EMBEDI (https://embedi.com)

Home (https://embedi.com) / Blog (https://embedi.com/blog) / Analytics (https://embedi.com/blog/categories/analytics/) / Killchain of IoT Devices. Part 1

Categories:

- Analytics (https://embedi.com/blog/categories/analytics/)
- Research (https://embedi.com/blog/categories/research/)

Tags:

#ATM (https://embedi.com/blog/tags/atm/) #CISCO (https://embedi.com/blog/tags/cisco/)

#cybersecurity (https://embedi.com/blog/tags/cybersecurity/)

#D-Link (https://embedi.com/blog/tags/d-link/) #DJI (https://embedi.com/blog/tags/dji/)

#exploitation (https://embedi.com/blog/tags/exploitation/)

#firmware-security (https://embedi.com/blog/tags/firmware-security/)

#hardware (https://embedi.com/blog/tags/hardware/)

#hijacking (https://embedi.com/blog/tags/hijacking/) #intel (https://embedi.com/blog/tags/intel/)

#Microsoft (https://embedi.com/blog/tags/microsoft/) #mobile (https://embedi.com/blog/tags/mobile/)

#Office (https://embedi.com/blog/tags/office/) #RCE (https://embedi.com/blog/tags/rce/)

#router (https://embedi.com/blog/tags/router/) #SCADA (https://embedi.com/blog/tags/scada/)

#vulnerabilities (https://embedi.com/blog/tags/vulnerabilities/)

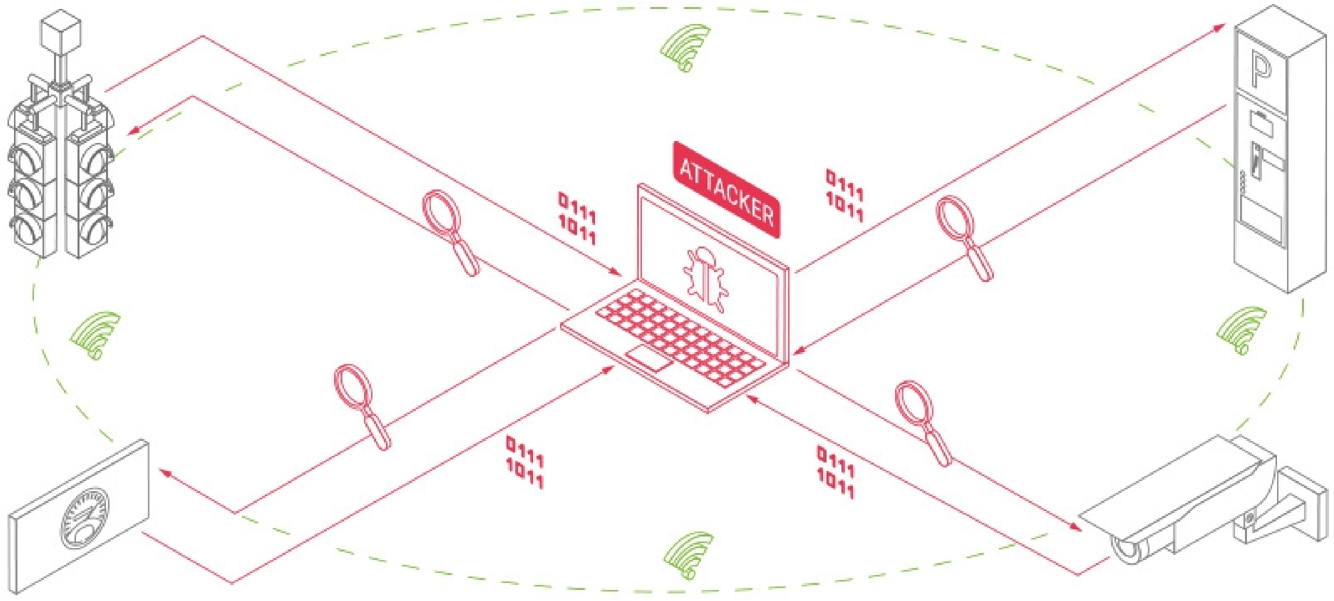
Popular articles:

Killchain of IoT Devices. Part 2 (https://embedi.com/blog/killchain-iot-devices-part-2/)

Killchain of IoT Devices. Part 1 (https://embedi.com/blog/killchain-iot-devices-part-1/)

8 June, 2017

Killchain of IoT Devices. Part 1



Category: Analytics (https://embedi.com/blog/categories/analytics/)
Tags: #cybersecurity (https://embedi.com/blog/tags/cybersecurity/), #vulnerabilities (https://embedi.com/blog/tags/vulnerabilities/)

Manufacturers are constantly trying to make smart-devices cheaper for both themselves and customers. Consequently, a manufacturer has to sacrifice security of a device in favor of its cost, size, and low energy consumption. These gadgets differ from each other by business logic, security logic, and human-device interaction method. Consumers should always keep in mind that every implemented security feature must be financed by manufacturers. Unfortunately, there are lots of smart-gadgets with poor security services available for a remote attacker. Users don't even think that their devices are dangerous and that these devices can be hacked in a matter of seconds.

So, it begs the question: is there anything new in the world of embedded devices, in comparison to traditional networks, that manufacturers must face extra costs to prevent security breaches? To answer this question, we're going to use the kill-chain model adapted for a smart-world.

The kill-chain model defines steps, that intruders must perform over their targets to achieve their goals. Security administrators can use this model as a tool that allows companies to increase their overall security level: each step of the kill-chain model should be performed by an attacker and consequently, security-specialists try to disrupt this chain or make each step extremely hard for cyber-criminals.

The kill-chain model breaks down an uninterrupted chain of attack steps as follows:

- reconnaissance – attackers attempt gathering information to achieve success with their future attack;
- weaponization – attackers create exploits, tools, malware;
- delivery – attackers' weapon is delivered to a victim;
- exploitation – attackers exploit a vulnerability in a victim's system to trigger their malicious software (or malware) code;
- installation – attackers gain a foothold on the victims system by installation a backdoor with a malware ;
- command and control – creating a command communication for a remote control of a device;
- actions on objectives – attackers start their malicious activity, according to their goals.

We are going to divide our discussion of the kill-chain model into two chapters: you can learn its first three steps here, other steps will be covered in the second chapter.

The main difference that manufacturers and consumers should understand is that embedded-devices are no longer abstract entities: they are tangible and closer to human than any previous cyber technology. You can come across them everywhere in your daily life and still be unaware of their existence: smart-watches or fitness trackers on your wrist, smart-sensors in your car's engine, smart-locks that make doors and windows in houses or plants more secure, medical-sensors that monitor your health in hospitals, and so on. The purpose of smart-gadgets is to interact with other devices and to be available for human control. Nowadays devices are like tiny servers that can be available outside.

The world of smart-devices uses a bunch of entirely new protocols that allows devices to be more resource saving, secure, and useful.

By using the data-link layer and physical layer protocols, like RFID or Bluetooth, without the network functionality layer, we can create an ecosystem of IoT devices. So, these devices can be unavailable outside from the traditional Internet.

Therefore, at the reconnaissance step, an attacker can extract information from the net such as used protocols (IPv6LoWPAN, 5G and others), IP-address, open ports, whether it communicates with Cloud or any other external services. An attacker can find an ecosystem, consisted of devices that are unavailable from the net – such devices may be detected only in their communication area by special sniffers, like Ubertooth. In other words, cyber-criminals can gather information either remotely (e.g., search engine Shodan enables them to find victims in a few seconds) or by being within the range of communication protocols (e.g., cyber-criminals can adapt wardriving, when attackers moving in a car detecting vulnerable Wi-Fi spots, for other protocols).

One can't predict what types of information will be collected by an attacker. For example, smart-gadgets use DNS requests containing information about their manufacturers, like well-known service names. Therefore, cyber-criminals have a good chance to hack a device by using unfixed vulnerabilities that are common for some manufacturers.

Numerous advantages of smart-gadgets, like ease of operation and mobility, allow consumers to use smart devices outdoors: on city streets and other places, where they couldn't have been used before. As a consequence, an attacker can interact with them directly. Devices may have interfaces for testing and debugging, like UART, JTAG, SPI. By using these interfaces, cyber-criminals can gather all the information about the software installed on a victim's device.

So, the reconnaissance step enables hackers to identify the type of a victim's device, used protocols, communication channels with Internet services, hardware constituents and software. Also, it is extremely useful for attackers to learn a software version that runs a device, because intruders can use well-known vulnerabilities to attack a device by exploiting flaws in an identified software. In addition, attackers may refrain from using their hacking tools, as a device is surely protected against some types of attacks.

The next step is the weaponization, where intruders prepare their hackers' stuff. An attacker needs to know the features of a victim's system and construct a weapon, according to these features. Basically, smart-devices run RTOS and Linux-based operating systems on RISC-architecture. RISC-architecture differs from that of traditional PC's, which is based on CISC-architecture in a number of instructions. Hence, cyber-criminals have to adapt their tools to a new environment, because misconfigured malicious software can alert victims with error notifications or even cannot be launched.

The delivery step is quite similar to the traditional one, but we should understand that the risk of being compromised with phishing attacks decreases significantly, because embedded-devices won't surf the net and download any files for their own entertainment involuntarily.

The world of smart-gadgets is still quite young, but we are sure, that in a few years this technical approach will become an essential part of our everyday life. Smart-devices have their advantages which encourage IT specialists to invent new services. Full insight into IoT pros and cons enables us to make this technology safer, and, consequently, closer to reality. Unfortunately, modern devices are weak and our next discussion will cover the most common vulnerabilities, which can be used to exploit smart-gadgets.

()

(https://www.linkedin.com/shareArticle?mini=true&url=https://embedi.com/blog/killchain-iot-devices-part-1/&title=Killchain of IoT Devices. Part 1)

(http://www.twitter.com/intent/tweet?url=https://embedi.com/blog/killchain-iot-devices-part-1/&text=Killchain of IoT Devices. Part 1)

Subscribe to our newsletter to stay in touch

Enter your email here Submit

Solutions (https://embedi.com/solutions/) Blog (https://embedi.com/blog/)
Our news (https://embedi.com/news/) Resources (https://embedi.com/resources/)
About (https://embedi.com/about/)

(https://www.facebook.com/Embedi/) (https://www.linkedin.com/company/embedi)
(https://twitter.com/_embedi_) (https://github.com/embedi/)
(https://www.youtube.com/channel/UC9XR2noZynNxvQcg0G9ooKA)