CYBER SECURITY ANALYSIS OF IOT DEVICES TRANSMITTING DATA IN THE THINGSPEAK PLATFORM CLOUD

DRAGOS-ALEXANDRU ANDRIOAIA[1*]

[1] *"Vasile Alecsandri" University of Bacau, Calea Marasesti 157, Bacau, 600115, Romania*

Abstract: The IoT platforms have started to be used more and more due to numerous applications in which they can be used. With the growth of devices that transmit data to the cloud of IoT platforms, security challenges have also emerged. The security of IoT platforms can be analysed, identifying vulnerabilities to attacks on each layer of the IoT architecture. In this paper, the authors test, through an active sniffing attack, the cybersecurity of the IoT devices that transmit data to the Cloud of the ThingSpeak platform. Through this attack, it will analyses whether IoT devices send the data to the ThingSpeak platform's cloud in the clear, without encrypting it.

Keywords: IoT security, sniffing IoT attacks, ThingSpeak, IoT, IoT attacks

1. INTRODUCTION

With the increase in the number of IoT devices, so has the number of IoT platforms. IoT platforms can provide control and monitoring of data transmitted by IoT devices [1]. Among the most used IoT platforms we can remember: IBM Watson IoT, Oracle Integrated Cloud IoT, Amazon Web Services (AWS), Microsoft Azure IoT suite and ThingSpeak.

ThingSpeak is an open-source IoT platform that allows real-time visualization and analysis of data transmitted by IoT devices in the cloud. Moreover, with MATLAB analytics in ThingSpeak, data can be processed and then we can view and analyse the result of the processing. The platform API used to retrieve data sent by IoT devices uses THE HTTP and MQTT protocols [2].

The security of IoT systems is given by the vulnerabilities that can occur on each layer of architecture, perception layer, network layer, middleware layer and application layer. On the perception layer we can have, sensors of temperature, humidity, light etc. We can still have technologies like GPS or RFID here. This layer can be affected by attacks of type: Node catching, Eavesdropping attacks, Code injection attack, Booting attacks and Side-channel attacks. The network layer is responsible for transmitting data from the perception layer on the middleware layer. May be affected by the following types of attacks: DDoS attack, Phishing attacks, Sinkhole attack and RFID spoofing. The middleware layer is used to confirm the authenticity of users and to transfer data. On this layer we can encounter the following attacks: Insider attack, SQL injection attack and Man-in-The-Middle attack. Last layer, the application layer provides end-user services and may be affected by the following attacks: Sniffing attacks, Reprogram attacks, Data theft and Service interruption attack [1, 3].

Following a Sniffing attack, the data flow between IoT and Cloud devices can be intercepted, and if there is no minimum encryption, the information transmitted can be disclosed.

[*] Corresponding author, email: dragos.andrioaia@ub.ro

doi.org/10.29081/jesr.v28i3.003

In this paper, the Cyber Security of the devices that transmit data in the cloud of the ThingSpeak platform was analyzed.

2. METHODOLOGY FOR TESTING CYBER SECURITY THROUGH A SNIFFING ATTACK OF THE IOT DEVICE THAT TRANSMITS DATA TO THE THINGSPEAK PLATFORM CLOUD

2.1. Implement the IoT environmental temperature monitoring system using the NodeMCU development board and ThingSpeak cloud platform.

The block scheme of the IoT system used for temperature monitoring is shown in Figure 1. The data collected by the temperature sensor is transmitted to the Samsung platform's cloud by connecting the System On Chip (SOC) ESP8266 (NodeMCU) WiFi module to an Internet-connected home router [4, 5].

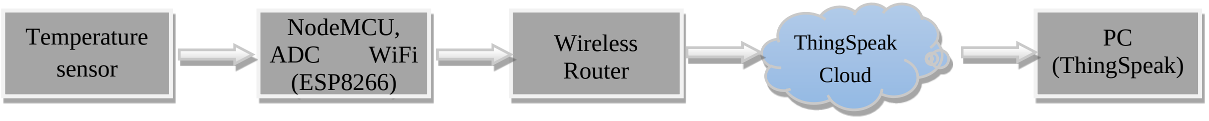


Fig. 1. System block diagram.

The information stored on the ThingSpeak server can be accessed via an open Browser from an Internet-connected terminal. The ThingSpeak platform allows you to display the temperature variation graph over a selectable time.

The electrical wiring scheme can be viewed in Figure 2. The KY-028 sensor was used in the electrical temperature determination scheme, which can measure the temperature value in the range -55°C to 125°C. Temperature information is given on the basis of the change in the electrical resistance of the thermistor. The temperature value is converted into analog information and is transmitted to pin A0 of the NodeMCU development plate.

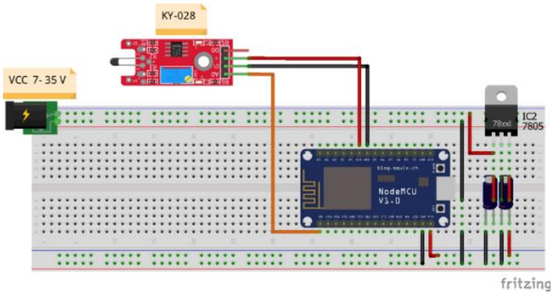


Fig. 2. Electrical wiring scheme.

NodeMCU is a development board containing SoC ESP8266, developed by Espressif Systems. It contains, a 32-bit microcontroller (Tensilica L106), 50K RAM, a 2.4GHz WiFi module, 17 GPIO input and output pins and an analog-digital converter (ADC). The processor can work at speeds between 80~160MHz, the current consumed is in the range 10uA~170mA and the aliments voltage is 3.3V [5, 6].

The ThingSpeak platform allows you to purchase real-time data as well as view it as charts. After the user account has been created, you must create a channel to view the temperature variation graph relative to time. A Keys API will be generated at the end of the channel configuration. Using the ThingSpeak API we can publish information on the channel from my NodeMCU module [7].

NodeMCU programming was performed using Arduino IDE. The source code of the program developed for the microcontroller of the SOC ESP8266 module, allows the processing of information from the temperature sensor and sends it via the WiFi connection between NodeMCU and the home router to the Internet to the ThingSpeak server.

2.3. Implementation of a sniffer-type cybernetic attack

Sniffing allows a security tester to analyse network traffic. Sniffing can be active or passive. The active sniffing involves redirecting traffic through the security tester in order to capture and monitor packages. Traffic redirection can be achieved by means of an MITM attack. Passive sniffing allows a tester to monitor and capture network traffic without initializing an attack to redirect traffic. The block diagram illustrating the MITM attack implemented within the local network can be viewed in Figure 3 [8, 9].

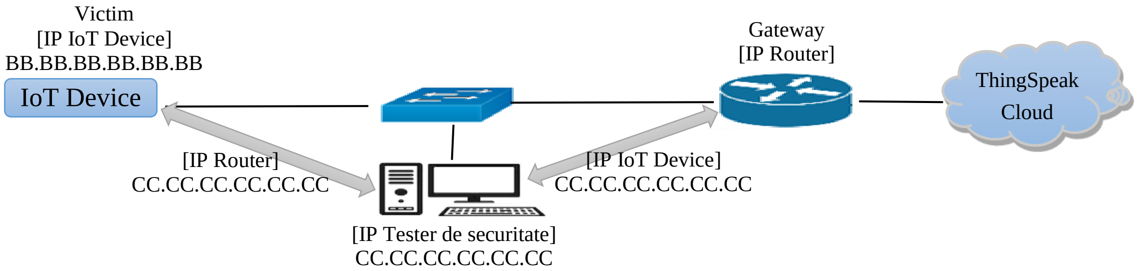


Fig. 3. MITM attack.

In an MITM attack, the attacker performs ARP poisoning between the victim (IoT Device) and the gateway. In the first step, the attacker "intoxicates" the target host, with ARP responses announcing the MAC address corresponding to the IP address (gateway), then the attacker "intoxicates" the GATEWAY with ARP responses by announcing the MAC address corresponding to the IP address of the victim. A device on the network that receives an ARP response, even if it has not submitted the ARP request, must update its cache table (the so-called "cache-ARP"). This has the effect, that all packets of data exchanged victim and gateway will go through the attacker, who tries to extract sensitive information from them. ARPspoof is a tool that can be used to deploy an MITM attack. The steps of an MITM attack are [9-12]:

- It will be done forward to traffic using the syntax:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

- It will inform the victim that the attacker's PC is the router:

```
arpspoof -i [network adapter] -r -t [IP IoT Device] [IP Router]
```

- We inform the router that the attacker's PC is the victim:

```
arpspoof -i [network adapter] -r -t [IP Router] [IP IoT Device]
```

After the MITM attack is met, a sniffing tool will be used to listen to traffic. Wireshark is one of the most widely used sniffers tools, which can capture and display network packages in real time.

3. RESULTS AND DISCUSSION

After creating and configuring the ThingSpeak channel, the NodeMCU development board transmitted data on temperature variation relative to time in the IoT platform cloud. The temperature variation graph in relation to time in the 09AM – 1PM time frame, displayed via a ThingSpeak channel, can be viewed in Figure 4.

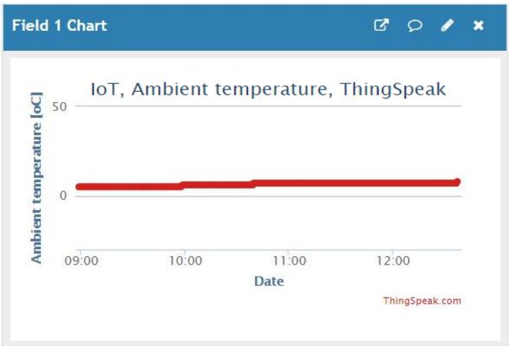
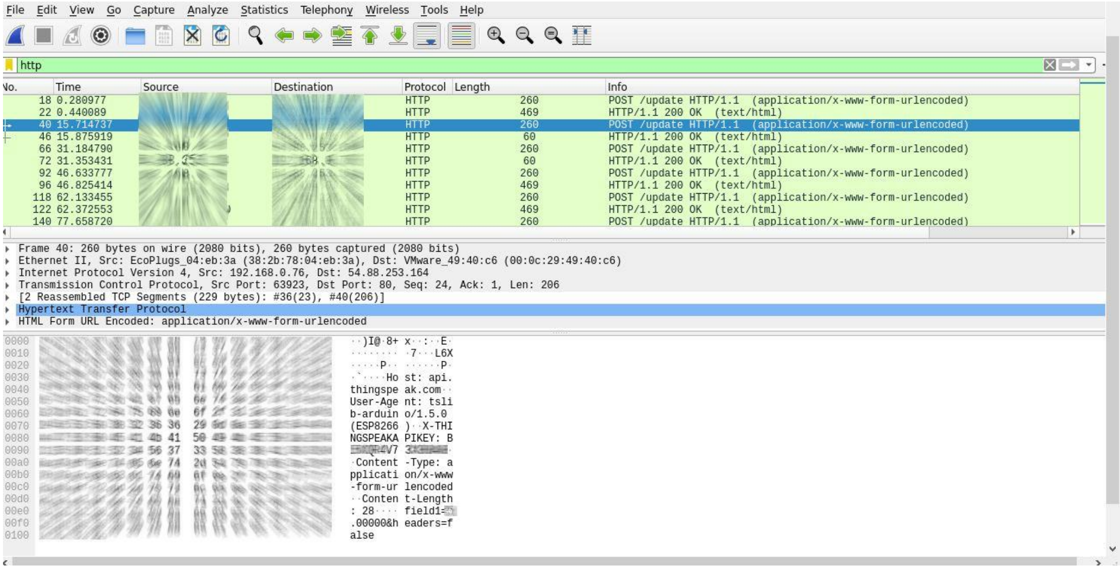


Fig. 4. Temperature variation graph in relation to time in the time range 09AM – 1PM.

The active sniffing attack was implemented from the local network to which the IoT device was connected. For its implementation, the security tester used a PC that had SO Kali Linux installed. Data packets, redirected via the ARPspoof tool and analysed through the Wireshark tool, can be viewed in Figure 5.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time       Source      Destination  Protocol Length  Info
   18 0.280977   [redacted]  [redacted]   HTTP     260     POST /update HTTP/1.1  (application/x-www-form-urlencoded)
   22 0.440089   [redacted]  [redacted]   HTTP     469     HTTP/1.1 200 OK  (text/html)
   40 15.714737  [redacted]  [redacted]   HTTP     260     POST /update HTTP/1.1  (application/x-www-form-urlencoded)
   46 15.875919  [redacted]  [redacted]   HTTP      60     HTTP/1.1 200 OK  (text/html)
   66 31.184790  [redacted]  [redacted]   HTTP     260     POST /update HTTP/1.1  (application/x-www-form-urlencoded)
   72 31.353431  [redacted]  [redacted]   HTTP      60     HTTP/1.1 200 OK  (text/html)
   92 46.633777  [redacted]  [redacted]   HTTP     260     POST /update HTTP/1.1  (application/x-www-form-urlencoded)
   96 46.825414  [redacted]  [redacted]   HTTP     469     HTTP/1.1 200 OK  (text/html)
  118 62.133455  [redacted]  [redacted]   HTTP     260     POST /update HTTP/1.1  (application/x-www-form-urlencoded)
  122 62.372553  [redacted]  [redacted]   HTTP     469     HTTP/1.1 200 OK  (text/html)
  140 77.658720  [redacted]  [redacted]   HTTP     260     POST /update HTTP/1.1  (application/x-www-form-urlencoded)
```

```
▸ Frame 40: 260 bytes on wire (2080 bits), 260 bytes captured (2080 bits)
▸ Ethernet II, Src: EcoPlugs_04:eb:3a (38:2b:78:04:eb:3a), Dst: VMware_49:40:c6 (00:0c:29:49:40:c6)
▸ Internet Protocol Version 4, Src: 192.168.0.76, Dst: 54.88.253.164
▸ Transmission Control Protocol, Src Port: 63923, Dst Port: 80, Seq: 24, Ack: 1, Len: 206
▸ [2 Reassembled TCP Segments (229 bytes): #36(23), #40(206)]
▸ Hypertext Transfer Protocol
▸ HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0000  [redacted]  ··)I@·8+ x··:··E·
0010              ········ ·7···L6X
0020              ·····P·· ······P·
0030              ·`····Ho st: api.
0040              thingspe ak.com··
0050              User-Age nt: tsli
0060              b-arduin o/1.5.0
0070              (ESP8266 )··X-THI
0080              NGSPEAKA PIKEY: B
0090              [redacted]V7 3[redacted]·
00a0              ·Content -Type: a
00b0              pplicati on/x-www
00c0              -form-ur lencoded
00d0              ··Conten t-Length
00e0              : 28···· field1=[redacted]
00f0              .00000&h eaders=f
0100              alse
```

Fig. 5. Analysis of data through the Wireshark tool.

After analysing the data using the Wireshark tool, it can be found that the IoT device transmits the data in clear. An attacker who manages to intercept the connection between the IoT device and the ThingSpeak cloud platform can extract Write API Key as well as the transmitted data.

4. CONCLUSIONS

With the advent of the cloud and the speed of data transmission over the Internet, the number of security vulnerabilities has also increased. Many users are reluctant to transmit their data in cloud because this data could be intercepted, decrypted and disclosed.

With the increase in the number of IoT devices connected to the Internet, so has the number of security attacks. Security attacks are based on the vulnerabilities of each layer of IoT art. For the detection of security attacks, most researchers propose solutions based on Machine Learning.

This article analysed the security of data transmitted by IoT devices in the ThingSpeak platform cloud when an attacker implements an active sniffing attack. From the results obtained, it can be found that IoT devices transmit the data in clear. An attacker who manages to intercept the communication, can extract Write API Key that allows him to enter fake data into the user's cloud account but can still see the transmitted data, so data privacy is affected.

REFERENCES

[1] Madhusanka, L.A.B., Pardeep, K., Mika, Y., IoT security: advances in authentication, Ed. John Wiley & Sons Ltd., 2020.
[2] Nettikadan, D., Raj, M.S.S., Smart community monitoring system using Thingspeak IoT Plaform, International Journal of Applied Engineering Research, vol. 13, no. 17, 2018, p. 13402-13408.
[3] Mirza, A.R., Muhammad, A.Q., Sajid, H.G., Saleem, U., Security issues in the Internet of Things (IoT): A comprehensive study, International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, 2017, p. 383-388.
[4] Andrioaia, D.A., Culea, G., Puiu, P.G., Environmental temperature and humidity monitoring system using Raspberry pi 4 and ThingSpeack, Journal of Engineering Studies and Research, vol. 27, no. 3, 2021, p. 20-23.
[5] Popescu, C., Culea, G., Intelligent low-power smart home architecture, Journal of Engineering Studies and Research, no. 3, vol. 24, 2018, p. 33-37.

[6] Anzola, J., Jiménez, A., Tarazona, G., Self-sustainable power-collecting node in IoT, Internet of Things, vol. 7, no. 1, 2019, p. 1-12.
[7] Kalia, P., Ansari, M.A., IOT based air quality and particulate matter concentration monitoring system, Materials Today: Proceedings, vol. 32, no. 1, 2020, p. 468-475.
[8] https://thingspeak.com/ (20.12.2021).
[9] Singh, G.D., Learn Kali Linux 2019, Ed. Packt Publishing, India, Mumbai, 2019.
[10] Yuri, D., Erdal, O., Cybersecurity - attack and defense strategies, Ed. Packt Publishing Limited, 2018.
[11] Morey, H., Brad, H., Asset Attack vectors: building effective vulnerability management strategies to protect organizations, Ed. APress, 2018.
[12] Akashdeep, B., Varun, S., Security incidents and response against cyber attacks, Ed. Springer, 2021.