Hacking (autonomous) Vehicles

A brief survey of recent work

SparkFun AVC

Updated: 17 September 2016

cryptotronix

Overview

1. Introduction

2. HOPE XI Talks

3. Blackhat 2016 Talks

4. DEF CON 2016 Tracks

5. DEF CON 2016 Car Hacking Village

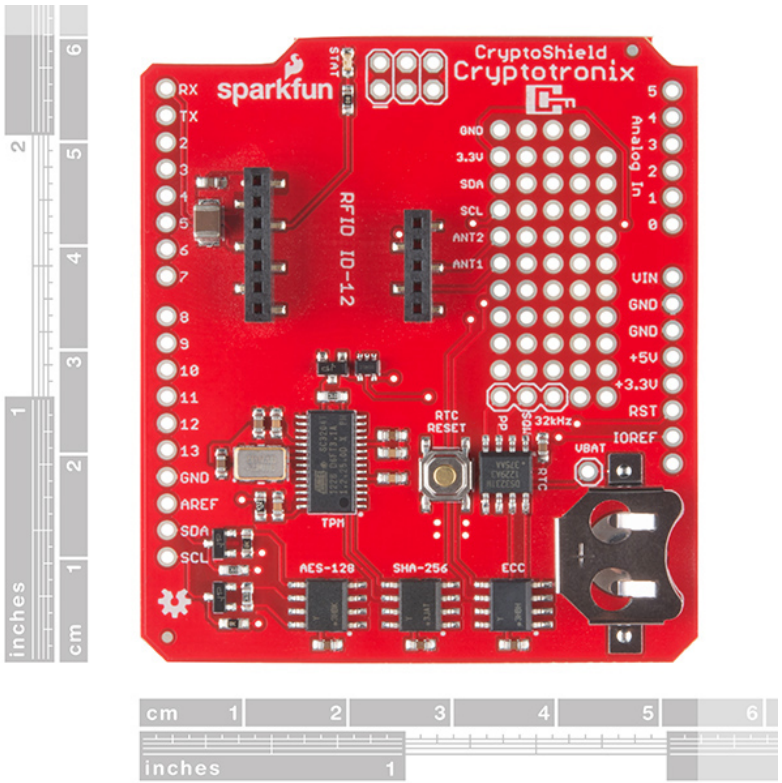
6. Conclusion

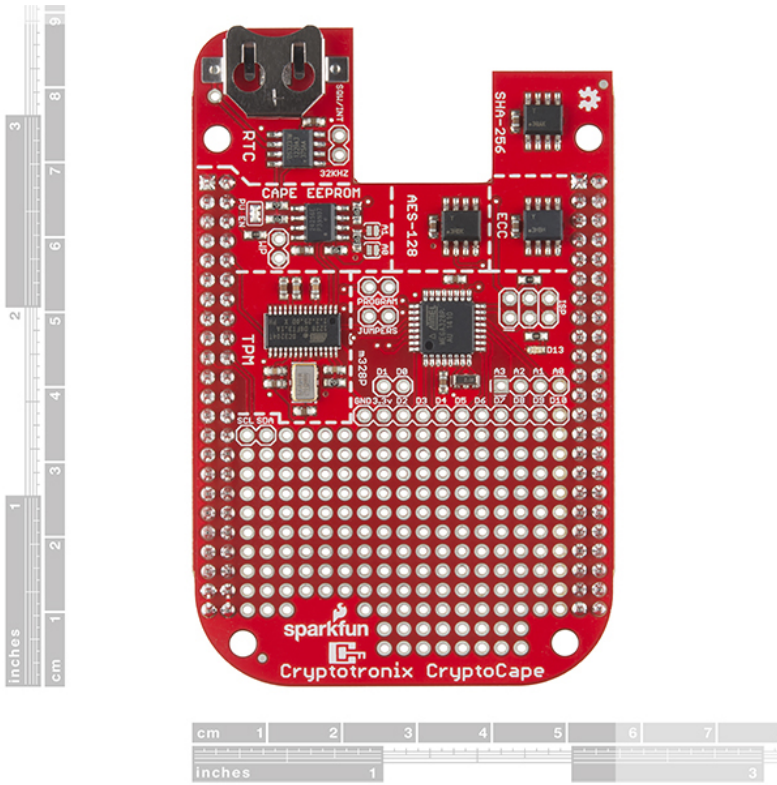
Introduction

Hi, I'm Josh!

- Owner of Cryptotronix
- SparkFun Hacker-in-Residence 2014
- CryptoCape & CryptoShield
- DEF CON 22: NSA Playset: CHUCKWAGON
- BSides Portland: Cryptowarez

CryptoThings





Why this talk?!

Why this talk?

Why this talk?!

Why this talk?

1. SparkFun is awesome

Why this talk?!

Why this talk?

1. SparkFun is awesome
2. Wanted to share the latest research

Why this talk?!

Why this talk?

1. SparkFun is awesome
2. Wanted to share the latest research
3. I hope to see others giving security talks at SparkFun AVC!

Goal

Increase security awareness among hackers, makers, builders, and consumers!

Demotivating Quotes

Demotivating Quotes

Cory Doctorow

A car is a computer that drives.

Demotivating Quotes

Cory Doctorow

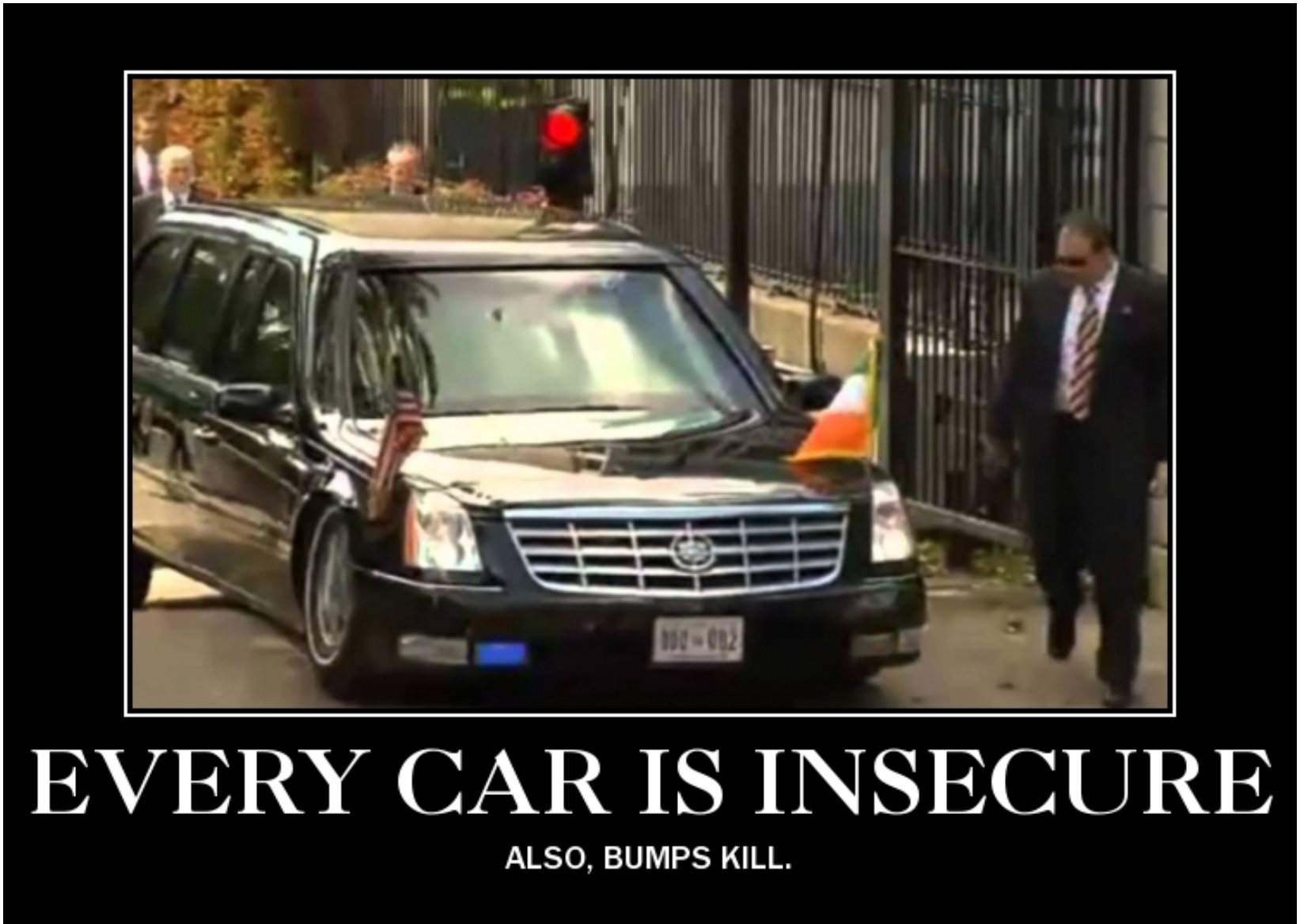
A car is a computer that drives.

Sandy Clark

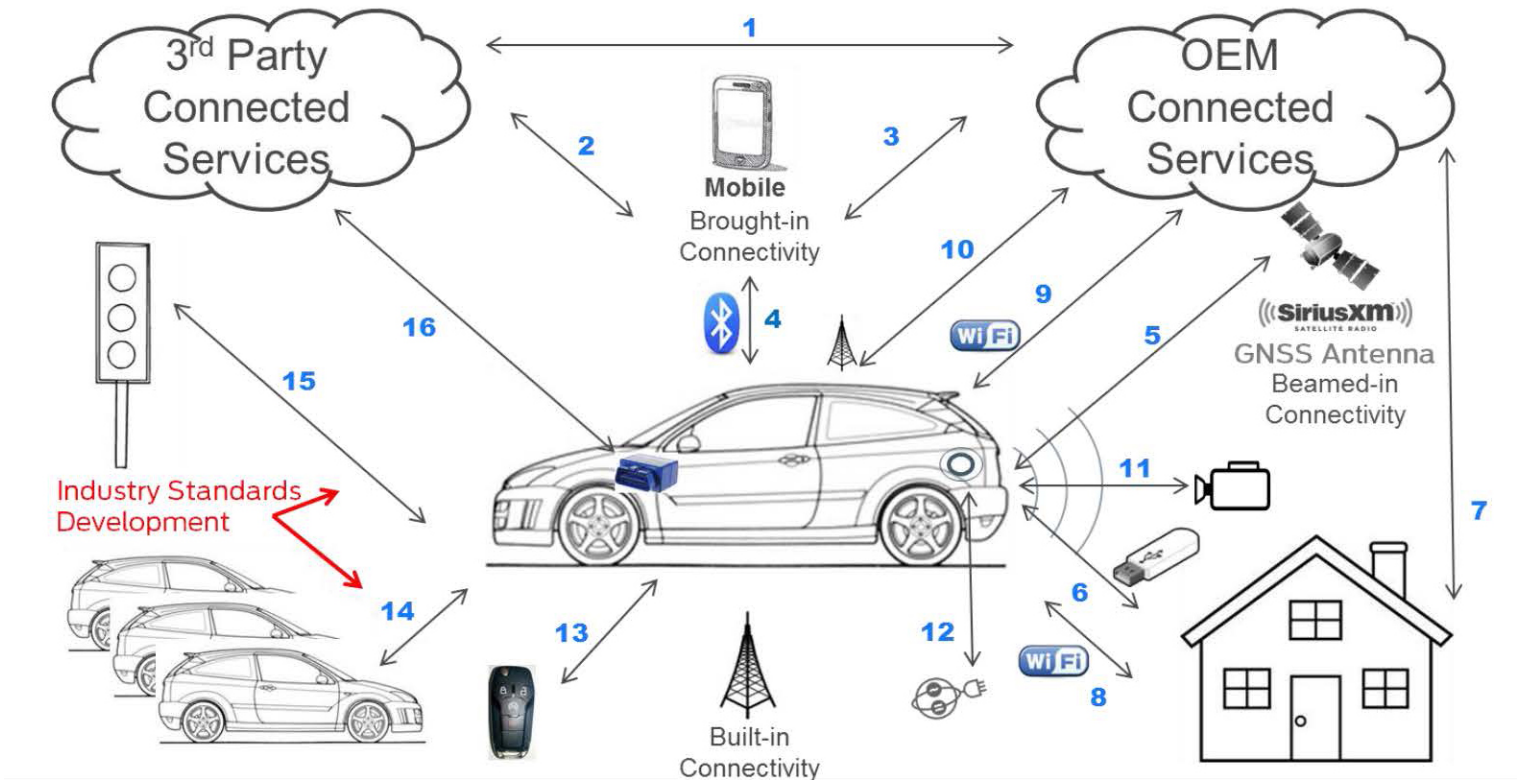
1. *Everything is made of software.*
2. *Software is insecure.*

Therefore...

Therefore...



Connected Car



Source: http://articles.sae.org/14503/

CAN & OBDII

Related Tutorials

Getting Started with OBD-II

OCTOBER 8, 2015

A general guide to the OBD-II protocols used for communication in automotive and industrial applications.

CAN-Bus Shield Hookup Guide

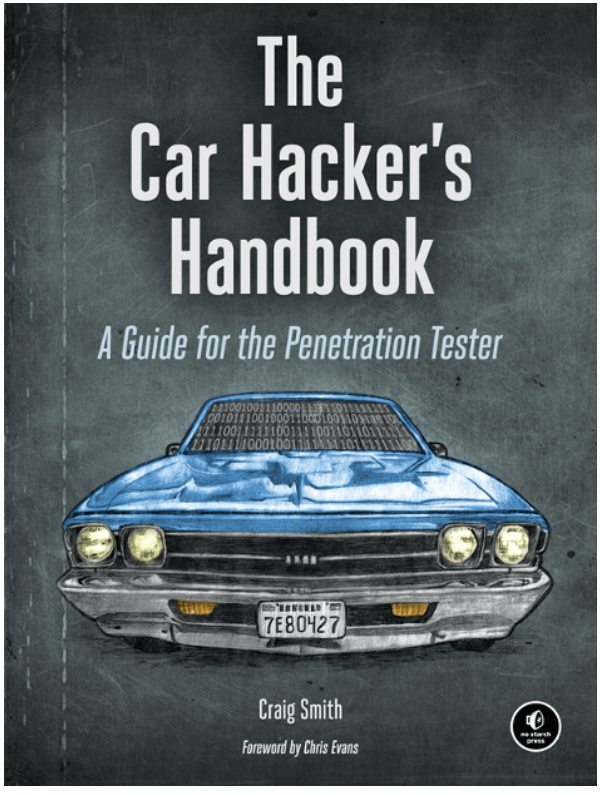
OCTOBER 8, 2015

A basic introduction to working with the CAN-Bus shield.

Source: `https://learn.sparkfun.com/tutorials/getting-started-with-obd-ii`

HOPE XI Talks

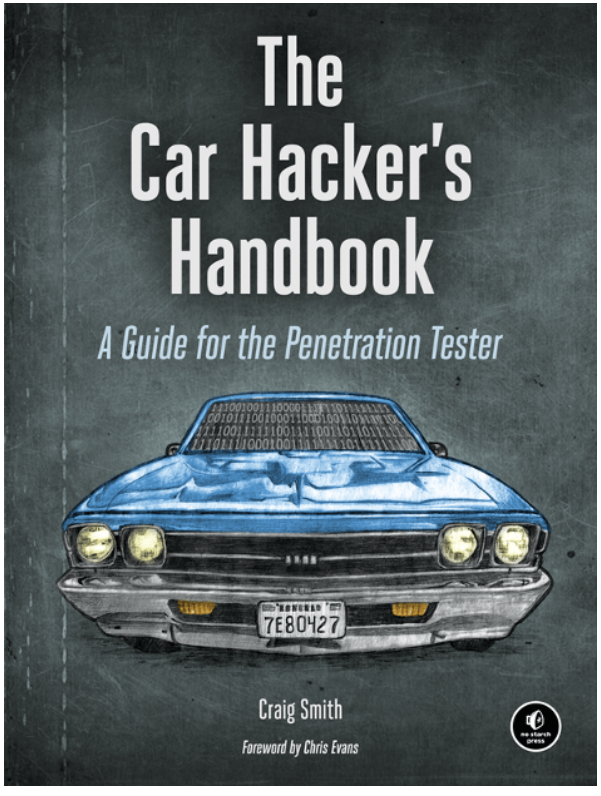
Car Hacking Tools - Craig Smith and Eric Evenchick



- You *really* want this book
- List of tools, how to create your own car hacking test bench, how to attack ECUs

Source: `https://www.nostarch.com/carhacking`

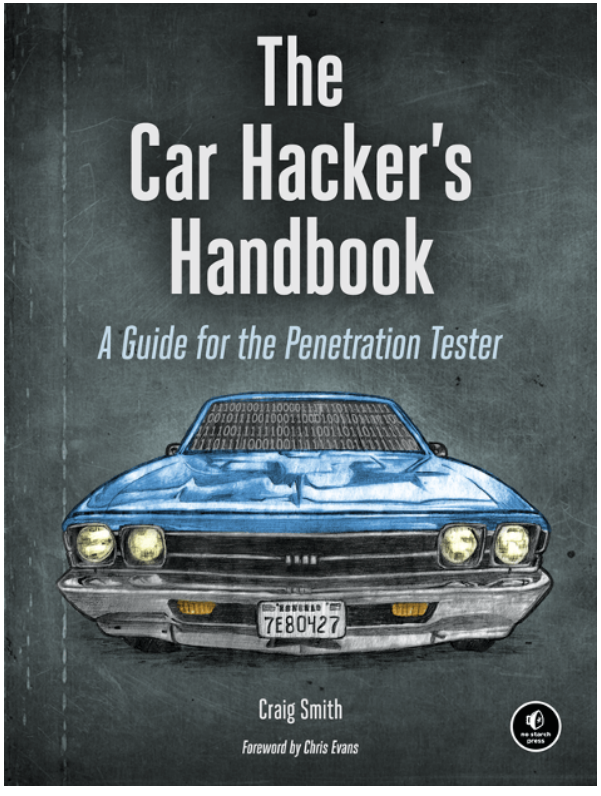
Car Hacking Tools - Craig Smith and Eric Evenchick



- You *really* want this book
- List of tools, how to create your own car hacking test bench, how to attack ECUs
- UDSim - `https://github.com/zombieCraig/UDSim`
- `http://opengarages.org`

Source: `https://www.nostarch.com/carhacking`

Car Hacking Tools - Craig Smith and Eric Evenchick



Source: `https://www.nostarch.com/carhacking`

- You *really* want this book
- List of tools, how to create your own car hacking test bench, how to attack ECUs
- UDSim - `https://github.com/zombieCraig/UDSim`
- `http://opengarages.org`
- 50% off e-book from `nostarch.com`, use code JUSTBECAUSE.

Car Hacking Tools - Craig Smith and Eric Evenchick

- CANtact - CAN to USB Converter based on the STM32F0
- CANtact-app `https://github.com/linklayer/cantact-app`
- Python library
- Open source hardware

Blackhat 2016 Talks

CANSPY - Arnaud Lebrun and Jonathan-Christofer Demay

Source: `http://ubm.io/2cBdRuA`

- Wanted a tool to meet the CAN timing constraints (up to 1Mbps, so no UART).
- Also needed a MITM configuration (multiple I/F).
- Open source framework
- STM32F4DISCOVERY Board
- Lots of RT firmware work
- `https://bitbucket.org/jcdemay/canspy`

Advanced CAN Injection - Miller & Valasek

Advanced CAN Injection - Miller & Valasek

- CAN Message injection: contention and conflicton issues.
- 2010 & newer vehicles attacks are speed limited.

Advanced CAN Injection - Miller & Valasek

- CAN Message injection: contention and conflicton issues.
- 2010 & newer vehicles attacks are speed limited.
- A *lot* of reverse engineering of binary blobs.
- Two problems
    1. Real ECU is spewing real data

Advanced CAN Injection - Miller & Valasek

- CAN Message injection: contention and conflicton issues.
- 2010 & newer vehicles attacks are speed limited.
- A *lot* of reverse engineering of binary blobs.
- Two problems
    1. Real ECU is spewing real data
    2. Target ECU is expecting a counter

Advanced CAN Injection - Miller & Valasek

- CAN Message injection: contention and conflicton issues.
- 2010 & newer vehicles attacks are speed limited.
- A *lot* of reverse engineering of binary blobs.
- Two problems
    1. Real ECU is spewing real data
    2. Target ECU is expecting a counter
- *message un-confliction*, exploits a CAN bus counter.

Advanced CAN Injection - Miller & Valasek

- CAN Message injection: contention and conflicton issues.
- 2010 & newer vehicles attacks are speed limited.
- A *lot* of reverse engineering of binary blobs.
- Two problems
    1. Real ECU is spewing real data
    2. Target ECU is expecting a counter
- *message un-confliction*, exploits a CAN bus counter.
    1. Start to reprogram the ECU, it goes into boot-rom mode, then stop, then drive, which takes the ECU offline.

Advanced CAN Injection - Miller & Valasek

- CAN Message injection: contention and conflicton issues.
- 2010 & newer vehicles attacks are speed limited.
- A *lot* of reverse engineering of binary blobs.
- Two problems
    1. Real ECU is spewing real data
    2. Target ECU is expecting a counter
- *message un-confliction*, exploits a CAN bus counter.
    1. Start to reprogram the ECU, it goes into boot-rom mode, then stop, then drive, which takes the ECU offline.
    2. PSCM: PAM in boot-rom, fake speed with counter trick, send PAM message to turn steering wheel.

Advanced CAN Injection - Miller & Valasek

- CAN Message injection: contention and conflicton issues.
- 2010 & newer vehicles attacks are speed limited.
- A *lot* of reverse engineering of binary blobs.
- Two problems
    1. Real ECU is spewing real data
    2. Target ECU is expecting a counter
- *message un-confliction*, exploits a CAN bus counter.
    1. Start to reprogram the ECU, it goes into boot-rom mode, then stop, then drive, which takes the ECU offline.
    2. PSCM: PAM in boot-rom, fake speed with counter trick, send PAM message to turn steering wheel.
    3. Brakes as well.

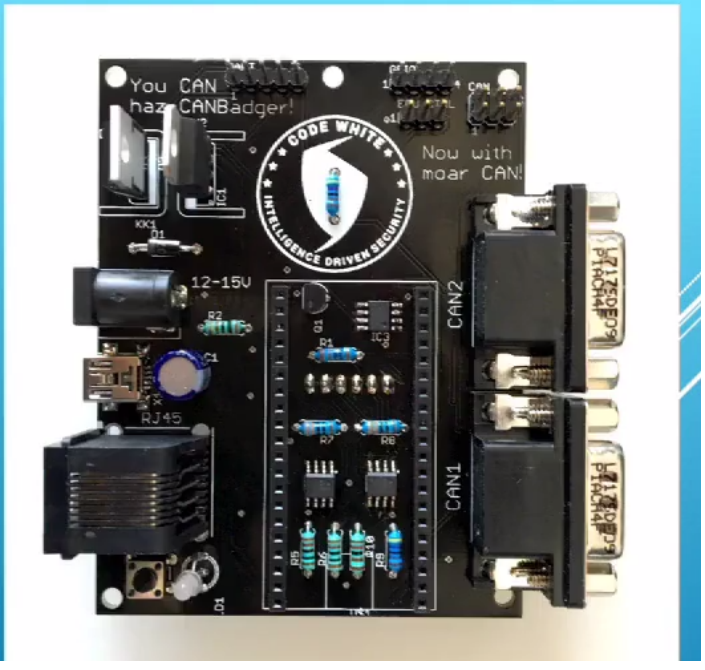
Advanced CAN Injection - Miller & Valasek

- CAN Message injection: contention and conflicton issues.
- 2010 & newer vehicles attacks are speed limited.
- A *lot* of reverse engineering of binary blobs.
- Two problems
    1. Real ECU is spewing real data
    2. Target ECU is expecting a counter
- *message un-confliction*, exploits a CAN bus counter.
    1. Start to reprogram the ECU, it goes into boot-rom mode, then stop, then drive, which takes the ECU offline.
    2. PSCM: PAM in boot-rom, fake speed with counter trick, send PAM message to turn steering wheel.
    3. Brakes as well.
- Recommends IDS for CAN Bus.

DEF CON 2016 Tracks

CANBadger Hardware Overview

- Powered by mBed LPC1768 or LPCXPresso LPC1769
- 128KB XRAM
- 2x DB9 CAN Interfaces + 2x Debug headers
- SD card
- ECU Power control by software
- UART
- 4 GPIOs
- Standalone mode, USB mode (CDC Device), or Network mode
- Can be powered by PSU, External battery, or OBD2
- Has a blinky dual color LED. Everyone loves blinky LEDs, right?
- Complete board assembly under $25



CAN I Haz Secretz? Vidal & Noeischer

- CANBadger can control GPS via UART

CAN I Haz Secretz? Vidal & Noeischer

- CANBadger can control GPS via UART
- How do those insurance dongles work?

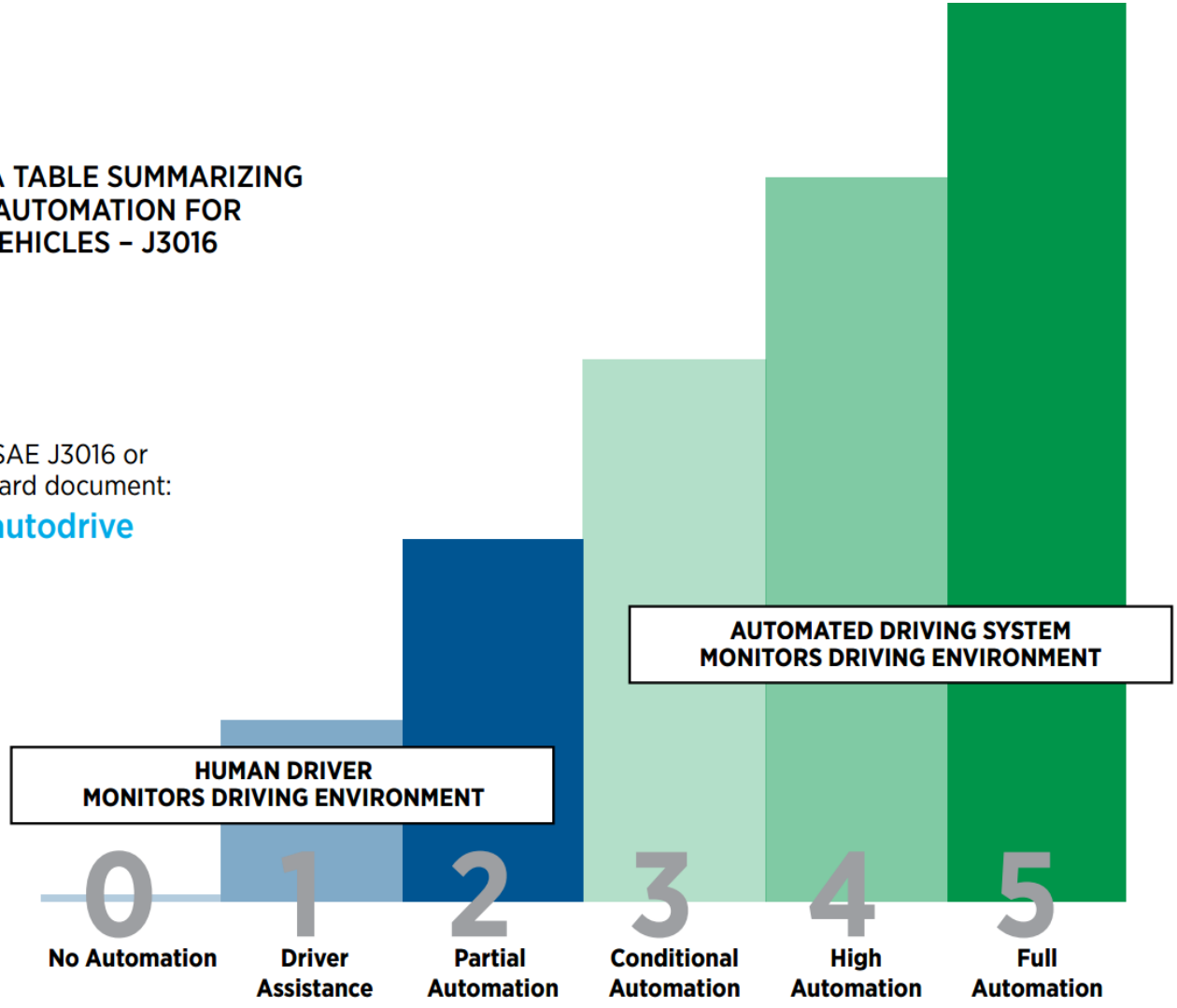
CAN I Haz Secretz? Vidal & Noeischer

- CANBadger can control GPS via UART
- How do those insurance dongles work?
- CANBadger has emulator. Records data and playbacks.

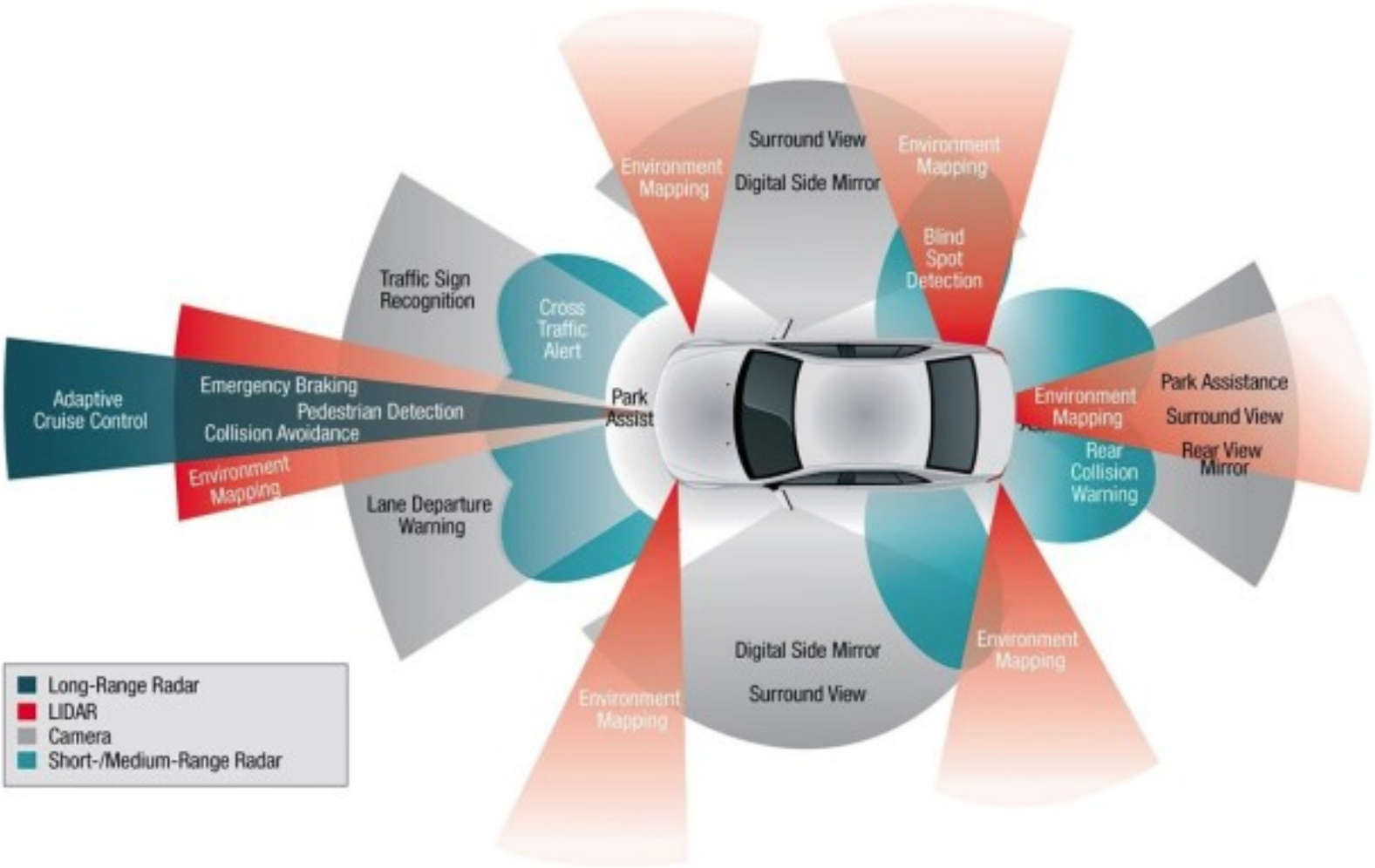
Can you Trust Autonomous Vehicles–Liu,Yan,Xu

OVER FOR A TABLE SUMMARIZING
LEVELS OF AUTOMATION FOR
ON-ROAD VEHICLES – J3016

Learn more about SAE J3016 or
purchase the standard document:
www.sae.org/autodrive



Can you Trust Autonomous Vehicles–Liu,Yan,Xu



Can you Trust Autonomous Vehicles–Liu,Yan,Xu

- How can we attack the sensors? The reliability of the sensors affect the reliability of the driving.

Can you Trust Autonomous Vehicles–Liu,Yan,Xu

- How can we attack the sensors? The reliability of the sensors affect the reliability of the driving.
- First fatal tesla crash using autopilot on May 7, 2016.

Can you Trust Autonomous Vehicles–Liu,Yan,Xu

- How can we attack the sensors? The reliability of the sensors affect the reliability of the driving.
- First fatal tesla crash using autopilot on May 7, 2016.
- Spoof tesla HMI

Can you Trust Autonomous Vehicles–Liu,Yan,Xu

- How can we attack the sensors? The reliability of the sensors affect the reliability of the driving.
- First fatal tesla crash using autopilot on May 7, 2016.
- Spoof tesla HMI
- attacking ulta-sonic sensors (proximity)

Can you Trust Autonomous Vehicles–Liu,Yan,Xu

- How can we attack the sensors? The reliability of the sensors affect the reliability of the driving.
- First fatal tesla crash using autopilot on May 7, 2016.
- Spoof tesla HMI
- attacking ulta-sonic sensors (proximity)
    1. Prevent cars from taking your parking spot :)

Can you Trust Autonomous Vehicles–Liu,Yan,Xu

- How can we attack the sensors? The reliability of the sensors affect the reliability of the driving.
- First fatal tesla crash using autopilot on May 7, 2016.
- Spoof tesla HMI
- attacking ulta-sonic sensors (proximity)
    1. Prevent cars from taking your parking spot :)
    2. attacks: jamming, spoofing, quieting (Arduino + ultrasonic transducer or signal generator)

Can you Trust Autonomous Vehicles–Liu,Yan,Xu

- How can we attack the sensors? The reliability of the sensors affect the reliability of the driving.
- First fatal tesla crash using autopilot on May 7, 2016.
- Spoof tesla HMI
- attacking ulta-sonic sensors (proximity)
    1. Prevent cars from taking your parking spot :)
    2. attacks: jamming, spoofing, quieting (Arduino + ultrasonic transducer or signal generator)
- attacks on cameras (blinding with laser pointer)

Can you Trust Autonomous Vehicles–Liu,Yan,Xu

- How can we attack the sensors? The reliability of the sensors affect the reliability of the driving.
- First fatal tesla crash using autopilot on May 7, 2016.
- Spoof tesla HMI
- attacking ulta-sonic sensors (proximity)
    1. Prevent cars from taking your parking spot :)
    2. attacks: jamming, spoofing, quieting (Arduino + ultrasonic transducer or signal generator)
- attacks on cameras (blinding with laser pointer)
- Takeaways
    1. Sensors should fail safe.
    2. sensor should have anomaly detection
    3. Redundancy: MIMO, different types, sensor data fusion

DEF CON 2016 Car Hacking Village

CHV Badge Nathan Hoch

CHV Badge

1. The badge supports 2x Dual Wire CAN (ISO 11898-2) channels with full gateway support.
2. Fully-controllable pass-through
3. Interrupt messages or drop it
4. Uses PAWN. `http://www.compuphase.com/pawn/pawn.htm`
5. The badge also sports a 128×128 color LCD which is fully accessible via the PAWN scripts.

Conclusion

Insights

Insights

CAN Bus feels like the early Internet

Exploit the boundaries of assumptions.

Insights

CAN Bus feels like the early Internet

Exploit the boundaries of assumptions.

- Defensive design.

Insights

CAN Bus feels like the early Internet

Exploit the boundaries of assumptions.

- Defensive design.
- Reliability engineering is security engineering.

Insights

CAN Bus feels like the early Internet

Exploit the boundaries of assumptions.

- Defensive design.
- Reliability engineering is security engineering.
- See Peter Neumann and *Computer Related Risks*

Get more security researchers at AVC!

Get more security researchers at AVC!

1. I wonder if I could trigger a competitor's stop switch :)

Get more security researchers at AVC!

1. I wonder if I could trigger a competitor's stop switch :)
2. Ultrasonic-proof (quieted) obstacles

Get more security researchers at AVC!

1. I wonder if I could trigger a competitor's stop switch :)
2. Ultrasonic-proof (quieted) obstacles
3. Actively malicious obstacles targeting sensors

Get more security researchers at AVC!

1. I wonder if I could trigger a competitor's stop switch :)
2. Ultrasonic-proof (quieted) obstacles
3. Actively malicious obstacles targeting sensors
4. Pen-test pit-stop

Get more security researchers at AVC!

1. I wonder if I could trigger a competitor's stop switch :)
2. Ultrasonic-proof (quieted) obstacles
3. Actively malicious obstacles targeting sensors
4. Pen-test pit-stop

Get more security researchers at AVC!

1. I wonder if I could trigger a competitor's stop switch :)
2. Ultrasonic-proof (quieted) obstacles
3. Actively malicious obstacles targeting sensors
4. Pen-test pit-stop

Make AVC entries resilient to attacks

You know, like real-world systems should be!

Das Ende

- `www.cryptotronix.com`
- Just ask for Josh ;)