w3c IVI Exploitation Discussion

Craig Smith
craig@theialabs.com
@OpenGarages

How a Hacker Examines a System

- Remove the target component
- Build a test bench
- Target Upload/Update Capabilities
- Access for JTAG/Disks
- Goal is to get to the OS

Low Hanging Fruit

- Right now exploitation is easy.
  - Poor update systems
  - Outdated versions with known CVEs
  - Misconfiguration with security "assumed"
  - Lack of encryption
  - Lack of segregation
  - No OS hardening

Goals

- Code Execution of course!
  - Vehicle Control
  - Vehicle Theft
  - Privacy and Spying

Stunt Hacking

- Currently my biggest headache

Exploitation Hurdles

- Possible VM

- Not connected to target bus

- Telematics are seperated

  – Really depends on the goal

Recent Published Hacks

ANDY GREENBERG   SECURITY   07.21.15   6:00 AM

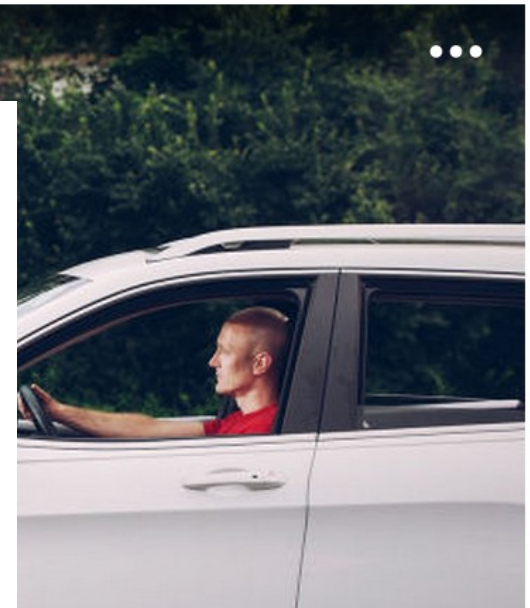## HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Hackers Remotely Kill a Jeep on the Highway—With Me in It

Technology

Car hack uses digital-radio broadcasts to seize control

By Chris Vallance
BBC Radio 4

22 July 2015 | Technology

Q&A on Detail Exploitation