Smart Grid Use of GPS Time:
Protecting Synchrophasor Timestamps

Kevin M. Skey
Dr. Michael L. Cohen

March 23, 2016

Approved for Public Release; Distribution Unlimited. Case Number 16-0662

MITRE

Bottom Line Up Front

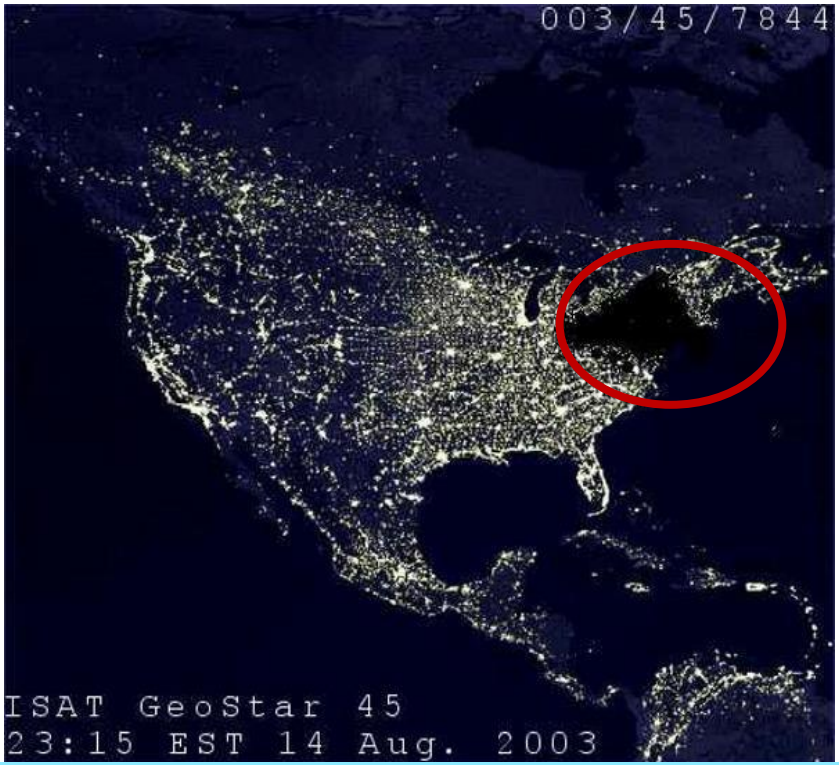
- **Cyber security for Synchrophasor technology is a consideration when integrated into system operations**
  - GPS supplies the time which is used to “time tag” synchrophasor data
- **Cyber attackers look for weaknesses in access points to gain entry into a system**
- **GPS used for Synchrophasor timestamping represents one such access**
- **GPS spoofing has been demonstrated to impact time and should be a security concern**
  - However, readily fieldable protections are available

Approved for Public Release;
Distribution Unlimited. Case Number 16-0662

MITRE

GPS Time in Power Grid Operations
Why should I care?

- **Power Grid has a vital dependence on precise time for:**
  - Time-stamping of operational data (e.g. supervisory control and data acquisition - SCADA)
  - Wide area situational awareness
  - Synchronization of operations
  - Grid management and control
  - System and asset protection



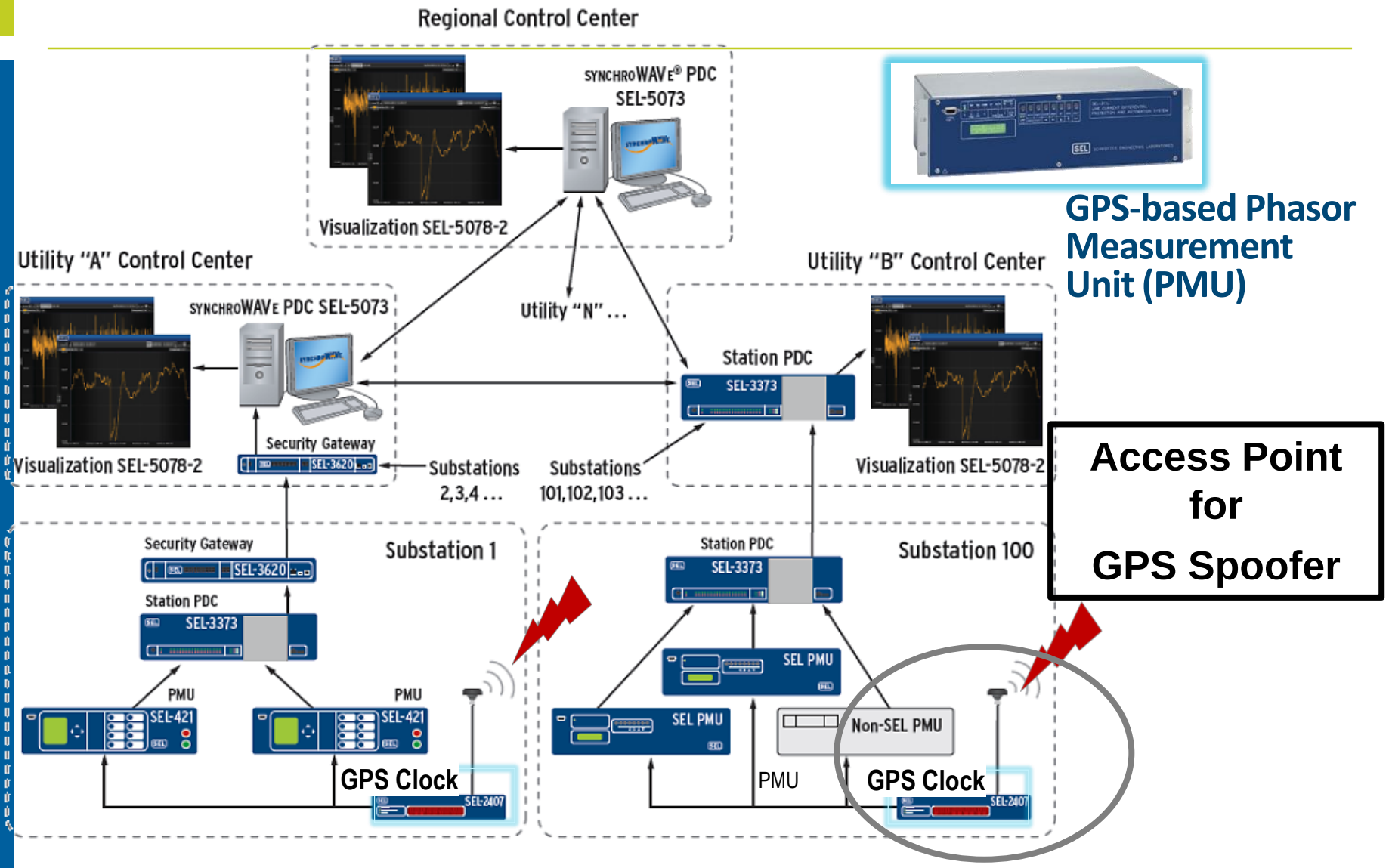
Synchronized time enables the combining of wide area phase measurements to assist in minimizing cascading blackouts and/or restoration

GPS provides the synchronization

MITRE

Phasor Measurement Unit: GPS Time Vulnerability

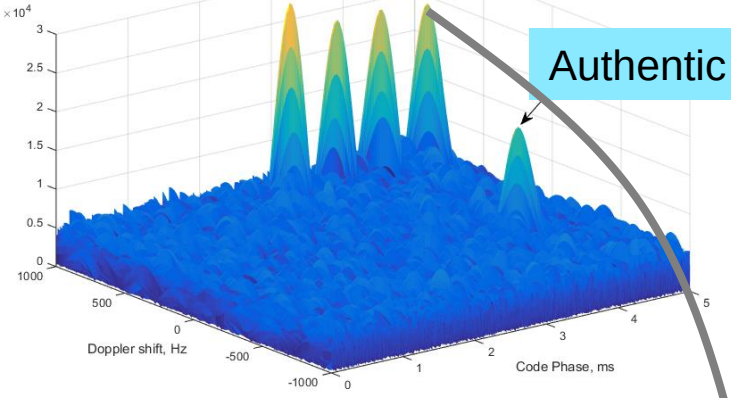
Antenna Provides Access to the System



MITRE

One Method for GPS Spoofer Access

GPS Signal
Rx Acquisition

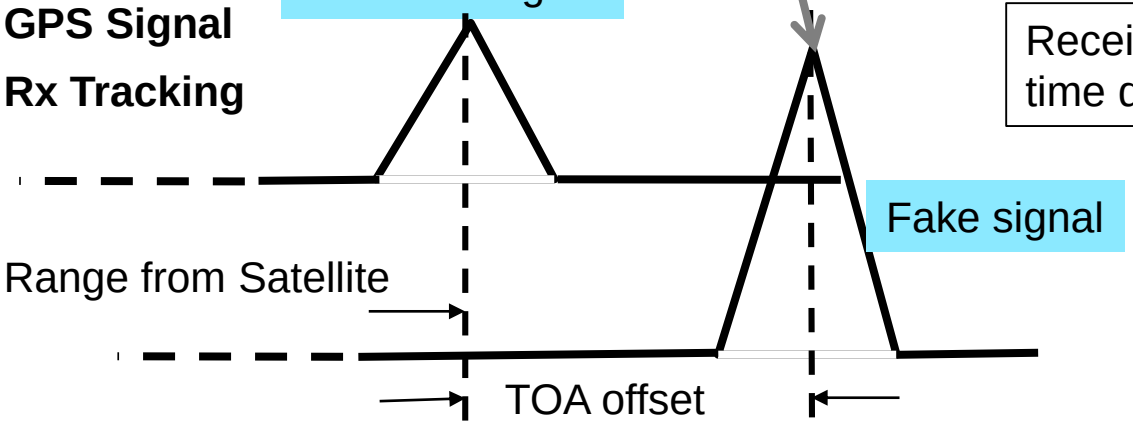


Denies GPS through Jamming
- Forces receiver into acquisition

Transmits “strong” fake signals
- Receivers prefer strong signals and lock

Receiver “hands off” fake signal to track

Receiver calculates incorrect time due to signal offset



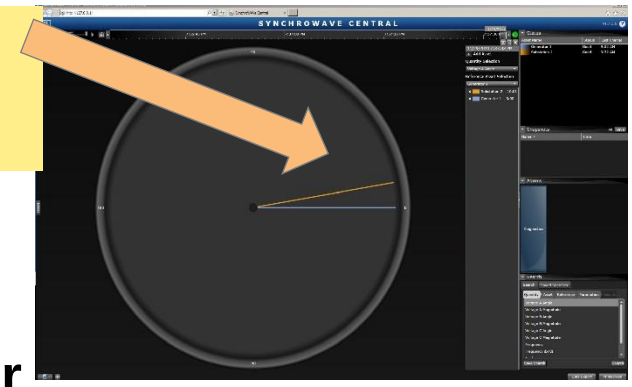
Time-of-Arrival (TOA) offset translates to time error

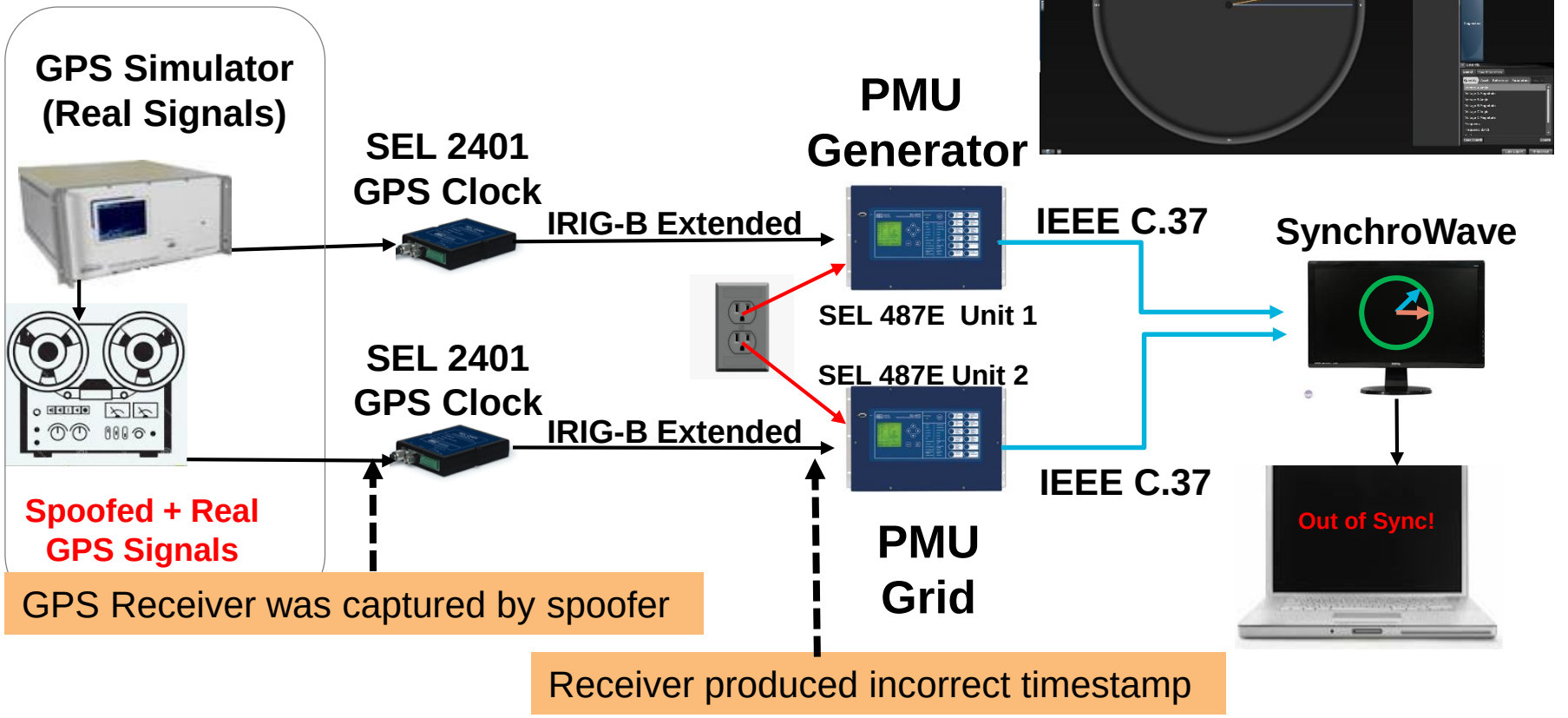
This type of attack can be easily mitigated

MITRE

Synchrophasor Effect from GPS Spoofing Attack

Lab demonstration resulted in the false appearance of an incorrect phase offset





MITRE

Pace of Threat is Increasing

Going Up Against Time: The Power Grid's Vulnerability to GPS Spoofing Attacks

August 1, 2012 - By GPS World

By Daniel P. Shepard, Todd E. Humphreys, and Aaron A. Fansler

Vulnerability exploitation has been demonstrated
- Required sophisticated attacker
- Expert knowledge of GPS

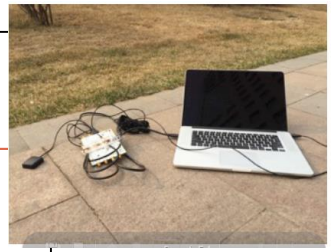
Google search (21 Feb 2016)
- Time Spoofing -> 1,340,000
- GPS Spoofing -> 383,000
- GPS Time Spoofing -> 292,000

However, Spoofing is now common knowledge; Techniques are prolific in open sources

GPS SPOOFING

Low-cost GPS simulator

DEF CON 23



HUANG Lin, YANG Qing
Unicorn Team – Radio and Hardware Security Research
Qihoo 360 Technology Co. Ltd.

We are not navigation experts.
How can we do GPS spoofing?

Low cost open source hardware and software is available;
Cook book approach easing level of entry for attackers

MITRE

Timing Attack Effectiveness

- **Timing attacks have various degrees of effectiveness**
  - Dependency on the built in protections and consistency monitors of a particular GPS receiver and/or integrated timing equipment
- **May require exact location of receiver antenna and satellite transmit signal characteristics**
  - But not difficult for stationary receiver
- **Effectiveness of attack cannot be directly observed**
  - Practice makes perfect
  - More susceptible when the attacker knows your equipment and configuration

Simple mitigations can raise the bar for the attacker

Approved for Public Release;
Distribution Unlimited. Case Number 16-0662

Spoofing Protection Approaches

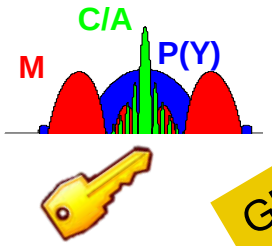
Solution Complexity/Cost/Time to Field

Enterprise System Level: **Service Providers**

*Signal Encryption

*System Augmentation (e.g. GNSS, WiFi, Cellular)

*Authentication

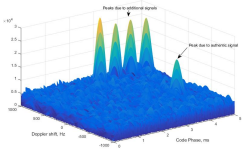


Enhanced receiver processing: **Receiver Manufacturers**

*Signal Measurement

*Inertial technology (IMU)

*RF Power Monitor



Kalman/IMU integrated

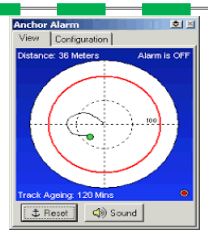
Tracking loop peak detect

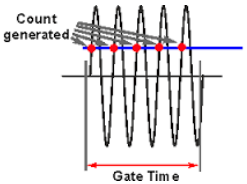
Time/Frequency Peak Detect

Integrated Protections: **Equipment Providers**

*Consistency Checks (e.g. Pos, Vel, Time)

*Oscillator integration





System Integration: **Owner Operators**

*Antennas

*Augmentations

*Better Clocks

Power Detectors

Antennas

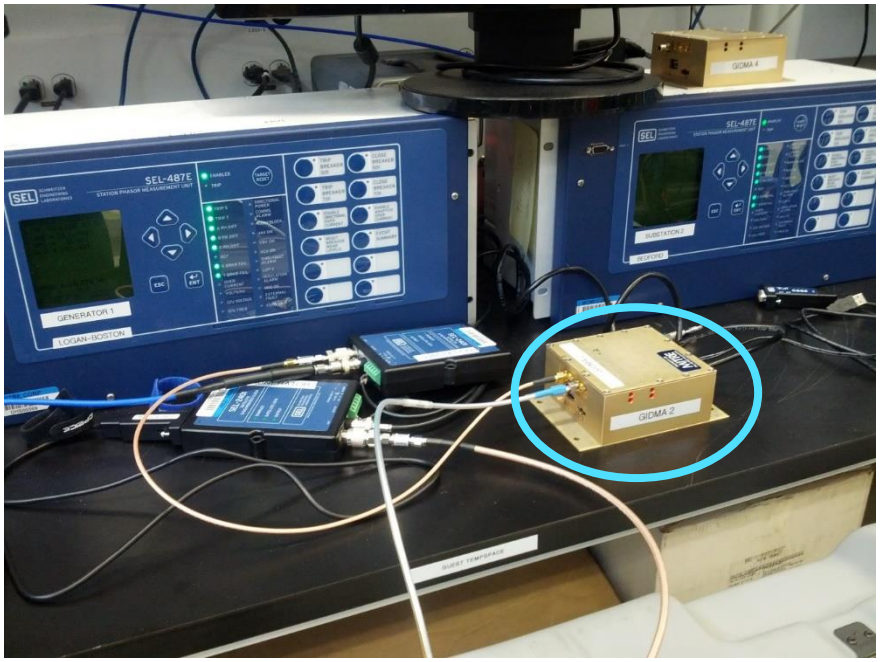
Oscillator-based Clocks

Near-term solutions that can be fielded or added to existing equipment

MITRE

GPS Interference Detection and Mitigation Applique (GIDMA)

- **GIDMA provides a simple inline protection installed between the antenna and GPS C/A code receiver to block some spoofer attacks from access**
- **In most attacks, the GPS Spoofer signal strength is stronger than the real GPS signal**
- **GIDMA is able to detect the increased power then blocks the RF signal from the receiver before it can be accessed**
- **It prevents a false timestamp and "loss of GPS" is indicated**
- **Once the Spoofer attack has ceased, the RF signal is restored**

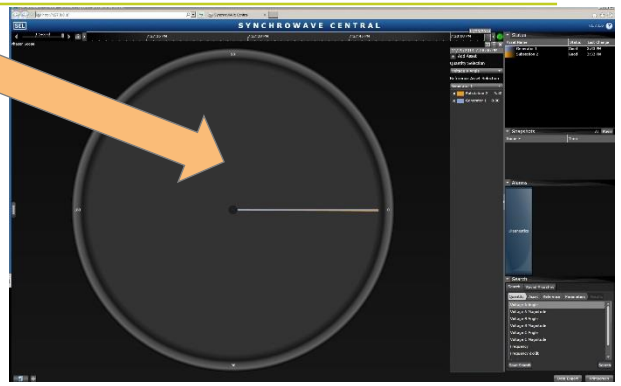


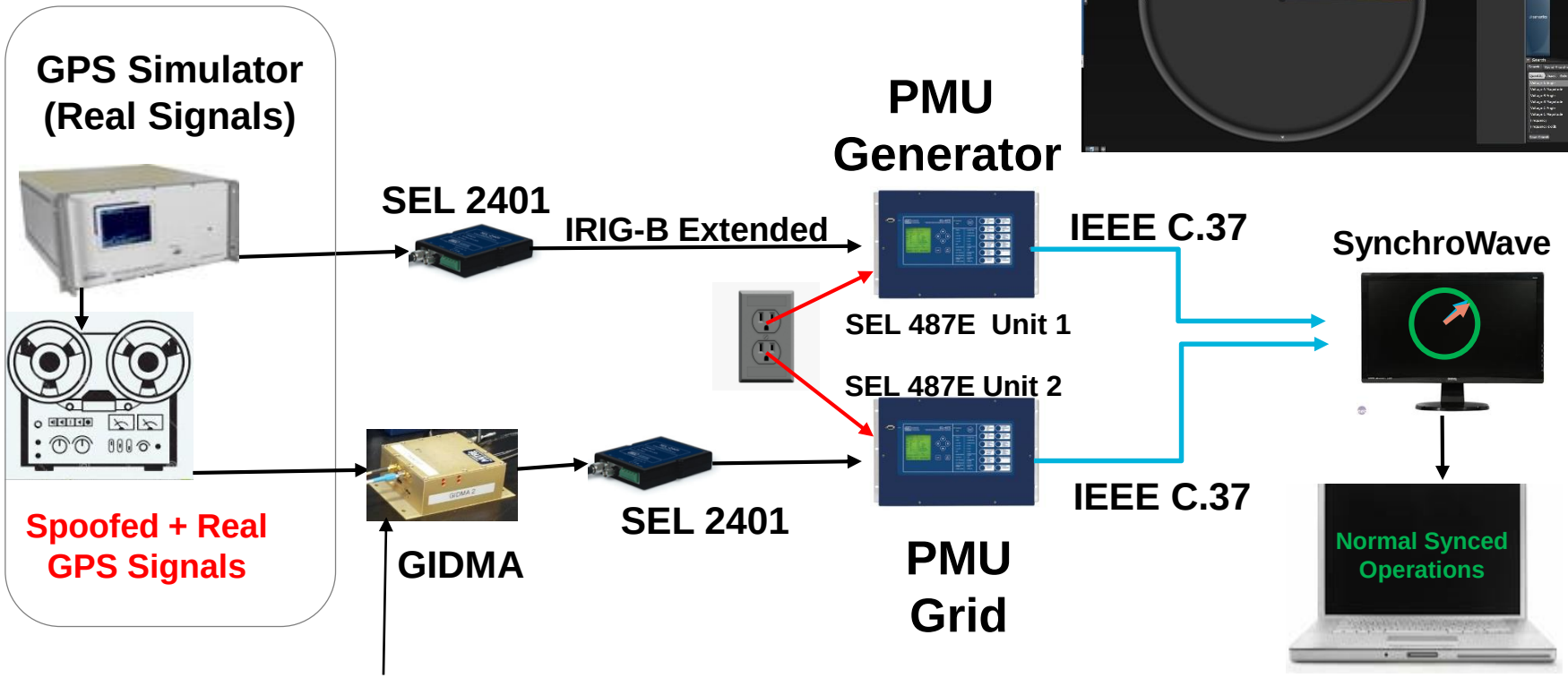
GIDMA Lab Demonstration

MITRE

Synchrophasor Effect from GPS Spoofing Attack…With GIDMA Mitigation

Lab demonstration of GIDMA preventing the spoofer from impacting the phase comparison





Detects GPS Spoofing and blocks fake signal from entering the receiver

Approved for Public Release;
Distribution Unlimited. Case Number 16-0662

MITRE

GPS Time Anomaly: 26 Jan 2016
Time off by 13 microseconds

"Air Force Official Press Release – GPS Ground System Anomaly:

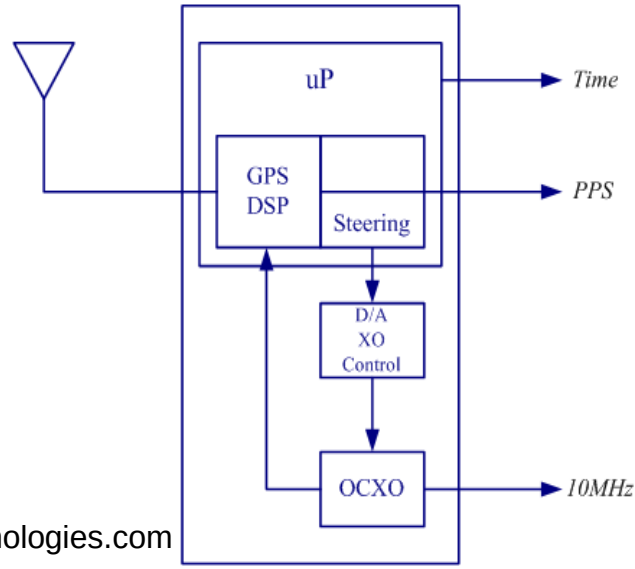
On 26 January [2016] at 12:49 a.m. MST, the 2nd Space Operations Squadron at the 50th Space Wing, Schriever Air Force Base, Colo., verified users were experiencing GPS timing issues. Further investigation revealed an issue in the Global Positioning System ground software which only affected the time on legacy L-band signals. This change occurred when the oldest vehicle, SVN 23, was removed from the constellation. While the core navigation systems were working normally, the coordinated universal time timing signal was off by 13 microseconds which exceeded the design specifications. The issue was resolved at 6:10 a.m. MST, however global users may have experienced GPS timing issues for several hours. U.S. Strategic Command's Commercial Integration Cell, operating out of

GPS system operation issues should also be a concern

Approved for Public Release;
Distribution Unlimited. Case Number 16-0662

Timing equipment with GPS Disciplined Oscillators (GPSDO):
A First Line of Defense to Consider

- **Timing equipment integrated with high quality oscillators with various degrees of stability**
  - GPS syncs (or steers) the Oscillator-based clock rather than directly using time from the GPS Receiver



- **Maintains time through a GPS service outage**

Ocsillator Type	Drift/Day	Hold Over Period
TCXO	10 mSec	24 hours
OCXO	100 uSec	35 days
Rubidium	8 uSec	140 days

Source: http://endruntechnologies.com

- **Possible to measure anomalous divergence between oscillator and GPS clock**
  - Alarm when out of spec
  - Detect spoofing (less sophisticated attacks) or anomalous GPS system behaviors
  - Mitigation behaviors are vendor specific and may require expert knowledge of equipment operation

http://www.nist.gov/pml/div688/grp40/receiverlist.cfm

MITRE

Summary

- **Understanding the robustness of your GPS-based timing solution is important when it's a significant dependency on the system**
- **Some GPS receivers have a demonstrated vulnerability to spoofing that can be propagated into critical down stream Grid operation**
- **Cyber/Security assessment and testing should be performed to understand impacts of incorrect time stamps in PMU data**
- **GIDMA demonstrated one possible and simple GPS protection to increase robustness against spoofing**
- **FFRDCs and government labs continue to develop robust protection practices and technologies for GPS-based applications**

Approved for Public Release;
Distribution Unlimited. Case Number 16-0662

Contact Information

Kevin Skey, MITRE

Senior Principal Engineer

Position, Navigation and Time (PNT) Technologies

781-271-3390

skey@mitre.org

MITRE