SwRI
SOUTHWEST RESEARCH INSTITUTE

GPS cyber-security work

Ben Abbott – Institute Engineer
Gerardo Trevino – Research Engineer

Applied Sensing Department

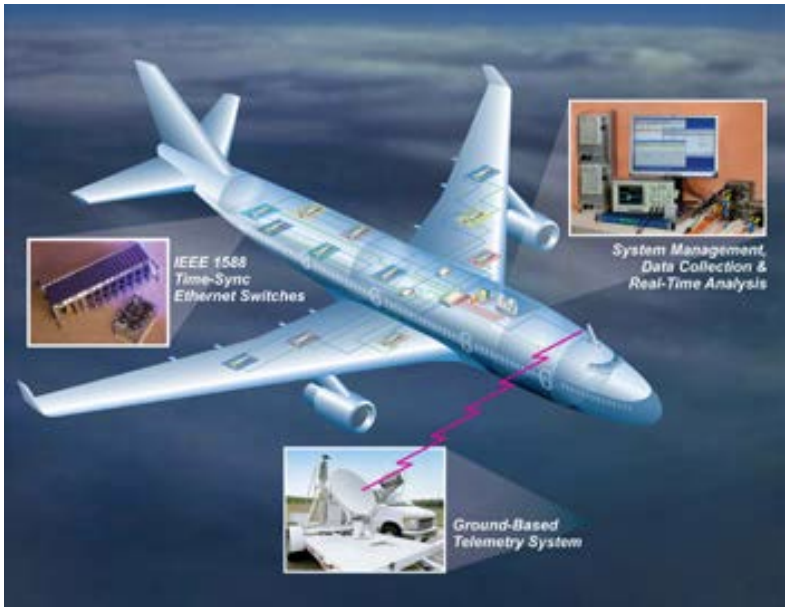

How we ended up at NASPI

Distributed Instrumentation

➔ GPS timing protection

➔ PMU work

➔ Atlanta



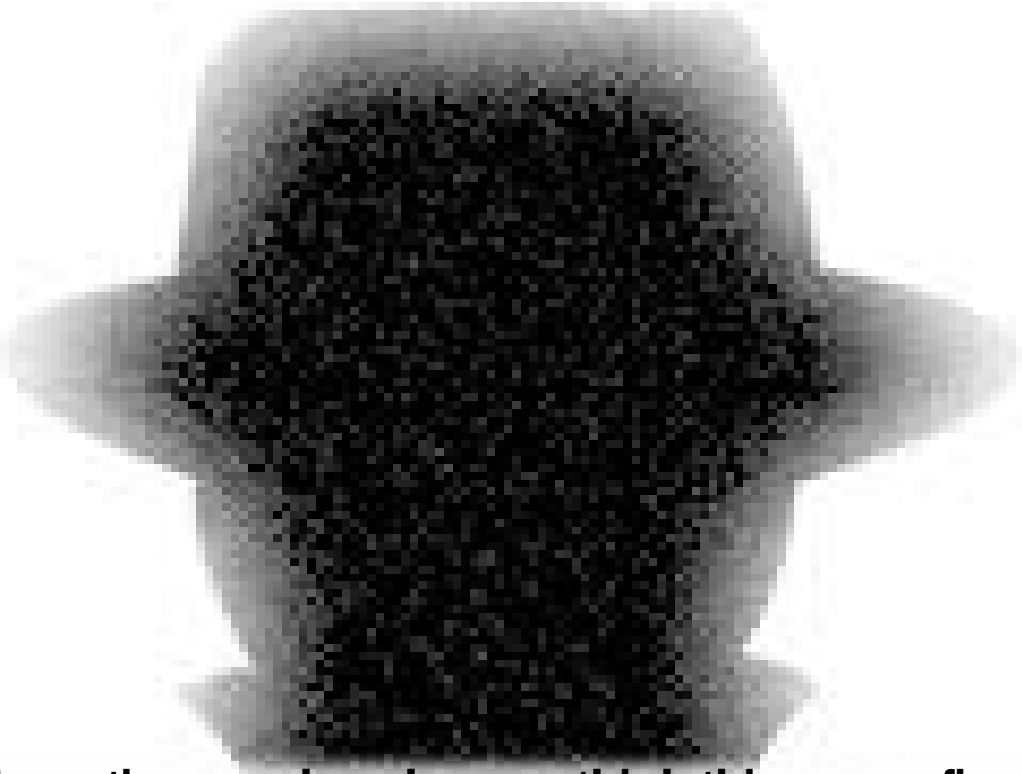
Why are we are doing this?

- Industry desire for millisecond response time
  - Requires clock synchronization
- Time synchronized applications/uses
  - **PMU / Synchrophasors**
  - Substation Automation Algorithms
  - Falling Conductor Algorithms
- Potential impacts
  - Current GPS hardware is vulnerable
  - Disruption of time synchronized applications
  - Data quality may be impacted without time quality alerts

- Why GPS?
  - The Good
    - Accurate, cost-effective time source
    - Easy synchronization of distant devices
  - *The Bad*
    - *Drawback: vulnerable to RF natural anomalies and malicious attacks*

http://www.baynews9.com/content/news/baynews9/news/article.html/content/news/articles/cfn/2013/12/4/kissimmee_power_subs.html
http://www.information-age.com/technology/mobile-and-networking/123457158/google-backed-start-up-launches-low-orbit-internet-satellites

The Ugly



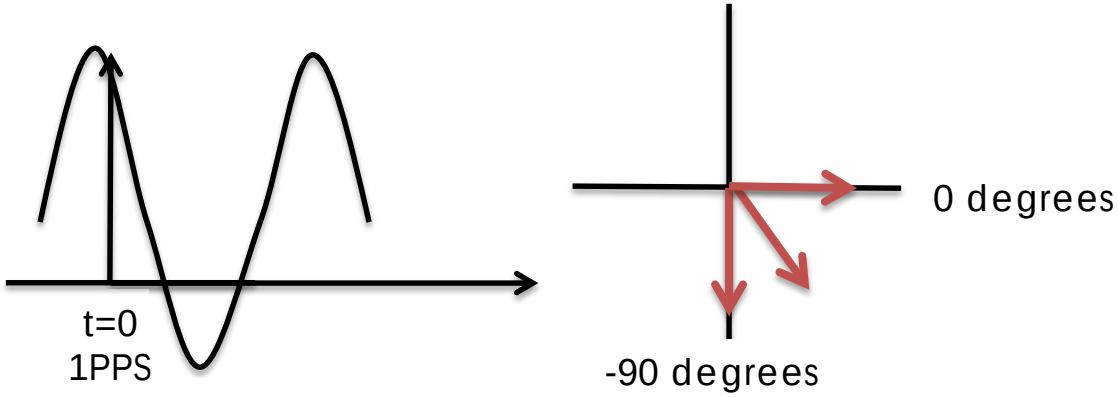
Move time and make you think things are fine

Move time and make you think things are bad and get you to break things

*Image is modification of the Blackhat conference logo

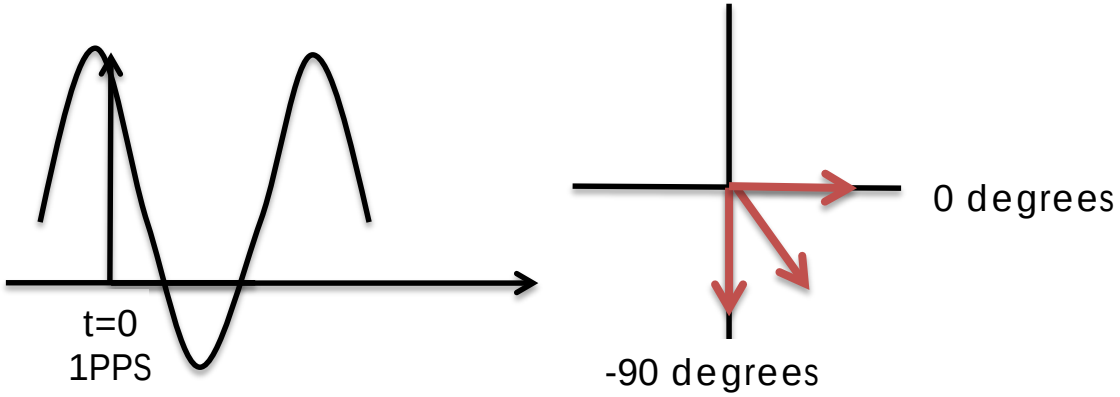
What if GPS time is wrong?

- Phase angle change of 90º is about a 4.17ms drift
- 10 degrees of phase angle change equals 463µs
- C37.118.1-2011 Standard mandates ~23usec



What if GPS time is wrong?

- Phase angle change of 90º is about a 4.17ms drift
- 10 degrees of phase angle change equals 463µs
- C37.118.1-2011 Standard mandates ~23usec

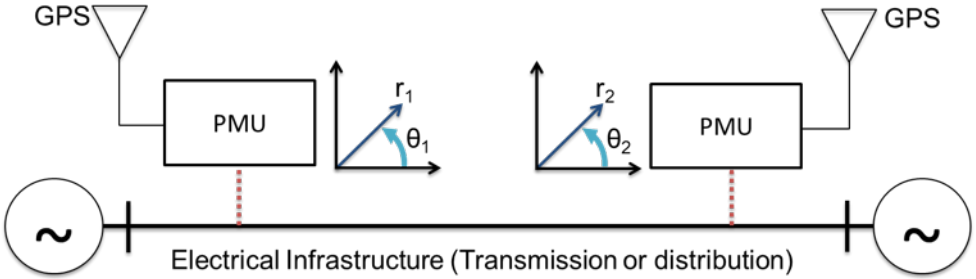


It's not where the phase is,
it's when the phase is...

But, is it real?

Chicoasen-Angostura transmission link in Mexico

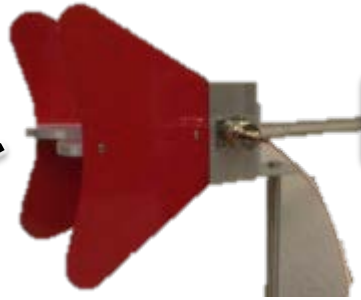
- GPS Spoofing causes fault in both of the 400-kV lines, creating angular instability with phase angle difference greater than manual threshold
- Generator trip could cause damage to generator and transmission lines



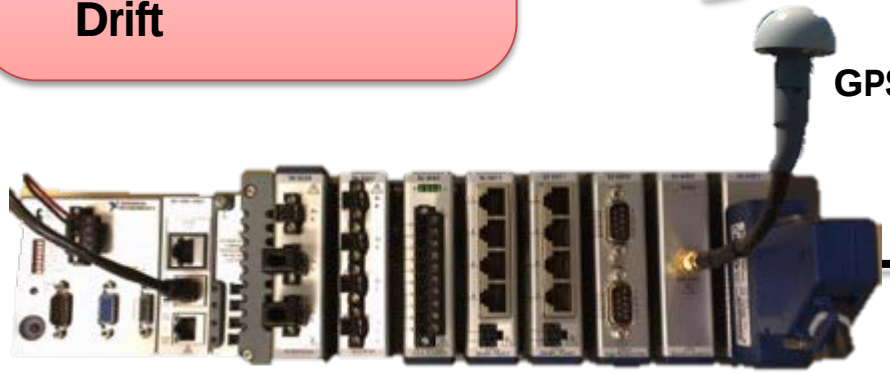
***2011 "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks" UT Austin & Northrup Grumman*

30 minutes later

- Jitter
- Fast Spoofing Drift
- Slow Spoofing Drift

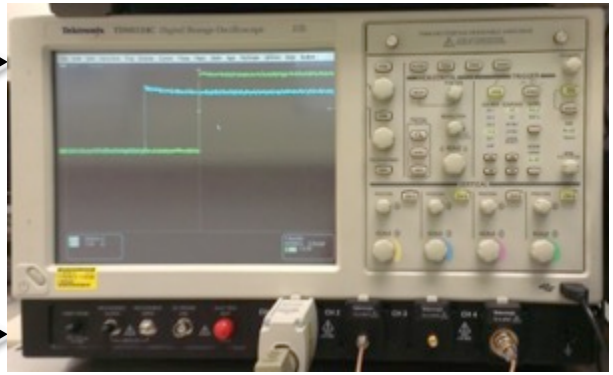


- Jamming

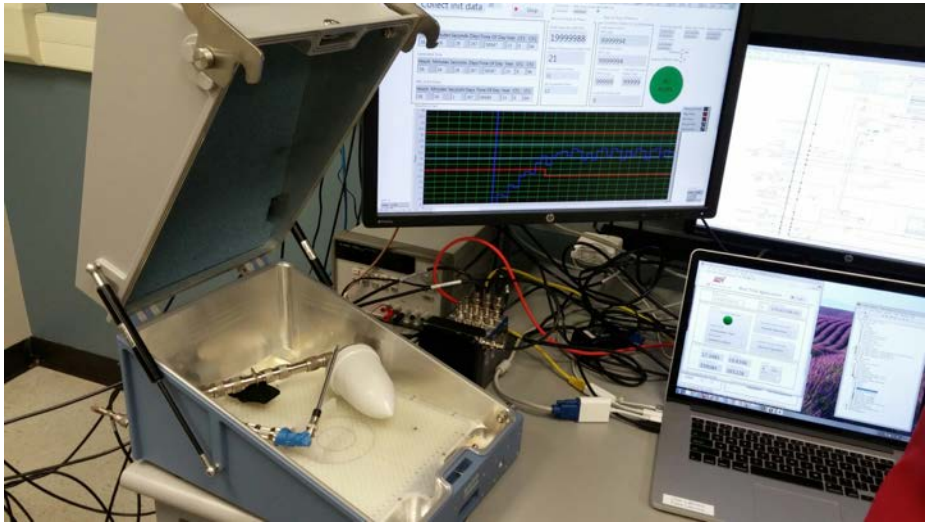


GPS Signal

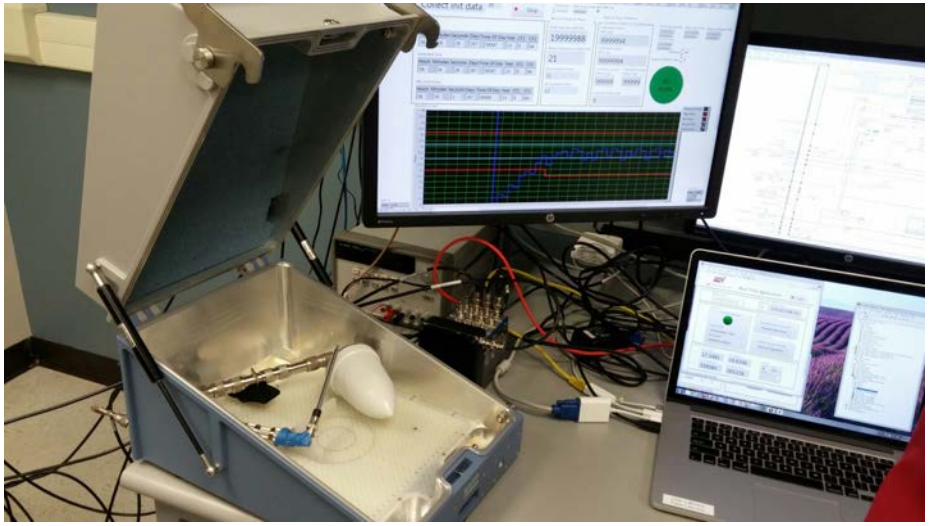
PPS



…some more stuff
…and a little more gear

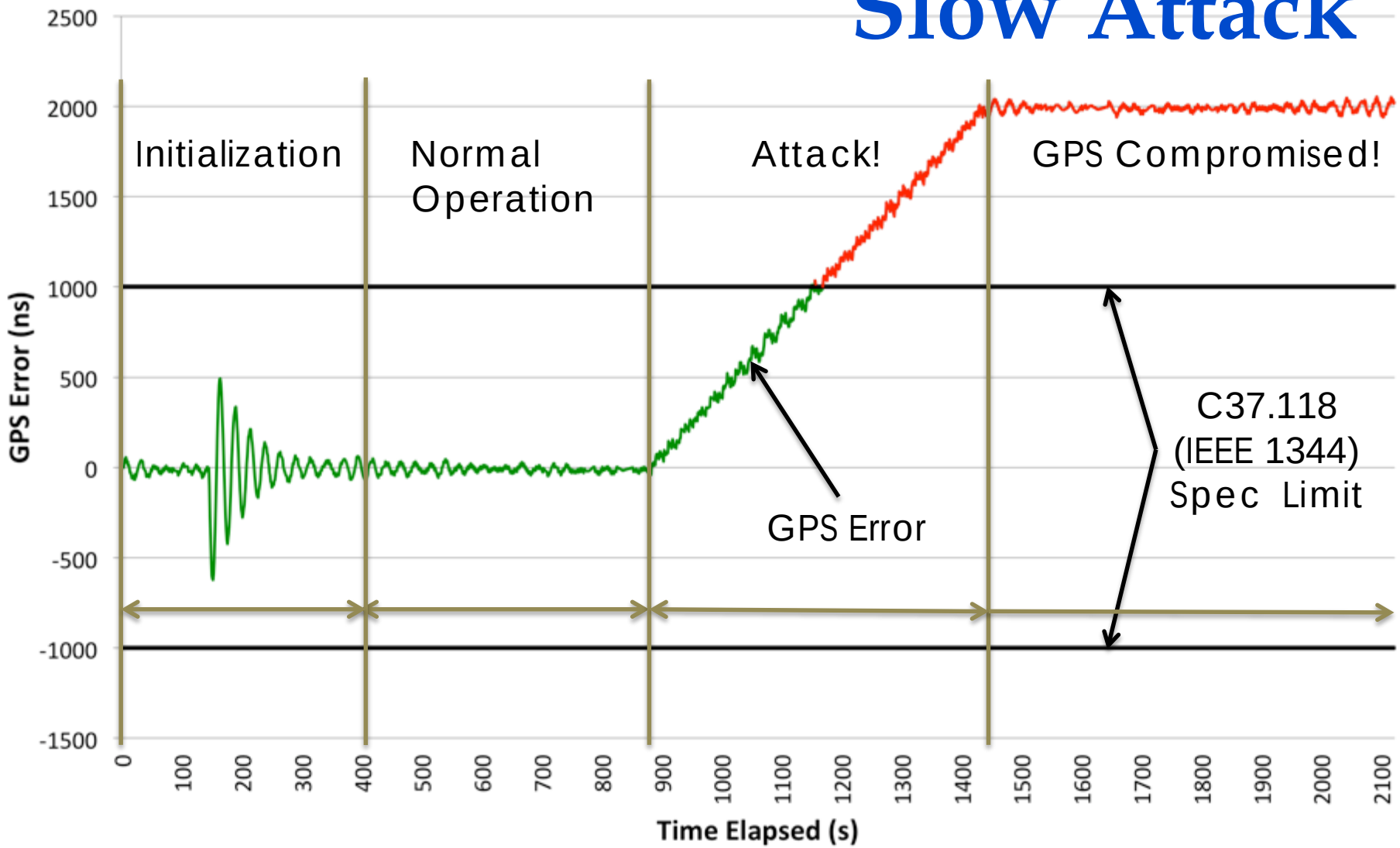


…some more stuff
…and a little more gear

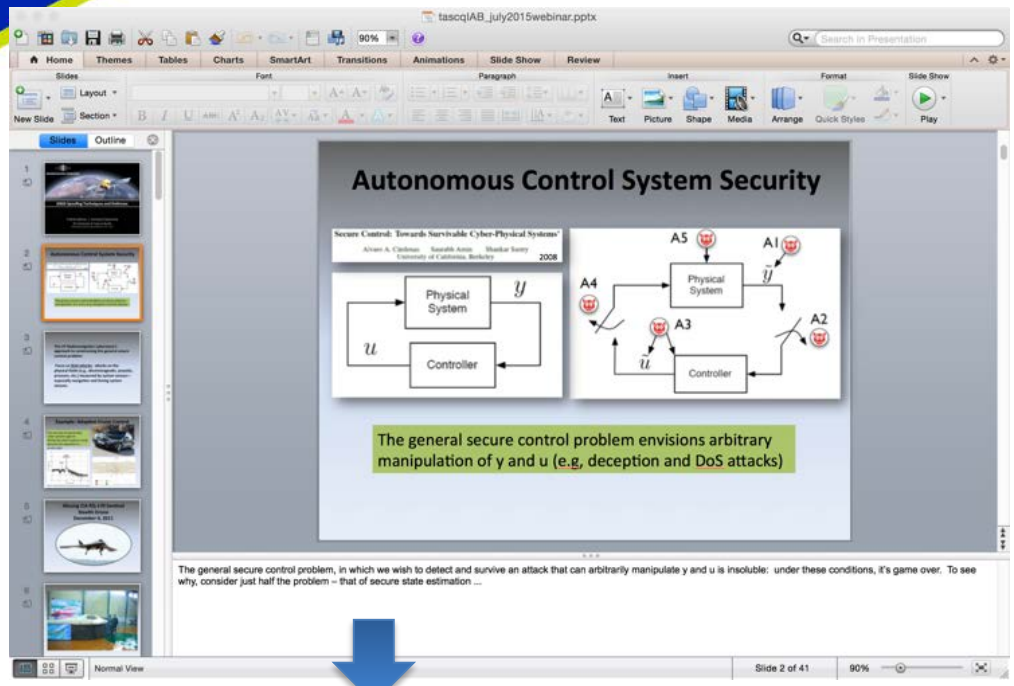


We believe there are <u>no current products</u> that are safe from GPS/GLONASS attacks

Slow Attack


Initialization
Normal Operation
Attack!
GPS Compromised!
GPS Error
C37.118 (IEEE 1344) Spec Limit
GPS Error (ns)
Time Elapsed (s)
2500
2000
1500
1000
500
0
-500
-1000
-1500
0
100
200
300
400
500
600
700
800
900
1000
1100
1200
1300
1400
1500
1600
1700
1800
1900
2000
2100

Others confirm Protecting the RF is not Possible



"The general secure control problem, in which we wish to detect and survive an **attack that can arbitrarily manipulate y and u is insoluble**: under these conditions, it's game over. To see why, consider just half the problem – that of secure state estimation ..." [Humphreys, UT Austin]

Austin]

Even GPS mistakes cause problems

www.itnews.com.au/news/satellite-failure-caused-global-gps-timing-anomaly-414237

teaching | fortran | colorado | cbc | wsn | audio | mac | irigb arduino | SwRI I2Net: Home | pmu | www.swri.org/3pu | Winscope

The security risks of the Internet of Things | Another nationwide outage hits Telstra customers | AusPost locked in digital fight to keep passport business | FBI delays Apple hearing after finding possible way to hack iPhone | ACCC c booking

GOVERNMENT IT | INFOSEC | FINANCE IT | TELCO | Follow Us

eports | Blogs | Topics | CXO Challenge | Whitepapers | What's On

Satellite failure caused global GPS timing anomaly

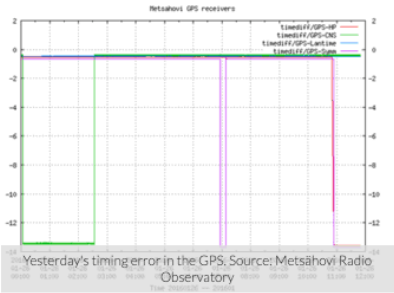
By Juha Saarinen
Jan 28 2016
11:17AM

11 Comments

Created 13 microsecond error.

A time spike in the global positioning system which rippled through the world yesterday was caused by a satellite launched in 1990 failing and triggering a software bug, United States officials have confirmed.

The problem was first noted by Metsähovi Radio Observatory in Finland, where an atomic clock measured a discrepancy in GPS timing of 13 microseconds.



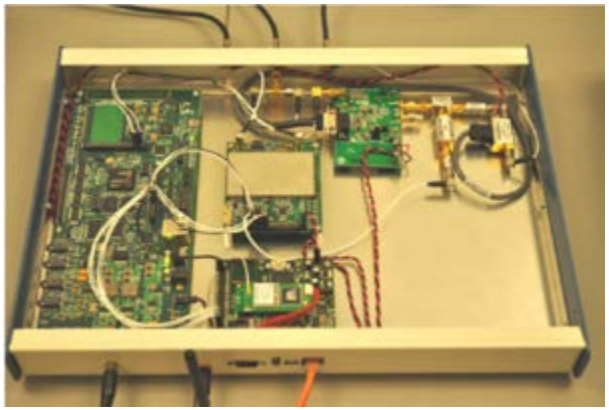
Yesterday's timing error in the GPS. Source: Metsähovi Radio Observatory

- 13 msec GPS signal error
- PMU and Synchrophasors reported errors globally
- 12 hours of disruption

What Does This Mean?

- Jamming/Spoofing GPS/GLONASS is <u>EASY</u>
- GPS is not likely to change
- We want to Protect GPS
  - But,
    - Protecting RF is an **<u>EXPENSIVE</u>** option
    - The RF Attack Surface is **<u>LARGE</u>**
    - Many attacks have not been shown **<u>YET</u>**

[1]



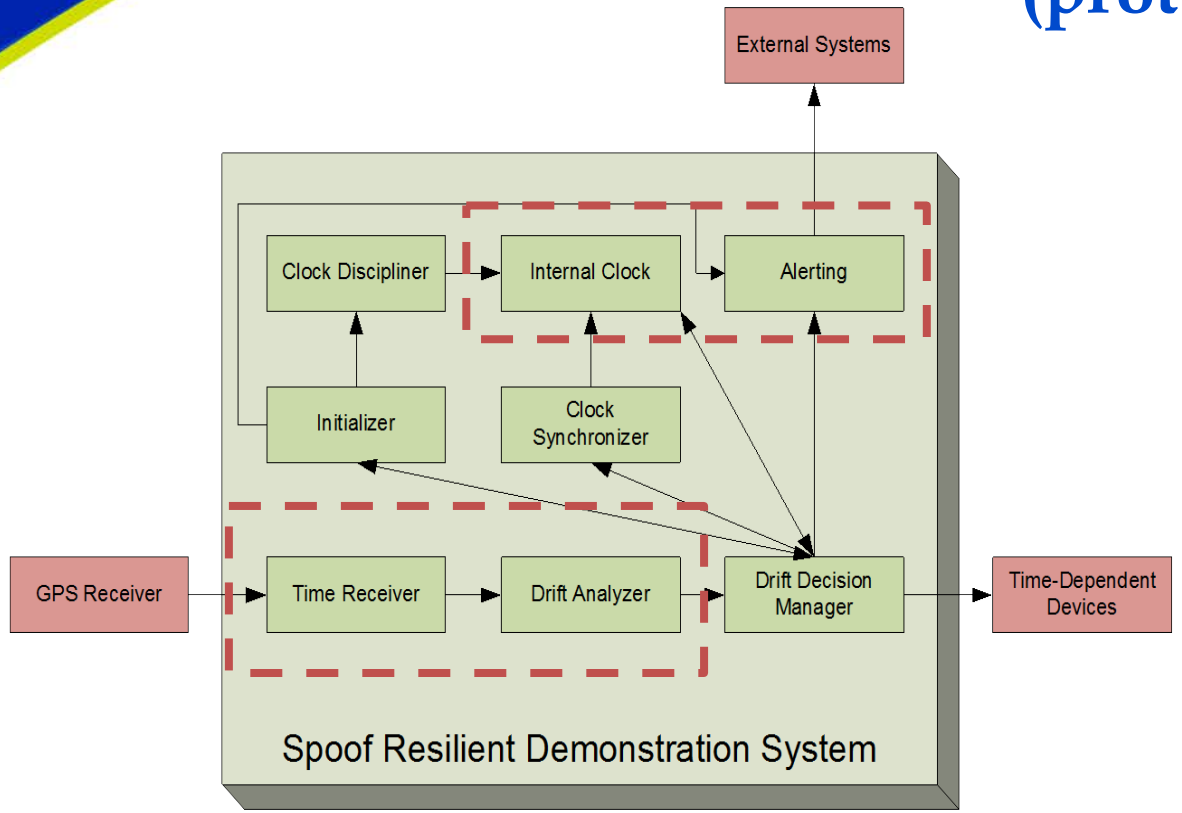
[2]

It is the attacks we don't know about that scare us…

[1] Fox News. http://www.foxnews.com/tech/2013/07/26/exclusive-gps-flaw-could-let-terrorists-hijack-ships-planes/
[2] Shepard et al. "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks"

RF battle is lost →trench warfare

(protect from the inside)



Key Takeaways

- Time can be very important and is very hard to protect
- Which PMU **killer app** will be most susceptible to compromised GPS/GLONASS?

  ➔ the one most vulnerability to incorrect time
- Wrong time may be used to
  - hide a problem that exists
  - to make it look like a problem exists

SwRI
SOUTHWEST RESEARCH INSTITUTE

Thank you!