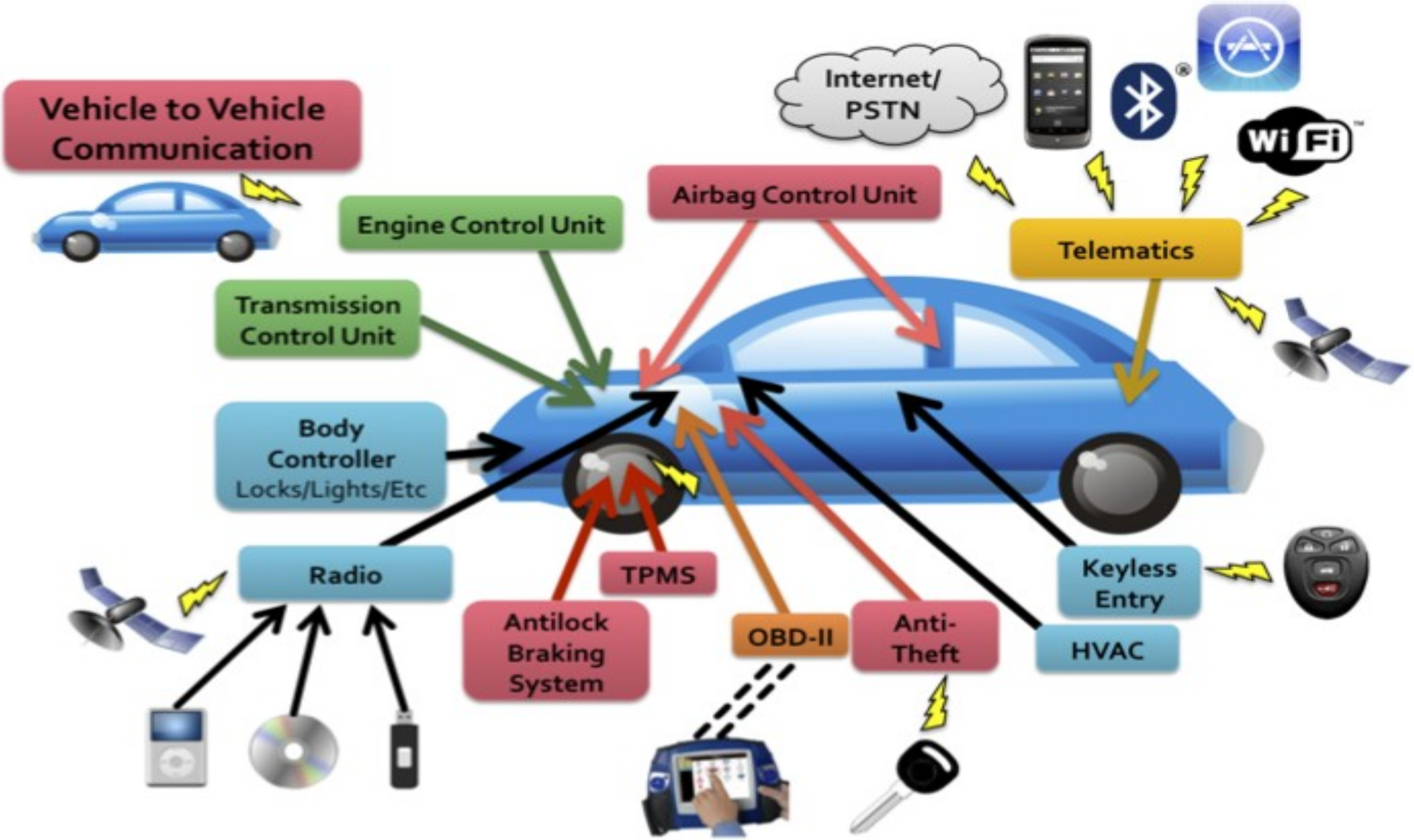
Automotive Exploitation Techniques

Craig Smith
@OpenGarages

SHAKACON
SUN, SURF, & C SHELLS™

Identifying Exploits

Attack Surface

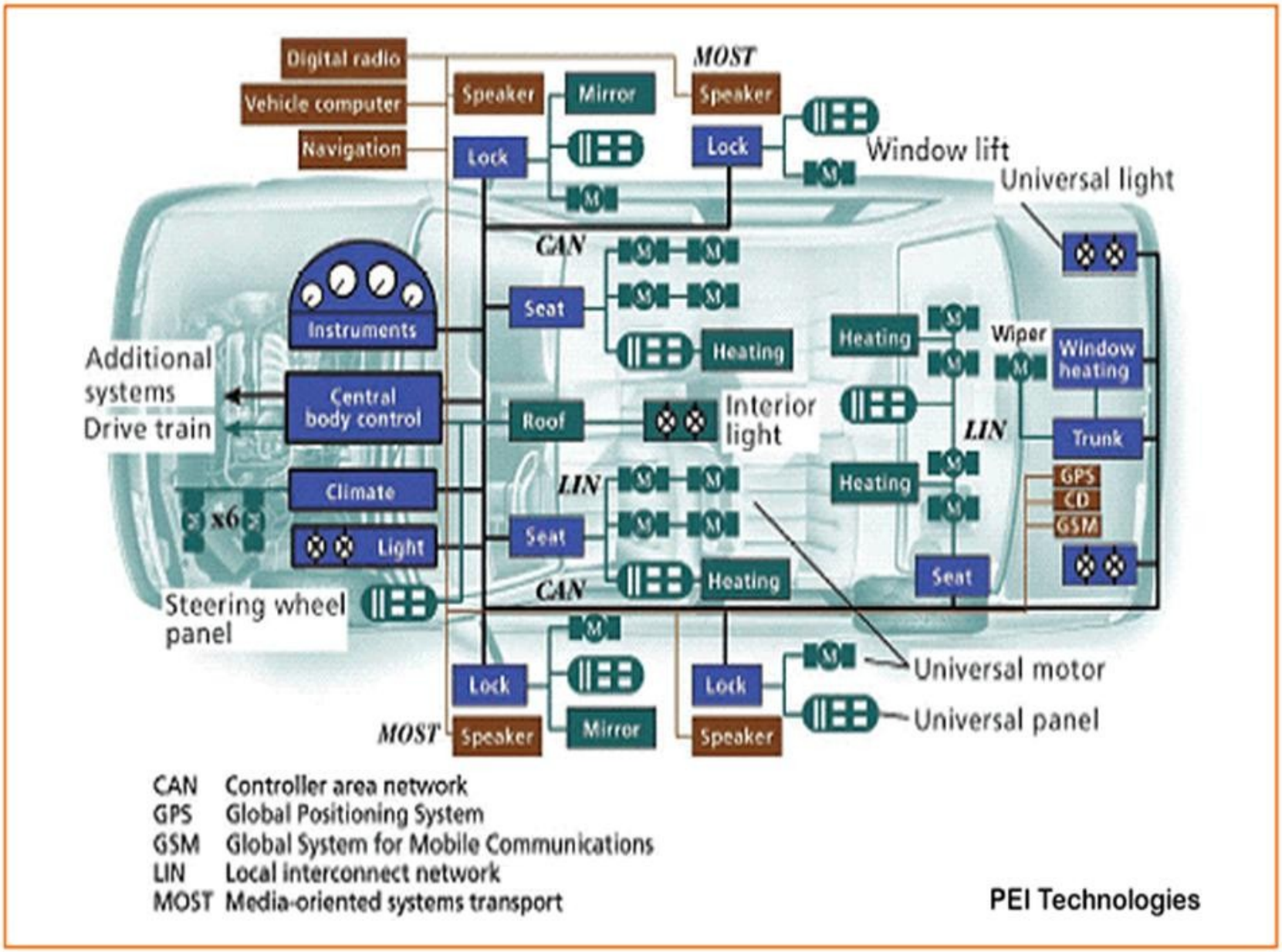


Common Components

Payloads

- Run on IVI
  - Listen over MIC
  - Pull contacts
  - Communicate with CELL
- Manipulate vehicle Components
  - Affect Steering and Controls
  - Unlock Vehicle
  - Start Car
- Reflash firmware
  - Permanent Changes
  - Bypass protections

Vehicle Network Payloads



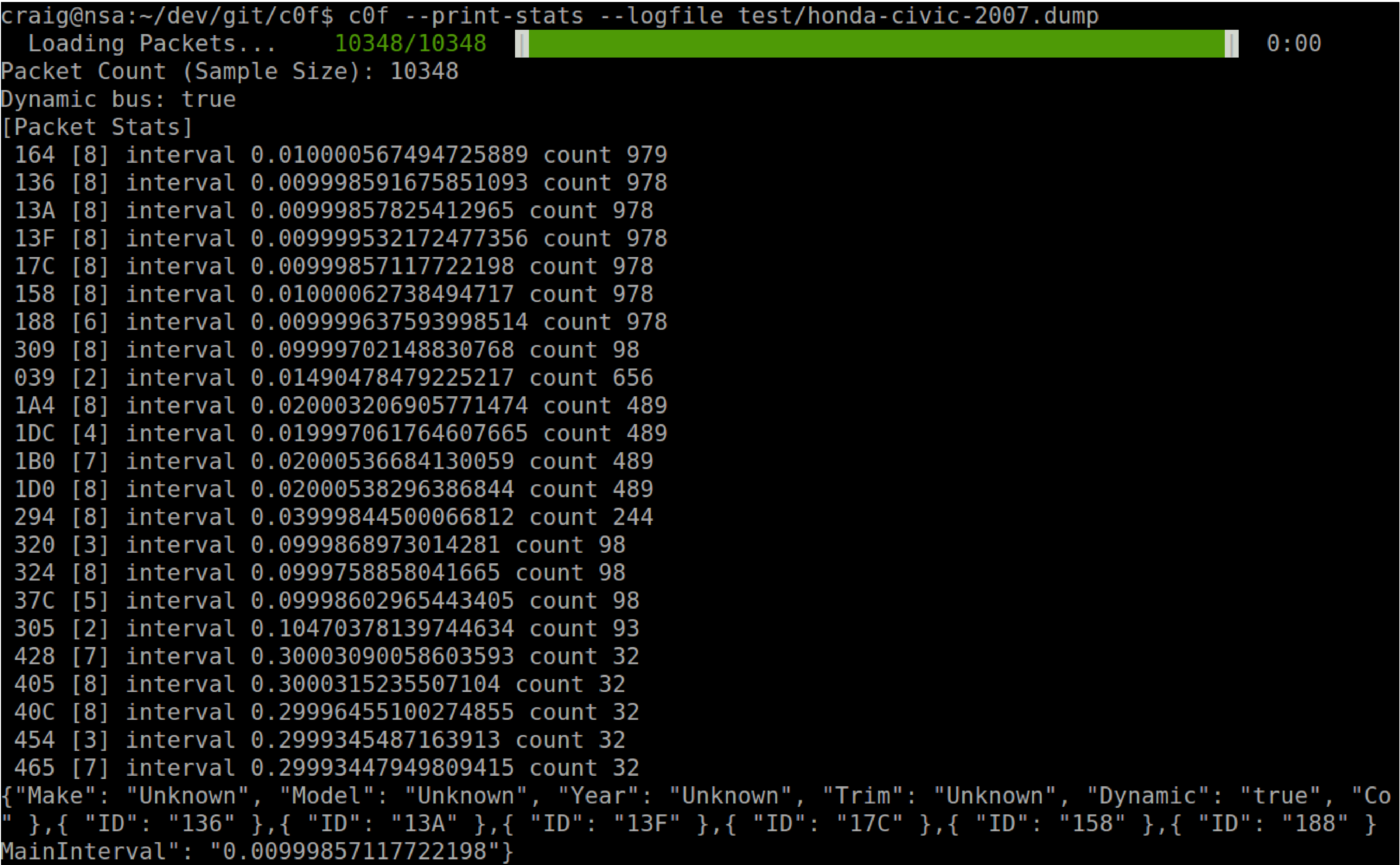
CAN Bus Complications

- Can't shutoff the device you want to spoof
- Need to talk more often than original source
- Each Make/Model is different
- IDS Systems?

Passive Vehicle Detection

- CAN of Fingers (c0f)

How c0f works



```
craig@nsa:~/dev/git/c0f$ c0f --print-stats --logfile test/honda-civic-2007.dump
  Loading Packets...    10348/10348                                                    0:00
Packet Count (Sample Size): 10348
Dynamic bus: true
[Packet Stats]
 164 [8] interval 0.010000567494725889 count 979
 136 [8] interval 0.009998591675851093 count 978
 13A [8] interval 0.00999857825412965 count 978
 13F [8] interval 0.009999532172477356 count 978
 17C [8] interval 0.00999857117722198 count 978
 158 [8] interval 0.01000062738494717 count 978
 188 [6] interval 0.009999637593998514 count 978
 309 [8] interval 0.09999702148830768 count 98
 039 [2] interval 0.01490478479225217 count 656
 1A4 [8] interval 0.020003206905771474 count 489
 1DC [4] interval 0.019997061764607665 count 489
 1B0 [7] interval 0.02000536684130059 count 489
 1D0 [8] interval 0.02000538296386844 count 489
 294 [8] interval 0.03999844500066812 count 244
 320 [3] interval 0.0999868973014281 count 98
 324 [8] interval 0.0999758858041665 count 98
 37C [5] interval 0.09998602965443405 count 98
 305 [2] interval 0.10470378139744634 count 93
 428 [7] interval 0.30003090058603593 count 32
 405 [8] interval 0.3000315235507104 count 32
 40C [8] interval 0.29996455100274855 count 32
 454 [3] interval 0.2999345487163913 count 32
 465 [7] interval 0.29993447949809415 count 32
{"Make": "Unknown", "Model": "Unknown", "Year": "Unknown", "Trim": "Unknown", "Dynamic": "true", "Co
" },{ "ID": "136" },{ "ID": "13A" },{ "ID": "13F" },{ "ID": "17C" },{ "ID": "158" },{ "ID": "188" }
MainInterval": "0.00999857117722198"}
```

Utilizing c0f results in Exploits

$ c0f --fpdb test/sample.db --logfile test/honda-civic-2007.dump

Loaded 1 fingerprints from DB

{"Make":"Honda","Model":"Civic","Year":"2009","Trim":"Hybrid","Dynamic":"true","Common":[{"ID":"164"},{"ID":"136"},{"ID":"13A"},{"ID":"13F"},{"ID":"17C"},{"ID":"158"},{"ID":"188"}],"MainID":"17C","MainInterval":"0.00999857117722198","Confidence":64}

Bonus Identification

```
$ c0f --find-pattern bBbBbbbB --logfile test/sample-can.log --quiet --no-print-fp
{ "Matches": [  { "ID": "095", "Position": "6", "Values": [ "0", "1" ] }] }

$ grep 095# test/sample-can.log | head
(1398128223.810456) can0 095#800007F40000**01**08
(1398128223.820460) can0 095#800007F40000**00**17
(1398128223.830460) can0 095#800007F40000**01**26
(1398128223.840462) can0 095#800007F40000**00**35
(1398128223.850465) can0 095#800007F40000**01**08
(1398128223.860468) can0 095#800007F40000**01**17
(1398128223.870470) can0 095#800007F40000**01**26
(1398128223.880471) can0 095#800007F40000**00**35
(1398128223.890477) can0 095#800007F40000**01**08
(1398128223.900480) can0 095#800007F40000**00**17
```

Where to get c0f?

- https://github.com/zombieCraig/c0f
- Gem install c0f

F1337 Management

F1337 Mgmt Structure

Checks Server
For Commands
In Queue

Enter Commands
For Vehicles over
Web Interface

NBC Demo

Client API

- Request
  - ?poll=<VIN|UID>&methods=<SUPPORTED>
- Response (multi-line)
  - Wipers <on|off>
  - Lights <on|off|flash>
  - Flood <rpm|temp|fuel>
  - Cansend <dev> <packet>
  - Cansend stop

Command Interface

- Web based AJAX. PHP back-end
- Terminal Emulation
- Login Credentials
- Fleet Management
- Basic scripting capabilities

Future Direction

- Grouping of vehicles
- DB Backend with saved state
- Additional reporting (DTC, GEO Location)

Where to get F1337?

What Can Be Done?

5-Star Cyber Safety

Formal Capacities

1. **Safety By Design**
2. **Third Party Collaboration**
3. **Evidence Capture**
4. **Security Updates**
5. **Segmentation and Isolation**

Plain Speak

1. Avoid Failure
2. Engage Allies To Avoid Failure
3. Learn From Failure
4. Respond to Failure
5. Isolate Failure

Further Research

- Open Garages
  - http://opengarages.org
  - @OpenGarages
- IamTheCavalry
  - http://iamthecavalry.org
  - @IAmTheCavalry

Car Hacker's Handbook

Next Version Teaser ToC (3x size):


IF YOU TURN RIGHT DURING A NASCAR RACE...
YOUR GONNA HAVE A BAD TIME
memecenter.com
MemeCenter