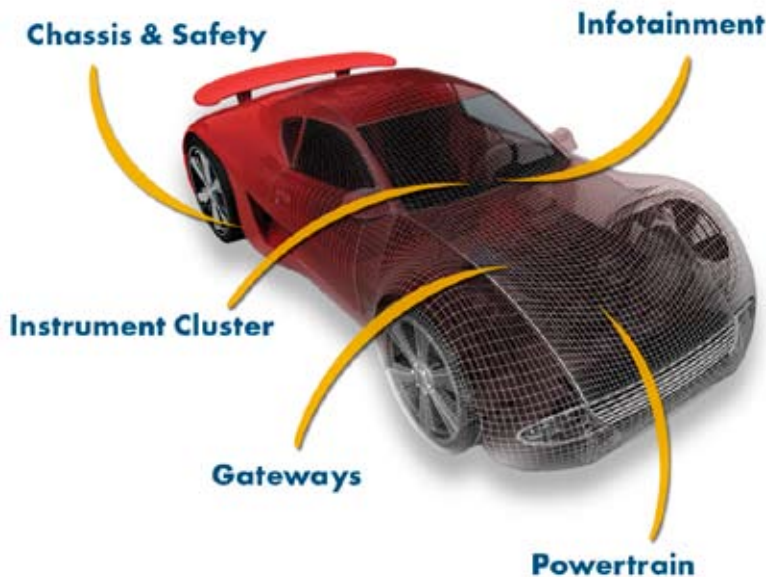




David Kleidermacher discusses the important emerging security threats and the core principles and approaches that must be used to counter them in next-generation automotive systems

Concerns for the next generation

Fig. 1: Examples of automotive ECUs



In 2010, US car makers introduced a feature to enable car owners to manipulate the locks and start the engine from anywhere on the planet using a smartphone. This connectivity piggybacks on the car's remote telematics system, which has become standard in many models.

Just prior to this smartphone introduction, a team of university researchers published a study demonstrating how such a car's critical systems – brakes, engine throttling and so on – could be maliciously tampered with by exploiting vulnerabilities in the car's embedded systems.

The researchers learned how to bridge from the low security network to the critical systems using fuzzing techniques. Brakes and engine were disabled while the car was in motion, demonstrating that the attacks could indeed place passengers in peril.

Connecting the automobile to wide-area networks is exactly the trigger that brings in the threat of sophisticated attackers. A single flaw may allow a remote attacker to perpetrate damage to an entire fleet of vehicles.

"In our car we identified no fewer than five kinds of digital radio interfaces accepting outside

input, some over only a short range and others over indefinite distance," said the researchers. "Taken together, ubiquitous computer control, distributed internal connectivity and telematics interfaces increasingly combine to provide an application software platform with external network access."

Ironically, the remote telematics – a safety and security system – may now provide the means for distributed, remote attacks.

What the researchers do not talk about is what we can do about embedded automotive security today. Small changes could be made to isolate better the network subsystems. Strong cryptographic authentication must be used for all network connections. Trusted platforms and remote attestation must be used to prevent rogue firmware installs from exposing the car network to attackers. ECUs with mixed criticality functionality must employ high assurance partitioning and access control: the rear-view camera must not be affected by iTunes.

Modern electronics

Fig. 1 shows a selection of electronic components within the modern automobile. High-end luxury cars contain as many as 200 microprocessors across 100

components or electronic control units (ECUs). Multiple networks of varying types, including Controller Area Network (Can), Flexray, Local Interconnect Network (Lin), and Media Oriented Systems Transport (Most), connect these ECUs. The car OEM integrates ECU components and software from dozens of tier one and two suppliers. While the OEM often defines requirements for these ECUs, it does not rigorously control their actual contents or development process.

It should be no surprise that this situation has become untenable. OEMs are suffering from the longest pole in the tent syndrome: a single ECU, delivered late or with serious reliability problems, may be all that is needed to cause shipping delays or customer-visible failures that lead to recalls and poor reputation. Add to this the new challenge of security: a single vulnerability in a critical component, such as the gateway to safety-critical networks and functions, can allow in remote attackers.

Threats and mitigations

The realm of security threats to cars can be coarsely classified in three domains: local-physical, remote and internal-electronic. Combinations of these threat domains will often be required in order to inflict damage.

Local-physical

Examples of local-physical threats would be someone physically tapping into the drivetrain's Can network and disrupting communications or damaging an ECU via power surge or excessive heat application. Such an invasive attack can quite easily disable critical car functions. However, a local attacker, such as a disgruntled mechanic or maligned spouse, can harm only one car and is therefore



Fig. 2: Examples of next-generation extra-vehicular communications

unlikely to get the attention of security teams. Furthermore, a car's massively complex, distributed electronic system is simply impractical to protect from physical attack. So we generally punt on this class of threats.

There is, however, one exception, and it is an important one. Somewhere within one or more ECUs, private cryptographic keys are stored for use in creating protected communications channels and to provide local data protection services. Communications may include car to service centre or other OEM infrastructure, car to multimedia provider, car-to-car, car to power grid (electric vehicles), car to smartphone or even car to bank. Fig. 2 shows some examples of long-range radio connections in next generation vehicles.

Data at rest protection may be required for automotive algorithms, multimedia content and cryptographic material.

Private keys must be kept in storage that can withstand sophisticated physical attacks, both invasive and non-invasive, because the loss of even a single private key may enable an attacker to establish connections into remote infrastructures where widespread damage and property loss can ensue. OEMs must be able to achieve high assurance of key protection across the entire life cycle, from creation to embedment into ECUs, delivery and integration

within the car, and in the field. Embedded systems cryptographic experts can help OEMs and their suppliers with guidance and oversight in this area.

Remote

These are the classics: hacker tries to probe the car's long range radio interfaces for vulnerabilities in network security protocols, web services and applications to find a way into the internal electronics complex. Unlike high-end data centres, the car is unlikely to be outfitted with a full complement of IDS, IPS, firewalls and UTMs. Regardless, recent intrusions at Sony, Citigroup, Amazon, Google and RSA starkly demonstrate that these defence mechanisms are Swiss cheese against sophisticated attackers.

When the Stuxnet attack came to light in 2010, US DoD Cybercom chief General Keith Alexander suggested that the USA's critical infrastructure ought to be isolated on its own secure network, distinct from the internet. While this may seem heavy-handed, it is precisely the kind of thinking needed. The car's critical systems must be strongly isolated from ECUs and networks not critical for safe operation.

Internal

While physical network isolation is desirable, touch points will inevitably exist. For example, the

“The car's critical systems must be strongly isolated from ECUs and networks not critical for safe operation”

car's navigation system, in some markets, must be disabled while the car is in motion, implying communications between systems of widely differing safety criticality. Furthermore, a strong future trend towards consolidation – where more powerful multi-core microprocessors are used to host disparate systems, turning many ECUs into virtual ECUs – increases the risk of software-borne threats such as privilege escalation due to operating system vulnerabilities, side-channel attacks on cryptography and denials of service.

Therefore, the car's internal electronics architecture must be designed from the ground up for security. Touch points between critical and non-critical systems and networks must be justified at the highest management levels, and these electronic touch points must be analysed and certified devoid of vulnerabilities at the very highest assurance levels, such as ISO 15408 (Common Criteria) evaluated

“Manufacturers must work closely with embedded security specialists early in the design and architecture of in-car electronics and networks and must raise the bar on security-driven engineering and software assurance”

assurance level (EAL) 6+.

Phase – Principles of High Assurance Software/security Engineering – that espouses minimisation of complexity, software component architecture, principle of least privilege, secure software and systems development process, and independent expert security validation must be learned and adopted by OEMs and promulgated to ECU suppliers.

Conclusion

Car manufacturers and tier ones may not have been thinking a lot about security when they

designed the cars hitting roads today, but clearly that must change. Manufacturers must work closely with embedded security specialists early in the design and architecture of in-car electronics and networks and must raise the bar on security-driven engineering and software assurance. Finally, the automotive industry is sorely in need of an independent standards body to define and enforce a high assurance security certification programme for in-vehicle electronics. ●

David Kleidermacher is CTO for Green Hills Software