

2015 Year in Review

Edward Fok
USDOT – FHWA Resource Center, San Francisco
2016 TRB Annual Meeting

Highlights

I. Vehicle Hacks

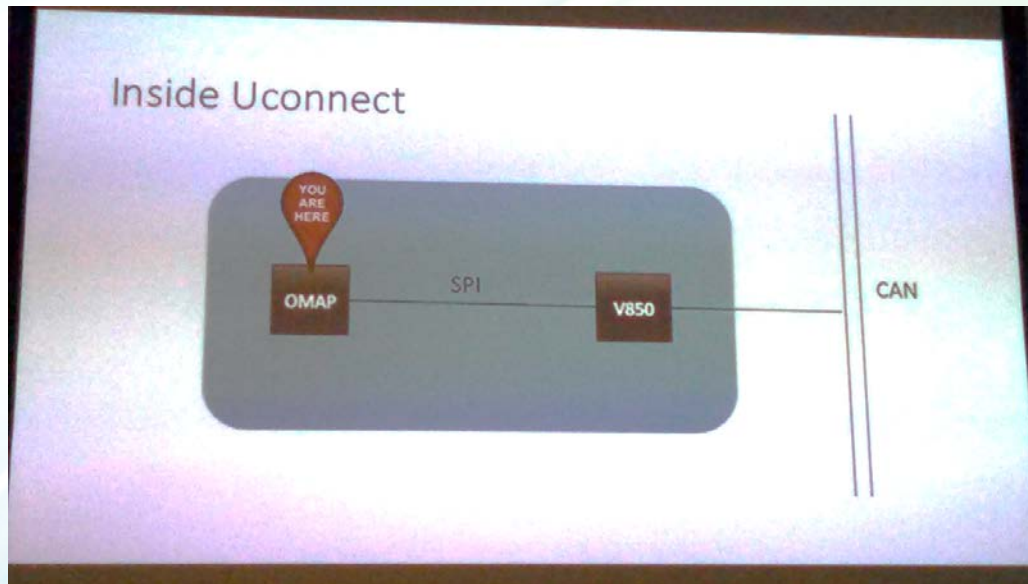
- a. Jeep Chrysler
- b. Tesla
- c. GM OnStar

II. Globalstar SPOT Message

III. DEFCON

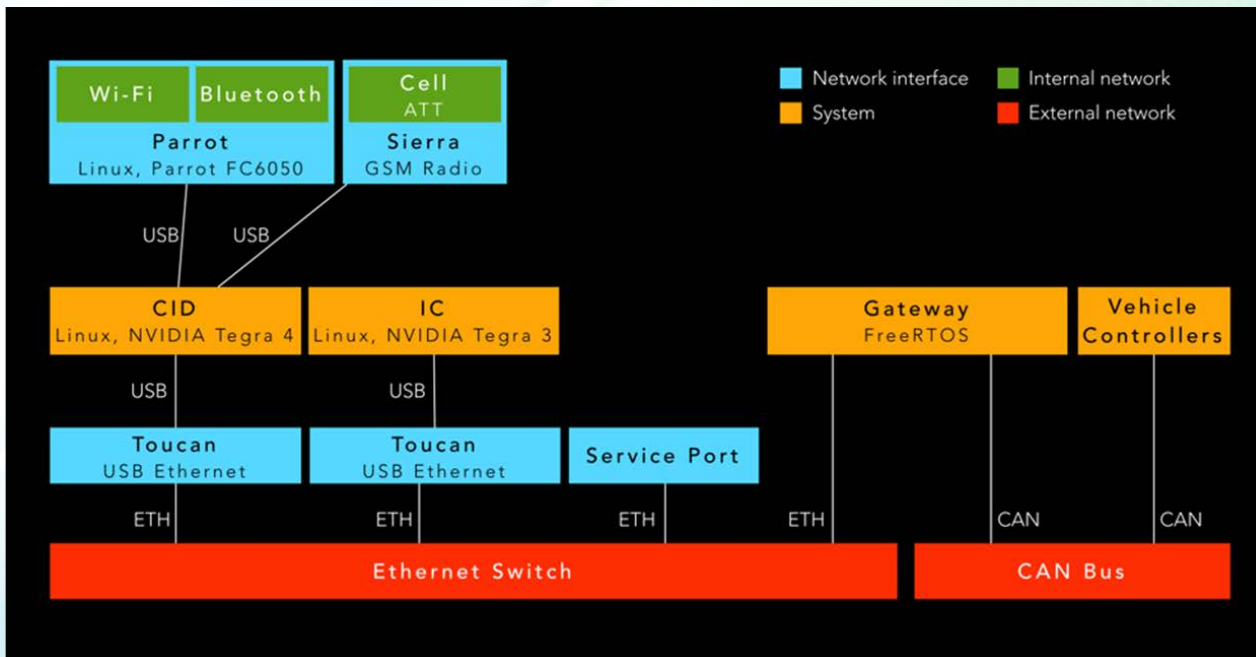
- a. Car Hacking Village
- b. Traffic Signal Hacking Competition
- c. GPS Spoofing Kit

Chrysler/Jeep/UConnect Hack



- D-BUS process visible from port 6667 within the Sprint network
- Compromised comm allow access to the OMAP ARM multi media processor
- Flash V850 Microcontroller from the OMAP chip over the Serial Peripheral Interface
- Compromised V850 are able to send CAN Messages.

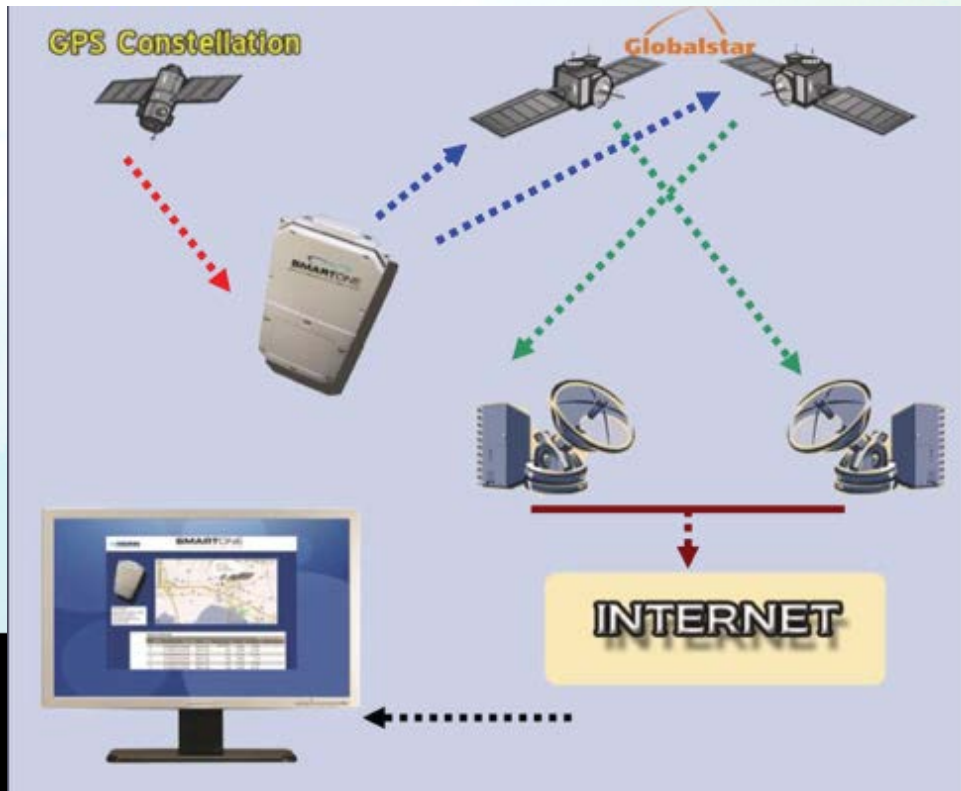
Tesla Hack



- **Static crypto key**
- **Vulnerable services on Center Information Display**
- **Fixed URL for updater from Tesla Server discovered on Instrument Cluster control unit**

SPOT Simplex Message

1. USRP B200 Radio ~\$800
2. No Authentication or Encryption
3. Message validated using checksum – reverse engineered



Military / Classified
Trailers / Containers
Air Quality Monitoring
Personnel Tracking
Fire Detection and Prevention
Water Quality Monitoring
Tank Level Gauging
Perimeter / Border monitoring
Asset / Vehicle Tracking
Remote Meters
Buoys
Ship Movement
Fishing vessel monitoring
Power line monitoring
Dispersed sensors

DEFCON Highlights

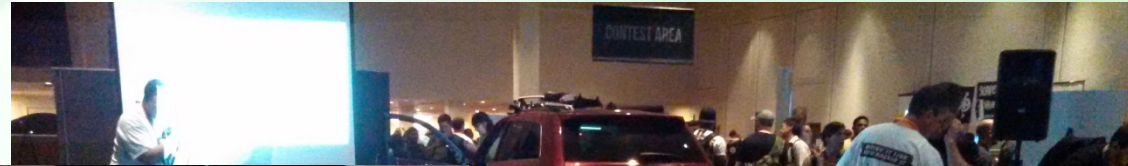
Car Hacking Village

- Significant interest on day 1
- Mainly an exercise in body work removal

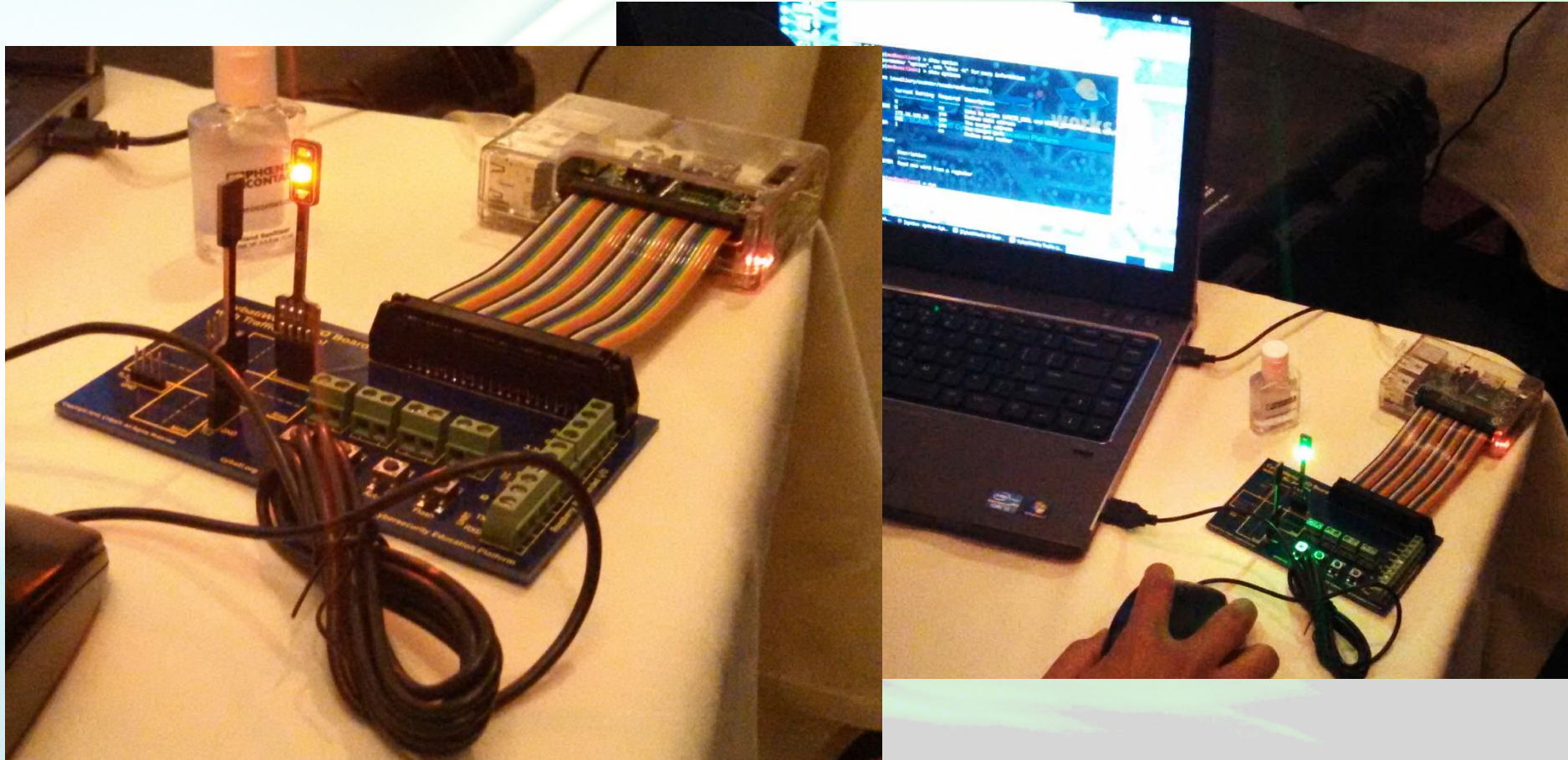
Traffic Signal Hacking Competition

- Custom architecture – not related to real hardware
- Raspberry Pi hacking competition

Car Hacking Village/Body Shop Class



Traffic Signal Hacking Competition



Synthetic GPS

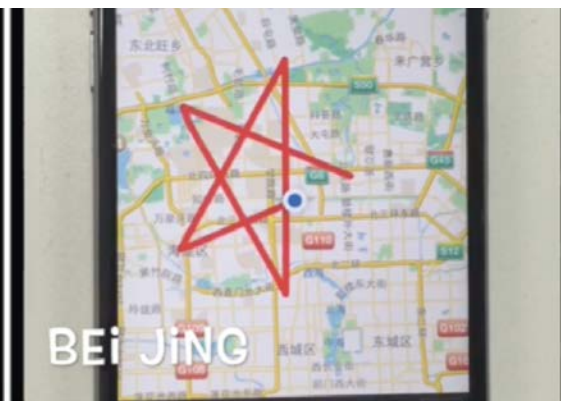
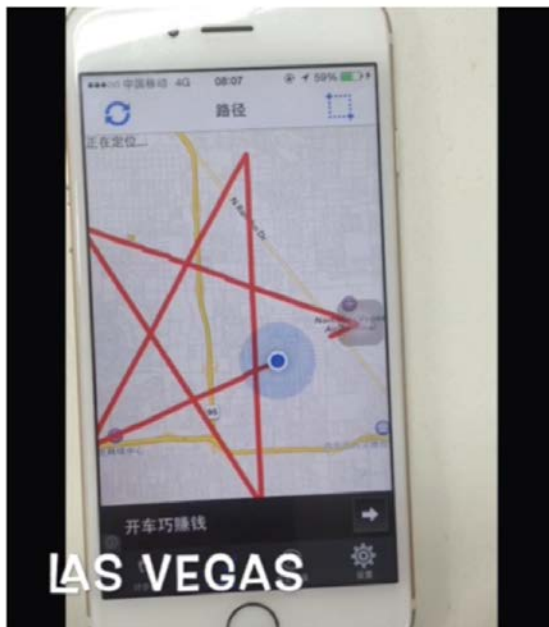
DIY GPS Signal Generator

- GPS Receiver, computer BladeRF
- Ephemeris data from NASA
- DIY Doppler Correction

Capability

- Position and velocity generation
- Time generation

Available as a kit during DEFCON for \$1500 from 360 Unicorn Team, China.



New Threats and Risks

Disclaimer: These are NOT OFFICIAL GOV POSITIONS

Threat level proportional to ability to monetize exploit.

Globalstar – SPOT Message are not signed or encrypted

- Injection of false message
- Denial of Services
- Both can enable more sophisticated attacks.

Car Hacking

- Physical access is needed to at least one vehicle
- Most like avenue of attacks involves Monetization
 - Blackmail targeted at OEM and vehicle manufacturers.

New Tools for the defense

Proven benefit of over the air updates

- Jeep – Reporting to patching 30 days to 10 months
- GM – 5 years
- Tesla – 1 week

DARPA Cyber Grand Challenge

- Potential of automating vulnerability assessment
- Winner will compete against human at DEFCON 24
- Can we use this to assess vulnerabilities of transportation systems?

DARPA Cyber Grand Challenge



- Automate network vulnerability discovery and exploitation
- August 4, 2016
- 7 Teams
 - ForAllSecure
 - Deep Red
 - TECHx
 - Shellphish
 - Disekt
 - Codejitsu
 - CSDS
- Winner will play against human Team at DEFCON 2016

SLICE MAPPING
Hilbert curve

SLICE SPACING
Instruction count

INDEPENDENT FILAMENTS
 AUTO-LOAD TRACES

INPUT 0

11	97,732 INST	●
10	10,823 INST	●
9	25,369 INST	●
8	34,500 INST	●
7	11,914 INST	●
6	10,847 INST	●
5	11,914 INST	●
4	94,924 INST	●
3	943,511 INST	●
2	232,014 INST	●
1	232,262 INST	●

Terminated normally with code 1

X ! Submission 4	X ! Submission 5
<pre>0x08048f05 lea edi, [edi+0x01] 0x08048f08 jne 0x08048f00 0x08048f00 cmp byte [esi+edi+0x01], 0x00 0x08048f05 lea edi, [edi+0x01] 0x08048f08 jne 0x08048f00 0x08048f00 cmp byte [esi+edi+0x01], 0x00 0x08048f05 lea edi, [edi+0x01]</pre>	<pre>0x080492e1 call 0x080488a0 0x080488a0 push ebx 0x080488a1 push edi 0x080488a2 push esi</pre>

RUN FORWARD RUN BACKWARD
JUMP TO START JUMP TO END
STEP INTO BACK INTO
STEP OVER BACK OVER
STEP OUT BACK OUT
HALT

Password fail – 2015 Edition



BY COUNT

Welcome1	30,465	123456	2,972
STORE123	21,362	summer11	2,610
Password1	15,383	Welcome01	2,512
password	9,466	Welcome123	2,438
Hello123	9,400	Changeme1	2,336
12345678	7,008	job12345	2,317
training	5,281	Welcome4	2,183
Welcome2	4,181	Password2	2,056
holiday	3,063	password1	2,053
Happy123	2,987	Welcome3	2,047
		Welcome22	2,029
		Spring10	1,907
		abcd1234	1,849
		Password123	1,714
		Summer11	1,473

Percentage of Unique Active Directory Samples Containing Password

However, Password1 is still widely used. By reviewing the number of samples (unique files of a single Active Directory environment) in which a particular password is found, Password1 is being used in more environments than Welcome1.



BY PERCENT

Password1	38.7%	12345678	9.2%
password	34.5%	Welcome2	7.6%
Welcome1	16.0%	Spring2012	6.7%
123456	12.6%	Summer2012	6.7%
P@ssw0rd	11.8%	Password3	6.7%
Passw0rd	10.9%	Hello123	5.9%
Password123	10.9%	Welcome3	5.9%
Password2	10.1%	Fall2012	5.9%
Summer12	10.1%	Spring12	5.9%
password1	10.1%	pa\$Sw0rd	5.9%
		p@ssw0rd	5.9%
		p@ssword	5.0%
		p@ssword1	5.0%
		Summer11	5.0%
		password9	5.0%

Password	Frequency
123456	120511
12345	48452
password	39448
DEFAULT	34275
123456789	26620
qwerty	20778
12345678	14172
abc123	10869
pu**y	10683
1234567	9468
696969	8801
ashley	8793
f**kme	7893
football	7872
baseball	7710
f**kyou	7458
111111	7048
1234567890	6572
ashleymadison	6213
password1	5959
madison	5219

Questions?



← Happy New Year!