LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-830476

Best Practices for Timing Attack Mitigation

C. J. Applegate, A. C. Campbell

January 4, 2022

Disclaimer

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

Best Practices for Timing Attack Mitigation

Homeland Security

Science and Technology

This report was prepared by Lawrence Livermore National Laboratory in collaboration with the Electric Power Research Institute for the U.S. Department of Homeland Security, Science and Technology Directorate. This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. LLNL-TR-830476

POINT OF CONTACT

Lawrence Livermore National Laboratory
P.O. Box 808, Livermore, CA 94551-0808

Authors:

Chloe Applegate, Deputy Associate Program Leader for Cyber Systems Analysis

Alex Campbell, Analyst

TABLE OF CONTENTS

INTRODUCTION

GPS signals play essential roles in the electric subsector by providing precision timing used to synchronize and record measurements from a range of equipment. However, previous research has demonstrated that GPS signals can be spoofed or jammed relatively easily in order to interfere with timing-reliant equipment.

This document outlines utility best practices for mitigating against timing attacks in the electric subsector based on an assessment of the difficulty and impact of realistic timing attacks and testing of the effectiveness of technologies capable of mitigating them. This analysis builds on research establishing the vulnerability of GPS-reliant timing equipment to jamming and spoofing by elaborating the difficulty, consequences, and mitigations for timing attacks that adversaries might realistically attempt. While timing attacks are relatively low-cost, low-sophistication, and capable of systemic consequences in the electric subsector, they can be effectively mitigated through well-targeted and diverse mitigations.[1]

Based on results from mitigation testing, development of attack scenarios for precision timing manipulation, an analysis of critical points of failure for a representative grid model, and software assurance testing, this report describes the following recommendations for utility best practices to protect against and mitigate potential GPS timing attacks.

RECOMMENDATIONS

- Catalog precision timing equipment
  - Maintain accurate, up-to-date inventory of what systems rely on timing, what timing acquisition components are used, and what mitigation solutions are in place
  - Prioritize mitigations at high-risk locations, where disruption could have outsized effects, and at legacy equipment that lacks hardening
- Practice defense-in-depth
  - No one mitigation solution is comprehensive: layer defenses to combine different detection, alert, and remediation capabilities against different spoofing attacks
  - In addition to mitigations, practice redundancy in failover and alarm systems
- Tailor mitigations to a network's configuration and risk
  - Mitigation technologies can be prioritized based on threat, risk acceptance, cost, and other related elements
- Include timing attacks in planning
  - Incorporate timing attacks into cybersecurity planning: develop and practice incident response plans for timing attacks
  - Evaluate timing attack vectors during procurement, and when integrating timing across new networks like 5G and private long-term evolution (LTE)

[1] For more, see DHS Resilient PNT Conformance Framework: https://www.dhs.gov/publication/st-resilient-pnt-conformance-framework

APPENDIX A. METHODOLOGY AND FINDINGS

The utility best practices recommendations were derived from testing and analysis led by Lawrence Livermore National Laboratory (LLNL) in collaboration with the Electric Power Research Institute (EPRI). Testing and analysis included (1) mitigation testing, (2) critical failure analysis, and (3) attack scenario development. A brief description of each of these efforts is outlined below.

Mitigation Testing

As part of this effort, a diverse range of commercial mitigation solutions for GPS timing attacks was tested, simulating jamming and a range of spoofing attacks. These tests were intended to test the ability of mitigation technologies to detect, respond to, and recover from jamming and spoofing attacks.

Results: The mitigation technologies had varying levels of success across different attack types. While all were able to maintain synchronization during attacks, some did not reliably detect or alert. Based on the depth of understanding a utility has of their network, there could be multiple pathways to securing networks against timing attacks. For utilities limited in full network knowledge or risk characterization or limited in resources, a defense-in-depth approach to security systems would be recommended. For utilities with ample resources to tailor approaches based on network configuration or relevant risks, a tailored approach matching mitigation technologies to the relevant threat, risk acceptance, and other related factors should be considered.

Critical Failure Analysis

LLNL leveraged a critical failure analysis tool, Squirrel, to identify network manipulations that could lead to a specific critical failure in networks based on a consequence of interest. The analysis considered low voltage conditions as the consequence of interest, and primary indicator of a successful spoofing attack. The underlying rationale for the selected consequence of interest was the assumption that a planned attack would seek to maximize end user inconvenience, which can reasonably be accomplished via low system voltages and the potential for load loss via under-voltage load shedding (UVLS). As such, the consequence of interest was determined to be a condition where either bus voltages in the monitored area fall below 90% of nominal, or situations where the simulator did not converge (DNC), in the synthetic models. 90% of nominal voltage was chosen to reflect a transmission planning requirement pursuant to North American Electric Reliability Corporation (NERC) TPL-001-4.

Results: Timing attacks that disrupt up to 10 co-located transmission lines could lead to regional load loss. However, hardening less than 5% of lines in a synthetic transmission network model could eliminate almost all failures observed in the network. A crown jewel analysis of the network identifies lines and components that are involved in most PNT-type attacks; thus, it is recommended that mitigation technologies are placed at prioritized, high-risk locations.

Scenario Development

Five representative scenarios were developed based on attack mechanisms theorized in open literature, providing a starting point for assessing the difficulty of PNT attacks against electric

grid infrastructure. Each scenario was broken down into component steps and assigned a comprehensive difficulty score using LLNL's Quantitative Intelligent Adversary Risk Assessment (QIARA) difficulty scoring framework.

The scenarios included:

1. Out-of-sync PMU triggers differential relay
2. Vulnerability in GPS receiver firmware exploited to disrupt WAMPAC system
3. Insider-enabled attack on FACTS compensator
4. GPS time spoofing of DLR data during heatwave
5. Simultaneous pinpoint spoofing at generators

Results: The analysis showed that timing attacks can be accomplished with little training, specialized equipment, or non-public information. However, the most impactful timing attacks generally required physical or cyber components that are vulnerable to the same mitigations defined in critical infrastructure security protocols such as the North American Electric Reliability Corporation's Critical Infrastructure Protection standards (NERC CIP). This analysis demonstrates that timing attacks merit concern, and should be integrated into existing planning for cyber and physical security.