Risk reducing automotive hardware cybersecurity threats

Alison Young[1], Alastair Walker[2]

[1]LORIT CONSULTANCY, Glasgow, Scotland. alison.young@lorit-consultancy.com
[2]LORIT CONSULTANCY, Edinburgh, Scotland. alastair.walker@lorit-consultancy.com

Abstract

Cyber security has grown enormously as a topic in the automotive sector over the last 2 or 3 years. A great emphasis has been placed upon software cyber security measures, but arguably hardware plays a more important role in cyber security solutions than that of software.

Hardware security – whether for attack or defence – differs from software, network, and data security because of the nature of hardware. Often, hardware design and manufacturing occur before or during software development, and as a result, we must consider hardware security early in product life cycles. Yet, hardware executes the software that controls a cyberphysical system, so hardware is the last line of defence before damage is done – if an attacker compromises hardware then software security mechanisms may be useless.

Hardware also has a longer lifespan than most software because after we deploy hardware we usually cannot update it, short of wholesale replacement, whereas we can update software by uploading new code, often remotely.

Keywords

Cybersecurity, malicous attacks, trojan circuits, cryptographic interfaces

1 Introduction

Cybersecurity is a subject that has grown significantly in the last 2 or 3 years in in the automotive sector. With numerous potential security vulnerabilities in the modern car much attention has been placed on software integrity, but there are many hardware vulnerabilities and these are arguably more challenging to address than software weaknesses, due to the early point that a solution must be implemented and due in many cases no ability to rectify the problem once the product has been supplied to the customer.

This paper looks at many of the potential vulnerabilities and the corresponding solutions to address these weaknesses.

Threats from malicious attacks[1] on an autonomous car infrastructure are now far more significant, as high-altitude electromagnetic pulse (HEMP) which would have previously impacted individual cars, could in the future bring the entire automotive infrastructure of a city to a halt.

Threats from within an organisation or chain of organisations involved in the development of increasingly complex electronic hardware are also an increasing concern for microcontroller or complex logic manufacturers. Trojan circuits have already been implemented in well-established manufacturers products

The third type of vulnerability addressed in this paper, is the type of weakness that the average hacker would be able to expoilt

2 Background

2.1 The Hardware Cybersecurity Challenge

As the vulnerabilities in automotive systems become better understood, the days that purely adding software mechanisms to address cybersecurity vulnerabilities is no longer adaquate.

Hardware is not only a key consideration in the vulnerabilities of systems, it can also play a key role in cybersecurity mitigations.

Hackers tend to be injeous individuals and wil exercise all kinds of strategies to find weaknesses and vulnerabilities in systems, for this reason solutions implemented in hardware have to be extremely robust, as the hardware maybe fixed for the entire life-cycle of the product.

3 Hardware Cybersecurity Threats

3.1 Destructive Threats

There have been many papers written on the subject of Emission Security[1] (EMSEC). Many originating from the US Militatry. With adaquately encripted data, most threats in the automotive industry should be mitigated, however radiated emissions and common power supply lines can still be vulnerable points in a system.

Not considered here, but a source of much discussion is the ability to damage electronic devices through the use intense radation levels that could leave a device vulnerable

3.2 Malicious Threats

Due to the complex stucture of modern integrated circuits (IC) there are often many different organisations involved from the initial concept through to fabrication, this also typically includes third parties such as development tool suppliers. With so many different organisations and phases it becomes easier for an attack that plants a trojan circuit in the silicon[2], between the design and fabrication phases. Trojan circuits do not prevent the device working as defined in the specification, they add something extra, that allows the integrated circuit to be compromised at a later date. Detection of trojan circuits can be a very challenging activity.

3.3 Hardware Cybersecurity Design Weaknesses

As in the case of software, where Commercial Off the Shelf (COTS) is more attactive to hackers, as it is widely available and well known. Using standard 3rd party hardware interfaces is another source of vulerability. If a standard interface component is utilised and it has known weaknesses then these will be known to individuals in other organisations and could be expoited.

Attacks can be applied by either overvoltaging the device or under voltaging the power supply. Generally most microcontrollers will have brownout and reset circuits to prevent the microcontroller from operating outside its guaranteed operating conditions. However not all microcontrollers including those used in automotive applications have over voltage detection. The brownout circuits of some

microcontrollers also have unknown characteristics, hence as an additional measure the use of an interna or external power supply monitor IC can ensure that both over and under voltage conditions are not only detetcted but the microcontroller is halted when the condition is detected.

In addition to the power supply monitoring it is also important to ensure overvoltaging will not damage the circuitry, hence again compromising the operation adequate transient or overvoltage protection and or fusing should be designed into the product.

Buffer overflow is one of the most common methods for a hacker gaining access to a system. Predominately this is considered to be a software phenonom, however, if hardware also exhibits this weakness, the hardware can be the cause of the vulnerability.

Interface and debug ports are another area where vulnerabilities exist in devices. Software encryption and authentication are often discussed as mechanism to reduce the risk of attacks. In hardware use of bespoke connectors, disabling interfaces in hardware when not required are means of improving security in hardware.

In contrast to the destructive EMC issues highlighted in section 3.1, there is also the potential for information to be extracted from transmissions from a device, this can be either radiated or conducted transmitted information or through common power supply lines

4 Techniques for reducing Hardware Cybersecurity Risks

4.1 Defence Against Malicious/Destructive Attacks

To protect automotive networks against HEMP attacks could be a very costly exercise and ultimately the potential magnitude of a malicous electromagnetic pulse can not be predicted. However, sensible screening of circuitry should follow industry standard EMC guidelines[3].

As is the case in the world of functional safety and as defined in ISO 26262 [4] graceful degradation of functionality can be implemented, such that each item that fails in the network due to HEMP will not impact the remainder of the network and shall switch in a controlled manner into a safe or inactive state.

4.2 Detection of Trojan Circuits

Due to the compelxity of modern ICs, inspection and testing are not adquate for detetcing trojan circits, destructive approaches are too costly and cannot be applied to all ICs.

Two methods that are potential mitigations are side-channel analysis and trojan activation. Side-channel analysis relies on variations in signals, usually analogue e.g. power dissipation, current, temperature or timing.

Trojan activation techniques attempt to trigger a trojan circuit during silicon design authentication to make the malicious behavior observable or to improve side-channel analysis techniques. A motivating assumption is that attackers are likely to target the least-activated circuitry in an IC, so researchers have explored methods for generating inputs that activate an IC where trojan circuits are likely to be hidden.

Developing a reference device or ‘golden sample’ is a key aspect of any detection strategy. Then measurement of parameters such as power consumption or leakage current will be able to highlight the differences between the golden sample and versions containg trojan circuits.

Using two different chips from different fabs that check and compare the same feature is also a technique for detecting trojans.

4.3 Cybersecurity Design Solutions

4.3.1 Cryptographic Interfaces

Most mircocontroller manufacturers use techniques to reduce the likelyhood of the microcontroller being compromised through the standard interfaces. These generally take the form of hardware security circuitry and are based on cryptographic modules, examples being, Renesas Secure Hardware Extension (HSE), Microchip Hardware Crypto Engine, NXP and Infineon Hardware security Modules(HSM) or the NXP Cryptographic Acceleration Engine.

One major concern in this type of circuit is the posibility of hardware trojans being built into the circuit, in such a case the security of the chip could be comprimised.

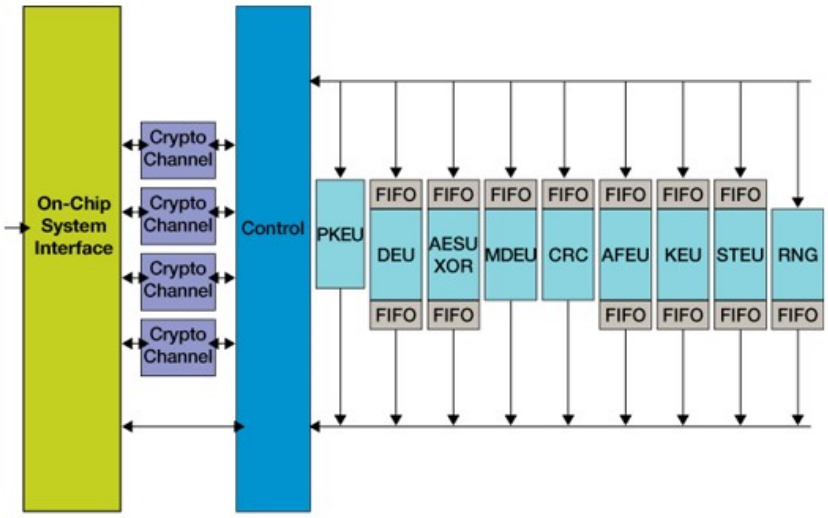

Figure 4.3.1 Typical Cryptographic Interface

4.3.2 Over & Undervoltage Protection

Detection and protection against over and under voltage can be relatively simply implemented in circuits. If a power supply moves outside the specified operational region the circuitry should cease to operate e.g. switch to a reset state. Protection circuitry should prevent destruction of the main circuitry e.g. microcontroller wherever possible. However a determined hacker may apply tests to devices when they are not in the normal working environment, hence such case are more difficult to defend against. If a device is to deliberately overstressed in the search for vulnerabilities, then the device should fail such that no key information can be extracted following the attack.

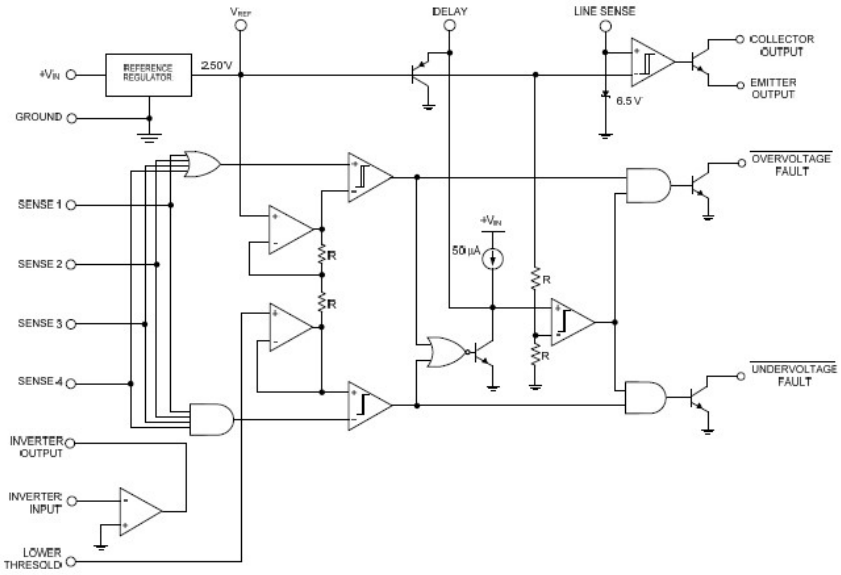

Figure 4.3.2 Microsemi SG1548 Over and Undervoltage Detection IC

4.3.3 Buffer Overflows

Hardware-assisted approaches to buffer overflow protection improve upon accuracy and performance of software-only schemes for dynamic attack detection. One common solution is to maintain a shadow of the return address in hardware Figure 4.3.3 by creating a return address stack or monitoring the location of the return address for any unauthorized modifications

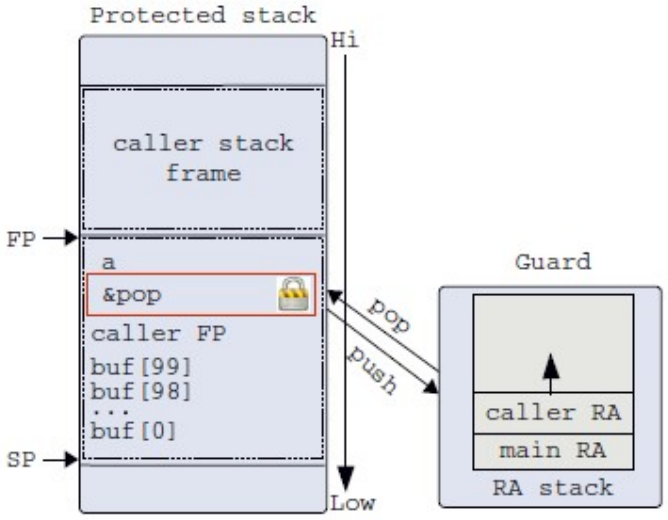

Figure 4.3.3 Hardware Protection for Buffer Overflow

4.3.4 Mechanical Measures

Using bespoke interfaces and connectors, will not prevent a hacker gaining access to the interface, but they can hinder progress or deter the less motivated of hackers.

Deactivating interfaces through hardware means also hinders a hacker's ability to gain access to the microcontroller or programmable logic

5 Conclusion

There many potential cybersecurity vulnerabilities both identified and mitigated in modern integrated circuits. However, not all products use either the most modern devices for cybersecurity protection. This paper describes vulnerabilities and pragmatic solutions for reducing cybersecurity vulnerabilities. Even if using basic microcontrollers in a product additional measures can be built around it to provide a suitable cybersecurity solution. For IC manufacturers producing the more sophisticated microcontrollers there are potential weaknesses through trojan circuits, but again these can be detected through the appropriate measures.

6 Literature

[1] Addressing Electromagnetic Threats to U.S. Critical Infrastrucure - JINSA's Gemunder Center EMP Task Force DR. Bryan Gabbard and Ambassador Robert Joseph

[2] Hardware and Security: Vulnerabilities and Solutions - Gedare Bloom, eugen Leontie, Bhagirath Narahari, Rahul Simha

[3] Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations - Markus G. Kuhn and Ross J Anderson University of Cambridge

[4] ISO 26262-6:2011 Road Vehicles - Functional Safety - Product Development at software level

[5] Tamper Evident Microcontrollers - Adam Waksman, Simha Sethumadhavan

7 Author CVs

Alison Young
Alison Young is an engineer with over 15 years' experience in the automotive industry. After graduating from Heriot Watt University in Edinburgh she spent 6 years with Jaguar Land Rover working on hardware-in-the-loop simulation of powertrain and body systems. Following this she worked 8 years for NXP as a system safety architect, she was involved in the definition of new leading edge automotive microcontrollers

Alastair Walker
Alastair Walker is an engineer with over 25 years development experience in medical, automotive and aviation industries. He is a TÜV Rheinland Functional Safety Engineer and has extensive knowledge of developing embedded systems in safety related industries, such as ECG stress test, cryotherapy and electrical muscle stimulator systems, automotive inverters and aviation transponders.