GPS SPOOFING: NO LONGER A FISH STORY

Michael Shalyt
CEO and Co-Founder
Aperio Systems
@MShalyt
Outline

- Intro – the world is being measured.
- Good examples of bad data.
- GPS forgery and pirates.
- “Fingerprinting”: the natural encryption of physics.
Michael Shalyt, CEO

**Physics:** B.E. Electrical Engineering, BA Physics, MSc Quantum Computing, International Physics Olympiad bronze medal.

**Cybersecurity:** Researcher and team leader at 8200 (IDF intelligence). Head of malware research at Check Point.

- Very multidisciplinary.
- Highly skilled.
- Background from military intelligence, Cloudlock (now Cisco) and Check Point.
THE MEASURED WORLD
The Trillion Sensor World
The Trillion Sensor World
Operational Data Flow

- HMI, Historian etc.
- OPC servers
- Switches
- PLC
- Modbus
- A/D
- Sensors
- Reality
WHEN GPS IS LYING
On Device – Voluntarily

Fake GPS Location - Hola

Hola  Tools

PEGI 3

Offers in-app purchases

This app is compatible with all of your devices.

Add to Wishlist  Install
On Device – Voluntarily

- Spoofing for cheating.
- Bans if spoofing detected.
- Example: “Rubber Banding” effect.
On Device – Non-Voluntarily

Unmanned Aircraft Capture and Control via GPS Spoofing

Andrew J. Kerns
Department of Electrical and Computer Engineering
The University of Texas at Austin
Austin, TX 78712
akerns@utexas.edu

Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys
Department of Aerospace Engineering
The University of Texas at Austin
Austin, TX 78712
dshepard@utexas.edu, jahshan@utexas.edu, todd.humphreys@mail.utexas.edu
On March 2014, 2 graduate students from the Technion (Haifa, Israel) created fake drivers on the Waze framework – thus fooling the system into believing in a traffic jam.

Waze went on to reroute traffic to other streets – while the actual road remained empty.
GPS Jamming

Data Centre ▶ Networks

US military tests massive GPS jamming weapon over California

Aircraft warned to stay out of area

By Iain Thomson in San Francisco 7 Jun 2016 at 22:21 56 ▶ SHARE ▼
GPS Jamming

Jamming GPS Signals Is Illegal, Dangerous, Cheap, and Easy
When a tanker vanishes, all the evidence points to Russia

In June, 37,000-tonne tanker vanished from GPS off the Russian coast. All the evidence points to Russia. But what’s really going on?
GPS Forgery (Spoofing) – How To
Protecting GPS From Spoofers Is Critical to the Future of Navigation

GPS is vulnerable to spoofing attacks. Here’s how we can defend these important navigation signals

GPS Forgery (Spoofing) – What For?

- Military deception.
- Hijacking cargo: directing victims into a trap.
- Hijacking cargo: hiding the theft from “homebase”.
- Tampering with “homebase” state awareness (shipping, air control, Waze etc.)
- Autonomous movement control (cars, ships, drones...)
- And many other scenarios.
Kill Chain for Damaging Physical Systems

Phases of the Intrusion Kill Chain

- **Reconnaissance**: Research, identification, and selection of targets. Pairing remote access malware with exploit into a deliverable payload (e.g., Adobe PDF and Microsoft Office files).
- **Weaponization**: Transmission of weapon to target (e.g., via email attachments, websites, or USB drives).
- **Delivery**: The weapon installs a backdoor on a target’s system allowing persistent access.
- **Exploitation**: Outside server communicates with the weapons providing “hands on keyboard access” inside the target’s network.
- **Installation**: The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target.
- **Command & Control**: Attackers must forge reported data to overcome safety mechanisms and control room operators.
- **Actions on Objective**: Sending damaging commands while the operators are blinded to the real system state.
GPS Forgery (Spoofing) – How?

- Hardware based (antennas, broadcast signals)

**GPS Signal Repeater Forwarder Transmitter Amplifier Antenna L1 DB2 15 Meters**

*Price: $149.00*

*Buy it Now or Best Offer*

*Free Shipping*

The outdoor antenna with RF cable connect to the "INPUT" of repeater, the antenna connect to the "OUTPUT" of repeater, and then power the repeater you will see indication light, then it work. - Reflect...

**GPS Signal Repeater Forwarder Transmitter Amplifier Antenna L1 DB2 30 Meters**

*Price: $425.60*

*Buy it Now or Best Offer*

*Free Shipping*

The outdoor antenna with RF cable connect to the "INPUT" of repeater, the antenna connect to the "OUTPUT" of repeater, and then power the repeater you will see indication light, then it work. - Interf...
GPS Forgery (Spoofing) – How?

- Software based (go between the hardware + driver + OS layer and the app layer).
SAVING THE DAY

(AND LOCATION BASED PRODUCTS)
According to The Department of Homeland Security (Nov 2017):

- Obscure antennas. Install antennas where they are not visible from publicly accessible locations or obscure their exact locations by introducing impediments to hide the antennas.

- Add a sensor/blocker. Sensors can detect characteristics of interference, jamming, and spoofing signals, provide local indication of an attack or anomalous condition, communicate alerts to a remote monitoring site, and collect and report data to be analyzed for forensic purposes.
Defending Against Spoofing

- Extend data spoofing whitelists to sensors. Existing data spoofing whitelists have been and are being implemented in government reference software, and should also be implemented in sensors.

- Use more GPS signal types. Modernized civil GPS signals are more robust than the L1 signal and should be leveraged for increased resistance to interference, jamming, and spoofing.

- Reduce latency in recognition and reporting of interference, jamming, and spoofing. If a receiver is misled by an attack before the attack is recognized and reported, then backup devices may be corrupted by the receiver before hand over.
"Hide antennas" – engineering complication and questionable efficiency (overriding signal can easily be strong enough to bypass obstacles).

"Dedicated sensor" – can be very efficient with the right algorithms, but adds hardware, bandwidth and engineering requirements.

"Whitelisting sensor hardware" – yeah...

"Use better GPS tech" – that’s rarely up to the end costumer/operator.

"Detect and report forgery ASAP" – the key concept. But how?
Next week/month:
- Standard best practices for endpoint device health.
- Sanity tests – when device is in a known location make sure the readings show it correctly, accurately and without “glitching”.

Next 6 months:
- Compare internal location logs to planned/known routes (if you aren’t collecting location logs – start collecting location logs 😊).
- Try achieving at least 1 redundancy layer (different location protocol, inertia/speed sensors etc.) for cross-validation.
- Get an anti-forgery algorithm or product.
The Power of Physics

- Gas powered power plant (~1GW capacity).
- ~5K sensors measuring every part of the process.
- Important values like RPM, gas flow rate, temperature etc.
- Easy to see modes of operation.
Gas flow rate during different modes of operation.
Each mode and each sensor can be fingerprinted.
Physical fingerprinting is a strong tampering and spoofing detection tool.
“Is This State Physical?”
THANKS FOR LISTENING!

Michael Shalyt
shalyt@aperio-systems.com
WWW.APERIO-SYSTEMS.COM
Data Structure

![Diagram of data structure with fields:
- Sync Char 1
- Sync Char 2
- Class
- ID
- Length (Little Endian)
- Payload size depending on Length and/or Class, ID
- Checksum]

- Dec 181
- Hex B5 (ISO 8859.1 for μ)
- 1 Byte Message ID
- Payload length excluding Sync Char, Class, ID, Length, and Checksum fields
- 2 Bytes Checksum

---

Dec 98
Hex 62 (ASCII for b)
1 Byte Message ID
Defending Against Spoofing – Add Sensors

- For civil users, multi-constellation receivers that can track multiple GNSS such as GPS, GLONASS, Galileo, and BeiDou simultaneously can be effective against spoofers, because an adversary would have to produce and transmit all possible GNSS signals simultaneously to spoof the target receiver.

- An additional measure of protection can be added by aiding the navigation solution with an inertial measurement unit (IMU), as an adversary cannot spoof the Earth's gravitational field or vehicle dynamics and cause the inertial unit to think it has moved in a way that it hasn't.