RSA Conference 2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HTA-T09

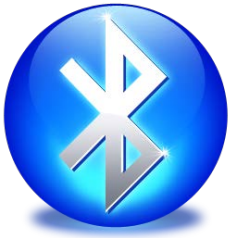
Collision Investigator: Aftermath of the Auto Hacks

Craig Smith
craig@TheiaLabs.com
OpenGarages.org
@OpenGarages
@IAmTheCavalry

#RSAC

Traditionally Hackable

I am The Cavalry



I am The Cavalry

I am The Cavalry

I am The Cavalry


¯_(ツ)_/¯

What makes vehicles a good target?

1) Accessibility
2) Fun
3) History of Tinkering
4) High shock value

What makes vehicles an unlikely target?

1) Covers many specialties
2) “Hard”

I am The Cavalry

Traditionally Secure

- Encrypting All the Things
- Firewalls and IDS
- PKI Lockouts and Control

I am The Cavalry

I am The Cavalry

I am The Cavalry

I am The Cavalry

Demo Disclaimer

CAN Bus Packet Layout

```
Interface   ID    DLC
     can0   666   [8]  01 02 03 04 05 06 07 08
                                 Data
```

```
can0  7DF   [4]  03 22 F1 A1
can0  7E8   [8]  10 0E 62 F1 A1 41 41 41
can0  7DF   [3]  30 00 00
can0  7E8   [8]  21 41 41 41 41 41 41 41
can0  7E8   [8]  22 41 AA AA AA AA AA AA
```

7DF = Our Packets

7E8 = Response from ECU

I am The Cavalry

```
can0  7DF   [4]  03 22 F1 A1
can0  7E8   [8]  10 0E 62 F1 A1 41 41 41
can0  7DF   [3]  30 00 00
can0  7E8   [8]  21 41 41 41 41 41 41 41
can0  7E8   [8]  22 41 AA AA AA AA AA AA
```

0x22 = ReadById
0xF1 0xA1 = ID to read from Memory
0x62 = Positive Response

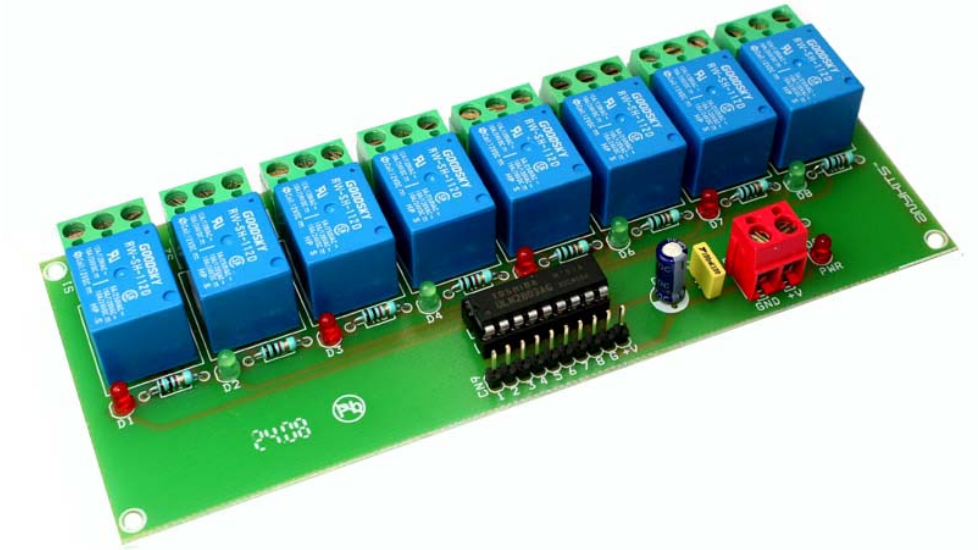
```
can0  7DF   [3]  02 27 01
can0  7E8   [8]  06 67 01 FA 91 A4 68 00
can0  7DF   [7]  06 27 02 01 02 03 04
can0  7E8   [8]  03 7F 27 35 00 00 00 00
```

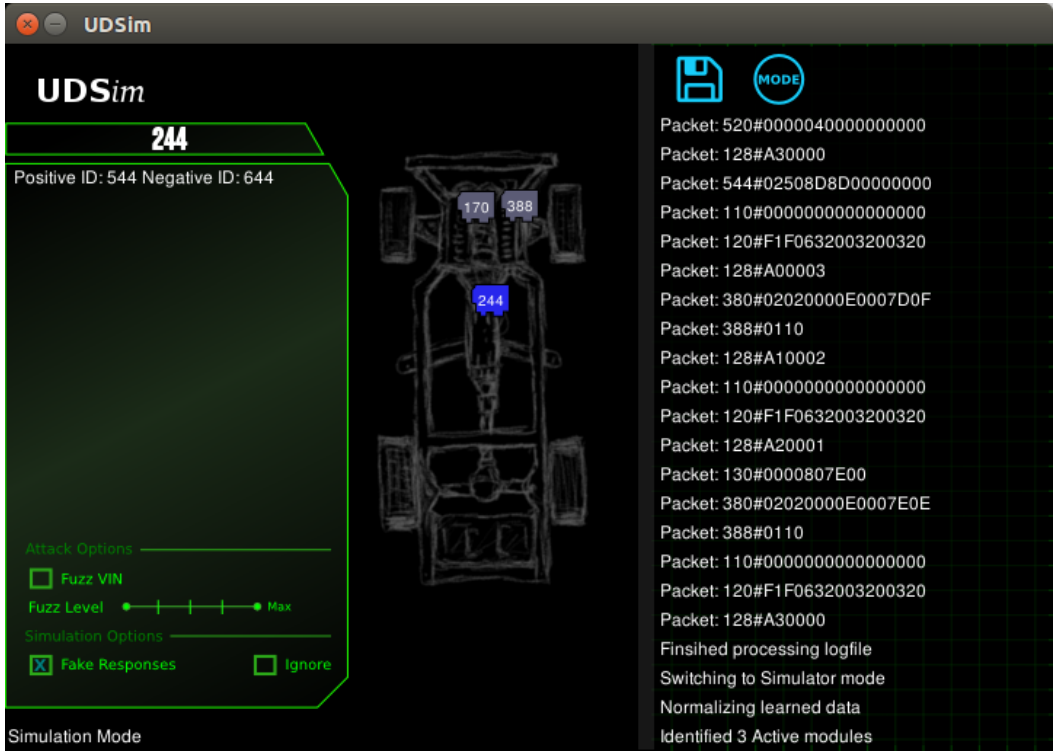
0x27 = SecurityAccess
   0x01 = GetKey
   0x02 = SendResponse
Key in this case = 0xFA91A468
0x7F in a response is an Error

I am The Cavalry

Issues with this method

- Small Keyspace
- Inefficient Lockouts
- Memory Leakage





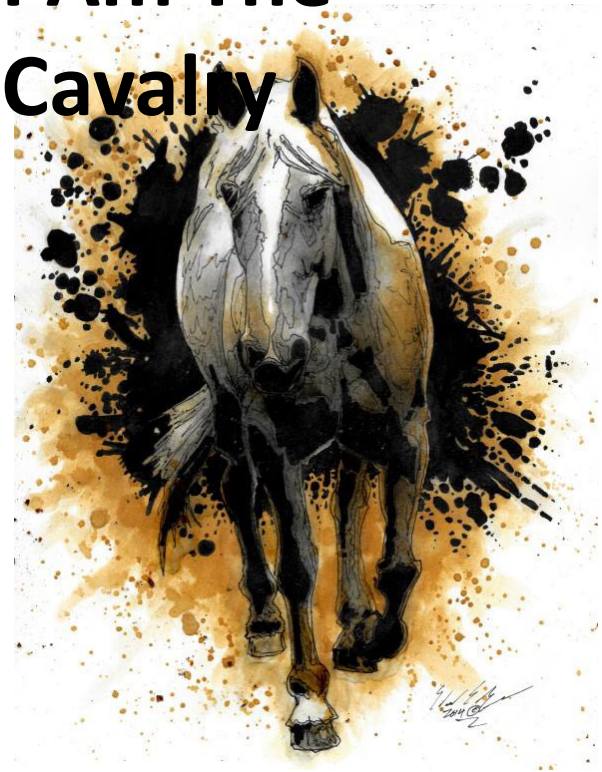
I am The Cavalry

I am The Cavalry

Allow unsigned updates

Use physical verification

I Am The Cavalry



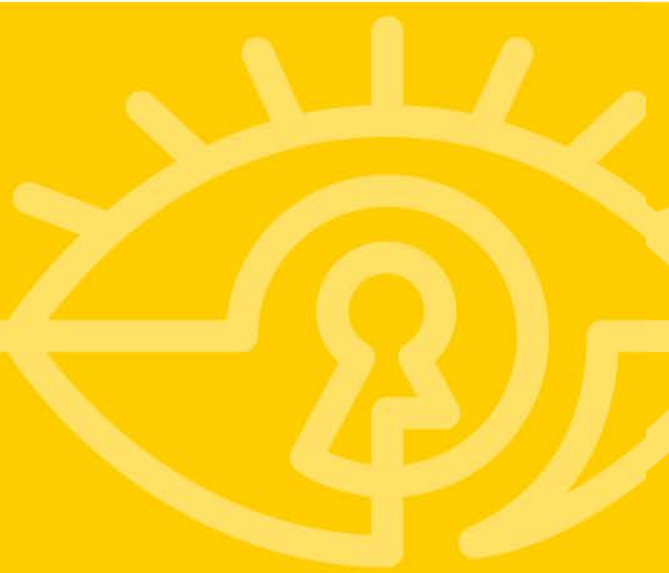
I am The Cavalry

- Safety By Design
- Third Party Collaboration
- Evidence Capture
- Security Updates
- Segmentation and Isolation

I am The Cavalry

“Apply” Slide

- Next week you should:
  - Look at what you are doing and compare them to the 5 stars
- In the next three months:
  - Identify products for an immediate Threat Model review
  - Have a published method for researchers to submit findings
- Within six months you should:
  - Performed a threat model on all of your products
  - Determine what it will take to implement an Over-The-Air (OTA) patching system for your product



Subhead if needed