Journal of Emerging Computer Technologies
Research Article
Received: *2020-12-09* | ***Reviewing:*** *2020-12-11* & *2021-01-18*| ***Accepted:*** *2021-01-26* | ***Online:*** *2021-02-20* | ***Issue Date:*** *2021-06-30*

Secure Connection between Google Home and IoT Device

Ekrem YİĞİT
Dokuz Eylul University
Department of Computer Engineering
İzmir, TURKEY
ekrem.yigit@ceng.deu.edu.tr

***Abstract*— This article presents a more secure connection between the NodemCU and Blynk, using the AES algorithm. it is aimed to prevent a vulnerability in the connection of Google Home devices with IoT during the Blynk IoT connection phase.**

Although the Blynk application offers a personal key, the network information linked in the memory of the physical device is vulnerable. The data is placed in the software by encrypting beforehand, and the connection is provided by decrypt during the connection. This study contributes to the prevention of security weaknesses caused by keeping software data on NodemCU as Plain Text in physical memory

Keywords—AES, IFTTT, IoT, Connection, Secure, Memory, EEPROM Introduction, Home Mini

I. INTRODUCTION

Google Home is a device developed by Google that can be customized both with its own functions and with many devices connected via Wi-Fi. It offers an interface that is managed by voice commands and can be customized.

Approximately 6 weeks after the release of Google Home devices, the logs kept on the devices were checked and it was determined that the device recorded the sounds as a log hacker can use these data to penetration attempts or fishing attacks. Researchers have found that smart speakers can be hacked with the help of laser-powered "light commands." Researchers suggest smart speaker makers can fix this vulnerability by adding a light shield around the microphone or using two different microphones on opposite sides to listen to voice commands.

The project is to operate the IoT device with safe commands sent from google home. In the project, the main target is to connect to the cloud from the google home device via IFTTT, then to get the light effect by taking data from the cloud using the NodemCU IoT device and Blynk.

NodemCU is a circuit board with high quality ESP8266 Wi-Fi module that can be programmed from Arduino IDE application and can communicate easily. It is aimed to provide cloud interaction by communicating with this device over the internet by making web transactions thanks to HTTP libraries. IFTTT (if this then that), If this happens, do it. It is an abbreviation of one of the simplest code phrases. This assign device to be triggered and the that assign action that works on device that is triggered. Webhooks service is a IFTTT service that connect to Blynk and IFTTT on Cloud Service. Webhooks is used to send requests to the URL we enter. Blynk server information and the TOKEN information used are entered as URLs and connection is provided and control is provided via IFTTT. In this URL, the pins on the device are entered and the controls of various pins are provided. Finally, my project is to identify vulnerabilities in communication on Blynk and IFTTT connections and to use these two components effectively in the safest possible way.

II. RELATED WORKS

The interaction of end-users with online IoT devices has been increasing for the last 10 years and with the increasing interactions, the usage of these IoT devices has started to be observed beyond the intended use. IoT devices need lightweight and new security mechanisms like random number generators [1-3], authentication protocols [4,5] and privacy protected connection methods. IFTTT enables users to use their home assistant devices heterogeneously on multiple platforms with IoT via the internet connection tool. With the widespread use of this environment, users are satisfied with the increase in interaction and they started to load more work on their systems.

In order to meet the increasing demand for products, studies on the field of security in a competitive environment have been quite incomplete. According to the researches carried out today, more than 50% of the 19323-connection established over home assistant devices did not find any security factor.

While the picture taken from the phone is in a private structure, the smart home device translates this picture information into a Public form. In the scenario described, the hacker sees the system vulnerabilities related to IFTTT, which enables the connection of the smart home device to the phone, and the Home Assistant will also make private content public and make confidential data accessible [6].

Security problems related to 45 smart home appliances and IoT devices connecting with them are discussed. It is determined that the most common vulnerability is users. Users endanger their own security by using Home Assistants with different levels of security for the same or similar jobs or IoT devices attached to them. In this research [7], which presents this vulnerability as the simplest and most effective solution, the use of multiple IoT and Home Assistant was shaped and the relational relationships were explained to the users.

It is not very difficult to steal users' IFTTT accounts with various online attack methods. Attackers who will change the authorizations made through this IFTTT account on another device for their own malicious purposes can cause damage as much as cyber-attacks with increasing device interactions [6].

This framework [8], developed to prevent a bad interaction via IFTTT, inserts the MAC address of the device to which the user connects to the IoT device to a PUF at the beginning,

and returns the output it receives as OTP, allowing access only from the devices authorized by the user at the beginning.

The most important prioritization on the market is always the cost of IoT devices and the platforms actually used. In costing-priority product planning, security is placed in the background. Extra cost or does not require any hardware. The answer that best meets these needs is the AES algorithm, which is also described in another research [9]. Offering both fast and secure service at once, AES also does not cause negative effects on IoT device performance [10].

Due to the lack of encryption in the transmission of data from IFTTT to IoT device of systems that are tried to be created with IFTTT account security and device connection methods seen in various studies, there are also vulnerabilities in leaking many data by logging them, so AES encrypt as an effective and cost effective method. With the method, both the data coming from IFTTT and Google Home Assistant is encrypted, and then the data is decoded without coming to the IoT device and secure transmission of the data [9].

Çepik et. al presented a study in 2020 about security vulnerabilities on the connection between Google Home and IoT device. They tested if this communication is vulnerable to an NTP attack [11].

III. PROPOSED WORK

The 2 basic devices of the project are the Google Home Mini and NumedCU IoT device. The microphone section on the device must be active. Make AES decryption on NumedCU, AES library has been added to Arduino IDE. The necessary encryption functions can be realized with this library. Password and SSID are necessity to connect NumedCU via Blynk. SSID and password If the information is added directly into the post to provide a link, a security flaw occurs here. While connecting, this two information in the software pose security risks. The attacker can discover certain data on NodemCU by reverse engineering methods via EPPROM.

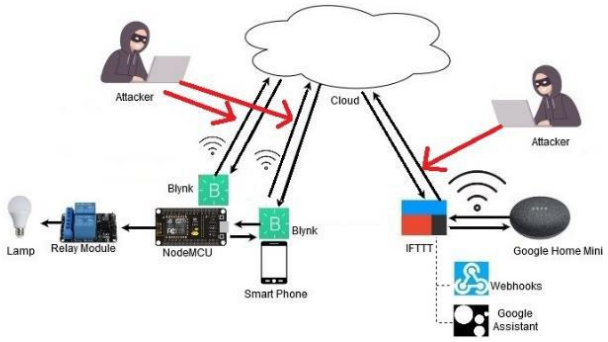

Figure 1. Representation of Possible System Vulnerabilities

All data entered while communicating with Blynk in NodemCU is kept in EEPROM. It is seen in the research that it is possible to access the data in EEPROM physically via a USB [12]. The attacker, who accesses the data via USB, can easily access the internet information on which the device is used, since no hardware measures are taken.

In another study to prevent EEPROM access in terms of hardware, by adding extra parts, the hardware vulnerability of the attackers was prevented but the software vulnerabilities could not be blocked [13].

The attackers' access to the information of the internet connection is a danger to all devices on that connection. To eliminate these risks, SSID and password will be added by encrypting with 128bit AES key in this study and this encrypted data will be provided by decryption while the connection is provided. 128Bit 16ASCII characters will be used for the key.

Reverse engineering of Arduino memory has been handled in the study in which it is possible to access information in the software [14]. The key size of the AES algorithm has a direct effect on performance in various algorithm encounters. When high security is targeted, performance/security threshold has been seen in the examinations; AES is more successful in this rate [15]. After a secure connection is established, the command to turn on the bulb coming from the cloud will be realized.

IV. TEST RESULTS

The main goal of the project is to add the user-known internet information to the program in a previously encrypted form and to provide an encrypted internet connection. Communication with four devices and a common internet connection has been tested.

The commands set via IFTTT to the Google home device were given as HTTP request, and the connection with the IoT device was tested and the lamp was successfully controlled. Button on / off communication to Blynk port 0 was transmitted in HTTP request format.

```
EkremEv
Encrypted: 2nqyFb+a9uGmJw52SAZtSg==
Decrypted: EkremEv
EkremEv
Encrypted: feRuuTz/lmkPbVaUh0i3Fg==
Decrypted: EkremEv
EkremEv
Encrypted: I6VVDN72z+Erlbtv2jvAyA==
Decrypted: EkremEv
EkremEv
Encrypted: A0NCgvzNjquSq9YR+NddSA==
Decrypted: EkremEv
EkremEv
Encrypted: C+AEieiqT2bgLmuZc6ECvg==
Decrypted: EkremEv
EkremEv
Encrypted: k8x53C+MKWj5Fk2PQpVUQA==
Decrypted: EkremEv
EkremEv
Encrypted: Nku4H7Q6t4aSgNfw79ODkA==
Decrypted: EkremEv
EkremEv
Encrypted: 6HZEKJk4D/zL3uUUfTiBeg==
Decrypted: EkremEv
EkremEv
Encrypted: 7YtI/cP7RrHtxr3SZv26Dw==
Decrypted: EkremEv
EkremEv
Encrypted: 2oPq27mZI6tX1NS+NBMakQ==
```

Figure 2 Arduino IDE Serial Port Output

On the security side of the application, Blynk internet connection has been tested to properly encrypt and decrypted data. As seen in the figure below, the software used on the IoT device processes the data properly. When performing the tests,

the IV has been re-created while performing each encryption in 16 bytes.

The connection made with the SSID and password of the user, which was previously encrypted, was successfully implemented. These devices, which generally communicate with the cloud, have become a necessity in order to provide sufficient trust. As mentioned in many studies like [16], NodemCU does not have sufficient security, so it is coded into additional security algorithms.

V. CONCLUSION

As a result, data in the NodemCU memory is not available in a meaningful way. All of important data are kept in encrypted form in memory and communication is provided in encrypted form. Even if the attacker has accessed to NodemCU via USB or software, the attacker will see data encrypted with AES, which he cannot make sense of. This prevents the device from being physically hijacked or the attacker from exploiting vulnerabilities.

REFERENCES

[1] Cabuk, U. C., Aydın, Ö., & Dalkılıç, G. (2017). A random number generator for lightweight authentication protocols: xorshiftR+. Turkish Journal of Electrical Engineering & Computer Sciences, 25(6), 4818-4828.

[2] Aydın, Ö., & Dalkılıç, G. (2018, July). A hybrid random number generator for lightweight cryptosystems: xorshiftLplus. The 3rd International Conference on Engineering Technology and Applied Sciences (ICETAS).

[3] Aydın, Ö., & Kösemen, C. (2020). XorshiftUL+: A novel hybrid random number generator for internet of things and wireless sensor network applications. Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, 26(5), 953-958.

[4] Lee JY, Lin WC, Huang YH. A lightweight authentication protocol for internet of things. In: 2014 InternationalSymposium on Next-Generation Electronics (ISNE); New York, USA; 2014. pp. 1-2.

[5] Aydın, Ö., Dalkılıç, G., & Kösemen, C. (2020). A novel grouping proof authentication protocol for lightweight devices: GPAPXR+. Turkish Journal of Electrical Engineering & Computer Sciences, 28(5), 3036-3051.

[6] Milijana Surbatovich, Jassim Aljuraidan,Lujo Bauer,Some Recipes Can Do More Than Spoil Your Appetite: Analyzing the Security and Privacy Risks of IFTTT Recipes" WWW '17: Proceedings of the 26th International Conference on World Wide WebApril 2017

[7] OmarAlrawi,Chaz Lever,ManosAntonakakis,FabianMonrose,Security Evaluation of Home-Based IoT Deployments, 2019 IEEE Symposium on Security and Privacy, 19-23 May 2019

[8] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[9] Bennet Praba1,Shivam Kumar,Ankur Saxena, Sourabh Patel "Securing Assistant Based Home Automation using AES Algorithm" Department of Computer Science and Engineering SRM Institute of Science and Technology, Chennai, India,2019

[10] Ross Mcpherson James Irvine, "Using Smartphones to Enable Low-Cost Secure Consumer IoT Devices," Department of Electronic and Electrical Engineering, Royal College Building, Glasgow G1 1XW, U.K..

[11] Çepik, H., Aydın, Ö., Dalkılıç, G. (2020) Security Vulnerability Assessment of Google Home Connection with an Internet of Things Device. In:7th International Management Information Systems Conference, İzmir, Turkey (9-11 December 2020.

[12] Kingpin, "Attacks on and Countermeasures for USB Hardware Token Devices," Proceedings of the Fifth Nordic Workshop on Secure IT Systems, 2000

[13] Grand, Joe. "Practical secure hardware design for embedded systems." Proceedings of the 2004 Embedded Systems Conference, San Francisco, California. 2004.

[14] Torroja, Yago, et al. "A serial port based debugging tool to improve learning with arduino." 2015 Conference on Design of Circuits and Integrated Systems (DCIS). IEEE, 2015.

[15] Kumar, M. Anand, and S. Karthikeyan. "Investigating the efficiency of Blowfish and Rejindael (AES) algorithms." International Journal of Computer Network and Information Security 4.2 (2012): 22.

[16] Utpala, Kuchi NSSSS, N. Suresh Kumar, K. Praneetha, D. Hema Sruthi, and K. Sai Avinash Varma. "Authenticated IoT Based Online Smart Parking System with Cloud." Pramana Research Journal 9, no. 4 (2019).