RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HTA-R05

Combatting Spoofed GPS in Forensics

Bobby Kuzma, CISSP, CCFP
Systems Engineer
Core Security Technologies
@BobbyAtCore

#RSAC

GPS becomes critical…

By David Earl
BIO »

Police have GPS evidence that puts teen murder suspects at crime scene

15-year-old Courvoisier Sims was wearing a juvenile probation tracking device, police say

UPDATED 5:31 PM CST Dec 30, 2015

GPS becomes critical…

UT Austin Researchers Spoof Superyacht at Sea

MONDAY, JUL 29, 2013

This summer, a radio navigation research team from The University of Texas at Austin set out to discover whether they could subtly coerce a 213-foot yacht off its course, using a custom-made GPS device.

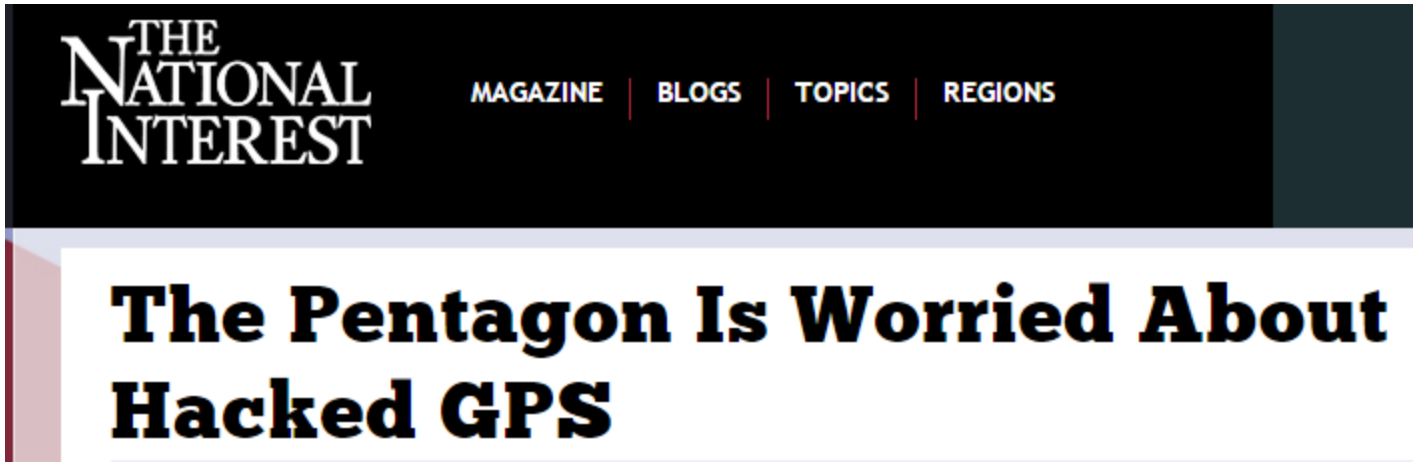
GPS becomes critical…

TECHNOLOGY

TEXAS STUDENTS HIJACK A U.S. GOVERNMENT DRONE IN MIDAIR

By Colin Lecher Posted June 28, 2012

GPS becomes critical…



GPS becomes critical…

WORLD | PASSCODE | PASSCODE VOICES | CRITICAL INFRASTRUCTURE

Opinion: Were US sailors 'spoofed' into Iranian waters?

In 2011, Iran spoofed – or faked – Global Positioning System signals to send a CIA drone off course. Did it do the same to trick Navy vessels into Iranian waters?

By Dana A. Goward, Contributor | JANUARY 15, 2016

Save for later

GPS becomes critical…

WORLD | MIDDLE EAST

Exclusive: Iran hijacked US drone, says Iranian engineer (Video)

In an exclusive interview, an engineer working to unlock the secrets of the captured RQ-170 Sentinel says they exploited a known vulnerability and tricked the US drone into landing in Iran.

By Scott Peterson, Staff writer ▼ Payam Faramarzi*, Correspondent
DECEMBER 15, 2011

Save for later

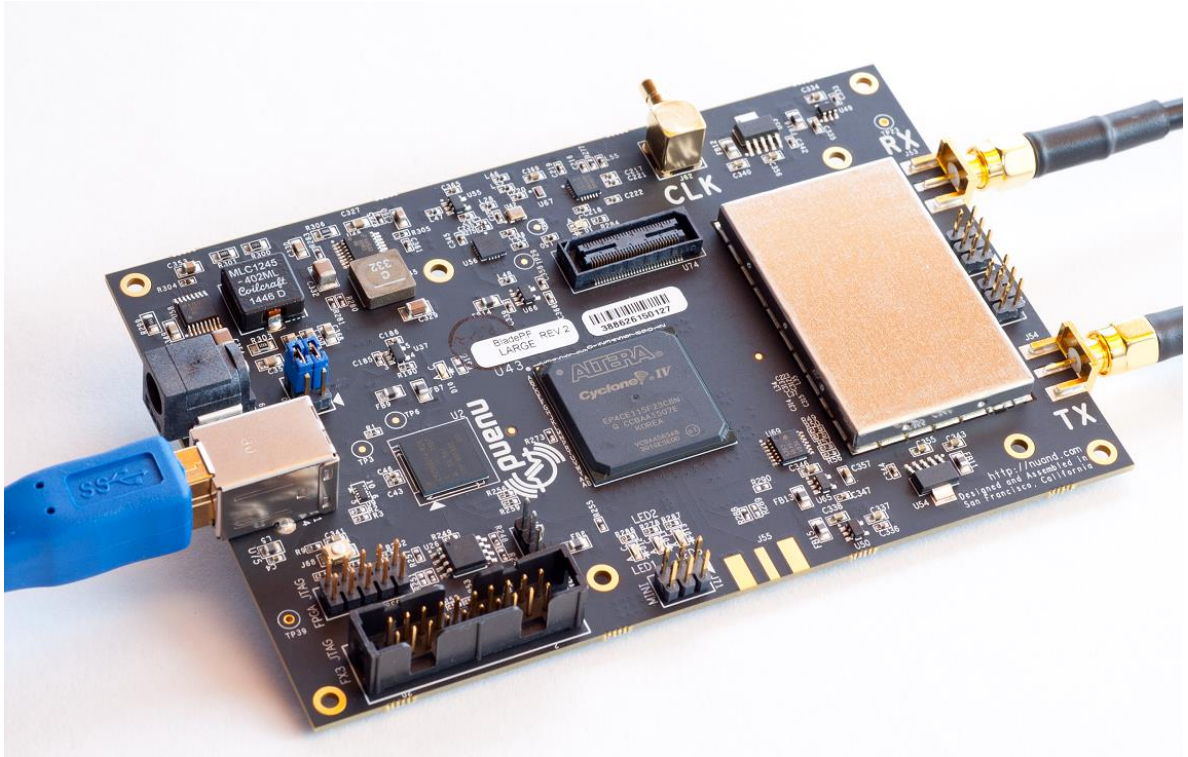
Sepahnews/AP | View Caption

GPS spoofing evolves from this…

GPS spoofing old style

- Complex
- Difficult to acquire
- Expensive

Into this…



GPS spoofing new style

- Not Quite as Complex
- Easy to acquire
- Inexpensive

What we'll be talking about

- How GPS (and BeiDou, Galileo, GLONASS, and IRNSS) works
- Avenues for spoofing attacks
- How GPS can be spoofed
- Methodologies for detecting spoofed tracks

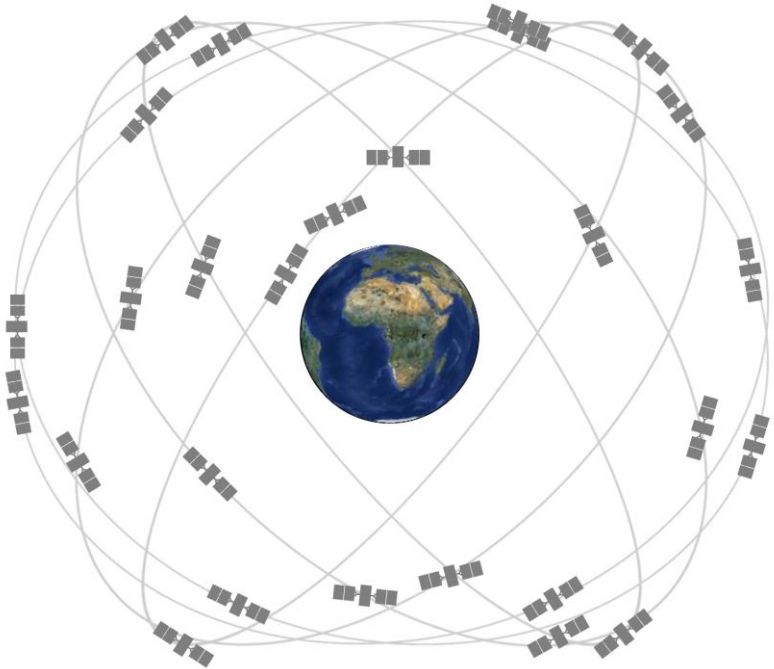
Let's start with why!

- This has potential real world impact
- New technologies are fun
- I get bored very easily

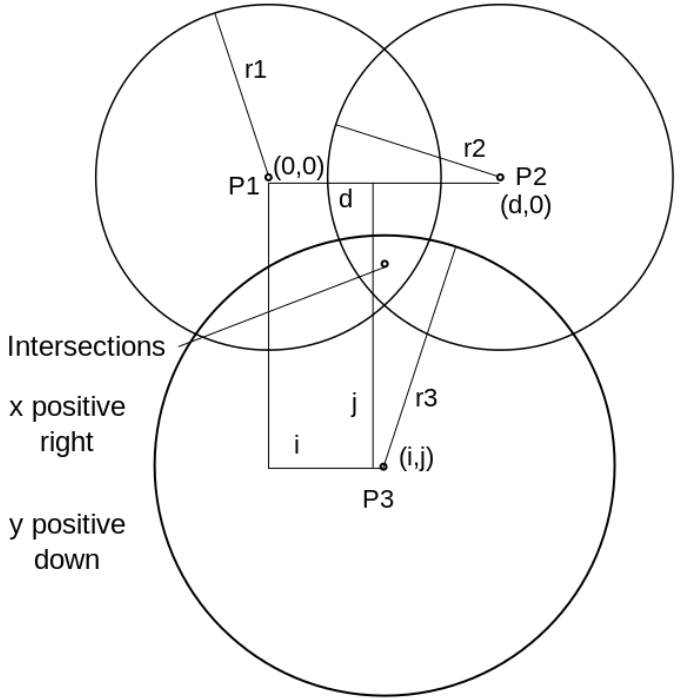
But first, a demo…

- What: I'll be broadcasting a spoofed GPS signal to the equipment onstage.
- Why: So we have something to analyze later
- Also: This takes a few minutes, and is boring to watch.
- WARNING: If you don't want to participate, disable GPS on your phones NOW.

How GNSS systems work



How GNSS systems work



How GNSS systems work

$$P^1 = ((x^1 - x)^2 + (y^1 - y)^2 + (z^1 - z)^2)^{1/2} + c\tau - c\tau^1$$

$$P^2 = ((x^2 - x)^2 + (y^2 - y)^2 + (z^2 - z)^2)^{1/2} + c\tau - c\tau^2$$

$$P^3 = ((x^3 - x)^2 + (y^3 - y)^2 + (z^3 - z)^2)^{1/2} + c\tau - c\tau^3$$

$$P^4 = ((x^4 - x)^2 + (y^4 - y)^2 + (z^4 - z)^2)^{1/2} + c\tau - c\tau^4$$

GNSS gives us

- Spatial positioning in three dimensions
- Temporal positioning in a single dimension.

Attacks abound

- GPS is vulnerable to attacks impacting both positioning and timing.

Attacks on location

- Navigation systems
- Location systems (like monitoring systems for probation)
- False location histories
- Security interlocks (drones, etc)

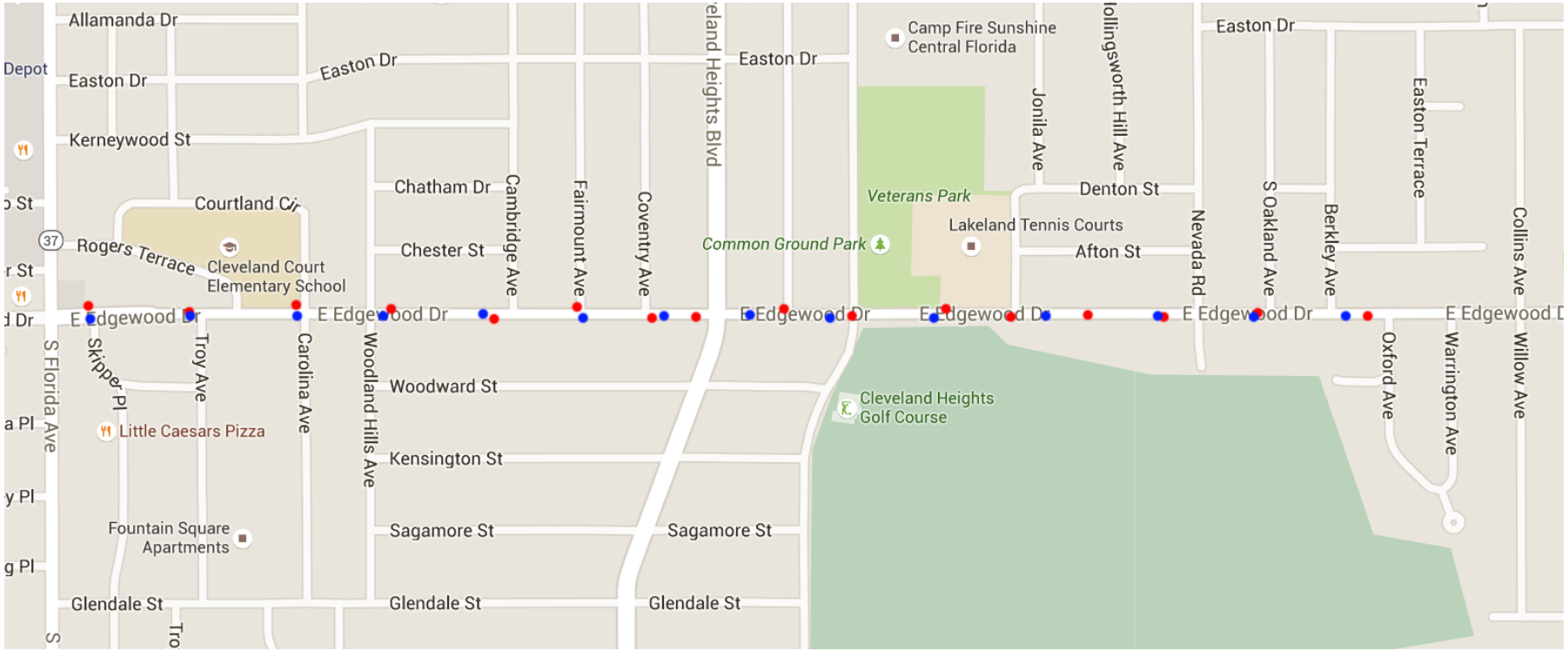
Attacks on time

- Industrial controls
- Time lock safes
- Authoritative Time Attacks

What do you need to spoof GPS

- Ephemeris Data for the time you're spoofing
- A track to lay down
- Lots of math
- Relativity matters!

Take GPS track data



Now, about that demo

- I'll capture the track that we've been laying down

My thought process

- The real world is full of random… stuff
- We could resort to complex math… but I'm bad at math
- So we look at simple techniques…
- And some of them work!

Noise and spatial “jitter”

- Straight lines… aren’t
- Calculate the average distance from the line.

Noise and spatial “jitter”

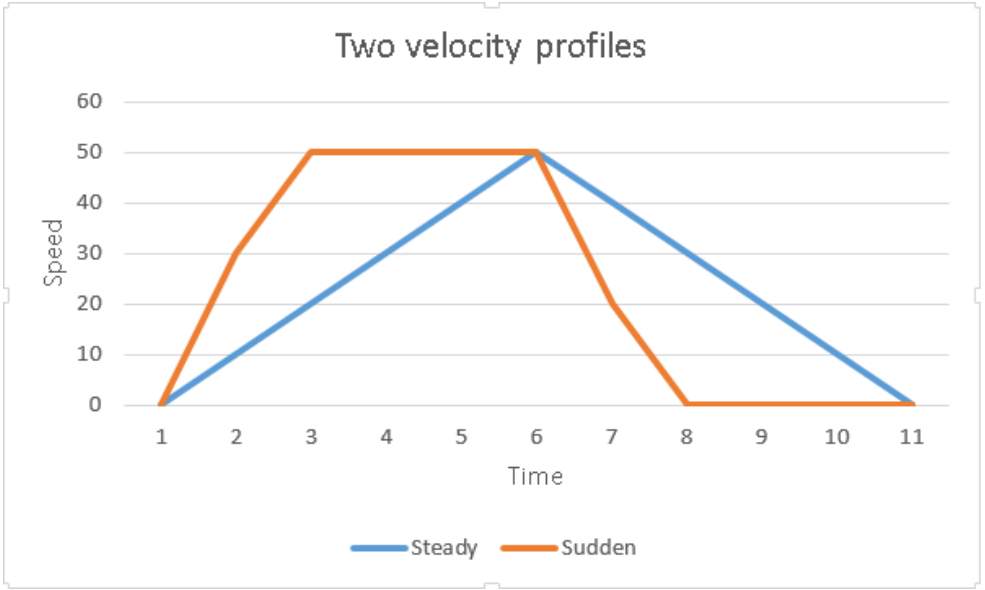
- Errors caused by multipath, ephemeris data errors, weather, interference, solar conditions add up.
- Testing shows lower amounts of “jitter” when spoofed GPS tracks are reviewed
- This is due to the reduction of outside factors impacting the signal.

Velocity profiling

- Tracks give you a relatively low resolution sampling of position.
- Unusually regular velocities are an indicator of spoofing

Velocity

- Radically different velocity profiles yield similar track results



Secondary data

- Some devices support wifi
- Check for artifacts of seen wifi networks
- Compare to Wifi Geolocation Databases like Mozilla Location Service and WiGLE

The State of Things

- Only “civilian” GPS systems are susceptible (right now)
- No commercial solutions using spoofing detection!
- Lots of academic work on detecting spoofing in real-time…
  - “GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals”, Psiaki Et Al (2011)
- This is new ground… plenty of opportunities for research

Next steps and further research

- Profile position jitter on more devices
- Integrate with GIS and traffic datasources to identify discrepancies
- Look into Jitter-detection from Optics
- Test additional spoofing methods

ANALYSIS SCRIPT DEMO

“Apply”

- Review your protocols for processing GPS track evidence
- Build a workflow for automatically calculating key parameters
- Seek corroborative evidence, always!

Any Questions?

- bkuzmacissp@gmail.com
- @BobbyAtCore