White Paper

Securing Communication in Next-Generation Vehicles

Key Elements for an Automotive Communication Security Test Regime

TABLE OF CONTENTS

Introduction

In comparison with the earliest automobiles, today's vehicles are incredibly sophisticated—relying on a range of in-vehicle networks (IVNs) to support a host of electronic and diagnostic functions.

Currently, common IVNs include:

- **CAN (Controller Area Network) Bus**—Used to connect various electronic control units (ECUs) that control everything from the engine to airbags and windows
- **LIN (Local Interconnect Network)**—A low cost, but limited, alternative to CAN bus
- **MOST (Media Orientated Systems Transport)**—Used to deliver in-vehicle media
- **FlexRay**—Often supports "x-by-wire" capabilities, delivering the necessary speed and reliability

Modern vehicles are also increasingly connected to the world around them. Europe's new eCall system will see cars automatically send airbag, impact sensor and positioning information to the emergency services in the event of a crash, while vehicles already take advantage of cellular networks to relay telematics information, and support Advanced Driver Assistance Systems (ADAS)—for example, BMW's ConnectedDrive.

In the next few years, this level of sophistication is only going to grow. But as our vehicles become smarter, more sophisticated, and better connected, they will also become subject to new, potentially life-threatening security risks.

In this white paper, Spirent explores how current trends in IVN design and vehicle connectivity are set to impact security, and offers recommendations for those teams working to protect next-generation automotive communications—from securing systems, to testing security performance.

We hope you will find this paper useful. If you have any specific challenges or questions, or would like more detailed information on any of the topics covered, don't hesitate to get in touch.

Security Challenges for Automotive Communication

The security challenge can be broken down into three key areas.

Wireless access—Placing a Wi-Fi hotspot within a vehicle effectively opens it up to the Internet, and potentially exposes its systems to a huge variety of possible attacks through the local Wi-Fi.

Navigation—Satellite navigation systems not only come with their own set of security vulnerabilities (such as signal jamming and spoofing) but are increasingly connected to other crucial systems.

In-vehicle networks—IVNs are vulnerable to attack through maintenance interfaces, and through their connection to a vehicle's wireless and cellular systems.

Over the last few years, the potential for hacking attacks on automobiles has regularly made headlines.

In 2010 and 2011 computer scientists from the University of California and the University of Washington published papers describing methods of attack that utilise everything from Bluetooth and wireless systems to diagnostics ports and media players[1]. According to the research, such access points can be exploited to gain control of an alarming range of critical systems—from a vehicle's lights and locks, to its engine and brakes.

Recent Def Con hacking conferences[2] have also seen a number of talks given on methods of exploiting particular vehicle vulnerabilities.

Despite this, few proven hacking attacks have taken place. Two likely explanations are:

INVs have been comparatively hard to target. Although it's possible to hack into a vehicle's CAN bus or FlexRay network, it requires specialist expertise—beyond a casual hacker's skillset.

Wireless traffic has been routed through secure, Virtual Private Networks. Today, wireless is mainly used by infotainment systems and ADAS. When such systems connect to the Internet, it's through the OEM's own data centre and Virtual Private Network (VPN)—ensuring the risk of a successful, Internet-based attack is relatively small.

1 Comprehensive Experimental Analyses of Automotive Attack Surfaces http://www.autosec.org/pubs/cars-usenixsec2011.pdf
2 https://www.defcon.org/

New Challenges on the Horizon

The coming years, however, hold new and significant security challenges for those working to safeguard automotive communication, brand reputation, and driver and passenger safety.

The Advent of Ethernet/IP

One important development is the advent of automotive Ethernet/IP. With BroadR-Reach® now effectively established as an industry standard for the technology, and significant performance and cost benefits to be gained, many in automotive R&D are now working to exploit the technology's potential in IVN applications.

Unlike CAN bus and FlexRay, however, Ethernet/IP is well known to hackers—indeed, anyone can attack an Ethernet/IP network using tools readily available on the Internet.

Increasingly 'easy' access

As noted above, as vehicles become more connected, they also risk becoming easier to access. Potential points of attack include:

- **Maintenance interfaces**—While it is possible to attack traditional IVNs directly through a vehicle's maintenance interface, a shift to Ethernet/IP networks would make such attacks much easier for anyone with a laptop and basic hacking skills to execute.
- **Wi-Fi access points**—Wi-Fi access points, if inadequately secured, offer hackers the chance to attack systems from anywhere within 10-15m of the vehicle.
- **Cellular modems**—Hackers can call a car's cellular modem, and use audio signals to launch an attack.
- **Car2x Wi-Fi**—Frequently used to warn drivers approaching roadworks, Car2x Wi-Fi (based on the 802.11p standard) affords would-be attackers yet another way into a vehicle's critical systems.

Threats From Tablets and Smartphones

As more vehicles offer drivers and passengers the chance to connect their tablets and smartphones by Bluetooth or Wi-Fi, infected personal devices are set to pose an ever greater threat.

The Need for a Direct Internet Connection

Driver assistance technologies are evolving, and the volume of traffic a vehicle's wireless system has to handle is increasing as a result. In the future, this volume will simply be too great to be sent through an OEM's VPN and data centre.

Even if crucial telematics data continues to be handled in this way, such data is likely to account for only 20% of the total wireless traffic—meaning a vehicle will still need an additional, direct connection to the Internet, and still be effectively reachable by anyone, anywhere.

The Impossibility of Strictly Separating the Communication System

With a vehicle open for attack through an increasing number of entry points, the ability to counter the spread of threats within its networks is crucial. But, since a network dedicated to vehicle control needs to communicate with a network dedicated to infotainment, the strict separation of systems is impossible.

Securing Next-Generation Automotive Communications

Given the range and severity of these threats, it's unsurprising that pressure is mounting on the automotive industry's major players to prove their vehicles are secure—indeed, in December 2013, U.S. Senator Edward Markey requested that 20 leading automakers reveal their procedures for testing the vulnerability of vehicle components and wireless systems[3].

Spirent is often asked if there are standards that can be followed to ensure architectures are secured. There aren't, and the reason why is simple—if security standards existed, hackers could quickly examine and exploit them.

While you won't find clear standards on how to protect your in-vehicle communications, there are important measures you can take.

Based on over 25 years' expertise in securing networks, these are Spirent's key recommendations.

Protect Your Access Interfaces

Wi-Fi, cellular modem and cable connector interfaces should be protected with firewalls (as is standard practice in IT and telecommunications networks).

3 Reuters, http://www.insurancejournal.com/news/national/2013/12/06/313092.htm

Protect at the Domain Level

Firewalls should also be used to between domains (e.g., Infotainment, Vehicle Control, External Communications) to prevent the spread of threats.

Again, this principle is regularly applied in IT networks, where it's common practice to put a firewall between strictly internal and publically accessible systems—creating a Demilitarized Zone (DMZ) that is open to the world, while providing extra protection for the rest of the Local Area Network (LAN).

Applying this principle in vehicles could prevent a smartphone's virus from spreading to critical systems, and potentially compromising vehicle control.

Virtually Separate Your Domains

It may be impossible to physically separate your domains—since, as outlined above, they need to be able to communicate with each other—but you can separate domains into Virtual Local Area Networks (VLANs).

As well as helping to prevent the spread of threats, VLANs offer the chance to prioritise one domain over another, ensuring the traffic from safety-critical systems takes precedence over traffic related to infotainment.

Spirent also recommends using secured VPNs for the transmission of safety-related communications to external places (such as Telematics information being sent back to the OEM), and for Car2x communications (such as roadwork warning systems).

What You Need to Test

As noted earlier, there are no clear standards when it comes to security. Ultimately, you'll need to design your own test regime. We recommend it includes the following tests.

Testing Internal/External Networks

Conformance

It's crucial that the devices within your vehicle operate to the international standards laid down by bodies such as The Institute of Electrical and Electronics Engineers (IEEE) and the European Telecommunications Standards Institute (ETSI). If they don't, they are open to exploitation.

You can find more information on conformance testing in our white paper Validating BroadR-Reach Protocol Conformance, which also includes a list of important protocol conformance tests for automotive applications.

Fuzzing/Negative testing

In addition to being sure that your devices conform to all relevant standards, you need to know how well they will function in exceptional circumstances. Fuzzing or Negative testing lets you determine how in-vehicle software responds to unexpected (i.e., invalid or random) data inputs, and is set to prove another vital technique in securing tomorrow's vehicles.

Vulnerability tests

As vehicles start to connect directly to the Internet, and Ethernet gains traction as an IVN, vehicle designers will need to test vulnerability to a broad range of attacks that are well-established in the wider IT world:

- **Distributed Denial of Service (DDoS)**—DDoS attacks aim to suspend or disrupt the services of host connected to the Internet—posing a serious threat to safety-critical systems.
- **Malware**—from self-replicating viruses capable of spreading throughout a vehicle, to Trojan Horses designed to bring specific systems to their knees.

Testing Security Devices

Testing the conformance and vulnerability of in-vehicle devices is only half the challenge. It will also be essential to test the functionality and performance of the security measures used to protect them.

Testing security devices is challenging work. A firewall must not only block unwanted traffic, but consistently allow wanted traffic to pass. In an automotive environment such functionally is particularly important—a firewall must be able to block a malicious attack without preventing essential communications from reaching, for example, the vehicle's brakes.

To effectively test firewall operations, R&D teams will need sophisticated testing tools, capable of:

- Simulating both 'good' and 'bad' traffic (e.g., a wanted web download alongside an unwanted virus)
- Simulating the infected devices, such as laptops, that could connect to IVNs
- Recreating the high loads possible in real attacks (if your firewall stops functioning at loads of 95%, hackers will be quick to exploit this 'back door')

Testing Global Navigation Satellite System (GNSS) Vulnerability

GNSS systems have their own set of vulnerabilities, notably to signal jamming and spoofing.

Even a low-power signal jammer has the power to disrupt GNSS navigation over an area of several miles. As GNSS-based navigation services become increasingly integrated into the driving experience, the ability to test navigation system performance in scenarios where GNSS access is limited or denied is essential.

Spoofing attacks involve false GNSS signals being used to trick, and gain control of, a vehicle's navigation system. As GNSS technology becomes ever more ubiquitous, evaluating a GNSS receiver's ability to recognise and reject spoofed signals is set to become an important security test.

Spirent Solutions for Automotive Ethernet

The Spirent C1/C50 hardware platform provides automotive test engineers with a fully integrated BroadR-Reach test solution. The C1/C50 includes Spirent's TestCenter Packet Generator and Analyzer software for advanced performance and functional testing of Layer 2/3 In-Vehicle Networks and components.

Additional Spirent test packages are available separately, including:

- Device/Network security and robustness
- Protocol conformance
- Pre-defined, automated Test Suites (such as IEEE1588v2 or AVB)

For detailed information please visit our Website: www.spirent.com/go/automotive

Spirent also offers a number of solutions for testing satellite navigation systems. A range of GNSS simulators is available, as well as software tools to verify the correct performance of in-vehicle systems. To assess system performance when GNSS signals are subject to interference, Spirent also offers a software package to help improve receiver resilience.

For detailed information please visit our Website: http://www.spirent.com/Positioning-and-Navigation/Transport

SPIRENT

1325 Borregas Avenue
Sunnyvale, CA 94089 USA

AMERICAS 1-800-SPIRENT | +1-818-676-2683 | sales@spirent.com

EUROPE AND THE MIDDLE EAST +44 (0) 1293 767979 | emeainfo@spirent.com

ASIA AND THE PACIFIC +86-10-8518-2539 | salesasia@spirent.com

Rev A. 02/14