IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 60-63
www.iosrjournals.org

Everything Can Be Hacked

Saquib Shakil Ahmed
Department ofComputer Science & Engineering,Nagpur Institute of Technology, Nagpur, India

ABSTRACT:*The devices in modern world are no longer safer to use in day to day life. As the technology is enhancing rapidly, this comes with a price i.e. risks of getting hacked and the vulnerabilities in those devices can be easily found. This paper will concentrate on demonstrating the attacks on real world devices which people in society generally don't know. These devices are automobiles and medical implanted devices. All of these devices possess networking capabilities therefore they are bound to have a buzz because devices in a network can be accessed by a hacker by applying network hacking techniques. This paper will show snapshots of live attacks on automobiles with software interfaces. The paper would try to show the sensitivities and consequences of the attacks on these devices like medical devices and automobiles. The attacks could be even life threatening to a person if someone gains illegal access to patient's implanted medical (like pacemaker) device or automobile of a person while he/she is driving.*

Keywords: *Automobiles, Hacks, Implanted medical devices, Networking capabilities, Vulnerabilities*

I. INTRODUCTION

People are living in highly vulnerable and dangerous society as far as network security is concerned. Now for normal human being perspective hacking is just about gaining illegal access or having control of some other computer in a network. But that is not only hacking because **e**verything around us can be hacked not just computers. So our first target in considering the real world attack on devices is automobiles. Real world cyber-attacks are not just only on computers but can be done on various devices which are controlled by software. Each device working with software and having networking capabilities are vulnerable and bound to get hacked. Some of them are as follows:

- Automobiles having wireless network (Bluetooth or WI FI), cellular network and radio stations
- Medical Implanted devices like Pacemaker, ICD defibrillator and NPR

The above mentioned attacks will be shown with the live snapshots and the steps taken to implement those attacks. The light will be spread upon the consequences of those attacks. In presentation the audience will come to know about the sensitivity of these attacks.

II. TARGETS

1. Automobiles

The paper presents several targets which can be hacked in real world scenario, here is the first one i.e. automobiles

1.1 Introduction

Automobiles are no longer just mechanical devices. Today's automobiles contain a number of different electronic components networked together that as a whole are responsible for monitoring and controlling the state of the vehicle. Each component, from the Anti-Lock Brake module to the Instrument Cluster to the Telematics module, can communicate with neighboring components. Modern automobiles contain upwards of 50 electronic control units (ECUs) networked together. The overall safety of the vehicle relies on near real time communication between these various ECUs. While communicating with each other, ECUs are responsible for predicting crashes, detecting skids, performing anti-lock braking, etc.When electronic networked components are added to any device, questions of therobustness and reliability of the code running on those devices can be raised. Whenphysical safety is in question, as in the case of the automobile, code reliability is even a more important and practical concern. The paper would try to show the live attack snapshots and the vulnerabilities in the ECU's.

1.2 Automotive Embedded system

The modern car is collection of various embedded electronic components as shown in figure1.Some of them is as follows:

1.2.1 Electronic Control units (ECU's)

Modern sedan contains over 100 MB binary code spread across 50 independent computers called ECU'swhich communicate with one another via digital internal buses called CAN BusCommunication is done by exchanging CAN packets. These packets are broadcast to all components on the bus

1.2.2 Controller Area network (CAN)

The typical modern car has digital buses to communicate among ECU's based on CAN standard.High speed and low speed CAN buses are there like High speed bus interconnect powertrain components.The CAN buses are bridged to support subtle interaction requirements.

1.2.3 Telematics

The ubiquitous computer control, distributed internal connectivity and telematics interface combine to provide application S/W platform with network access.

1.3 Security Challenges in CAN

The underlying CAN protocol has a number of inherent weaknesses that are common to any implementation. Key among these:

1.3.1 No authentication Fields or Identifier Fields

As shown in figure 2, CAN packets contain no authenticator fields or even any source identifier fields meaning that any component can indistinguishably send a packet to any other component. This means that any single compromised component can be used to control all of the other components on that bus, provided those components themselves do not implement defenses

1.3.2 Broadcast Nature

Since CAN packets are both physicallyand logically broadcast to all nodes, a maliciouscomponent on the network can easily snoop on all communicationsor send packets to any other node on thenetwork. CARSHARK leverages this property,allowing usto observe and reverse-engineer packets, as well as to injectnew packets to induce various actions.

1.4 Attack Methodology

1.4.1 Packet Sniffing and Target Probing

The S/W observe traffic on CAN buses to determine how ECU's communicate, This revealedwhich packets were sent as soon as the components were activated.Combination of replay and informed probing discover how to control the radio.

1.4.2 Fuzzing

Range of valid CAN packets is small so damage can be done by fuzzing the packets.This means iterative testing of random packets(Brute force).

1.5.Security Access

To perform sensitive actions ECU's need to be authenticated. The Multiple levels of Fuzzing access or brute forcing is possible

IDH: 07, IDL: 26, Len: 08, Data: 02 **27 01 00 00 00 00 00**
IDH: 07, IDL: 2E, Len: 08, Data: 05 67 01 **54 61 B6 00 00**
IDH: 07, IDL: 26, Len: 08, Data: 05 27 02 **D0 B6 F1 00 00**
IDH: 07, IDL: 2E, Len: 08, Data: 02 **67 02 00 00 00 00 00**

The first packet requests security access level 01. The seed is returned, "54 61 B6".After some calculation, the sender sends back the result of manipulating the seed, "D0 B6 F1". Since this is the correct value, the ECU responds with an error free response.

1.6.In-Car Setup

1.6.1 Communicating with CAN bus

For Communicating with CAN bus the ECOM cable is used .It is basically connected with laptop.

1.6.2 Connecting Laptop using ECOM and other cables

As shown in figure 3The laptop is running custom CARSHARK CAN network analyzer and attack tool. Thelaptop is connected to the car's OBD-II port.

1.6.3 CARSHARK Software Interface

As shown in figure 4 CARSHARK is being used to sniff the CAN bus. Values that have been recently updated are in yellow. The left panel lists all recognized nodes on high and low speedsubnets of the CAN bus and has some action buttons. The demo panel onthe right provides some proof-of-concept demos.

1.7.**Live Attack example via CAN packets**

On the MS CAN bus of ford, there is packet used by automobile to indicate if a door is ajar(slightly open) that uses 11-bit identifier 0x03B1.It seems packet is sent every two seconds. **When no door is ajar the packet looks like**

DH: 07, IDL: 26, Len: 08, Data**: 0**0 00 00 00 00 00 00 00

This packet was captured using Carshark application with ECOM cable and OBD-II-connector.**When door is ajar the packet looks like**

IDH: 07, IDL: 26, Len: 08, Data: **8**0 00 00 00 00 00 00 00

Single byte difference indicates the status of door to the instrument panel. when this packet is written to the CAN bus, the car will indicate the driver door Ajar even if it is not. The snapshot of this example is shown in figure 5.

III. IMPLANTED MEDICAL DEVICES

2.1 Introduction

The next target in the discussion is implanted medical device. The implanted medical devices are nothing but the devices which are implanted in patient's body to improve healthcare like pacemaker or ICD. In 1926 the first pacemaker was invented then in 1980 the first internal pacemaker was invented. So in medical field the technology has grown rapidly and in 2006 we hit an important milestone as far as network security is concerned because in 2006 the implanted medical devices started to have networking capabilities. So if the medical device possesses networking capabilities then the vulnerabilities can be found with ease and these devices can be hacked.

2.2 Wirelessly induced fatal heart rhythm

As shown in figure 6, the ICD is a defibrillator and this goes into the person to control their heart rhythm and these have saved many lives. In order to not have to open the person every time you want to reprogram the ICD or do some diagnostics on it, they made the ICD to communicate wirelessly. So the wireless capabilities of ICD gave rise to the vulnerabilities in ICD thus control it.

2.3 Attack Methodology

The attackers reverse engineered the wireless protocols and they build the device as shown in figure 7, with a little antenna that could talk the protocol to the device and thus control it. In order make their experience real they took some ground beef and bacon and they wrapped it all up about the size of human being's area where the device would go and they stuck the device inside it and performed many successful attacks.

2.4 Successful Experiments

- Triggered ICD identification
- Disclose patient data: name, diagnoses and other data
- Disclose cardiac data
- Change ICD's clock
- Change therapies including disable the deive
- Power denial of services: Run down the battery

IV. CONCLUSION

Automobiles have been designed with safety in mind. However, you cannot have safetywithout security. If an attacker (or even a corrupted ECU) can send CAN packets, thesemight affect the safety

of the vehicle. This paper has shown, for two differentautomobiles, some physical changes to the function of the automobile, including safetyimplications, that can occur when arbitrary CAN packets can be sent on the CAN bus.With this information, individual researchers and consumerscan propose ways to make ECU's safer in the presence of a hostile CAN network aswell as ways to detect and stop CAN bus attacks. This will lead to safer and resilientvehicles in the future.As far as medical devices are concerned the technology is often adopted without considering the security consequences so before implanting a device inside the person the threats should be taken care of. Hopefully this paper would awake the manufacturers and safer medical devices can be build to improve healthcare.

REFERENCES

[1]"Experimental Security Analysis of Modern Automobile", Karl Koscher, Shwetak Patel, Franzika Rosener, Brain Kantor, Stefan Savage,*IEEE Symposium on Security and Privacy*

[2] "Adventures in automobile network and control units", Dr. Charlie Miller & Chris valasek

[3] R. Charette. This car runs on code. Online: *http://www.spectrum.ieee.org/feb09/7649, Feb. 2009.*

[4]T. Hoppe, S. Kiltz, and J. Dittmann. Security threats toautomotive CAN networks –practical examples and selectedshort-term countermeasures in *SAFECOMP, 2008.*

[5]S. Mollman. From cars to TVs, apps are spreading to the realworld. Online: *http://www.cnn.com/2009/TECH/10/08/apps. realworld/, Oct. 2009.*

[6]M. Wolf, A. Weimerskirch, and T. Wollinger. State of theart: Embedding security in vehicles. *EURASIP Journal on Embedded Systems, 2007.*

[7] Y. Zhao. Telematics: safe and fun driving. Intelligent Systems,*IEEE, 17(1):10–14, Jan/Feb 2002.*