A Review Of Bluetooth Security In The Automotive Environment

Article · July 2004

DOI: 10.1049/cp:20040594

Martin Glavin
National University of Ireland, Galway
134 PUBLICATIONS **1,504** CITATIONS
SEE PROFILE

F. Morgan
National University of Ireland, Galway
64 PUBLICATIONS **527** CITATIONS
SEE PROFILE

A Review Of Bluetooth Security In The Automotive Environment

Pauric Doherty, Alan Molloy, Martin Glavin, Fearghal Morgan

Department Of Electronic Engineering,
National University Of Ireland, Galway
Galway, IRELAND
Email: {pauric.doherty, alan.molloy, martin.glavin, fearghal.morgan} @nuigalway.ie

Abstract – **This paper outlines the security issues automotive designers must consider when integrating Bluetooth into existing in-vehicle networks like CAN, TTCAN, and MOST. It also proposes possible solutions to secure the sensitive information within an in-vehicle network, allowing Bluetooth to be a securely integrated wireless automotive technology of the future. Bluetooth has become the de-facto standard for wireless short-range communication within the PDA and mobile phone sector. Automotive designers have begun implementing audio gateways as factory fitted components within today's top-of-the-range cars. Several security issues within Bluetooth have been highlighted recently within the mobile phone sector and automotive designers must protect the in-vehicle networks from both identified and possible future security risks.**

Keywords – **Bluetooth, Security, In-Vehicle Networks, CAN, TTCAN, MOST, Automotive Security**

I. INTRODUCTION

Bluetooth [1] has firmly established itself in the telecommunication and personal area network sector. Increased use of in-car mobile phones, has led to integration of Bluetooth technology into car entertainment/multimedia audio systems to replace the use of traditional wired car kits. A recent study from ABI Research [2], estimates that the level of factory fitted Bluetooth hardware will increase from 1% of the total cars manufactured in 2004 to 16% in 2008. The Controller Area Network (CAN) [3] has been used in the automotive industry since the mid-eighties, and has become the standard in-vehicle network (IVN) to connect engine management electronics as well as body electronics and entertainment control units. Time Triggered Controller Area Network (TTCAN) [4] is an optimization of CAN which allows time critical information to be successfully delivered on a CAN network within specific time constraints. This system is useful for emergency vehicle systems e.g. brake sensors and traction control, to provide real-time responses. Other IVN's like CANopen [5] and SAE J1939 [6] also exist. CANopen is a Higher Level Protocol (HLP) that runs on a CAN network. CANopen was designed for motion-oriented machine control networks, such as material handling systems in an industrial setting. CAN is now used in various fields, such as medical equipment, off-road vehicles, maritime electronics and public transportation. Media Oriented Systems Transport (MOST) [7] is another IVN designed to connect complex electronic devices like Global Positioning Systems (GPS), radios, video displays and audio amplifiers.

While the integration of these technologies will bring many benefits, it may also bring some danger. Because of the diversity of IVN's and the diversity of information transmitted on these networks, both critical control and entertainment information should be protected from malicious network attacks. With the addition of Bluetooth to the automotive environment, the traditional security of these wired networks could be compromised. We illustrate some of the possible security issues that arise with the use of Bluetooth [8] in an automotive environment and propose some solutions to protect the extremely important information contained within an automotive network. The Networking technologies being analysed are outlined in Section II of this paper; section III goes on to discuss the security issues within Bluetooth technology. Section IV outlines possible solutions to secure the Bluetooth and internal vehicle networks.

II NETWORKING TECHNOLOGY

a) Controller Area Network (CAN)

CAN is a one of the most common networks in the automotive and industrial settings. The CAN standard originally developed by Bosch in the 1980's was designed as a serial 2-wire transmission network that could support speeds of up to 1 Mbps and have a maximum distance of about 1km at a speed of 50 kbps. CAN is a hot plug-and-play system that allows intelligent nodes to connect and disconnect to and from a live network. CAN is an inexpensive system comprising a pair of shielded wires, and a collection of CAN transceiver and controller chips. For example, information relating to an automobiles ignition system, immobiliser and central locking, as well as entertainment information etc. can all easily exist within a standard CAN network.

CAN was designed as a multi-master bus technology, where every node can request the bus simultaneously. A controller area network does not identify nodes on the network, instead CAN prioritises messages to be transmitted on the bus. This allows critical data to be prioritised for urgent transmission from any set of nodes. A CAN system can be subdivided into individual autonomous sub-systems. For example, a brake controller need only be concerned with messages relating to the brake sensors & actuators and can therefore ignore all other messages. This effectively partitions the Engine Management Unit (EMU) into individual ECU (Electronic Control Units), and thus simplifies the programming required to control every mechanism within the EMU. Today, the trend is towards a parent EMU, connecting all distributed control elements, the ECU's, to considerably reduce EMU complexity and cabling distances.

b) Time Triggered CAN (TTCAN)

TTCAN is based on the CAN (Controller Area Network) data link layer. It may use standardised CAN physical layers, and high-speed transceivers or fault-tolerant low-speed transceivers as specified in [3]. TTCAN provides mechanisms to schedule CAN messages as being both time-triggered and event-triggered. This allows CAN-based networks to operate closed loop control systems and increase the real-time performance in CAN-based in-vehicle networks. Systems like the brake controller and actuator systems require time triggered responses like those offered by TTCAN.

c) Media Orientated Systems Transport (MOST)

MOST is a fibre optic network optimised for automotive applications. MOST is a low overhead, low cost interface for simple devices such as microphones and speakers connected to intelligent devices, e.g. GPS devices and video displays. MOST allows more intelligent devices to automatically determine the features and functions provided by all other devices on the network. These devices can then establish sophisticated control mechanisms to take away distractions from the driver of the car as different subsystems try to communicate information to the driver.

d) Bluetooth

Bluetooth is a wireless communication technology designed as a short-range, low power, low cost technology. It is targeted at personal area networking and cable replacement. Bluetooth operates in the 2.4 GHz ISM (Industrial, Scientific and Medical) band and competes with other technologies like Wireless Local Area Network (WLAN), Digital Enhanced Cordless Telecommunications (DECT) cordless telephones, wireless (2.4GHz) speakers and cameras as well as other short-range network technologies like Home RF, ZigBee and Ultra Wide Band (UWB)

Bluetooth uses Fast Frequency Hopping Spread Spectrum (FHSS) and operates with 1600 hops/second over a maximum of 79 channels to avoid as much interference as possible. Bluetooth therefore limits the effect of other 2.4GHz ISM technologies on its transmissions. Bluetooth also uses variable power rates to limit interference. Bluetooth power levels can be adapted to ranges of 1, 10, or 100 metres depending on the application domain. The 1-metre band provides an ideal range for personal area networking (PAN) applications, connecting devices such as a PDA, cell phone, and wireless headset. The 10 and 100 metre ranges are ideal for office environments when required to connect to a Bluetooth enabled PC, or Bluetooth access point. Bluetooth has a maximum theoretical connection speed of 1 Mb/s but with packet formatting and overhead it has a one-directional maximum speed of 723.2 kbps has a bi-directional bit rate of 433 kbps.

Bluetooth allows a maximum of one master and seven active slaves to communicate together in one network called a piconet. A piconet can also support 256 'parked' slaves that maintain contact with the master but do not participate actively in network communication. These slaves can become active members if requested by the master when an available active slave resource becomes available. This allows a large number of devices to communicate successfully within a given range. Bluetooth also supports communication between piconets to form what is known as a scatternet. In scatternet formation, a master in one piconet can be a slave in another piconet. It will then split its network time between both networks.

In 1998, five companies, Ericsson, IBM, Intel, Nokia and Toshiba came together to form the Bluetooth Special Interest Group (SIG) [1]. The SIG promotes the Bluetooth standard and is responsible for its development and profile definitions to allow interoperability between Bluetooth devices. Bluetooth supports both voice and data so it is a likely contender to satisfy most personal device connection requirements. Bluetooth's application targets initially were the mobile telecommunications industry and personal computer environments. However, Bluetooth has since been adopted by the automotive, health care, home automation, and toy industries. The Bluetooth Automotive Group is developing profiles that can be used to aid the integration of Bluetooth into vehicles of the future. A currently implemented profile is the Security Identity Module (SIM) Access Profile. This is used to synchronise a mobile phone's address book with the in-vehicle, Bluetooth-enabled computer so that the driver can easily select a contact to call with minimal distraction to their driving. There are many profiles currently under investigation by the SIG automotive group, which will make Bluetooth a standard entity within the automotive environment.

III BLUETOOTH SECURITY STRUCTURE

Bluetooth has several built-in security features to secure a Bluetooth network from unauthorised access. To successfully set up two devices to communicate, a pairing procedure exchanges link keys to setup a secure connection. After successfully pairing the devices, they can then communicate freely. This Bluetooth security feature allows only known trusted parties to connect to these devices.

The Bluetooth Link level is where most of the security mechanisms are defined. A simplified Bluetooth stack diagram is illustrated in figure 1 for reference. The Bluetooth frequency hopping sequence, specified in the RF layer also provides some security, as the hop sequence must be known in order to track communications within any specific piconet. The Bluetooth link level, i.e. Logical Link Control Access Protocol (L2CAP) mechanisms includes authentication, pairing and encryption. There are four entities used for maintaining the security of a Bluetooth device at the link level.

- A 48 bit unique Bluetooth device address
- A 128 bit random private authentication key
- An 8 – 128 bit private encryption key, PIN (Personal Identification Module)
- A 128 bit random number which changes frequently and is 128 bits in length

Bluetooth authentication uses a challenge-response scheme in which a claimant's knowledge of a secret key (or PIN) is checked through a 2-move protocol using symmetric secret keys. The latter implies that a correct claimant/verifier pair shares the same secret key (PIN). Encryption can then be applied to the link and can be either one-way or two-way depending on the participating devices capabilities. The current version of the Bluetooth Specification V1.2 has greatly enhanced some of the possible attacks on the PIN function. In earlier Bluetooth versions it was possible to continually try a set of PIN's until the correct one was found and access was granted. In Bluetooth version 1.2 this issue has been rectified by an exponential back-off algorithm that only allows retries from the same Bluetooth address after an exponentially growing waiting period.

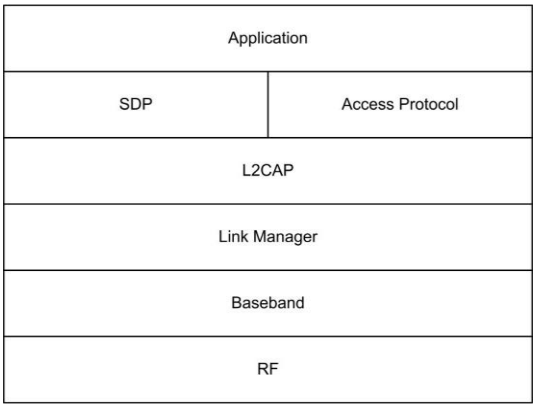

Figure 1: A simplified Bluetooth stack.

Because Bluetooth is an ad-hoc network, certain parameters must be available without any security, as there are no known properties of any available device within range. Bluetooth caters for this using the Bluetooth Generic Access Profile (GAP). The GAP has divided security into three modes

- Mode 1: No Security
- Mode 2: Application/Service based (using L2CAP)
- Mode 3: Link-layer (PIN authentication/ MAC (Media Access Control) address security/encryption)

In Security Mode 3 the Bluetooth device initiates security procedures before any L2CAP channel is established whereas security mode 2 does not. Bluetooth also defines separate security levels for devices and services.

For Bluetooth devices, there are two levels of security

- Trusted – unrestricted access to all services
- Un-trusted – restricted access to services

For a Bluetooth devices' services there are three security levels defined

- Requiring authorization and authentication
- Requiring authentication only
- Open to all devices

A security flaw currently not addressed by the Bluetooth standard relates to device discoverability. Bluetooth defines two modes of discoverability.

- Discoverable Mode, allowing a Bluetooth device to respond to a general inquiry from another Bluetooth device.
- Non-Discoverable Mode restricting a device from responding to an inquiry.

Devices that are marked non-discoverable do not respond to general inquiries but do respond to direct name and service inquiry requests. Once the address of the Bluetooth device is known, the device contacted will give information such as class, name and clock-offset. An attacker could obtain device information by searching each MAC address, and sending an HCI_Remote_Name_Request [9] command. Any addressed device that is in non-discoverable mode would return its name to the calling device. [10].

Several other attacks on Bluetooth have been identified recently and are described in Section IV. These attacks are all identified on mobile phones, e.g. Bluejacking, BlueSnarfing, and one referred to as a backdoor attack. Other lower level attacks on the Bluetooth radio layers also exist e.g. cipher attacks, however these generally require the use of specialised equipment.

IV BLUETOOTH ATTACKS AND SOLUTIONS

a) Bluetooth Discoverability

The issue of Bluetooth discoverability cannot be fixed using a software-only solution. Discoverability and responses to low level requests are all predefined within the radio baseband level. Discoverability is not a severe breach of security but it can provide information that would enable attacks against particular services. All higher-level Bluetooth services must be protected by software in order to maintain a high level of wireless security.

b) Cipher Attack

Cipher Attacks are attacks on the information that is transmitted wirelessly between devices. It is not possible to detect these attacks from within a Bluetooth device. The Cipher Attack is an attack in which an attacker can break the security of the Bluetooth communication link cipher, requiring 2^{100} bit operations as put forward by M. Saarinen [11].

The weakness is in the 128-bit key, which is fundamentally to do with the SAFER+ (Secure And Fast Encryption Routine [12]) cipher algorithm. The SAFER+ algorithm is a block cipher algorithm, but it has been adapted to a stream cipher algorithm in the Bluetooth specification. SAFER+ is based on a 128-bit key implementation of the SAFER algorithm. Other stronger algorithms exist, such as Triple-DES [13], which are based on the public key encryption principle. However their greater complexity requires more battery and processing power to compute. This goes against two of the three fundamental design goals of Bluetooth, i.e. low power, low cost and small size.

The stream cipher generated by the SAFER+ algorithm with a random 128-bit key has been previously considered adequate to an ad-hoc based network like Bluetooth. The Bluetooth SIG could consider the implementation of a stronger ciphering algorithm to counteract the possibility of cipher attacks using today's more powerful analysing equipment.

c) Bluejacking

'Bluejacking' is a term used to describe the sending of an anonymous message to a Bluetooth enabled device. It is primarily applied to mobile phones.

In a mobile phone, it is possible to send a contact (v-card) or a note to another Bluetooth enabled phone without the receiver knowing from whom the message came. This is as a result of how the information is sent. It is sent as a 'fire-and-forget' data packet with no information regarding the sender or user. This allows people to advertise products and services to users' mobile phones without traceability, which gives rise to the possible transmission of virus type data into systems without adequate protection.

Bluejacking was originally a non-malicious security breach but recently embedded viruses have also begun to appear. The Bluetooth standard, allows a Bluetooth enabled device to send an anonymous message to any other Bluetooth device in range. Automotive designers must block or ignore these unidentified messages and must protect the sensitive information contained within the IVN's from any software attacks. Bluejacking, and the interest expressed in it as an advertising medium has led to the discovery of another Bluetooth security issue called ‘BlueSnarfing’.

d) BlueSnarfing

BlueSnarfing is where an attacker targets specific makes of mobile phones in order to obtain private information e.g. calendar, IMEI (International Mobile Equipment Identification) number and inbox information.

BlueSnarfing has grown from the Bluejacking attack. In affect BlueSnarfing reverses the scenario of Bluejacking by instructing a Bluetooth device to retrieve as well as transmit, a mobile phone's address book and calendar without leaving any trace of the intrusion. This is only possible if the device is in "discoverable" or "visible" mode. However, there are tools available that allow even this simple safety net to be bypassed.

BlueSnarfing is common to mobile phone software, which leaves sensitive memory open to intrusion. Automotive designers must secure all memory access and not allow this breach when integrating Bluetooth with the already existing IVN’s of an automotive. Information stored within an ECU or EMU can be safety critical, e.g. maximum or minimum mechanical tolerance values. The security of this information is fundamental to the safe operation of the vehicle.

e) Backdoor Attack

The backdoor attack is an intrusion into a Bluetooth device when the attacking device remains untraceable.

The BackDoor attack involves establishing a trust relationship through the "pairing" mechanism, but ensuring that it no longer appears in the target's register of paired devices. In this way, unless the owner is actually observing their device at the precise moment at which a connection is established, they are unlikely to notice anything untoward, and the attacker may be free to continue to use any resource granted by that trusted relationship.

The Backdoor attack is possibly the most dangerous attack discovered to date, as the attacking device is completely untraceable. One method described in [10] is a form of defense from the backdoor attack in which bonding information checks should be implemented within the bonding and the higher-level security software. This would reveal devices that are trying to establish a trusted bond, and would perform authentication by always notifying the device user to input the secret PIN. It is good practice to check the “paired devices” information regularly in order to detect a malicious trusted device. Automotive designers should always alert the vehicle driver to any bonds or connections made to the cars Bluetooth enabled system.

f) User Authentication

Bluetooth user authentication is another scenario where the presence of a Bluetooth link introduces insecurity. The Bluetooth protocol is used to authenticate the device and not the actual user of that device. Consider a device used to control or update software features in a car. The device’s integrity is potentially undermined by the fact that Bluetooth security checks are designed to authenticate the device and it’s permissions and does not consider the identity of the user. So while the Bluetooth enabled automobile may provide some intelligent wireless functionality, it is no different in terms of security than the key to the vehicle in the wrong hands.

Bluetooth user authentication gives rise to authentication-based security threats. For example, an automobile equipped with a non secured Bluetooth node could potentially allow, not only a passenger to gain access to the vehicle’s multimedia devices, but also to engine management information or other information existing within the IVN’s.

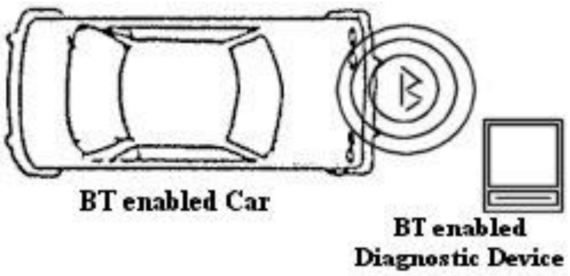

Figure 2: Bluetooth Diagnostic Device

To protect against this, service engineers could use a secure Bluetooth method to update software components with the EMU or the ECU’s. A passenger should never gain access to the information within the IVN. Automotive designers must implement higher-level security measures in order to protect the IVN’s from both an unintentional passenger attack and a malicious external user attack. This security software would exist as a secure embedded software package that would limit the information retrievable using higher level and more secure PIN type mechanisms.

One solution would be to limit access through software using user-authentication as well as device authentication. A three-tier hierarchy of access classes would cover most possible scenarios such as,

- Automobile updates by factory engineers using factory enabled Bluetooth devices

- Service engineer access for engine modifications and alterations using Bluetooth enabled diagnostic systems See Figure 2.
- User access for temperature control, multimedia applications and in-car entertainment using Bluetooth enabled PDA's, smart phones or laptops.

User classes could be factory programmed. The Bluetooth SIG could define a factory-level class that would permit access to all IVN information, and define a class that would permit service engineers to perform post production authorised updates and adjustments to a vehicle. This class-based authentication should also be combined with a secure PIN type user authentication that would authenticate both correct device and correct user, should the device ever be used by an un authorized person. Another alternative would be to perform a bonding procedure within the factory that would authenticate the factory-based device to allow full control of IVN information. This would be performed either using hard-coded in-factory bonding or secure initial bonding performed within a 'clean' radio-proof environment.

Service engineer access would be similar to factory engineer's access. However, a hard coded relationship would limit access to a single service engineer. A diagnostic machine Bluetooth class could also be established and issued to recognized service centers. This would allow device authentication from the diagnostic machine, combined with a PIN authentication known by the service engineer, to grant access to update and adjust certain information within the IVN.

All of the above schemes use a combination of device authentication at a low level as well as higher-level user authentication. Device authentication can be performed based on a unique set of Bluetooth MAC addresses from specific vendors. This would allow preprogrammed trust relationships, known only to the automotive manufacturers. User authentication could be performed based on a more complex version of the PIN example and would limit access to specific users and would create a much securer Bluetooth system.

V CONCLUSIONS

This paper has discussed some of the IVN's currently implemented in today's automobiles and the type of information transmitted around these networks. We have described some of the Bluetooth security measures already in place within the Bluetooth specification. Some telecommunication sector Bluetooth implementations have exhibited fundamental flaws discovered and highlighted by common users. Bluetooth's security may be considered adequate for small ad-hoc networks, such as a connecting a PDA to a mobile phone, but for larger ad-hoc networks, carrying sensitive information like in-vehicle messages relating to ignition systems, lock systems and immobiliser systems, Bluetooth security is insufficient on its own. Even after the basic Bluetooth security issues have been corrected, more sophisticated security methods need to be implemented on the upper levels of software that run on the Bluetooth stack. The security specification only considers Bluetooth device authentication and not the more functional, user authentication. Security must be built above the defined Bluetooth security measures. This includes the use of better authentication systems using possible distributed secret PIN schemes, predefined trust relationships, defined and known only by the automotive designers and engineers, allowing Bluetooth to be a securely integrated wireless automotive technology of the future.

ACKNOWLEDGEMENTS

The authors acknowledge the support of Enterprise Ireland under the Innovation Partnership's scheme, and Connaught Electronics, CEL.

REFERENCES

[1] Bluetooth SIG, The Official Bluetooth® Wireless Info Site. http://www.bluetooth.com/

[2] ABI Research Study, "Automotive Wireless Networks", Published 2003

[3] ISO-11898 (1993). Road Vehicle – Interchange of Digital Information – Controller Area Network (CAN) for High-Speed Communications. ISO.

[4] TTCAN Time Triggered Controller Area Network ISO 11898-1: 2003, "Road vehicles -- Controller area network (CAN) -- Part 1: Data link layer and physical signalling"

[5] CANOpen CiA DS 301: "CANopen Appliction Layer and Communication Profile"

[6] SAE J1939, "SAE 1939 Standards Collection"

[7] MOST® Media Orientated Systems Transport, "MOST Framework: Most Cooperation"

[8] M. Jakobsson, S Wetzel, "Security Weaknesses in Bluetooth". RSA Conference 2001.

[9] HCI_Remote_Name_Request() - Specification of The Bluetooth System, V1.2 http://www.bluetooth.org (Section 7.1.19, pg 560)

[10] Ollie Whitehouse, October 2003, War Nibbling: Bluetooth Insecurity, @Stake Research Report

[11] “Cryptography-Research Digest #890, Volume #1”, Markku-Juhani O. Saarinen, University of Finland

[12] SAFER+ algorithm J. L. Massey, “On the Optimality of SAFER+ Diffusion”, Second Advanced Encryption Standard Candidate Conference (AES2), Rome, Italy, March 22-23,

[13] Triple-DES algorithm ANSI X9.17, "American National Standard, Financial Institution Key Management (Wholesale)", 1985. ISO/IEC 8732:1987, "Banking - Key Management (Wholesale)".