Riot: tracking disruptive technology and its impact in industry

Automotive Cybersecurity: A ticking time bomb we may just prevent from going off

Executive Summary Only

Riot: tracking disruptive technology and its impact in industry

1). Introduction

Recent History
The Paradigm Shift – Autonomous Vehicles
Background Discussion—Cisco and Linaro

2). Current Security Approaches

Context
Emerging Tools
Smartphone Apps – a big problem
The Infamous Jeep Hack
The Risk's Scope
The Lower Stack Layers – Expanding Codebases

3). Industry Perspectives

BlackBerry QNX
- Domain Controllers
- Today's Security
- The Future
- Seven Pillars

Rohde & Schwarz
- Optimism
- Recalls
- Externalities

Lynx
- Hardware
- The Jeep touch-point
- The Automotive Market

Executive Summary

Automakers are being all too slowly drawn to modern security techniques to plug the security holes in connected cars. Riot questions whether that transition can happen swiftly enough to avert potential disaster.

There are already tens of millions of vehicles in the US which are connected via LTE or other cellular connections to the internet, opening them up to a straightforward IP attack. As the attack surface grows, closing in on 100 million cars, they make a more tempting target for organized crime, nation state attacks, terrorists, and random hackers.

The simple question is can the major automakers make them truly safe, before someone mounts a successful attack – whether that is one car at a time, or a fleet of hundreds of thousands at once.

In this paper, titled *Automotive Cybersecurity: A ticking time bomb we may just prevent from going off*, Riot takes an in-depth look at how professional security businesses are trying to steer automakers towards safety, and asks how many more years before they will be reasonably well protected.

But in this investigation Riot finds that automakers are not going down the obvious route of agreeing a standard, and moving rapidly towards its implementation in their next generation of connected cars.

Instead each of them is attacking the problem their own way, on their own turf, moving towards a new security architecture one step at a time, with each using a variety of techniques, from long encryption keys, deep packet inspection, virtual signatures, and daily over-the-air (OTA) updates.

Much of it owes something to Private Key Infrastructure (PKI), but not all of it, and each of them is looking at systems like ARM Trustzone to define a safe hardware Root of Trust (RoT). This approach will mean there is more room for more suppliers in the short term, but could just as likely mean that some automakers will remain vulnerable for some time to come. The lack of progress among some smaller car makers is quite frightening.

In the long term it is likely that the eventually successful security system will be open source, as much because Chinese companies refuse to rely on proprietary US systems which they have to license, or vice versa.

But most car makers already understand that they must separate network traffic into different domains, in a manner very similar to current techniques used in enterprise networking.

So as the automotive industry is entering what is a difficult transition period, it is still

years from a standardized approach to securing vehicles in a hyper-connected world and the clock is ticking. If one vendor manages to defend his turf, at the expense of a standardized approach, the mayhem around a single destructive hack of any car, even a rival brand, will still create industry-wide hysteria.

This puts us in mind of the early cellular industry, before the GSMA took control and standardized everything.

And yet across the entire ecosystem, multi-layered services are all preparing for industry-wide launch - first in the US, and then more broadly. These range from generic navigation, in-car entertainment services, to safety, such as vehicle location services and remote re-start.

Today we are at the beginning of such services and a handful of brands have truly useful car services, which currently extend to only a single-digit percentages of their owners. But expectation is high that a wider gamut of driver, owner and manufacturer services are just around the corner.

The more beneficial such services become, and the more widely they are installed, the more likely they are to be attacked, either to disrupt revenue or ultimately as a route into remote physical control of a vehicle.

What follows are the accounts of security stakeholders in the automotive industry, capturing perspectives from suppliers – because the automakers themselves collectively declined our repeated requests for interviews. This is another case of security by obscurity, a strategy the technology industry knows has never worked - by keeping all their thoughts about security a strict secret.

The real route to security is through open standards, which can be hardened by a wide base of users finding different attack vectors during the standardization process, and then sealing such exploits, in the same way the humble SIM card came about.

Sample Content

Introduction

Cars are entering a difficult transition period, as the automotive industry acquires the necessary skills to build secure vehicles that make use of a connection to the internet. Connected cars are truly here, and self-driving cars are just around the corner – but the automotive industry is still years from a standardized approach to securing these vehicles in a hyper-connected world.

Without such a security framework, each car represents dozens to hundreds of potential backdoors for potential attackers – so how much danger does this status quo present?

What follows are the accounts of security stakeholders in the automotive industry, capturing perspectives from suppliers – as the automakers themselves collectively declined our repeated requests for interviews. Of those automakers that confirmed why they did not want to participate, we were told that they simply did not speak about security-sensitive technologies in their products.
Connected cars aren't exactly new. GM is considered the first automaker to launch such a vehicle, doing so with the 1996 Cadillac Deville, Eldorado, and Seville – all of which housed its now-familiar OnStar system, which was developed by Motorola Automotive (later acquired by Continental).

OnStar was an emergency alert system, which could dial out to a call center in case of a crash, in order to dispatch help. The system initially used just the Mobile Network Operator's (MNO) voice networks, but the introduction of data capabilities to these 2G networks allowed OnStar to add new features – like GPS coordinates. OnStar added diagnostics features in 2001, and later navigation, off the back of this internet connection, and now supports WiFi hotspots, stolen vehicle assistance, and navigation discovery.

Collectively, the capabilities and complexity of the connected car and its in-vehicle infotainment (IVI) system have risen since OnStar's debut – and now typically feature navigation as the core application, with entertainment services being the next most prominent feature. US automakers are increasingly moving toward supplying connected cars as standard, with most of the premium models in a range featuring the technologies, and the package slowly trickling down their ranges.

These days, a connected car will house an in-vehicle WiFi hotspot, using an embedded LTE connection in the car to provide occupants with high-speed WiFi for their mobile devices – with Audi being the first to do so, in 2014. Typically, the car is sold with some amount of trial months, before its owner needs to strike up a deal with an MNO – something that many customers are irked by, as they believe connectivity is a service that should be provided by the automaker directly.

Who Should Read this Report?

"Automotive Cybersecurity: A ticking time bomb we may just prevent from going off" is one of a dozen think piece style White Papers, which come at part and parcel of our Riot service. Any stakeholder in the Internet of Things, whether they are based in an MNO, a major enterprise, an equipment vendor or a software house should be reading this report and all the other outputs of Riot, a C Suite level down to product marketing.

Why has Rethink written this Report?

Rethink Internet of Things (Riot) is a weekly service which covers the Internet of Things, AI, and Cloud processing. It is a paid subscription service costing just $650 a year.

It consists of two issues each week;
The first is a curated view of the week's news, known affectionately as **Around The Web**, which has linked to every major point of interest in the
The second is a set of **essays on current issues** in the development of IoT, AI, and Cloud processing consisting of around 25 pages of analysis and thought leadership.

Pricing and rationale

These reports make up the remainder of the Riot service and they have just gone monthly and archived issues include:

IoT M&A and significant deals—Quarterly
How the LPWAN market will shake out
Insurance and the Internet of Things
A primer of Enterprise IoT security
Labor automation robotics and AI
The Riot Survey
Beware the Five Myths of the IoT

These are each priced separately at $650, and yet they are FREE with a subscription to Riot (which also costs $650) - So it makes sense to buy into the entire service.

Riot: tracking disruptive technology and its impact in industry

Riot is published by:
Rethink Technology Research Ltd,
Unit G5, Bristol & Exeter House, Lower Station Approach,
Temple Meads, Bristol, BS1 6QS
Tel: +44 (0) 117 925 7019
Website: www.rethinkresearch.biz

Riot's main contributors

Editor and Senior Analyst: Alex Davies alex@rethinkresearch.biz
Analyst: Thomas Flanagan tommy@rethinkresearch.biz
Analyst: Jack Vernon jack@rethinkresearch.biz

Rethink leadership

CEO: Peter White peter@rethinkresearch.biz
Research Director: Caroline Gabriel caroline@rethinkresearch.biz

About Rethink

Rethink is a thought leader in quadruple play and emerging wireless and IoT technologies. It offers consulting, advisory services, research papers, plus three weekly research services; **Wireless Watch** which has become a major influence among leading wireless operators and equipment makers and **Faultline**, which tracks disruption in the video ecosystem, which has become required reading for anyone operating in and around quad and triple play services and digital media. **Riot** is Rethink's latest research service.

Sales contact details

John Constant +44 (0)1794 521 411
Email: john@rethinkresearch.biz