Using GPS Spoofing to Control Time
Dave, Karit, @nzkarit

Security Consultant at ZX Security in Wellington, NZ

Enjoy radio stuff

Pick Locks and other physical stuff at Locksport
Today

- GPS (Global Positioning System)
- GPS Spoofing on the cheap
- Let’s change the time!
  - So what?
- Attacking NTP Servers
- How we can detect spoofing
GPS

- Tells us where we are
- Tells us the time
We Trust GPS Right? Right?????

- Anyone in the room not currently trust GPS locations?
- Anyone in the room not currently trust GPS time?
- Anyone feel that this will change by the end of the talk?
You have to trust it right?

- GPS too important to life?
- GPS must be great and robust? Right?
- Important services rely on it:
  - Uber
  - Tinder
And some other things as well

- NTP Time Source
- Plane Location
- Ship Location
- Tracking Armoured Vans
- Taxi law in NZ no longer knowledge requirement
So why don’t I trust it?

Truck driver has GPS jammer, accidentally jams Newark airport

An engineering firm worker in New Jersey has a GPS jammer so his bosses don't know where he is all the time. However, his route takes him close to Newark airport, and his jammer affects its satellite systems.
Black Cabs in London

- Have GPS jammers to mess with Uber
Jammers Boring.......
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
Professor fools $80M superyacht’s GPS receiver on the high seas

Todd Humphreys says defenses are scant: "nobody knows how to use a sextant."

by Cyrus Farivar - Jul 30, 2013 12:30pm NZST

A team from the University of Texas spoofed the GPS receiver on a live superyacht in the Ionian Sea.
The Chinese are in the NTPs

Time is on my side

Forging Wireless Timing Signals to Attack the NTP Server

Yuwei Zheng @HITB
Haoqi Shan @HITB
From: Qihoo360 Unicorn Team
Now we are talking

osqzss / gps-sdr-sim

Software-Defined GPS Signal Simulator
What we need

- A box
- An SDR with TX
  - I used a BladeRF
  - HackRF
  - USRP
- So less US$500 in hardware
- Also some aluminium foil to make a Faraday Cage
- So it is now party trick simple and cheap
  - This is the big game changer from the past
Setup
@amm0nra patented Faraday Cage

- Make sure you measure signal outside to ensure none is leaking
- Be careful
The Law

- INAL (I’m not a lawyer)
- GPS isn’t Open Spectrum
- So Faraday Cage
- Keep all the juicy GPS goodness to yourself
Remember

- Your SDR kit is going to be closer to the device
  - So much stronger signal
  - Got to have line of sight though
- GPS Orbits ~20,000 km
  - So signals weak
  - Signal is weaker than the noise floor
Noise Floor

- Received Signal Strength
- Noise Floor
- Power (dBm)
- SNR (dB)
- Time (Secs)

GPS C/A
NOISE FLOOR, 2 MHz BW

POWER (dBm)

FREQUENCY (MHz)
Right so what can we do?

- Got some simulator software and a bladeRF what could people get up to?
A trip to Bletchley Park?
How does the tool work?

- Two methods, first one two steps
  - 1. Generate the data for broadcast
    - About 1GB per minute
    - Static location or a series of locations to make a path
    - Has an Almanac file which has satellite locations
    - Uses Almanac to select what satellites are required for that location at that time
  - 2. Broadcast the data
How does the tool work?

- Generate in real time
- Need a fast enough computer
- 1. Generate and broadcast
Limitations of tool

- By default only 5 mins of transmit data
  - Need to change a value in code for longer
  - Approx. 1GB a minute hence the limit
- Pi3 about three times slower than real time, so must be precomputed
  - Pi3 there is a file size limit
    - <4GB from my experience, so 4-5 minutes of broadcast per file
  - Can just chain a series of pre computed files together
Generate a Path

- To do the path give the generator a series of locations at 10Hz
- Can’t just give a series of lat/long in a csv 😞
  - ECEF Vectors or
  - NMEA Data rows
- There are convertors online 😊
A Path
So what can we do?

- with GPS location spoofing
Keep an armoured van on track as you take it to your secret underground lair

Have a track following its normal route while drive it somewhere else
Uber trip with no distance?
Planes

- For places like Queenstown planes have Required Navigation Performance Authorisation Required (RNP AR)
  - When not visual conditions
  - As approach is through valleys
    - Can’t use ground based instrument landing systems
  - If go off course going to hit the ground
Can we use this to change time?

- NTPd will take GPS over serial out of the box
- The NTP boxes also use NTPd behind the UI
  - NTPd uses its own license, so easy to spot in manuals etc
If you move time too much >5min NTPd shutdown

No log messages as to why

When starting NTP you get “Time has been changed”

And NTP will accept the GPS even if it differs greatly from the local clock
If we turn the logging up

With debugging enabled

- Feb 24 02:36:21 ntpgps ntpd[2009]: 0.0.0.0 0417 07 panic_stop +2006 s; set clock manually within 1000 s.
- Feb 24 02:36:21 ntpgps ntpd[2009]: 0.0.0.0 041d 0d kern kernel time sync disabled
Would a Sys Admin notice?

- If NTPd crashes but starts via watchdog or a manual restart
  - Will people look deeper?
  - Will people check the time is correct?
So how can we move time?

- We can’t do big jumps in time
- We will have to change time in steps
Introducing TardGPS

- Python Script
- Wraps the real time version of the GPS Simulator
- Moves time back in steps
  - So as not to crash NTPd

- Talked in more detail at Kiwicon 2016

- Slides:

- Code:
  - https://github.com/zxsecurity/tardgps
Note

- This will only work on an Air Gapped network
Network Layout

Diagram showing:
- Hacker
- Local Machine
- GPS Broadcast
- Radio
- Target Laptop
- NTP Server
Local machine
Mon Sep 26 15:26 UTC 2016

Target machine
Mon Sep 26 22:49:28 UTC 2016

user@ubuntu:~/tardgps$ ./tardgps.py

Time difference (to nearest minute)
0 min
Timebased One Time Password

- **TOTP**
- E.g. Google Auth
- A new token every 30 seconds
Do you want to disallow multiple uses of the same authentication token? This restricts you to one login about every 30s, but it increases your chances to notice or even prevent man-in-the-middle attacks (y/n)
## TOTP Implementations

<table>
<thead>
<tr>
<th>Library</th>
<th>Default</th>
<th>No Default</th>
<th>Default Reuse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Auth libpam</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Two Factor Authentication (Wordpress Plugin)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OATHAuth (MediaWiki Plugin)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Library</th>
<th>Support</th>
<th>No Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Github - pyotp/pyotp</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Github - mdp/rotp</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Github - Spomky-Labs/otphp</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Github - pquerna/otp</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Support is a method that does verify with prior context
What to look for in a TOTP

- Make sure there is a setting related to reuse
- Make sure it is set to not allow reuse
Also other 2FA solutions

- HOTP - HMAC-based one-time password
  - Also in Google Auth
- U2F
  - One token can be used on many sites
  - One user can subscribe more than one token
- Friends don’t let friends SMS
SUDO

- SUDO counts time in a different way, using OS Clock Ticks
  - so you can’t roll back time and bypass sudo password check timeout
- sudoer file `timestamp_timeout=X`
- Uptime works in a similar way
Uptime during jump

Mon Nov  7 01:40:30 UTC 2016
01:40:36 up 4 min, 2 users, load average: 0.00, 0.04, 0.03

Fri Nov 18 13:01:14 UTC 2016
13:01:17 up 7 min, 2 users, load average: 0.21, 0.08, 0.05
Forensics

- Incident Response becomes interesting when your logging starts showing:
  - Nov 18 13:45:43 important-server: Hacker logs out
  - Nov 18 13:46:54 important-server: Hacker performs l33t hack
  - Nov 18 13:47:47 important-server: Hacker logs in

- Through time manipulation or cron running: date set ‘some random time’

- Also if move time forward could make logs roll and purge
  - If no central logging
From a Stringray Manual

(Thanks to @VickerySec to finding this)

External GPS - Sometimes an external GPS device will emit erroneous GPS ticks, causing the Gemini activation license to expire.
Physical Access

- What can we do if we have access to the data centre roof?
- GPS unit with aerial on roof serial down
- GPS unit in server and radio down wire from roof
  - Attach transmitter to wire with attenuator

- Use server 127.0.20.0
  - ntpd then knows to look at /dev/gps0 and /dev/pps0 for import
Serial

- NMEA Data – Serial Data (/dev/gps0)
  - $GPGGA,062237.000,4117.4155,S,17445.3752,E,1,9,0.97,177.1,M,19.0,M,,*4A
  - $GPRMC,062237.000,A,4117.4155,S,17445.3752,E,0.16,262.97,120217,,A*7E
  - Hour, Minute, Second, Day, Month, Year
- Pulse Per Second – PPS (/dev/pps0)
PPS

- Doesn’t contain time value
- It indicates where a second starts
- Less processing on the GPS Receiver so comes through in a more timely manner
- Rising edge can be in micro or nano second accuracy
NTP Setup

- I had NTPd running on a raspberry pi
- GPS receiver via UART serial on GPIO pins
- One wire was for PPS
How to spoof PPS

- Link the PPS pin to another GPIO pin
- Set that pin high and low as applicable
So what happens

- If run PPS with a different timing the NEMA data will keep correcting
- So will keep pulling it back
- So within ±1 second
- Maybe an issue in finance, telecoms and energy
  - Where fractions of a second count
Can we just remove the NMEA data?

- If pull serial NTPd Tx wire
- Stops the source in NTPd, even if getting PPS signal
- So can’t manipulate time just through PPS manipulation
NMEAdesync

- Python Script
- Moves time back in steps
- So as not to crash NTPd

- Talked in more detail at BSidesCBR
- Slides:
- Code:
  - https://github.com/zxsecurity/NMEAdesync
NMEAdesync

- Similar in concept to tardgps
- Though changing the data in the NMEA data rather than GPS Signal

- Adjust the time
- Adjust how fast a second is
- Also does the PPS generation

- Offers more control than tardgps
  - No GPS signal tom foolery
NMEAdesync under the hood

- Python Script
  - stdout $GPRMC and $GPGGA
  - PPS high/low on pin
- Loop
  - socat stdout to /dev/pts/X
  - Symlink /dev/pts/X to /dev/gps0
- ntpd takes it from there
NMEA desync running

- I could get similar behaviour as tardgps
- But simpler to execute as don’t have the radio aspect
- Though will require physical access to the roof of the building
Their clients

Our involvement on the globe

- **European Airports** - NTP time synchronization in air traffic control centers
- **Mobile operators** - NTP servers for global time sync
- **All locale powerplants** - NTP servers for global time sync
- **Atomic powerplants** - NTP servers for time sync
So what did it do?

- If jumped time a large amount forward
  - It just worked
  - Didn’t need TardGPS
- Backwards did require TardGPS or NMEADesync
  - Behaved like NTPd earlier
Network Setup

IP Address: 192.168.0.16
Subnet Mask: 255.255.255.0
Gateway IP: 0.0.0.0
SNMP IP for traps: 192.168.0.1
Mac Address: 100.18.1.33
GET /par?1=123456&Bl=Submit HTTP/1.1
Host: 192.168.0.16
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
DNT: 1
Referer: http://192.168.0.16/getpwd.html
Accept-Language: en-US, en; q=0.8
Connection: close

HTTP/1.1 200 OK
Server: Ubicom/1.1
Content-Length: 1123

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<link rel="stylesheet" type="text/css" href="styles.css">
<title>NetworkSetup</title>

<p align="center">NetworkSetup</p>
</head>
</html>
Writing new password to system...
How can we detect this?

- GPS Signal Spoofing
GPSnitch

- Talked in more detail at Unrestcon 2016
- Slides on ZX Security’s Site:
  - https://zxsecurity.co.nz/events.html
- Code on ZX Security’s Github:
  - https://github.com/zxsecurity/gpsnitch
What does GPSnitch Do?

- Time offset
- SNR Values
- SNR Range
- Location Stationary
Useful for

- NTP Servers
- Also GPS units wanting to know location
How can we detect this?

- NMEA Serial Spoofing
NMEA Snitch

- https://github.com/zxsecurity/NMEAsnitch
- Records the NMEA sentences
- Looks at the ratios and sentences per second
Output per second

<table>
<thead>
<tr>
<th>Sentence</th>
<th>per second</th>
</tr>
</thead>
<tbody>
<tr>
<td>$GPGGA</td>
<td>1</td>
</tr>
<tr>
<td>$GPGSA</td>
<td>1</td>
</tr>
<tr>
<td>$GPGSV</td>
<td>0.6</td>
</tr>
<tr>
<td>$GPRMC</td>
<td>1</td>
</tr>
<tr>
<td>$GPVTG</td>
<td>1</td>
</tr>
</tbody>
</table>
What does it do?

- Alert when the rate of sentences doesn’t match the norm
NTP Setups to avoid GPS Spoofing

- 3+ Upstream
  - Allows for bad ticker detection and removal
- Multiple Types of upstream
  - I.e. don’t pick 3 GPS based ones
  - GPS, Atomic
- Don’t pick just one upstream provider
  - Rouge admin problem
  - Maybe one overseas so gives you a coarse sanity check of time
“Air gapped” networks

- But GPS is travelling across the air…
- Consider atomic, caesium, rubidium
Changes for NTPd or NTP Server

- Incorporate GPSnitch
- Additional logging for when daemon shuts down due to a time jump
- On daemon restart after a large time jump occurs, prompt user to accept time jump
Thanks

- bladeRF – Awesome customer service and great kit
- Takuji Ebinuma – for GitHub code
- @amm0nra – General SDR stuff and Ideas
- @bogan & ZX Security – encouragement, kit, time
- Fincham – GPS NTP Kit
- Unicorn Team – Ideas from their work
- Everyone else who has suggested ideas / given input
- DefCon – For having me
- You – For hanging around and having a listen
- GPSd – Daemon to do the GPS stuff
- GPS3 – Python Library for GPSd
Thanks
GPSnitch

- **Slides:** [https://zxsecurity.co.nz/presentations/201607_Unrestcon-ZXSecurity_GPSSpoofing.pdf](https://zxsecurity.co.nz/presentations/201607_Unrestcon-ZXSecurity_GPSSpoofing.pdf)
- **Code:** [https://github.com/zxsecurity/gpsnitch](https://github.com/zxsecurity/gpsnitch)
GPSnitch

- **Slides:** [https://zxsecurity.co.nz/presentations/201607_Unrestcon-ZXSecurity_GPSSpoofing.pdf](https://zxsecurity.co.nz/presentations/201607_Unrestcon-ZXSecurity_GPSSpoofing.pdf)

- **Code:** [https://github.com/zxsecurity/gpsnitch](https://github.com/zxsecurity/gpsnitch)
tardgps

- Code: [https://github.com/zxsecurity/tardgps](https://github.com/zxsecurity/tardgps)
How To

- Code
  - https://github.com/osqzss/gps-sdr-sim/
  - https://github.com/osqzss/bladeGPS
  - https://github.com/keith-citrenbaum/bladeGPS - Fork of bladeGPS for Linux

- Blog
  - http://en.wooyun.io/2016/02/04/41.html

- Lat Long Alt to ECEF
Libraries Used

- **GPS3 Python Library**
  - [https://github.com/wadda/gps3](https://github.com/wadda/gps3)

- **GPSd Daemon**
References

References

References

- https://documentation.meraki.com/@api/deki/files/1560/=7ea9feb2-d261-4a71-b24f-f01c9fc31d0b?revision=1
- http://www.microwavejournal.com/legacy_assets/images/11106_Fig1x250.gif
- https://pbs.twimg.com/profile_images/2822987562/849b8c47d20628d70b85d25f53993a76_400x400.png
- https://upload.wikimedia.org/wikipedia/commons/4/49/GPS_Block_IIIA.jpg
- https://www.yubico.com/wp-content/uploads/2015/04/YubiKey-4-1000-2016-444x444.png
- http://www.gpsntp.com/about/
References