AGENDA

- Overview
- Security Environment of the Car
- Ethernet Solution Areas
- Summary
In-car Security a Hot Topic

- Academic research
  - Experimental Security Analysis of a Modern Automobile
  - Comprehensive Experimental Analyses of Automotive Attack Surfaces

- Media
  - Car Hackers Use Laptop to Control Standard Car
  - Disruptions: As New Targets for Hackers, Your Car and Your House

Each Describes a Set of Attacks on Production Vehicles

- Instrumentation and control
- Laptop-based hacking tools that connect through the OBD port (CAN)
  - Physical access mostly required
    - This has led some to reject much of this content
    - However some wireless vectors explored also
  - Developed through extensive lab-bench research and experimentation
  - Once developed, easily repeated
### SECURITY ENVIRONMENT OF THE CAR VS. IT ETHERNET NETWORKS

<table>
<thead>
<tr>
<th>In-car Network</th>
<th>IT Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed topology and Configuration</td>
<td>Plug-and-Play</td>
</tr>
<tr>
<td>Mass Produced</td>
<td>Somewhat Unique</td>
</tr>
<tr>
<td>Physically Open</td>
<td>Behind a Security Barrier</td>
</tr>
<tr>
<td>Global Service Eco-system</td>
<td>Central Control</td>
</tr>
<tr>
<td>Tight Initialization Requirements</td>
<td>“As and When”</td>
</tr>
</tbody>
</table>

- **With Access to a Mass-Produced Vehicle and Time/Resources, a Hacker can:**
  - Develop a set of “attacks” against the vehicle
  - Distribute these through communities on the Internet

- **A Single, Well-engineered Attack Could Have a Wide Impact**
WHAT MOTIVATES THIS BEHAVIOR?

**Malicious Attacks**
Intent to harm occupants or brand reputation

**Grand Theft Auto**
698,000 vehicles stolen in the US in 2013

**Simple Notoriety**
Making a name for themselves or tech challenge

**Financial Gain**
To sell products intended as counter-measures

**Non-Malicious**
Non-standard repairs and modifications

- **HACKED Airbags**
- **HACKED Brakes**
- **HACKED Controls/Steering**
- **HACKED Entertainment System**
ATTACK CATEGORIES

Network Control
- Install or corrupt a device on the network to control the operation of other devices

Denial of Service
- Deny access to network resources to other devices on the network

Snooping or Information Theft
- Snoop the content of traffic on the network to extract information
ATTACK SURFACES

Ethernet OBD Port Access
Includes attacks on Service Equipment

Ethernet Port Access
Access to an open port, replace existing device

Gateway Devices
May have wireless interfaces

Firmware Corruption
Subvert operation of an existing network device

Many Entry Points into the Network that Should be Protected
ETHERNET SOLUTION AREAS

- Ethernet Basics
- Scope of Traffic
- Rate Limiting
- Device Authentication
- Encryption
**Packet Format**
- MAC source/dest address
  - See where a packet is coming/going
- VLAN tag – which VLAN
- CRC – integrity check

**Switched Ethernet**
- Segments are isolated at L2 by the switch
  - Forwarding/filtering based upon forwarding databases (FDB, MFDB)
    - Populated by a Control Plane through learning and configuration
- Ports can be administered through configuration
- Rich set of statistics standards for anomaly monitoring in software

**Offers a base-level of Security**
- But we need more
Where Do the Packets Go?
- While each link is a separate collision domain, Ethernet is still a broadcast network
  - Unknown unicast goes everywhere until learned
  - Broadcast/Multicast goes everywhere unless pruned
- This creates the potential for snooping, denial-of-service etc

Many Ways to Limit the Scope
- VLANs
- Multicast Filtering
- Unicast Filtering
  - Static Address Management – no flooding
- ACLs

Need-to-know Ethernet!
Create Multiple Broadcast Domains within the Physical Network

No Connectivity Between VLANs Without a Router

Broadly Deployed – all Switches Support this in Hardware

- VLAN tagging – the packet arrives with a VLAN ID
- Untagged – the switch assigns a VLAN based upon one of:
  - Port
  - Protocol
  - Fixed header fields (L2, L3)
  - Flexible match
An Ethernet Switch Implements a Filtering Database
- Tells it which destination port to use for a given destination address
- FDB is populated by source address learning
- Unknown unicast packets are flooded in the VLAN until learned
- FDB entries will age out if inactive (and therefore must be re-learned)

Flooding/Spoofing can Expose Security Holes

Various Ways to Reduce/eliminate this in Hardware
- Static provisioning of FDB (based upon prior knowledge)
  - Turn off MAC learning
- Port MAC locking: Learn only the first packet (SA) received and then make this static
- Software learning limits (number, address ranges, change frequency)
- Scope what happens to unknown unicast (limited or no flooding)
• Unless Filtered, Multicast Traffic Will Go to All Ports in the VLAN
• Most Hardware Has Many Programmable Options to Refine this
  • Associate a destination port bit-mask with an address
    – Can be statically populated, or done dynamically based upon protocol snooping
  • Define bit-masks for unknown addresses (IP, non-IP)
• Can More Precisely Define Where Multicast Goes
Precisely Configured Rules for Packet Forwarding

Historically an L3 Construct (IP Routers)

Also Available at L2 in Most Switches

An ACL:

- Is a list of \{ match, action \} pairs
  - Match: Masked bit-wise match on ethernet packet header (e.g. MAC DA/SA)
  - Action: Typically \{permit | deny\}, but others available also depending upon hardware.

- Once defined can be applied to a port or VLAN
- Allows for very precise definition of where traffic is allowed to go
  - e.g. \textit{this} station can only send to \textit{that} station
- Should be a good fit for the in-car network (if required)
  - Static rules based upon prior knowledge
  - Pre-configuration
Bandwidth Usage
- Ethernet (by default) does not impose limits on how much bandwidth a station can use
  - Basically a free-for-all - so one badly-behaved station can disrupt others
- Aside (on AVB)
  - AVB switches impose transmit limits at the class level, but not station (or flow)
  - End-stations are required to impose per-stream limits, but:
    - Can’t always assume this to be the case
    - Faulty behavior is a possibility also

Commonly Deployed Methods Have Evolved
- Storm control: Broadcast/Multicast/Unknown unicast – rate limit these classes of traffic per port
- Ingress/Egress metering: Limit overall traffic on a port
- Flow-based policing: In-profile/out-profile actions for given flows
  - Single-rate, Dual-rate, color-aware
  - See next slide
- Rich set of counters for software-based mechanisms

Again a Good Fit for the Car, Because We Know the Expected Patterns
FLOW-BASED POLICING (GENERAL)

CLASSIFIER: Packets based upon header fields (like ACLs)
MARKER: Update the packet according to security policy
  - Priority, VLAN, etc.
METER: Measure the utilization of a flow -> conditional actions
  - Policing
SHAPER/DROPPER: Also re-direct

Note: Some switch devices support this independently on both ingress and egress

© 2014 Broadcom Corporation. All rights reserved.
**DEVICE AUTHENTICATION/AUTHORIZATION**

- **By Default Ethernet is a Plug-and-Play Network**
  - Devices just attach and go

- **How Do You Authenticate a Device as Valid?**
  - Must be authenticated before letting it onto the network

- **802.1x**
  - Ethernet encapsulation for EAP
  - Very widely implemented

- **EAP – Extensible Auth Protocol**
  - Framework for exchange of authentication messages
  - Multiple exchange methods standardized
  - Each can carry a set of authentication keys and credentials for device verification
Method and Credentials Define Authentication Strength
- Often a trade-off between strength and convenience
- Convenience is less of an issue in a static network – can pre-provision more easily
- In-car network also needs to consider initialization time

Very Often Associated with User-based Logins
- But can apply equally well to unattended devices
  - e.g. pre-shared keys, X.509 certificates, Device IDs
- Many methods offer mutual authentication (EAP-PSK, EAP-TLS)
  - Require storage of security credentials on the device

IEEE 802.1AR – Secure Device Identity
- Defines device identity and cryptographic binding to the device
- Defines operation within EAP-TLS/802.1x
- Deployed mostly in highly secure point-of-sale devices today, but likely to become mainstream
- **802.1AE – MAC Security (MACSec)**
  - MAC-level encryption and message authentication
  - Key management through 802.1AF (now 802.1X-2010)
  - Requires hardware support (adds cost)
    - Not mainstream deployed at this point
  - Most suitable for a single infrastructure carrying mixed security domains

- **Can Also be Implemented at Higher Layers**
  - 1722 message encryption/authentication
  - IP Sec
  - Digital Content Protection (HDCP)
  - etc.
Security in the car is a concern

Ethernet as an infrastructure has been around for decades in IT networks, and has seen/countered many threats and attacks

There are several helpful features that will help secure the Ethernet infrastructure

Ethernet plays an important role in an overall security solution
Q & A