Applying Cybersecurity Processes to Autonomous Vehicles

Embedded Systems Security Group
Agenda

- Identify the problem
- Review the challenges
- Applying risk assessment techniques
- Security infusion to design process
- Conclusions/Wrap-up
- Questions/Contact
What’s the Problem?

• Problem?
  o How to apply conventional penetration testing methods to autonomous vehicle technology?

• Why address it now?
  o Autonomous Technology is transitioning out of the lab and into the streets.
  o Proactively address security to avoid “patching in” later.

• What can we do right now?
  o Generate discussion
  o Evaluate sensors
  o Develop requirements
  o Influence vendors
Types of Challenges

• **Experimental** - Just trying to make it work
  o Focused on meeting basic performance
  o Security seen as hindrance to prototyping
  o Operating in controlled environment
  o “Worry about it later”

• **Garbage In = Garbage Out**
  o Sensor data only as good as the source
  o Making assumptions about sensor performance based on limited testing
  o Sensor perception, sensitivity, and ranges highly variable
Types of Challenges

• Fusing data sources is difficult
  o Different units, manufacturers, libraries
  o Correlating objects between sensor types
  o Response magnitude may vary for materials/shapes

• Each sensor from a different manufacturer
  o Sometimes a sensor is a composition from even more suppliers
  o Technology layering and abstraction results in compounding corner cases
Types of Challenges

• Each sensor an embedded system
  o Limited insight into the system
  o Firmware updates
  o Debug ports, flash memory, configuration files
  o Network interfaces and protocols
  o Variety of interface libraries both Open Source and proprietary

• Constantly evolving sensor set (Next-best-thingitus)
  o Look, <Company name> just released a new sensor with better <property>!
  o Likely different than previous sensor or different manufacturer
  o Start security assessment all over again
Other Industries

- **Dedicated Short Range Communications (802.11p)**
  - DSRC motivated by federal infrastructure
  - Active standards development
  - Built with security in mind
  - Not evolution technology
  - A few ongoing pilot programs
    - Maybe security assessments should be included?

- **Military Applications**
  - Big budgets for security
  - Platforms tend to have high physical security
  - Small Numbers (relative to auto industry)
  - Strict revision control
  - See TARDEC VICTORY Program

SwRI Developed
Automated Tactical Vehicle
What Can We Do?

• Approach the problems from multiple angles:
  1. Involve In-House security resources (pen test, security policy, etc…)
     • Seek advice from existing In-House resources
     • Leverage institutional knowledge and experiences with other systems
  2. Engage with suppliers early
  3. **Integrate product lifecycle security**
  4. Identify avenues for exchanging and managing identified issues
  5. **Perform regular assessments**
  6. **Integrate external assessments and replicate results in-house**
  7. Monitor Hacker state of the art
     • Attend conferences
     • Review hacks or reports of other sensors
     • Many manufactures use similar tech
**Supplier Communication**

- Engage with vendor security team (if available)
- Some vendors more aware than others
- Some will be non-traditional automotive suppliers
- Establish POC on both sides for relaying:
  - Sending/receiving security findings
  - Design or process changes
  - Technology that may be shared across multiple platforms
- Consider hosting vulnerability reporting database
Lifecycle Security

ISO 26262/J 3061 Process:

- Security Requirements Development
  - Item Definition
  - Initiation Safety Lifecycle
  - Hazard Analysis and Risk Assessment
  - Functional Safety Concept

- Concept Phase
  - Initiation of Development System
  - Specification
  - System Design

- Product Development System
  - Requirements Specification
  - HW Architecture Design
  - HW Integration
  - HW Qualification
  - HW-SW Interface Requirements

- Hardware Development
  - SW Test
  - SW Safety Acceptance

- Software Development
  - SW Implementation

- Production and Operation
  - Product Release
  - Safety Assessment
  - Safety Validation
  - Integration

- Risk Modeling
- Asset Tracking
- Secure Over-the-Air Update
- Secure Code Practices
- Coding Analysis
- Penetration Testing
- Sensor Security
- Secure Interface Design

SwRI
Sensors Assessment

• Start evaluations of essential sensors
  - LIDAR, Radar, Vision, etc...
  - Subject models to security testing
  - Model and track vulnerabilities

• “Smart” Sensors
  - Typically contain embedded systems
  - Firmware images and onboard flash
  - Debugging ports
  - Variety of on-sensor functions
  - Networking capabilities (Ethernet, CAN)

• Typically “development friendly”
  - Well documented & publicly available
  - Configuration and demo applications
  - Sensors getting cheaper

• The result: Hackers Playground
System Assessment

• Will become more difficult as system matures
  o Need to track libraries used to develop system
  o Version control of multiple systems
  o Securing communications between modules

• Strict interface control
  o Data flow between user controls and safety critical
  o Autonomy Kit <-> Passenger Interface
  o System safety hypervisor

• Computer Vision
  o Demonstrated system classification manipulation
Outside Assessments

• Work with outside teams for better coverage
  o Request procedures & equipment lists not just findings
  o Replicate in-house
  o Build up assessment arsenal
  o Expand intuitional knowledge
Conclusion

• Involve In-House security resources
  o Seek advice from existing In-House resources
• Engage with suppliers early
• Integrate product lifecycle security
  o Identify avenues for exchanging and managing identified issues
• Perform regular assessments
• Integrate external assessments
  o Replicate results in-house
  o Request Procedures/Equipment/Source
  o Feed findings back into development process
• Monitor Hacker state of the art
Questions/Contact

Daniel Zajac
Daniel.Zajac@SwRI.org
(210) 522-4293
Senior Research Engineer

Edward Cain
Edward.Cain@SwRI.org
(210) 522-2417
Research Analyst

References: