MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

University of Cyprus

MAI650 Internet of Things

Vasos Vassiliou

September - December 2023

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CS6xx Internet of Things (8 ECTS)

Course purpose and objectives: The purpose of the course is to provide an overview on IoT tools and applications and to introduce to students hands-on IoT communication concepts through lab exercises.

Learning outcomes: Upon completion of this course, students will be able to explain the definition and usage of the term “Internet of Things” in different contexts. More specifically, the students will know how to apply the knowledge and skills acquired during the course to build and test a complete, working IoT system involving prototyping, programming and data analysis

Teaching methodology: interactive face-to-face lectures, group activities and discussions, in class/lab activities, student presentations and guest lectures or significant recorded public lectures

Assessment: Final exam (50%), midterm exam (20%) and assignments/project (30%).

Main text:

Rajkumar Buyya, Amir Vahid Dastjerdi, Internet of Things Principles and Paradigms, Morgan Kaufmann; 1st edition, 2016

J. Biron and J. Follett, "Foundational Elements of an IoT Solution", O'Reilly Media, 2016.

Other reading:

Jamil Y. Khan and Mehmet R. Yuce, Internet of Things (IoT) Systems and Applications, 2019, ISBN 9789814800297

David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, and Jerome Henry, IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things, 2016, Cisco Press.

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

INTRODUCTION

Security and Privacy in IoT - Introduction

CONTENTS

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

INTENDED LEARNING OUTCOMES

Upon completion of this introductory unit, students will be:

1. familiar with the security terminology
2. familiar with different types of IoT Attacks
3. familiar how IoT Devices can be exploited

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

Introduction

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Security and Privacy

- IoT is connected to the largest untrusted network, the Internet, making it more vulnerable and appealing for malicious interventions.

- Some IoT application rely on accurate and on time information, for example:
  - Smart City
  - Smart Transportation
  - Monitoring critical infrastructures
  - Smart thermostat

- Loss of information can result to inaccurate environmental measurements and erroneous decision making.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Security and Privacy

- Users' Privacy may be compromised
  - Smart City applications can draw attention to perpetrators as the IoT applications become massive databases for the city.
  - Citizens cannot control the security level of the IoT and their privacy may be compromised

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

Security Terminology

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Security Terminology

- **Asset**
  - Items you value
  - There are many types of assets, involving hardware, software, data, processes, or combinations of these.
  - Devices that are part of the IoT

- How assets can be harmed?
  - Vulnerability: is a weakness that could be exploited to cause harm
  - Threat: is a set of circumstances that could cause harm
  - Attack: Act that causes damage to information or systems
  - A human who exploits a vulnerability perpetrates an attack on the systems.

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

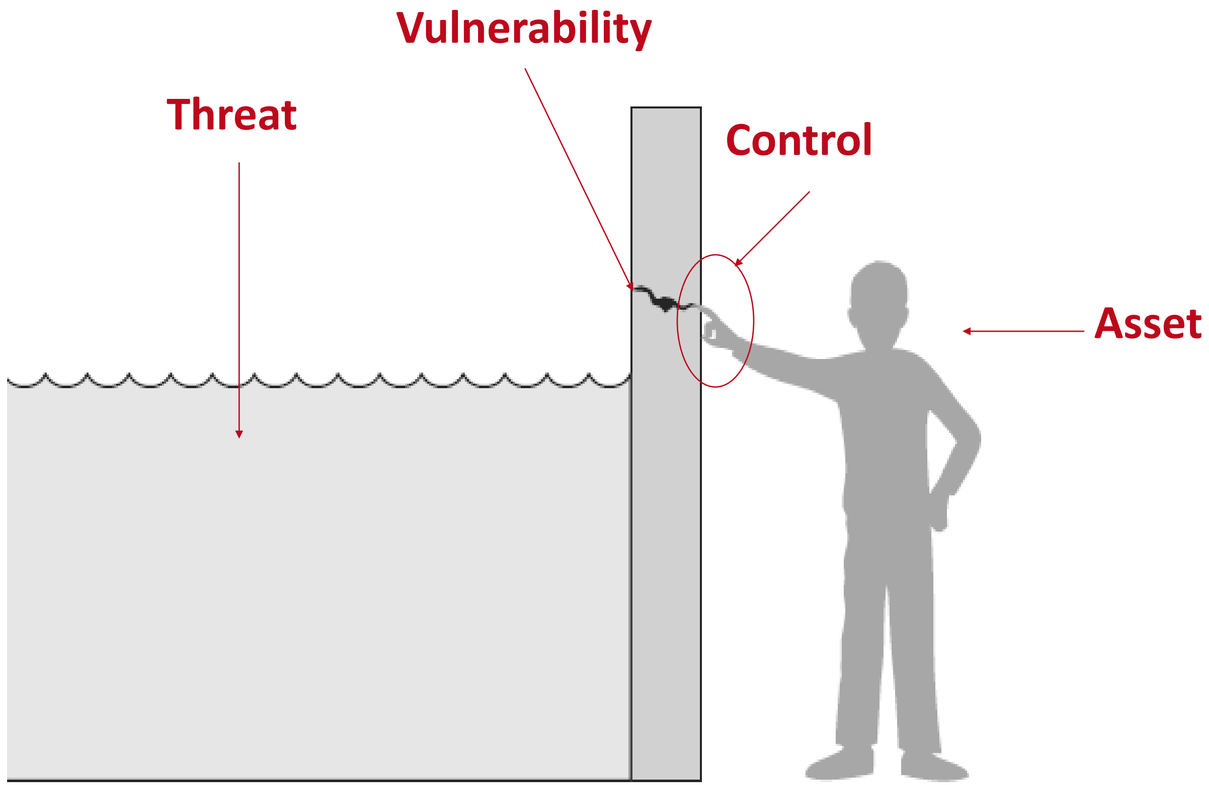
Security Terminology

- **Exploit**: Technique used to compromise a system
- **Exposure**: Condition or state of being exposed to attack
- **Risk**: Probability that something unwanted will happen

- How we address these problems?
  - We use a control or countermeasure as protection. That is, a control is an action, device, procedure, or technique that removes or reduces a vulnerability.
  - **Control, safeguard, or countermeasure**
    Security mechanisms, policies, or procedures

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Security Terminology



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

IoT Attacks

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Attacks

- Attacks aim in diminishing or eliminating a network's capacity to perform its expected function
  - Exploiting vulnerabilities in the system

- Security is a prominent area in the IoT and needs to be considered in all IoT architectural components.

- Three categories of attacks
  - Intrusion
  - Blocking
  - Malware

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Types of Attacks

Intrusion

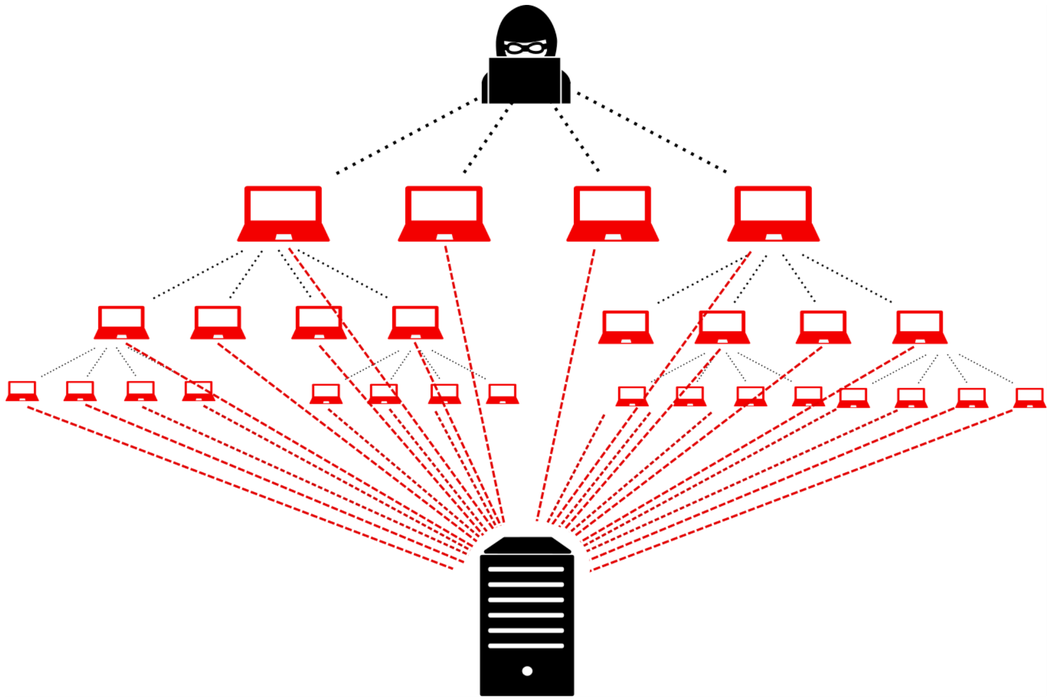
- Unauthorized access to a system

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Types of Attacks

Blocking

- Denial of Service Attack (DoS)
- Distributed DoS (DDoS) e.g. Mirai



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Types of Attacks

Malware

- Penetration of malicious software in an IoT aimed at performing unwanted and unauthorised actions.
  Examples: Ransomware, Viruses, Trojan horse and spyware

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Types of Attacks

Physical attacks

- **Vandalism**: Physical damages to the device by the attacker that gains physical access to the IoT environment

- **Theft**: The necessity to replace a damage or stolen device and may result in unplanned production

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Types of Attackers

Hackers

- Attempt to gain access to unauthorized resources
- Circumventing passwords, firewalls, or other protective measures

Disgruntled Employees

- Usually unhappy over perceived injustices
- Steal information to give confidential information to new employees
- When an employee is terminated, security measures should be taken immediately

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Types of Attackers

Terrorists

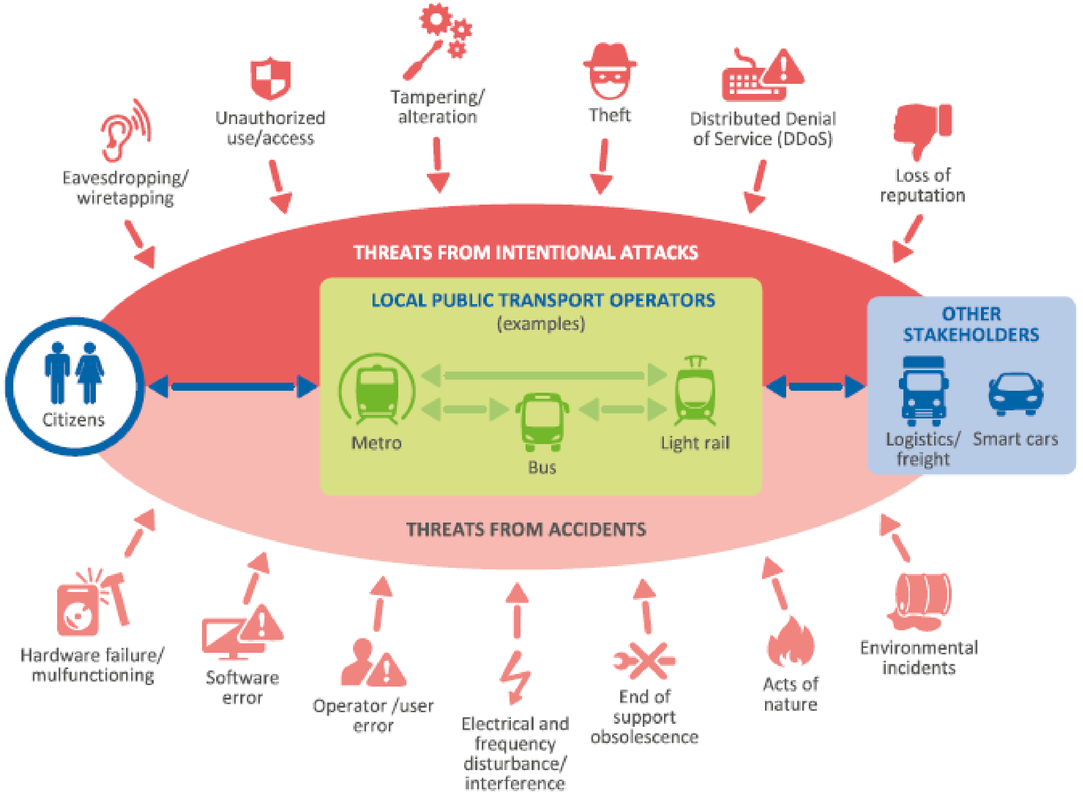
- Attack computer systems for several reasons
- Making a political statement
- Achieving a political goal
  Example: release of a jailed comrade
- Causing damage to critical systems
- Disrupting a target's financial stability

Government Operations

- A number of countries see computer operations as a spying technique

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Threats: Intelligence Public Transport (IPT)



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

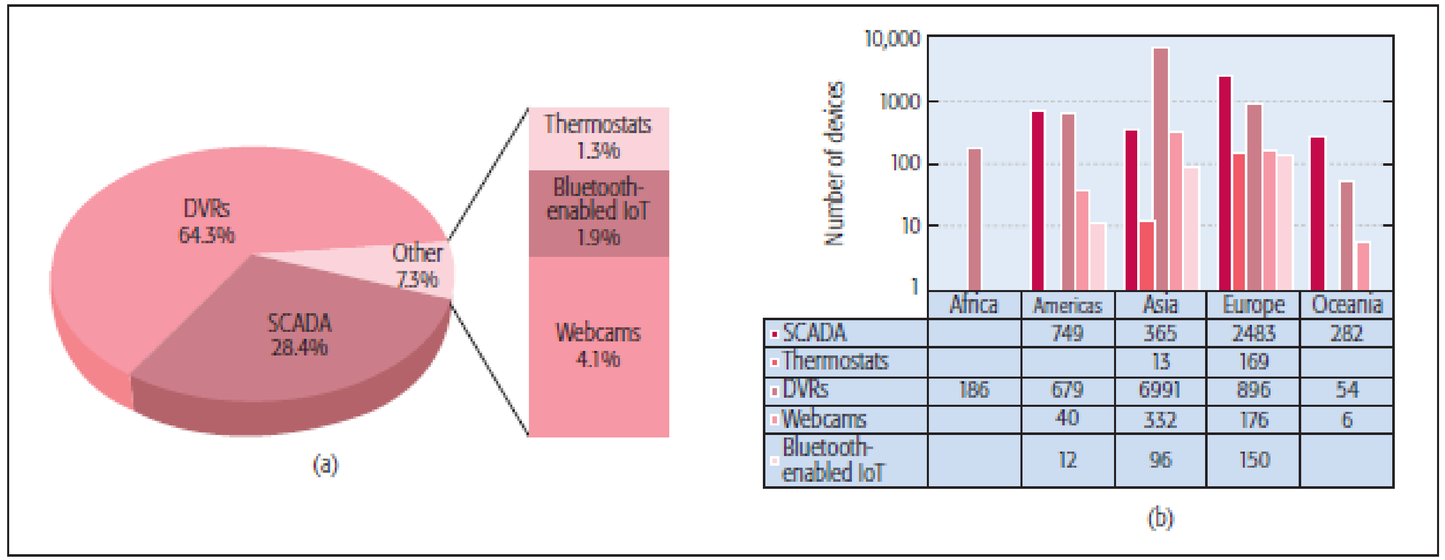
Master programmes in Artificial Intelligence 4 Careers in Europe

Exploited IoT Devices

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Exploited IoT Devices



Distribution of exploited IoT devices a) by type b) by type and region

F. Shaikh, E. Bou-Harb, N. Neshenko, A. P. Wright, and N. Ghani, "Internet of Malicious Things: Correlating Active and Passive Measurements for Inferring and Characterizing Internet-scale Unsolicited IoT Devices," IEEE Comm.Mag. (March 2018)

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Mirai Botnet – September 2016

- Scan the Internet for the IP address of Internet of things (IoT) devices
- Holds a list of IP Address ranges that it will not infect, including private networks and addresses allocated to the United States Postal Service and Department of Defense
- Uses a table of more than 60 common factory default usernames and passwords, and logs into them to infect them
- Overall, IP addresses of Mirai-infected devices were spotted in 164 countries.
- 500 000 known Mirai botnets

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Mirai Botnet – September 2016

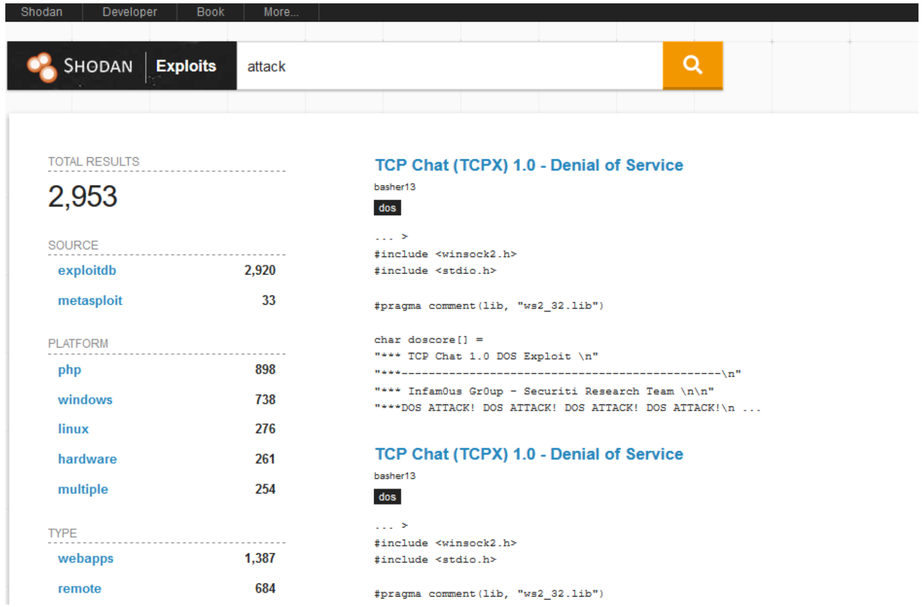
- Microprocessor is an IC which has only the CPU inside them
- They use same kind of CPU architecture than your PC or your smartphone
- Run a full Operating System: usually Linux-like
- PC with no keyboard, mouse nor screen

Username	Password
root	xc3511
admin	vizxv
support	admin
user	888888
Administrator	xmhdipc
service	default
supervisor	juantech
guest	123456
admin1	54321
administrator	support
666666	(none)
888888	password
ubnt	root
tech	12345
Mother	user

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Exploited IoT Devices

- Shodan:
  - a search engine for the Internet of Things.
  - Shodan allows users to find devices that are publicly accessible on the internet, and which may be vulnerable to hackers.
  - https://www.shodan.io



*Accessed 05/08/19

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Goals of IoT Security

- Providing Secure Connectivity
  - Secure connectivity with trusted users and networks
- Secure Remote Access
  - Provide secure remote access to IoT users
- Ensuring Privacy
  - IoT information need to be protected
- Providing Nonrepudiation
  - Ensuring that the sender cannot deny sending a message and the recipient cannot deny receiving it
- Confidentiality, Integrity, and Availability (C-I-A Triad)
  - Confidentiality: ensures that an asset is viewed only by authorized parties
  - Integrity: ensure that an asset is modified only by authorized parties
  - Availability: ensure that an asset can be used by any authorized parties

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

Summary

- ❑ Introduction
- ❑ Security Terminology
- ❑ IoT Attacks
- ❑ Exploited IoT Devices

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423