I AM THE Cavalry

Five Star Automotive Cyber Safety Framework

Introduction

Modern cars are computers on wheels and are increasingly connected and controlled by software. Dependence on technology in vehicles has grown faster than effective means to secure it. Security researchers have demonstrated vulnerability to accidents and adversaries over more than a decade. See timeline of automobile computer security research.

On August 8th, 2014 I Am The Cavalry published an open letter to the Automotive Industry.

This letter urges carmakers to:

- Acknowledge that vehicle safety issues can be caused by cybersecurity issues;
- Embrace security researchers as willing allies to preserve safety and trust;
- Attest to these five foundational capabilities to improve visibility of their Cyber Safety programs;
- Initiate collaboration now to avert negative consequences in the future.

Safety By Design

The public is informed and assured of your commitment to safety when you publish the extent to which you ensure that software is reasonably free of flaws. The goal is to convey confidence to the general public and to allow consumers to make informed choices among market alternatives. Software manufacturers, such as Microsoft and others, make this attestation and could serve as a model for automakers.

Do you have a published attestation of your Secure Software Development Lifecycle, summarizing your design, development, and adversarial resilience testing programs for your products and your supply chain?

Key Elements:

Standard Based: Use of vetted ISO, NIST, or Industry standards would both accelerate an organization's maturity and ensure more predictable, normalized, comprehensive practices.
Supply Chain Rigour: Well-governed, traceable hardware & software supply chains enable more defensible products and more agile remediation times –especially amidst variable quality, security, and provenance.
Reduction of Elective Attack Surface & Complexity: There are relationships between security and: complexity, interfaces, attack surfaces, code flaws per thousand lines of code, etc. As such, more secure designs seek to minimize these types of exposure.
Independent,
Adversarial Resilience Testing: Adversarial testing should be carried out by qualified individuals, independent of those who designed and implemented the code. These individuals can be internal resources under a different organizational branch or third-parties.

Third Party Collaboration

A collaboration policy supports a positive, productive collaboration between the automotive industry and security researchers. Researchers are invited to contribute to automotive safety as willing allies to help discover and address flaws before adversaries and accidents can impact vehicle safety. Such coordinated exchanges are more positive, productive, and impactful than other alternatives. Your attestation serves as a commitment and a protocol for teaming.

Do you have a published Coordinated Disclosure policy inviting the assistance of third-party researchers acting in good faith?

Key Elements:

Standard Based: Use of vetted ISO standards for vendor side disclosure practice and for internal vulnerability handling (ISO 29147 and ISO 30111) accelerate an organization's maturity and ensure predictable, normalized interfaces to researchers and facilitators.
Positive Incentives: Positive "Recognition & Reward" systems can further encourage and stimulate participation in bug reporting. Several prominent
"Hackathon," "Hall of Fame," and "Bug Bounty" programs have proven successful and continue to drive iterative improvements. Exemplars can be provided.
Known Interfaces: Independent vulnerability disclosure coordinators have normalized the interfaces between affected manufacturers and third-party researchers. These include non-profits organizations, bug bounty companies and government agencies. This too can support both greater efficiency and greater participation.

Evidence Capture

Safety investigations drive substantial improvements, and records of electronic systems operations give visibility into root causes that may otherwise be opaque. These records can plainly show sources of error, be they malfunctions, design defects, human error or deliberate attack. Those waiting for proof of hacking or electronic sabotage will not find evidence without such logging and evidence collection in place. This capability will require more effort, over time, than others on this list, but it is foundational for improving safety in the long-term so starting now will help us achieve this goal.

Do your vehicle systems provide tamper evident, forensically-sound logging and evidence capture to facilitate safety investigations?

Key Elements:

Logging and Legal Standards: Lowest Common Denominator syntax and verbosity would increase the value within a manufacturer and across the industry. Also, conforming to existing legal standards of care around cyber forensics would be prudent (e.g. for chain of evidence).
Improve effectiveness of NHTSA: The National Highway Transportation Safety Administration (NHTSA) investigates automobile safety issues. In the absence of a "black box" similar to airplanes, these investigations lack full visibility into potential causes of safety issues. Collecting and retaining data as recommended will facilitate their investigations and improve their ability to perform causal analyses.
Privacy Sensitivity: The universal benefits/subset of features of a "black box" can meet its intended functions without requiring privacy and surveillance infractions of citizens across the complexities of various states / countries / jurisdictions. Debates over the capture of data like GPS or other recordings of citizens can be decoupled from safety.

Security Updates

Security flaws require the ability to be remediated in a prompt, reliable manner. If emergent security issues cannot be remediated quickly, the window of exposure is increased and the cost of recall and restitution will grow significantly. The recent HeartBleed flaw put thousands of devices at risk. Without the ability to update software in the field, similar automobile flaws would require carmakers to undertake a costly factory recall or accept the consequences of perpetual, critical security issues.

Can your vehicles be securely updated in a prompt and agile manner?

Key Elements:

Secure Updating System: While updating is a necessary capability, an insecure update design could facilitate adversaries or trigger accidents. Authenticity and quality verification preserves the integrity of the updates and leads to a safer mechanism that can prevent digital tampering or unexpected failures.

Service Level Agreements (SLA): While it is critical to be able to update a vulnerable system, valuable aspects like Mean Time To Repair (MTTR) will vary amongst manufacturers. Those who commit to a faster delivery and/or a higher standard of quality will better ensure safety.

Robust Notification and Communication: Public communication should be transparent and forthright. Decades of experience in the software industry have taught that the best way to ensure security and safety are: notification of when and where flaws exist, their severity, contents of the update, and clear instructions.

Segmentation & Isolation

If systems share the same memory, computing, and/or circuitry, these systems allow for loss of life and limb. Such risks are entirely avoidable and merit a higher standard of care. For instance, a malicious InfoTainment application or a compromise over Bluetooth or wireless should never have the ability to take control over critical functions such as disabling the brakes, deploying airbags, or turning the steering wheel. Hacking the InfoTainment system should never cause an accident.

Do you have a published attestation of the physical and logical isolation measures you have implemented to separate critical systems from non-critical systems?

Key Elements:

"Air Gaps": Physical separation is the only way to ensure that non-critical systems can not adversely impact primary, operational, and safety systems (e.g. Hacking the stereo can never cause a crash). While some manufacturers are planning, discussing, or implementing logical isolation techniques, methods to circumvent these measures are routinely discovered and demonstrated.

System Integrity and Recovery: Techniques exist to indicate when a system has been compromised. Earlier detection can reduce the total duration and extent of the compromise as well as catalyze remediation. In some cases, a "fail safe" or "safe mode" can be an automatic fallback safety mechanism. Any choices should be scrutinized with experienced adversary/threat analysis as they may introduce new attack or denial of service opportunities.

Enhanced Assurance: Given the potential for harm, a higher rigour and level of assurance is merited. Third-party review and validation of architecture, implementation, and adversary resilience testing can raise confidence. Similarly, Operating System choices such as Mandatory Access Control (MAC) architectures reduce risk. "Formal Methods" of engineering and more secure protocols merit consideration. Evaluation examples may be instructive (e.g. "Common Criteria EAL 5+").