2022 8th International Conference
on Energy Efficiency and Agricultural Engineering
EE&AE 2022

30th June - 2nd July 2022, Ruse, Bulgaria

Identification, vulnerability research and cybersecurity of Raspberry Pi devices

Filip Krastev, Nikolay Hinov

Technical university of Sofia, Bulgaria fkrastev@tu-sofia.bg, hinov@tu-sofia.bg

GOAL OF THE STUDY

The development of IoT technologies and IoT devices finds more and more applications in people's life. Along with improvement of the quality-of-life, IoT devices appear to be a great concern from security point of view. "Insecure" devices like Raspberry Pi are easy to takeover from the first boot of their OS, showing the need of more research on that subject.

One of the mostly used IoT devices is Raspberry Pi. It is a kind of personal computer with the size of a credit card, but with enough powers to compete with desktop PCs. Unfortunately, Raspberry's are shipped with OS having default credentials and SSH port open to log in.

Main objective is to investigate, simulate and detect vulnerabilities. The goal of this case study is to simulate specific vulnerability based on Raspberry Pi and it's OS. Secondary goal is to show how quickly flaw devices can be exploited and then be used for mining, for network mapping, for infecting more or for whatever reason a hacker would have. This imposes great security risks, and more research should be made to address them.

METHODOLOGY OF THE INVESTIGATION IS A SCRIPT IN PYTHON THAT:

- Scans over the network for suspected vulnerable Raspberry Pi's by MAC address
- Then establishes an SSH session on the open port 22 to the Pi using default credentials
- Send predefined or custom commands (payloads) to vulnerable Raspberry's
- The corrupted device will execute every command passed by the script, including elevated privileged root commands with "sudo"

MAIN RESULTS FROM THE STUDY

1. Identification of Raspberry Pi devices available on the network;
2. Verification that already identified Raspberry Pi devices can be accessed with default username and password;
3. When 1 and 2 are accomplished, attempts to inform the user. Then user is forced to choose between two options: change the default password or to create a new user with new password, and then delete the default user "pi";
4. Warning banner message is sent to the user on his terminal or on a pop-up window in the graphical UI followed by a warning that system will be forcedly shutdown;
5. A methodology that easily detects Raspberry Pí's with weak credentials was developed and packed with several options to fix automatically the default password problem.

EXPERIMENT DESCRIPTION

The experiment needed an invasive approach to simulate, investigate and finally propose a solution to the studied problem. The effective protection should be applied also automatically and remotely. Following exact same steps and procedure, the experiment was conducted in two scenarios – real and virtual. The real part of that experiment ends with static analysis and its topology is shown on Figure 1. The virtual part ends with dynamic analysis and the network topology shown on Figure 2.

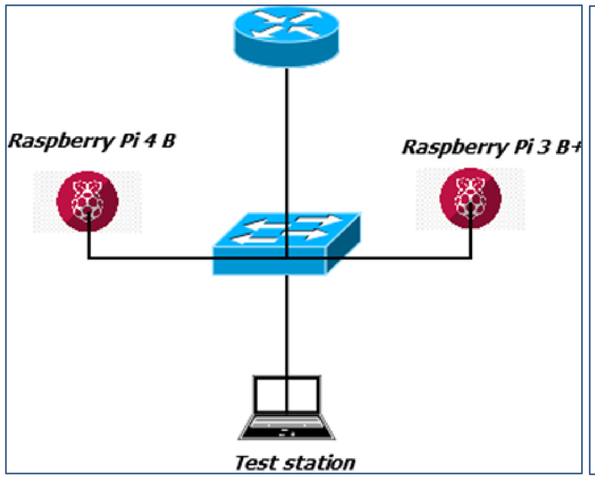

Fig. 1. Real life scenario topology

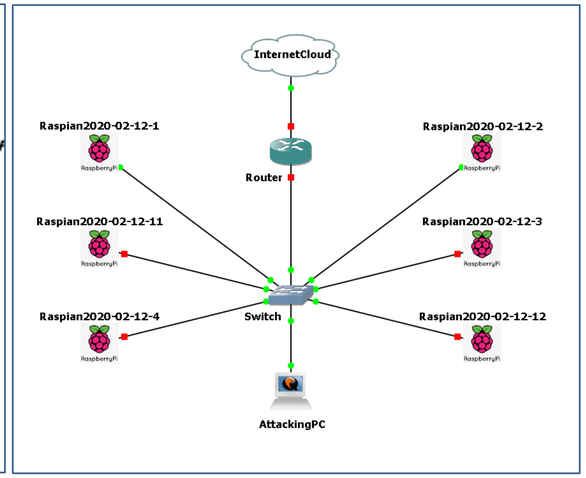

Fig. 2. Virtual lab setup topology

CONCLUSIONS

IoT devices like the Raspberry Pi will mostly find application in modern society, in smart cities, healthcare, private homes and in smart agriculture as well. Manufacturers of Raspberry Pi must be held responsible for the discussed vulnerability. It is impossible to influence in any way the manufacturers to change their policies. From the conducted experiments, it becomes clear that it's a severe flaw from cybersecurity point of view which should be addressed accordingly.

Depending on specific use case, the developed methodology can be used for penetration testing, device discovery and manipulation. Also it can be used as a tool to demonstrate and investigate different security aspects with students in cybersecurity classes.

Being an important topic in cybersecurity discussion, future development and work on the subject may involve creation of specifically modified version of the Raspberry OS with more tightened security. That custom OS should be installed remotely and automatically using the methods described in the study.