Building an Automotive Cybersecurity Testing Lab

Justin Montalbano

DELPHI

Innovation for the Real World
Agenda

- Introduction
- Delphi Cybersecurity
- CyberSEAL Lab
- Importance of Cybersecurity Testing
- Processes
- Tools
- People
- Facility
- Q&A
Introduction

- Cybersecurity Lab Technical Manager @ Delphi
  - Ethical Hacker / Web / Networking
  - Automotive / Medical / Manufacturing
  - Enjoys
    - Exploring nature
    - Family
    - Breaking things
Delphi Cybersecurity

Vision
- Establish Delphi as a Global Leader in Automotive Cybersecurity with scalable secured products

Pillars of Cybersecurity
- Engineering
  - Focus on helping our engineers develop secure automotive components
- Process & Tools
  - Focus on developing processes for the organization to follow in regards to security as well as the tools used for testing and securing products
- Lab (Testing / R&D)
  - Focus on pen tests of our products and research into newly developed cybersecurity products
Cybersecurity Engineering & Assessments Lab (CyberSEAL)

**Mission**

- Red Team
  - Testing, Validation and Training
- Research and Development
- Influence
  - Cybersecurity in Academia
- Cybersecurity Certification

**Testing Facility**

- Garage Bays
- Lab Workbenches
Importance of Cybersecurity Testing

- Different types of cybersecurity testing:
  - Red team testing (production/updates)
  - Compliance (requirements) Testing
  - Incident Response Investigations

- Long Term Cost Saving
  - On average, the cost to fix a bug, post-release, is 30x the cost of doing security by design.

- Catch vulnerabilities before they show up in the wild (YouTube, social media)

- Save brand from “hacking” damage

*Source: National Institute of Science and Technology*
Importance of Cybersecurity Testing

- Cannot have safety without cybersecurity.
- Confirms security requirements are implemented and effective
- Provides assurance to senior management.
- Mitigates low hanging fruit and known vulnerabilities.
- Potential to discover new bugs in updated systems.
- Ensures a level of customer trust with your company.
- Helps build a security culture within an organization.

Every company should have some form of a cybersecurity testing process, whether it be internal, external or a mix of both.
Processes
Process Models
Types of automotive testing models

• Automotive testing models:
  – Full Vehicle Assessments
  – ECU/Component Assessments
Process Methods

There are specific types of methods for testing different technologies. Currently no automotive defined cybersecurity testing method.

- **Risk Based Assessment Methodology (RBAM)**
- SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
- OWASP Testing Guide (web focused)
- PCI Penetration Testing Guide (payment industry focused)
- Penetration Testing Execution Standard (PTES)
- Penetration Testing Framework
- Information Systems Security Assessment Framework (ISSAF)
Process Methods

NIST 800-115
Technical Guide to Information Security Testing and Assessment

Process for Assessing “Computer Security”
1. Planning
2. Discovery
3. Attack
4. Reporting

Risk Based Assessment Methodology (RBAM)
Detailed Delphi Processes

**Threat Analysis Risk Assessment (TARA)**
The process of determining the potential threats a system possesses as well as the risks associated with each individual threat. (threat modeling)

**Output:** TARA Report

**Vulnerability Assessment**
The process of performing penetration tests on a system to find common vulnerabilities and provide mitigation techniques to those specific vulnerabilities.

**Output:** Vulnerability Report, Mitigation Report

**Verification Assessment**
The process of verifying that product teams have successfully mitigated the recommended mitigations to the discovered vulnerabilities.

**Output:** Verification Report (rubber stamp)
Tools
Testing Tools

Areas to focus tools around

- **Hardware**
  - Debugging ports / Chip Programmers

- **Software**
  - Operating Systems / Applications

- **Interface(s)**
  - RF (Wifi, GPS, Bluetooth, V2X, TPMS, Key Fob, sensors, etc.)
  - USB
  - Cellular (LTE, GSM, CDMA)
  - Network(s) (CAN, Ethernet, MOST, etc.)
Testing Tools
List of tools and their use

- Vehicle Diagnostic Tool (dealership tool)
  - Reset vehicle fault/error codes
- Oscilloscope / RF Signal Analyzer / Logic Analyzer
  - Signal decoding and interpretation
- Intrepid Vehicle Spy / Vector CANoe / SAINT2
  - Vehicle simulation / emulation
- USB Rubber Ducky / Facedancer21 / USB Kill
  - USB interface testing
- Bus Pirate / JTAGulator / JTAG/SWD Debugger
  - Debug port testing
- HackRF / BladeRF / YARD Stick One / Ubertooth One / Pineapple / RF Shield
  - Radio frequency interface testing

- Linux Test Machines
- Cell Site Simulator
  - Cellular Testing
- Protecode SC / Black Duck
  - Software Composition Analysis
- Coverity / Veracode
  - Static Code Analysis
- Wireshark / Burp Suite / Fiddler
  - Traffic analyzer/manipulator
Testing Tools
Photos

- Oscilloscope
- Spectrum Analyzer
- Raspberry Pi
- HackRF One
- Bus Pirate
- JTAGulator
- BladeRF
- Segger jlink
Management Tools

- Git / File Sync
- Task / Project Management
- Secure File Storage / Distribution
- Automated Testing Suite
People
Organization of People
Roles for cybersecurity testing team

- Technical Manager
  - Oversee the lab operations
- Lab Engineer Lead(s)
  - Leads, organizes and executes assessments
- Lab Engineer(s)
  - Organizes and executes assessments
- Interns
  - Learns, organizes and executes assessments
- Liaison between testing & product development
  - Arranges products for testing and works with product teams to review/integrate
Organization of People
Skillsets essential for cybersecurity testing

- **Formal Education:**
  - Information Assurance, Network Security, Electrical Engineering, Computer Science or Computer Engineering

- **Work Experience:**
  - Penetration testing for enterprise, embedded and/or other connected systems
  - Development of test plans and deep understanding of electronics, full stack (OSI Model)

- **Certificates:**
  - Certified Penetration Testing Consultant (CPTC), Certified Penetration Testing Engineer (CPTE), GIAC Certified Penetration Tester (GPEN), Offensive Security Certified Professional (OSCP)

- **Common Titles:**
  - Security Analyst, Security Consultant or Security Engineer

- **Where to find these people?**
  - College Hackathons, Information Security Conferences (SANS, DefCON, BSides, Blackhat, GrrCON, etc.)
Facility
Facility for Testing

- An independent team with a dedicated lab is essential to harvest security personnel.
- Depending on the cybersecurity automotive testing model you follow (component level or full vehicle), different setups can be configured.
- Can look into 3rd party contracting for a testing facility, but may be more costly in the long run. Although, 3rd party testing validation is always encouraged and should not be neglected.
Key Take Aways

- Cybersecurity testing is crucial to securing ECUs.
- You cannot have safety without security.
- Integrate cybersecurity testing into development processes.
- Ensure your lab is equip with the proper tools to test with a red team perspective.
- Build a team of hackers to influence a culture of security throughout your organization.
- Encourage an independent testing facility(ies) and team to build a “go-to” cybersecurity team.
- 3rd Party contracting can help assist in areas of low resources, but can be expensive long term.
Q&A