Toward Tomorrow’s “Organically Secure” Vehicle

Autonomy promises to be one of the most significant safety mechanisms the world has ever built. But autonomy and security go hand in hand; autonomy and trust exist in equal measure. If we trust the autonomous technology in the vehicle, we will deploy it widely, and, if we do not, it will remain a laboratory curiosity. Trust depends crucially on security in and around the car. Simply stated, the more we trust in the safety and security of self-driving cars, the more we will use them, and the more society will benefit.

FASTR believes that we collectively have the opportunity, and responsibility, to rearchitect the vehicle in such a way that cybersecurity is at its very foundation. This must be coordinated across the entire, evolving automotive supply chain. We believe that tomorrow’s connected and automated vehicles should be “organically secure”—systematically more able to deal with inevitable cybersecurity threats in a safe and predictable manner and, ultimately, to self-heal.

Accelerating the realization of tomorrow’s organically secure vehicles demands tangible research deliverables today—reference architectures, proofs of concept and other theoretical and applied research—that would help automakers reduce risks and liabilities, foster trust in autonomous vehicles and accelerate the safety and quality-of-life benefits that these vehicles promise. FASTR supports inclusive, diverse, multifaceted cybersecurity research collaboration across the evolving automotive ecosystem. We recognize that automotive security is not a problem that can be solved by a single organization or technology or in silos—and that the magnitude and scope of the emerging challenges demand no less than an industry-wide response.

The Shared Challenge

Today software is wrapped around the vehicle. Tomorrow’s automobile will be built around software. This has profound implications for the auto industry, the ecosystem that supports it and the way vehicles will be built. The automobile of the future will have a significantly expanded cyber-attack surface. Focus on automotive security will continue intensifying rapidly among industry and government.

All existing security technologies have evolved to address the emerging threats of their time, and we can expect automotive security to do so as well. But it is also true that public safety could be jeopardized, and breaches and awareness of potential security issues could inhibit deployment of autonomous vehicles and realization of their potential benefits, without a substantially more concerted and coordinated effort in cybersecurity today. The risk is with slowing the adoption of the revolutionary societal benefits from autonomous driving: dramatic reduction in accidents, alleviation of city congestion, mobility for all, and more. The unprecedented adoption of technology into modern vehicles without rigorous Security Design Lifecycle methodologies applied in a “system-of-systems” approach will create unacceptable risks.

Vehicles today are undergoing dramatic transformation of software, content, connectivity, services and autonomy. Forecasts call for 250 million connected cars on roadways by 2020. Analysis points to the market for partially and fully autonomous vehicles to approach $77 billion in 2035, with perhaps 12 million fully autonomous units being sold annually around the world. And — as documented in “Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk,” a report based on responses from 16 major automobile manufacturers to questions from U.S. Sen. Ed Markey in 2014 — nearly all cars have vulnerable wireless technologies, and almost all access points of the vehicle can be compromised.3

We are moving from a current state of limited but expanding vehicle connectivity (telematics, infotainment, etc.) to a highly complex, fully connected environment including vehicle to vehicle (V2V), vehicle to infrastructure control (V2I), or, more generally, vehicle-to everything (V2X). The wireless interfaces on modern vehicles have evolved to include all of the conveniences that modern life demands, such as Wi-Fi, Bluetooth, cellular, global positioning system (GPS), digital broadcast radio and even tire-pressure monitor systems.

A pervasive, highly developed state of vehicle automation is taking shape. Along the way, the connected vehicle will rely more and more on external systems and networks to support new services and interactions. In addition, while today's telematic data analytics primarily concentrate on vehicle performance and location, tomorrow's will be focused on highly sensitive consumer experience and personal data (e.g., advanced multi-factor authentication including 3D facial recognition, passengers in attendance, contextual voice processing records, payment history and details, location, driving habits, V2X communication records, etc.).

These are seismic shifts that the automotive ecosystem is undertaking, calling up significant, interrelated requirements for trust in security:

- Trust in data confidentiality—Vehicle and operator data must not be divulged without the permission of the operator.
- Trust in data and system integrity—Vehicle and operator data must not be compromised or altered.
- Trust in data and system availability—Vehicle and operator data must be available to the systems and services that rely on them.

Today’s modern luxury vehicle contains more than 100 million lines of code and is approaching 100 Electronic Control Units (ECUs) within the vehicle. While the industry labors mightily to fuse together automotive security across this exploding and complex architecture, the challenge clearly expands beyond the borders of any one software application or hardware chip alone in addressing the growth of tremendous security vulnerabilities.

To deliver on the requirements for multi-layered, seamless trust and security—and arrive at the essential organically secure vehicle—two strategies are key. First, the complexity of today’s vehicle must be comprehended in layers: communication channels must be protected among vehicles and devices, within the communications infrastructure and within the data center. Second, recognizing that automotive original equipment manufacturers (OEMs) rely on complex supply chains, these supply chains must be organized to align with best practices for security and production of verifiably trustworthy technology components. The automotive security challenges demand both a deep and wide solution.

---

What can be done?

• **Defense in depth** — Threat modeling, vulnerability assessment, security architecture, trusted supply chains and cybersecurity assurance are needed throughout all layers of automotive security:

  • **In-vehicle systems** (platform boot integrity and Chain of Trust, secure storage for keys and data, secure communication, secure debug, tamper detection and protection from side channel attacks, etc.)

  • **Connectivity and the cloud** (fast cryptographic performance, device identification, isolated execution, message authentication, etc.)

  • **End-to-end use cases**, automated driving (over-the-air updates, intrusion detection and prevention systems, anomaly detection, network enforcement, certificate-management services, anti-malware and remote monitoring, biometrics, etc.)

• **Hardware security features** — Multi-layered defense in depth demands security features in the silicon. Hardware-hardened, trusted execution environments, secure boot, secure key storage, crypto accelerators, hardware virtualization, etc. are critical to the overall security integrity of the vehicle architecture.

• **Vehicle Security Design Lifecycle** — It is critical that formal and predictable processes be implemented to ensure compliance to security policies. An intentional and proactive approach to consolidation and interconnection of vehicle systems must be present from the outset of design, and it must continue right through to the production and operation stages. Best practices for production processes must contribute to design components being correctly implemented. Code reviews, component-and system-level penetration tests, continuous validation of security assumptions, inbound and outbound materials processes, maintenance and upgrade plans and feedback loops for continuous learning and improvement are key for clearly linking implementation back to secure design properties.

• **Threat intelligence** — Threat analysis and risk assessment must continue throughout the life of tomorrow’s organically secure vehicle. Techniques such as over-the-air software or firmware patches and upgrades can help quickly close vulnerabilities (and significantly reduce recall costs). Threat intelligence can help prioritize cybersecurity threats by associated risk and illuminate appropriate incident response.

The Evolving Automotive Ecosystem: A Unified Approach

Automakers have a long history of working together (sharing antenna, battery and powertrain technologies, for example), and significant activity is taking place across the growing automotive ecosystem, with communities of interest developing and rallying around various aspects of the security challenges. Still, the cast of contributors in the automotive ecosystem is rapidly evolving, and, until now, coordination has been poor across the increasing diversity of players.

Whereas automotive OEMs are experts at building cars through supply chains, they traditionally have not looked at the car as a system (or as software) in the way that advanced cybersecurity, machine-learning, communications or autonomous-carsharing experts might.
The autonomous space, with its increased reliance on software and connectivity, is rapidly expanding the traditional automotive ecosystem to include a broader group of companies than ever, and a unified approach across all of them through technology-sharing initiatives is necessary for automotive security. A holistic, systems-level approach across the full cast of contributors to the organically secure vehicle of the future is required:

- OEMs
- Transportation network companies
- Automotive supply chain providers (Tier 1s and Tier 2s)
- Autonomous vehicle specialists
- SoC providers and hardware and software suppliers
- Specialist automotive security companies
- Academics, researchers and hackers

Enabling Innovation in Automotive Security, FASTR

FASTR (Future of Automotive Security Technology Research) seeks to enable innovation in automotive security by delivering the actionable applied and theoretical R&D needed now to ensure trust in the connected and autonomous vehicle of the future. FASTR brings together the auto industry veterans and disruptors, technology giants and startups, academics and hackers from across the evolving automotive supply chain delivering advanced concepts, to drive the agile, iterative research that the automotive ecosystem needs today. Founded by Aeris, Intel Security and Uber in 2016, and formerly known as the "Automotive Security Review Board," FASTR will:

- Deliver pre-competitive technological building blocks, such as white papers, reference architectures, code samples, workshops and best-known methods that automotive OEMs can customize and use to drive requirements across their supply chains.
- Study future automotive cyber-physical security risks, identify mitigating technologies and solutions and publicly and privately share critical findings and recommendations to the industry.
- Collaborate with like-minded organizations worldwide to help the automotive industry get in front of next-generation security risks and technologies making the world a safer place.
- Help the automotive industry get cybersecurity right, from the beginning.

Call to Action

Join us. FASTR seeks to collaborate with complementary, like-minded organizations and individuals worldwide. Your expertise, input and perspective are needed as FASTR marshals industry-wide collaboration on the creation of future architectures and greenfield approaches—not temporary fixes to legacy solutions—to ensure the safety and security of autonomous vehicles and connected cars moving forward. Get involved today.

Email: info@fastr.org, visit fastr.org and connect with us at @FASTR_org.