Vehicular Communications 9 (2017) 8–18

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

Towards a systematic security evaluation of the automotive Bluetooth interface

Madeline Cheah [a,*], Siraj A. Shaikh [a], Olivier Haas [a], Alastair Ruddle [b]

[a] Centre for Mobility and Transport Research, Coventry University, Coventry, UK
[b] Future Transport Technologies, HORIBA MIRA, Nuneaton, UK

ARTICLE INFO

Article history:
Received 19 October 2016
Received in revised form 22 December 2016
Accepted 23 February 2017
Available online 1 March 2017

Keywords:
Automotive security
Operational and field testing
Threat model
Wireless security
Bluetooth

ABSTRACT

The modern vehicle requires connectivity in order to enable and enhance comfort and convenience features so desired by customers. This connectivity however also allows the possibility that an external attacker may compromise the security (and therefore the safety) of the vehicle. In order to answer this problem, we propose a framework for a systematic method of security testing for automotive Bluetooth interfaces and implement a proof-of-concept tool to carry out testing on vehicles using this framework. From our findings, we conclude that the method enabled us to enumerate multiple weaknesses and that by continuing to extend the work, we would discover more.

1. Introduction

The modern vehicular system is opening up, with wireless interfaces and services implemented for customer comfort and convenience. The introduction of these interfaces means that malicious external influences are now possible, as demonstrated by seminal experimental analyses on individual vehicles [11,29,38]. These influences can be construed as “cyberattacks” or “hacks”, which have come to mean an attempt to manipulate an insecure system to cause negative consequences such as harm, damage or destruction. In cyber-physical systems – defined as a system where computational and physical processes are integrated [30] – the harm may not be limited to logical assets (such as personal data theft or loss) but could conceivably also cause physical harm, such as is the case with a vehicle. Protection and defence mechanisms are therefore necessary in order to mitigate or nullify the consequences of an attack. Several challenges stand in the way of implementation although experimental analyses on a vehicle’s possible entry points have been performed. The primary concern here is that the placement and details of countermeasures requires knowledge as to where, in the system, security vulnerabilities or weaknesses exist in the first place, and what its nature is.

Bluetooth is a pervasive interface and was therefore chosen for this study because of the potential negative impact should it be compromised. There have been estimates that vehicles with a Bluetooth interface number at nearly nine million currently, with a forecast of 21 million vehicles to have Bluetooth by 2018 [19]. Market growth for information systems, of which Bluetooth is a major enabler, is anticipated to grow to $1.6 billion by 2020, with at least a 40% rise in automotive wireless technology [2]. Bluetooth is a low power, short range wireless communication technology, capable of forming ad-hoc networks. Security issues with this technology are well documented [15].

The main contribution of the paper is a systematic method of evaluating the security of the automotive Bluetooth interface, something that has not yet been performed. This is needed to maximise the effectiveness of the security evaluation and is implemented through a proof-of-concept tool based on attack tree modelling and penetration testing methods. This tool was then used to evaluate the Bluetooth interface on a range of built-in automotive infotainment systems.

The rest of this paper is structured as follows: Section 2 discusses related work, whilst Section 3 looks at Bluetooth security, both generally and specific to the automotive domain. We describe our methodology in Section 4 and present our proof-of-concept tool development and validation in Section 5. We discuss our findings in Section 6 and consider future directions in Section 7.

* Corresponding author.
E-mail addresses: cheahh2@uni.coventry.ac.uk (M. Cheah), siraj.shaikh@coventry.ac.uk (S.A. Shaikh), o.haas@coventry.ac.uk (O. Haas), alastair.ruddle@horiba-mira.com (A. Ruddle).

http://dx.doi.org/10.1016/j.vehcom.2017.02.008
2214-2096/

2. Related work

There are several challenges with securing wireless interfaces in vehicles. Any security mechanism will require additional processing overhead, and on the hardware level, has ramifications in provision of energy and in physical assembly and design, such as placement of additional wiring. Even should such concerns be addressed, well-established defences at software level such as the use of cryptography, firewalls and intrusion detection systems (IDS) cannot be implemented without considerable change in architecture due to the use of sufficiently different protocols and topologies within the automotive domain. Even post-release, patches, unless performed over-the-air, for discovered vulnerabilities are difficult to apply once units are sold.

All of the above is dependent on acquiring knowledge and information regarding existing vulnerabilities and holds true not just of Bluetooth attacks, but also generally. Some exploits have already been demonstrated in literature on the vehicle as a whole [11,29] or on various subsystems [22,42,46,51,52], some are reported through "hacker" conferences such as Black Hat [38] whilst still others can be inferred through technological trends.

Although these papers show an impressive range of experimentation and an in-depth knowledge of the target system, they have not mapped out a process or taxonomised their findings. Furthermore, information on the practical aspect of security testing is scarce; because automotive systems are complex with many different technologies integrated into the single vehicle, many papers dealing with experimental analysis by necessity limit their scope to a single interface, protocol or technology which are extremely diverse in nature. Of the papers that involve practical security analysis on vehicles, only one details attacks on an automotive system (at a high level) via Bluetooth [11], although many agree that Bluetooth is a viable entry point for an attacker [42,56,14,36,22,25]. Despite the paucity of information, from the number and variety of reported threats, vulnerabilities and exploits, it is clear that a systematic description of the problem is required.

A systematic security evaluation method has many advantages. There is a disparity between what an attacker must find in order to exploit the system (potentially just one vulnerability) and the number of flaws a defender would have to safeguard in order to protect the system (as many as possible). An ad-hoc approach to finding vulnerabilities – which by implication means a subjective prioritisation of what and where to test [32] – potentially results in flaws being overlooked. A methodical approach increases the likelihood of determining flaws, thereby mitigating this problem [48]. Systematic analyses can also be supported by a variety of tools and utilities, for example, through the use of graph-based modelling, and in this case also means that, not only is the final result documented, but all the details that led to the system compromise [13].

Systematic evaluations have been described in model-based testing studies such as [34] and security specific model-based testing [48] is an active field of research. These have inspired our method of systematism, in particular the use of attack trees. However, although this approach provides rigour and confidence, we have no trustworthy model from which to generate tests. This is because the Bluetooth specification is embedded in other systems (such as the embedded system's operating system and other firmware) for which we would need to include to provide a complete model representation of the implementation and for which there is very little information. Furthermore, whilst model-based security testing may provide coverage of security weaknesses in a system, applications thereof (e.g. [23]) have required that models be available or pre-built in order to formally examine. The barrier to using such methods is as above, that the information required to do so is not available, both due to commercial confidentiality and the obscurity of subcomponents within the system (many of which are third party). This also precludes other methods of enabling systematic evaluation such as attack graphs, for which formal model checking could be performed.

Automotive specific systematic methods of evaluation are described in the "E-safety vehicle intrusion protected applications" (EVITA) project [17]. The EVITA project ultimately aims to provide a secure architecture for automotive on-board networks and evaluates the realisation of this using two "views" the first of which is a magnified view. Attack tree modelling (discussed further in Section 4.2) is used to support these processes, although the end goal of verifying whether assets are really protected somewhat differs from the aim of this paper which is to identify unprotected assets through a methodical evaluation. The second view, called a compositional view, deals with looking at attack categories (and related security guarantees) to ensure that omitted attacks are minimised. The latter is a valuable exercise, however, where a system already exists with unknown properties (and therefore unknown guarantees) as is the case with this paper, the ability to analyse coverage in such a way is limited. Methodical evaluation methods are also presented in the J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems [47], drawing from EVITA, although information provided has been examples thereof rather than application to a system.

3. Bluetooth

Bluetooth is more complex than most wireless standards, due in part to the Frequency Hopping Spread Spectrum (FHSS) mechanism designed to reduce narrowband interference. Channel hopping occurs once every 625 μs and in some cases also uses Adaptive Frequency Hopping (AFH), whereby channels that can cause interference are avoided [8]. Data whitening is also performed by XOR-ing each packet with a pseudorandom sequence, in order to facilitate signal transmission.

Adding to the complexity is also the fact that not all Bluetooth implementations are identical; Bluetooth standards specify various service profiles that could be used in order to customise the technology, whether that be to enable "hands-free" communication, allow file transfers or grant access to phonebooks and messages [4]. Profiles consist of information regarding dependencies, user interface details and specific protocols required by the service. This information is vital in detailing what the device is capable of doing, and, from an adversary's point of view, also gives information on potential weaknesses. The vast majority of services embodied by these profiles communicate via the Radio Frequency Communications (RFCOMM) and Logical Link Control and Adaptation Protocol (L2CAP) layers and, where there is an open channel, could be used to send or extract data. The number and nature of accessible ports on a remote device depend on the services being offered along with whether a user is paired and connected.

The pairing process, essentially the method by which two or more devices synchronise their "hops", is well documented and in the interest of brevity is only outlined here. A complete introduction may be found in [8]. The pairing process uses one of two mechanisms:

- **Legacy pairing:** This has been superseded by Simple Secure Pairing (SSP) in the Bluetooth 2.1 specification, although many older platforms still use this mechanism. The pairing exchange involves the derivation of a link key from the Bluetooth address, the PIN and a random number. This link key is then stored locally and used in subsequent authentication and encryption processes. The primary danger to this mechanism is the fact that the PIN is the only aspect providing entropy, ex-