



# Synchrophasor Security Fabric Testing

Dr. Phongphun Kijsanayothin and Dr. Rattikorn Hewett

Shad Holt, P.E.

supporting the initial hardware install and connection to PMU network



# Project Objective



To demonstrate the use of the **Security Fabric (SF)** for providing

- secured communication of Synchrophasor data between two endpoints via Internet Protocols



# Tasks



- Perform “blackbox” security testing to evaluate the effectiveness of the proposed SF framework
- Two testing activities:
  - **Phase 1:** Verification of **given** 74 security requirements of 11 of NIST IR 7268 categories
  - **Phase 2:** Penetration testing by injecting attacks via vulnerability exploits



# Tasks



- Perform “**blackbox**” security testing to evaluate the effectiveness of the proposed SF framework
- Two testing activities:
  - **Phase 1:** Verification of **given** 74 security requirements of 11 of NIST IR 7268 categories
  - **Phase 2:** Penetration testing by injecting attacks via vulnerability exploits
- Execution of testing activities:





# Phase 2



## Phase2 Activities:

- Coding scripts to identify Vulnerability, e.g.,
  - Scan network ports
  - Test unsecured software
- Injecting attacks that exploit the vulnerability found

## Results and Status:

- At least seven vulnerabilities being found. One of which can cause denial-of-service to the synchrophasor network
  - Most of them came from SF misconfiguration
  - Can be fixed easily
- Scripts for testing and details of vulnerability exploits will be included in the final report (mid of November)



# Vulnerabilities Summary



Denial of Service



Violate PCI DSS section 1.3.7



Man in the middle attack



Eavesdropping

Vulnerability	SF Components				
	ePDC	RDTMS	ePO	AD	ESM
CVE-2012-0002 Microsoft Remote Desktop Use-After-Free DoS					
X.509 Certificate Subject CN Does Not Match the Entity Name					
SMB Signing Disabled					
TLS/SSL support weak cipher					
Remote Desktop Protocol over SSL supports weak RC4 cipher					
TLS/SSL Server supports SSL version 2.0					
Open Database Access					

**Solution:** Upgrade and reconfigure the application



# Phase 1



## Phase1 Activities:

- **Requirement acquisition:** Assist in the interpretation of the testing requirements according to NIST standards
- **Testing Specification:** Providing feedbacks and assisting in defining proper security specifications for selected requirements
- **Verifying** that each given specification satisfies the corresponding NIST security requirement

## Results and Status:

- Due to changing **given** specifications, about 10% of the specifications still remain to be tested
- 85% out of 90% of tested cases are satisfied



# Verification Status



- SF specifications received from McAfee on Sept 16

Categories of Requirements	Total # of Requirments	Selected
1. Access Control	21	15
2. Audit and Accountability	16	13
3. Assessment and Authorization	6	2
4. Configuration Management	11	3
5. Continuity of Operations	11	2
6. Identification and Authentication	6	4
7. Incident Response	11	1
8. Development and Maintenance	7	2
9. Risk Management and Assessment	6	2
10. Communication Protection	30	26
11. Information Integrity	9	4

**74** requirements in 11 Categories



# Verification Status



- Received SF specifications from McAfee on Sept 16

Categories of Requirements	#Req.	Selected	Satisfy
1. Access Control	21	15	75%
2. Audit and Accountability	16	13	85%
3. Assessment and Authorization	6	2	100%
4. Configuration Management	11	3	100%
5. Continuity of Operations	11	2	100%
6. Identification and Authentication	6	4	100%
7. Incident Response	11	1	100%
8. Development and Maintenance	7	2	100%
9. Risk Management and Assessment	6	2	50%
10. Communication Protection	30	26	80%
11. Information Integrity	9	4	?

85% out of 90% of tested cases are satisfied



# Examples of unsatisfied specs.



## SG.SC-24 Honeypots

### Requirement

The Smart Grid information system includes components specifically designed to **be the target** of malicious attacks for the purpose of detecting, deflecting, analyzing, and tracking such attacks.

### Verification Result

Honeypots must have two features

1. **Detect** – able to identify the attack
2. **Isolate** – a part of system, which **seems** to contain information value to attackers (but it is a fake system)

Currently, SF has only detect feature **BUT no isolate feature**



# Examples of unsatisfied specs.



## SG.RA-6 Vulnerability Assessment and Awareness

### Requirements

1. Monitors and evaluates the Smart Grid information system according to the risk management plan on an organization-defined frequency to **identify vulnerabilities** that might affect the security of a Smart Grid information system;
2. ...

### Specification

Applies to Security Fabric with **presence of automated vulnerability scans** (NOTE: requires a vulnerability detection engine that feeds into ESM, such as McAfee Vulnerability Manager Product. **This is not currently bundled in security Fabric.**) ...

Need to test with the presence of vulnerability scanner



# Examples of unsatisfied specs.



## SG.SC-22 Fail in Known State Requirements

The Smart Grid information system fails to **a known state for defined failures.**

### Specification

In the case of a failure, the system will maintain the current policy definitions.

### Verification Result:

The proposed system must **define what their failure states** (known state) are and **describe how those states are secured** from loss of confidentiality, integrity, or availability.



# Summary



- Phase 1 : 85% out of 90% of tested specifications satisfy with requirements
- Phase 2 : at least 7 vulnerabilities were found but all of them can be fixed easily

## **What's next?**

- Deliver the draft version for testing results by mid of Nov 2014
- In order to obtain 100% satisfactory results of test specifications, we need to revise the given specifications



# Vulnerabilities (1)



- **Vulnerabilities** MS12-020 Vulnerabilities in Remote Desktop
- **Affected Component** ePDC and RDTMS on SF platform
- **Effect** Denial-of-Service
- **Solution** Update Remote Desktop Services on both machines



# Vulnerabilities (2)



- **Vulnerabilities** X.509 CN mismatch entity name
- **Affected Component** ePO and ESM
- **Effect** cannot detect and prevent active eavesdropping attacks
- **Solution** Update X.509 certificate



# Vulnerabilities (3)



- **Vulnerabilities** SMB signing disabled
- **Affected Component** ePO
- **Effect** less effective to prevent man in the middle attack against SMB
- **Solution** Enable SMB signing



# Vulnerabilities (4)



- **Vulnerabilities** TLS/SSL support weak cipher algorithm
- **Affected Component** **AD** (RC4 128 bit with MD5)
- **Effect** may enable an attacker to launch man-in-the-middle attacks and tamper with sensitive data
- **Solution** Configure TLS/SSL to disallow connection with weak cipher



# Vulnerabilities (5)



- **Vulnerabilities** Remote Desktop support weak cipher
- **Affected Component** **RTDMS**, **ePDC** on SF platform and **AD** (RC4 40bit and 50bit)
- **Effect** may enable an attacker to launch man-in-the-middle attacks and tamper with sensitive data
- **Solution** Configure Remote Desktop Server to disallow connection using weak cipher



# Vulnerabilities (6)



- **Vulnerabilities** TLS/SSL support SSL version 2.0
- **Affected Component** AD
- **Effect**
  - No protection from man-in-the-middle attack during the handshake
  - Weak MAC construction and relying only on MD5
  - ...
- **Solution** Configure TTL/SSL server to disallow connection with SSL version 2.0



# Vulnerabilities (7)



- **Vulnerabilities Database Open Access**
- **Affected Component ePO**
- **Effect** violation of PCI DSS section 1.3.7 to have databases listening on ports accessible from the Internet, even when protected with secure authentication mechanisms
- **Solution** Configure the database to allow only access from trusted system