Remote Control Automobiles

Corey Thuen, Digital Bond Labs
@CoreyThuen
thuen@digitalbond.com

http://digitalbond.com

Literature Review

CANBus is insecure by design

Research has shown pwnability

Response has largely been:
“Big deal, requires physical access.”

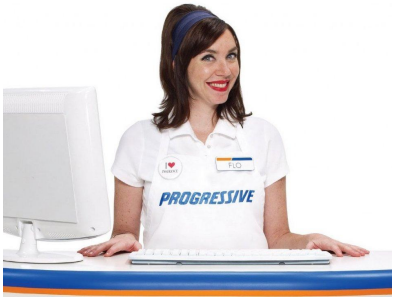
Fair enough but….

We have seen that CANBus is an insecure-by-design protocol and an attacker who has access to the main bus is able to control vehicle systems.

So far this has required physical access to the vehicle. The focus of this research was on remote access mechanisms and attack vectors.

CANBus Isolation is Ending

Many companies want your car data



Some want more than just your data

Miss a Payment? Good Luck Moving That Car

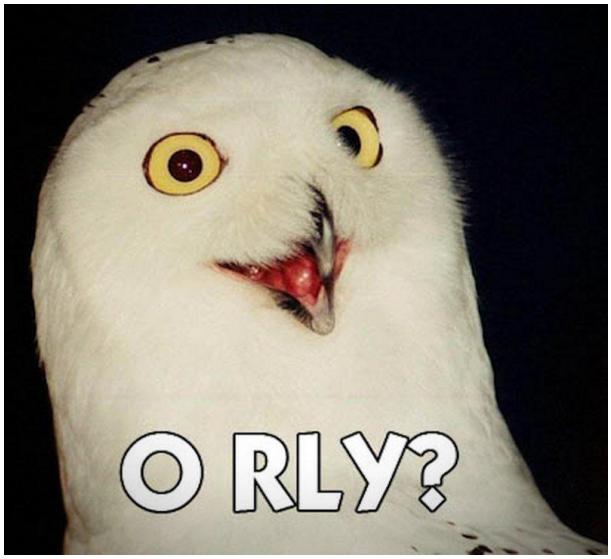
By MICHAEL CORKERY and JESSICA SILVER-GREENBERG SEPTEMBER 24, 2014 9:33 PM 981 Comments

As auto lenders reach out to those with poor credit, they are increasingly using starter interruption devices, technology that allows them to remotely disable a car, to spur timely payment. Video by Sean Patrick Farrell on September 25, 2014. Photo by By Sean Patrick Farrell on September 24, 2014. Photo John Gurzinski for The New

Network Connectivity of Legacy Systems

Insecure by Design systems are being connected to the net/cloud/borg (parallel to Industrial Control Systems)

"*Quite honestly, the vehicles and systems and components today are quite robust and resistant to cyber-security threats.*" - Andrew Brown, Delphi's chief technologist, provider of the Verizon OBDII dongle


O RLY?

Digital Bond Labs

Work with Critical Infrastructure vendors and asset owners to provide Component Security Consulting Services:

- Source Code Security Review
- Hardware Security Review
- Blackbox Testing/Binary Analysis
- Protocol Fuzz Testing

Digital Bond Labs

Thomas Fox-Brewster Forbes Staff

I cover digital crime, privacy and hacker culture.

FOLLOW

SECURITY 1/15/2015 @ 10:51AM | 44,291 views

Hacker Says Attacks On 'Insecure' Progressive Insurance Dongle In 2 Million US Cars Could Spawn Road Carnage

+ Comment Now + Follow Comments

Corey Thuen has been braving the snow and sub-zero

Virginia.gov

Search the Governor's site

Governor Terry McAuliffe

For Immediate Release: May 15, 2015
Contacts: Office of the Governor: Brian Coy, (804) 225-4260, Brian.Coy@governor.virginia.gov

Governor McAuliffe Announces Initiative to Protect Against Cybersecurity Threats

RICHMOND – Governor Terry McAuliffe announced today that the Commonwealth of Virginia is establishing a public-private working

digital bond

SECURING THE CRITICAL INFRASTRUCTURE

http://www.forbes.com/sites/thomasbrewster/2015/01/15/researcher-says-progressive-insurance-dongle-totally-insecure/

https://governor.virginia.gov/newsroom/newsarticle?articleId=8430

Embedded Security Patterns

"A system is *good* if it does what it's supposed to do and *secure* if it doesn't do anything else."

-- Dr. Eugene "Spaf" Spafford, Purdue

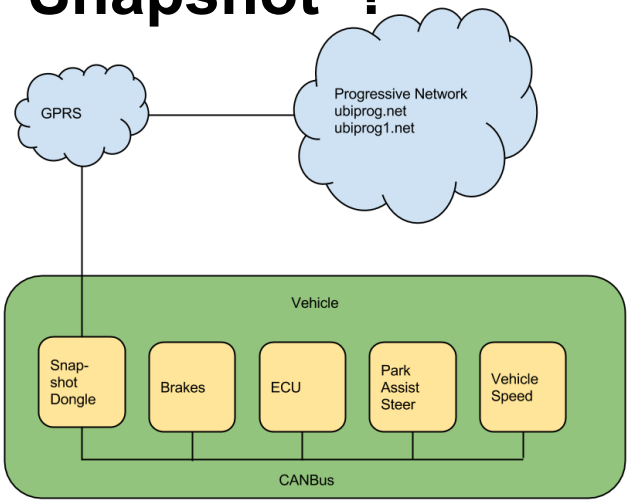
DB Labs has performed many assessments which reveal common security shortcomings

Let's Have a Look

Progressive insurance was chosen because of their free trial offer for ease of acquiring a device (https://www.progressive.com/snapshot/tdx/SocialNetworking/SocialNetworking).

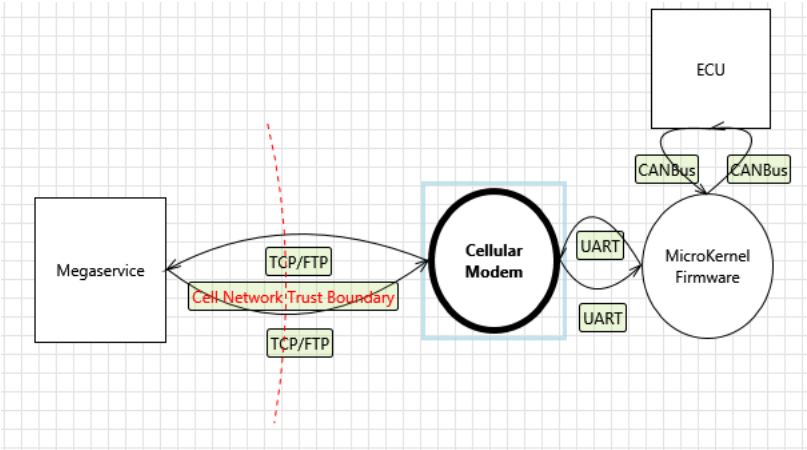
Any other such dongle would have worked equally well and this research was intended to address the issue as a whole, not specifically a single vendor.

What is “Snapshot”?



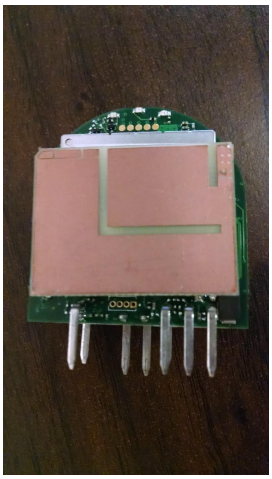
Snapshot is an OBDII dongle that users plug into their OBDII port in order to allow progressive to collect information and provide “usage based insurance.”

Communications Threat Model

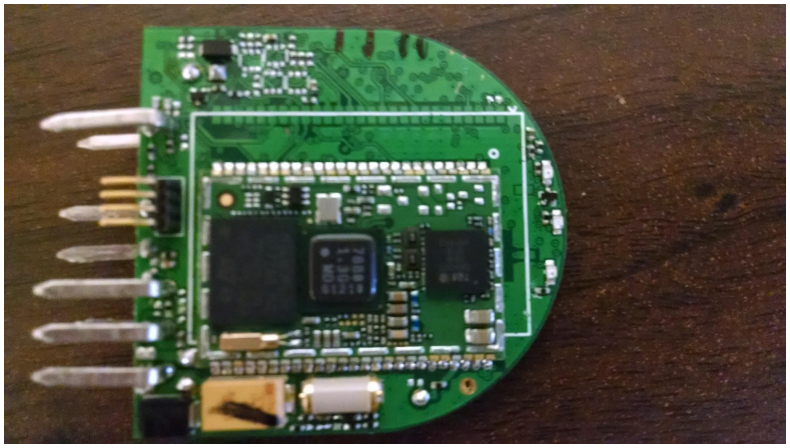


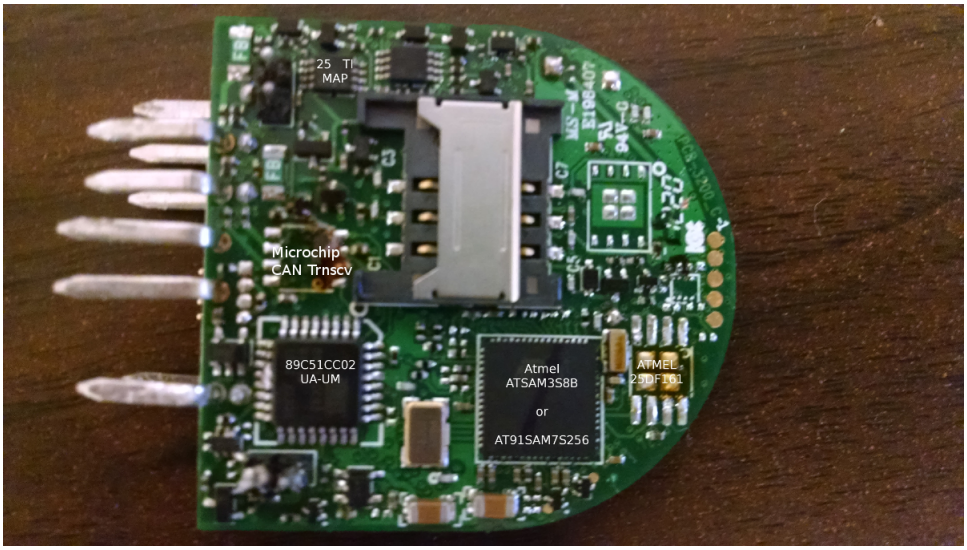
Threat models are extremely useful for identifying attack avenues and prioritizing targets of evaluation.

Hardware Analysis

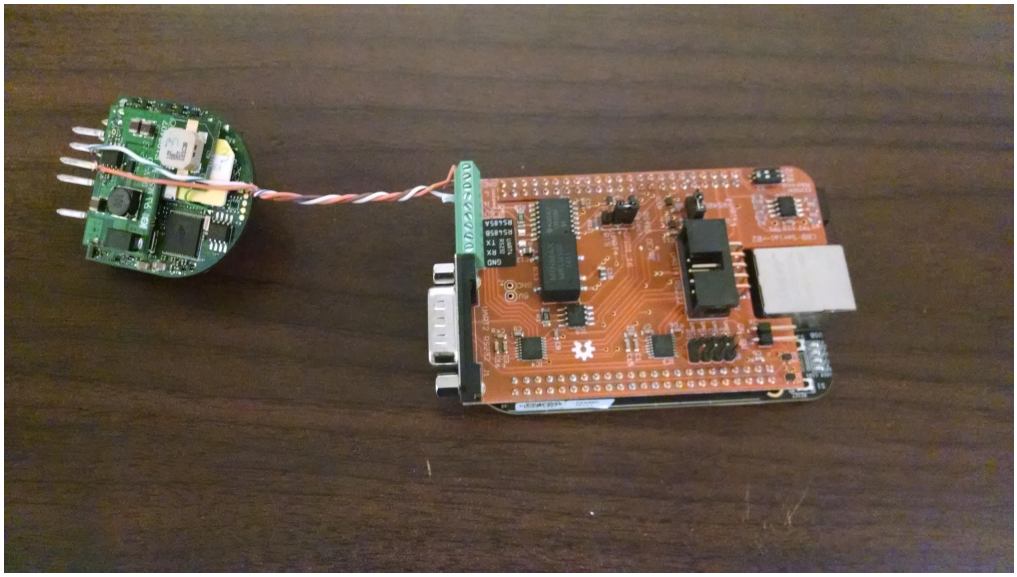



SN#: P078375D
XPYLEONG100

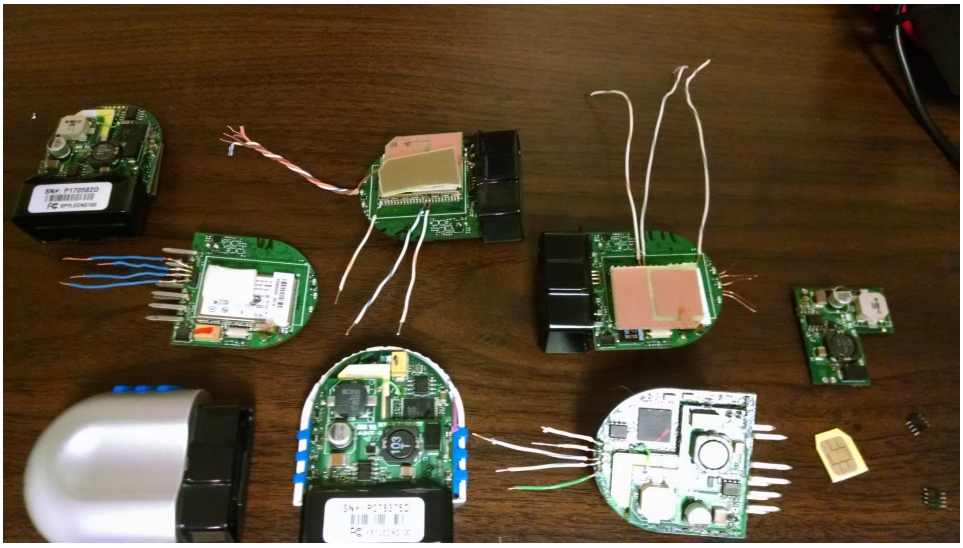




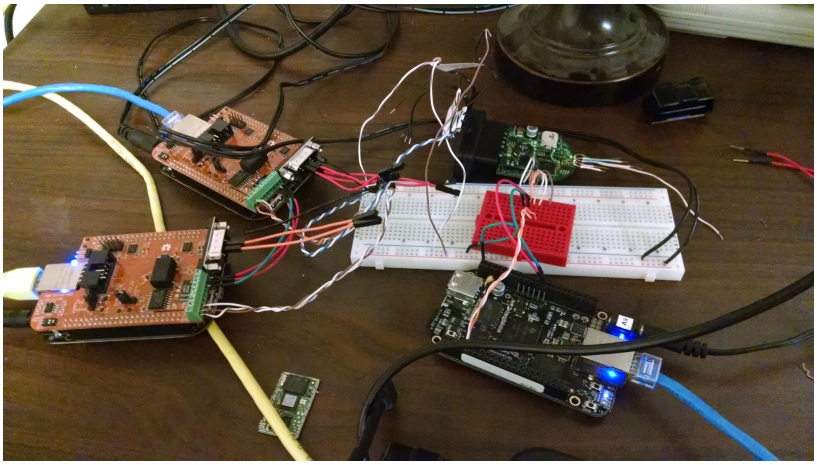
Chip identification is step1. The missing chip in the bottom right was the flash which was removed in order to pull the data in a chip reader.




PUSH
ON OFF



Analysis Environment



digital bond

SECURING THE CRITICAL INFRASTRUCTURE

Analysis environment consists of:
2 beaglebones with CANBus shields on the left which are a “virtual car” created by using real data taken from my Tundra as well as dynamically generating data.

A fake cellular modem running on the beaglebone at the bottom. This replaces the COTS (consumer off-the-shelf) cellular modem that the dongle uses for communication. This simulates an attacker controlled modem and/or communications as the focus of the research was the software running on the dongle itself, not the particular modem they happened to purchase. To create this fake modem, reference sheets for the modem were used to generate mutational and generational fuzzers of serial communications.

The dongle itself in the upper right connected to the CAN and the fake modem.

Firmware Analysis

Acquire via

- Chip Reader
- JTAG
- Read Request

Firmware Analysis - Strings

* Sensitive Strings removed at request of Progressive

```
D:
\Xirgo\projects\MN_Projects\Ocarina\Releases\SamRev31
32\SamRev3132A9\libraries\chip\sam3s\source\pmc.c
xIyKyHDh
RES MCT 41 OK
PRDC200702
PROD.UBIPROG.NET
PROD.UBIPROG1.NET
wcp.prod.ubiprog.net
ftp.prod.ubiprog.net
RES MCT 41 OK
PRDC200702
PROD.UBIPROG.NET
PROD.UBIPROG1.NET
wcp.prod.ubiprog.net
ftp.prod.ubiprog.net
Reading FAT at: %lx Count: %d
Disable TCP direct-link mode
Check SIM for SMS Messages...
%02d/%02d/%02d,%02d:%02d:%02d
```

```
D:
\Xirgo\projects\MN_Projects\Ocarina\Releases\SamRev3132\SamRev
3132A9\libraries\chip\sam3s\source\pio_it.c
_dwNumSources < MAX_INTERRUPT_SOURCES
pPin != NULL
dwFound != 0
Error - memory allocation error in timer.c
%s - Wrote Disconnection Event to RAM
Wrote Disconnection Event RAM->FLASH
%s - Wrote Connection Event to RAM
Wrote Connection Event RAM->FLASH
Trying to enter sleep mode (@%ld)
Wakeup Sources: Motion, Supply Voltage, RTT (for %ld seconds)
Wakeup Sources: Motion, Supply Voltage, RTT (@%ld)
Failed to enter sleep mode (Aborted)
Received valid FlashCmd_TripWrite
Received valid FlashCmd_TripEndWrite
AT+UFTPC=4,"%s","filedata"
AT+UFTPC=6,"%s"
RX DELAY: %ld ms
Stalled with %ld bytes @ %lx
Downloaded %ld bytes
```

Detour - Open Source Intelligence

Firmware analysis

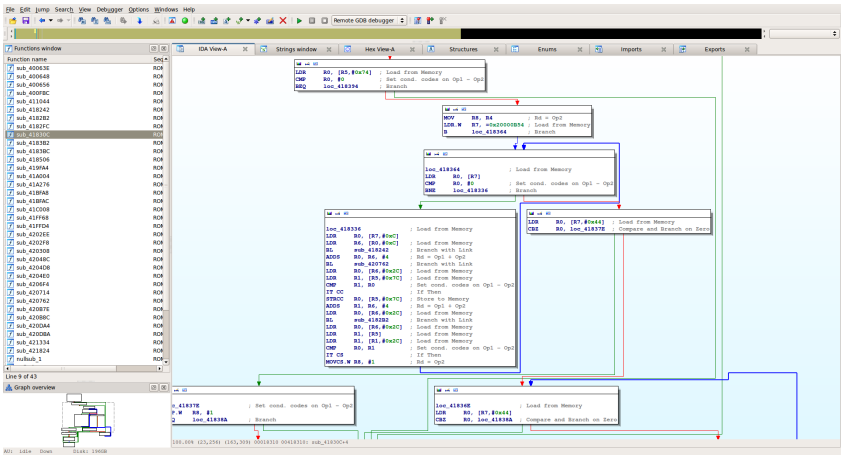
Xirgotech

- Consumer solutions
- Fleet management solutions
- Government contracts

FreeRTOS

strcpy and other banned functions used frequently

Firmware Analysis - Reversing



Used to identify insecure execution patterns, such as occur with banned insecure functions like strcpy.

CANBus Fuzzer

Mutation Based - Toyota Tundra used as baseline

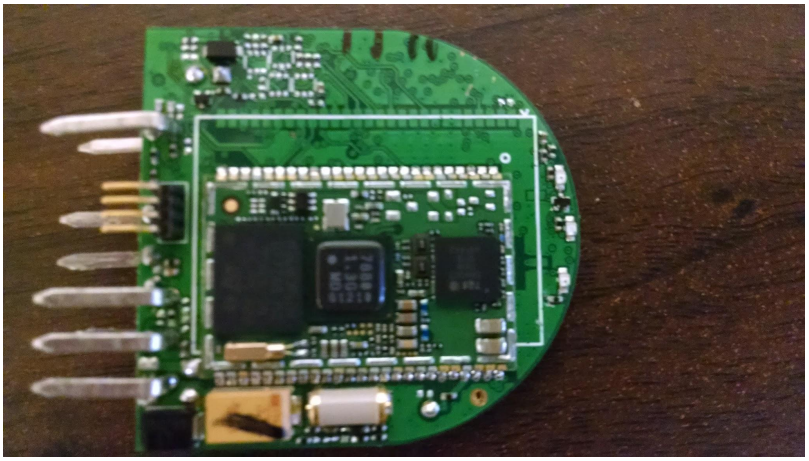
Generational - OBDII spec used as reference

CANBus Fuzzer

```
can0  025   [8]  0F 8A 1F 66 64 64 64 77
can0  0B0   [6]  00 00 00 00 11 00
can0  0B2   [6]  00 00 00 00 11 00
can0  1E3   [2]  40 26
can0  223   [8]  00 08 00 00 00 00 00 35
can0  020   [3]  20 00 07
can0  0B0   [6]  00 00 00 00 11 00
can0  0B2   [6]  00 00 00 00 11 00
can0  025   [8]  0F 8A 1F 66 64 64 64 77
can0  0B4   [8]  00 00 00 00 00 00 00 BC
can0  224   [8]  00 00 00 00 00 00 00 18
can0  2D0   [8]  00 00 01 00 10 00 00 EB
can0  442   [8]  40 02 00 00 04 00 00 00
can0  2C1   [8]  08 0E 1A 20 62 FF 00 7C
can0  2C6   [8]  00 00 00 00 00 00 00 D0
can0  2C4   [8]  00 F3 00 10 00 80 A1 F2
can0  020   [3]  20 00 07
can0  022   [8]  01 FE 01 FE 00 31 00 59
can0  025   [8]  0F 8A 1F 66 64 64 64 77
can0  0B0   [6]  00 00 00 00 11 00
can0  0B2   [6]  00 00 00 00 11 00
can0  0BA   [3]  21 FB D9
can0  1E3   [2]  40 26
can0  223   [8]  00 08 00 00 00 00 00 35
can0  2E1   [1]  00
can0  020   [3]  20 00 07
can0  0B0   [6]  00 00 00 00 11 00
can0  0B2   [6]  00 00 00 00 11 00
can0  025   [8]  0F 8A 1F 66 64 64 64 77
can0  0B4   [8]  00 00 00 00 00 00 00 BC
can0  224   [8]  00 00 00 00 00 00 00 18
```

A fuzzer was created to test the CANBus attack vector. While unlikely, and not very valuable, causing a crash of the dongle from CAN would still be entertaining.

Cellular Hardware

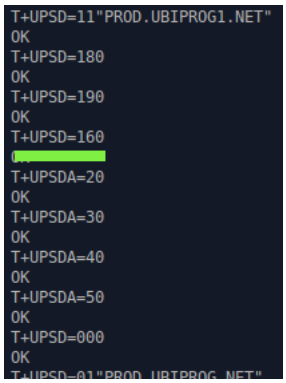


Cellular UART Analysis

AT+UPSD=
<profile_id> <tag> <val>

<tag>:

- 1: APN
- 6: Authentication
  - 0 (default): none
  - 1: PAP
  - 2: CHAP

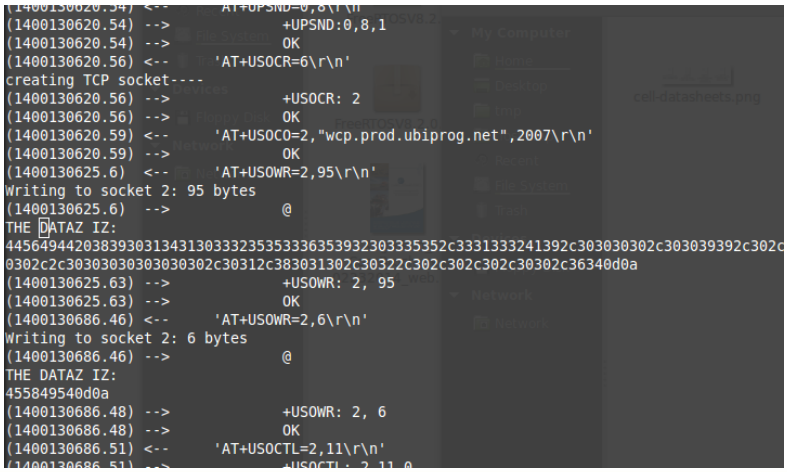


An **Access Point Name** (APN) is the name of a gateway between a GPRS, 3G or 4G mobile network and another computer network,

Cellular MitM

```
(1400165035.49) -->             OK
(1400165035.52) <--     'AT+UPSD=1,1,"PROD.UBIPROG1.NET"'
(1400165035.52) -->             OK
(1400165035.54) <--     'AT+UPSD=1,8,0'
(1400165035.54) -->             OK
(1400165035.57) <--     'AT+UPSD=1,9,0'
(1400165035.57) -->             OK
(1400165035.59) <--     'AT+UPSD=1,6,0'
(1400165035.59) -->             OK
(1400165035.62) <--     'AT+UPSDA=2,0'
(1400165035.62) -->             OK
(1400165035.64) <--     'AT+UPSDA=3,0'
(1400165035.64) -->             OK
(1400165035.67) <--     'AT+UPSDA=4,0'
(1400165035.67) -->             OK
(1400165035.69) <--     'AT+UPSDA=5,0'
(1400165035.69) -->             OK
(1400165035.72) <--     'AT+CREG?'
(1400165035.72) -->             +CREG: 2,1
(1400165035.72) -->             OK
(1400165052.24) <--     'AT'
(1400165052.24) -->             OK
(1400165053.26) <--     'AT+CGED=3'
(1400165053.26) -->             +CGED: RAT:"UMTS",
(1400165053.26) -->             URR:"ID",
(1400165053.26) -->             DC:002, BP:0005, M:003, ERR: 0, RC: 0, OOS:0
(1400165053.26) -->             Cell-ID:016578c, DLF:10813, ULF: 9863, SC:13
(1400165053.27) -->             Cell:U, SC:6, RSCP LEV:13, ECN0 LEV:28, DLF:
```

Cellular MitM - TCP Sockets



Cellular MitM - TCP Socket Payloads

Dongle cloud infrastructure systems use no authentication, encryption, or other security methodologies

```
$hexdump -C tcp-socket-send.bin
00000000  44 56 49 44 20 38 39 30  31 34 31 30 33 32 39 35  |DVID 89014103295|
00000010  33 36 32 39 32 30 33 35  35 2c 33 32 33 32 41 39  |362920355,3232A9|
00000020  2c 30 30 30 30 2c 30 30  39 39 2c 30 2c 50 52 44  |,0000,0099,0,PRD|
00000030  43 32 30 30 37 30 31 2c  30 30 30 30 2c 2c 30 30  |C200701,0000,,00|
00000040  30 30 30 30 30 30 2c 30  31 2c 38 30 31 30 2c 30  |000000,01,8010,0|
00000050  32 2c 30 2c 30 2c 30 2c  30 30 2c 36 34 0d 0a 45  |2,0,0,0,00,64..E|
00000060  58 49 54 0d 0a                                    |XIT..|
00000065
```

Findings

Lack of Security Controls

Poor Coding Practices

Findings - Lacking Security Controls

Authentication

- Cellular
- Cloud Infrastructure
- Hard coded

Code Verification

- Cryptographically signed firmware updates
- Encrypted Storage

Secure Communications

- Encryption over untrusted networks
- Non-Repudiation of activity
  - Insurance Fraud

Separation of Concerns

- Compromised CPU should not have arbitrary write access to CANBus

Findings - Secure Coding Practices

Rule #1: Banned Function usage

- strcpy()
- memcpy()
- etc

Input Validation

- Fuzzing can cause device to behave erratically

Arithmetic patterns:

- Integer overflow
- Integer underflow

Findings - Summary

- Security was not a consideration during development
- No modern development methodologies
  - Unit testing
  - Validation
  - Firmware signing - Intellectual property protection
- No end-to-end validation
  - Red Teaming
  - Third party testing

Defense

Defense

Secure Development Lifecycle

Threat Modeling

Segmentation & Separation of Concern

- e.g. Isolation of OBDII IDs vs arbitrary write

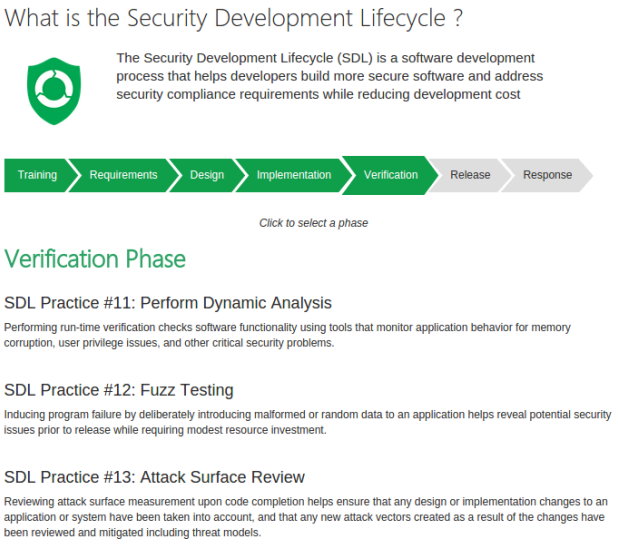
THIRD PARTY TESTING AND VALIDATION

- Internal
- External

Defense

Use modern Software Development methodologies

TEST YOUR STUFF!



Defense

Tool - Digital Bond Labs' "CAN Protector"

a.k.a the "CANdom"

https://github.com/digitalbond/canbus-protector

Defense

Tool - Digital Bonds' "CANbus Blackbox"

CAN data collector for forensic collection and analysis designed to survive any crash

Currently in development

Future Work

- Ongoing Vehicle Security Research
  - Virginia State Police Project
  - More 3rd Party Dongle Testing
  - Other vehicles to test
- Modify Dongle to Control Vehicle
- OBDII Security/Separation - Fixing Insecure by Design
- Radio Communications Attacks
- IDA FLIRT from symbol compiled RTOS

What is FLIRT? FLIRT stands for Fast Library Identification and Recognition Technology. This technology allows IDA to recognize standard library functions generated by supported compilers and greatly improves the usability and readability of generated disassemblies. This would help with reverse engineering RTOS.

Conclusions

- 3rd parties are attaching insecure by design systems to the cloud/net/borg
- 3rd parties are doing this poorly and not taking advantage of modern security technologies
- Vendors have to care. Isolation will not hold

Questions?

Corey Thuen, Digital Bond Labs
@CoreyThuen
thuen@digitalbond.com