2015 Year in Review

Edward Fok

USDOT – FHWA Resource Center, San Francisco

2016 TRB Annual Meeting

EDWARD FOK

Digitally signed by EDWARD FOK
DN: c=US, o=U.S. Government, ou=DOT FHWASacramentoCA, ou=FHWA FHWASacramentoCA, cn=EDWARD FOK
Date: 2016.02.09 13:39:05 -08'00'

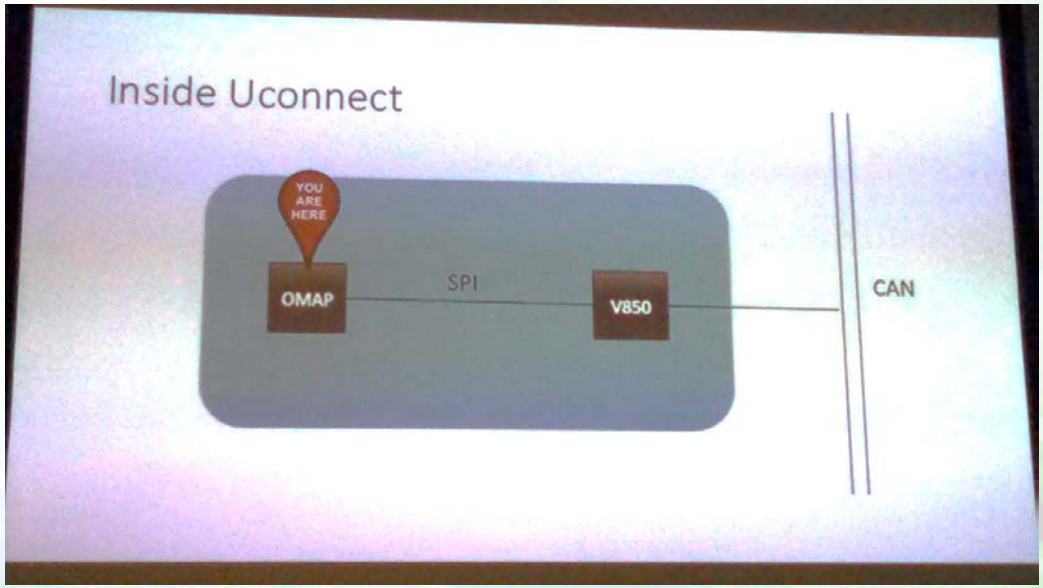
Highlights

I. **Vehicle Hacks**
   a. Jeep Chrysler
   b. Tesla
   c. GM OnStar

II. **Globalstar SPOT Message**

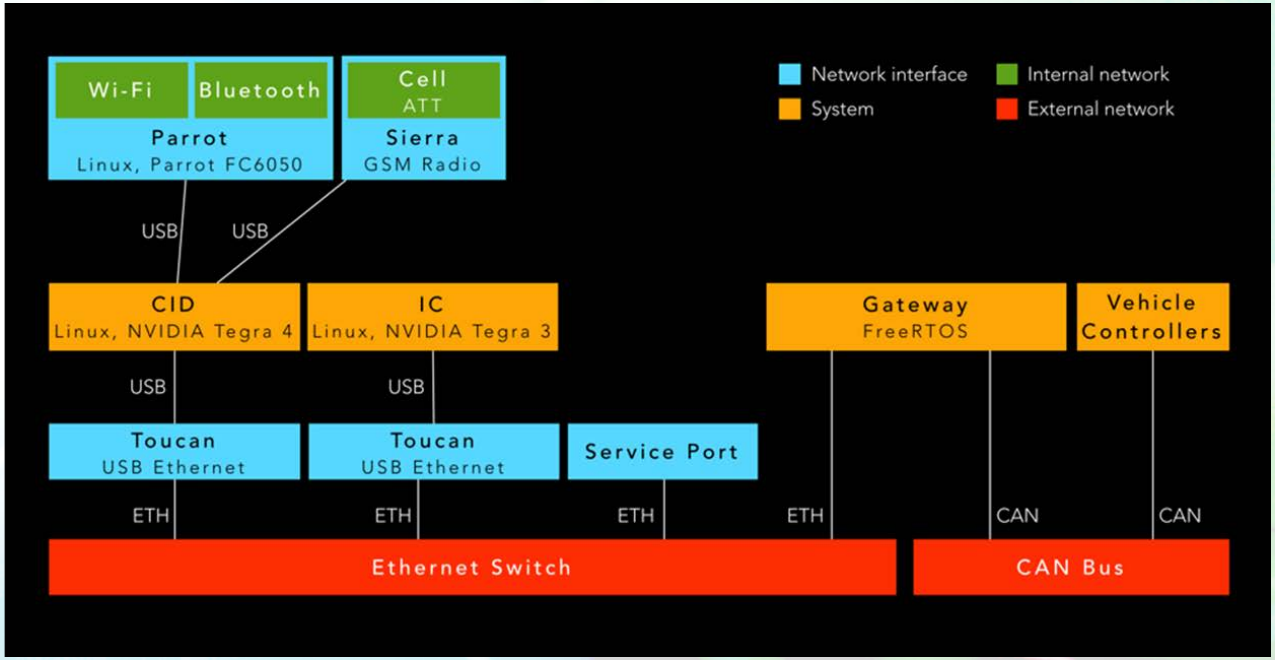
III. **DEFCON**
   a. Car Hacking Village
   b. Traffic Signal Hacking Competition
   c. GPS Spoofing Kit

Chryslar/Jeep/UConnect Hack



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

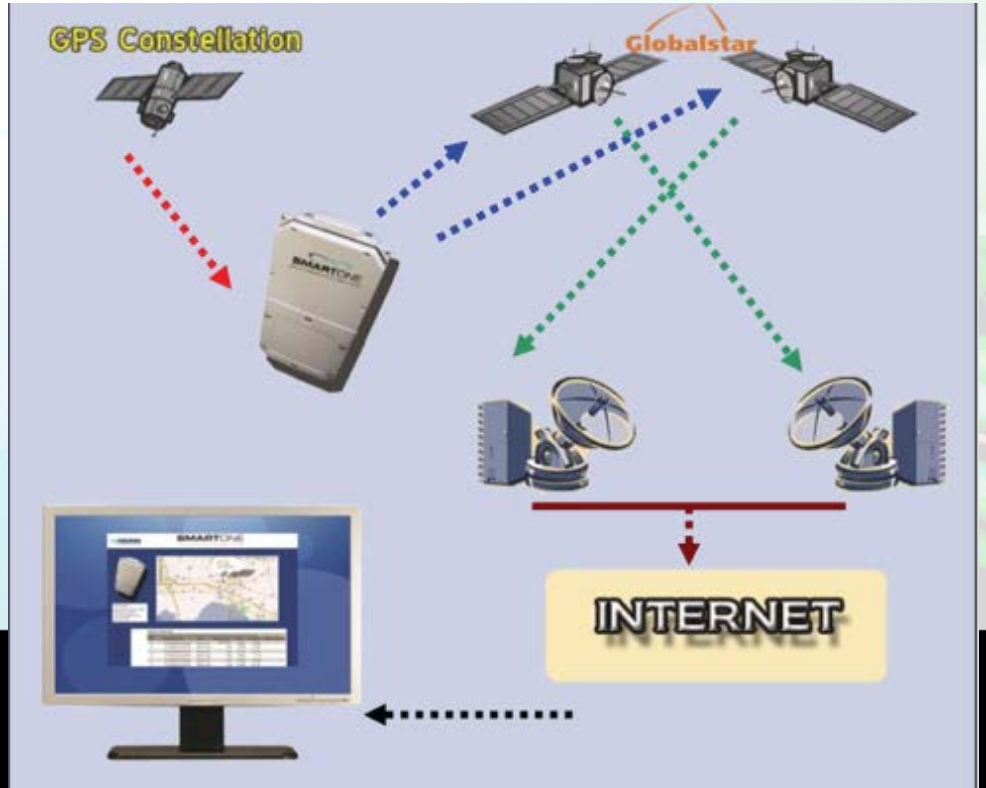
Tesla Hack



- 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

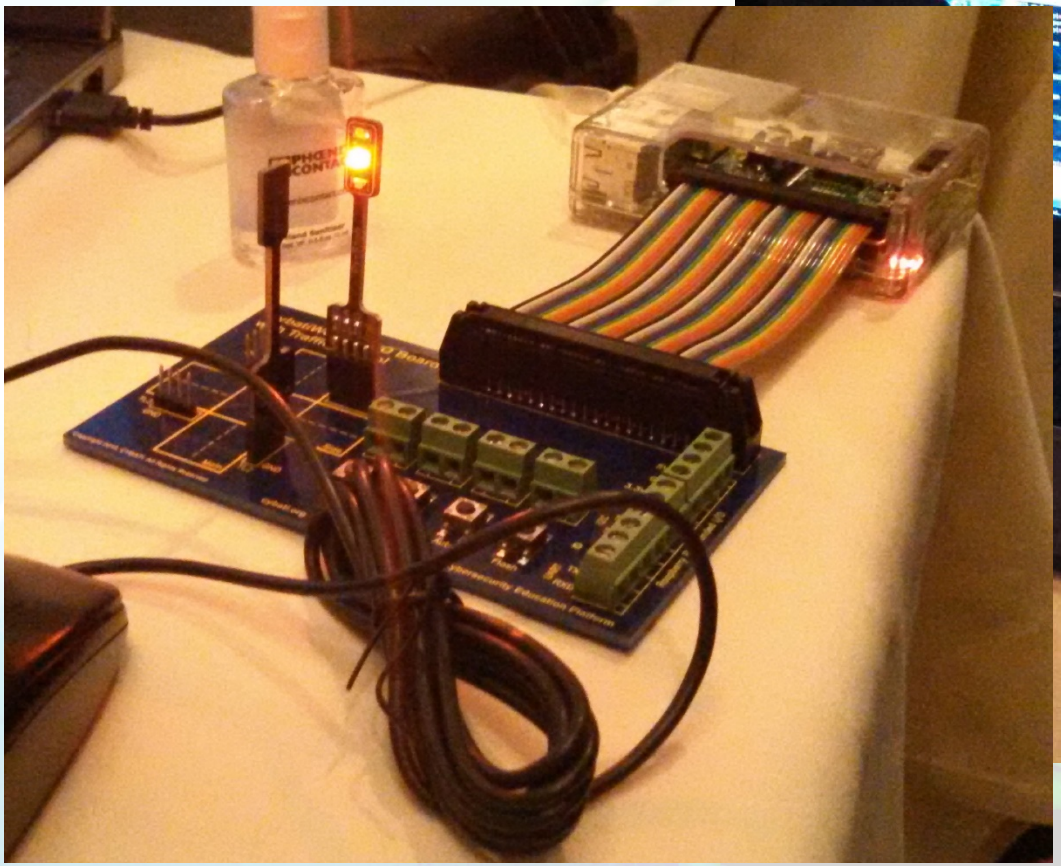
- Significant interest on day 1
- Mainly an exercise in body work removal

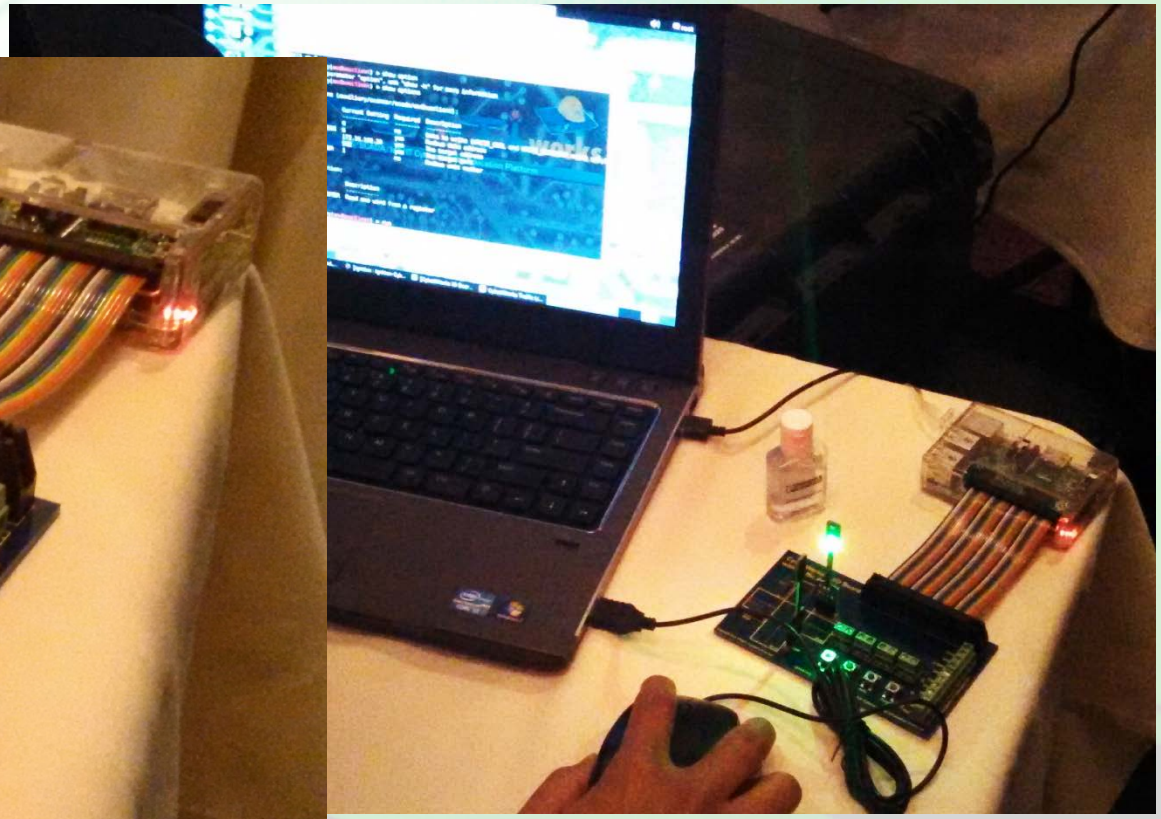
Traffic Signal Hacking Competition

- 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**

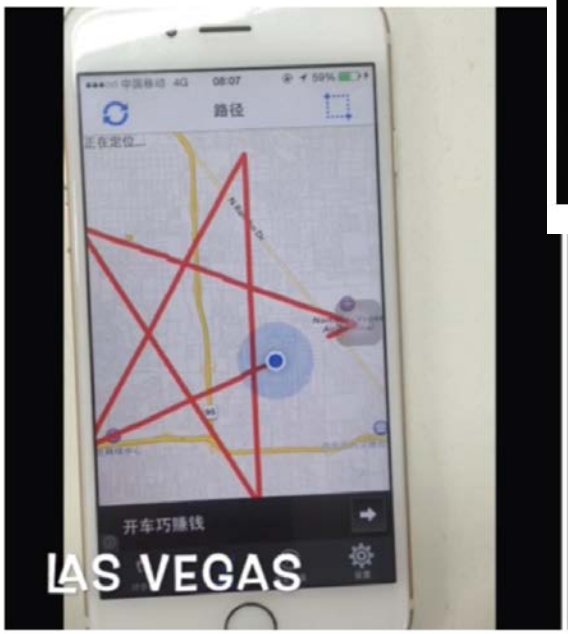
Capability

- **Position and velocity generation**
- **Time generation**

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


BYD AUTO
14:32
兴趣点
路牌
雷达圈
全路径
N
嘎雄村
桑尼
纳木错
返回桌面
菜单
目的地

秦EV


路径
开车巧赚钱
LAS VEGAS


BEi JiNG

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

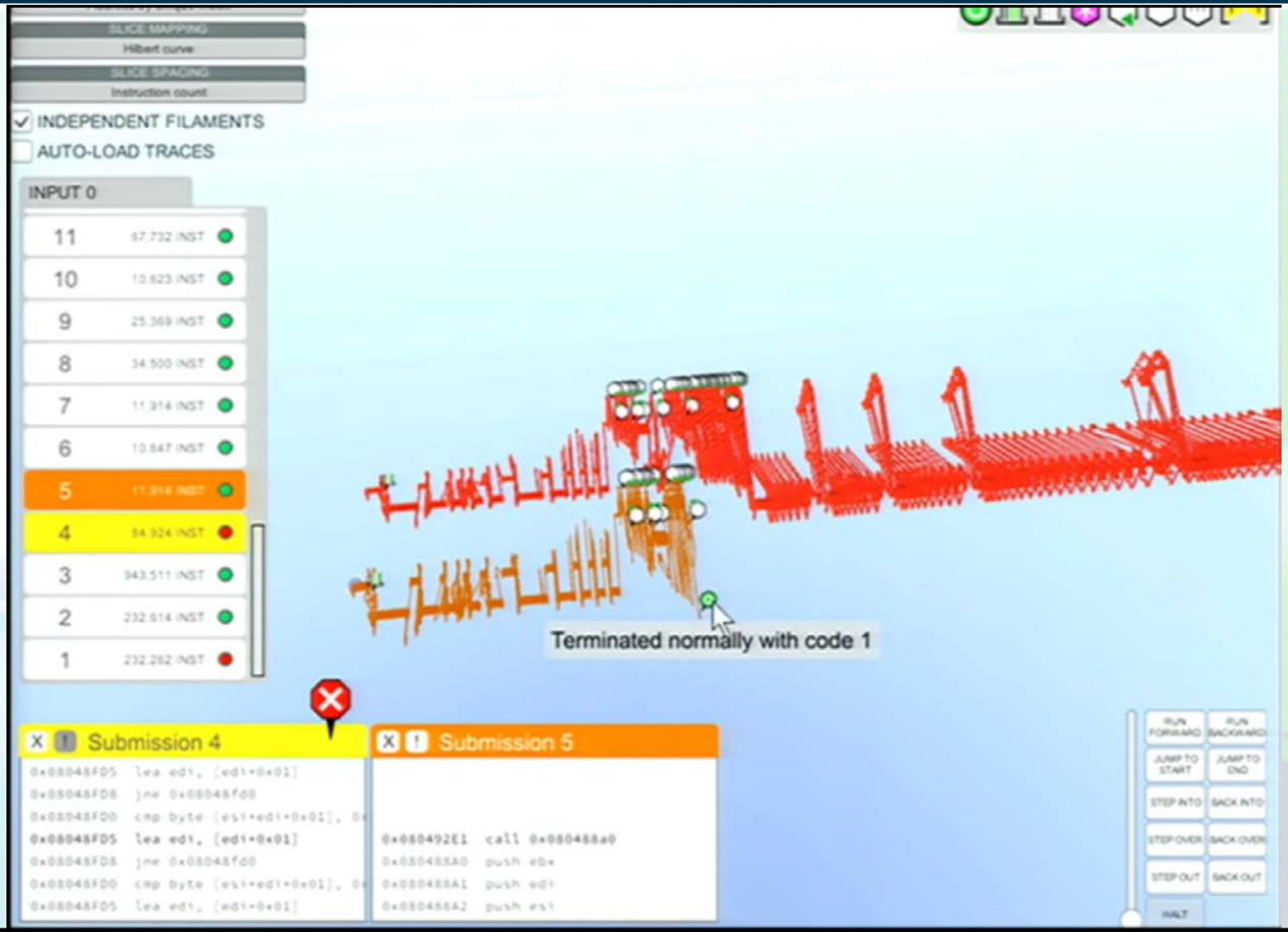
- Jeep – Reporting to patching 30 days to 10 months
- GM – 5 years
- Tesla – 1 week

DARPA Cyber Grand Challenge

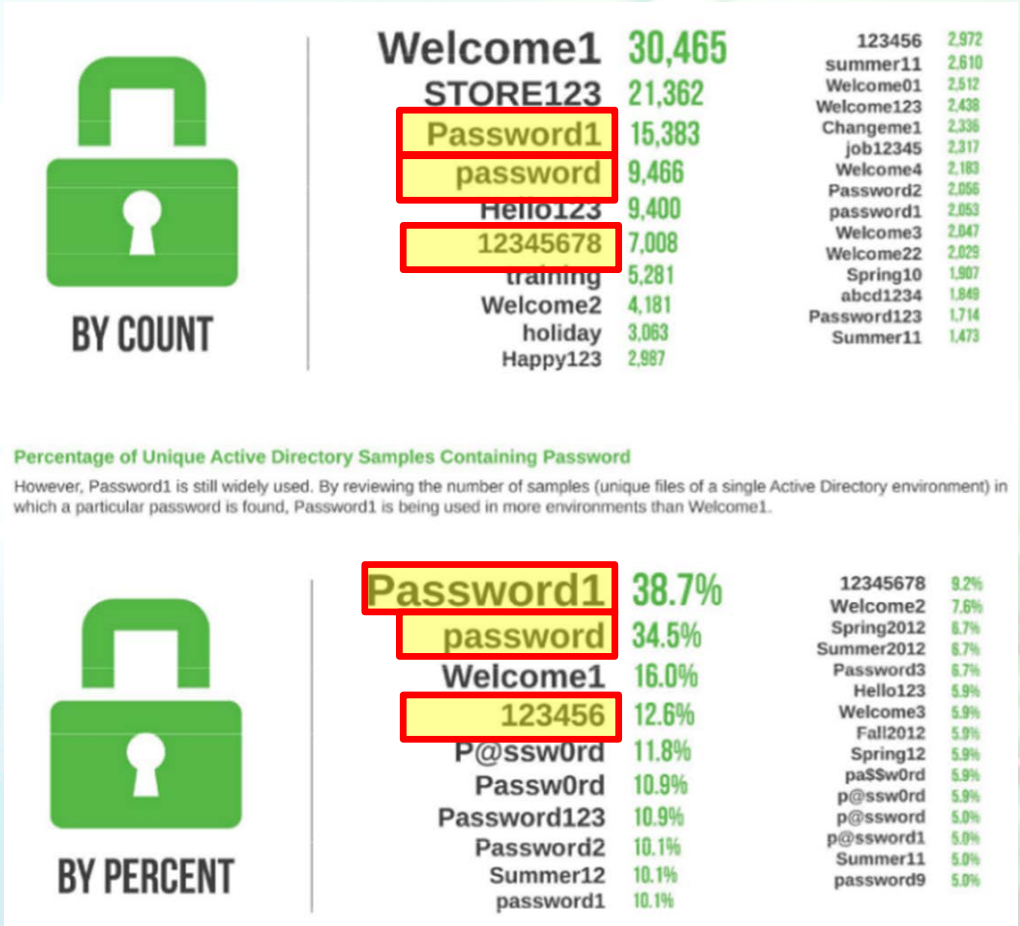
- Potential of automating vulnerability assessment
- Winner will compete against human at DEFCON 24
- Can we use this to assess vulnerabilities of transportation systems?

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
10
9
8
7
6
5
4
3
2
1
Terminated normally with code 1
Submission 4
Submission 5
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



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!