Kings Place 3rd October 2019

Christian Farrow  B.Sc. (Hons) MinstP
Technical Services Manager
Introduction

- Cybersecurity Landscape
  - Hackers Everywhere
  - Even in the PSTN?
- Making a Time Spoofer
  - It’s not just the recipe
- Can we make an Anti - Time Spoofer?
  - ...and other ways to beat the bad guys
“Everything is a computer”
- Smartphones, Massive IoT, speakers, thermostats, fridges, pacemakers, insulin pumps, cars, planes, chemical plants...

“All computers can be hacked”
- Current software development is inherently insecure
  - “move fast & break things”
  - Constant updates & patching

“Cyberwar is the new normal”
- Constant sniffing/probing/attack

https://www.schneier.com/books/click_here/
Schneier, B. Click Here to Kill Everybody - September 2018
W. W. Norton & Company ISBN: 978-0393608885
Power Industry

Ukraine Grid Cyberattack

- In December 2015, attackers compromised SCADA and opened circuit breakers in at least 30 substations.

- Interruption of service to over two hundred thousand customers.

- Switched to manual mode of operation to restore power.

- Started with phishing emails that infected corporate machines – if able to infect asset management machines, even easier to get to grid assets.

Credit: Gowri Rajappan, Ph.D. Solutions Director for Security and NERC CIP [https://www.doble.com/product-category/security/](https://www.doble.com/product-category/security/) Email: grajappan@doble.com
Telecom Industry threats

- In the past “Private Networks”
- Internet Connectivity changed that
  - SDN/NFV
- Internal attacks
  - Disgruntled/aggrrieved employee
- External attacks
  - Extortion, Money, Mayhem
  - ”for the LOLs”
Telecom Industry threats
Telecom Industry threats - Fake BTS

- Software Defined Radio – SDR
  - Digitally controlled, analogue RF in/out
- Example shown based on LimeSDR (~$300)
- Commercial versions of Fake BTS available as “Lawful Intercept” to Law Enforcement & Government Agencies – colloquially known as a “Stingray”
  - Indiscriminate or targeted?
**Telecom Industry threats - iPhone**

- **Google “Project Zero” vulnerabilities**
  - [https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html](https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html)
  - “Earlier this year Google's Threat Analysis Group (TAG) discovered a small collection of hacked websites. The hacked sites were being used in indiscriminate watering hole attacks against their visitors, using iPhone 0-day.”

- **Monitoring:**
  - calls
  - mic/camera
  - photos/files
  - location
  - un-encrypted access to whatsapp etc.

### Diagram:

- Chain 1: 10.0.1-10.1.1
- Chain 2: 10.3-10.3.3
- Chain 3: 11.0-11.4
- Chain 4: 12.0-12.1
- Chain 5: 11.4.1-12.1.2

---

*Just one of 1000s!*
Telecom Industry threats – critical infrastructure

- Classic DoS – flood SIP/SS7 or other elements?
- 5G Functional Decomposition
  - Control plane function in COTS server/datacentre
- Power outage? How long can UPS last?
- GPS Jamming
  - “Who can shout the loudest” – not subtle
  - Easy to locate
  - That classic game of cat & mouse – [Schneier] “Bad guys have to stay one step ahead”

*Can we spoof a GPS signal that we can precisely control to bring down telecom infrastructure...?*
4G/5G Architecture – GNSS attack surface

- LTE-A / 5G Basic Service +/-1.5usec
- 5GNR Advanced Services +/-130nsec
What exactly is GPS?

Clock (timing) errors add a 4th unknown, hence 4 satellites require for precise fix.
Getting the right time wrong (on purpose)

GPS spoofing attack on time synchronization in wireless networks and detection scheme design

Publisher: IEEE

3 Author(s) Qi Zeng; Husheng Li; Lijun Qian

© 2019 Chronos
Getting the right time wrong (on purpose)

EVERYTHING FAILED!

REAL-TIME SIMULATOR
Time Control

Time Spooﬁng Attack Parameters

Select Proﬁle:
- Linear with Ceiling, Exponential, Logarithmic

Load Attack Parameters

Enter Attack Parameters:
- α: 1e-10 seconds/sec²
- β: 1e-9 seconds/sec
- t₀: 0 seconds
- t₁: 100 seconds

Attack Control

Receiver Type: TEST RECEIVER

Record:
- Record:
- Record Filename:
- Duration: 1000000 seconds

GPS Simulator
Getting the right time wrong (on purpose)

- 2015 Colleagues at Spirent & Calnex presented detailed lab based spoofing scenarios using 2 x (expensive) simulators
Getting the right time wrong (on purpose)

- 2019 – using similar simulators as part of testing process
  - Legitimate uses:
    - Leap second scenarios
    - Re-creating GPS outages/failures
    - Repeatable test conditions
  - No RF broadcast
    - Direct connection only
  - Needs accurate ref clock + complex software control
  - Cost many £10,000s
Getting the right time wrong (on purpose)

- Another research project Chronos is involved in with Spirent
Getting the right time wrong (on purpose)

- Remember the LimeSDR?
- Chronos Hardware/Embedded team uses one as a GPS simulator in the lab to test leap-second scenarios
  - Lab environment, with Intel NUC running Ubuntu, LimeSDR + direct connection to unit under test
- I wondered...

“could I make a portable (battery powered) GPS simulator with LimeSDR + Raspberry Pi?”

...?????
Getting the right time wrong (on purpose)

- Yes. Of course!
  “Everything you can think of has already been done and is on the internet”

Getting the right time wrong (on purpose)

- Wireless Attack

WALB (Wireless Attack Launch Box)

What is WALB?

- WALB is a Raspberry Pi2/Pi3 and HackRF based lunch box sized portable RF signal generator.
- The intended purpose of the WALB development is to test or demonstrate the security issue of wireless devices and location based applications.
- By preparing a I/Q binary data, it is possible to generate any signal in the frequency range available to HackRF.
- For GPS and ADS-B, real time signal generator module is included in WALB.
- It uses HackRF as a SDR unit with enhanced GPS-SDR-SIM for GPS signal generation.
- It has a 8x2 LCD and a rotary encoder with two color LED and a push switch for the operation of WALB.
- Since WALB works with battery powered, you can use it anywhere you like.
- Adding new simulation scenario or signal generation, it can be achieved by SSH login and simply edit the menu items using your favorite text editor.
- By preparing the binary I/Q signal file of 8 bit signed, you can generate arbitrary RF signals.
- To do so, you simply need to edit and add TEXT menu items specifying the filename of I/Q file, frequency, and sample rate.
- If you prepare an external program to generate the I/Q signal in real time, you can also add the program and/or script in the menu.
- You can set or chose GPS spoofing scenario by predefined location and/or date & time.
Building the spoofer

- Plug LimeSDR into (linux) laptop
- Google “LimeSDR Fedora Install”
- Follow 4 or 5 installation steps
  - Working SDR! – tested as FM receiver 😊
- Google “LimeSDR GPS simulation”
- Follow 4 or 5 installation steps
- Repeat with LimeSDR connected to RasPi
- Add some shell script/web front end
Building the spoofer

- LimeSDR
- RasPi 4B
- GNSS ref
- LimeSDR Power (8.4V Li-ion)
- RasPi Power (5V USB)
“Spoofing Time Attack (in a Lunch) Box” - STAB

- STAB features
  - RasPi wifi – web GUI
  - Lock reference to GNSS to get stable & accurate time
  - Disconnect GNSS – use CSAC holdover
  - Initiate time attack remotely
  - Portable, ~8hr runtime (LimeSDR)

- **Cost:** ~$400 ! (box was free)
  
  **Approx time to build:** 1 day

- Future enhancements: 1PPS, heatsinks, power

- Currently being evaluated with partners as part of a research project
Time jumps backwards – receiver(s) crashed – REQUIRED POWER RESET

Time steered forwards – spoofing stopped – some REQUIRED POWER RESET, some ALARMED & RESTARTED

Time steered backwards – spoofing stopped – some ALARMED & restarted, some carried on and outputs jumped forward
How real is the STAB threat...?

Could a “smart” receiver detect spoofing?

- **Monitor Power Level**
  - Spoofed signal is likely to have higher power level
  - Monitor relative signal strengths: each signal should have a fixed relative power offset – if this changes suddenly, there’s a problem

- **Monitor Position**
  - Fixed infrastructure timing receiver shouldn’t be moving!

- **Compare & Bound (pseudo)range rates**
  - Code and carrier range rate changes will be different for spoofed signal

- **Doppler Check**
  - Spoofed likely to be stationary, Doppler may be incorrect

- **Verify Nav data**
  - Compare almanac/ephemeris and check for missing/default data

- **Detect Jumps**
  - Check for sudden changes
Mitigation – getting the right time right

- Build our own GPS sim in case real GPS is spoofed!
- Monitor GPS from our antenna against a stable reference (time/freq from our local (PRC—ePRTC) clock + surveyed location)
- If we decide we are being spoofed/jammed we can supply our simulated GPS signal to our critical infrastructure
- The “GPS firewall”
  – Not restricted to just GPS
- The complete GNSS Firewall
The GNSS Firewall

- Multi-constellation receivers
  - Go some way to being able to check GPS vs. GLONASS vs. Galileo etc.

- Add some sensible network engineering
  - Backup sources for time/freq
  - PTP/SyncE
  - Configure devices to qualify/compare inputs where possible

- GNSS signal hardening becomes part of the overall defence
GNSS Firewall Deployment models

**Firewall using Validated Output**
- NPT/PTP SyncServer etc.
- Validated

**Firewall using Hardened Output**
- Equipment requiring GPS/L1 signal
- Optional MAC
- Optional Cesium

**Firewall deployed for monitoring, not in GPS signal path**
- GPS Splitter
- Equipment requiring GPS/L1 signal

**Optional**
- TimePictra with BlueSky
- Validated Output
Critical Infrastructure providers need to recognise the threat
– Many read the news, but have not felt the pain
– Visibility is a smart first step towards proactively securing GNSS reception... rather than waiting for disaster to strike

Ability to quickly recover from anomalous GNSS events is greatly aided by real-time diagnostics and reporting
– Most users don’t actively monitor the health of GNSS...the “set it and forget it” culture needs to be changed
– Knowing is half the battle: Situational awareness reduces time spent identifying and localizing the issue
Mitigation – getting the right time right

- CyberSecurity practice should include the whole attack surface
  - Time is a piece of that jigsaw

- Network Engineering should protect GNSS
  - Redundancy, Back-ups, Augmentation
  - SyncE, NTP/PTP, Cs – LF radio also

- GNSS Firewalls are available
Christian Farrow  B.Sc. (Hons) MinstP
Technical Services Manager

Christian.Farrow@chronos.co.uk