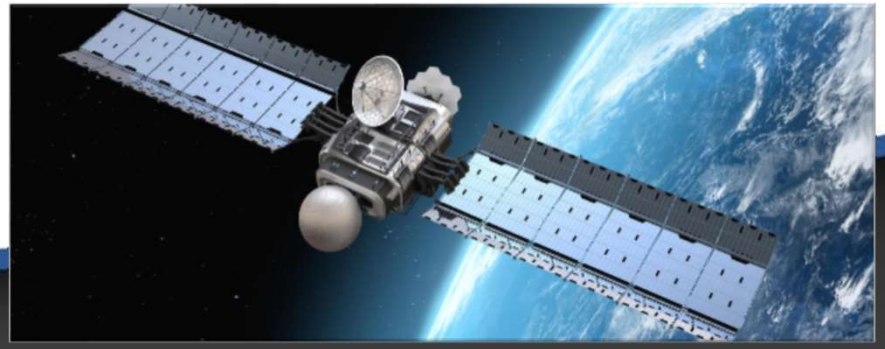
Legal GNSS Spoofing
and its Effects on Autonomous Vehicles

Victor Murray, CISSP®
Southwest Research Institute
Group Leader R&D

Introduction

- Global Navigation Satellite Systems (GNSS) are Awesome!

- What's Not So Awesome?
  - Public versions lack integrity mechanisms making them vulnerable to spoofing



Review of GNSS Inherent Security Issues

How could systems respond to spoofing?

- Missing integrity mechanisms
- Transmits using low power
- External interference
  - Reflections from buildings
  - Tunnels or overpasses
  - Weather

Prior Pubs Of Spoofing on Automated Vehicles (AVs)

- GPS spoofing experiment on drone (Humphreys)
  - UT spoofing: takeover and downing of small drone
  - https://www.youtube.com/watch?v=i4ctPFwlKas
- GPS Spoofing: Low Cost GPS Simulator
  - Unicorn team - drone manipulation (DefCon 23)
  - https://en.calameo.com/read/004474480397d2632c1e3
- IRAN'S ALLEGED DRONE HACK: TOUGH, BUT POSSIBLE
  - RQ-170 UAV purportedly downed by spoofing
  - https://www.wired.com/2011/12/iran-drone-hack-gps/

So what can happen if systems aren't tested for GNSS issues?

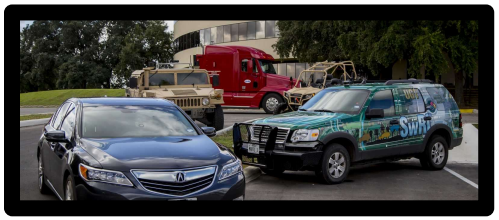
Our Experience

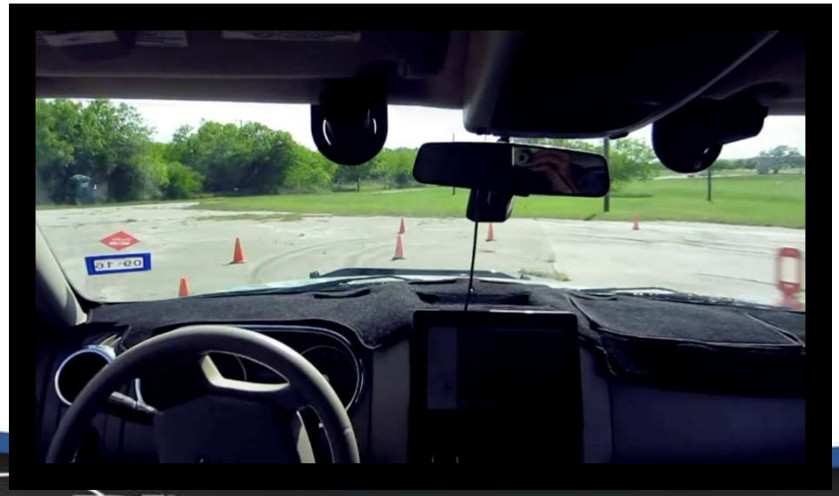
- **Hired to work on drones**
  - Analyzed issues
- **Patterns: errors in sensors caused planes to crash**
  - GNSS, Rate Gyro, Accelerometer, Pitot/Static, Magnetometers
  - Most common: GNSS
- **Our next step**
  - Build a better system in order to test a AV prior to being deployed
  - Received IR&D Funding Focused Specifically on GNSS

Agenda

- **Our Testing System Including Our Vehicles**
  - Automated Vehicle (AV) Fleet
  - Hardware
  - Software
- **Testing Results**
  - Position Translation
  - Velocity
  - Halt
- **Recommendations and Takeaways**

Fleet and AV We Used





- Fleet outfitted with our own autonomy kits
- Configured to drive by GNSS waypoint for purpose of this test
- Performed attacks remotely in real time

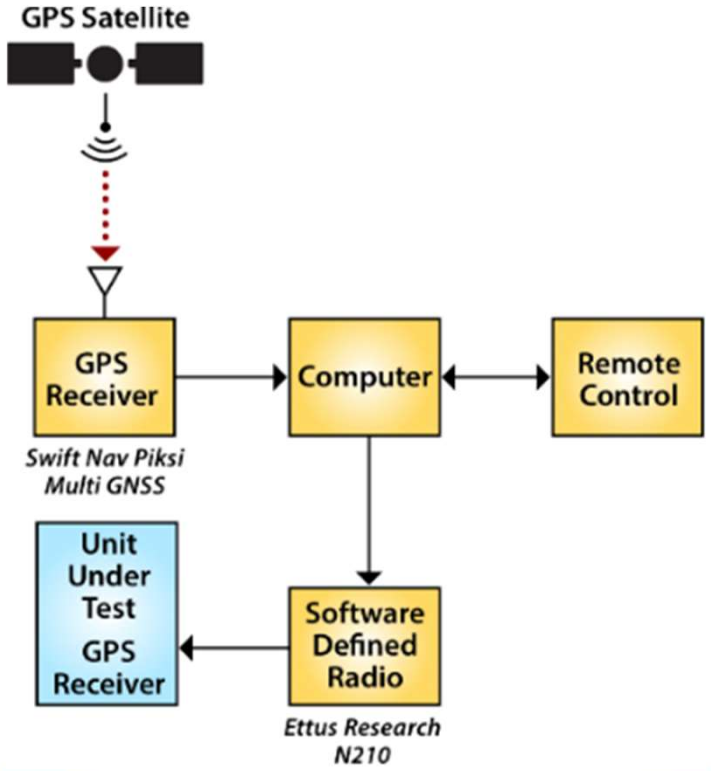
To be legal, how did we comply?

What is Illegal and Legal in the US?

- **What is illegal?**
  - Spoofing is illegal in the U.S. Per the **communications** act of 1934 As amended 47 U.S.C. § 301
- **What is considered legal?**
  - Broadcasting is allowed under
    - Experimental license (47 C.F.R. §5.53)
    - Under a waiver of the FCC rules (47 C.F.R. §1.3)
  - Allow rebroadcasting spoofed signals when fully enclosed in a Faraday cage
  - FCC regulations allow broadcasting up to 1 watt in ISM bands (900MHz, 2.4 GHz, 5.8GHz),

Our System Is 100% Legal

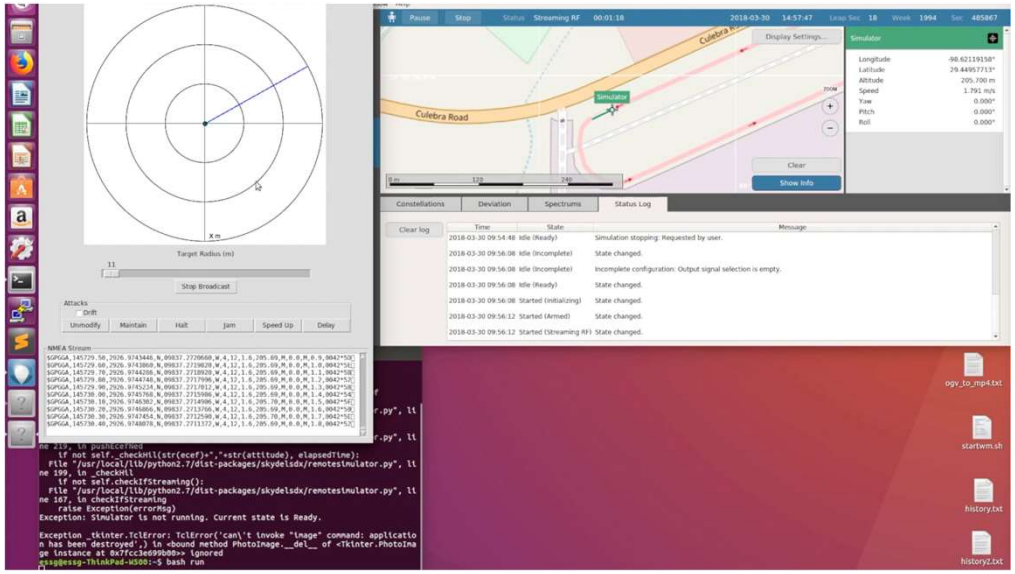
SwRI's Legal Spoofing System



- **Remote Control of Computer over**
  - Wi-Fi
  - Cellular

Frequency Translation
- *Signal broadcast in unlicensed band*
- *900MHz*
- *On-vehicle signal translated back to base frequency*

SwRI's Controlling Software



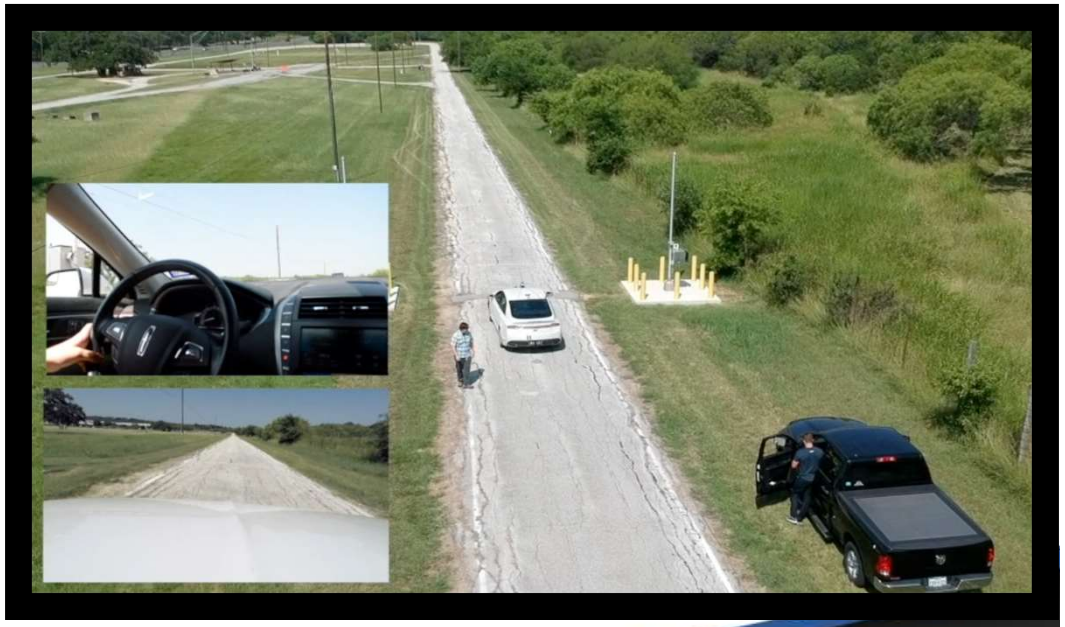
- **Designed for real time**
- **Can pass through GNSS unmodified or manipulated**
  - Left or right
  - Speed up or slow it down
  - Adjust timing

Types of Testing Results

- Offset Attacks
- Velocity
- Halt

Offset Attacks: Manipulate Movements

- **Up to 10 meters at a time**
- **Left or right movement**
  - Force lane changes
  - Nudge car off the road
- **Moving forward or backwards**
  - Turn early/late



Velocity Attacks: Vehicle Speed Varied

- **Attacked *during turning* of vehicle**
  - Would turn too far
  - Turns harder
  - Run off the road
- **Modified *before turn***
  - Caused vehicle to turn early or late
- **Attacked when *driving straight***
  - No immediate reaction
  - Controlled speed by wheel speed (not by GNSS)

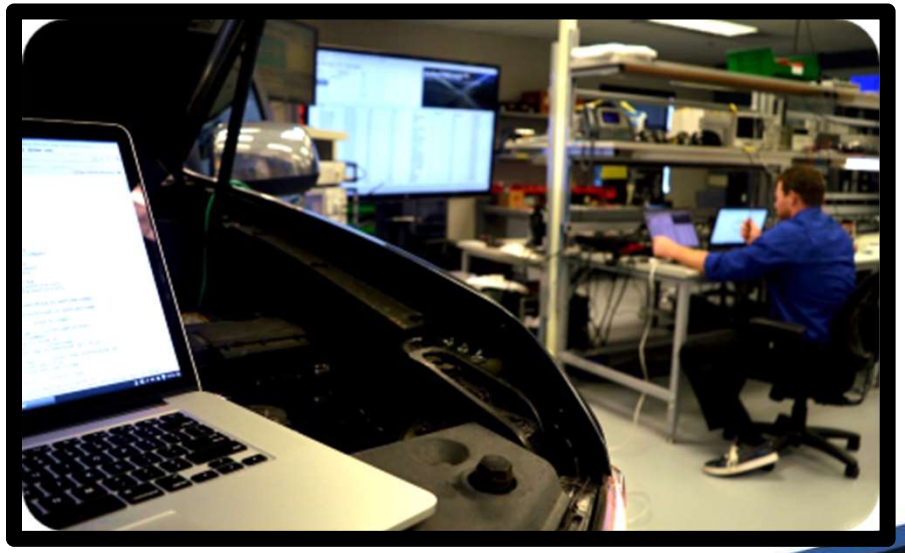
Bringing Vehicle to a Halt

- **While slowing down**
  - Speed of car was unaltered
- **Once stopped**
  - Control system became unstable

AV had similar result when GNSS location was delayed by a couple seconds

Recommendations to Enhance a Safety Critical System

- **Use multiple constellations**
- **Don't rely solely on GNSS**
- **Monitor GNSS signal** (e.g. power)
- **Compare to other localization estimates**
- **Verify response to position errors and spoofed signals**
- **Longer Term**
  - Add integrity mechanisms to GNSS (e.g. digital signature, encryption)



Takeaways

- **GNSS signals can be legally spoofed in a field environment**
  - Fully enclosed, ISM broadcast
  - Remote control of AV had significant limitations

- **The sky is not falling. ☺**
  - Combining GNSS with other localization methods helps assure estimates are correct

Acknowledgements

- **Ben Abbott, Ph.D.**
  - Created idea for basis of this research and mentored others working on the project
- **Ben Lindow**
  - Wrote most software for the project
- **Jimmy Li, Ph.D.**
  - Performed all aspects of RF design

Questions?