

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: HTA-T09

Collision Investigator: Aftermath of the Auto Hacks



Connect **to**
Protect

Craig Smith

craig@TheiaLabs.com

OpenGarages.org

[@OpenGarages](https://twitter.com/OpenGarages)

[@IAmTheCavalry](https://twitter.com/IAmTheCavalry)



#RSAC

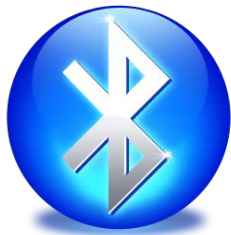


Traditionally Hackable





#RSAC



I am The Cavalry

RSAConference2016



#RSAC



I am The Cavalry

RSAConference2016



#RSAC



I am The Cavalry

RSAConference2016



#RSAC

על (צ)ל

I am The Cavalry

RSA[®]Conference2016



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"



Traditionally Secure

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



I am The Cavalry



#RSAC



I am The Cavalry

RSA[®]Conference2016



I am The Cavalry



Demo Disclaimer





CAN Bus Packet Layout

Interface	ID	DLC	01	02	03	04	05	06	07	08
can0	666	[8]	<div data-bbox="913 609 1607 647" style="border-top: 1px solid black; border-left: 1px solid black; border-right: 1px solid black; height: 35px; position: relative;"><div data-bbox="1203 656 1315 702" style="position: absolute; bottom: 5px; right: 5px;">Data</div></div>							



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



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

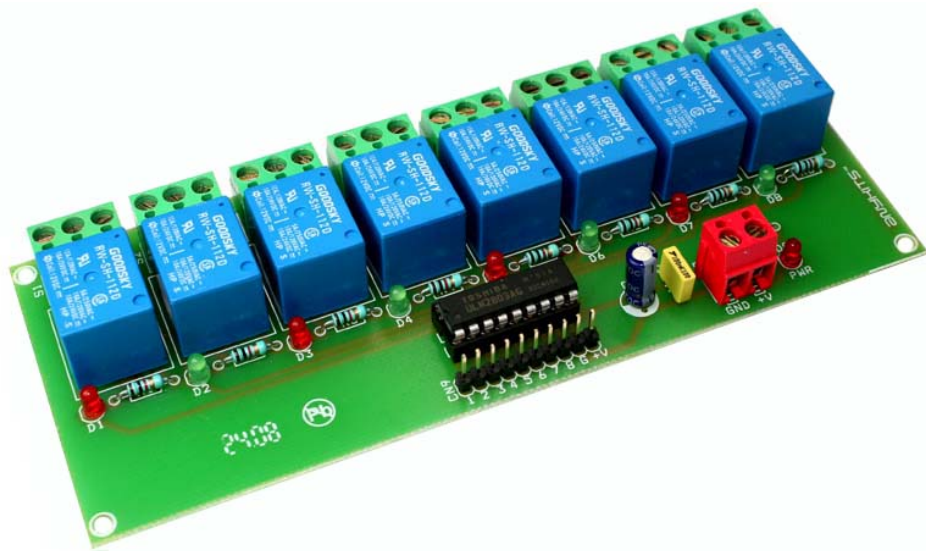
Key in this case = 0xFA91A468

0x7F in a response is an Error



Issues with this method

- Small Keyspace
- Inefficient Lockouts
- Memory Leakage





UDSim

244

Positive ID: 544 Negative ID: 644

Attack Options

☐ Fuzz VIN

Fuzz Level Max

Simulation Options

☒ Fake Responses ☐ Ignore

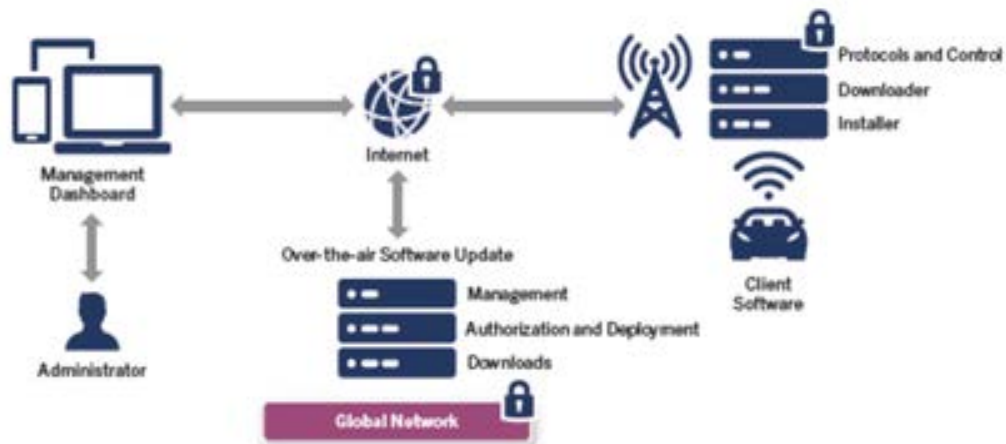
Simulation Mode

170 388 244

Packet: 520#0000040000000000
Packet: 128#A30000
Packet: 544#02508D8D00000000
Packet: 110#0000000000000000
Packet: 120#F1F0632003200320
Packet: 128#A00003
Packet: 380#02020000E0007D0F
Packet: 388#0110
Packet: 128#A10002
Packet: 110#0000000000000000
Packet: 120#F1F0632003200320
Packet: 128#A20001
Packet: 130#0000807E00
Packet: 380#02020000E0007E0E
Packet: 388#0110
Packet: 110#0000000000000000
Packet: 120#F1F0632003200320
Packet: 128#A30000
Finished processing logfile
Switching to Simulator mode
Normalizing learned data
Identified 3 Active modules



OTA Software Update





Allow unsigned updates

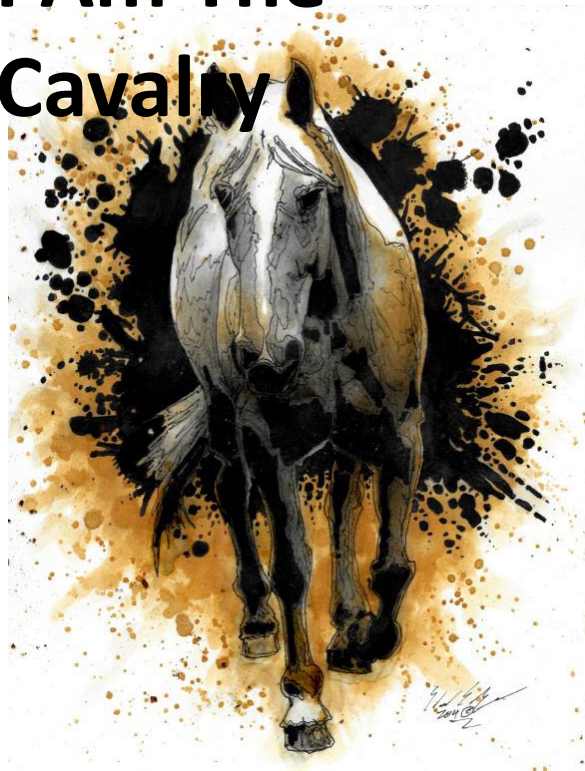


Use physical
verification



#RSAC

I Am The Cavalry



I am The Cavalry

RSAConference2016



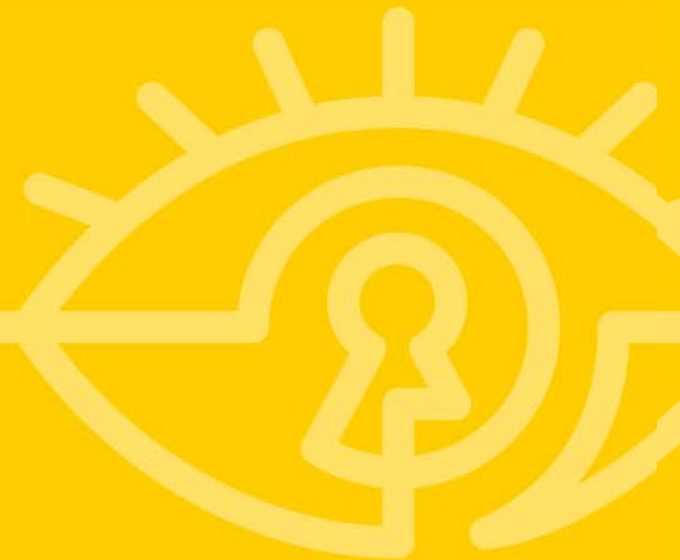
- ★ Safety By Design
- ★ Third Party Collaboration
- ★ Evidence Capture
- ★ Security Updates
- ★ Segmentation and Isolation

“Apply” Slide



#RSAC

- 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