Scientific Research Publishing

Smart Grid and Renewable Energy, 2022, 13, 235-247
https://www.scirp.org/journal/sgre
ISSN Online: 2151-4844
ISSN Print: 2151-481X

False Alarm Attack and Protection of Smoke Detector

Ryan Nakata, Depeng Li

Department of Information and Computer Sciences, University of Hawaii at Manoa, Honolulu, USA
Email: ryan,depengli@hawaii.edu

How to cite this paper: Nakata, R. and Li, D.P. (2022) False Alarm Attack and Protection of Smoke Detector. *Smart Grid and Renewable Energy*, **13**, 235-247.
https://doi.org/10.4236/sgre.2022.1310015

Received: August 26, 2022
Accepted: October 28, 2022
Published: October 31, 2022

Abstract

Carbon monoxide can cause serious illness or even death if the functionality of smoke alarms fails in the residential home and, in fact, more than 350 persons die every year due to the leak of carbon monoxide. However, vulnerabilities and threats to smoke/CO alarms have not been well-studied. In this paper, through interconnect, a power replay attack has been studied in order to trigger a false alarm. The experimental results demonstrate the smoke alarm can be manipulated. This paper also concentrates on providing a sequence of security methods to defend the smoke alarm system. In future, how to protect smart detectors against attacks will be studied as this can force them to leave high-quality mode of operations.

Keywords

False Alarm, Hardwired Interconnected Smoke Alarms

1. Introduction

Carbon monoxide (CO), an odorless, colorless, and tasteless gas, is the cause of death for over 350 people every year [1]. The most popular way to detect carbon monoxide relies on alarms in residential home. These alarms have to operate all the time since if they fail its owner will die.

In the United States, many states mandate the use of smoke detectors in residential home [2]. In most states, it is also required that new homes/renovated homes must be fitted with hardwired smoke detectors that allow for indefinite operation. For example, according to the 1994 Uniform Building Code Section 310.9.1 adopted by Hawaii, residents are required to install smoke detectors in all new and renovated dwelling units.

Without functional smoke/CO detectors, people can die since CO poisoning is

very dangerous, especially during the winter. However, attackers or adversaries (*terms are interchangeable in this paper*) may manipulate smoke detectors if their vulnerabilities are exploited. Adversaries can even falsify alarms which might be very irritating. Due to the severe consequence resulted from the malfunctioning hardwired smoke detectors, it becomes necessary to invest more into their security and usage.

However, few researches focus on this threat. To the best of our knowledge, there are only a couple of studies *i.e.* [3] and [4] working in this area: in [3], a smart smoke detector has been designed by using opto isolator to read the 9 volt relay signal which can be sent out as the text notification in Apps. In [4], silencing hardware backdoor method has been developed. However, neither of them explores the potential power replay attack against the smoke detector and therefore no corresponding countermeasure has been developed.

In this paper, how the power replay attack against existing hardwired smoke detectors is investigated. Furthermore, to countermeasure the specific vulnerability, we also analyze a variety of security means regarding how to protect the hardwired smoke detectors. In detail, the following contributions have been made:

1) It is developed that a harvesting attack via interconnect by replaying a 9 Volt signal which triggers the false alarm in the smoke alarm system.

2) Our attack is composed of the Raspberry Pi, bread boarded circuit and the battery. The script programs have been developed to load the blue tooth communication and to activate the replay of the 9 Volt interconnect signal.

3) To protect the smoke alarm system, a number of security methods have been proposed ranging from tamper resistance to redesigning the smoke alarm system.

2. Background

2.1. Mechanism of the Smoke Alarm

As illuminated in **Figure 1** [5], wired smoke/CO alarms communicate with each other through an input called the interconnect. During a normal smoke detector's operation, all detectors constantly check the interconnect wire for a 9 volt signal. Once a 9 volt signal is read on the interconnect input, the alarm is triggered. In order for the interconnect system to function properly when one detector senses smoke/CO it then needs to alert all of the detectors on the same circuit. To accomplish the detectors are all wired in parallel on their interconnect line. Thus, when one alarm goes off, it sends a 9 volt power replay signal down the interconnect line, on BRK/Firex/Gentex/Kidde/Lifesaver alarms, triggering the rest of the alarms around the house.

2.2. Vulnerabilities, Attack and Security Assumption

In this subsection, we first study the smoke alarm system's vulnerability and then exploit an attack from the perspective of an adversary under our security assumption.

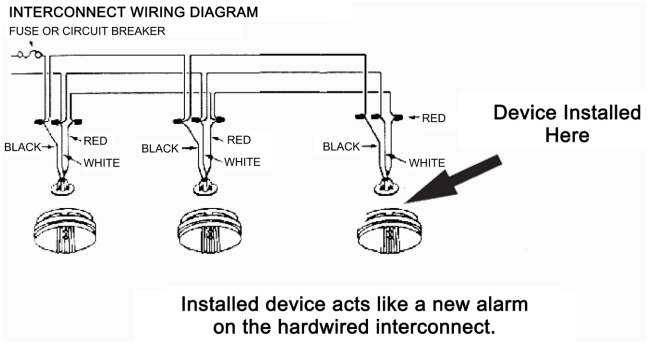

Figure 1. Smoke Detector Wiring Diagram, modified from Cheung [5]. This figure shows how the interconnect works and where we put our device. (*Black*: *hot wire*, *White*: *neutral*, *Red*: *the interconnect wire*).

1) *Vulnerabilities Analysis*

To be simplified, we examine the means to replay the signal and furthermore, to verify, under current circumstance, whether it is feasible to launch such kind of attack.

Generally, adversaries may trigger false alarms in order to distract victims and to coerce them to action. It could also happen in the hardwired smoke detector system. For example, adversaries may be able to replay the interconnect signal from one detector and it will essentially set off all the detectors because these alarms are connected to each other.

Furthermore, when launching the false alarm attack on-site, adversaries need the space to hide their attacking devices/tools. A power supply is required to power their device/tools since a battery cannot provide power in an extended period of time. To verify its feasibility, we have testified this method on-site. While analyzing how smoke detectors are wired in houses [3], we realize that wired smoke detectors are powered by the same 110 V AC (black and white cables on the smoke detector, referred to **Figure 1**) that we can get them out of a regular wall outlet. Therefore, it is possible for us to power our attacking device by using the power supply of the smoke detector. This makes our attack much easier because, 1) we do not need add an extra power supply such as battery, 2) we do not need worry about the battery consumption problem of our attack devices/tools, and 3) it significantly reduces the amount of physical space in order to accommodate our devices/tools.

2) *Rough Attack Idea*

Our idea is to replay the 9 volt interconnect signal in different kinds of smoke detector systems. Currently, the existing smoke detector communication system can be classified into two categories: the hardwired interconnect and the wireless smart home system (e.g. the Nest Wireless Smoke Detector). We target the former by using a micro-controller (e.g. Raspberry Pi and Arduino) to attack the hardwired interconnect detector. Note that the hardwired interconnect devices usually rely on availability/reliability rather than security. Regarding the latter, wireless radios such as Zigbee are used to trigger the alarm. But the scope of this

paper only focuses on the former (Figure 2, Figure 3) and the attack against the latter will be our future work.

The parallel circuit architecture deployed by the hardwired interconnect of the smoke detector system cannot isolate the falsified interconnect signal. It means that if one alarm is compromised, the entire system is broken. Taking advantage of this weakness, we install a hardware backdoor between the smoke/CO alarm and interconnect wire. Consequently, we falsely activate all alarms connected to the same interconnect line of the smoke detector system in a residential home.

In detail, to accomplish this, we equip our attack by adding a USB power brick in parallel. This supplies sufficient power to our Raspberry Pi. Since our device has an indefinite power source, the likelihood of failure due to power loss is significantly reduced as compared to other solutions in which the battery power is mandatory.

3) *Security Assumption*

We assume the victim's alarm system is not tamper-resistant. This allows the adversary to install their own attack devices/tools inside the alarm system without leaving visible or audible signs of tampering.

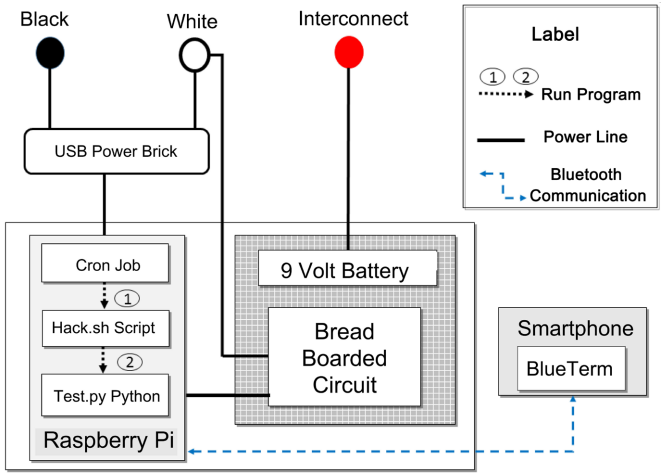

Figure 2. Power replay attack architecture.

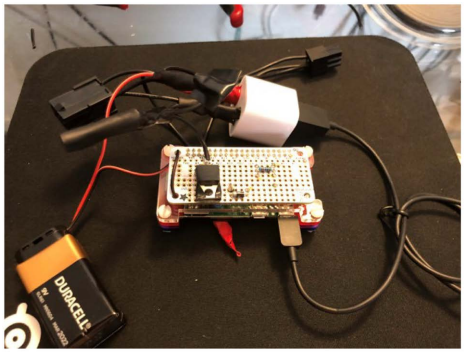

Figure 3. All Components Together. The 9 volt battery is used to send the 9 volt interconnect signal which is controlled by a N-channel Mosfet.

3. Implementation of Power Replay Attack

In this section, we first outline our power replay attack. Then, we demonstrate how the attack is implemented. After that we discuss the architecture of our attack system following with details about each component. At last, we illuminate the results with a set of figures (**Figures 4-9**) ranging from code snippets to hardware prototype.

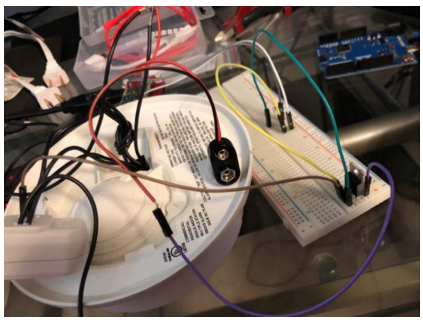

Figure 4. How To Connect Different Parts Together and Breadboard Test. Testing that the proof of concept works, itemizing the parts, and making a permanent prototype. The included parts are 1) Bread Board, 2) N-Channel Power MOSFET –30 V/60 V, 3) 1N4001-Diode, and 4) Resistor-10K. This test's purpose to protect the system against attacks. This list is slightly modified from bildr.org blog [6].

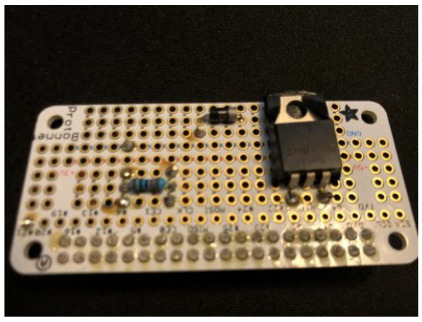

Figure 5. Bread Boarded Circuit Connects Mosfet to Pin21 of RaspberryPi. When the Raspberry Pi triggers *Hi* on the Pin, the mosfet lets the 9 volt battery flow onto the interconnect circuit of the smoke detectors.

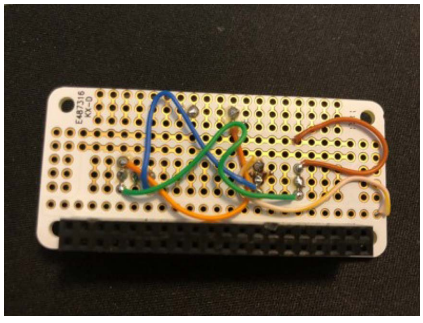

Figure 6. How to connect different parts (Back of Bread Boarded Circuit).

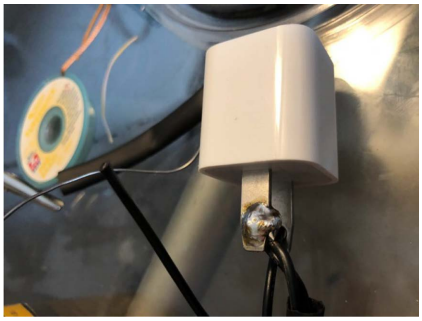

Figure 7. iPhone USB charger connected to white and black neutral wires. The charger is used as a power source for the raspberry pi zero w.

Figure 8. Device and all of its components are in compaction. The electrical tape is used as a case to consolidate all the components which makes the device take up less space minimizing the amount of space the device takes up.

Figure 9. Device Installed in Ceiling. Once the smoke detector is installed in ceiling, there is no way to find the hardware in plant since they are hidden inside the ceiling.

3.1. Outline of Power Replay Attack

Our goal is to launch the power replay attack against the Gentex smoke/CO detector. As depicted in **Figure 2**, our attack system is composed of 4 components, 1) the 9 volt battery, 2) the bread boarded circuit, 3) the Raspberry Pi Zero W and 4) the smart phone. The 9 volt battery is used to send the power replay signal through the interconnect. Regarding the connection, both black hot and

white neutral are soldered to the USB Phone charger (refer to **Figure 1** and **Figure 7**) which powers the Raspberry Pi. The white neutral connects the bread boarded circuit (refer to **Figure 5** and **Figure 6**). The Raspberry Pi GPIO Pin 21 controls the Mosfet on the bread boarded circuit.

3.2. Brief Description of the Execution of Power Replay Attack

In our power replay attack, the first step is to setup the Raspberry Pi Zero W with the scripts and set the Cron Job to run the scripts on startup (allowing the device to be plug and play). After we setup our device with the needed programs we are ready to execute our attack. First we plug Raspberry Pi in and wait for it to turn on and run our scripts. After that, we connect it with BlueTerm (android bluetooth console app). The next step is to enter value "1" in the console. Its purpose is to replay 9 Volt signal over the interconnect. In contrast, if we input "0", the power replaying of the 9 volt signal over the interconnect is stopped (refer to test.py subsection III (F)).

3.3. Considerations

Why we select Raspberry Pi: To implement my Interconnect Replay Attack, we decided to use a *Raspberry Pi Zero W*. That is because it is one of the smallest readily available microcontrollers on the market while Wi-Fi and Bluetooth are both included.

Why we choose to use a 9 *volt battery*: The signal that needs to be replayed is a continuous 9 volt signal on the detector's red interconnect input (refer to **Figure 1**). Most smoke detectors use a 9 volt battery as a backup power supply (in the case of a power outage). By using a 9 volt battery we are able to power replay with the same voltage, that would occur under normal operation, while using a similar source to the original smoke detector's power. To achieve this, we have designed a circuit that will supply 9 volts DC to the interconnect wire using a 9 volt battery [6].

Bluetooth Communication: In this implementation, we select a wireless communication channel and choose Bluetooth 4.0 due to its range and compatibility with almost any phone. Moreover, we use a Bluetooth 4.0 console application called "BlueTerm" on the android device to connect to the onboard Raspberry Pi to send commands. Bluetooth 4.0 has a range of 200 feet. One scenario that takes advantage of the range of Bluetooth 4.0 would be an adversary sitting outside of a victim's house from a car to send commands remotely. In our testing, we are able to activate the alarms in a 2nd floor apartment from the ground floor.

Accommodation of our Devices: In order to make our device small enough to fit inside the space above a smoke detector, we decided to go with a prototype bread board shield for the Raspberry Pi Zero W allowing our device to be more permanent and easier to fit behind smoke detectors. To prevent damage and shorting to our device, we decided to wrap all of its components with electrical

tape. Using electrical tape instead of an enclosure also helps to minimize its size footprint.

3.4. Proof of Concept

The smoke alarm that our attack target is the Gentex line of smoke detectors. We realize that a 6 pin PCIE Power Cable can be modified by filing the key holes so that they would fit Gentex's connectors. With the use of adapters that connect to our modified PCIE connectors on our device should be able to work on other manufacturers' alarms with easy plug and play ability as well.

We have successfully proved a proof of concept that Gentex smoke detectors are vulnerable to Interconnect Replay Attacks. While implementing this attack, we found a way to indefinitely power our device while keeping it easy to install/uninstall.

Once the device is installed, it is visually impossible to distinguish whether or not a hardware backdoor has been installed unless they are removed. The device will also not impact the normal operation of the smoke detector under routine test conditions. For us, it is important not to interfere with the normal device operation in such a way that the attacking device can secretly manipulate the system for longer periods of time.

3.5. Detailed Steps of Execution

Figure 3 depicts the picture of how the physical components connect with each other in our prototype. Regarding the software, on the Raspberry Pi, the Python program *i.e.* test.py (refer to subsection III (F)), the script *i.e.* Hack.sh (refer to Figure 10) and Cron Job (refer to Figure 11) will be set-up before the attack.

At the beginning of the attack, the Raspberry Pi Zero W will establish the bluetooth communication [7] with the Android App BlueTerm on the smart phone. After that, the BlueTerm app will send messages (e.g. 1—*start* or 0—*stop*) to the Raspberry Pi via the bluetooth communication channel. Then, the Raspberry Pi Zero W sends the 9 Volt replay signal to the interconnect which triggers the false alarm on the hardwired smoke detector.

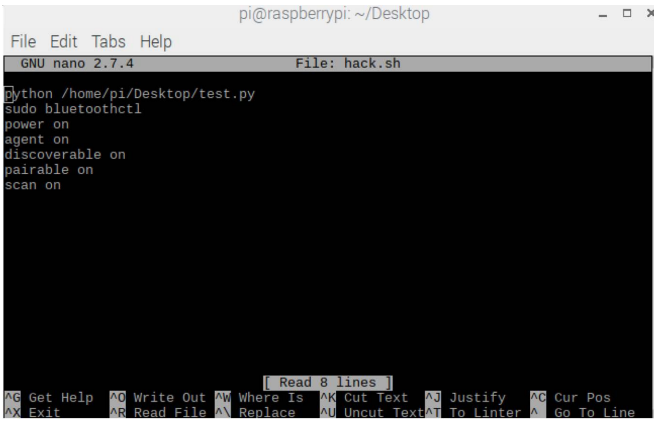

Figure 10. Console Command/Shell Script of Hack.sh.

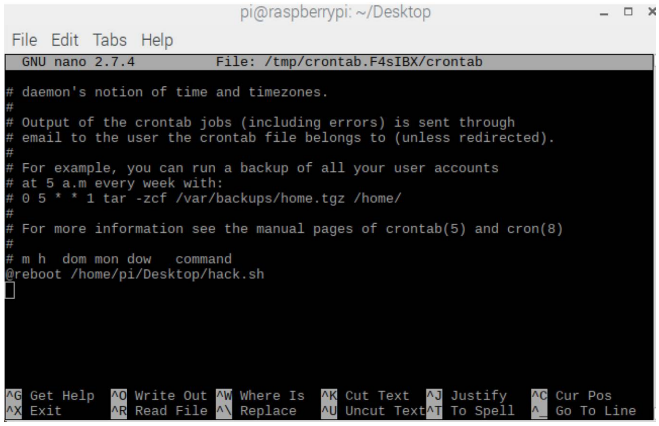

Figure 11. Cron Job that Runs Hack.sh on reboot.

In terms of the sequence to activate our attacking system, here is the flow: 1) when the Pin 21 is set to *High*, the 9 volt signal is sent to onto the interconnect, 2) all the smoke detector on the interconnect can detect the 9 volt power replay since they are wired in parallel (refer to **Figure 1**), 3) the false alarm is triggered and sounded.

3.6. Python Program and Script Codes

Source Code of Test.py is shown below:

```
import bluetooth
import RPi.GPIO as GPIO
#calling for header file which
#helps in using GPIOs of PI
LED=21
GPIO.setmode(GPIO.BCM)
programming the GPIO by BCM pin numbers.
(like PIN40 as GPIO21)
GPIO.setwarnings(False)
GPIO.setup(LED,GPIO.OUT)
#initialize GPIO21 (LED) as an output Pin
GPIO.output(LED,0)
server.socket=bluetooth.BluetoothSocket(bluetooth.RFCOMM)
port = 1
server.socket.bind(("",port))
server.socket.listen(1)
client.socket,address = server.socket.accept()
print "accepted connection from" address
while (True):
data = client.socket.recv(1024)
print "Received:
if (data == "0"):
if 0 is sent from the Android App,
```

```
turn OFF the LED
print ("GPIO 21 LOW, LED OFF")
GPIO.output(LED,0)
if (data == "1"):
if '1' is sent from the Android App,
turn OFF the LED
print ("GPIO 21 HIGH, LED ON")
GPIO.output(LED,1)
if (data == "q"):
print ("Quit")
break
client.socket.close()
server.socket.close()
```

4. Security Analysis and Countermeasures

In this section, we propose countermeasures to enhance the security level of smoke detector system from the perspective of 1) optimized smoke detector system and 2) tamper proof.

4.1. Optimized Smoke Detector System

1) Use pseudo random number system: It will be more secure if we switch the interconnect system from a high/low (9 volt) interconnect system to a pseudo random number system. In this new random number system, the detector is equipped with two extra buttons, a listen button and a broadcast button. When a user first installs their wire interconnect smoke detectors, the user will set all of the other detectors in listen mode and then pick one to broadcast. When the user hits the broadcast button it will then send a randomly generated number as a seed to all the other detectors. This will then allow all of the devices to sync their seed. Every time an alarm is set off, it will send the new random number generated through the interconnect for the other devices to check with their own random number they generated. Since all the devices should have the same starting seed in theory, they would all generate the same sequence of random numbers. This solution would make it more secure so that it is hard for an attacker to guess the starting seed and what number would be generated next in the sequence.

2) Design a new circuit: the new circuit can detect the removal of the alarm from its mounting bracket. In the existing smoke alarm system, once these alarms are initially installed, there is no reason for anyone to remove it. Replacing the battery on most alarms does not require the removal of the alarm from its bracket. Therefore, in our solution, if the alarm is removed from its mounting plate, the alarm should trigger/set a status light (showing that the alarm has been removed since its original installation) and/or a notification is pushed to its owner warning them that their smoke alarm has been removed from its mount.

4.2. Tamper Proof

One of the ways manufacturers can prevent replay attacks on their devices is by making them more tamper proof. We listed 3 suggestions below:

1) Deploy rail system: An electrical current will be run through the mounting bracket and back to the smoke detector. When the smoke detector is uninstalled it will then break the connection between the bracket allowing the alarm to detect that it has been removed. When the connection between them is broken, the alarm should go off and or warn the owner that their device is being tampered with. As a nondestructive method, it makes the device more tamper proof.

2) Permanently connect interconnect: manufacturers should make the interconnect connector permanently linked together once installed. This method prevents attacks in a sense that adversaries have to damage the alarm in order to install a hardware backdoor.

3) Tamper proof stickers: manufacturers can add tamper proof stickers allowing users to install them if they want to. This allows the user to be aware of whether their life saving alarm has been tampered with or not. (This tamper proof method is often used at gas stations to prevent the installation of card skimmers).

5. Related Works

To the best our knowledge, there are no specific power replay attacks similar to our attack. In this section, we briefly introduce some related research.

5.1. Attacks on Smoke Detectors

[3] is the most related research of ours in which the researchers make their smoke detectors smart by using an opto isolator to detect whether or not 9 volts flows through the interconnect cable. Using this, he generated text notifications that were sent to the owner whenever an alarm detected smoke. This research clearly explains how smoke detectors were wired in residential homes.

5.2. Other Power Replay Attacks

In [8] and [9], the power replay attacks on electronic door locks have been launched. The idea is to replay the power required to activate the actuator that engages the unlocking mechanism.

In [4], the means to silence hardware backdoor have been studied. They appropriately categorize these hardware attacks which give us a better understanding of attack vectors on hardware devices.

In the panel [10] at Defcon 25 2017, researchers demonstrate how to sniff IR signals of motion detectors and therefore how to deactivate them remotely by replaying the deactivate IR signal.

6. Future Works

Our future work mainly focuses on enhancing our attack capability, making our

attack more reliable, and targeting more smoke/CO manufactures. First, in order to improve devices' availability, we intend to implement a watch dog circuit that can continuously reset the device after a certain amount of time. This can fix the device's errors by restarting it after a set period of time. Second, we would also like to add a method in which we can remotely wipe the data off the Raspberry Pi to prevent forensic analysis on the device in the case that it is found. Third, a better way to communicate with the Raspberry Pi would be optimal so that more functions can be added to the project. Fourth, we also would like to decrease the required space of our device so that it can be installed faster.

Last but not the least, we have also explored the possibility to reuse our attack against some other smoke detectors. Firex, for example, has designed a smart smoke/CO detector [11] which is installed on an interconnect smoke detector circuit with the purpose of making it smart through the use of Apple's Home Kit. It was compatible with the major manufacturers such as BRK/Kidde/Lifesaver. In order for the smart detector to communicate over the interconnect, adapters are deployed. Regarding their product, the compatible detectors use the same interconnect and are vulnerable to the same Power Replay Attack. Therefore our attack against Interconnect Replay Attacks on smoke detectors can apply to this product if we added adapters to our attack device/tool.

7. Conclusion

The power replay attack against the smoke/CO alarm system is a serious problem due to the fact that the well-functioning smoke/CO alarm system can save lives. However, in this paper, we have successfully implemented a proof of concept attack exploiting a vulnerability, *i.e.* the power replaying of a 9 volt interconnect signal through the hardwired interconnect of Gentex smoke detectors. We believe that, with the proliferation of micro controllers, manufactures can prevent such kind of attacks and any kind of other variants with the purpose to save lives.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] https://www.cdc.gov/mmwr/preview/mmwrhtml/mm6303a6.htm

[2] FEMA. The United States Fire Administration.

[3] https://gist.github.com/darconeous/

[4] https://ieeexplore.ieee.org/document/5958021/

[5] https://www.edcheung.com/automa/smoke_det.htm

[6] bildr.org. High-Power Control: Arduino + n-Channel Mosfet. http://bildr.org/2012/03/rfp30n06le-arduino/

[7] Controlling Raspberry pi gpio Using Android App over Bluetooth.

https://circuitdigest.com/microcontroller-projects/controllingraspberry-pi-gpio-using-android-app-over-bluetooth

[8] Oh, S., Yang, J.-S., Bianchi, A. and Kim, H. (2014) Poster: Power Replay Attack in Electronic Door Locks. *IEEE Symposium on Security and Privacy*, San Jose, 18-20 May 2014, 1-2.

[9] Oh, S., Yang, J.-S., Bianchi, A. and Kim, H. (2015) Devil in a Box: Installing Backdoors in Electronic Door Locks. 2015 13*th Annual Conference on Privacy*, *Security and Trust* (*PST*), Izmir, 21-23 July 2015, 139-144.

[10] https://www.youtube.com/watch?v=gFTiD7EnVjU

[11] https://www.firstalertstore.com/store/products/onelink-wifi-hardwired-smoke-and-carbon-monoxide-alarm-ac10-500.htm