Current State of Connected Car Security

Robert Shein, Manager, ONE Cyber
November 14, 2017

Current Trends in Vehicle Hacking

- Attacks are becoming easier to perform.
  - Devices for interacting with vehicle systems are becoming less expensive and easier to use.
  - New devices are being introduced on the market with supporting software to make it simple for security researchers and criminal hackers to experiment with attacks on cars.
    - Examples: Macchina M2, Seeed Studio CAN-bus Shield v2.0, EVTV CanDue
    - All of these cost between $80-$150 USD (9,000-17,000 JPY).
- The security research community has taken significant interest in car hacking.
  - The DefCon security conference has had a “car hacking village” for the past two years, where attendees can learn and test car hacking techniques against real automotive systems.
- Overall assessment: vulnerability research related to connected vehicles will continue to accelerate in pace. Within the next 2 years, car hacking will be relatively simple to experiment with for any researcher who is willing to spend $100.

Examples of Commonly-Accessible Tools

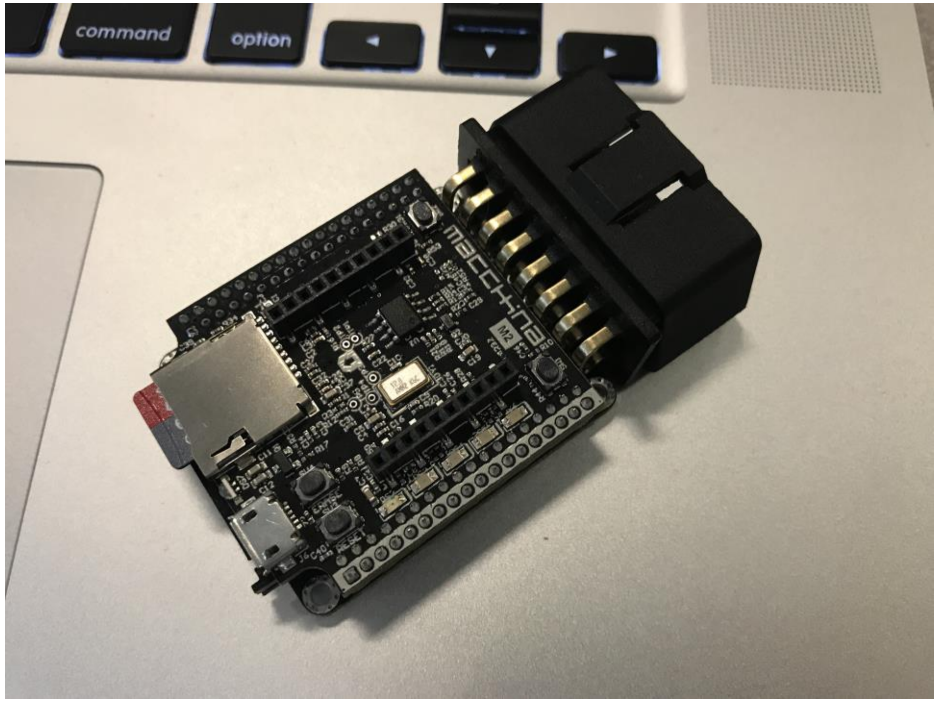


Photo by Robert Shein

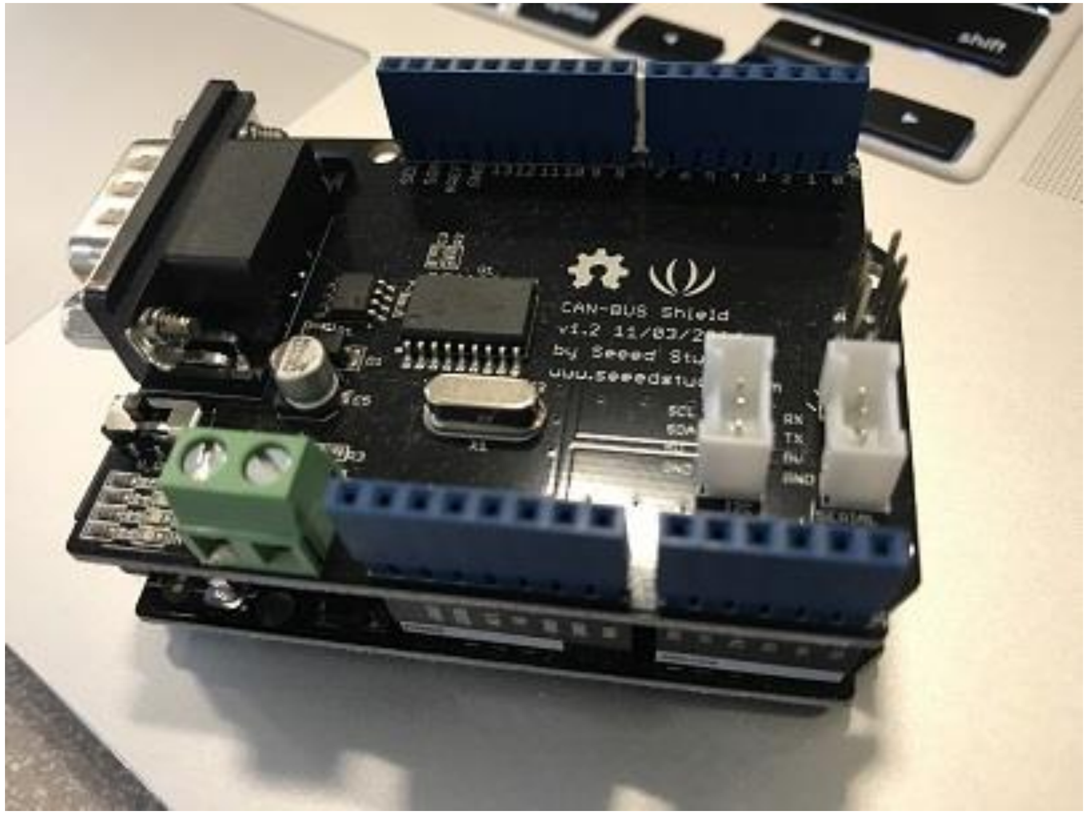
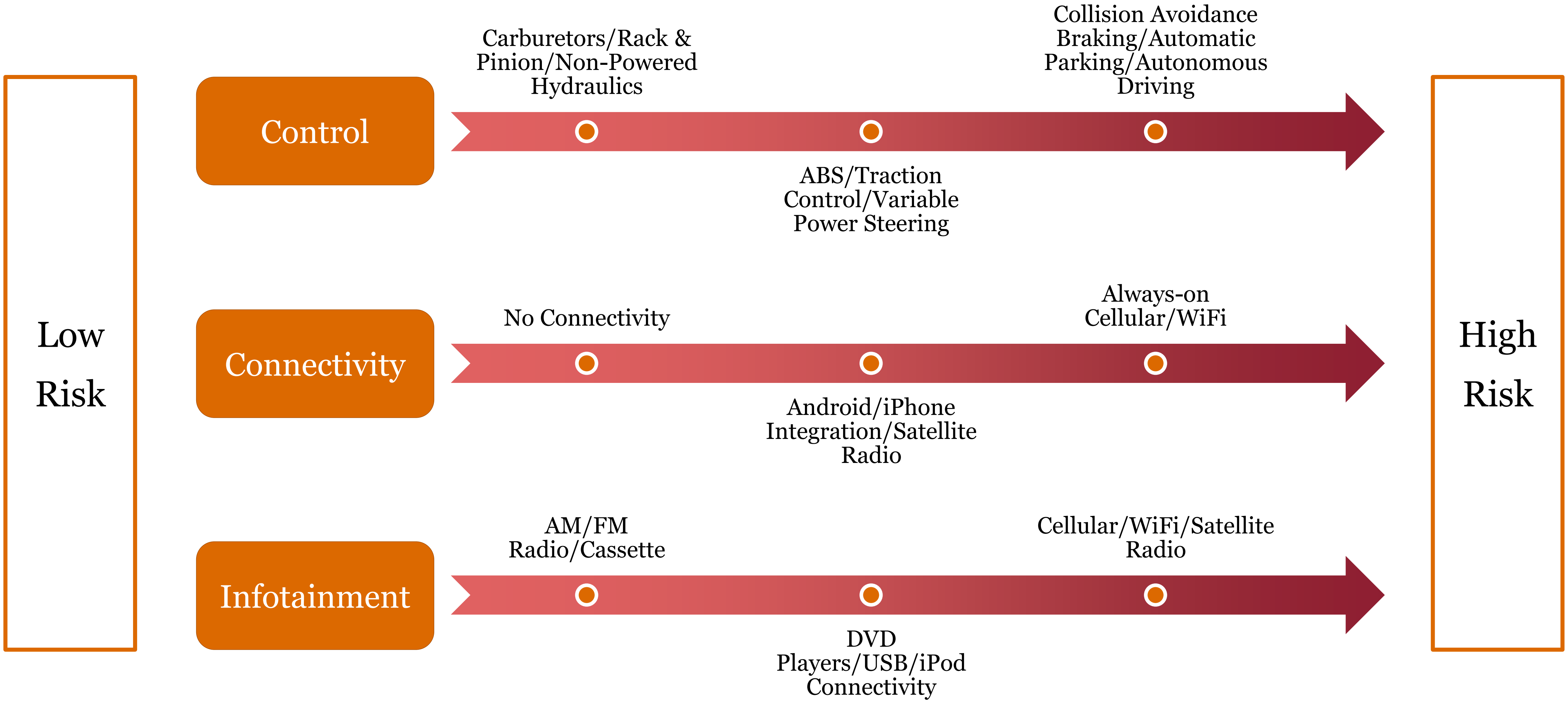


Photo by Robert Shein

Progression of Connectivity/Features/Attack Surface



Low Risk

Control

Carburetors/Rack & Pinion/Non-Powered Hydraulics

ABS/Traction Control/Variable Power Steering

Collision Avoidance Braking/Automatic Parking/Autonomous Driving

Connectivity

No Connectivity

Android/iPhone Integration/Satellite Radio

Always-on Cellular/WiFi

Infotainment

AM/FM Radio/Cassette

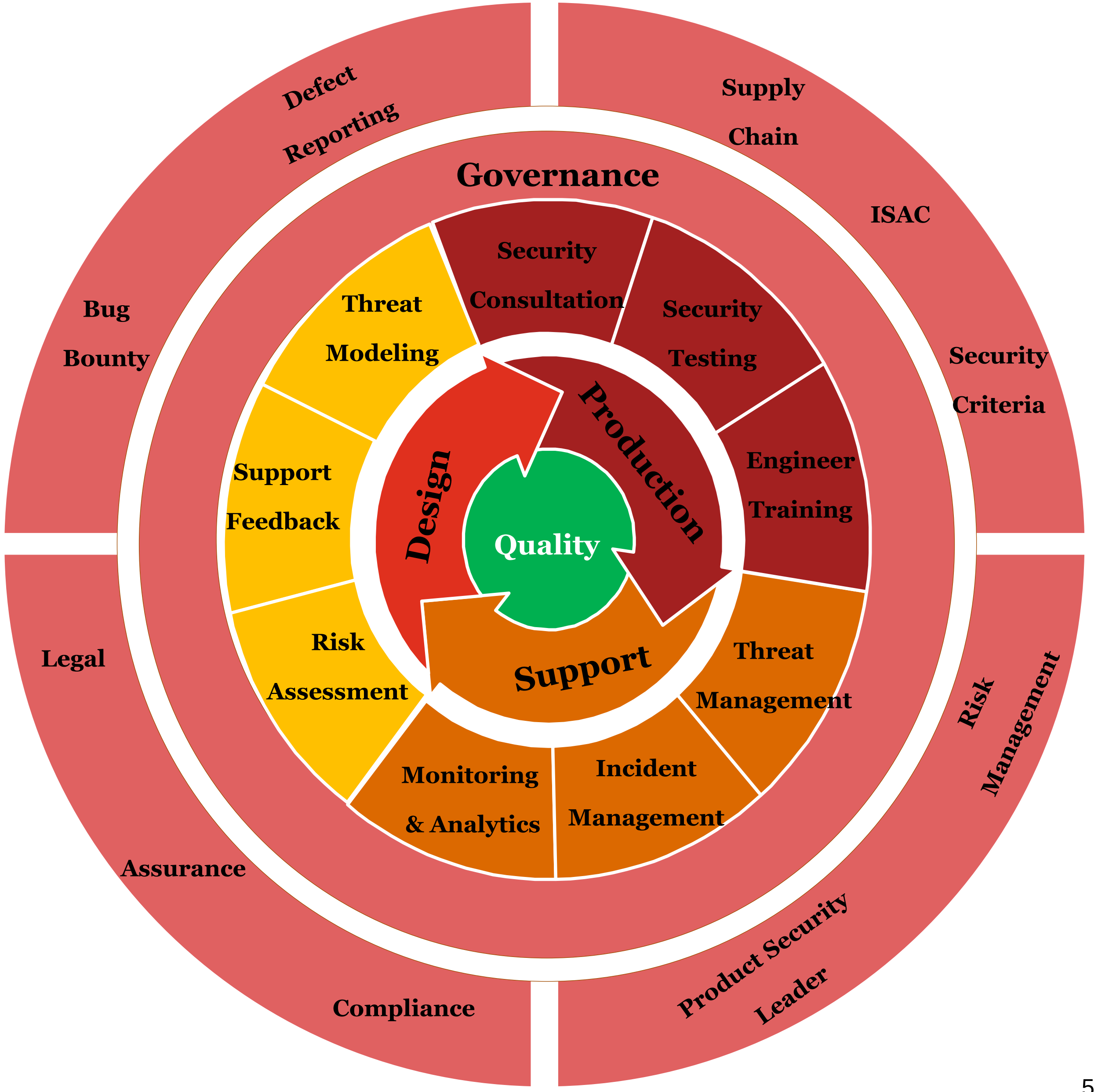
DVD Players/USB/iPod Connectivity

Cellular/WiFi/Satellite Radio

High Risk

Secure Engineering Process

- Vulnerabilities are defects – this is a quality problem
- Embed cyber risk discipline throughout the engineering process to reduce security related defects
- Identification of design risk and threat issues before they become development or production issues. Fixing issues earlier reduces the cost of remediation
- Raise the level of cyber risk awareness across the engineering organization
- Provide security assessment, consultation, and assurance throughout the lifecycle
- Provide governance and oversight to address threats and risks programmatically through the established quality process
- Transition manufactures from reactive to proactive supplier management programs
- Security is kaizen



Connected Car Security: Challenge/Approach/Impact

Challenge	Approach	Impact
Third-party solutions typically have poor security and many significant vulnerabilities	Penetration testing/security testing of connected car components and services	Increasing security quality of vehicles, with improvement from year to year; findings from testing now feed secure engineering processes
Lack of visibility into security of solutions from outside vendors in the connected car space	Third-party risk assessment/management program development	Risks from outside vendors are now managed and mitigated; defects and issues related to outside vendors are tracked and addressed
Difficulty communicating and enforcing security requirements in connected car	Security requirements development and management program	Contractual language and security requirements are part of the procurement process, with security testing to validate that vendors meet requirements

Questions?