BY BRAD BARTON + SAJAY RAI EDITED BY STEVE MAR

WHO SHOULD AUDIT THE CONNECTED CAR?

Today's high-tech vehicles pose complex risks beyond the driver's control.

Connected cars that alert drivers to potential dangers or even automatically brake to avoid them promise greater automobile safety and efficiency. But the risks these advanced vehicles pose shift dramatically from driver attention and road hazards to cyber threats and the integrity of vehicle control systems. This threat was demonstrated when researchers were able to remotely take control of environmental, entertainment, and engine systems on a 2014 Jeep Cherokee.

Assessing related risks and controls is similar to other technology development initiatives. Internal auditors for automakers, equipment manufacturers, and business and government customers should learn the basics about connected cars and what can be done to address their risks.

Internal Connections

By definition, connected cars are linked to internal and external systems and services. Inside the vehicle, there's the Controller Area Network (CAN) bus that links internal micro-devices such as the engine control unit, transmission, braking, and diagnostic systems to various monitoring and control systems. This structure was originally developed in the early 1980s to accommodate the growing number of connected components while reducing the amount of wiring needed to connect onboard components. CAN relies on a serial bus protocol for message transport, fault/error detection, timing, etc. Because the CAN protocol does not support security, security must be designed into devices connected to the bus. As such, a security review should be part of any audit of devices connected to the CAN bus.

Also internal to the vehicle are physical ports for diagnostic and peripheral connections. On-board diagnostics (OBD) is a physical connection present in all vehicles produced since the early 2000s. OBD provides a standard connection for service technicians to attach diagnostic equipment and read status and error code information generated by sensors on the vehicle. OBD's direct access to the vehicle's internal sensors and control devices could make this connection susceptible to exploit.

Another risk is the Universal Serial Bus (USB) connectors that are common on many entertainment systems found in newer vehicles. These interfaces not only support streaming audio for entertainment, but they also can be used to update engine and system controls software. Given reports of how USB ports can be compromised, auditors should consider related risks in their connected car program.

External Connections

Moving on to external connections, the automotive industry has been developing wireless communications

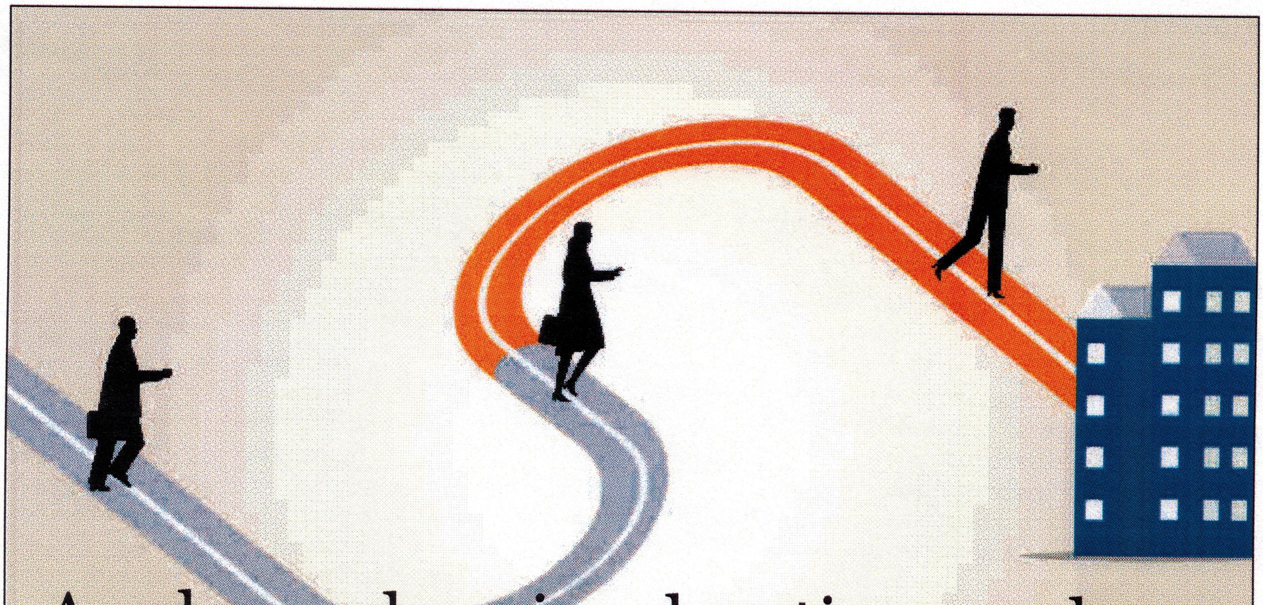
SEND ITAUDIT ARTICLE IDEAS to Steve Mar at steve_mar2003@msn.com called vehicle to x (V2x) that allow vehicles to talk to each other and to roadway infrastructure. Here, the connections are established on the fly to allow for exchange of data relating to positioning, traffic signals, and on-the-road services. Variants on the V2x nomenclature include vehicle to vehicle, vehicle to infrastructure, and vehicle to pedestrian. Each variant sets up a wireless connection to accommodate the services, entertainment, or vehicle support. Threats to V2x connections include malicious attempts to communicate false hazard information and the privacy of information broadcast from car to car.

Other wireless communications that can support vehicle connections such as Bluetooth, cellular, and Wi-Fi have well-documented weaknesses. What differentiates them when incorporated into vehicles is their ability to interface with vehicle controls and safety functions. The risks increase when wireless communications are used to update vehicle control software, perform system diagnostics, or change performance and safety settings. One of the most important security-related questions is whether operating and safety systems within the vehicle are connected or isolated from these external communication channels. If they are not isolated, robust authentication systems should be in place to ensure that only authorized updates and signals can be sent to the vehicle.

Auditing Cars

Auditors who are assessing risk and testing appropriate mitigation processes should begin by examining the environment in which the connected car software is designed and written. Here, traditional controls should be in place, including perimeter security, strong authentication, threat detection, and appropriate response processes. All the necessary controls for maintaining a secure development environment are well-known, so the auditor should verify their presence and operating effectiveness. A connected car audit program should include this type of security review as the starting point.

For automakers and technology vendors, a connected car audit program must examine the software development processes to ensure there is appropriate attention paid to security throughout the design and testing steps. Although relatively new to the automotive industry, secure software development is a mature practice in adjacent industries. Fundamental to good development practices are steps to ensure appropriate



TO COMMENT on this article,
EMAIL the author at brad.barton@theiia.org

risk assessment, security design reviews, testing, authentication, and privacy. Risk assessment should be based on the fundamentals of confidentiality, integrity, and availability. Across all three risk areas, unique considerations arise when communicating to and from a moving vehicle. The Automotive Information Sharing and Analysis Center's Automotive Cybersecurity Best Practices guide summarizes security expectations and can be the core of a connected car audit program.

For auto buyers, such as businesses and government agencies operating auto fleets, internal audit can contribute by advising the organization on spelling out expectations in requests for proposals or purchasing documents. Examples of such expectations may be included in future U.S. government guidelines for purchasing connected devices.

Finally, privacy issues are a growing concern worldwide. Auditors should address how privacy compliance will be incorporated into the design and operation of vehicle systems. This includes data stored and analyzed in a remote cloud or data processing center. Auditors should examine practices for the collection and use of personal information. The Alliance of Automobile Manufacturers' Privacy Principles for Vehicle Technologies and Services explains the reasons for collecting vehicle operating data, and addresses fundamental considerations for maintaining consumer confidence in its transparency, appropriate use, retention, and accountability. The principles can be a good guide for planning a privacy audit.

Driving Awareness and Response

System development and privacy issues are among many reasons that internal auditors should expand their audit scope to encompass connected vehicles. Vehicle advancements that rely on outside connections are already available and expected to be widespread soon. In the best-case situations, the audit team will only need to confirm enterprise awareness and appropriate response to these risks. But in the other cases, audit can be the spark that initiates necessary actions to recognize and mitigate risks posed by this technology. Ia

BRAD BARTON, CISA, *is chief operations, risk, and compliance officer of Securely Yours LLC in Bloomfield Hills, Mich.*
SAJAY RAI, CPA, CISSP, CISM, *is president and CEO of Securely Yours LLC.*