Wireless Communication between Vehicle and Smartphone using ARM7

Suphiya M. Tamboli[1] Dr. Y. S. Angal[2]
[1,2]Department of Electronics & Telecommunication Engineering
[1,2]JSPM'S BSIOTR, PUNE

Abstract— Modern vehicles are increasingly being interconnected with computer systems, which collect information both from vehicular sources and Internet services. Vulnerabilities likes improper validation, exposure and randomness. These vulnerabilities include device address validation, invalid states and exposed keys. Man-In-The-Middle (MITM) attacks on Bluetooth Secure Simple Pairing (SSP) and other attack of falsification are major findings. In this article I come up solution that allows a Smartphone to establish a secure session layer over an insecure radio connection, which provides additional security guarantees regardless of the security mechanisms. Hierarchically distributed control system architecture which integrates a Smartphone with classical embedded systems, and an ad-hoc, end-to-end security layer is designed to demonstrate how a Smartphone can interact securely with a modern vehicle without requiring modifications to the existing in vehicle network as a result, the entire application layer is transparently secured with implementation of RSA algorithm for encryption.

Key words: Embedded Architecture, Two wheeled vehicle, Bluetooth, Smartphone

I. INTRODUCTION

The current trend in automotive products and services is to improve the accessibility of the vehicles through novel services, which require a connection to some Internet-based source. This is used both to collect information on the external environment (e.g., traffic conditions, weather forecasts, vehicle position and orientation, often integrated within the on-board vehicle control systems), and to offer "infotainment" services. In doing so, the new devices that interact with the vehicle (e.g., modern infotainment systems, GSM, and Bluetooth connections)lead to an increased attack surface, which may enable an adversary to break into the vehicle itself, causing severe safety hazards. Recently, several researchers highlighted this aspect and successfully demonstrated attacks against different vehicles. 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., Smartphone 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.

II. SYSTEM ARCHITECTURE

The System architecture defines the whole control logic of vehicle system, it also demonstrates the how a smartphone can be securely communicate with vehicle system. The main part of our system is Electronic Control Unit[ECU]. A gateway Electronic Control Unit (ECU) is a central network interconnecting system to link various field buses in a vehicle. A gateway ECU is used to interconnect Controller Area Network (CAN) and Local Interconnect Network (LIN) field buses for Low Price Vehicles (LPVs). A gateway ECU is required for addressing the communication and network challenges in today's vehicles. Various existing commercial gateway ECU, and derive the specification for a gateway ECU suitable for LPVs.

The designed gateway ECU has been successfully validated using two other nodes– one node with LIN and another with CAN networks. Gateway ECU has optimal functionality and is cost effective solution for LPV segment.

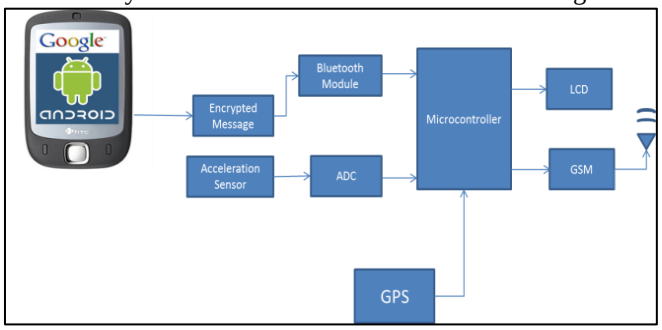

Fig. 1: System Overview

The trends in automotive networks and electronics show that the LPV needs to have only CAN and LIN networks in next one to two decades. In short, gateway ECU has optimal balance between functionality and cost, and is best suitable for LPVs. In now days, each new function was implemented as a standalone ECU, which is a sub-system composed of a microcontroller and a set of sensors and actuators. The evolution of automotive electronics since 1960 was tremendous starting from simple ignition control to Xby-wire technology by 2010.As the electronics increased, the Need for functions to be distributed over several ECUs and the need for information exchanges among them have been evolved. The different performance requirements throughout a vehicle, as well as competition among the companies in automotive industry, have led to the design of a large number of communication networks. A gateway is required to manage all these in vehicle networks and messages effectively. Network gateway is a device or a piece of software in a computer that forwards and routes data packets along networks.

Second part is to obtain the security for vehicle control system via Bluetooth. Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio in theism band 2.4 to 2.485 GH) from fixed and mobile devices, and building personal area networks(PANs). Invented by telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization. A master Bluetooth device can communicate with a maximum of seven devices in a piconet (an ad-hoc computer network using Bluetooth technology), though not all devices reach this maximum. The devices can

switch roles, by agreement, and the slave can become the master(for example, a headset initiating a connection to a phone necessarily begins as master—as initiator of the connection—but may subsequently operate as slave).

Bluetooth is a standard wire-replacement communications protocol primarily designed for low-power consumption, with a short range based on low-cost transceiver microchips in each device. Because the devices use a radio (broadcast) communications system, they do not have to be in visual line of sight of each other, however a quasi optical wireless path must be viable.

III. SECURITY ARCHITECTURE

Public Key Cryptography Using RSA for Encryption.

This algorithm RSA is used for public key encryption and it generate digital signature for encryption Algorithm works on a public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key. DSA is faster at signing than RSA, but RSA is faster during the verification phase, since authentication requires both phases the difference doesn't matter. As I said above DSA can only be used for authentication while RSA can be used for both authentication and to encrypt a message. However, SSH only uses the keys for authentication, so again the difference doesn't matter.

The RSA algorithm steps for key generation are

1) Generate two different primes p and q
2) Calculate the modulus n = p × q
3) Calculate the f(n) = (p - 1) × (q - 1)
4) Choose public exponent an integer e such that 1 < e < f(n) And gcd(f(n), e) = 1
5) Select the private exponent a value for d such that d = e-1mod f(n)
6) 6. Public Key = [e, n] 7. Private Key = [d, n].

A. Session Layer

The main goal of our system is to obtain security through radio interface against the attacks. In this layer first stage is to obtain trusted relation between vehicle and smartphone that is mobile device and ECU. Second stage defines the real time communication requirements are meet. It is implemented by using symmetric cryptography. Due to the constraints of the scenario (e.g., distribution of the mobile application through app stores, connectivity capabilities of the ECU), user do not assume any precomputed, static credentials or cryptographic keys on the mobile device, nor use a public-key infrastructure on the ECU vehicle's owner is able to initiate the first stage by enabling the one-off authorization procedure on the vehicle's side.

B. Wireless Connectivity Bluetooth

The connectivity to the outside world is implemented with the help of a radio interface module connected to the in-vehicle network; more precisely, a special ECU that we call in the following "Gateway ECU'. This ECU acts as a gateway between the internal network and the external world. In our work, we consider the Bluetooth standard as the wireless communication protocol, but the presented concept can be applied to other communication protocols as well. The Bluetooth protocol has a two-phase session setup: after the so-called pairing process, which allows the peers get to know each other and set up the network properties. the actual communication between the peers is enabled. During the pairing process, different security features can be applied for a secure network session depending on the Bluetooth version supported by the peers. For instance, the owner of each device must check that the information displayed on each peer (e.g., a random number) is consistent, or has to choose a (static) personal identification number (PIN), usually propagated out of band. Most of the current Bluetooth authentication schemes are driven by a human-based processing. Bluetooth v2.1 enforces the secure simple pairing (SSP) protocol which mitigates these security threats and takes into account the constrained resources as well as I/O capabilities of Bluetooth devices. The SSP provides confidentiality and authenticity unidirectional or mutual for all peers in a wireless personal-area network.

C. Security Requirements

The results of our analysis are the following security requirements, which describe the background of our security framework. First the execution of any data is based on its context. Second is no dependencies on proprietary subparts of an ECU and its interfaces towards other entities. Third is Cryptographic mechanism must be under the developer's authority and last fourth one is End-to-end confidentiality and authenticity between the application layer of a service user and an ECU.

D. Cryptographic Approach

Cryptographic schemes to protect the integrity and confidentiality of the data that they process. Algorithms such as the Advanced Encryption Standard (AES). Cryptology is the art of communicate in secure and usually secret form.

It can be divided into the science of making codes and algorithms, i.e., cryptography, and the science of breaking codes or extracting the meaning, i.e., cryptanalysis.

IV. SECURITY FEATURES

The Bluetooth specification defines security at the link level, allowing flexibility in the application security design. This flexibility, however, can come with a price if application designers do not take care in the design process. This link level security is also referred to as Baseband level security and employs authentication and encryption mechanisms. The Bluetooth system provides for three basic security services: Confidentiality addresses information compromise issues from eavesdropping .Authentication – addresses the issue of being able to confirm the authenticity of the identity of devices with whom we are communicating with, and Authorization – addresses the issue of whether the device in question is allowed to access the specific information requested.

V. EXPERIMENTAL RESULTS

I represent the experimental results and explain the feasibility of my proposed solution. In our experimental setting, the Gateway ECU is installed on an electric two-wheeled vehicle .The Gateway

ECU implements intelligent, range-extending algorithms. This security protocol has the two main working modes: pairing and payload exchange. Pairing is active when the mobile device is paired with the vehicle, after the typical Bluetooth pairing mechanism has taken place. In pairing mode, I measured the performance of the asymmetric cryptography both on the mobile device and on the Gateway ECU, and the performance of the key-generation routine (on the mobile device). The payload exchange mode activates when the AES key are actually exchanged, and encrypted or decryption takes place. In this mode, I analyzed the performance of the decryption (on the mobile device) and the performance of the encryption ECU). The payload consists of 64 bytes of data, which includes a padding scheme for supporting arbitrary payload size.

VI. CONCLUSION

I analyzed the discussed the security issues related to modern, smartphone-based automotive embedded architectures. To estimate such issues, I designed, implemented and evaluated a security layer that protects from an attacker that has full control over the Bluetooth wireless link between the mobile device and the vehicle.

REFERENCES

[1] Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W.Xu, M.Gruteser, W.Trappe, and I. Seskar, "Security and privacy vulnerabilities of in car wireless networks: A tire pressure monitoring system case study," in Proc.19th USENIX Conf. Security, Berkeley, CA, USA, 2010, pp. 21 –21.
[2] A. Bogdanov et al, "PRESENT-An ultra-lightweight block cipher," in Proc. Int. Workshop Cryptography Hardware Embed. Syst. (CHES),2007, pp. 450–466, ser. LNCS, no. 4727 Springer.
[3] F. Stajano, Security for Ubiquitous Computing. Hoboken, NJ, USA: Wile, 2002.
[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, "Smartphone- based vehicle-to-driver/environment interaction system for motorcycles," IEEE Embed. Systems Lett., vol. 2, no. 2, pp. 39–42, Jun. 2010.
[6] A. Dardanelli,M. Tanelli, and S.M. Savaresi,"Active energy management of electric vehicles with cartographic data," presented at the 2012 IEEE Int. Electr. Veh. Conf., 2012.
[7] Microchip Technology Inc., 16-bit dsPIC® NIST Special Publication 800-121 Revision 1,Guide to Bluetooth Security: Recommendations of the National Institue of Standards and Technology 2012.
[8] C. Hager and S. Midkiff, "Demonstrating vulnerabilities in Bluetooth security," in Proc. IEEE Global Telecommun. Conf. (GLOBECOM'03), 2003, vol. 3, pp. 1420–1424.

