Connect Vehicles: A Security Throwback

Chris Valasek (@nudehaberdasher)
Director of Vehicle Security Research
Introduction
Hello

- Chris Valasek
- Director of Vehicle Security Research
- IPS Dev -> Windows RE -> Car Hacking
- chris.valasek@ioactive.com
- @nudehaberdasher
- Fun fact: Severely allergic to cats
Agenda

- Why Cars?
- Technical Overview
- Automotive Attacks
- Manufacturer Concerns
- State of the Union
- Thoughts
- Q & A
Why Cars?
Software everywhere

Millions of cars & drivers

Figure 4-1: Number of Licensed Drivers by Gender: 1970-2009

https://www.fhwa.dot.gov/policyinformation/pubs/hf/pl11028/chapter4.cfm
Technology Driven Buying

“The nature of the buyer of small cars has changed – it has changed permanently,” he told MLive Thursday during a phone interview. “Now, the change in styling and the fact that you can pretty much find anything in a luxury car in a small car ... it’s enabling consumers who can afford a bigger car to consider a small car.”
Software + Hardware + Physical == Fun
Cars seem to be special…
Junk Hacking Must Stop!

From: Dave Aitel <dave () immunityinc com>
Date: Mon, 22 Sep 2014 14:53:47 -0400
Electronic Control Units (ECU)

- Some only take input from sensors
- Many take input from sensors and the vehicle network
  - Sophisticated ECUs may take physical action based upon network traffic (i.e. adaptive cruise control)
- A select few do both AND take input from the outside work
  - Telematics, Infotainment, TPMS, RKE
Some are simple…
Some are complex…
Some control physical actions…
How do they communicate?

Automotive Attacks
3 Keys

Network Architecture

Cyber Physical

Remote Attack Surface
Cyber Physical
Network Architecture
Remote Attack Surface

- Telematics (CDMA/3G/4G/LTE)
- Wi-Fi
- Bluetooth
- TPMS
- In-car apps
- V2V & V2I
Manufacturer Concerns
#1 Concern
Many others

- PII
  - GPS, BT_ADDR, TPMS
- Proprietary Information
  - Security keys, algorithms, general processes
- DRM
  - Maintenance software & hardware
  - Nissan example
- ECU Functionality
  - Prius Steering
State of the Union
Disclaimer

- I obviously don’t have total insight into the automotive industry, only my interactions w/ vendors and working groups
- Very long development cycles make many of these issues difficult to address in a short timeframe
  - Cars for 2018 are basically ‘done’ now
Misconceptions

“requires a physical presence inside the vehicle, partial disassembly of the instrument panel...”

FROM CARJACKING TO CAR-HACKING
CAN HACKERS TAKE CONTROL OF YOUR CAR?
“Our focus, and that of the entire auto industry, is to prevent hacking into a vehicle’s by-wire control system from a remote/wireless device outside of the vehicle. Toyota has developed very strict and effective firewall technology against such remote and wireless services. We continue to try to hack our systems and have a considerable investment in state of the art electro-magnetic R&D facilities. We believe our systems are robust and secure.”

- John Hanson | Toyota Motor Sales U.S.A
Protect from the outside (only)

Statement from Toyota
All of this would be obvious to the driver. Our focus, and that of the entire auto industry, is to prevent hacking into a vehicle’s by-wire control system from a remote/wireless device outside of the vehicle.
We’re not good at this game
Trust of Remote ECUs

* There is development of new technologies for process isolation / restriction
Complete Trust of CAN
No attack detection
Patching!

http://www.wsws.org/asset/f31eb70f-4657-4cdb-9134-51834510c96P/recall_notice.jpeg?rendition=image480
You remind me of…
Edge protection only
Lack of...

### Defined integrity levels

<table>
<thead>
<tr>
<th>System</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Untrusted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local System</td>
<td>400</td>
<td>300</td>
<td>200</td>
<td>100</td>
</tr>
<tr>
<td>Local Service</td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Network Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Elevated (full)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User tokens</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authenticated</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>World (Everyone)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anonymous</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All other tokens</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Shell runs here

http://www.adopenstatic.com/images/resources/blog/MIC1.jpg
Security through Obscurity

T-0052-11.cuw

1 |CALIBRATIONrO-Lf0\Yer
2 attach.atrrrrq008[Format]
3 Version=2
4
5 [Vehicle]
6 Number=1
7 DateOfIssue=2011-11-08
8 VehicleType=-
9 EngineType=2ZR-FXE
10 VehicleName=PRIUS
11 ModelYear=10
12 ContactType=CAN
13 KindOfECU=ENG & ECT
14 NumberOfCalibration=1
15
16 [CEU01]
17 CPUImageName=1nk#590RC3USA.xx
18 NewCID=39715300
19 LocationID=0002000100070720
20 ECUType=FOREST-2
21 NumberOfTarget=3
22 01_TargetCalibration=39715800
23 01_TargetData=423450498DA3E3E4D
24 02_TargetCalibration=39715100
25 02_TargetData=423533C3A46A494B
26 03_TargetCalibration=39715200
27 03_TargetData=424433493A4B4B4D
28
Ineffective Patching

**History** [edit]

**Windows Update web site** [edit]

Windows Update was introduced as an Internet web site with the launch of Windows 95. A link to Windows Update on the Start Menu gave access to additional downloads if Update offered additional desktop themes, games, device driver updates, and optional components such as NetMeeting.[2] Windows 95 and Windows NT 4 were retroactive updates designed for those operating systems, starting with the release of versions of Internet Explorer 4 for those operating systems. The initial focus of Windows Update 1 Outlook Express, Internet Explorer and other applications appeared later, as did access to beta versions of upcoming Microsoft software, most notably Internet Explorer 5.1 Windows Update in December 1998. Microsoft attributed the sales success of Windows 98 in part to Windows Update.[3]

Windows Update requires Internet Explorer or a third-party web browser that uses Microsoft's MSHTML layout engine, as it must support the use of an ActiveX control to have changed from version to version, it has always scanned the computer to find what operating system components and software are installed, and compared the versions of components then interfaces with the Windows Installer to install or update those components, and to report the success or failure of those installations back to Microsoft's servers.

The first version of the Windows Update web site (usually referred to as "V3") did not require any personally-identifiable information to be sent to Microsoft. In order for the software on Windows Update was downloaded to the user's computer when they visited the Windows Update web site. As the number of updates offered by Windows Update increased, the number of updates grew to exceed 400KB, which caused delays of more than a minute for dial-up users.[4]

http://en.wikipedia.org/wiki/Windows_Update#Microsoft_Update

* Wish I had stats on how many patched after it was completely automatic
No SDL

Security Testing

Code Review

Developer Education

SSDLC

Time is flat circle

http://media3.giphy.com/media/4Dy1Btpt0qUZa/200_s.gif
Complications

• Automotive development cycles are costly & long
  – Cars for 2018 are pretty much ‘set’ today
• Problems fixed today will still exist for a long time
  – Avg U.S. car is 11.4 years old
• Certain processes are required to be present & easy
  – ODB-ii ensures CAN diagnostics will be around for the foreseeable future
Thoughts

• Security seems to be an afterthought
  – Transparency issue?
  – This is changing: http://fortune.com/2014/09/24/general-motors-appoints-its-first-cybersecurity-officer/

• Hard to justify security when there is no immediate threat
  – MSFT 2006 v. MSFT 2014
  – Server v. Client side

• V2V will bring additional complications

• Patching is a HUGE problem right now
  – OTA updates will help address the issue

• People are concerned because a breach could mean physical harm, as opposed to personal financial loss

• I’m Chris and I’m here to help!
Thanks!

- Chris Valasek
- Director of Vehicle Security Research | IOActive
- chris.valasek@ioactive.com
- cvalasek@gmail.com
- @nudehaberdasher