



Moving Targets

Location-Based Threats And
Mitigations

by David Kane-Parry



Introduction

- David Kane-Parry, Principal Security Analyst.
- Leviathan Security Group at leviathansecurity.com.
- Previous Toor* Speaker.



Intro To GPS

- Global Positioning System
 - Satellites
 - Monitoring Stations
 - Receivers
- Funded for more precise nuclear strikes.
- Opened to public after KAL 007 is shot down.



GPS Satellites

- 30 healthy and in orbit.
- Line-of-sight to 8 from any point.
- 4 or more needed for accuracy.
- Broadcasts:
 - Atomic clock time.
 - Satellite health.
 - Satellite orbit.
 - Health and orbit for other satellites.



Civilian & Military GPS

- Broadcasts CDMA encoded.
- Civilian uses public codes, military uses private codes.
- Military can deny civilian service on regional basis.
- Military service is more resistant to jamming.
- Civilian accuracy previously degraded.



GPS Monitoring Stations

- Monitor raw GPS signal.
- Correct orbiting data.
- Upload back to satellites.
- Modern satellites can correct orbit by monitoring other satellites.



GPS Receivers

- Compares clock times to determine transit time.
- Compares transit time and orbit to determine position.
- May re-use atomic clock time to calibrate local clock.
- If it works > 18 km & 515 m/s, it's a weapon.



GPS Applications

- Navigation
- Social networking
- Geotagging
- Geocaching, etc.



GPS Data Sources

- Device Storage
- Online Service Storage
- Network Transfer
- Installed Application



GPS Wins

- Where you are.
- Where you are not.
- Where you have been.
- Where you are headed.
- How fast you are moving.
- What time you think it is.



The Threat Of Where You At

- Need directions from your secret lair?
- Really stuck at the office?
- Where do you summer?



The Threat Of Where You Been

- Where were you on the night of the break-in?
- How many times a week were you checking in to that bar before your accident?
- How often were you at the location of some chance encounter?



The Threat Of Where You Goin'

- Do you know how fast you were going?
- Needles in a very small haystack.
- Need directions to your secret dead drop?



The Threat Of GPS Spoofing

- What are the consequences of resetting clock to min time?
- What are the consequences of resetting clock to max time?
- What are the consequences of trusting location data?



The Threat Of GPS Profiling

- Can you get GPS in a war-torn area?
- Congrats, you've owned a military device.
- Can you get the military CDMA encoding?
- Congrats, you don't need that military device anymore.



The Threat Of GPS “Evidence”

- Legal standards are only best effort.
- GPS signal can be spoofed.
- GPS devices can be rooted.



Mitigations For Platform Developers

- Enable fine-grained controls:
 - Enable/disable GPS system-wide.
 - Enable/disable GPS on per-application basis.
 - Enable/disable GPS information available to apps.
- Provide secure geocoding APIs.
- For high-sensitivity environments, authenticate calling apps.



Mitigations For App Developers

- Consider if GPS is appropriate.
- Consider that GPS cannot be trusted.
- Consider that GPS may be sensitive in your context:
 - Don't save it if you don't have to.
 - If you have to save it, tightly control access.
 - If you have to transfer it, encrypt it.



Mitigations For Users

- Consider if GPS is appropriate.
- Consider that GPS cannot be trusted.
- Consider that GPS may be sensitive in your context:
 - Mind the circumstances that an app uses GPS
 - Mind if/where GPS data is saved.
 - Mind if/when/how GPS data is transferred.



Questions/Comments?

dkp at [leviathansecurity.com](mailto:dkp@leviathansecurity.com)