Automotive Security Technical Briefing

Jon Williams

October 28th 2015
The Connection Challenge

New driver assistance systems, digital instrument clusters, and head units with infotainment all require advanced computing power inside the vehicle
What we are protecting

- **Components (Parts)**
  - Against Tampering
  - Against Counterfeiting

- **Systems**
  - Against Hacking
  - Data Theft
  - Cross contamination

- **Business**
  - Revenue streams
    - DRM and feature enablement
  - Remote update
Secure Foundation

- **INTEGRITY**
  - Secure Partitioning certified to EAL 6+
  - Enables secure consolidation of components to a single Processor
  - Protect Automotive safety functions from interference from non automotive functions
  - Protect the vehicle bus

- **INTEGRITY MULTIVISOR**
  - Builds on INTEGRITY’s secure partitioning
  - Hosts Guest Operating Systems in secure partitions
    - A hacker may get into the guest but cannot get out of the partition
  - Enables open, non-secure applications to be hosted on the same processor as Automotive grade applications
Securing the device – basic building blocks

- To ensure the device works as required through its life cycle

1. Unique secrets and cryptographic keys must be added securely at the point of manufacture
2. There must be a secure and tamperproof trusted boot process for the firmware
3. There must be software agents on the device, utilising the cryptographic keys to
   - Authenticate incoming information and files
   - Authenticate and sign outgoing information
   - Only allow firmware updates from trusted sources
GHS INTEGRITY Security Services

Complete end-to-end embedded system security

ISS Security Toolkits
- Commercial and Suite B algorithms
- Network Security (TLS, IPSEC, SSH etc)
- Hardware Crypto Cores
- Secure Boot
- File System Encryption
- Manufacturing Initialization
- INTEGRITY Control Manager
- Security Architect 360™

ISS Device Lifecycle Management
- Secure Application Store for trusted delivery of all enterprise and embedded applications
- Manufacturing Key, Certificate, and Signature Generation
- Supply Chain Management
- Secure Device Management
- Counterfeit detection
- Feature Enablement
- Digital Rights Management

ISS Embedded Security Services
- Architecture Studies
- Security Assessments
- FIPS & Safety Certifications
- Penetration Testing & Vulnerability Assessments
- Expert Engineering Services
- “Crypto boundary” development
- PKI applications
- Trusted platforms
Automotive Solutions

- ISS Vehicle Security Toolkit
  - IEEE 1609.2 Wireless Stack
  - Cryptographic Module
  - Secure Load
  - Credential Management Libraries

- DLM Security Credential Management System
  - Selected for CAMP and other US OEMs
  - Generate Certificates
  - Basis for V2V and C2C
  - Leverage system for Remote Software Update
DLM Automotive Firmware-Over-The-Air

1. Manufacturers and OEMs release software updates and data for signature

2. Approved files and packages are signed and distributed to App Store for pick-up

3. Vehicles authenticates to FOTA Service to discover and download pending updates

4. Vehicle ICM assembles FOTA update and verifies signature before accepting

Uses the same standards-based SCMS solution as V2X, for secure authentication and download of software updates
Summary: Green Hills in Automotive

- Green Hills is the gold standard for safety and security
  - More certifications at the highest achievable levels than any other RTOS
- INTEGRITY microkernel supports complete, measurable freedom-from-interference on multicore SoC’s
- Security Services
  - Key injection and DLM
  - Tamperproofing
  - Car to X
- Functional Safety experts for ISO 26262
  - Safe Multicore SMP
  - Interference Freeness of Partitions
  - Proven, experienced safety team
    - Safety architecture assistance and assessment
    - Safety certification development and support
- Green Hills is long term, critical supplier to the automotive industry
  - Compilers/debuggers – since 1995
  - INTEGRITY for critical systems – since 2005
  - INTEGRITY Multivisor – since 2009
Questions?