PMU Time Source Security

Erich Heine
<eheine@illinois.edu>
Information Trust Institute

Authors:
Erich Heine, Tim Yardley,
Dr. Alejandro Dominguez-Garcia, Daniel Chen

ILLINOIS
DARTMOUTH
UC DAVIS
WASHINGTON STATE UNIVERSITY

Overview

- PMU time synchronization and it’s vulnerabilities
- TCIPG work in:
  - GPS spoofing
  - Bad Data Detection for PMU Measurements
  - Testbed tools for understanding time attacks
- Future directions and concerns on this topic

Background: PMU Synchronized Data

- PMUs report data at time t_0
- Data delivered to dependent systems
  - PMUs send data via IP network to PDC
  - PDC sends collated (time aligned) data to other systems
- Time synchronized data used in:
  - Wide Area Monitoring Systems
  - System Visualization
  - Enhanced State Estimation
  - Event analysis

Time Synchronization Considerations

- Data delivery over IP networks takes a non-deterministic amount of time
  - Time alignment must happen somewhere (usually PDC)
  - Necessitates a data arrival window (t_w)
  - Late data is dropped or only used in historical contexts (e.g. post event analysis)
- Clock accuracy considerations
  - Real world means tolerances, in the case of PMUs +/- 1us
  - Synchronized accurate clocks are expensive so use a common external source

Background: Consequences Inaccurate Time

- A PMU reports data based on its understanding of the time
- Inaccurate time on a single PMU will result in:
  - Incorrect point on wave values
  - Incorrect computed relationships between point in the system
  - Data discrepancies which are difficult to trace
- Broader consequences can include:
  - False alarms to operators
  - Incorrect control actions
  - Slower event response times

Attack Surface Analysis

- Can a time source be compromised? Yes:
  - GPS spoofing
  - Network attacks spoofing or breaking time daemons
- What constraints does a time attack have? (How much can my clock be offset without detection via side-effect?)
  - Maximum window defined by:

    $$(t_0 + t_w) - t_d$$

    (t_d is the time it takes most packets to transit PMU->PDC)
  - Time must not offset reported values past target system sanity check thresholds.

Attack Surface Analysis Cont.’d

- What protections already exist?
  - Most time protocols have provisions for sudden time changes (PMUs may or may not report this)
  - Some spoofing may be catchable with advanced error correction in receivers
  - Advanced network monitoring may catch packets from a PMU being consistently late as an odd network latency

- Overall assessment: potentially exploitable vulnerabilities exist.

TCIPG Work to Address This

- Overview of TCIPG work on Time Source Security
- GPS spoofing
- Bad Data Detection for PMU Measurements
- Testbed tools for studying and understanding Time Source Security
- Work with industry towards a more resilient time-synchronization framework.

GPS Spoofing

- Researchers
  - Dr. Alejandro Dominguez-Garcia
  - Xichen Jiang
  - Brian Harding
  - Dr. Jonathan Makela

- Summary:
  It is possible to spoof GPS signals such that receivers report a nearly correct position but incorrect time.

GPS Spoofing Cont.'d

- How GPS works:
  - Receiver monitors signals broadcast from n >= 4 satellites
  - Signals contain:
    - Time information
    - Satellite location and motion information (known as: ephemerides)
  - Receivers compute time and location:
    - Comparing satellite location and transmission time against an internal reference clock
    - Iterating over the n signals to account for reference clock biases and errors

GPS Spoofing Cont.'d

- The attack:
  - Broadcast a GPS signal from a spoofing device
    - Gradually overpower GPS signals
    - Receiver locks to spoofed signal rather than the satellite being spoofed
  - Signal modifications
    - Changes to ephemerides
      - Must be within a defined range
      - Must result in receiver calculated location within a bound
      - Chosen to maximize offset used to correct for receiver reference clock bias.

GPS Spoofing cont'd

- Experiments
  - Attack simulated in Matlab
  - Small ephemerides change bounds to prevent detection*
  - 15m bound on computed location.

- Results:
  - Able to achieve a maximum 52° phase shift in a particular PMU with 4 satellites visible, ephemerides bound to within 2% of original values, and receiver computing a location within 15m of previously computed location.

GPS spoofing countermeasures and mitigation

- Receivers instrumented to handle sudden changes to ephemerides data
- Multiple antenna setups to verify signal angle of arrival
- Comparison of ephemerides data against external source (e.g. the internet)
- Extra signal processing to search for the original signal as well as the spoofed signal.

GPS Spoofing related and future work

- TCIPG researchers implementing spoofing algorithm using a commercial GPS spoofing device for testing real receivers

- UT-Austin researchers have been testing GPS receivers and PMUs against various GPS spoofing attacks

Bad Data Detection for PMU Measurements

- Researchers
  - Daniel Chen
  - Jiangmeng Zhang
  - Dr. Zbigniew Kalbarczyk

- Summary
  Using data available from SCADA systems and other PMUs, straightforward detection of bad angles from PMUs is demonstrable.

Bad Data Detection for PMU Measurements cont.'d

- Problem description
  - A PMU is reporting an incorrect (bad) angle, potentially as a result from a time source attack
  - SCADA measurements not affected
  - Assume time source attacks can only be carried out against a subset of measurements
    - Targeted GPS spoofing
    - Time server for a single substation or utility

Bad Data Detection for PMU Measurements Cont.'d

- Approach
  - Use available redundant data from
    - Other PMUs
    - SCADA system
  - Use traditional state estimation to provide a baseline estimated angle
  - Use the baseline and gathered measurements in a chi-squared test to determine bad or potentially bad data points

Bad Data Detection for PMU Measurements Cont.'d

- Experimental Setup in TCIPG testbed
  - RTDS simulation
    - Provided SCADA values
    - Drove PMUs
  - Inline angle data modifier
    - Custom adaptor for OpenPDC to modify one PMU's reported angle as in a time source attack
  - Implementation of State-estimation and Chi-squared detection algorithm

Bad Data Detection for PMU Measurements Cont.'d

- Results
  - Able to detect bad measurement and identify offending PMU
  - Use of the testbed helped rapidly iterate algorithm improvements, find bugs, etc.
  - Hardware in the loop allows us to extend this form of experimentation to real devices experiencing real spoofing (future work)

Testbed Tools for Time Source Security

- Researchers
  - Erich Heine
  - Nathan Edwards
  - Jeremy Jones
  - Tim Yardley
  - Dr. Alejandro Dominguez-Garcia

- Summary
  Direct testing the effects of time source spoofing can cause problems so create tools and devices to emulate it.

Testbed Tools for Time Source Security

- Overview
  - Direct GPS spoofing outside of an isolated room is can affect legitimate devices and cause problems
  - Fully emulated or isolated time source environments are expensive and difficult to properly calibrate
  - Emulated or simulated PMU streams don't allow for device testing or easy verification

Testbed Tools for Time Source Security

- Approach
  - Create devices and software to modify legitimate inputs to real time sources.
  - Focus on techniques that modify signals on wires rather than broadcast radio signals
  - Flexible use tools for broad range of experimental setup and reusability

Testbed Tools for Time Source Security

- Example: GPS spoofing
  - Uses a relatively inexpensive GPS signal spoofer
  - Output feeds directly into antenna feed of GPS clock
  - Implements the GPS spoofing work outlined above
  - Multiple GPS clocks in the TCIPG lab allow for some spoofed some un-spoofed signals.

Testbed Tools for Time Source Security

- Example: IRIG-B signal delay
  - IRIG-B is a simple 1KHz amplitude modulated digital signal.
  - Time synch comes from PPS over phase locked loop
  - Signal from clock delayed by a series of op-amp phase shifters
  - Delay controllable by interfacing a computer to the board and digital potentiometers.

Future Directions for TCIPG

- Detection of time source attacks
- Further testbed integration of tools
- Investigation of secure time source techniques
- Integrate research to improve time synchronization for a more resilient power grid.

Questions?