IBM Institute for Business Value

Driving security

Cyber assurance for next-generation vehicles

Automotive industry leadership

IBM has a long history of helping industry after industry capitalize on complex systems and transform businesses. As a global manufacturer ourselves, we understand the issues that automotive companies face. Our automotive industry solution portfolio for product and complex system development, advanced mobility, manufacturing productivity and service excellence has been developed and continuously refined through implementations with clients around the world, ranging from secure chip assurance to top-level business consulting. IBM has partnered with the automotive industry for many years, helping transform its organizations and create new business opportunities while satisfying customer expectations—the biggest and most important driver of change in the automotive industry.

By Christopher Poulin

Today's instrumented and intelligent

automobiles offer a plethora of driver features—from creature comforts like synching smart phones with vehicle systems to safety features like emergency assistance systems and real-time driver alerts. Connected vehicles also offer advantages for automakers, such as the ability to proactively detect and respond to warranty and maintenance issues. However, along with these advances come the risks associated with system and vehicle security breaches, as well as concerns over data privacy. To mitigate such threats, the automobile industry must continue to make security a top priority by building protection against computer incursions. In fact, digital security must be infused into every step of the manufacturing process—from design through production, the supply chain and the maintenance ecosystem.

Researchers have proven that modern, computerized **vehicles can be hijacked** with just a laptop computer and easily obtained software.

Manufacturers should **review the end-to-end architecture** for connected vehicle solutions to identify threat vectors, attack surfaces and design actions to protect the vehicle, occupants and service providers.

The **integrity of the entire automotive supply chain**, including all hardware and software components, should be analyzed and monitored leveraging standards and best practices.

For over a hundred years, automobiles have been isolated machines of metal and motor with the single purpose of transporting passengers and cargo from one place to another. Over the past 50 plus years, the automotive industry has adopted electronics and information technology to meet regulatory requirements for safety, emissions control and fuel efficiency; improve diagnostics; and satisfy market-driven requirements for comfort, convenience, communications and entertainment.

With the advent of a perpetually connected society, people naturally expect to expand the digital experience into their vehicles. Consumers want to play music from their smart phones through their car speakers, make hands-free phone calls with information displayed on their dashboard, start their engines and warm up or cool down the cabin while still in line at the grocery store and more. In effect, car owners want their vehicle to become a personal node on a network of rolling, connected devices. And automakers have a complementary interest in monitoring vehicles remotely to proactively detect and respond to warranty and maintenance needs.

But this functionality comes with risks and potentially fatal consequences. Researchers have already proven that modern, computerized vehicles can be hijacked with just a laptop computer and easily obtained software. Hackers have demonstrated that they can display false telemetry on the dashboard, wrest the steering away from the in-cabin driver and even apply the brakes or switch off the engine remotely when the vehicle is at high speed on a crowded freeway.[1] A British company has demonstrated a prototype device capable of stopping cars and other vehicles using a blast of electromagnetic waves.[2] It's only a matter of time before malicious hackers determine a financial incentive or political motive to turn what is now a parlor trick into a widespread threat to the global transportation system. Just as hacking commercial systems has evolved from nuisance activities conducted by disenfranchised teenagers to highly profitable cybercriminal enterprises, the same—unfortunately—can be expected with automobile hacking.

In addition to safety dangers, drivers and passengers face security and privacy threats. Private information on smart phones, such as e-mail, text messages, contacts and other personal data, could be stolen by intruders or hackers. Burglars could use vehicle location, provided by global positioning systems (GPS), to ensure a home's occupants are still miles away, giving the thieves confidence to conduct a thorough search for valuables to maximize their take.

The challenge for the automotive industry is multifaceted: the component technologies are complex, the integrated vehicle is complex, the in-service lifetime is long, the underlying supply chains are complex, and the vehicle operating environment is laden with threats.

Because many of the technologies involved in the connected vehicle are new for the automotive industry—and the technologies themselves are still evolving—there are associated security risks for consumers and manufacturers. At stake is damage to an automobile manufacturer's brand reputation and ensuing negative impact to the customer perception, theft of customer data (and possibly identity), and the potential for injury or loss of life.

Automobile manufacturers, dealers, repair persons and end users must adapt to new technological concepts and production methods, not just to ensure the safety, efficiency and comfort of automobile drivers and passengers, but also to ensure their privacy and data security. They must continue to make safety a top priority, but must now include protection against computer incursions.

At IBM, we have worked with the top manufacturers of automobiles, automotive components and services around the world to understand the risks and threats to instrumented, connected, intelligent vehicles, so we can devise practices to help ensure safety and security. The result is a security model that follows modern vehicles from rough sketch to scrap metal, which we call **design, build, drive** (see Figure 1).

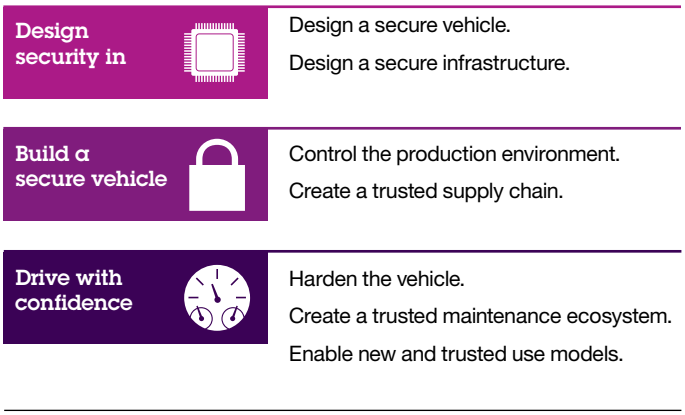

Figure 1: Design, build, drive: Help ensure safety and security throughout the entire lifecycle process.

Design security in

Design a secure vehicle

Research and development (R&D) for connected vehicles occurs across several organizations and teams over multiple years. To develop complex systems with security in mind, the R&D environment needs to be secure and certified to adhere to relevant standards, and practices for secure engineering need to be enforced. These requirements carry across the entire supply chain.

The design point for security should include:

- Adherence to technical standards such as ISO26262, AUTOSAR, MISRA and Automotive SPICE[3]
- Establishment of a security methodology for design and development
- Maintainability over long in-service lifetimes
- "Fail safe" contingencies
- Assertions related to trusted technology providers[4]
- Trust assertions and mechanisms for software.

The design process should include a security focus from the outset and a baseline statement of risks and threats for each component, subsystem and network in the connected vehicle. The means and methods of testing the range of threats that may be exposed in the in-service life of the connected vehicle must be defined and exercised. Because of supply chain complexity, the threat model should ideally be available to the entire design team.

Each software and hardware component and system should be designed with security as a first-order requirement. As the vehicle is assembled into a system of systems, integration introduces additional threats by expanding the points of exploitation. The consolidated security test plan should reflect the union of the results.

Each component and system should be designed with security as a first-order requirement.

Design a secure infrastructure

Connected vehicles allow passengers to interact with them, while in the cabin or across the world. For security, the communications between the vehicle and a remote user are mediated by the service provider, often the automaker. The communication should be encrypted and impervious to tampering. In addition, the service provider needs to protect its network and monitor transactions to detect suspicious activity.

The manufacturer's network should uniquely identify and authenticate users and control access to remote services such as starting or stopping the engine, unlocking the vehicle and applying the brakes. Manufacturers must also carefully protect sensitive information like GPS coordinates and consumer personally identifiable information (PII).

Infrastructure components, such as connected traffic lights and toll lanes, should also be secured from tampering. For example, someone could wreak havoc by falsifying traffic conditions and rerouting all vehicles to a surface road when there is, in fact, no traffic jam on the main artery. Worse, all cars on a road could be forced to brake suddenly as a result of a critical—but false—message informing each vehicle it's about to rear-end the one it's following. Fraud is also a concern. For example, cyber criminals could falsify infrastructure components and collect forged toll payments.

Build a secure vehicle

Control the production environment

Manufacturing plants have become increasingly automated and reliant on information technology to increase productivity and quality. The automotive industry has been one of the greatest innovators and initial beneficiaries in the use of automated assembly, as well as data analytics in quality control to drive down defects.

The integrity of the IT and production systems and the facilities themselves must be assured; if a control system is compromised by malware, the very machines designed to produce automobiles efficiently and with exacting standards can be coerced into introducing flaws into the final product. The end result could be injury to the operators of the vehicles, brand reputation damage to the automakers, or theft of intellectual property and practices.

Assembly plants contain standard IT systems, like servers, workstations, networking equipment and storage devices. They also operate industrial control systems. While there are well-understood security controls for standard IT systems, including authentication and access control, firewalls and endpoint protection, industrial control systems often run on antiquated or esoteric operating systems, contain hard-coded administrative credentials, or are simply not well understood by IT professionals. Nevertheless, industrial control systems need to be protected from electronic subversion to avoid threats, such as Stuxnet, a 500-kilobyte computer worm that infected the software of at least 14 industrial sites in Iran.[5]

Secure production environments and trusted supply chains are crucial to building a secure vehicle.

To secure production assembly, automakers should:

- *Understand the functions, applications, interfaces and protocols associated with each system used in manufacturing.* In effect, keep a current asset inventory of critical cyber assets, including system owners, authorized roles and users, and interaction with other information system assets.
- *Have a codified security policy that guides implementation and maintenance of critical assets.* The security policy must take into account availability of systems and data, as well as integrity and confidentiality.
- *Implement access and security controls to protect the equipment and data*, guided by the security policy.
- *Instrument systems to monitor events and perform analytics* to detect not only failures, but also suspicious activity potentially indicating a security threat.

Create a trusted supply chain

Two key security tenets, integrity and availability, have critical impact on the automotive supply chain.

Integrity of automotive components means preventing counterfeit or malicious components that jeopardize the vehicle's quality or safety from entering the vehicle parts supply chain. To help ensure hardware and software component integrity, manufacturers need to consider a number of questions: Where did the component originate? Who has had access to it since it was created? Has the component been tampered with or altered? Assurance of components should occur before the parts are shipped to the factory, during shipment and upon arrival, again after the car is completed but before it reaches the dealer, and even after the owner has purchased the car.

Because cars are built with components that are created all over the world and shipped to manufacturing plants, availability is also crucial. When the earthquake and tsunami off the coast of Tōhoku devastated parts of Japan, the impacts to the automotive industry were felt far outside of Asia. In addition to factory shut downs in Japan, companies worldwide suffered power cuts and parts shortages. Even the Swedish carmaker Volvo and Detroit's General Motors stopped some production because of parts shortages.[6] IT system outages can also affect availability. Often due to the unintended consequences of a misconfiguration or coding error, such outages can be as devastating as natural disasters, shutting down production and shipping.

Securing the integrity and availability of the global automotive supply chain is complicated by the distributed manner in which components are created and by joint ventures. Two (or more) supply chains must be integrated without loss of integrity or availability or other negative impact on the manufacturing process.

Standards can help automotive manufacturers secure their supply chain, such as the International Organization for Standardization's ISO 28000:2007, which specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain.[7] And the Automotive Industry Action Group (AIAG) has a working group specifically focused on the security of the automotive supply chain.[8]

Two government initiatives that automotive manufacturers can get involved in to help manage integrity in the supply chain are the U.S. Customs Trade Partnership against Terrorism (C-TPAT) and Canada's Partners in Protection (PIP).[9] Both voluntary, these programs focus on improving the security of the supply chain with respect to terrorism.

When companies join C-TPAT they sign an agreement to work with the U.S. Customs and Border Patrol to protect the supply chain, identify security gaps, and implement specific security measures and best practices.[10] Similarly, the Canada Border Services Agency (CBSA) program, PIP, enlists the cooperation of private industry to enhance border and trade chain security.[11]

Another goal of these standards and working groups is to implement controls throughout the process and support "trusted" trader programs to improve security and integrity of components in the chain without slowing down manufacturing speeds.

Drive with confidence

Harden the vehicle

In the 1950s and '60s, it took a mechanical engineer to design vehicle control systems; now it takes a computer scientist. Today, many vehicle control components are computer controlled by up to 100 million lines of software for a high-end car.[12] The magnitude of vehicle software compared to other well-known things illustrates the true complexity of the vehicle (see Figure 2). This software is managed by anywhere between 70 to 100 Electronic Control Units (ECUs), which are connected to many Controller Area Networks (CANs).[13] The prevailing security model to date has been that vehicle control systems exist in a closed environment.

However, the threat surface has expanded beyond the chassis to the global Internet as many vehicles are now outfitted with Bluetooth, USB ports and even near-field communications sensors, allowing passengers to play music through the vehicle's entertainment system, make and receive calls hands free, pay for purchases from within the car and even customize dashboard gauges. Car manufacturers provide remote safety and assistance services over mobile networks (e.g., General Motors OnStar, BMW Assist, and Lexus Link), and any hobbyist can now "jack in" to or hack vehicles through the On-Board Diagnostics (OBD-II) port.

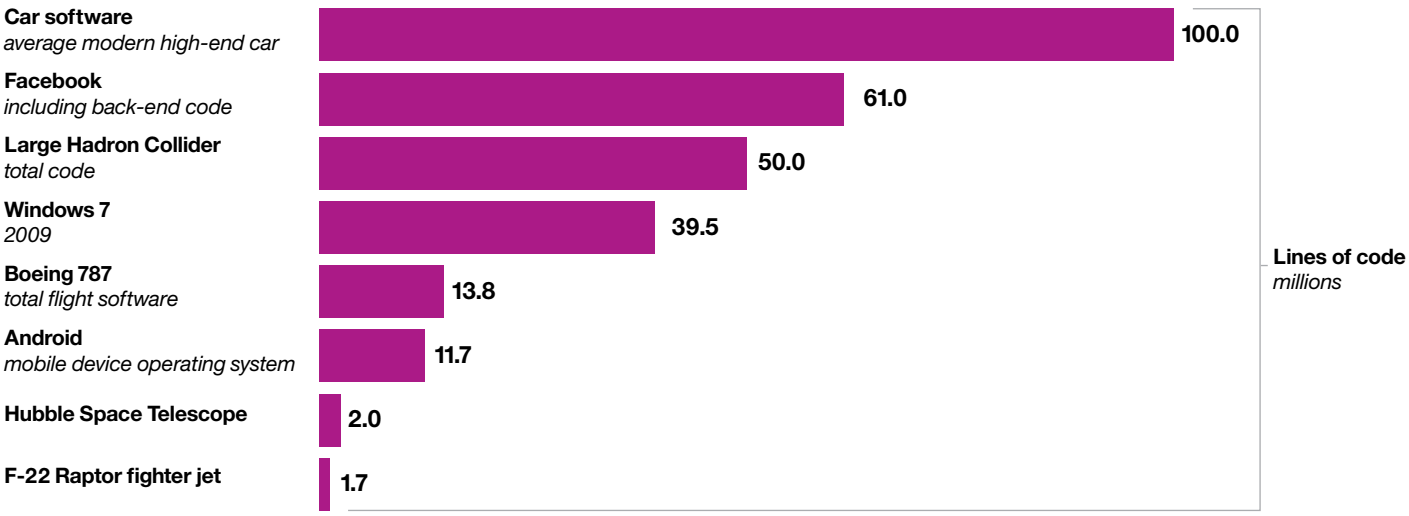

Figure 2: Even at 100 million lines of code, software in cars is only going to grow in both amount and complexity.

Source: "Codebases." Information is Beautiful website. http://www.informationisbeautiful.net/visualizations/million-lines-of-code/; Charette, Robert N. "This car runs on code." IEEE Spectrum. February 2009. http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code

Even seemingly harmless functions employ wireless technology, such as the Tire Pressure Monitoring System (TPMS), which communicates telemetry between sensors in the tires to the vehicle's control network.[14] These communications channels change the vehicle threat profile, giving attackers many choices to gain access to the vehicle's electronics. It's not only wireless networks that expose the vehicle to attack: it's been proven possible to infect the vehicle by inserting a CD or USB drive containing malware, which can modify firmware on ECUs. Firmware over the air (FOTA) or remote updates to ECUs and other components must also be protected from tampering that could compromise the safety and security of the vehicle and its occupants.

We suggest systematically analyzing and mitigating the external attack surface of a modern automobile, as well as ensuring proper design, integration, testing and maintenance.

To provide a safe travel experience for drivers, passengers and pedestrians alike, a technology redesign is necessary at the ECU level. Such a redesign should:

- *Protect the ECU:* Validate the integrity of ECU firmware to resist unauthorized tampering or execution of malware.
- *Protect the CAN bus:* Provide a method allowing an ECU to verify the identity of other ECUs on a network bus, decide which controls and messages they are allowed to send, and validate that those controls and messages haven't been tampered with or forged.

- *Secure data flowing to, from and within the vehicle:* Protect sensitive or personal information from being captured in transit by encrypting data over the air and on the CAN. Encryption can also help prevent hijacking and spoofing of control commands.
- *Analyze data patterns:* With sophisticated attacks, it's not always possible to prevent malicious activity. However, instrumenting and analyzing data patterns from individual cars and fleets can detect anomalies that may be signs of coordinated attacks. By generating meaningful events in a format useful to big data solutions, analytics can identify suspicious activity before the vehicle's systems are compromised and the attacker causes damage.

Create a trusted maintenance ecosystem

Before a new connected vehicle owner first sits behind the steering wheel, a number of preparatory steps for final delivery should be accomplished, including updating electronics and ECUs with the most current software and firmware and setting up access with maintenance and support services, as well as third-party, value-add services and subscriptions like traffic and weather feeds.

Initial personalization of connected vehicles is most straightforward when the vehicle is privately owned. Fleet, rental and on-demand vehicles may have limited functionality if mobile devices need to be registered with the auto manufacturer before the operator can use them for even basic functions such as unlocking the vehicle. Re-setting or re-initializing personalization and device pairing when vehicles are sold and bought during their lifetime may be problematic if the manufacturer or authorized dealership is not involved. At a minimum, these situations could result in inconvenience; at worst, the accident or emergency notification system could be inoperable.

Once the vehicle is in service, automakers have the opportunity to leverage the connected vehicle infrastructure to provide preventative updates and upgrades to the software and the services mentioned, as well as functional upsells. On one hand, automatic updates can help close off security vulnerabilities and keep vehicle owners safe from electronic threats; yet, ironically, the mechanism that provides this capability, over the air updates, increases the vehicle threat surface.

During a vehicle's in-service life, owners and operators may interface with a wide range of computing systems and computing services in support of maintenance, customer support or value-added services, such as satellite radio, etc. These systems can contribute to security and privacy risks by exposing information or points of service access.

Finally, automobile manufacturers need to account for upgrades to cryptographic software and data during the in-service lifetime of connected vehicles. Vehicle security and privacy are dependent on cryptographic services and the underlying keys, algorithms and digital certificates, which all must be updated regularly.

Enable new and trusted use models

The introduction of intelligent, sustainable vehicles is redefining personal mobility around the world. To stay competitive and differentiated in the market, automakers have created open, scalable and flexible mobility services that are customizable. They're also paying attention to "non-car owners" who opt for alternate mobility services like public transportation and car-sharing. Car2go, offered by moovel GmbH (a fully-owned subsidiary of Daimler AG and a division of Daimler Financial Services AG), is a unique car-sharing service that allows members to rent vehicles by the minute and return them to open parking spaces in designated areas. The company is also introducing electric cars with recharging stations at convenient locations.[15]

These types of programs offer a variety of benefits:

- Using electric vehicles for short-distance transport is ecologically sound.
- Keeping vehicles on the go as much as possible reduces long-term parking, a waste of precious urban real estate.
- Producing smaller vehicles to accommodate the many single-passenger transportation needs further supports vehicle density.

But with the benefits come risks. Consumers must be able to immediately find free vehicles within a short walking distance, reserve those vehicles and pay, all using mobile devices. In addition, information must be shared with third parties such as utility companies, local and national government, and telecommunications and technology providers to ensure a positive user experience. The hand-off points require careful control to ensure only information that's needed is shared and to prevent unauthorized access to that information. In addition to customer privacy concerns, there are also concerns related to systems compromises since portals to these services must exist on the public Internet. And because the networks all share some level of trust, a breach of one entity may open up transitive, malicious access to all connected enterprises.

Another security concern is that vehicles are no longer controlled by a single owner or family. The shared nature of urban mobility services means that a previous occupant has the opportunity to subvert the vehicle's information and control systems. At best, they may eavesdrop on phone calls, text messages and passenger conversations; at worst, they may sabotage the vehicle's control systems to cause harm to subsequent occupants.

Automakers must take these security scenarios into consideration and ensure that both intra-vehicle systems and inter-vehicle communications are designed to detect and resist suspicious activity.

Offering drivers personalized features—and peace of mind

A global provider of automobiles wanted to enter the connected vehicle market and provide secure, personalized access to vehicle information services on customer mobile devices. These services included access to radio, Internet and social networks from the vehicle telematics systems.

The solution integrates strong authentication and authorization of consumer devices with the vehicle and automaker's service network, providing assurance to vehicle owners that their convenience does not introduce safety or privacy dangers. Policy-driven security is also provided at the service network portal. And, because the service ecosystem is complex, the solution offers secure integration and federated single sign-on with third-party service providers using industry standards.

The rapid and secure integration of consumer and partner services will continue to scale as the automaker gains broader consumer adoption and provides the flexibility to accommodate new offerings to keep pace with customer demands.

Steps to take immediately

- *Assess the design and development processes.* While safety is job one, connected vehicle security is a fundamental requirement to ensure not just safety, but also privacy. Review the end-to-end architecture for connected vehicle solutions to identify threat vectors, attack surfaces and design actions to protect the vehicle, occupants and service providers. Focus on a system-of-systems approach for development by considering security across all aspects of engineering: software, electrical and mechanical. Use strategic reuse to reduce risk of non-secure components.
- *Review the IT production and in-service IT infrastructures.* Assembly lines and the infrastructure used to communicate with connected automobiles once they're on the road are supported by traditional IT networks and systems. Risk assessments and design reviews provide confidence that the infrastructure is resilient to attack and reinforced by appropriate IT security technology.

- *Assess the supply chain.* The integrity of the entire supply chain, including all hardware and software components, must be analyzed and monitored. Standards and best practice guides should be leveraged in this process.
- *Apply analytics solutions:* Apply big data analytics to identify attempted attacks on vehicle control and telematics systems, preserving the safety and privacy of the driver.

Conclusion

Connected vehicles are intended to be designed and built with security as a foundational requirement. However, vehicles are no longer islands of electro-mechanical engineering; rather, they are components of a larger system of systems, which integrates the vehicle, roads, manufacturer and consumer to provide a safe, secure transportation experience.

Much as they expect anti-lock brakes, airbags and seat belts as standard features rather than aftermarket or retrofitted options, today's consumers demand digital security that is delivered unobtrusively with the vehicle. This realization will drive new revenues for forward-looking suppliers and manufacturers, as well as decreased costs for consumers and original equipment manufacturers. Those that can deliver the safety and convenience features consumers desire while also assuring their safety and security stand to leverage the true power of the connected vehicle.

To learn more about this IBM Institute for Business Value study, please contact us at iibv@us.ibm.com. For a full catalog of our research, visit **ibm.com**/iibv.

Access IBM Institute for Business Value executive reports on your tablet by downloading the free "IBM IBV" app for iPad or Android from your app store.

About the author

Christopher Poulin is a Research Strategist with IBM's X-Force security research group. He focuses on emerging technologies and the threats to their security, organizational privacy and consumer safety. He has over 25 years of experience in information security, beginning in the U.S. Department of Defense and spanning a variety of roles from software development to building a boutique security consultancy. Christopher is currently focused on threat intelligence and security for the Internet of Things, including connected vehicles. He can be reached at cpoulin@us.ibm.com.

Contributors

John Cohn, IBM Fellow, Corporate Technical Strategy

Sebastian Wedeniwski, IBM Distinguished Engineer, CTO Global Automotive Industry

Michael Rowe, Program Director, Connected Vehicle and Internet of Things

Diana Kelley, Executive Security Advisor, IBM Security Systems, IBM Software Group

Jim Whitmore, Open Group Certified Distinguished Architect, IBM Software Group Architecture & Technology, Secure Engineering Initiative

Ben Stanley, Global Automotive Lead, Institute for Business Value

IBM Institute for Business Value

IBM Global Business Services, through the IBM Institute for Business Value, develops fact-based strategic insights for senior executives around critical public and private sector issues. This executive report is based on an in-depth study by the Institute's research team. It is part of an ongoing commitment by IBM Global Business Services to provide analysis and viewpoints that help companies realize business value. You may contact the author or send an e-mail to iibv@us.ibm.com for more information.

References

1 Seabaugh, Christian. “Video find: Watch hackers hack into Toyoto Prius, Ford Escape.” Motor Trend. July 25, 2013. http://wot.motortrend.com/video-find-watch-hackers-hack-into-toyota-prius-ford-escape-389065.html

2 Vallance, Chris. “RF Safe-Stop shuts down car engines with radio pulse.” December 3, 2013. BBC News. http://www.bbc.co.uk/news/technology-25197786

3 ISO: International Organization for Standardization (www.iso.org); AUTOSAR: AUTomotive Open System ARchitecture (http://www.autosar.org/); MISRA: The Motor Industry Software Reliability Association (www.misra.org.uk); Automotive SPICE: Software Process Improvement and Capability Determination (www.automotivespice.com).

4 In the absence of an automotive industry specific standard and accreditation process, consider the Open Trusted Technology Provider Standard and accreditation process, OTTP-S, defined by The Open Group.

5 Kushner, David. “The real story of Stuxnet.” IEEE Spectrum. February 26, 2013. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

6 Glinton, Sonari. “Japan Disaster Breaks Auto Supply Chain.” The European Institute. http://www.europeaninstitute.org/Documents/japan-disaster-breaks-auto-supply-chain.html

7 “ISO 28000:2007, Specification for security management systems for the supply chain.” International Organization for Standardization website, accessed June 4, 2014. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=44641

8 “Customs/Supply Chain Security.” AIAG website, accessed June 4, 2014. http://www.aiag.org/staticcontent/committees/workgroup.cfm?FC=SC&grp=Customs&group=SCSI

9 “C-TPAT: Customs-Trade Partnership Against Terrorism.” U.S. Customers and Border Protection website, accessed June 4, 2014. http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism; “Partners in Protection.” Canada Border Services Agency website, accessed June 4, 2014. http://www.cbsa-asfc.gc.ca/security-securite/pip-pep/menu-eng.html

10 “C-TPAT: Customs-Trade Partnership Against Terroism.” U.S. Customers and Border Protection website, accessed June 4, 2014. http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism

11 “Partners in Protection.” Canada Border Services Agency website, accessed June 4, 2014. http://www.cbsa-asfc.gc.ca/security-securite/pip-pep/menu-eng.html

12 “Codebases.” Information is Beautiful website, accessed June 4, 2014. http://www.informationisbeautiful.net/visualizations/million-lines-of-code/; Charette, Robert N. “This car runs on code.” IEEE Spectrum. February 2009. http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code

13 Charette, Robert N. “This car runs on code.” IEEE Spectrum. February 2009. http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code

14 Rouf, Ishtiaq, et al. “Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study.” http://www.winlab.rutgers.edu/~Gruteser/papers/xu_tpms10.pdf

15 Car2Go Web site, accessed June 10, 2014. https://www.car2go.com/en/austin/; “Daimler launches all-electric Car2Go carshare service.” Mother Nature Network. November 27, 2011. http://www.mnn.com/green-tech/transportation/blogs/daimler-launches-all-electric-car2go-carshare-service#. “moovel GmbH.” moovel website, accessed June 19, 2014. https://www.moovel.com/en/US/about-us.html

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
June 2014

Please Recycle

GBE03610-USEN-00