Security Needs for the Future Intelligent Vehicles

Michael Jenkins and Syed Masud Mahmud
Wayne State University
ABSTRACT

The need for active safety, highway guidance, telematics, traffic management, cooperative driving, driver convenience and automatic toll payment will require future intelligent vehicles to communicate with other vehicles as well as with the road-side infrastructure. However, inter-vehicle and vehicle to roadside infrastructure communications will impose some security threats against vehicles' safety and their proprietary information. To avoid collisions, a vehicle should receive messages only from other authentic vehicles. The internal buses and electronics of a vehicle must also be protected from intruders and other people with malicious intents. Otherwise, a person can inject incorrect messages into an authentic vehicle's internal communication system and then make the vehicle transmit wrong information to the other vehicles within the vicinity. Such an event may have catastrophic consequences. Thus, a detailed study of the security needs of the future vehicles is very important.

In this paper, we will present the results of a comprehensive study related to various types of security threats against a vehicle's electronic communication system. The paper will identify various types of security attacks against a vehicle's electronic system. The paper will also address various issues that are related to the design of secure microcontrollers, secure electronic modules, secure communications through the vehicle's internal buses and privacy-protected secure peer-to-peer communications.

INTRODUCTION

There has been much interest in recent years to extend the functionality of vehicles to include active safety, traffic management, telematics, drive-by-wire, multimedia, remote diagnostics and software uploads, etc. Many of the proposed systems rely on wireless ad hoc networks and involve communications between a source vehicle and a target entity (inter-vehicle communications), where the target entity might be another vehicle or a roadside structure. Information from other vehicles, such as speed, acceleration, and position, will be provided either to the driver or to an active system like by-wire. Decisions are made based on this information. While these systems will improve the driving experience through enhanced safety, communications, and convenience, the once isolated vehicle will now be subject to threats and attacks that were not readily possible before.

Leaving the ad hoc network unprotected or easily hacked opens the door for attackers to broadcast false signals, repeat a legitimate broadcast at a later time, or block network signals (denial-of-service) altogether. Any of these situations could result in accidents.

Attacks on in-vehicle networks are possible through remote or physical access. Denial-of-service attacks are created on some in-vehicle networks if the network is flooded with high-priority messages (CAN), or through the introduction of malicious sleep frames (FlexRay and LIN). Other in-vehicle network attacks exist that would make the network inoperable [1].

In addition, vehicle controller software might be acquired through interception of software uploads and flash access code, or physical access of code storage locations. Disassembly and reverse engineering techniques applied to executables uncover the source code and might reveal one or several C-language vulnerabilities, opening the way for malicious code. Most PC users are familiar with software attacks by computer viruses, worms, Trojan horses, etc. The results range from slower execution of programs and the alteration of files, to stolen passwords and confidential information, and to denial-of-service. While much harm can come from these activities, it pales in comparison to the life-threatening situations that could arise if the software on fast-moving vehicles is compromised.

This paper is a survey of security threats and attacks on future intelligent vehicle systems and gives a general outline of what needs to be done to secure future systems. The paper is organized as follows. The next section defines secure communications, looks at security mechanisms including encryption techniques,
and finally general attack types. Following that is a brief look at what constitutes a future vehicle electrical system. The electrical system is broken down into inter-vehicle communications, in-vehicle networks, and control modules. The section titled Security Threats and Attacks investigates potential and documented threats and attacks on the electrical system. Following that, a general list of needs is presented to foster secure vehicle communications and information. Finally, the Conclusion offers a brief overview of the paper.

SECURE COMMUNICATIONS, SECURITY MECHANISMS, AND ATTACK TYPES

SECURE COMMUNICATIONS

There are a number of aspects to what constitutes a secure communication [2]. Secure communications should ensure that the data received is exactly the same as the data sent (data integrity), with no modifications, insertions, deletions, or replay. The identities of the communicating parties should be verified (authentication). The data should be protected from unauthorized parties (data confidentiality). A communication system should be available (availability) and access limited (access control) to authorized users. Finally, some means to prove that the transmitting entity sent a message and the receiving entity received the message is desired (nonrepudiation).

SECURITY MECHANISMS

Security can be achieved through both software and hardware. To achieve secure communications, mechanisms include encipherment, digital signatures, access control, data integrity, authentication exchange, traffic padding, routing control and notarization. Of all these methods, encipherment covers most of what constitutes a secure communication.

Encipherment, or the use of cryptographic algorithms to protect and obscure data, can be grouped into three different classes [3, 4].

- **Symmetric ciphers** involve the use of a secret key to encrypt data by a sender. The original message is known as plaintext and the encrypted message is called ciphertext. The ciphertext message is sent to a receiver who uses the same secret key to decrypt the message and retrieve the original plaintext message. Symmetric ciphers are faster to code and decode and are used to protect the transmission of large amounts of data. Key management becomes an issue since both parties share the same key. Examples of symmetric ciphers include the stream and block ciphers AES, 3DES, DES, and RC4.
- **Asymmetric ciphers**, also known as public-key algorithms, use a public key known to all parties for encryption and a private key for decryption. This class of ciphers is used to initiate sessions (authentication), to digitally sign messages, and for key exchange. Asymmetric ciphers tend to be slow to execute due to the more intense computational algorithms employed in their execution. Some examples are RSA and Diffie-Hellman.
- **Secure Hash algorithms** convert messages into unique fixed length messages. Each message has a unique fingerprint. Hashes are used for Message Authentication Codes (MACs) to enhance data integrity. Some examples include MD5 and SHA.

ATTACK TYPES

Attacks can be either passive or active [2]. A passive attack involves monitoring communications with no alteration of data, otherwise known as **eavesdropping**. Listening to phone conversations or traffic analysis to discover sensitive information like passwords or credit card information are examples.

Active attacks involve the manipulation of data. These attacks include **masquerade, replay, modification of messages**, and **denial-of-service**. A masquerader pretends to be someone they are not and broadcasts false messages. When proper authentication of communications is not in place, this becomes an issue. Replay involves the capture of a legal transmission and the replay of that transmission at a later time to disrupt the system. Replay becomes important in transmissions in which something was true at a particular point in time but not afterwards. Modification of messages modifies, inserts or deletes data. Finally, denial-of-service renders communication impossible. Jamming of signals is just one example of this type of attack.

Attacking encrypted messages is accomplished through **cryptanalysis** and **brute-force** attacks. Cryptanalysis relies on knowledge of the algorithm used and perhaps some sample plaintext-ciphertext pairs or some knowledge of probable keys. A brute-force attack tries every possible key on a piece of ciphertext until readable plaintext appears. With the use of supercomputers, brute-force attacks are not improbable.

FUTURE VEHICLE SYSTEMS

In this paper, the future vehicle electrical system of concern is divided into three separate systems. The first system, termed the **inter-vehicle communication system**, is used for vehicle communications outside of the vehicle. These systems include the **ad hoc networks**, as well as **vehicle positioning systems**. The second system is the **in-vehicle network** used for communications between vehicle modules. These networks include CAN, LIN, FlexRay, and MOST, among others. The last system, the vehicle **module**, includes the controller with its sensors and actuators. While many controllers have built-in CAN controllers, we choose to separate the two functions.
INTER-VEHICLE COMMUNICATIONS

Ad Hoc networks

Ad hoc networks are short-range, often temporary networks that do not require a base station or infrastructure to enable communications and support nodes that are in motion. This makes them ideal for vehicle communications between other vehicles and to short-range roadside structures. This paper examines three ad hoc systems that are potential candidates for vehicle network use.

- **Dedicated Short Range Communications (DSRC)** [5] is a short-range wireless technology proposed for mobile, ad hoc networks by the Crash Avoidance Metrics Partnership Vehicle Safety Communications Consortium, consisting of BMW, DaimlerChrysler, Ford, GM, Nissan, Toyota, and VW, along with the U.S. Department of Transportation. DSRC operates in the 5.9 GHz band and has a range of 1000 m. It supports various communication types including one-way from and to the vehicle, two-way, point-to-point and point-to-multipoint communications. The latter includes the ability to broadcast messages from a vehicle to the environment. In addition, it has the shortest latency (< 100 ms) between communications of any current wireless technology, although this figure is based on encryption-less communication.

- **Bluetooth** is a short-range wireless technology used today in wireless handsets, wireless connections to a LAN or peripheral devices, and the synchronization of PDA devices with PCs [6]. Current and proposed vehicle applications include hands-free use of cell phone and control of lights, radio, wipers, etc., remote start of engine, remote monitoring of various parameters including tire pressure, and automatic toll payment. Class 1 Bluetooth-enabled devices have a documented range of 100 m and the more common Class 2 devices have a documented range of 10 m, although experiment has shown a more extended distance. Bluetooth operates in the 2.4 GHz ISM (industrial, scientific, and medical) band and supports two-way and point-to-point communications. Bluetooth has a published latency of 3-4 seconds, although with established networks research has shown that value to be 30 milliseconds.

- The **IEEE 802.11** standard was designed as a wireless extension to the wired Ethernet standard (IEEE 802.3). IEEE 802.11 became known as WiFi, for “Wireless Fidelity”. WiFi systems can operate in an infrastructure mode, where a wireless device connects to a wired base station, or in ad hoc mode (“peer-to-peer”). Currently there are four versions of 802.11. The table 1 shows the four versions with specifications.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Max Speed (Mb/s)</th>
<th>Frequency Band</th>
<th>Compatibility With</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b</td>
<td>11</td>
<td>2.4 GHz</td>
<td>b</td>
</tr>
<tr>
<td>802.11a</td>
<td>54</td>
<td>5 GHz</td>
<td>a</td>
</tr>
<tr>
<td>802.11g</td>
<td>54</td>
<td>2.4 GHz</td>
<td>b, g</td>
</tr>
<tr>
<td>802.11n</td>
<td>100</td>
<td>2.4 GHz</td>
<td>b, g, n</td>
</tr>
</tbody>
</table>

**Table 1: WiFi Specifications**

The maximum range for this technology is 1000 m and it supports both two-way and point-to-point communications. Table 2 below compares the three technologies.

<table>
<thead>
<tr>
<th>Wireless Technologies</th>
<th>DSRC</th>
<th>Bluetooth</th>
<th>IEEE 802.11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Range</td>
<td>1000 m</td>
<td>100 m</td>
<td>1000 m</td>
</tr>
<tr>
<td>Two-Way</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Point-to-point</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Point-to-multipoint</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Latency</td>
<td>200 µs</td>
<td>2-3 s 30 ms</td>
<td>3-5 s</td>
</tr>
</tbody>
</table>

**Table 2: Wireless Technologies**

Vehicle positioning systems

Vehicle positioning systems assist drivers with exact location, driving distances to prospective locations, and route planning. In addition, GPS systems can provide very accurate time information.

- **Global Positioning Systems (GPS)** are radio-based navigation systems that offer three-dimensional position, velocity and time information for all sorts of vehicles. 24 low-power emitting satellites make up the system as well as 5 ground stations. GPS works by accurately measuring the time that it takes to receive radio signals from 3 of the 24 satellites and, through the process of trilateration, determining where in space the receiver is.

- A proposed position system, called **verifiable multilateration** [7-9], uses ground-based towers,
similar to cell towers, and trilateration to determine the exact position of a vehicle. This technique uses distance bounding, a method that measures the time between sending and receiving a signal from a tower to a vehicle and also uses digital signatures to prove that the vehicle in question is \(x\) meters from the tower.

IN-VEHICLE BUS SYSTEMS

Vehicle Buses

There are several vehicle buses in use. This paper looks at four that are in use currently

- The **Local Interconnect Network** (LIN) \([10]\) is a low-cost, single wire sub network used for power doors, windows, and mirrors as well as light and rain sensors, or anywhere where bandwidth and safety-criticality are not issues. LIN was introduced in vehicles in the year 2001. LIN has data rates of up to 20 kBit / s, uses a single master that polls up to 16 slaves and thus eliminates collisions, and has the capacity for synchronization of nodes. In addition, LIN provides a special sleep mode controlled by sleep and wakeup messages, and uses checksums and parity bits for error checking.

- The pervasive **Controller Area Network** (CAN) \([11]\) has become the most common vehicle bus since its introduction in 1986 at the SAE World Conference in Detroit. Modules utilizing CAN range in complexity and safety-criticality from medium (park assist module) to high (engine and transmission control, antilock brakes). The CAN bus has a multi-master architecture where messages are prioritized according to their message ID, with the lowest numbered ID having the highest priority. This method (Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)) guarantees collision-free transmissions. CAN also offers error detection chiefly through the so-called Cyclic Redundancy Check (CRC) field and with parity bits, as well as a mechanism for detection and disconnection of faulty controllers.

- **FlexRay** and **Time-Triggered CAN** \([12]\) were introduced in order to meet the demands of very high safety critical applications, such as the by-wire systems. They use the Time Division Multiple Access (TDMA) method that utilizes synchronous nodes and fixed time slots for every node. Within a time slot, some asynchronous activity with priority access similar to CAN is also reserved for less time-critical messages. These protocols feature higher data rates (10 Mbit / s) and error tolerance using CRC, channel redundancy, and, within FlexRay, a bus guardian that detects and handles logical errors.

- **Medium Oriented System Transport** (MOST) \([13]\) is a serial bus that offers up to 24 Mbit / s bandwidth and is used chiefly with fiber optics to transfer voice, audio, and video. Like the TDMA methods above, MOST offers both synchronous and asynchronous data transmissions. MOST uses sender and receiver addresses and has a control channel that allows devices to request and release one of the 60 data channels. Errors are handled by an internal system that detects errors using parity bits, status flags, and CRC, and disconnects faulty nodes.

Table 3 compares the various in-vehicle buses.

<table>
<thead>
<tr>
<th>Bus</th>
<th>LIN</th>
<th>CAN</th>
<th>FlexRay</th>
<th>MOST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecture</td>
<td>Single</td>
<td>Multi</td>
<td>Multi</td>
<td>Multi</td>
</tr>
<tr>
<td>(Single or Multi Master)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>Polling</td>
<td>CSMA/CD</td>
<td>TDMA</td>
<td>TDM</td>
</tr>
<tr>
<td>(Synchronous Asynchronous)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transfer Mode</td>
<td>S</td>
<td>A</td>
<td>S and A</td>
<td>S and A</td>
</tr>
<tr>
<td>Data Rate Mb/s</td>
<td>.02</td>
<td>1</td>
<td>10</td>
<td>24</td>
</tr>
</tbody>
</table>

### Table 3: In-Vehicle Bus Specifications

MODULES

Module controllers vary in size and complexity \([14]\). Some modules, like engine control modules, perform thousands of calculations based on numerous sensors and calibrations, have high throughput requirements, have many safety-critical functions, and large software program sizes. On the other hand, modules, like tire pressure modules, have low performance requirements.

Likewise, there are numerous hardware chips available. System-on-chip designs offer CPU, memory, and sometimes CAN transceivers on one chip. These designs make it more difficult to monitor internal bus activity except through invasive techniques. Other systems rely on external memory to the CPU as well as external peripherals and are more challenging to secure.

SECURITY ATTACKS

INTER-VEHICLE COMMUNICATIONS ATTACKS

Ad Hoc Networks

As of this writing, no aspects of secure communications (authentication, data confidentiality, etc.) are in place for **DSRC** \([5]\), so almost any scenario is possible. The following examples underscore the need for secure communications with vehicle-to-vehicle and vehicle-to-roadside structure communications.

- A **masquerade** can occur if an attacker broadcasts false information from a trusted roadside structure or other vehicle. For instance, consider a situation...
where an accident occurred ahead of another vehicle and the accident is out-of-sight of that vehicle (say over a hill and at night). An attacker broadcasts messages from a trusted roadside structure to the vehicle that the way ahead is clear. Trusting that information, the vehicle proceeds ahead without slowing down and an accident occurs.

- **Replay** can occur in the following scenario. Suppose at a particular location and point in time, a vehicle broadcasts a legitimate signal to vehicles behind it that the way is clear. An attacker records this message. Later at night the road freezes and the attacker rebroadcasts the message at the same point to other vehicles behind it. Again, the vehicles trust the information and proceed without slowing down.

- An example of a **modification of message** attack follows. Suppose that a roadside structure broadcasts the message "Accident ahead but afterwards the way is clear". A vehicle, the attacker, receives this message. The attacker in turn rebroadcasts the message to vehicles behind it but leaves out "Accident ahead but afterwards".

- **Jamming** the wireless network is a form of a **denial-of-service** attack. Sabotaging roadside structures are other ways of disrupting or denying service.

- If financial transactions are involved, say in toll collection, payment for location-based services, etc., **eavesdropping** will most certainly be involved to gain credit card or password information.

**Bluetooth** has security mechanisms in place. However, there have been documented attacks.

- One of the main vulnerabilities with Bluetooth resides with the PIN [6]. The PIN, usually a 4-digit number, is a small number that can easily be hacked using brute force techniques. In "Cracking the Bluetooth PIN" [15], Yaniv Shaked and Avishai Wool described both passive and active methods for obtaining the PIN. Using a Pentium III, 450 MHz and a Pentium IV 3 GHz HT computer, they demonstrated that the PIN could be revealed in 0.3 and 0.06 seconds respectively.

- The normally short-ranged Bluetooth class 2 devices (10 m) can be extended to a distance of one mile by using directional antennas. This method, known as Bluetooth sniping, makes attacking these devices easier.

- A Bluetooth virus was created by a group of virus writers known as 29a and presented to anti-virus groups. It was written as a proof-of-concept experiment. The virus requires that the user download software to the device and has not propagated "in the wild".

The former security mechanism for **IEEE 802.11 wireless LANs**, the so-called Wired Equivalent Privacy or WEP, proved to have weaknesses [16] and was subsequently attacked [17]. This attack was a direct cryptanalysis attack on the stream cipher RC4. The result of this successful attack eventually lead to an improved mechanism based on the block cipher Advanced Encryption Standard (AES) known as WiFi Protected Access 2 (WPA2). As of this writing, there are no reported successful breaches of AES-based security.

**Vehicle Positioning Systems**

**GPS** satellites emit low-power signals. With the use of a GPS simulator an attacker (masquerade attack) could overpower the signal and send false signals [7]. A modification of message attack occurs if any ∆t is added or subtracted from a legal signal and transmitted to the environment, thus falsifying exact position data. Lastly, denial-of-service is achieved through jamming the selective frequencies.

**IN-VEHICLE BUS SYSTEM ATTACKS**

Vehicle bus systems are vulnerable to attacks from the vehicle owner, garage personnel, and third parties. Buses are completely exposed and, with the proper equipment, eavesdropping and masquerading may be possible. Current communication between controllers is unencrypted, with no peer-to-peer authorization, and documentation on bus structure and protocols is readily available. The following details specific threats to the buses discussed above [1].

- There are a number of means to shut down or limit accessibility (denial-of-service) to **LIN** networks. One method disables the master and thus cripples the network. Another method introduces sleep message frames. Moreover, modifying the message field responsible for time synchronization (SYNC) renders nodes that rely on time synchronization inoperable.

- The most common type of attack on **CAN** is denial-of-service. This is achieved by continually transmitting high-priority messages (low numbered message ID), thus effectively jamming the network. Moreover, introducing malicious code that sets or posts error flags related to a specific controller would disable it through the CAN mechanism that locates and disconnects faulty controllers.

- **FlexRay** also has its vulnerabilities that can deny service to nodes. The network can be rendered inoperable if more than \(n/3\) SYNC messages are introduced within one communication cycle, where \(n\) is the number of FlexRay nodes. The bus guardian feature can be used, as in CAN, to disable specific controllers when malicious error frames are introduced. Also, like LIN, denial-of-service can be achieved through directed sleep frames.

- Disabling the timing master in a **MOST** network would effectively shutdown the network. In addition, continuous bogus channel requests would be a denial-of-service attack for other nodes that want bus access. Moreover, for asynchronous data transmissions, denial-of-service attacks similar to
MODULES

Modules are as physically accessible as the vehicle bus and can be attacked both through software and hardware. Attacks can occur with non-encrypted, as well as encrypted devices.

Software Attacks

The very nature of software makes it vulnerable to attacks. Software complexity and changeability are two reasons. For real-world programs, the complexity of the software translates to the increased likelihood of a bug or threat [18-20]. Changing and updating software is a common occurrence to introduce new functionality or to fix bugs. This process leaves the software open to attacks, particularly if remote software uploads are an available feature.

Attacking software generally requires some knowledge of the source code to find and exploit vulnerabilities [19]. Should the executable become available, hackers have a variety of tools available to reverse engineer the code. A debugger is a software program that attaches itself to other software programs and allows control of those programs. Debuggers allow stepping, setting breakpoints, and viewing variables and memory. Debuggers are available in two types: the user-mode type for debugging applications and the more powerful kernel-mode type for device drivers and operating systems. Disassemblers convert machine code to assembly code. Since assembly is device specific, the tool must understand the device’s assembler. Decompilers convert machine code to assembler or source code. Decompilers have the same requirements as disassemblers but in addition must know the source language.

Moreover, most embedded software for vehicles is written in the C and C++ languages. There are many C-language vulnerabilities, some of which, if exploited, can result in crashing a program (denial-of-service) or transferring control to malicious code (worms, viruses). A partial list [20] of C-language vulnerabilities include: generic logic errors; misused C functions like strcpy, sprintf, and strcat; format stings; generic incorrect bounds checking; loop constructs; off-by-one vulnerabilities; non-null termination issues; skipping beyond a null-terminated byte; signed comparison vulnerabilities; integer-related overflows; different-sized integer comparisons; double free vulnerabilities; and out-of-scope memory usage.

A type of malicious code that affects low-level system functionality is a kernel rootkit. Kernel rootkits are loadable modules or drivers (executables) providing complete access to system functionality, including the ability to read and write to memory.

Hardware Attacks

Hardware attacks can be classified as either invasive or non-invasive. Invasive attacks physically open a device to gain access to system internals. Examples of invasive attacks include micro-probing and reverse engineering. On the other hand, non-invasive attacks do not destroy the device but use other means (side-channel attacks) such as timing analysis, power analysis, fault induction, and electromagnetic analysis to gain secure information. Side-channel attacks are similar to a thief breaking into a house through a window rather than a multi-locked door (cracking the cryptographic algorithm through cryptanalysis).

- Invasive micro-probing techniques are used with system-on-chip designs to discover the general layout of the chip as a precursor for non-invasive techniques or to simply read internal bus messages. The first step is to remove the outer coating of the chip packaging (de-package) using a fuming acid. Afterwards, successive layers of the chip are de-packaged and observed through microscopy. All processor internals such as the instruction decoder, data and memory buses, ALU, ROM, memory boundaries, etc. are discovered. Values on buses and interfaces to components are analyzed with manual micro-probing or e-beam microscopy. While this technique may not reveal all necessary information, it is useful for certain non-invasive techniques explained below.

- In “Cipher Instruction Search Attack on the Bus-Encryption Security Microcontroller DS5002FP”, Markus Kuhn [21] describes a non-invasive physical attack on the DS5002FP processor. This processor uses bus encryption for data and software that is stored externally in SRAM. The attack, similar to a brute-force attack, uses special hardware to present guessed encrypted machine instructions to the processor, repeatedly reset the processor, and observe the CPU reaction. The object is to discover the encrypted CPU instructions like MOV and NOP, as well as the address of a parallel port. Once discovered, memory dumps are output in plaintext to the port. This information is then disassembled and the protected software revealed.

- The timing analysis attack is a side-channel attack that analyzes the time that a processor takes to perform cryptographic computations [22] and involves predictions about the key value. The technique presumes that a key value is presented, bit-by-bit, to the crypto hardware or software and that the computation time per bit is non-constant. In this case two operations exist, one for a value of 0 for the bit and one where the value is 1. The attacker measures the time for a set of inputs (bit value 0 and 1) and then measures the correlation between the measured time and the estimated time for each input. The actual value used should show the strongest correlation. After that, subsequent key values are presented.
• The power analysis attack, also a side-channel attack, is similar to timing analysis, but uses the correlation between computations performed for key evaluation and the current drawn by the device [23]. This attack assumes that the power consumption of the micro is largely because of gate transitions and the parasitic capacitance of internal wiring. Power consumption increases with a greater number of state transitions and if transitions are occurring at larger gates or greater capacitive loads. The attack involves presenting a large number of key values to the processor and collecting power traces with each key.

• Electromagnetic analysis attacks are similar to both timing and power analysis attacks [24]. This attack measures the electromagnetic radiation emitted by a micro and has been shown to reveal protected information. Since the internal structure of the device is necessary for an electromagnetic attack, invasive techniques are used prior to employing this technique.

• Boneh, DeMillo, and Lipton [25] showed that attacks are possible on cryptographically protected processors through fault induction. An induced fault is a flipped bit in a register caused by random hardware glitches such as power transients, high temperature, static electricity, magnetic field, etc. The attacks exposed the key values for RSA, RSA based on the Chinese Remainder Theorem, Fiat-Shamir, and Schnorr’s algorithms.

NEEDS FOR SECURING VEHICLE COMMUNICATION AND INFORMATION

The attacks on various vehicle systems mentioned above underscore the need for both communication and information security. The following lists many of those needs.

• Inter-vehicle communications authentication to identify legitimate sources. These sources include other vehicles and roadside structures.

• Inter-vehicle communications encryption for data confidentiality. While not all messages sent to and from other vehicles and roadside structures need encryption [26], some sensitive information does. Financial transactions, password protection and software uploads are examples.

• Inter-vehicle communications data integrity to insure that the data sent and the data received are the same.

• A firewall or gateway between inter-communication networks and in-vehicle networks to screen messages that are sent and received, route incoming messages to the appropriate place, and possibly encrypt and authenticate outgoing messages.

• Use of in-vehicle bus encryption for confidentiality. In addition, if new encryption keys are passed to vehicle modules by some controlling source, bus encryption prevents eavesdropping.

• The ability to change encryption keys and some form of key management. Brute force attacks can potentially break any encryption key. Changing keys regularly protects the system from this type of attack.

• The failure of a system, either through some defect, a natural disturbance, or malicious behavior, such as signal jamming, is an issue. Providing some system redundancy for safety-critical applications is a means to assure reliability and system robustness.

• Nonrepudiation, or the proof that a message was sent by an entity and received by another, is useful for recreating the scene of an accident or proof of responsibility in an accident. Data recorders can be used for this situation.

• Awareness and elimination of software vulnerabilities in embedded system code and techniques to impede reverse engineering and disassembly should executables fall into the hands of hackers.

• Module authentication protects against the illegal insertion of controllers within a vehicle system. Trusted modules broadcasting false information endanger both the host vehicle and other vehicles that rely on that information.

• Tamper resistant module hardware guarantees that encryption keys, code, and sensitive data are not readily available to hackers. Methods exist that address each of the physical and side-channel attacks described above, including message blinding, randomized clock signals, data-masking, reduction of signal amplitudes, the introduction of noise in power measurement data, aggressive shielding techniques, non-localized internal chip component layouts, and sensors to monitor and respond to environmental changes.

CONCLUSION

The brave new world of future intelligent vehicles promises another level of vehicle performance in the area of safety, traffic management, highway guidance, remote repair, and driver convenience. However, these improvements open the door for attacks not just on inter-vehicular communications, but also with the rest of the communication and information system. This paper investigated the meaning of secure communications, the potential and real threats and attacks on future vehicle systems, and the security needs for those systems. For future work, the authors intend to address the issues outlined above and create a coherent vehicle system that considers security for all future intelligent vehicle needs.

REFERENCE


CONTACT

Syed Masud Mahmud, Ph.D.
Associate Professor
Department of Electrical and Computer Engineering
Wayne State University
Detroit, MI 48202
Phone: (313) 577-3855
Fax: (313 577-1101
Email: smahmud@eng.wayne.edu

Michael Jenkins
Ph.D. Student at Wayne State University
Department of Electrical and Computer Engineering
Wayne State University
Detroit, MI 48202
Email: mbj5@dcx.com