August 8th, 2014

An Open Letter to the Automotive Industry: Collaborating for Safety

Dear Automotive CEOs,

We request that you unite with us in a joint commitment to safety between the automotive and cyber security industries.

A hallmark of the automotive industry is extraordinary innovation in the face of market needs. 50 years ago, basic automotive safety features were an afterthought. Since then, the auto industry has steadily driven advances in safety features, safety engineering, and supply chain management in ways that software and cyber security disciplines must emulate.

Now the automotive industry faces a new challenge. Modern vehicles are computers on wheels and are increasingly connected and controlled by software and embedded devices. These new technologies enable innovations designed to increase vehicle safety and bring other positive features. Vehicle-to-vehicle communication, driverless cars, automated traffic flow, and remote control functions are just a few of the evolutions under active development.

New technology introduces new classes of accidents and adversaries that must be anticipated and addressed proactively. Malicious attackers, software flaws, and privacy concerns are the potential unintended consequences of computer technologies driving this latest round of innovation. The once distinct worlds of automobiles and cyber security have collided. In kind, now is the time for the automotive industry and the security community to connect and collaborate toward our common goals.

When the technology we depend on affects public safety and human life, it commands our utmost attention and diligence. Our cars command this level of care. Each and every day, we entrust our lives and the lives of those we love to our automobiles.

The goal of our outreach effort here is to catalyze greater teamwork between security researchers and the automotive industry. Our combined expertise is required to ensure that the safety issues introduced by computer technologies are treated with the same diligence as other classes of automotive safety issues.

Will you join us in this endeavor?

We propose five critical capabilities to lay a foundation for safety, both for collaboration and for increasing consumer confidence. This content was developed jointly with leading cyber security researchers and others working in and around the automotive industry. We crafted these capabilities to be objectively defined, lasting, and to allow for adaptation and innovation within each function.

We urge the automotive industry to adopt, develop, enhance, and attest to these capabilities. Just as they consider other safety features, concerned consumers will be better enabled to make purchasing decisions based on your attestations against these five areas. We will help you navigate this road to build greater protections for your customers and set a new standard for safety.

Five Star Automotive Cyber Safety Program
Further details and explanations can be found at https://www.iamthecavalry.org/auto/5star

1. **Safety by Design**
   VALUE: We take public safety seriously in our design, development, and testing.
   PROOF: As such, we have published an attestation of our secure software development lifecycle, summarizing our design, development, and adversarial resilience testing programs for our products and our supply chain.
2. **Third-Party Collaboration**
   VALUE: We recognize that our programs will not find all flaws.
   PROOF: As such, we have a published coordinated disclosure policy inviting the assistance of third-party researchers acting in good faith.
3. **Evidence Capture**
   VALUE: We want to learn from failures and enable continuous improvement.
   PROOF: As such, our systems provide tamper evident, forensically sound logging and evidence capture to facilitate safety investigations.
4. **Security Updates**
   VALUE: We recognize the need to address newly discovered safety issues.
   PROOF: As such, our systems can be securely updated in a prompt and agile manner.
5. **Segmentation & Isolation**
   VALUE: We believe a compromise of non-critical systems (like entertainment) should never adversely affect critical/physical systems (like braking).
   PROOF: As such, we have published an attestation of the physical/logical isolation and layered defense measures we have implemented.

We are eager to start working with you within the next 90 days and to begin promoting your current and future capabilities to the public. These attestations establish a foundation and serve to catalyze an ongoing collaboration to better prepare us for the next 50 years and beyond. Given our research and experience to date, we are encouraged to see some early investments toward these capabilities. While capabilities like evidence logging will take time to bring to market, valuable policy and capability attestations can begin now. On this journey, the challenges will be many and they will be significant, but together and through collaboration we can rise to meet them. Let's start now.

Respectfully,

"I am The Cavalry", members of the security research community, & concerned citizens
Signatures and instructions for signing can be found at https://www.iamthecavalry.org/auto/5star
Signatures are solely the opinion of the individual.