CONFIABILIDADE E SEGURANÇA CIBERNÉTICA
(DACYS)
PL04
*Jorge Pinto Leite (**JPL**)*
*Pedro Sousa Rodrigues (**DCR**), Nuno Peralta* (**NSP**)
{@isep.ipp.pt}

Exercise 1: IoT Landscape

Everything is connected. The world has changed and by the minute more devices have an Internet connection. The Internet changed from a global network of connected computers to a global network of 'things', of all things for that matter.
With the increase of connected systems, the attack surface also grows. Because of that is paramount to understand the potential attack vectors of today's reality.

1. What is the Mirai Botnet [1]?
2. Taking into account the Mirai bot, what vulnerabilities has it explored?
3. Explore some of the well-known IoT associated devices:
   (i) State Transfer (REST [2]);
   (ii) Simple Object Access Protocol (SOAP [3]);
   (iii) Message Queuing Telemetry Transport (MQTT [4]);
   (iv) Constrained Application Protocol (CoAP [5]);
   (v) Bluetooth Low Energy (BLE [6]);
   (vi) ZigBee [7].
4. Imagine that you are implementing an IoT network in your house. How would you secure such a network, taking into consideration the different protocols aforementioned?
5. Describe known attacks on each of the aforementioned protocols.

Exercise 2: Hardware hacking

Secure computing is a concerning topic. Some researchers say that having physical access to a device is only a matter of time until it gets compromised [8]. The topic of hardware hacking become ever so relevant in today's day and age. Cities are filled with sensors and cameras. The compromise of these devices can provide extra information to attackers and threaten our security and privacy rights.

1. What is UART [9]?
2. Why is it important to identify a UART port and secure it?

3. How can someone dump SPI [10] flash? What can they gain from it?
4. Download the firmware at https://www.downloads.netgear.com/files/GDC/D6000/D6000_V1.0.0.41_1.0.1_FW.zip
   (i) Analyse the firmware. What information can you obtain?
   (ii) Obtain the hardcoded credential in plaintext form from it.
   (iii) How you, a vendor, would protect firmware updates to be analysed in such a way?

Exercise 3: Building IoT networks

To understand how these IoT devices communicate, one should look at their comunications. IoT devices can implement several protocols to send information to an IoT hub that aggregates different sensors.

1. Implement an MQTT protocol exchange. You can rely on the follow link https://github.com/DamascenoRafael/mqtt-simulator [11]. Note: be sure to install the MQTT broker such as **mosquitto** [12].
2. Open Wireshark [13] and run the simulation. Inspect the packets.
3. What are the security considerations of what you see?
4. What changes would you make to the solution?
5. Implement certificates to secure communications. [14]

References

[1] "What is the mirai botnet? — cloudflare." [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

[2] "Representational state transfer," Oct 2022. [Online]. Available: https://en.wikipedia.org/wiki/Representational_state_transfer

[3] "Soap," Aug 2022. [Online]. Available: https://en.wikipedia.org/wiki/SOAP

[4] "The standard for iot messaging." [Online]. Available: https://mqtt.org/

[5] "Constrained application protocol," May 2022. [Online]. Available: https://en.wikipedia.org/wiki/Constrained_Application_Protocol

[6] "Bluetooth low energy," Oct 2022. [Online]. Available: https://en.wikipedia.org/wiki/Bluetooth_Low_Energy

[7] "Zigbee," Oct 2022. [Online]. Available: https://en.wikipedia.org/wiki/Zigbee

[8] "The cyberattacker's path of least resistance is shifting: Here's how you must adapt." [Online]. Available: https://www.beyondtrust.com/blog/entry/the-cyberattackers-path-of-least-resistance-is-shifting-heres-how-you-must-adapt

[9] "Universal asynchronous receiver-transmitter," Sep 2022. [Online]. Available: https://en.wikipedia.org/wiki/Universal_asynchronous_receiver-transmitter

[10] "Serial peripheral interface," Sep 2022. [Online]. Available: https://en.wikipedia.org/wiki/Serial_Peripheral_Interface

[11] R. Damasceno and M. Marcos, "Damascenorafael/mqtt-simulator: Easy-to-configure mqtt simulator written in python to simulate the sending of json objects from sensors or devices to a broker." [Online]. Available: https://github.com/DamascenoRafael/mqtt-simulator

[12] "Install mosquitto mqtt broker on ubuntu 20.04 server." [Online]. Available: https://www.vultr.com/docs/install-mosquitto-mqtt-broker-on-ubuntu-20-04-server/

[13] "Wireshark - go deep." [Online]. Available: https://www.wireshark.org/

[14] Steve, "Creating and using client certificates with mqtt and mosquitto," Aug 2022. [Online]. Available: http://www.steves-internet-guide.com/creating-and-using-client-certificates-with-mqtt-and-mosquitto/