An efficient lightweight Cryptographic Algorithm for Secure Control of Vehicle using Smart Phone

N. Mamtha[1], N. Leo Bright Tennisson[2], G. Rekha[3]

[1] *Student, Department of Computer Applications, Valliammai Engineering College, Tamil Nadu, India*
[2] *Assistant Professor, Department of Computer Applications, Valliammai Engineering College, Tamil Nadu, India*
[3] *Assistant Professor, Department of Computer Applications, Valliammai Engineering College, Tamil Nadu, India*

---***---

Abstract - *Vehicles are controlled and accessed through smart phones together with embedded systems. Communication between smart phone and Electronic Control Unit [ECU] in the vehicles is made over Bluetooth connection. This connection is secured by a security session layer which uses encryption algorithms. In this article we provide an encryption technique which is efficient, fast, and lightweight in terms of processing and provides sender device authentication on the receiving side. It is becoming widely popular to control and access vehicles through smart phones together with embedded systems. There exist vulnerabilities like improper validation, exposure and randomness. Especially in case of vehicles controlled by smart phones over Bluetooth there are possibilities for Man-In-The-Middle (MITM) attack and other attacks of falsification of information Recently, several researchers highlighted this aspect and successfully demonstrated attacks against different vehicles [1], [2]. Each of these works showed that it was possible to take control of certain functionalities of the vehicle, and interfere with safety-critical or sensitive components. These vulnerabilities hamper novel solutions (e.g., smart phones to unlock the vehicle door or to start the engine), because of the risk of successful attacks. Adding security mechanisms to vehicles is a challenging task, as the related embedded architectures are commonly designed with safety requirements rather than security ones in mind. We explicitly take the capabilities of the target architecture into account (i.e., no input capabilities on the vehicle side, limited output capabilities, and lack of a trusted execution environment on the mobile device). Latest research solution allows a smart phone to establish a secure session layer over an insecure radio connection, which provides additional security guarantees regardless of the security mechanisms already implemented in the physical layer (if any).As a result, the entire application layer is transparently secured.*

Key Words: Encryption, Bluetooth, Electronic Control Unit, Man-In-The-Middle, Embedded Systems, and Smart Phone etc…

1. RECENT WORK

Researchers had established a secure session layer over an insecure radio connection [3]. This security layer use encryption algorithms like AES and SHA-1. This method encrypts the message before it is transmitted from the smart phone and it is decrypted by the Electronic Control Unit [ECU] that is available in the vehicle. But no authentication is made about the sender's mobile device on the receiving side. There is a possibility of some other mobile device to pair with ECU in the vehicle. The encryption algorithms have a draw back in terms of processing burden and time constraints. Also these methods provide no authentication for sender's mobile device. In this article we present an enhanced security layer which is efficient, less complexity when compared to other encryption and provides authentication for sender mobile device on the receiving side.

2. SYSTEM ARCHITECTURE

Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here.

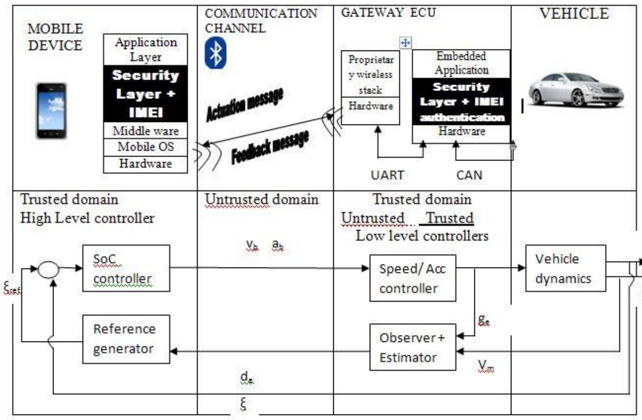

Fig -1: Architecture of Smartphone Vehicle Control System

We successfully implemented the aforementioned system architecture. Specifically, we implemented an intelligent range extender for lightweight electric vehicles, with the goal of optimizing the energy consumption by actively modifying the vehicle dynamic behavior, as detailed in [4]. This task is accomplished with a two-layer structure. A high-level controller keeps track of a reference profile, ξ_f, for the battery *state of charge* (SoC), ξ . The profile is generated by taking into account the route length and its elevation profile, as detailed in [6]. The mo-bile device implements the SoC controller within an *ad-hoc* app that we developed, which also includes navigation features that leverage on Internet-based services (e.g., Google Maps API). Furthermore, the low-level control loops enforce speed and acceleration constraints (v_b and a_b in, which allow meeting the desired energy consumption profile. The low-level controllers act on the gas handle opening g to guarantee that the dynamical behavior of the vehicle (i.e., speed v and acceleration a_e) is kept within the prescribed limits. The Gateway ECU implements and executes the low -level control loops on a 16-bits dsPIC micro-controller with a CPU speed of 20 Mips [7], and communicates with sensors and actuators *via* CAN bus. The Gateway ECU and the mobile device communicate *via* a Bluetooth layer. They exchange both initialization and real time control data. Initialization data is packed into a 48 bytes frame and the communication is unidirectional from the mobile device to the gateway ECU. On the contrary, the real time communication is bidirectional: The Gateway ECU sends a 64-bytes payload every 0.2 s (5 Hz), whereas the mobile device communicates 6 bytes control-data packet every time the vehicle travels 50 m. Simulation results and experimental data collected on a prototype light 4-wheeled

Toy vehicle prove the effectiveness and the robustness of the proposed approach. The vehicle equipped with the SoC con-troller saves approximately 20% of the energy supplied by the battery, with respect to a nominal driving behavior.

3. SECURITY ISSUES

The Bluetooth layer protocol has a two -phase session setup: after the *pairing process*, which allows the peers to get to know each other and set up the network properties, the actual *communication* is enabled. Depending on the protocol version, different security features are available. However, the early Bluetooth standard and its successors, with the introduction of the *secure simple pairing* (SSP) protocol [8], suffer from various security vulnerabilities due to weak cryptographic primitives, as discussed in [9], [10]. The security of most Bluetooth applications (e.g., in embedded scenarios) relies on a static PIN only, with no way to change it.

3.1 A Security Layer for Automotive Services

Given the application scenario and the aforementioned security issues, it is necessary to devise an *application-level security mechanism* that mitigates the vulnerabilities that lie in the wireless link. Such security layer must be independent from the underlying wireless layer and must allow secure communication between the mobile device and the vehicle. In our attack model the adversary knows the radio protocol in use, and is able to transmit and receive arbitrary data packets on the radio interface. The objective of the attacker is to obtain access to the information exchanged between the vehicle and the mobile de-vice, and ultimately manipulate the ECU execution flow. We concentrate on the application layer. Therefore, attacks against the physical layer (e.g., jamming) or attacks that require physical, even temporary, access to the vehicle (e.g., forceful shut-down) fall outside the scope of our security layer.

3.2 Security Analysis

When a vehicle is being accessed and controlled by mobile there is a possibility of another mobile device to pair with the ECU mounted on the vehicle either accidentally or intentionally. So apart from encrypting the communication message alone there must be security mechanism that authenticates the sender's device on the receiving side. This prevents any intruder mobile device which is paired to the ECU from accessing the vehicle.

3.3 Secure Session Layer

Above breech in the security system is tackled by our proposed special encryption method. Our proposed encryption algorithm uses hash function. This hash function computes hash value over the concatenation of message M and IMEI/SV International Mobile Station Equipment Identity number which is commonly shared by the mobile device and the ECU mounted on the vehicle.
Sender computes the hash value over the concatenation of M and IMEI number and appends the resulting hash value to M. Because the ECU on the vehicle possesses IMEI

number, it can recompute the hash value to verify. Because the IMEI number itself sent in encrypted form, an intruder cannot modify an intercepted message and cannot generate a false message

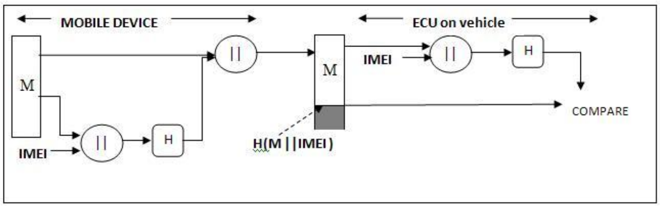

Fig-2 Encryption and Decryption with IMEI authentication

3.4 Algorithm

3.4.1Encryption

e=M||H(M||IMEI number)

- e is the encrypted message
- -Only Mobile Device and ECU share IMEI number
-

3.4.2 Decryption

H= H(M||IMEI number)

Compute the hash code of received message plus IMEI number

3.5 IMEI Number

The International Mobile Station Equipment Identity or IMEI is a number, usually unique, to identify 3GPP (i.e., GSM, UMTS and LTE) and iDEN mobile phones, as well as some satellite phones. It is usually found printed inside the battery compartment of the phone, but can also be displayed on-screen on most phones by entering *#06# on the dial pad, or alongside other system information in the settings menu on smart phone operating systems.

The IMEI number is used by a GSM network to identify valid devices and therefore can be used for stopping a stolen phone from accessing that network. For example, if a mobile phone is stolen, the owner can call his or her network provider and instruct them to "blacklist" the phone using its IMEI number. This renders the phone useless on that network and sometimes other networks too, whether or not the phone's SIM is changed.

3.5.1 Structure of the IMEI and IMEISV (IMEI Software Version)

The IMEI (15 decimal digits: 14 digits plus a check digit) or IMEISV (16 digits) includes information on the origin, model, and serial number of the device. The structure of the IMEI/SV is specified in 3GPP TS 23.003. The model and origin comprise the initial 8-digit portion of the IMEI/SV, known as the Type Allocation Code (TAC). The remainder of the IMEI is manufacturer-defined, with a Luhn check digit at the end. For the IMEI format prior to 2003, the GSMA guideline was to have this Check Digit always transmitted to the network as zero. This guideline seems to have disappeared for the format valid from 2003 and onwards.

As of 2004, the format of the IMEI is *AA-BBBBBB-CCCCCC-D*, although it may not always be displayed this way. The IMEISV drops the Luhn check digit in favour of an additional two digits for the Software Version Number (SVN), making the format *AA-BBBBBB-CCCCCC-EE*

4. Security Evaluation

The proposed encryption using hash function is simple and fast when compared to other encryption techniques like AES. Also they do not provide authentication for the sender's mobile device on the receiving side.

- A hash value h is generated by a function H of the form h = H (M || IMEI number). M is a variable length message and IMEI number is 14 or 16 bits. The hash value is appended to the message at the source at a time when the message is assumed or known to be correct.
- H can be applied to a block of data of any size
- H produces a fixed length output
- H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical
- For any given value h, it is computationally infeasible to find x such that H(x) = h.
- For any given block x, it is computationally infeasible to find y ≠ x with H(y) = H(x).
- It is computationally infeasible to find any pair(x, y) such that H(x) = H(y).

Experiment results showed that the proposed encryption or decryption techniques require an execution of 2.25 microseconds which is faster than the other encryption techniques. Apart from this execution other time limit like pairing of mobile devices, etc… are same as with the previous researches.

5. Conclusion

The proposed encryption technique proved to be efficient and lightweight in terms of processing time and speed. Also the article provides an holistic security which protects the message as well as allows the receiving side to ensure that the message is from authenticated sender device.

REFERENCES

[1] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of incar wireless networks: A tire pressure monitoring system case study," in *Proc. 19th USENIX Conf. Security*, Berkeley, CA, USA, 2010, pp. 21–21.

[2] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and

T. Kohno, "Compre-hensive experimental analyses of automotive attack surfaces," in *Proc. 20th USENIX Conf. Security*, Berkeley, CA, USA, 2011, pp. 6–6.

[3] A. Dardanelli, F. Maggi, M. Tanelli, S. Zanero, S. M. Savaresi, R. Kochanek, and T. Holz, A Security Layer for Smartphone-to-Vehicle Communication Over Bluetooth, IEEE EMBEDDED SYSTEMS LETTERS, VOL. 5, NO. 3, SEPTEMBER 2013

[4] A. Dardanelli, M. Tanelli, B. Picasso, S. Savaresi, O. di Tanna, and M. Santucci, "A smartphone-in-the-loop active state-of-charge manager for electric vehicles," *IEEE ASME Trans. Mechatron.*, vol. 17, no. 3, pp. 454–463, 2012.

[5] C. Spelta, V. Manzoni, A. Corti, A. Goggi, and S. M. Savaresi, "Smart-phone-based vehicle-to-driver/environment interaction system for mo-torcycles," *IEEE Embed. Systems Lett.*, vol. 2, no. 2, pp. 39–42, Jun. 2010.

[6] A. Dardanelli, M. Tanelli, and S. M. Savaresi, "Active energy manage-ment of electric vehicles with cartographic data," presented at the 2012 IEEE Int. Electr. Veh. Conf., 2012.

[7] Microchip Technology Inc., 16-bit dsPIC® Digital Signal Controllers.

[8] NIST Special Publication 800-121 Revision 1, Guide to Bluetooth Se-curity: Recommendations of the National Institue of Standards and Technology 2012.

[9] C. Hager and S. Midkiff, "Demonstrating vulnerabilities in bluetooth security," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM'03)*, 2003, vol. 3, pp. 1420–1424.

[10] K. Haataja and P. Toivanen, "Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures," *IEEE Trans. Wireless Commun.* vol. 9, no. 1, pp. 384–392, Jan. 2010 [Online]. Available: http://dx.doi.org/10.1109/TWC.2010.01.090935

BIOGRAPHIES

Ms. N. Mamtha is a Student Pursuing MCA course in Valliammai Engineering College. She is a talented, dedicated and hard working student.

Mr. N. Leo Bright Tennisson is an Assistant Professor, in Department of Computer Applications, Valliammai Engineering College. He has about 9 years of teaching experience in Engineering College and published various research papers in Conferences and International Journal

Ms. G. Rekha is an Assistant Professor, in Department of Computer Applications, Valliammai Engineering College. She has 7 years of teaching experience in Engineering College.