Review of the book

"Embedded Security in Cars"
by

Kerstin Lemke, Christof Paar & Mako Wolf (Eds.)

Springer 2006

ISBN: 978-3-540-28384-6

Review contributed by Andrew Waterhouse
(awaterhouse@pacresearch.com.au)
2019-02-12

1 Overview

Although this book was published around four years ago, it remains a very timely summary of security considerations in automotive electronics specification, design and use. Much of the material can be applied generically to embedded electronics, but there are also specific problems in vehicle electronics that need special attention.

2 Review in Detail

Because security is such a dry and monochromatic topic, I will start be telling you that I am writing this review while looking out on a giant cedar on a misty hilltop in folds of the Blue Mountains west of Sydney. My car is safely sheltered in what passes for my garage, and to the best of my knowledge, there is nothing computationally untoward going on in its electronic systems. The same might not be said for the electrical systems of the reviewer.

2.1 Introduction to Automotive Security

So, to the matter at hand. The first chapter of this nice little book gives a quick tour of the material lurking in the coming pages, noting that this selection of expert contributions does not pretend to be an exhaustive survey of vehicle security. Areas that are treated include vehicle control and monitoring systems, in-car and inter car communications, car systems programmability and infotainment content management, and anti-theft mechanisms.

The introduction importantly notes the increasing relevance of 'reverse engineering' attacks. As later chapters show, the security of many embedded designs hinges greatly on how secrets are stored and operated in electronic hardware. Advances in side-channel, fault and probing attacks mean the protection of secret keys is, alas, ever-more reliant on the intricacies of undisclosed hardware and program design features. After scorning 'security by obscurity' as an unworthy approach, we have had to invite it back to help address some intractable vulnerabilities.

2.2 Software 'Flashing'

The chapter on software flashing covers the relatively well trodden path of securing field injection of 'software' into embedded systems. The authors note that software these days doesn't just mean CPU instructions, but often direct gate and analogue cell array programming of hardware functions.

What distinguishes core vehicle control systems from other classes of in vehicle systems like infotainment is the potential safety consequences of a security breach, whether intentional or accidental. If we are to 'drive by wire', then we want those wires to carry their intended signals. Security not only helps keep adversaries out but also can help protect against unintentional misadventure.

In this chapter and elsewhere in the book, concerns are raised about the computational power required to complete security calculations (CRCs, MACs and digital signatures). However I am not so sure that these are real problems in a well-designed security architecture. The chip industry has some affordable answers if we pose the questions correctly, and process design and task scheduling can mostly ensure that the slowest computations occur when performance is not critical. Industry experience suggests that cryptography is not the only bottleneck in embedded systems and that cryptographic performance must be evaluated in context.

I am also not altogether comfortable with this chapter's assertion that the potential for symmetric key compromise in embedded systems is greater than for asymmetric keys. That entirely depends on which keys or key parts are used for which purpose. Secret key parts in asymmetric systems are no less vulnerable than their symmetric counterparts; and preventing the substitution of public key elements is a non-trivial problem in real world of signature verification.

Finally, I wonder whether we are heading towards the day when our cars have to log on to the internet at start-up to receive the latest patches. If my computer is any guide, I will spend a lot of my driving time waiting at the curb.

2.3 A Secure Software Delivery Method

The next chapter looks at the nuts and bolts of a possible secure software delivery mechanism based on the Trusted Third Party (TTP) approach. The concept works on paper, but my guess is that such a model, unless enforced by national standards bodies, will not prosper in the short term as it is requires a level of cooperation between rival manufacturers that is rarely seen around the globe. Placing a TTP at the centre of the universe also introduces a potential single point of failure. Nature teaches us that 'hybrid vigour' has its benefits.

2.4 Vehicle Theft Countermeasures

The next chapter is a good summary of the vehicle immobiliser scene. Harking back to the reverse engineering topic raised in the introduction, it points out that a little knowledge of the design and access to the relevant components has allowed otherwise well protected immobiliser systems to be easily bypassed. This is a good demonstration of how attackers will naturally gravitate to the Achilles heel of an otherwise good security design.

This chapter discusses the competing pressures for tightening up the methods of binding authentication tokens such as RF remote-control keys to vehicle transponders to reduce the problem of intruder attacks. I also points out the inconvenience that may arise when a car owner needs to replace or add a token where the binding method is strengthened. Heavy-handed security controls are not always going to win friends amongst consumers.

There is an interesting section in the chapter on the possible use of signal transmission delay bounding to stop middle-party attacks on ignition transponders, and the author's also touch on biometric and position detection countermeasures.

While car theft is not uncommon, we are perhaps reaching the point in newer models where the existing security measures are doing quite a good job of preventing opportunistic theft. However for well organised and pre-meditated theft, what we may need is for security measures to be so widely distributed and diverse in the vehicle electronics that the disincentives far exceed the benefits of trying to break the system.

2.5 Digital Tachographs

While this chapter is mainly a story about security in digital tachograph systems, what I actually liked most was its presentation of rigorous methodology for security lifecycle vulnerability analysis. In my experience many development engineers dive into highly technical designs without sufficient consideration of the 'whys and wherefores'. In this chapter, the authors start with first principles such as EU directives, the threat environment and the characteristics of the 'target' technology, and then lead us though the logical process of identifying potential vulnerabilities at every stage of the equipment lifecycle. I only wish this type of analysis was applied as a matter of course in design laboratories.

This chapter explores various security failings of the relevant European Commission (regulations) for tachographs – or at least the regulations as they were at the time the book was published. This includes vulnerabilities in motion sensor master key management and PIN management. The plausibility of tachographs being maintained in secure environments is questioned.

I think this chapter reinforces the message that security is sometimes a mirage. It looks solid from a distance, but becomes increasingly shaky the closer you get. In many real-world cases we must look to safeguards beyond those implicitly available on the embedded target to achieve our trust goals.

2.6 In-Vehicle Communications

The in-car communications world is becoming a very noisy and complicated place as the next chapter demonstrates. Various inter-module bus methodologies are in use, mainly but not always wired. Some are localised, and others span many vehicle subsystems. The authors hint at the various issues of authenticating, encrypting and firewalling these networks, but mainly this chapter serves only to alert the reader to vulnerabilities that merit further investigation and solutions.

I get the impression form this contribution that the gap between the abstract model of a truly secure vehicle and the implementation models for vehicles in the showrooms is only going to close slowly and asymptotically.

2.7 Inter-Vehicle Communications

Somewhat the same story applies to inter-vehicle communications as discussed in the next chapter. This contribution touches on various candidate inter-vehicle communications systems for use in the era of Intelligent Transportation Systems (ITSs). The authors raise interesting questions regarding the most popular approaches to disseminating information in ad hoc networks between vehicles. Overlaid on the theoretical challenges of getting 'maximum information transfer utility' is the ever present question of how protect that information. I agree with the authors that until we understand how the information transfer will take place in ad hoc vehicle networks, we really can't so much useful work on security solutions.

2.8 Cryptography

The inclusion of two short summary chapters on the state of the art in symmetric and asymmetric cryptography is good. We cannot assume that the automotive design professionals or managers to whom this book is addressed will always be experts in these matters too. The treatment here is to the point, however I came away thinking that if I was a cryptographic novice, I wouldn't be much the wiser about how to go about the security design for a given automotive function. In compensation, other chapters in this book give useful pointers.

At risk of being controversial, I am relieved that this section of the book did not digress onto the question "light weight cryptography". I know this concept is getting quite a deal of research and standards exposure right now, but if we have adequate tools in the 'right weight cryptography' domain, we need look no further.

2.9 Mobile Communications Security

This chapter gives a succinct overview of the most pervasive wireless communications methods likely to be found in a vehicle, ranging from GSM/UMTS through Bluetooth and Zigbee to Irda. It identifies the basics of any related security services.

What is interesting is how much wireless communications currently operates with available security features deliberately weakened or disabled. The admittedly rather simplistic general rule seems to be that unless money is involved or the legislators or regulators mandate it, strong security practice is often absent.

Leaving aside questions choice of specific algorithm (or 'choice of vulnerability' as some critics put it), I have always thought that the GSM authentication method of using cryptographic triples, and now UMTS using quintuples, is an elegant demonstration of how to solve practical problems relating to key distribution using a quantifiable risk of short term key compromise.

In any case, the message to implementers is clear: look at each communications interface in turn, determine the relevant threats and vulnerabilities, and then make some sound security decisions.

2.10 Side Channel Attacks

The chapter on side channel attacks and the following chapter on tamper resistance, get to the very heart of the question of whether we are serious about security. If we are to use of secrets, then we must make sure those secrets are well protected at all times.

The contribution on side channel attacks is an excellent summary of the current state of play, and shows just how hard it is for designers to hide keys from a well equipped and knowledgeable adversary. Truly adequate countermeasures can come at very considerable cost, and there are rarely easy solutions in sight.

2.11 Anti-Tamper Measures

The chapter on tamper vulnerabilities and safeguards is an excellent summary of the current state of play in trying to provide protection against direct attacks on hardware. Coupled with the preceding chapter, this material may leave the security practitioner in a rather pessimistic mood. There is some wonderful laboratory equipment within easy and economical reach today, and that makes life miserable for security implementers of all kinds.

For automotive electronics engineers, I think the message here is to be very careful about what hardware security assumptions you make, chose your chips and methods carefully and consult widely with experts in the field.

2.12 Digital Content Management

The chapter on digital content management addresses a number of security issues related to the consumption of licensed - perhaps subscription based – data within the advanced automobile environment. Areas covered range from navigation to entertainment. The latter, as we know, is a very fraught area at this time.

I think the authors of this chapter are overly optimistic in imagining the advent of centralised in-vehicle license management for highly disparate data types. My bet is that each industry sector will go down its own path to address its specific access issues. There will doubtless be similarities and overlaps, but I am doubtful about convergence. On the question of vehicle-specific digital content - for example unlocking of certain discretionary features of a vehicle's operation - it seems to be an open field for innovation, and not necessarily governed by standards.

2.13 Vehicle Infotainment Business Opportunities

The chapter on securing the exploitation of in-vehicle entertainment raises some interesting questions. The requirement for secure pricing and billing systems come into the picture, but so does the question of whether there is much marginal utility to the vehicle occupants for such paid services in a world of ready information

access. From the strict engineering perspective, we cannot answer such a question and can only offer tools to protect data when needed. I think the author rightly concludes that markets will determine the future of this area, with some gentle help from the regulators who are uneasy about the 'cockpit' becoming cluttered with ever more distractions.

2.14 M-Commerce in Vehicles

I am not sure that the author's use of the term 'M-Commerce' in the title of this next chapter aligns exactly with how I would use it. This chapter focuses on how service providers can make money out of vehicle occupants, rather then how vehicle occupants might engage in commerce in the normal business sense of the word.

I must also confess that I find discussions of electronic commerce business models much more challenging than the study of cryptography. The associated diagrams are always much more inscrutable, than say, the key expansion diagrams for a symmetric cipher. I suppose this is why I am in engineering and not marketing.

Nonetheless I found the discussion of the evolution Siemens' VDO business units and their C-IQ system in this chapter most interesting. C-IQ is about navigational tools augmented with more general travel information.

Navigation is king of course. In western countries, the paper-based street directory is almost a thing of the past. Since electronic geo-data acquisition and delivery involve considerable capital and operational costs, it is understandable that security methods are absolutely central to getting a return on investment for the providers. In regard to security, this chapter touches on algorithmic approaches and key distribution issues, but in short, we seem to be essentially looking at the question of digital rights management and not some other species of problem.

Beyond navigation I am not sure whether I want my car to remove the element of serendipity in travel (restaurants, points of interest and so on). I would always suspect my vehicle of having commercially motivated biases in that regard, and anyhow I imagine I would simply use the internet for this purpose rather than accessing a paid service. But then again, I am not of my children's generation.

3 Conclusions & Reflections

There are a couple of pertinent vehicle security topics that I can think of that are not specifically analysed by the contributors - electronic tolling and electronic license plates - but we can't ask for everything in one small book. Likewise, the potential for interplay between smart card based licenses and vehicle electronics is an intriguing area for future exploration

On shutting the book, I was left musing that as security practitioners we need to be on our guard against introducing unforeseen dependencies through our work. Some of the security schemes we are dreaming up may look good on paper, but unexpected usage issues can arise which make implementation problematic. Avoidance of single points of failure and the need for failsafe mechanisms are very high on the agenda for automobiles, and these can conflict with security objectives.

I was also left pondering on how far we have come from grass-powered transport, and whether, with all this electronic wizardry, we might be losing the art of simply looking out of the car window.

In any case, this book is an excellent security primer for those working in automotive electronics, and its lessons can be applied to many areas of embedded design beyond that. I commend it.