CRYPTOGRAPHY BASED CYBERSECURITY IMPLEMENTATION IN AUTOMOTIVES

Chandrika S[1], Dr.S.B.Rudraswamy[2]
[1,2]Department Of Electronics and Communications,
Sri Jayachamrajendra College Of Engineering Mysore
Email : chandrikas92@gmail.com[1],rudra.swamy@gmail.com[2]

Abstract

”Do we place our customers in danger?” is a question that gives the need for greater focus and commitment for OEMs on cybersecurity implementation and validation. This paper gives an insights into cyber security from an automotive perspective and shows the strong need for cyber security implementation in automotives by considering enemies within and outside of OEMs , vulnerability areas in automotives.It also gives an overview on cryptography based concepts like Public key, private key Infrastructure, Digital signature and Hashing which are used in cybersecurity implementation. It gives an clear insight on secure unlocking and secure programming in an ECU using cryptography based schemes and their validation.

Keywords: Original Equipment Manufacturers (OEM’s),Electronic Control Unit (ECU)

I. INTRODUCTION

There was a time when the car was called as a purely mechanical product. But with usage of computer based solution to control the ignition, which was the first function to be controlled electronically, started remarkable evolution in the way, where the cars evolved into software based product instead of mechanical. Now automotive electronics addresses demanding areas like, engine controls, body controls, sensors, access system, occupant comfort, safety, security and infotainment.

Automotive security was synonymous with theft prevention. But the exponential growth in use of softwares in automobiles to realize visions of the connected car and autonomous driving, security is now becoming synonymous with safety. Undoubtedly every vehicle manufacturer’s primary concern is safety. Recent experiments by researchers have demonstrated vehicles being remotely hacked into via their connected telematics unit and commanded to execute malicious code that allows the attacker to remotely control the vehicle by controlling critical functions like steering, brakes, and transmission etc. Thus, it has been proven beyond a shadow of doubt that security breaches in automobiles can have serious safety consequences. Therefore, vehicle manufacturers have to make security as much a priority as safety.

By advancing network in cars, the industry has enabled exciting new usages. Some preliminary versions are already in new models. These new usages are often referred to as cyber physical features, since almost all of them require collection of data from physical environment and cyber systems, making automotive operation decisions, and executing on such decisions with physical consequences. Some example usages include: Advanced driver assistant systems (ADAS),Advanced fleet management, Smart transportation and Autonomous driving [1].

Emerging usages drive the need for built-in security solutions and architectural design to mitigate emerging threats. The relationship between customers and their vehicles is very personal as most drivers see their cars as an extension of their private space much like their homes. Consequently unavailability of their vehicle caused by a large-scale security breach or a malfunction of safety components during driving would lead to a disruption of trust in the vehicle and its manufacturers. The ultimate goal of automotive manufacturers is to ensure that the new vehicle paradigm is protected and can operate to its full potential, even in a malicious operating environment.

II. ENEMIES WITHIN AND OUTSIDE OF OEMS

Most people have heard of hackers and malicious users. Many have even suffered the consequences of hackers criminal actions. So who are these people? The next few sections gives the lowdown on these attackers and the impacts of hacking on OEMs.

a) Defining Hacker: Traditionally, hackers like to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work In recent years, hacker has taken on a new meaning someone who maliciously breaks into systems for personal gain. Technically, these criminals are crackers (criminal hackers). Crackers break into, or crack, systems with malicious intent. The personal gain they seek could be fame, profit, and even revenge. They modify, delete, and steal critical information, often making other people miserable.

b) Defining malicious user: A malicious user meaning a rogue employee, contractor or other user who abuses his or her privileges is a common term in security circles and in headlines about information breaches. A long-standing statistic states that insiders carry out 80 percent of all security breaches

[2].

A. Understanding the enemy

Before we start assessing the security of systems, we have to know something about the people were up against. Many security product vendors and other professionals claim that computer systems should be protected from the bad guys both internal and external. But what does this mean? How do we know how these people think and work?

Knowing what hackers and malicious users want helps to understand how they work. Understanding how they work helps to look at information systems in a whole new way. Hackers can be classified by both their abilities and their underlying motivations.

Some are skilled, and their motivations are benign; theyre merely seeking more knowledge. At the other end of the spectrum, hackers with malicious intent seek some form of personal gain. Unfortunately, the negative aspects of hacking usually overshadow the positive aspects and promote the negative stereotypes.

Hackers see what others often overlook. They wonder what would happen if a cable was unplugged, a switch was flipped, or lines of code were changed in a program. Hackers who perform malicious acts dont really think about the fact that human beings are behind the firewalls, wireless networks, and web applications theyre attacking. They ignore that their actions often affect those human beings in negative ways, such as jeopardizing their job security and putting their personal safety at risk.

On the flip side, there are handfuls of employees, Contractors or consultants who intend to compromise sensitive information on your network for malicious purposes. These people dont hack in the way people normally suppose. Instead, they root around in files on server shares; delve into databases they know they shouldnt be in; and sometimes steal, modify, and delete sensitive information to which they have access. This behavior is often very hard to detect especially given the widespread belief by management that users can and should be trusted to do the right things.

As negative as breaking into computer systems often can be, hackers and malicious users play key roles in the advancement of technology. In a world without hackers and malicious users, the latest intrusion prevention technology, data leakage protection, or vulnerability scanning tools would not exist. Such a world may not be bad, but technology does keep security professionals employed and keep the field moving forward.

Unfortunately, the technical security solutions cant ward off all malicious attacks and unauthorized use because hackers and (sometimes) malicious users are usually a few steps ahead of the technology designed to protect against their wayward actions.

In whichever way we view the stereotypical hacker or malicious user, one thing is certain that Somebody will always try to take down computer systems and compromise information by poking and prodding where he or she shouldnt, through denial of service attacks or by creating and launching malware.

So appropriate steps has to be taken to protect systems against this kind of intrusion.

B. Why they do it?

Hacking is a casual hobby for some hackers they hack just to see what they can and cant break into, usually testing only their own systems. Defeating an entity or possessing knowledge that few other people have makes them feel better about themselves. Many of these hackers feed off the instant gratification of exploiting a computer system. They become obsessed with this feeling. Often, the more difficult the job is, the greater the thrill is for hackers.

The knowledge that malicious attackers gain and the selfesteem boost that comes from successful hacking might become an addiction and a way of life. Some attackers want to make your life miserable, and others simply want to be seen or heard.

Some common motives are revenge, basic bragging rights, curiosity, boredom, challenge, vandalism, theft for financial gain, sabotage, blackmail, extortion, corporate espionage, and just generally speaking out against the man.

Malicious users inside would look to gain information that helps them with personal financial problems, to give them a leg up over a competitor, to seek revenge on their employers, to satisfy their curiosity, or to relieve boredom.

C. Impacts of Hacking on OEMs

Companies suffer reduced valuation after public reporting of their car being hacked, usually in the form of a drop in sale. The trust of consumers in their vehicle, and subsequently their belief in the brand to develop safe vehicles would suffer. The ultimate risk for an OEM not pursuing a holistic cyber security strategy is a drastic reduction in sales. In addition, governmental fines or regulations for remediation of successfully conducted attacks on vehicles similar to violations of emission laws could sum up significantly, besides liability claims by affected customers.Apart from reputational damage ,other impacts on OEM's are listed below:

- The loss of intellectual property and business confidential information
- Opportunity costs, including service and employment disruptions, and reduced trust
- The additional cost of securing networks, insurance, and recovery from cyber attacks

III. EXPOSED ATTACK SURFACES

Attack surfaces refer to potentially vulnerable entry-points in the vehicle that can be tapped and exploited to gain unauthorized access.Figure 1 shows the attack surfaces in a vehicle.The increased use of software and the introduction of different wireless connectivity technologies have significantly expanded the attack surface of a vehicle and the attendant risk of exploitation. The objective is to find the weakest links between systems till the original target is successfully controlled. So the first task that hacker does is check for vulnerabilities in automotives.

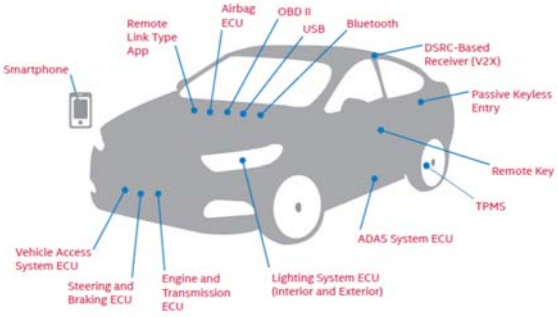

Fig. 1. Attack surfaces

An interesting analogy can be drawn in this regard. A Burglar trying to break into a house. The first thing that burglar would do is to check out what are the available ways to get into a house. Second thing that he would decide the easiest way to get break through the house and to make sure that he leaves no evidences for his track. This analogy is clearly tabulated in table 1.

The following are the primary sub categories of threats to vehicles:

- Man-in-the-Middle Attack: Interception of internal and/or external vehicle communication in order to obtain information from ECU to ECU communications or other critical software elements. This attack leads to get control over ADAS, Steering system, breaking, airbags etc. Vehicle bus communication and telematics control unit can be controlled.
- Side-Channel Attack: Utilizing weaknesses in hardware, software and communication

protocols in a connected system to an attack target in order to open an unprotected channel. Through side channel attacks, modification in the original functions can be achieved in the areas like Infotainment, telematics and comfort systems.

TABLE I
ANALOGY FOR HACKING

	Burglar (House)	Hacker(car)
Target	To find Valuables	Steal sensitive information, Reputational damage
Features	Secured lock Front door, back door,balcony, windows ,glass doors etc	ADAS,passive keyless entry,steering and breaking ECU,USB, Bluetooth Smartphone
Vulnerabilities	Frontdoor, back door, through balcony, break through windows,glass doors etc.	Feature with more software code, weakness in security implementation in a hardware and communication channel.
Ways of attacking	may break in through windows, break a door at its hinges, keys	Man in the middle attack, side channel attack,Dysfunctional Sensor Processing, Spoofing, Backdoor computing
Selection of a way to attack	Would select backdoor ,since it will take less effort by the burglar to break through.	Infotainment systems are often the ideal target since it involves huge code,there will be a way for hacking

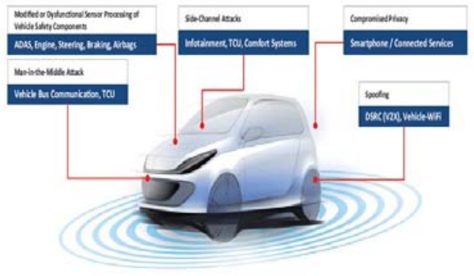
Modified or Dysfunctional Sensor Processing of Vehicle Safety Components
ADAS, Engine, Steering, Braking, Airbags
Side-Channel Attacks
Infotainment, TCU, Comfort Systems
Compromised Privacy
Smartphone / Connected Services
Man-in-the-Middle Attack
Vehicle Bus Communication, TCU
Spoofing
DSRC (V2X), Vehicle-WiFi

Fig. 2. ways of attacking a vehicle

- Dysfunctional Sensor Processing: Disturbing sensor input for further processing of vehicle maneuvers through modification of bus communication systems or unauthorized software modification directly onto ECUs. This attack leads to get control over ADAS, Steering system, breaking, airbags etc.
- Spoofing: Faking presence of communication partners and information that is used to control advanced sensor systems, activating maintenance functions within vehicles, thus creating new possibilities to modify vehicle systems configuration. This method would give access to Dedicated Short Range Communication (V2X), vehicle Wi-Fi.
- Compromised Privacy: Interception or readout of privacy related user data that are directly connected with personal details of drivers e.g. driving behavior, destination targets, billing details (within cloud services), etc [3].

IV. BASIC CONCEPTS IN CRYPTOGRAPHY

This section briefly explains the basic concepts in cryptography that it helps in understanding implementation of secure programming in an ECU.

a) Cryptographic algorithms: Cryptographic algorithms are used to verify authenticity and integrity and to ensure confidentiality. There are two types of cryptographic algorithms: symmetric and asymmetric. Asymmetric algorithms like RSA and ECC, which use a pair of unidirectional keys, offer more reliability than symmetric algorithms like AES which use a single, shared secret key.

However, asymmetric algorithms are computationally more intensive. For optimal resource usage, most schemes employ a combination of the two with an asymmetric algorithm for authentication and initial key exchange and a symmetric one for subsequent high volume operations.

b) *Private key/symmetric key:* Symmetric-key cryptography is a mechanism by which the same key is used for both encrypting and decrypting;it is more intuitive because of its similarity. This characteristic requires sophisticated mechanisms to securely distribute the secret-key to both parties.

c) *Public-key:* Public-key on the other hand, introduces another concept involving key pairs: one for encrypting, the other for decrypting. This concept is very clever and attractive, and provides a great deal of advantages over symmetric key. Transmitter of a message will have both private key and public key assigned to it. A message being transmitted can be encrypted using either private key or public key. When a message is encrypted using private key of the transmitter, then only public key of the transmitter can decrypt the message for its use while if message is encrypted using public key, then only its private key can decrypt the message.

d) *Public-key Infrastructure or PKI:* Public key cryptography (PKI) is a cryptographic technique based on asymmetric algorithms and digital certificates. It is an effective mechanism for verifying the authenticity and integrity of the system software. This is achieved using digitally signed software images which are verified by a secure boot mechanism on the ECU.

e) *Digital signature:* Digital signature is a mechanism by which a message is authenticated i.e. proving that a message is effectively coming from a given sender. Here the data to be sent is encrypted using the private key of the transmitter. Along with the encrypted message public key of the sender is also transmitted so that on reception, receiver can decrypt the message.

f) *Hashing:* For Digital signature, another technique used is called Hashing. Hashing produces a message digest which is a small and unique representation of the complete message. Hashing algorithms are a one-way encryption, i.e. it is impossible to derive the message from the digest.

g) *Certificate Authority:* A certificate is a piece of information that proves the identity of a public keys owner.Like a passport,a certificate provides recognized proof of a person’s (or entity)identity. Certificates are signed and delivered securely by a trusted third party entity called a Certificate Authority (CA). With a certificate instead of a public-key, a recipient can now verify a few things about the issuer to make sure that the certificate is valid and belongs to the person claiming its ownership [4].

V. METHOD FOR IMPLEMENTING SECURITY IN AN ECU USING CRYPTOGRAPHY SCHEME

The key tenets of automotive security are ensuring integrity, authenticity, availability, confidentiality and non-repudiation of the system.

- Integrity and authenticity of the hardware and software in the system, including firmware upgrades and downloaded applications.
- Authenticity, integrity and confidentiality of internal as well as external communications. Confidentiality of stored information.
- Availability of the critical components of the system at all times to ensure functional safety by preventing denialof-service attacks.
- Tamper-proof black-box collection of digital forensic data to aid in security breach investigations.

Security mechanisms to achieve most of the above goals fall broadly into two categories: cryptography-based schemes, and intrusion detection and prevention (IDPS) schemes.

Secure unlock and Secure programming are the two cyber secure features that can be implemented in an ECU using cryptography based schemes. Secure unlock is necessary to restrict the access to the critical data while secure programming is to make sure that original software code is not modified unless it has secured access to modify the original code.

A. Secure Unlocking of an ECU

A feature of locking and unlocking mechanism is implemented in an ECU to have restricted access to the data and for reprogramming of an ECU. While flashing an ECU with new software code, the ECU must be unlocked. Using cryptography the secured access to the data and secure programming of an ECU is achieved.

1) Security counter: Few of the Controller operations in an ECU are only allowed for authorized parties. OEMs will define supported unlocking protocols which they want to implement in an ECU. These unlocking protocols are used to permit the use of sensitive operations by the controller. Controllers in an ECU have a counter and a flag which are used to bypass the security feature supported by an ECU during its development.

Controller level functions are implemented such that the Security counter is written to a particular value that indicates the locked or unlocked state of an ECU. Controller with unlocking protocols implemented will have password and cryptography key table assigned to it. This password is used by Dynamic Link Library file linked to controller and used to decrypt the cryptography key table assigned.

2) Security Access: Advanced diagnostics requires a login diagnostic service to be performed to gain access to all of the functions of the ECUs. In commonly used standards, this diagnostic service is called Security Access which uses a seed/key algorithm for granting access. If the ECU is unlocked, all of its functionality will be available. The general procedure is carried out in the following sequence:

- The advanced diagnostic application requests a seed from the ECU.
- The ECU sends a seed back to the advanced diagnostic application.
- The seed is run through an algorithm in the advanced diagnostic application and the answer, the key, is sent to the ECU.
- If the received key corresponds to the expected key the ECU will unlock and grant access.

The design of the seed/key algorithm in the advanced diagnostic application is proprietary to the OEMs. There are two types of seed: static and dynamic. Static means that the same seed is returned irrespective of when or how many times it is requested and dynamic is stated to be updated at every single request. The latter can be dependent of e.g. the current time or a random parameter. There also exists a combination of the different types of seeds which is static over some time interval or a number of requests.

Since challenge (Seed) and response (key) lengths, as well as the algorithm to compute the key, are not specified in the standard, every vehicle manufacturer can implement an arbitrary seed length and algorithm. It is also not standardized if the seed is static or alternating.

B. Secure Programming of an ECU

For secure programming, diagnostic service security access is used. This service supports different sub functions. Sub functions available will be used for secure programming, access secured diagnostic services, and to check whether the normal operations are working well. These sub functions are also used to provide a privileged diagnostic service access to controllers exclusively for OEM manufacturing facilities. Using security access service and its sub functions, the below listed parameters can be read and controlled.

- Parameters to read stored information
- Parameters to control normal output functions
- Parameters to read dynamic values of ECU sensor inputs and outputs
- Parameters to read data packets which contains diagnostic information

When an ECU is programmable and required to read secured data, secured services then specific sub functions of security access must be supported. Parameters which are used to control normal output functions are sometimes secured so that no other than manufacturers can access these parameters to control these functions. Depending upon the ECU which are programmable and used to control output functions are supposed to be implemented with specific sub functions of security access.

For secure programming and to control secured output functions, cryptographic algorithm and seed key table based algorithm are used. When seed key table based algorithm is used to control secured output functions, seed key pair will be given by OEMs. While for secure programming, when cryptographic algorithm is used, Dynamic Link Library file generated by OEM is used.

Secure programming is achieved by using digital signatures to validate authorized software code programmed into an ECU.A digest of the software image encrypted using the OEMs private key is stored on the ECU. At start-up, the secure boot code of the ECU decrypts the stored digest using the OEMs public key, computes the digest of the stored software image, and loads the image only if the two digests match. Once loaded, the software image can then verify the authenticity and integrity of other components like the file system, downloadable applications,and software upgrade packages thus establishing a chain of trust rooted in the secure boot code.The flow how secure programming is done is shown in fig 3.

The software image is loaded if both the digests match which can then verify the authenticity and integrity of other components like the file system, downloadable applications, and software upgrade packages thus establishing a chain of trust rooted in the secure boot code.

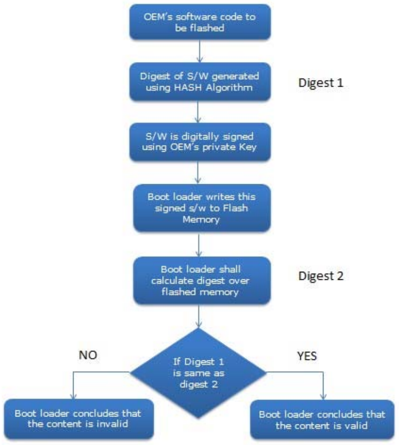
OEM's software code to be flashed
Digest of S/W generated using HASH Algorithm
Digest 1
S/W is digitally signed using OEM's private Key
Boot loader writes this signed s/w to Flash Memory
Boot loader shall calculate digest over flashed memory
Digest 2
NO
If Digest 1 is same as digest 2
YES
Boot loader concludes that the content is invalid
Boot loader concludes that the content is valid

Fig. 3. Secure programming

Although Secure Unlock and Secure programming features are implemented for safety and security purpose, there is a possibility that an Engineer who know in and out of the implementation, could hack the vehicle. In order to avoid such situations, OEMs will change the cryptography keys given for the implementation. This ensures that key values are changed for unlocking an ECU and it is kept confidential by manufacturing.

The quick wins to improve internal and external cyber security functions in vehicles are activities that implement secure best practices during the actual development phases. Furthermore it offers an opportunity to minimize the target area of each system, at least for most current attack scenarios. Testing and validation efforts need to be adapted or extended to include penetration and fuzz testing on all existing elements that are processing data of any kind coming from internal and external communication backbones in vehicles. The greatest weaknesses are usually created when interfaces between key components are not Specified correctly, lacking precise implementation.

Validation of secure unlock feature in an ECU strengthens security mechanism to prevent unauthorized module access for secured data and reprogramming of an ECU.

VI. CONCLUSION

The growth of vehicle cyber physical features like ADAS, fleet management system and carry-in devices, such as smartphones, portable silicon music-players and others are changing the paradigm of vehicle cyber risk that OEMs emphasizing more on cyber security implementation using cryptography based schemes and its validation to ensure that the vehicle is protected and can operate to its full potential, even in a malicious operating environment.

Although total security against any threat cannot be guaranteed by any security technology, every involved party responsible for development implementation and maintenance can reduce the risk and severity of an attack. Fundamental security elements implemented need to be tested and validated for their integrity by utilizing a substantial amount of test technologies and procedures. Current validation procedures for automotive components follows the stringent procedures of the test specifications agreed on by the OEM and its suppliers. Along with Validation of automotive components, OEMs are also emphasizing on Testing which is an area where OEMs need to innovate through new methods such as fuzz testing to ensure any vulnerable component or system will withstand even unknown attacks.

With greater awareness of cyber security and the evolution of highly automated vehicles, the case for cyber security becomes stronger much like safety is in todays environment.

REFERENCES

[1] Automotive Security Best Practices ,Recommendations for security and privacy in the era of the next-generation car.

[2] Hacking For Dummies, 4th Edition Published by John Wiley and Sons,
Inc.

[3] Car Hacking: For Poories,a.k.a. Car Hacking Too: Electric Boogaloo Chris Valasek, Director of Vehicle Security Research for IOActive.

[4] Automotive Cyber Security,Developing a thriving security ecosystem within automotive organizations,P3 north america, Inc. 25650 W 11 Mile Rd., Suite 300,Southfield, MI 48034, USA

[5] Embedded Security in Cars Securing Current and Future Automotive IT
Applications,Kerstin Lemke Christof Paar MarkoWolf (Eds.)

[6] Public Key Encryption and Digital Signature:How do they work?,CGI

[7] Responsibility for Vehicle Security and Driver Privacy in the Age of the Connected Car Sponsored by: Veracode, Duncan Brown February 2016

[8] THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPI-ONAGE Center for Strategic and International Studies ,July 2013

[9] State of the Art: Embedding Security in Vehicles Marko Wolf,1 Andre Weimerskirch,2 and Thomas Wollinger2

[10] Evaluation of Vehicle Diagnostics Security Implementation of a Reproducible Security Access Martin Ring, Tobias Rensen and Reiner Kriesten [11] Automotive Security,Author: Vinod Vasudevan, Senior Architect

[12] Security in Automotive Bus Systems Marko Wolf, Andr Weimerskirch, and Christof Paar

[13] Fundamentals of Cryptography:Algorithms and security services, Professor Guevara Noubir,North Eastern University

[14] CRYPTOGRAPHIC ALGORITHM METRICS,Norman D. Jorstad ,Director, Technology Identification and Analyses Center Landgrave T. Smith.

[15] Secure Key Management,A Key Feature for Modern Vehicle Electronics Christian Schleiffer, Marko Wolf, Andr Weimerskirch, and Lars Wolleschensky