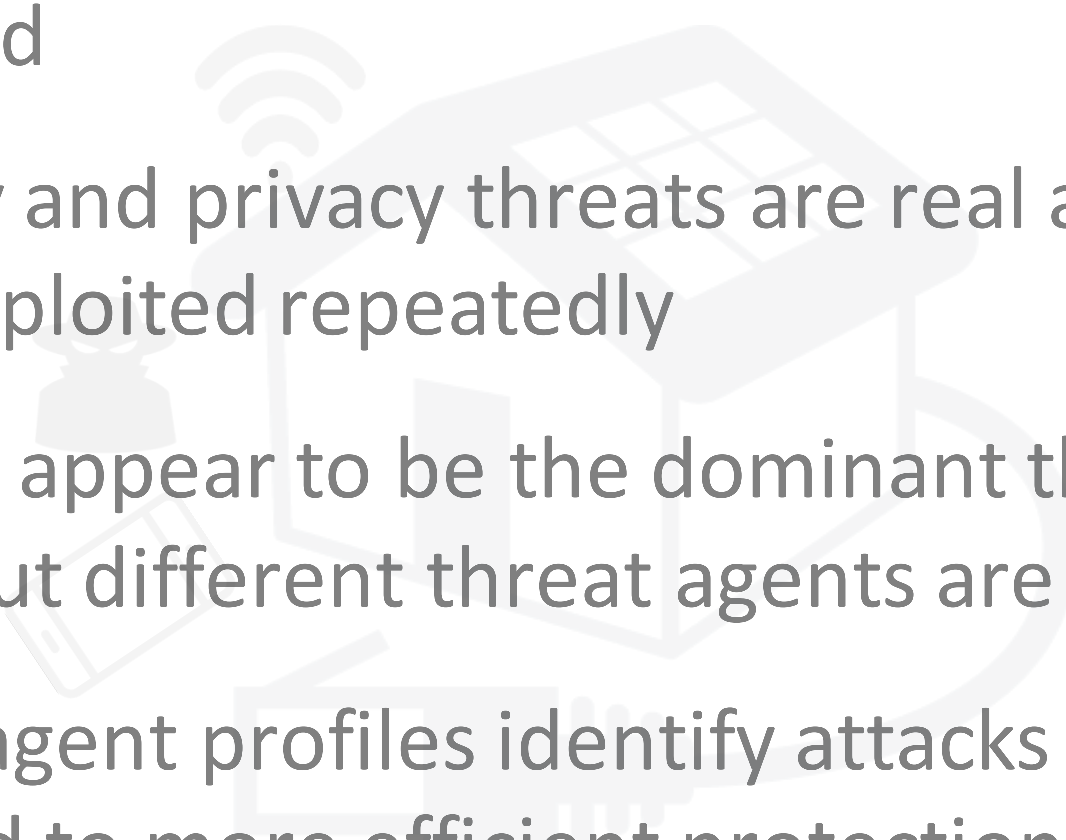
2 SECURITY EDUCATION & AWARENESS

- Default accounts in devices
- Weak password selection strategies

3 MODEL

- Shortage of IoT-based threat models
- Company-specific models

CLOSING REMARKS



- Home is the place where security and privacy is expected
- Security and privacy threats are real and have been exploited repeatedly
- Hackers appear to be the dominant threat agent but different threat agents are increasing
- Threat agent profiles identify attacks to expect and lead to more efficient protection strategies

FUTURE WORKS

What are possible avenues for future works?

- Formal modeling of attack descriptions

- Elaborating on the skills needed to attack smart homes

- Quantitative analysis of attacks on smart living spaces

Thank you for your attention!

✉ joseph.bugeja@mah.se

@BugejaJoseph

https://www.mah.se/iotap