A Process for Assessing the Security of Synchrophasor Intelligent Electronic Devices

Tommy Morris, PhD
Director, Critical Infrastructure Protection Center
Assistant Professor
Mississippi State University

Topics

- Experiences from a DOE ARRA smart grid investment grant project.
  - Project background
  - Cyber security requirements development
  - Device testing
  - IEEE C37.118 Intrusion Detection System (IDS) Framework

Project Details

- Western Interconnection Synchrophasor Program (WISP)
  - $107.8 million
  - Install 250-300 PMU
  - 2 Regional PDC to share data across the interconnection
  - to “identify and analyze system vulnerabilities in real time, as well as detect evolving disturbances on the Western bulk electric system.”

PMU
PMU
PDC
PMU
EMS
PDC
PMU
Historian
Eng'g Analysis
PDC
PMU
Transmission Line
Network

Cybersecurity Requirements Development

- Need requirements *traceable to industry standards* and recommendations.
- Cyber security requirements from
  - NISTIR 7628: Guidelines for Smart Grid Cyber Security (28)
  - Department of Homeland Security: Cyber Security Procurement Language for Control Systems August 2008
  - Utility requirements.

– Strategic partner meetings to derive requirements and develop conformance plan.

- Assumed PMU & PDC eventually NERC CIP Critical Cyber Assets (CCA).

28 NISTIR 7628 Requirements

Requirement ID	Title
SG.AC-4	Access Enforcement
SG.AC-7	Least Privilege
SG.AC-8	Unsuccessful Login Attempts
SG.AC-9	Smart Grid Information System Use Notification
SG.AC-10	Previous Logon Notification
SG.AC-12	Session Lock
SG.AC-21	Passwords
SG.AU-2	Auditable Events
SG.AU-3	Content of Audit Records
SG.AU-8	Time Stamps
SG.AU-9	Protection of Audit Information
SG.AU-10	Audit Record Retention
SG.AU-16	Non-Repudiation
SG.CP-10	Smart Grid Information System Recovery and Reconstitution

Requirement ID	Title
SG.CP-11	Fail-Safe Response
SG.IA-5	Device Identification and Authentication
SG.SC-3	Security Function Isolation
SG.SC-5	Denial-of-Service Protection
SG.SC-7	Boundary Protection
SG.SC-8	Communication Integrity
SG.SC-9	Communication Confidentiality
SG.SC-10	Trusted Path
SG.SC-12	Use of Validated Cryptography
SG.SC-19	Security Roles
SG.SC-20	Message Authenticity
SG.SC-22	Fail in Known State
SG.SC-26	Confidentiality of Information at Rest
SG.SC-29	Application Partitioning

23 DHS Procurement Language Requirements

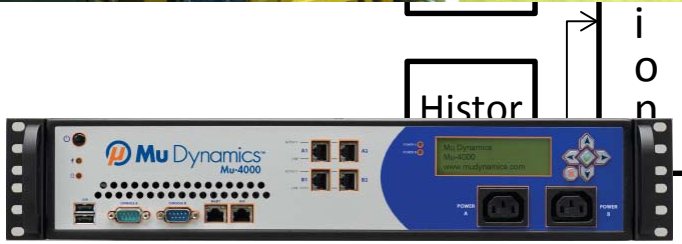
Req ID	Title
PROC.1	System Hardening 1
PROC.2	Changes to File System and Operating System Permissions
PROC.3	Hardware Configuration
PROC.4	Upgrade Access Control
PROC.5	Installing Operating Systems, Applications, and Third-Party Software Updates
PROC.6	Perimeter Protection
PROC.7	Session Management
PROC.8	Concurrent Logins
PROC.9	Account Logout and Timeout
PROC.10	Warning Banner
PROC.11	Least Privilege

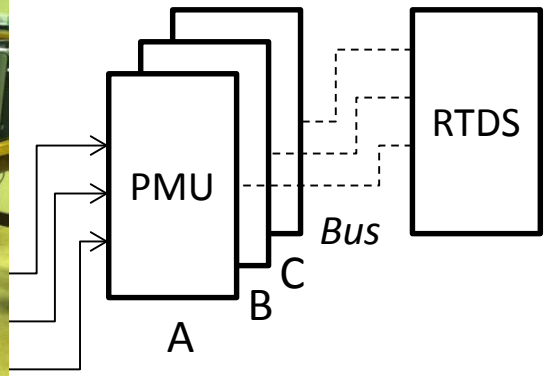
Req ID	Title
PROC.11	Least Privilege
PROC.12	Configurable Password Complexity
PROC.13	Password storage
PROC.14	Security Rollback During Emergency System Recovery
PROC.15	Password Encryption Algorithm
PROC.16	Password Complexity
PROC.17	Activity Logging
PROC.18	Audit Log Time Stamping and Encryption
PROC.19	Audit Log Impact on System Performance
PROC.20	Audit Log Entry Contents
PROC.21	User Accounts with Defined Role
PROC.22	TCP/IP Cybersecurity Features
PROC.23	Approved Cryptographic Algorithms

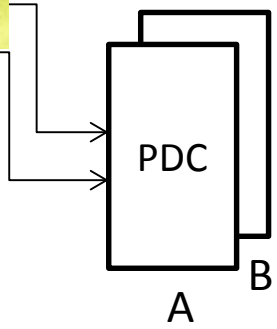
Testing Overview

- Device cyber security capability assessment
  - Identify cyber security features
  - Identify cyber security gaps
- Denial of service
  - Flooding attacks
  - Protocol Mutation (aka. Fuzzing)
- Other testing
  - Password confidentiality
  - Man-in-the-middle
  - Source code analysis
  - Confirmed security feature functionality
    - event logging, password requirements, settings persistence, etc.
  - Port scan - NMAP
  - Vulnerability scan - OpenVAS

Testbed





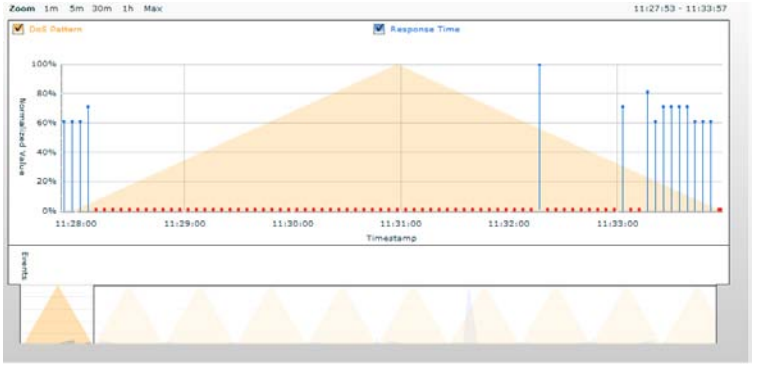


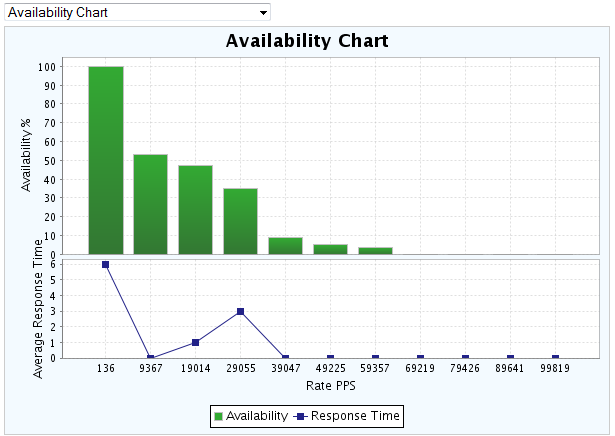
Histor

i o n r

Denial of Service (DOS)

- Well known DOS vulnerabilities.
  - LAND, Tear drop, Ping of death, etc.
- Flooding
  - High network traffic volume
- Protocol Mutation
  - ICMP, DNP3, UDP, TCP, MODBUS/TCP, HTTP, ARP, IEEE C37.118, and more

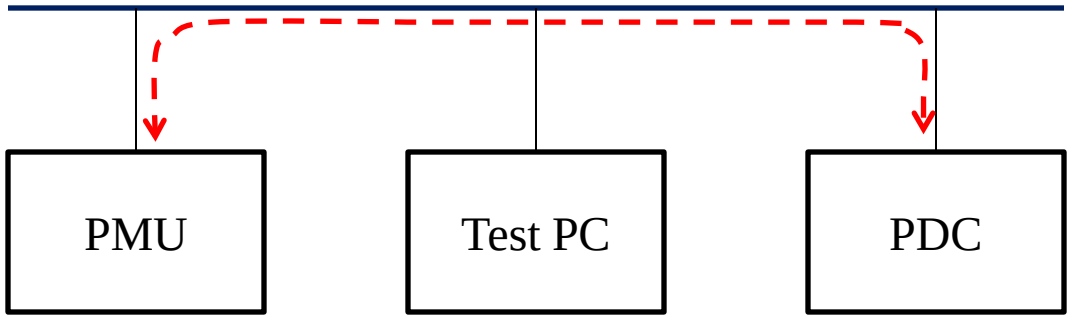




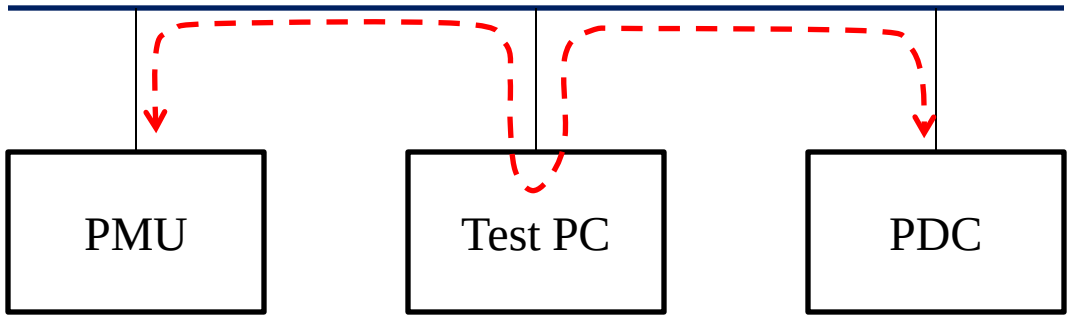
Protocol Mutation

- Break protocol rules to test device response.
- Attempt to predict future attacks.
- Two types of fuzzing.
  - Dumb fuzzing
  - Smart fuzzing
    - Used for IEEE C37.118 and MODBUS

Dumb Fuzzing



Normal PMU/PDC Communication



Test Arrangement

Test PC = EtterCap (man-in-the-middle client) +
Python fuzzing framework

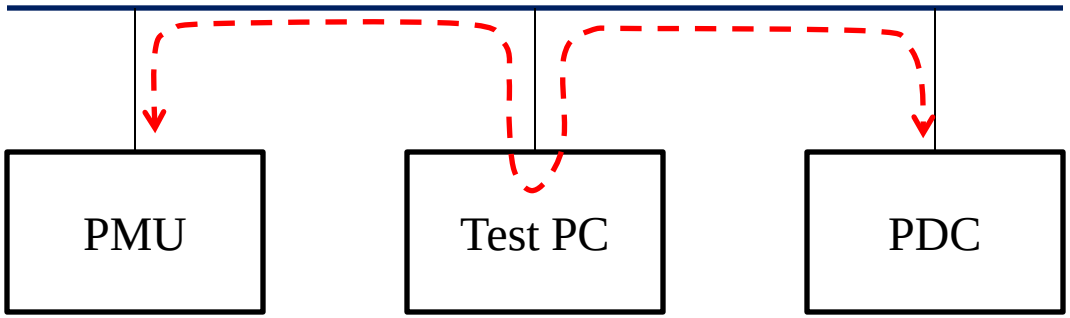
Dumb Fuzzing:

1. Capture IEEE C37.118 or MODBUS frame
2. Flip 1-10% of bits at random
3. Recalculate CRC
4. Forward frame to destination

Dumb Fuzzing

- Effectiveness
  - bits flipped at random can cause problems for network stack, OS, and applications using the tested network service.
  - Crash network stack, application, unwanted reboot of device under test (DUT)
  - identify vulnerabilities early and report to vendor
- Open questions
  - When have you flip enough bits?
    - Every bit flipped once? more times?

Smart Fuzzing



Test Arrangement

- Intelligently alter packets on test PC to achieve desired results.
- PMU transmits FR
- PDC receives T(FR) (T= transpose)
- vice versa

Smart Fuzzing Examples

- Alter config frame sent from PMU → PDC
  - change expected contents
    - number of phasors, types of phasors, polar vs. rectangular, etc.
- Alter data frame from PMU → PDC
  - change length field to not match packet length (too long, too short)
  - change payload contents
    - zero payloads, change time stamps, etc.
- Command and header frames also altered

Smart Fuzzing Advantages/Disadvantages

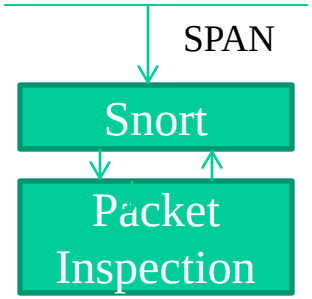
- Advantages
  - Deliberate testing leads to measureable functional test coverage
  - Easier to judge what testing has been done
- Disadvantages
  - Required domain expertise to develop a test plan

Synchrophasor Standards

- IEC 61850 90-5
  - Transport IEEE C37.118 frames
  - Add security features
    - Key management, key distribution
    - Crypto: identity establishment, authentication, encryption
- We have not tested this standard.

IEEE C37.118 Signature Based Intrusion Detection System (IDS)

- Real time IEEE C37.118 frame inspection
- Plug and play
  - add C37.118 devices on the fly
  - preprocessor detects PMU config packets
  - configures rules automatically
- Prototype
  - Currently limited to rules which inspect frame for protocol conformance
  - We have developed application specific rules for a MODBUS system



Snort

-Pass frames to packet inspection layer

-Receive alerts from packet inspection layer

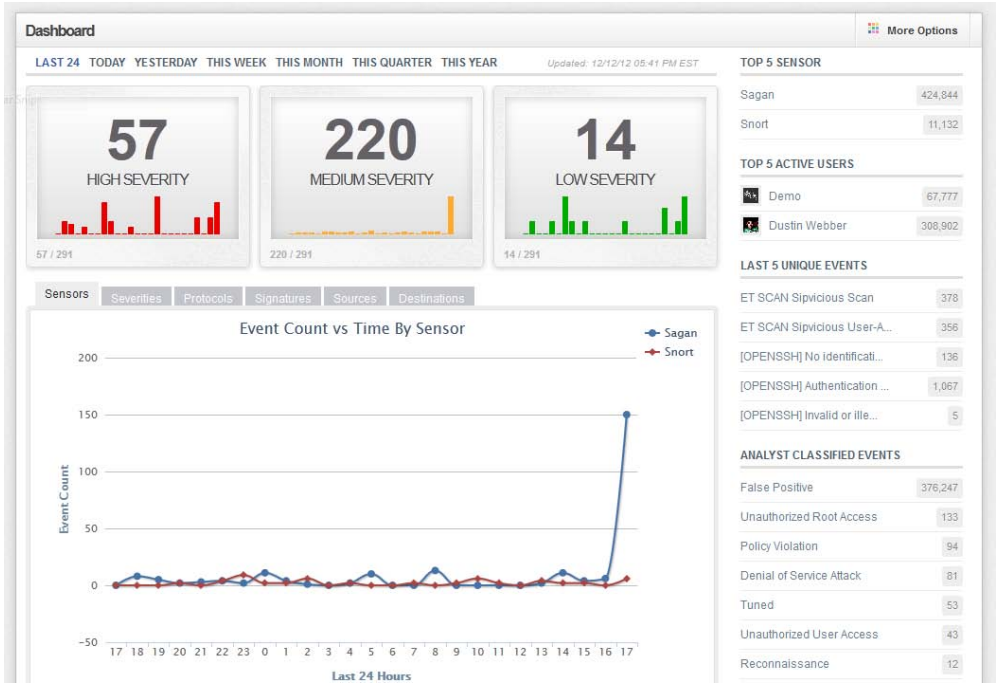
-Interface to syslog/Snorby

Packet Inspection Layer

-State based

-Deep packet inspection

-System model



Snorby GUI

PDC

SPAN

IDS

PMU

PMU

PMU

Conclusions

- Utility, vendors, and project partners successfully worked together to
  - Develop cyber security requirements for a large ARRA synchrophasor project.
  - Testing performed.
    - Vulnerabilities identified, shared with utility and vendors.
    - Risk scores assigned.
  - Vulnerabilities addressed
    - Firmware updates
    - New security features
    - System architecture changes
  - IDS Framework developed