An IoT Based Hardware Filter for Internal Network Security

S.A.D. Oshada Viduranga Chandrakumara.
CCV Solutions
Kalutara, Sri Lanka
oshada@ccvsolutions.com

Anuradha Jayakody
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
anuradha.j@sliit.lk

Abstract— **Establishing internal network security of IoT takes a significant importance in modern world. There were several incidents reported in relation to the attacks to the systems making critical damages and incurred significant cost to them. These attacks may cause destruction on to the lives of the people too. The most of attacks have been done remotely through injecting malware in to IoT devices or programmable logic controllers. Among these many devices are wifi enabled and firmware updatable. As a result the devices become more vulnerable.**

The Esp8266 is Wifi enabled microcontroller that is commonly used for low power wifi applications. It is one chip everything included and current market has many ESP8266 based devices. The automobiles, programmable logic controller (PLC) in bulding management, medical equipment, supervisory control and data acquisition (SCADA) are areas included in IoT security at critical level.

This research is focussed to find a solution for thsese issues in IoT security. The suggested solution is implemented through microcontroller. Research results revealed that the solution is very successful in accuracy and performance. There is an opportunity for future researchers to develop secure transmission and filtering mechanisam for any IoT device compatible.

Keywords- Wi-Fi; IoT; Code Injection; Bitcoin; Encryption; Device vulnerability; Filter;ESP8266; Remote Access.

VI. INTRODUCTION

The Internet of Things (IoT) is interconnected systems which is used for automate the processes in real world. It is used for many industries such as automobiles, building management, power stations and etc. The IoT devices consist of several microchips and it has limited computing power. These devices have many advantages because of tiny and low power consumption. The most of devices are connected through Wi-Fi to cloud or central server. The inputs and outputs of devices depend on cloud data or device programmed instructions. Most of them are used for security purpose and automate various critical business requirements. These Wi-Fi based devices are vulnerable because Wi-Fi technology has vulnerabilities. In the current market has lot of security breaches coming in to live with IoT.

The luxurious hotel in Austria called "Romantik Seehotel Jäegerwirt" got breached in 28 of January 2017. The electronic key system in the hotel got breached first. The attackers gained control over the general computer system and shutting down all the hotel computers. They demanded to pay $1,600 through Bitcoin [1]. The hotel management had no other option other than paying ransom because the door locks system did not have emergency open system and the system completely got locked down.

The independent security researcher found vulnerabilities syringe infusion pumps in 2017. He found that the pump can control remotely without proper authentication. He listed down exploits which is work with Medfusion 4000 unit [1]. This attack is very serious because the attacker can release lethal amount of dosage with remote access for example insulin dosage.

The "Charlie Miller" and "Chris Valasek" has demonstrated their car hacking exploit in 2015. They found many car models are vulnerable in current market [3]. In 2016 Mitsubishi Outlander Wi-Fi console vulnerabilities are discovered by security expert. The exploit has been allowed to access the vehicle remotely and turn off security alarm

VII. LITERATURE REVIEW

In 2017 Meera Mathew and Divya R S published a paper in IEEE "Super Secure Door Lock System for Critical Zones" [1].The research paper published in IEEE discuss about how to secure the electronic door lock [1]. They used the 2 way authentication method for securing the system [1].

In that research Radio-frequency identification (RFID) and One Time Password (OTP) were used to secure the system. They used PIC16F877A Microcontroller with ZigBee to implement the system [1]. The ZigBee transmit the data to the server to generate the OTP [1].

The symmetric block cipher algorithms are used in system. According to system diagram they connected Zigbee directly with PIC16F877A Microcontroller [1]. It means PIC16F877A microcontroller communicates with Zigbee through serial transmission.

The cryptographic process runs on the PIC16F877A microcontroller and the Zigbee connected with PIC16F877A microcontroller connected through serial Rx and Tx. The Zigbee is mostly used for sensor networks and it can connect with other nodes too.

The Zigbee can update its firmware wirelessly. It may help hackers to hack the Zigbee. The Zigbee was connected with microcontroller and microcontrollers can update the firmware wirelessly.The hackers can hack Zigbee due to it is open network and by using it they can inject the malware code to microcontroller to change the system's main functions. Infected node will spread the malware into other devices as well.

In 2017 "Chin-Tan Lee, Yi-Chin Chung, Tung-Chun Shen and Ko-Wei Weng" published a paper on the "Development of Electronic Locks Using Gesture Password of Smartphone Base on RSA Algorithm" in IEEE [2]. They used RSA algorithm for securing the transmission with server to microcontroller [2]. The Bluetooth module attached with Arduino Yun module to communicate with the microcontroller. The Bluetooth module allowed the mobile phone to connect with the device [2]. The relay module which connected with the Arduino Yun drives the motor to open and close the door lock [2]. They used 3 x 3 smart phone pattern unlock system to input the password, which they encrypted using RSA and transmitted it through Bluetooth to the Arduino Yun [2]. Arduino Yun transmitted the data to server for authentication. The server sends the message to Arduino Yun and it will open or close the door according to the data sent by the server [2]. Then Arduino Yun transmits the status report to the server and it will be stored in MySQL database. The Arduino Yun based on ATmega32u4 and Atheros AR9331 with 64MB DDR2 RAM and 16MB flash memory [2]. The RSA algorithm needs high computing power to encrypt and decrypt the data. These microcontrollers are impossible of handling a full RSA system which is currently used in day to day operations. They used random key for encryption and they may have used a tiny version of RSA to do it. It may help to secure the password. Bluetooth is vulnerable in most cases and many exploits ware available in an internet. The Bluetooth module is connected using the serial interface with Arduino Yun and that communication channel is not encrypted between Arduino Yun microprocessor and Bluetooth device. The Bluetooth interface can be used to inject the malware in to the system by using exploits. The Arduino Yun is a Wi-Fi enabled device which can be hacked using Wi-Fi hacking tools such as "Aircrack". The injection of malware code or change in code can be done through Wi-Fi. The Arduino Yun have a built in Ethernet port in it and users can connect to the router using Ethernet port, however someone can hack it through the router using Wi-Fi hack. The Arduino Yun microcontroller controls the encryption and decryption in client side by handling the microcontroller. This module is directly connected with Bluetooth and Wi-Fi interfaces. The microcontroller controls the door lock motor, status update and RSA algorithm. The hackers can inject the code by using those interfaces to change the code inside microcontroller and by doing that they can get full control of the door lock. The system is no longer useful if they change the code inside microcontroller. In this research they have not covered the attack that can be done through the serial interface of microcontroller. The faults of this system can be used for many other attacks for example the infected device can be used to infect any other Bluetooth or Wi-Fi enabled device such as smartphones. The hackers can use that information to do crimes or ask ransom from users. They can open and close high security zones such as military, banks, nuclear power plant and etc. It may be helpful to the thief to steal something which are of good value from those places and they can alter the status logs by using MySQL database connection, then IT system auditors cannot identify what was happened in there because of no log entry for it.

The 2017 Kumar Keshamoni and Sabbani Hemanth published the paper in IEEE under "Smart Gas Level Monitoring, Booking & Gas Leakage Detector over IoT" [3]. They discussed how to implement gas control using IoT [3]. They used MQ-2(gas sensor), LM35(temperaturesensor) and siren [3]. The system used Atmel at89 microprocessor and Esp8266 Wi-Fi module [3]. This microprocessor contains 8K flash and 2Kof EEPROM. The ESP8266 module contains 1MB of flash memory [3]. The gas leak system will trigger the siren and send an alert through Wi-Fi [3]. They used SPI/SDIO or I2C/UART interfaces for communication between microprocessor and ESP8266 [3]. In this system the microprocessor and the esp8266 is connected via serial interface and there is no encryption system as well. The hackers can easily enter the system through Wi-Fi. The Esp8266 had an Over-the-air programming capability that they can use to inject the malware code in to esp8266 module or microcontroller. The esp8266 have 1MB of flash which is more than enough space to inject a malware. The malware can be used to control a device or monitor the systems. The hackers can use this system by triggering the siren for evacuating the

people or make them rush and it may help criminals to do a crime. Hackers can do attacks by submitting false information to the system. They can submit false data and it may inform the controller. If the controller gets wrong action in the system it may lead to a catastrophic damage to the community. For example, if the system shows low pressure, he can increase pressure according to system data but if the pressure increase, the gas pipes may explode. In this research the security of device is not a concern. According to these three researches they have not addressed the security problem between Wi-Fi connection and system's main functions. This problem is still not touched in research and the last incident was the one that happened in Seehotel-jaegerwirt hotel due to this vulnerability.

In the 2016 ShariqSuhail, ViswanathaReddy, Rambabu, Dharma Savarni C. V. and V. K. Mittal published the paper on Multi-Functional Secured Smart Home in Conference on Advances in Computing, Communications and Informatics (ICACCI) Jaipur, India. They discussed how to implement multifunctional home security with IoT .they used 4 sensors to get inputs for the system.

The system was onsite and remotely accessible. They introduced the wireless door locks and automatic door open systems but they not introduce data validation system with hashing to know the data is correct or not.

The raspberry and Arduino are directly connected and it is not having any filtering system for incoming or outgoing traffic. They used Bluetooth and Wi-Fi devices and it is communicate through the raspberry pi Bluetooth system. Hacking through Wi-Fi attacker can get control of raspberry pi and he can control the Pi. The attacker can install software in to raspberry and reprogram or inject the code to Arduino. With help of that attack the attacker can get full control of it.

In 2017 Hakar Mohsin Saber and Nawzad Kamaran Al-Salihi published the paper on IoT: Secured and Automated House. They used 5 input sensors and 2 active outputs for control certain tasks.

The all of the sensors and outputs wired to AT Mega 2560 microcontroller. They connected with internet using W5100 microcontroller and send data to could through API. As alternative connection and SMS service they connected SIM900 Module.

They secured the data but could not gurantee the data is correct and accurate because they have not used any encryption systems or hashing for validate it.

In the system the users can control their applications remotely via Android app. The android app sends commands to device and the device can't verify because it had not encryption system implemented.

VIII. Problem Identification

In this research we discovered 2 major vulnerabilities.

A. Vulnerability One

In this vulnerability Wi-Fi and Main processor directly connected and which command coming through ESP8266 will be executed in main chip.

There is no any filter mechanism or encryption in data transfer process in this model but this model is widely used in current market.

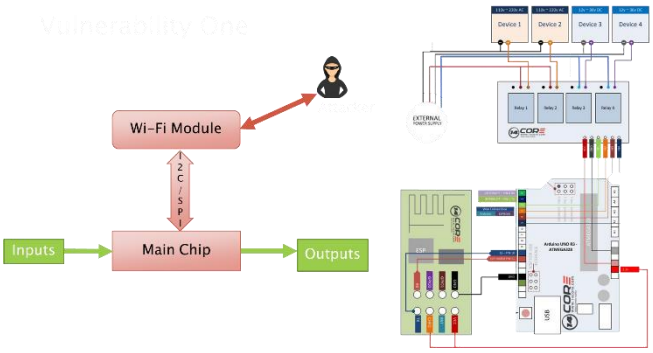

Fig.19: Vulnerability One

B. Vulnerability Two

In this vulnerability Wi-Fi and Main process inside of ESP8266.

There is no any filtering mechanism or encryption in data and all process done by one chip. This model is widely used in tiny low power application in current market

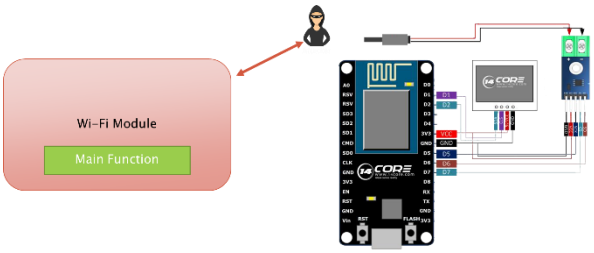

Fig. 20: Vulnerability Two

IX. Objectives of Research

- Develop a secure communication mechanism between devices.
- Isolate the main functionality from Wi-Fi.
- Develop the method to filter the incoming traffic, authenticate each data set.
- Prevent the system from code injection attack to secure the main functionality of the microprocessors.

X. Implementation

This research focuses on how to implement secure communication between devices in system. The ESP8266F will be used as the Wi-Fi connector device and Atmel At mega chips will be used for main process in this system the serial connection will not be connected directly to main process. It will be filtered out hardware or software-based filter before interacting with the main processor. The filter will drop all the data that not belongs to system. This filter will work as firewall in between the At Mega microprocessor and ESP8266.

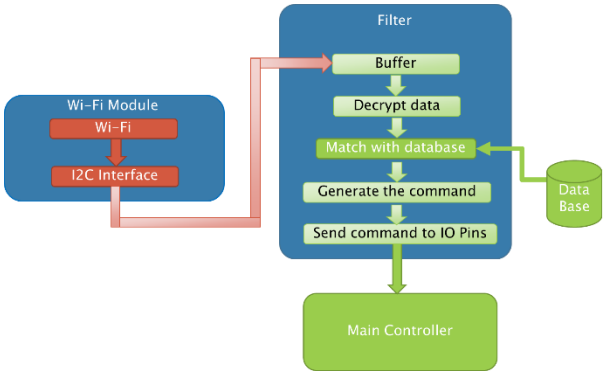

Fig. 21: System Diagram

This method will protect the main function from code injection attacks. The same data will go through 2 different process to verify and decrypt the data. The data will decrypt and verify in block by block. If the any of chips detected suspicious data received, it will stop transmission to next step.

The filter will receive the decrypted data. This filter will have fixed size buffer to load the data. System will load until it is completely filled character by character. If any suspicious character is found, it will drop the character immediately. This filter has a pattern matching, the pre-8 define words are only allowed to load in to buffer. After the buffer filled it will send the signal to the main processor and flush the buffer. The signals also predefine values in the filter. If the ESP8266 get infected my malware, the filters will identify it and isolate the system reset to default.

XI. Results

We used two Arduino Mega boards as filter and main controller. The Wi-Fi handle through NODE MCU which is consist of ESP8266F Module. In the testing environment we test our model and we got expected results out from it. We match the data with data base stored vales in SD card using string buffer in Arduino code. If it is not match with it drop the command.

```
if(inputstr.length()>5){
for (int i = 0; i < 3; i++){
 if(inputstr==comdb[i]){
  //send command to device   }
 else{    inputstr="";          }
            delay(500);
 }}
```

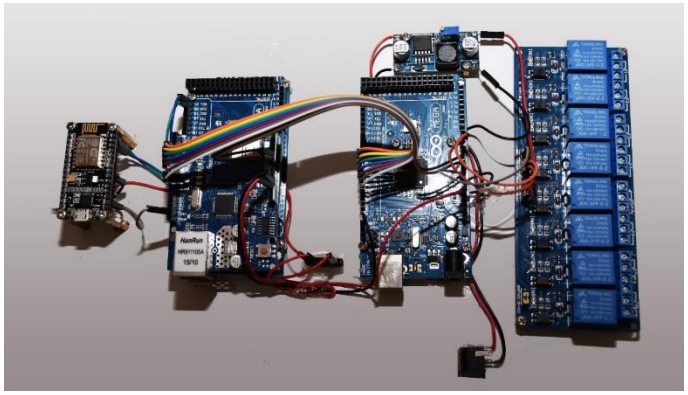

Fig. 22: Filter Hardware Implantation

To send the command to device we used binary number. We used 7 wire system to represent the binary. We got relevant decimal number for the command and convert it to binary using following code

```
void divide(int num){
   if(num>1){
     divide(num/2);
     }
   bin += num%2;}
```

After calculated binary value that value will represent through 7 wires system for isolate from the direct connection.

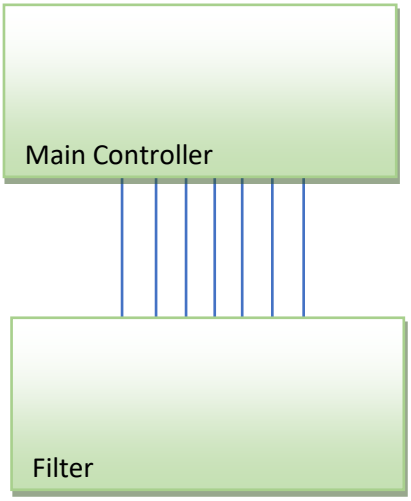

Fig.23: 7 wires system

In the system the binary number will identify through main controller and execute the process. According to given instructions. In this method the main processor is not connected to directly to filter and there is no way to inject the code in to it. the main controller function cannot be altered remotely. We manage to protect main controller functions from side channel attacks.

XII. Evaluation

Accuracy of device has been tested in the test environment. There is no other system was found for compare accuracy and security with hardware-based and most of systems are develop as software-based solutions. In the previous works and incidents proves that the current systems still vulnerable. The zero-day vulnerability may be available in black market and most of them are software based according to previous attacks happened in few months back. The test results show that filtering function is working perfectly.

The research based on hardware implementation and it is totally different approach compare to previous security implementation in IoT devices. According to that there is no any previous work as a benchmark for this solution to evaluate and develop the solution, has been evaluated based on theories and test results. As a solution for this problem 7 wire transmission system was introduced.

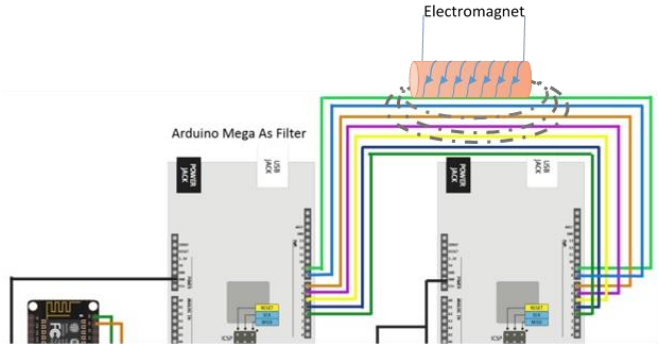

Fig. 24: Magnetic interference

Table I Magnetic interference test result

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
Normal	1	0	0	1	0	1	1
After magnetic interference	1	1	1	1	1	1	1

According to the result of injecting data or receiving data between filter and main controller is impossible. If the injection is happened it will affect all the bits and it will change to one. When try to receive it or tap it, attacker cannot identify which bit is on and which bit is off by analyzing magnetic wave power.

The following table shows the 2 different data transmissions with same magnetic power. To demonstrate it is assumed each wire had value 10 with Hall Effect sensor

Table II:Table 5.4.1 2 Different data transmission with same magnetic power

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	Total
No1	1	0	0	1	0	1	1	
Magnetic power values	10	0	0	10	0	10	10	40
No2	0	1	1	0	1	0	1	
Magnetic power values	0	10	10	0	10	0	10	40

According to this example attacker cannot receive exact data or transmit the value through this system. Compare 7 wire transmission with 2 wire transmission (RS 485, Serial and etc.), the 7 wire is more secure than 2 wire transmission.

XIII. CONCLUSION & FUTURE WORK

In this research found out method for stop the code injections and protect the main functions in main microcontroller, the filter act as firewall to drop unwanted commands. The 7 wire system makes physically isolated main controller and it is prevent attackers to getting reach to main functions.in the future 7 wire system can be develop for data transferring between devices. It will be valuable for critical applications like PLC.

REFERENCES

[1] K. Keshamoni and S. Hemanth, "Smart Gas Level Monitoring, Booking & Gas Leakage Detector over IoT," in *2017 IEEE 7th International Advance Computing Conference*, 2017.

[2] B. Barth, "scmagazine," 15 September 2017. [Online]. Available: https://www.scmagazine.com/medfusion-4000-wireless-syringe-infusion-pump-can-be-exploited-to-compromise-operations/article/689007/. [Accessed 30 May 2018].

[3] H. M. Saber and N. K. Al-Salihi, "IoT: Secured and automated house," in *2017 International Carnahan Conference on Security Technology*, Madrid, 2017.

[4] M. ShariqSuhail, V. iswanathaReddy, Rambabu , C. V. DharmaSavarni and V. K. Mittal, "Multi-Functional Secured Smart Home," in *Advances in Computing, Communications and Informatics (ICACCI)*, Jaipur, 2016.

[5] C.-T. Lee, Y.-C. Chung, . T.-C. Shen and K.-W. Weng, "Development of Electronic Locks Using Gesture Password of Smartphone Base on," in *2017 IEEE International Conference on Applied System Innovation*, Sapporo, 2017.

[6] M. Mathew and R. S. Divya , "Super Secure Door Lock System For Critical Zones," in *International Conference on Networks & Advances in Computational Technologies*, Trivandrum, 2017.

[7] M. BURGESS, "wired," 02 February 2017. [Online]. Available: http://www.wired.co.uk/article/austria-hotel-ransomware-true-doors-lock-hackers. [Accessed 30 May 2018].