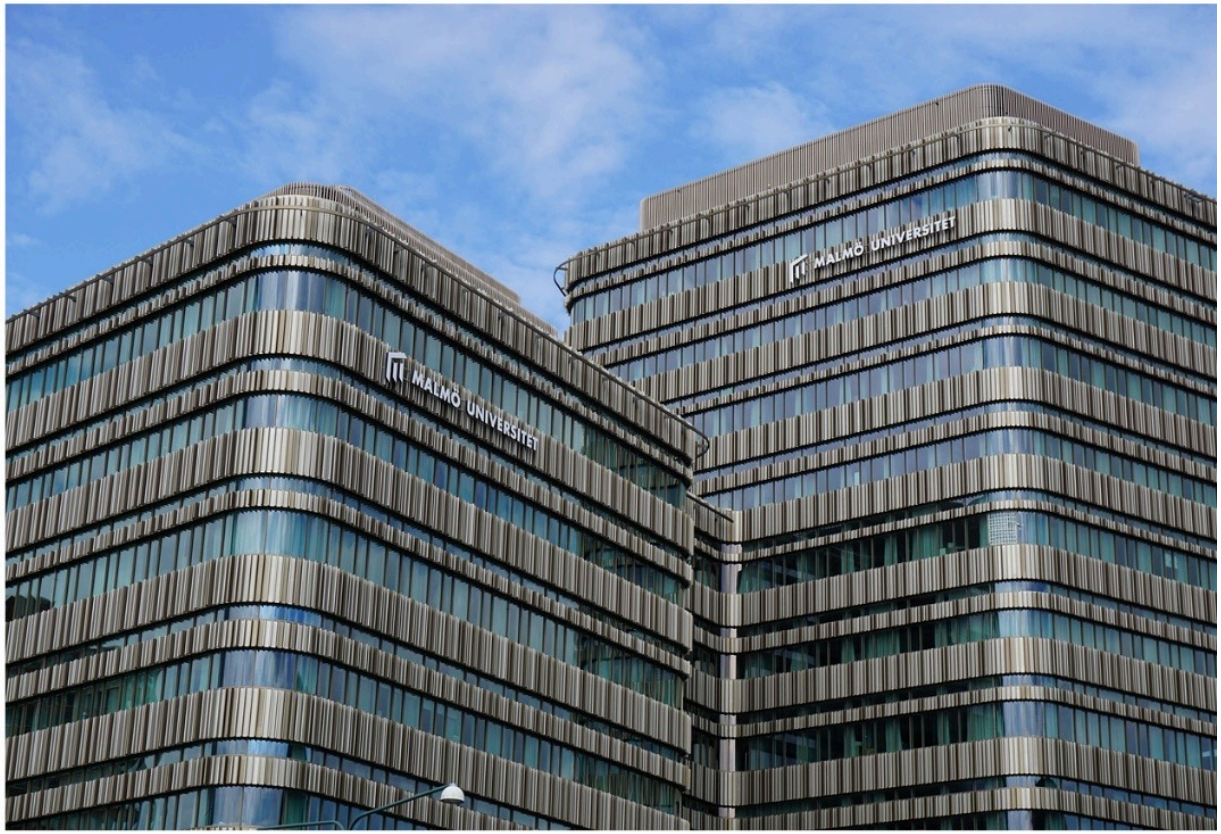
Securing the Internet of Things

Joseph Bugeja

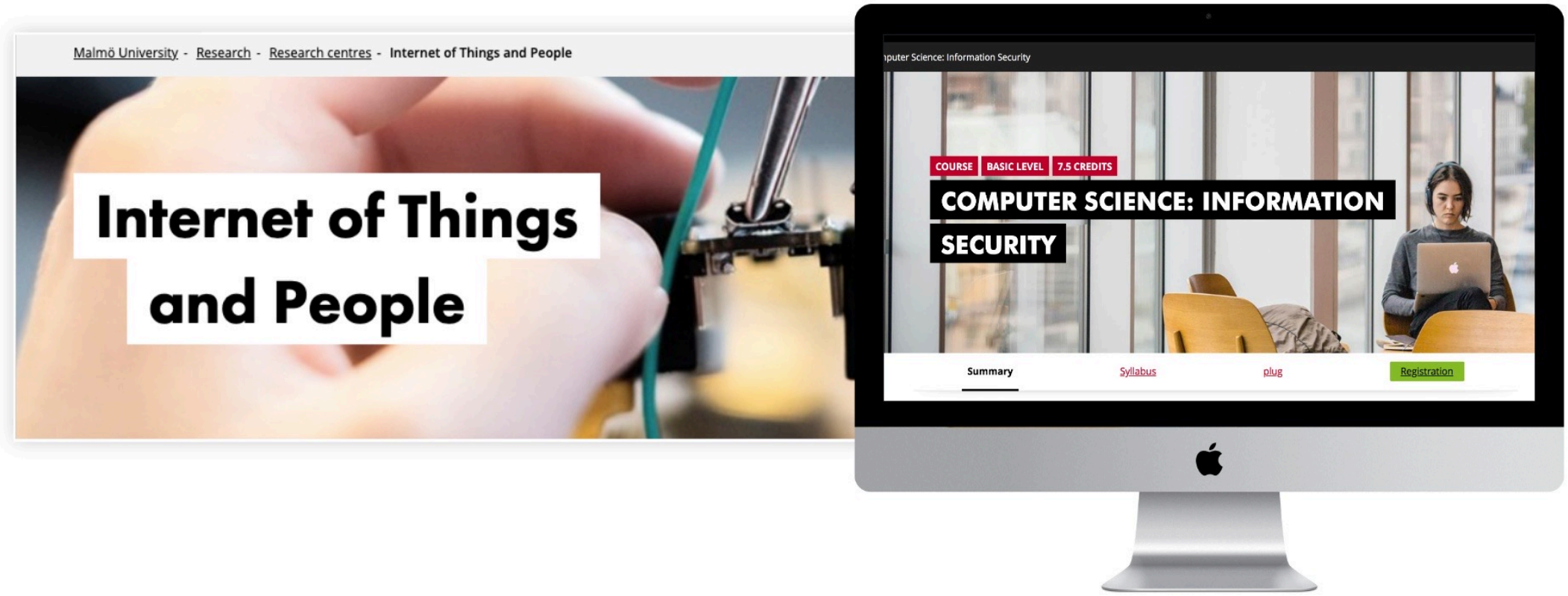
MALMÖ UNIVERSITY
INTERNET OF THINGS AND PEOPLE RESEARCH CENTER

About Me

- Postdoctoral researcher in Computer Science at Malmö University
- PhD in Computer Science and MSc in Information Security
- Research topics: security, privacy, IoT, and AI/ML



Researching and Lecturing at Malmö University



Agenda

- Introduction
- The Internet of Things
- Challenges in Securing the IoT
- Attacks and Malicious Threat Agents
- Safeguards

Introduction

A While Ago and Still

Fences

Locks

Signatures

The Landscape around us has changed

How can we secure these things?

E-Commerce

Smart speakers

Drones

From Lightbulbs to Vehicles can be a Target

Smart Lighting

Connected Cars

The Mirai Botnet

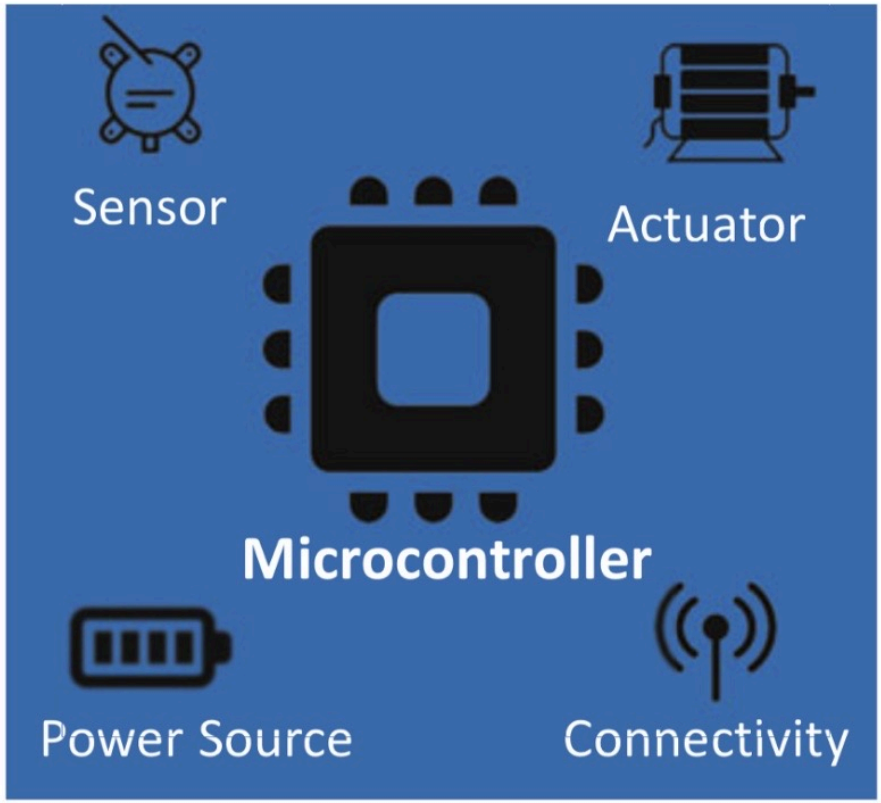
Securing the IoT is a Top Priority

“If everything is connected, everything can be hacked,” (EU Commission President, Sep. 2021)

European Commission President Ursula von der Leyen delivers 'State of the European Union' speech at the European Parliament in Strasbourg, France, 15 September 2021. [EPA-EFE/JULIEN WARNAND]

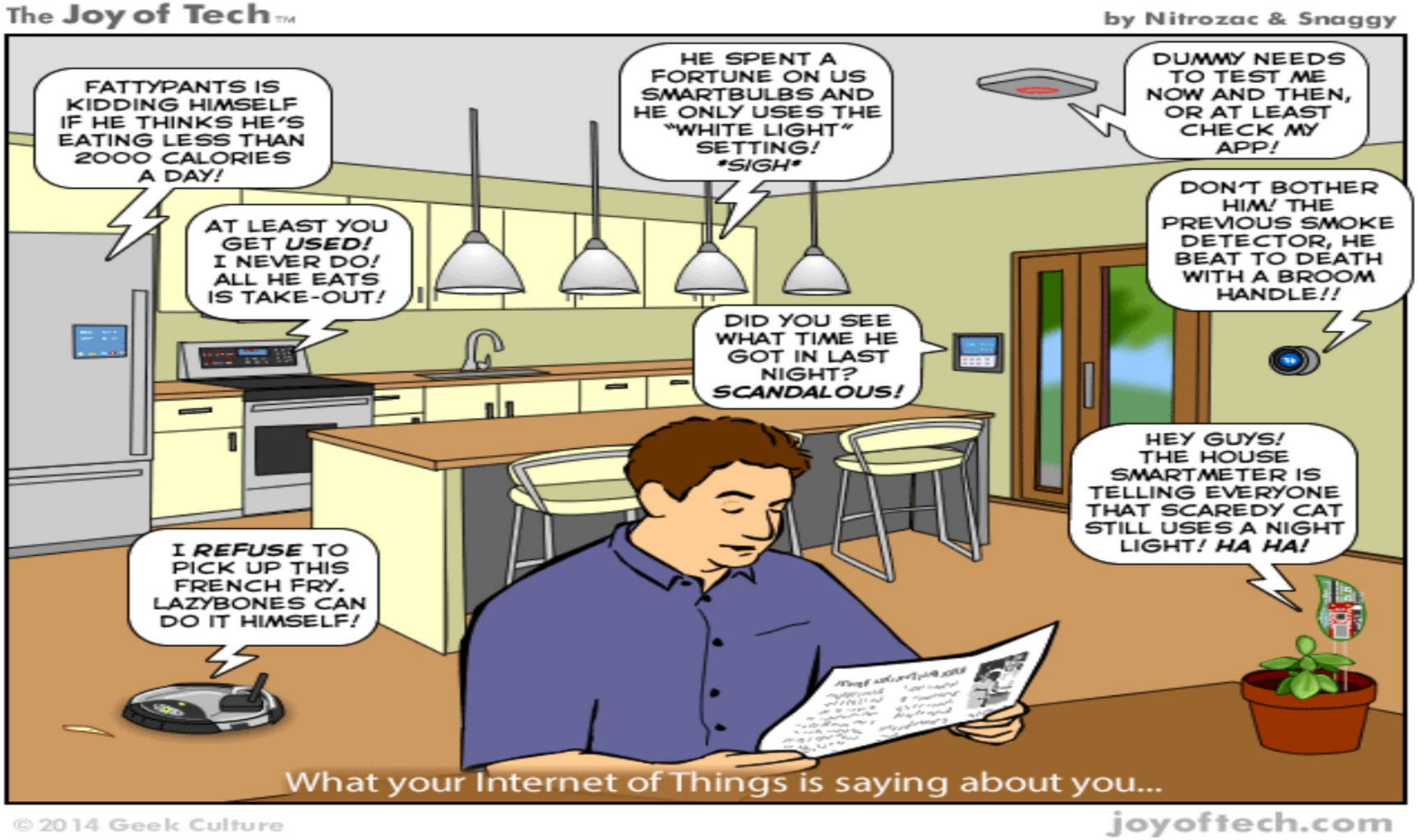
The Internet of Things

Things in an IoT Solution

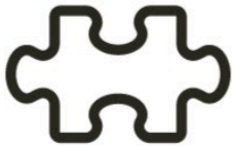


The Smart Connected Home

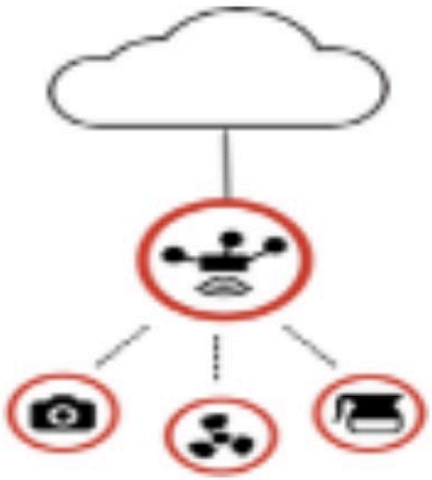
Digital Chatter happening inside the Smart Home



Challenges in Securing the Internet of Things



Some Network and Service Level Challenges



Heterogenous Protocols

Dynamic Communication

Longevity Expectations

Attacks and Malicious Threat Agents

Information Security Definition

Information security is generally defined as the preservation of *confidentiality*, *integrity* and *availability* of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved (ISO27001)

Denial of Service Attack on IoT Devices

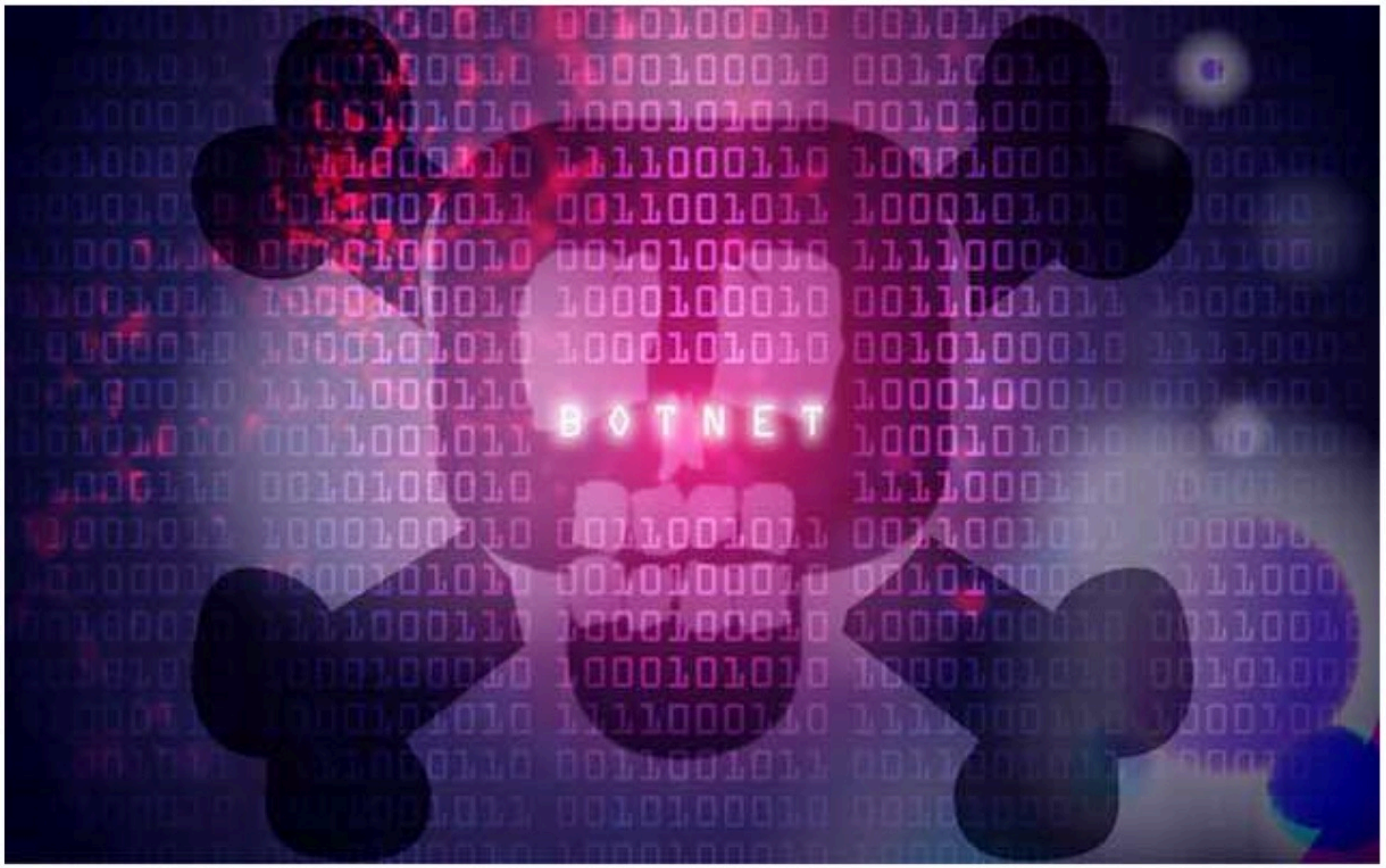
- Battery draining: By depleting the battery of a connected device, e.g., a smoke detector, an attacker will be able to disable a fire detection system

- Sleep deprivation: An attacker may attempt to send an undesired set of requests that seem to be legitimate but are not

- Outage attacks: Devices may stop functioning as a result of an unintended error in the manufacturing process, battery draining, sleep deprivation, etc.

Gafgyt Malware targeting Wireless Routers

- Gafgyt variant targeting small office/home wireless routers
- Uses remote code execution to gain access and recruit routers into botnets
- Causes a DoS



Malicious Injection as an Attack on Services

- Insufficient validation of the input may enable malicious input injection
- An attacker could inject a malicious input that causes the service providers to perform operations on behalf of the attacker
- For example, an attacker may add an unauthorized component that is capable of injecting malicious inputs into the servers. Afterwards, the attacker might be able to steal data, compromise database integrity, or bypass authentication
- Standard database error messages returned by a database may also assist the attacker

Vulnerabilities in Camera's Web and Mobile app

- Attackers can for example execute XSS in the web app and the mobile app may ignore server certificate validity
- Could allow for viewing video feeds, removing saved clips, install new firmware updates, etc.
- A direct connection to the device may not be required!

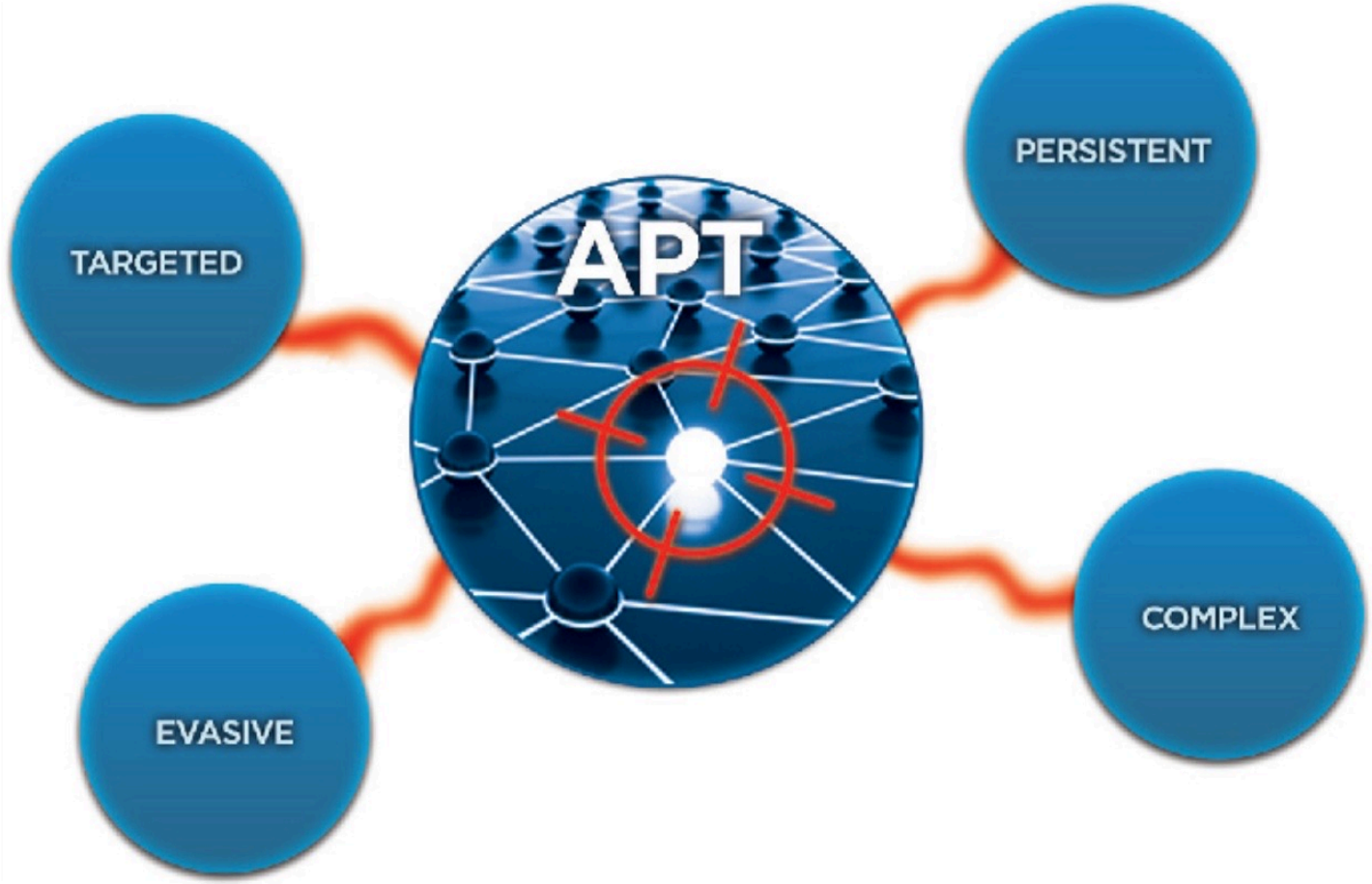
Focus on the Enemies

“Know your enemy and know yourself and you can fight a thousand battles without disaster” - Sun Tzu

Nation States

- Highly sophisticated individuals that are funded by governments and associated with a military unit
- Customized malware, spear phishing attacks, and zero-day attacks
- Cyber warfare, (counter-)intelligence
- Skill-level: Master

Advanced Persistent Threats

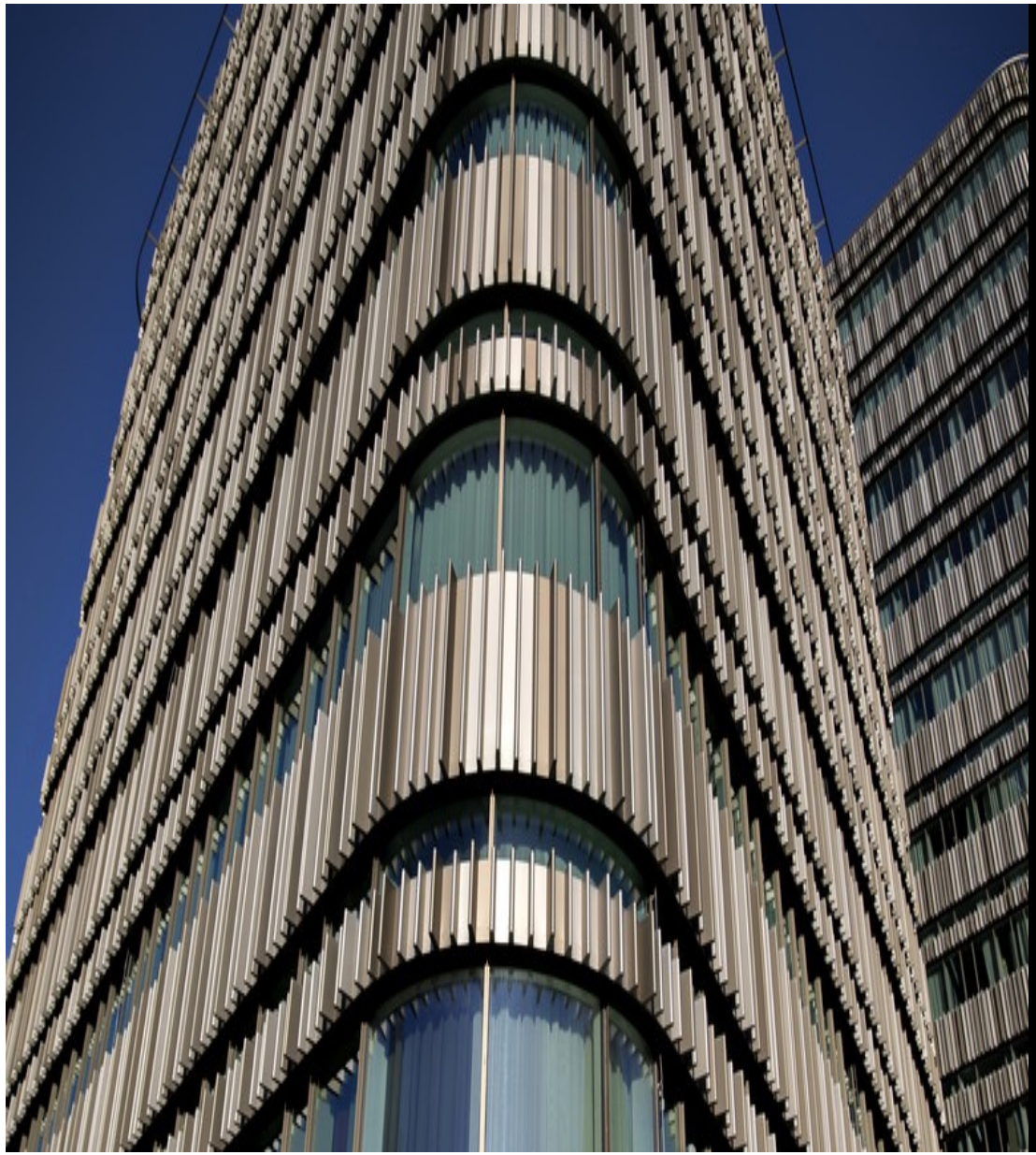


Source: Ask, M. (2013). Advanced Persistent Threat (APT) Beyond the hype Project report in IMT 4582 Network security at Gjøvik University College during spring 2013.

Safeguards

Defending against DoS Attacks

- Intrusion Detection Systems (IDSs) provide a reliable approach to defend against battery-draining and sleep deprivation attacks by detecting unusual requests to the node
- Certain IDSs are designed to meet the requirements of IPv6 connected nodes of IoT, making it possible to detect various routing attacks
- IDSs can also detect the existence of a malicious node that tries to inject invalid information, including code injection attacks, into the system or violate a policy



Thank you for your attention!

bugejajoseph.com

IamJosephBugeja

joseph.bugeja@mau.se