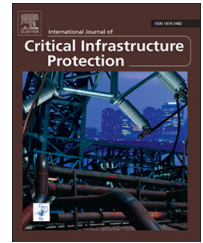


Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip

Exposing vulnerabilities in electric power grids: An experimental approach

Luigi Coppolino*, Salvatore D'Antonio, Luigi Romano

University of Naples "Parthenope," Centro Direzionale di Napoli Is. C4, 80143 Naples, Italy

ARTICLE INFO

Article history:

Received 6 December 2012

Received in revised form

29 November 2013

Accepted 23 January 2014

Available online 30 January 2014

Keywords:

Smart grids

Phasor measurement units

Synchrophasors

Phasor data concentrators

Security assessment

ABSTRACT

During the past few years, coordinated and targeted cyber attacks of unprecedented levels of sophistication have been conducted against critical infrastructures. Simple experiments and probes are now turning into concerted cyber operations, carried out for profit or political reasons. Examples of critical infrastructures include airports, railway networks, hospitals, energy plants and networks and dams. Among these, electric power grids are possibly the most critical assets, since virtually all the critical infrastructures strongly depend on power distribution networks for their operation. To improve the accuracy and coherence of supervisory control and data acquisition/energy management systems (SCADA/EMSs), utility operators are increasingly integrating emerging technologies for power data collection. This paper presents the results of a thorough security analysis of two key enabling technologies used for data collection in power grids: (i) phasor measurement units (PMUs) also known as synchrophasors and (ii) phasor data concentrators (PDCs). Evidence is provided to demonstrate that these technologies are vulnerable to traditional cyber attacks (due to weaknesses such as the lack of encrypted communications channels and weak password policies), as well as to emerging cyber attacks (due to the lack of input validation and sanitization).

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

The principal security goals for information technology (IT) assets are confidentiality, integrity and availability of data, services and communications systems. In the case of smart grids, cyber security requirements are particularly challenging to implement because they are imposed by the power domain as well as by the IT domain. Security strategies for the smart grid must guarantee both the resilience of the power infrastructure and the privacy of consumer information. The U.S. National Institute of Standards and Technology (NIST) [26] has produced a report entitled "Guidelines for Smart Grid Cyber Security" that presents a cyber security

strategy and architecture. The document identifies the following risks to the grid:

- Vulnerabilities and exposure to attacks and unintentional errors due to the increasing complexity of the grid.
- Novel vulnerabilities generated by the interconnection of different networks.
- Vulnerabilities and weaknesses caused by disruptions of the communications network and the introduction of malicious software/firmware and/or compromised hardware.
- Increased numbers of entry points and paths available for potential adversaries to exploit.

*Corresponding author.

E-mail address: luigi.coppolino@uniparthenope.it (L. Coppolino).

- Threats to data confidentiality and integrity caused by interconnected systems that can increase the amount of private information exposed and the risk when data are aggregated.
- New vulnerabilities introduced by the use of new technologies.
- Potential for compromise of data integrity, including customer privacy breaches due to increases in the collected data.

Reports by McAfee [16] and Symantec [31] discuss how critical infrastructures [1,6] are exposed to cyber attacks. The McAfee report describes “Night Dragon,” a major hacking initiative originating from China that specifically targeted power grids. The NIST report [26] identifies a number of research and development themes that must be addressed in the near future; these include phasor measurement unit security and protection.

Phasor measurement units (PMUs) and phasor data concentrators (PDCs) are key technologies used for power grid monitoring. A PMU, also known as a synchrophasor, is a device that measures the electrical waves on a power grid using a common time source for synchronization. A PDC is a node where phasor data from a number of PMUs or PDCs are correlated and output as a single stream to other applications. An assessment of the status of the power distribution network can be obtained by correlating information collected by multiple PMUs deployed in a single power grid.

Power grids are rapidly evolving to smart grids. According to the European Commission [28], a smart grid is “...an electricity network that can intelligently integrate the actions of all users connected to it – generators, consumers and those that do both – in order to efficiently deliver sustainable, economic and secure electricity supplies.”

Smart grids support new paradigms for power generation, consumption and delivery by leveraging advanced information and communications technologies and frameworks. A smart grid network (Fig. 1) incorporates several functional units. Each consumer hosts a smart controller and meter that are connected to a collector node. The collector node receives inputs from several end-points and transmits them to a utility station via the Internet. The utility is in charge of transmitting data to the distribution and transmission systems, typically via an intranet connection. The utility interacts with consumers by commanding their smart controllers and meters.

Given that power grids are evolving towards smart grids, successful attacks against the IT layers of a power grid could have a dramatic impact in the future, when smart grid architectures will include reconfiguration mechanisms that trigger automated actions when anomalous behavior [5] is detected in a power grid [33]. In this context, ensuring the integrity of measurements is of paramount importance, since their alteration could result in incorrect reconfiguration actions, and possibly monetary losses and blackouts with unpredictable cascading effects that could affect multiple countries [7,9,15]. A key project that is investigating the use of synchrophasor technology for power grid monitoring is NASPI (NASPInet) [8], an effort involving the North American Electric Reliability Corporation (NERC) [18], the U.S. Department of Energy and North American consumers and utilities. Another project is the Frequency Monitoring Network (FNET) [34], which seeks to detect power system anomalies using frequency disturbance recorders (FDRs) and information management systems (IMSSs).

This paper presents the results of a security analysis conducted on two key technologies that enable data collection in power grids, namely synchrophasor devices and PDCs.

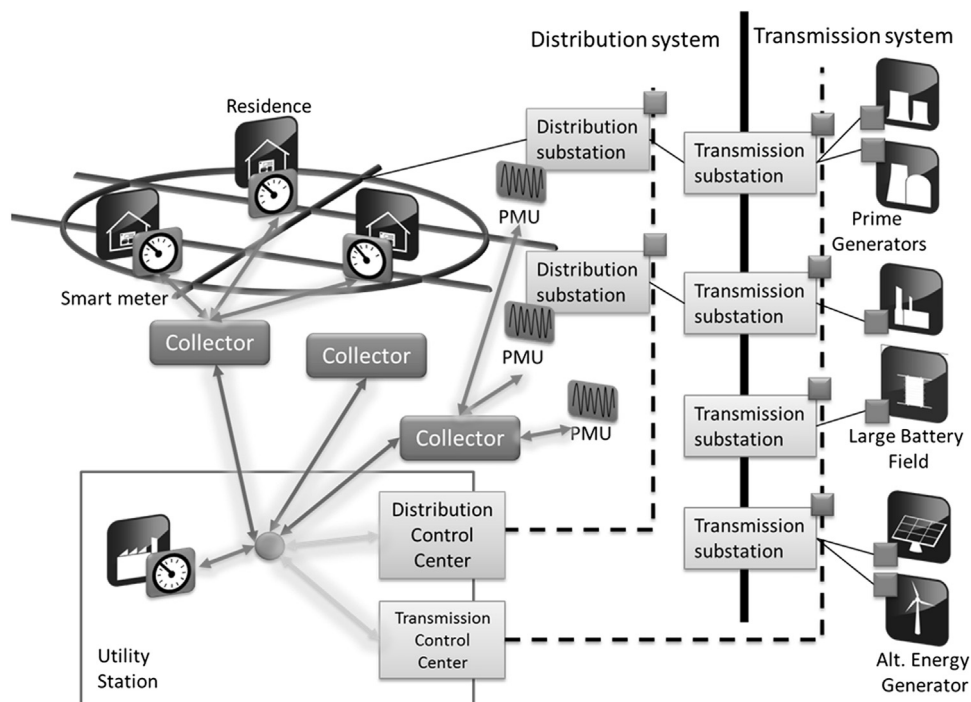


Fig. 1 – Schematic representation of a smart grid.

Preliminary results of this work are described in [4]. The current study was conducted on a commercial grade synchrophasor and a commonly used open-source PDC. The experiments involved three steps: (i) assessment of the security of the synchrophasor device as a stand-alone unit; (ii) analysis of the security of a simplified, yet realistic, networked testbed comprising the two key components of the data collection layer of a power grid architecture (synchrophasor and PDC); and (iii) analysis of a hardened version of the networked testbed. The paper presents evidence that state-of-the-art components of a power grid data collection infrastructure are affected by several vulnerabilities, such as unencrypted communications channels and weak password management. Some of these vulnerabilities are easily exploited by cyber attacks if additional security devices are not integrated and proper security-enhancing practices are not implemented. An important result of the experiments is that some of the more subtle vulnerabilities, such as those related to SQL injection [10], can affect the infrastructure even when common off-the shelf hardening devices are incorporated and state-of-the-art protection measures are implemented.

The remainder of the paper is organized as follows. Section 2 introduces synchrophasor and related technologies (including IEEE C37.118, the standard protocol for synchrophasor communications). Section 3 presents the objectives and the key results of the security analysis. Finally, Section 4 presents the concluding remarks.

2. Smart grids and phasor measurement units

An electrical power system (EPS) (or electrical system) comprises all the devices that are necessary to produce and transport electric power from production plants to final users. An EPS is normally organized in islands, called grids or power grids, that are interconnected for increased reliability and availability. All the components within an island operate in a synchronous manner, i.e., they operate at the same frequency; other islands may operate at different frequencies. PMUs [21] are devices that use GPS signals as a common time source and measure power system quantities at different locations across a wide-area system at the same instant of time. Unlike traditional SCADA systems [11] that are unable to measure real-time power line dynamics and angle evaluation, PMUs deployed throughout a power grid allow the collection of time-stamped real-time measurements at distinct – and typically distant – locations. The timestamps can be used to compare collected data with microsecond precision and ultimately assess the state of the grid. Gardner and Liu [12] describe how measurements collected by synchrophasors can be used to forecast serious events such as blackouts and how complex triangulation algorithms can be used to detect the exact points where the events occurred. A reference architecture for power grid monitoring incorporates synchrophasors positioned throughout a grid, PDCs that collect and correlate measurement data from the synchrophasors, and a superPDC (or central PDC) that gathers phasor data from all the remote PDCs and PMUs and passes the data to a visualization station. The IEEE C37.118 standard defines

the most widely used protocol for communicating synchrophasor data. In 2005, the IEEE C37.118 protocol was defined as an evolution of the IEEE 1344 standard [14] to facilitate the integration of synchrophasor technology. IEEE C37.118 also defines the protocols for phasor data transmission and synchrophasor device configuration.

IEEE C37.118 messages can be transmitted using TCP, UDP or higher-level protocols. The real-time data stream is occasionally interleaved with configuration messages. The data frames contain synchrophasor and frequency measurements and optionally other analog values (i.e., power flows) or status words (i.e., breaker status). The IEEE C37.118 standard is usually implemented as a client/server communication protocol, where the PMU acts as the server and the PDC as the client. The standard is designed for measurement collection from different PMUs and PDCs. For this reason, the data frames have an ID field that is used by PDCs to identify different sources. Note that the standard does not inherently support any security mechanisms for message exchange. Moreover, since there is no recommendation for the underlying transmission protocol, the standard could suffer from vulnerabilities that affect the lower (transmission) or the upper (message content) layers. These vulnerabilities can be exploited when devices are connected to public networks.

3. Security assessment

This section presents the results of the security analysis of two key technologies that enable data collection and storage in electric power grids. The analysis was performed on a top-end commercial-grade synchrophasor device and on a PDC application based on OpenPDC [20]. OpenPDC is an open-source PDC software system designed to process streaming time-series data in real time. OpenPDC, developed by the Tennessee Valley Authority [32], is the most widely used open-source platform for PDC application development. The OpenPDC platform is compliant with almost all the standard communication protocols used in the application domain (e.g., FNET, IEEE 1344 and IEEE C37.118) and allows for the generation of time-sorted concentrated data streams. Since the synchrophasor security assessment focused on commercial products, all references to vendors, models and versions are omitted. However, we have already informed the vendor (who very kindly donated the device, thus making the study possible) about the key results of the analysis. We believe that the vulnerabilities discovered in our experiments are also present in similar products available from other vendors.

The security analysis involved three phases:

- *Isolated device assessment*: This initial analysis focused on a key element of the smart grid data collection infrastructure (i.e., synchrophasor device).
- *Simplified testbed assessment*: This second analysis focused on the synchrophasor device as part of a testbed created using the official device documentation.
- *Hardened testbed assessment*: This final analysis focused on the synchrophasor device as part of a testbed created based on recommendations provided by major vendors.

Table 1 – Security assessment results.

Testbed description	Exposed weaknesses	Impact
Isolated device	1. Device fingerprinting	• Device allows remote identification
	2. Weak password management	• Easy to guess default passwords • Passwords need not be changed regularly • Easy to guess passwords are allowed • Device management communications are in the clear
	3. Unreliable channels: integrity, confidentiality, availability	◦ Passwords and sensitive data can be eavesdropped
Simplified testbed	4. Unreliable channels: integrity, confidentiality, availability	• PDC application communications are in the clear ◦ Exchanged data can be modified or dropped
	5. Poor input validation at the application level	• SQL injection
Hardened testbed	6. Poor protection from insiders	• Compulsory VPNs leave local communications in the clear
	7. Weak integration of legacy systems	• Integration of the synchrophasor with the central authenticator does not protect the device from insider attacks
	8. Poor input validation at the application level	• SQL injection

These recommendations, which were issued for other devices, are applicable to the technologies analyzed in this paper.

This section is organized into three subsections, one for each stage of the analysis. Table 1, which is provided at the end of this section, presents the key results of the three security assessment phases.

3.1. Isolated device assessment

In a power grid data collection infrastructure, multiple synchrophasors are deployed across the power grid to measure various parameters, including phasor measurements that provide indications of the grid state. The synchrophasor typically provides at least two network services: (i) remote control services that are accessible via a Telnet session in the case of the considered device; and (ii) data transmission services that allow for data transfer according to a communications protocol (IEEE C37.118 for the synchrophasor tested). When performing the security assessment of the device, we assumed that the device is physically secure, i.e., it is stored in a safe place and is protected by means of access control systems.

3.1.1. Information gathering

The first stage of a hacking action is normally called “information gathering.” It involves the collection of information related to the targeted system. A system is vulnerable if it allows external users to identify the system and the types of services and software applications running on it. In order to test the ability of the synchrophasor to hide such information, we launched an Nmap session on the device using the command: `nmap -v -p 1-65535 -A -O -T5 -PE 10.20.0.80`. It was possible to identify the vendor from the MAC address of

Not shown: 65532 closed ports		
PORT	STATE	SERVICE
21/tcp	open	ftp
23/tcp	open	telnet?
4712/tcp	open	tcpwrapped

Fig. 2 – Outputs of an Nmap session on the synchrophasor device (vendor information omitted).

the device (not shown in Fig. 2) along with other information (shown in Fig. 2).

The IEEE C37.118 standard assumes that Port 4712 is used for TCP connections and Port 4713 for UDP communications. Therefore, based on the vendor name and the services listening on Ports 23 and 4712/4713, it was possible to determine that the scanned device is a synchrophasor.

3.1.2. Password management and maintenance

The next stage of a hacking action is gaining access to the device. In our case, the device was password protected. The accounting system of the device has a hierarchical structure, i.e., the system has no formal users, and the only existing account provides different levels of permissions and privileges by using a different password for each level. The system has eight pre-configured levels. To get to the highest privilege level, the user must escalate through all the lower levels by providing the appropriate passwords. The privileges are granted for a limited time period that is configurable (default is 5 min). After this time, the privileges are withdrawn and the user is brought back to the lowest privilege level. The system protects against password brute forcing – after three consecutive failed attempts, access is forbidden for 30 s and an alarm is raised. The system allows remote access to be limited or excluded from certain ports. The password

management policies adopted by the device reveal the vendor's intent to put in place a strong authentication system. Nevertheless, a number of extremely dangerous, albeit easily fixable, weaknesses were discovered:

- The default passwords are common and simple alphabetic strings (e.g., TAIL, WATT, VOLTA) that are highly susceptible to dictionary attacks. No mechanism exists to ensure that the default passwords are changed (this usually results in users keeping the default passwords).
- Passwords are editable, but no constraints are imposed to ensure that strong passwords are used. Users are free to set weak or guessable passwords. This exposes the passwords to dictionary and brute force attacks.
- Multiple privilege levels can share a common password. Lazy users who are nonchalant about security could use the same password for all the privilege levels, rendering the multiple privilege level scheme utterly useless.
- Passwords do not expire and no password rejuvenation procedures are in place. This increases the likelihood of a successful brute force attack.

3.1.3. Remote management

Despite the known weaknesses of Telnet, remote management of the device is still performed using a Telnet session. Telnet sessions are conducted in the clear and, as shown in Fig. 3, even the authentication passwords are transmitted without encryption. The same is true for the other supported protocols that do not provide any inherent security mechanisms and conduct all communications in the clear, thereby exposing the synchrophasor to the same vulnerabilities as those encountered in a Telnet session.

An attacker is, therefore, able to sniff all the passwords and use them to gain access to the synchrophasor. Having gained complete control of the device, the attacker could modify the synchrophasor configuration and the collected phasor measurements.

3.2. Simplified testbed assessment

This section describes the results of the security assessment conducted on the data collection infrastructure. The testbed used in the analysis was built by implementing the recommendations provided in the official device documentation.

Fig. 4 shows the simplified, albeit realistic, testbed that incorporates a synchrophasor. The synchrophasor is connected to a PDC via the Internet. The PDC was implemented using the IEEE C37.118 input adapter provided by OpenPDC. The OpenPDC platform has a modular architecture that offers considerable freedom to create applications that perform complex elaboration of the received data. The architecture shown in Fig. 5 comprises three layers: (i) input adapter layer, (ii) action adapter layer, and (iii) output adapter layer.

The input adapter layer allows for the development of a module for interacting with any protocol used to send data to the application. The action adapter layer is where data processing and analysis are performed. The output adapter layer facilitates the integration of different presentation and storage media. In our application, phasor data from the various measurement points is transmitted using the IEEE C37.118 protocol and collected by an input adapter in the PDC application. The data is subsequently transferred to an output adapter, which stores all the measurements in a MySQL database.

prompt password:

0000	00	1d	92	9c	23	7c	00	30	a7	02	1c	52	08	00	45	00	# .0...R..E.
0010	00	37	13	e9	00	00	40	06	e3	84	c0	a8	01	02	c0	a8	.7....@.....
0020	01	01	00	17	04	76	11	74	59	a0	a8	64	9c	b4	50	18	v.tY..d..P.
0030	22	34	17	a6	00	00	0a	02	0d	0a	50	61	73	73	77	6f	"4.....Passwo
0040	72	64	3a	20	3f												rd: ?

sending password ("TAIL"):

0000	00	30	a7	02	1c	52	00	1d	92	9c	23	7c	08	00	45	00	.	0	...	R	...	#		...	E	.
0010	00	29	15	2b	40	00	80	06	62	50	c0	a8	01	01	c0	a8	.	)	.	@	...	b	P	...	...	...
0020	01	02	04	76	00	17	a8	64	9c	b4	11	74	59	af	50	18	...	v	...	d	...	t	Y	...	P	.
0030	00	fe	22	b0	00	00	54										..	"	...	...	...	...	...	...	...	
0000	00	30	a7	02	1c	52	00	1d	92	9c	23	7c	08	00	45	00	.	0	...	R	...	#		...	E	.
0010	00	29	15	2e	40	00	80	06	62	4d	c0	a8	01	01	c0	a8	.	)	.	@	...	b	M	...	...	...
0020	01	02	04	76	00	17	a8	64	9c	b5	11	74	59	b0	50	18	...	v	...	d	...	t	Y	...	P	.
0030	00	fe	35	ae	00	00	41										..	S	...	...	...	...	...	...	...	
0000	00	30	a7	02	1c	52	00	1d	92	9c	23	7c	08	00	45	00	.	0	...	R	...	#		...	E	.
0010	00	29	15	2f	40	00	80	06	62	4c	c0	a8	01	01	c0	a8	.	)	.	@	...	b	L	...	...	...
0020	01	02	04	76	00	17	a8	64	9c	b6	11	74	59	b1	50	18	...	v	...	d	...	t	Y	...	P	.
0030	00	fe	2d	ac	00	00	49										..	-	...	...	...	...	...	...	...	
0000	00	30	a7	02	1c	52	00	1d	92	9c	23	7c	08	00	45	00	.	0	...	R	...	#		...	E	.
0010	00	29	15	31	40	00	80	06	62	4a	c0	a8	01	01	c0	a8	.	)	.	@	...	b	J	...	...	...
0020	01	02	04	76	00	17	a8	64	9c	b7	11	74	59	b2	50	18	...	v	...	d	...	t	Y	...	P	.
0030	00	fe	2a	aa	00	00	4c										..	*	...	...	...	...	...	...	...	

Fig. 3 – Eavesdropping a password using Wireshark in a Telnet session.

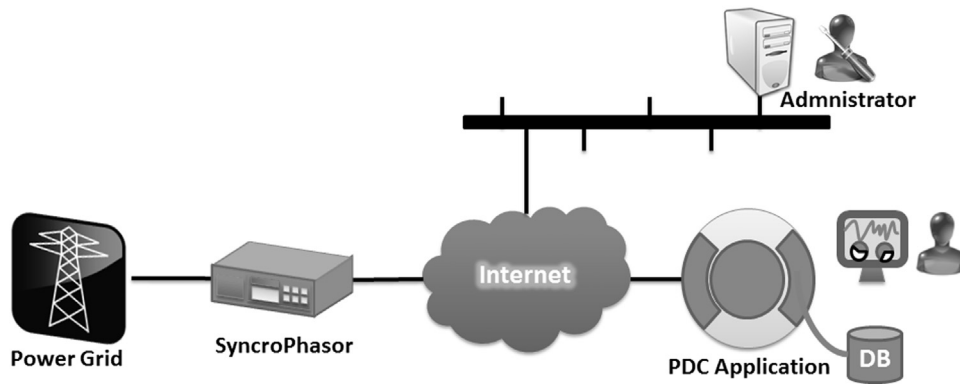


Fig. 4 – Simplified testbed used for analysis.

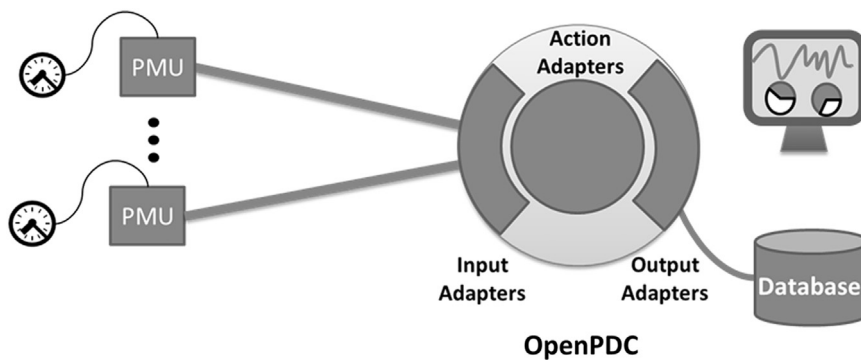


Fig. 5 – Phasor data concentrator application based on OpenPDC.

3.2.1. Weak communications

The synchrophasor used in the testbed supports two communications channels: (i) management communications and (ii) PDC application communications. With regard to management communications, we have already discussed the implication of using a Telnet session for transmitting device management messages. The weaknesses could be fixed using a virtual private network (VPN), but no suggestion is given regarding this or other countermeasures in the official device documentation. The installation guide only suggests that the device be directly connected to the network, leaving the security problems unsolved.

In the case of PDC application communications, the IEEE C37.118 protocol does not provide any encryption mechanisms and, thus, the communications are not inherently protected from eavesdropping. Any user who accesses a node that is in between the two endpoints of IEEE C37.118 communications (i.e., the synchrophasor and the PDC application) would be able to intercept and read all the messages (these messages contain measurement data or configuration information). Moreover, no authentication or other means of verification is used to identify the message source.

As shown in Fig. 6, the system is vulnerable to man-in-the-middle attacks. A malicious eavesdropper could easily read the messages exchanged between the synchrophasor and PDC for a period of time in order to discern the relevant communications parameters. The parameters could then be

modified during transmission or the synchrophasor could be impersonated by forging all the subsequent messages. In the second case, the attacker could further target the data collection infrastructure by exploiting vulnerabilities that affect the PDC application, as described in the remainder of this section.

3.2.2. Poor input validation at the application level

We analyzed the code of the OpenPDC IEEE C37.118 input adapter that was integrated in our PDC application. In particular, we focused on verifying whether or not the contents of incoming C37.118 messages are validated by the adapter before being forwarded to the application and database. We discovered that the message contents are not verified by the input adapter and that the adapter does not issue an error message when a string is included in the text field of a C37.118 message. Moreover, no sanitization is performed by the other adapters, which enables modified or fabricated content to be entered in the database that stores phasor measurements.

A PDC application is capable of receiving data streams from several synchrophasors deployed throughout the power grid being monitored and the application stores the data from each source in a different table. The number of synchrophasors can vary during the operation of the PDC application as new synchrophasors are installed and connected to the monitoring system. IEEE C37.118 is a “smart” protocol

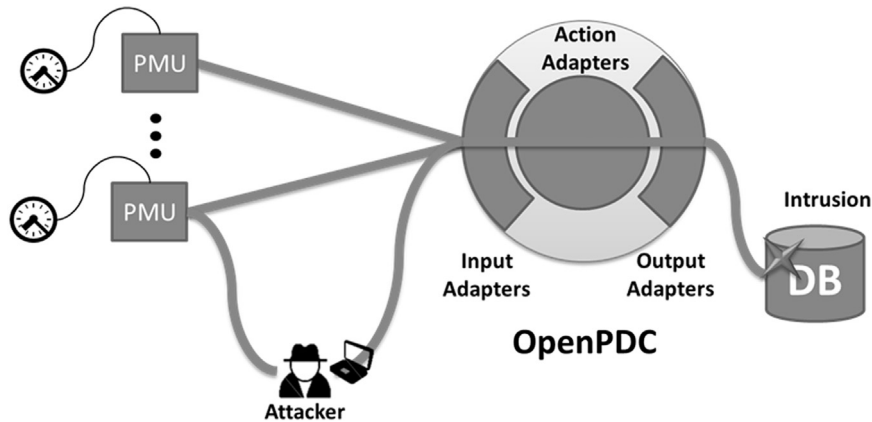


Fig. 6 – An attacker compromising an OpenPDC application.

because it assumes that a synchrophasor and PDC exchange configuration messages before the synchrophasor begins to send its measurements. The configuration messages announce the identity of the synchrophasor to the PDC and provide details about the structure and the type of the messages that will follow. The PDC application uses the information obtained from the synchrophasor configuration messages to create a new table in the database that stores the data received from the new synchrophasor. The name of the table is generated using the identifier associated with the synchrophasor and the structure of the records in the table is created based on the data that the synchrophasor is expected to send.

In such a situation, an attacker could exploit the blind trust that the application has in the message sender (synchrophasor) and inject SQL code into the application database. More precisely, the attacker could forge the synchrophasor identification name at will and perform an SQL injection attack on the PDC application simply by attaching some SQL code to the identification name provided to the application. The SQL code would then be executed in the database.

Numerous attacks are possible. A direct attack could delete the entire table containing measurements provided by a synchrophasor. Specifically, the attacker could attach a `DROP table_name;` command to his name, causing the entire measurement table to be deleted. This type of attack could be executed iteratively to erase the data collected from all the synchrophasors, which would significantly hinder assessments of power grid status.

Another attack relies on the injection of a `DELETE` command to selectively erase records from the database. This attack would be difficult to detect because it removes only a small portion of database data. A terrorist could use selective deletion to erase evidence of a physical attack on the power grid without bringing the whole database down, which would certainly alert the operators.

A smarter attacker could use a more subtle approach – change the names of the tables containing measurements by injecting well-crafted SQL `ALTER` commands. The attack could surreptitiously swap the names of different tables and associate measurements collected from one synchrophasor to another synchrophasor, deceiving the operators

monitoring the grid. This is potentially serious because, as mentioned previously, phasor measurements are used not only to prevent, but also to locate possible malfunctions or blackouts in the grid using triangulation. A finely tuned and orchestrated attack could trick the PDC application so that it incorrectly locates the position of an upcoming malfunction. The operator would rely on the incorrect information and proceed to implement countermeasures on a completely different – a stable – portion of the grid, allowing the malfunction to propagate and become a major outage.

3.3. Hardened testbed assessment

The final portion of the security analysis was conducted on a hardened testbed built by following recommendations provided by synchrophasor vendors (i.e., general documentation on power grid security and technical documents about other synchrophasors), but not directly related to the synchrophasor used in the testbed. Fig. 7 shows the hardened testbed. Unlike the simplified testbed, this testbed incorporates a demilitarized zone in which the synchrophasor is installed. This zone is separated from the Internet through a secure gateway (procured from the synchrophasor vendor) that allows for the management of VPNs from and to the PDC application and the remote management console. The secure gateway also acts as an authentication proxy, forwarding login requests directed to the synchrophasor to a central authentication point. This solution permits the enforcement of strong authentication strategies at the central authenticator and eliminates the authentication weaknesses discussed in the device-level analysis above. Although the new setup enhances the security of the infrastructure, many weaknesses still exist.

3.3.1. Poor protection from insiders

The use of compulsory VPNs (i.e., VPNs not initiated by the end nodes, but set-up between two domains by means of gateways) enables the channel between two communicating domains to be encrypted. This preserves the confidentiality and integrity of communications with the synchrophasor (i.e., it eliminates the possibility of eavesdropping or injecting/modifying data packets) along the Internet trunk used to

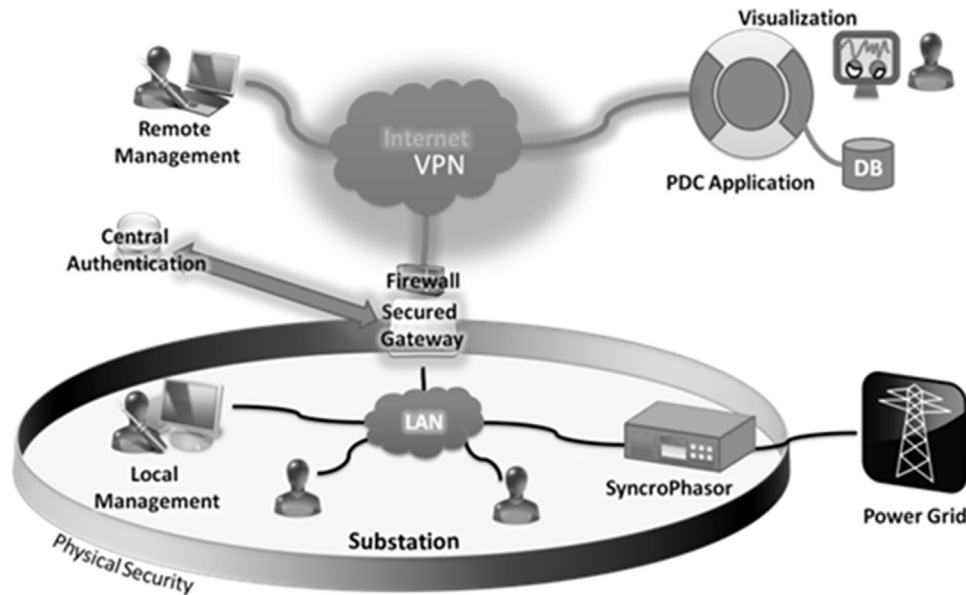


Fig. 7 – Hardened testbed used for analysis.

create the communications path. However, this solution (with respect to voluntary VPNs) still lacks a mechanism for preserving data confidentiality and integrity in the synchrophasor domain (i.e., the network trunk comprising the LAN in which the synchrophasor is installed and the portion beyond the secure gateway) as well as in the PDC and management domains. This potentially enables an attacker who has access to any of the involved domains (i.e., PDC, synchrophasor or remote management domains) to eavesdrop on passwords and/or other confidential information and to alter packets. It is important to emphasize that physical access to a domain is not required – an attack can leverage a virus or Trojan that has already compromised a machine in the domain.

3.3.2. Weak integration of legacy systems

Another weakness arises due to the integration of technologies that were designed and developed separately, specifically the synchrophasor and the central authenticator. Indeed, the synchrophasor was not designed to interact with the central authenticator, thus its integration with the central authenticator requires authentication to be completely disabled on the synchrophasor side. A proxy is in charge of intercepting login attempts and assigning their management to the central authenticator. On one hand, this makes it possible to apply stronger authentication policies to users in external domains, thus bypassing the proxy to reach the synchrophasor. On the other hand, this makes the synchrophasor vulnerable to malicious users who are connected to the same LAN in which the device is installed. Both these anomalies can be (partially) mitigated by restricting local domains to sets of machines that interact in order to collect smart grid data (i.e., the machine hosting the management console, PDC application and synchrophasor device).

Table 1 summarizes the results of the three security assessments.

4. Conclusions

As smart grids become operational around the globe, securing their control systems becomes a critical task. Compromises of grid monitoring functions could result in significant – and potentially damaging – effects on overall electricity power grid operations. This is a major security risk because attacks on electric power grids can dramatically impact virtually all societal activities.

In this context, the security assessment of the key technologies that enable data collection in electric power grids, namely, synchrophasors and PDCs, is of considerable importance. The assessment was performed on commercial-grade products, both open-source and proprietary. In fact, the realistic laboratory testbed used for the security assessment incorporates the same devices that are used by the North American Synchrophasor Initiative (NASPI) [19], the largest deployed phasor network.

The experimental results demonstrate that state-of-the-art components used to build smart grid data collection infrastructures have several vulnerabilities. Some of the vulnerabilities are easily exploited if proper security measures are not adopted and additional protection devices are not integrated. In particular, the exposure comes from traditional problems such as the lack of encryption in communications channels, the lack of input validation and sanitization, and the implementation of weak password policies. Of great concern is the fact that some of the vulnerabilities are also present in the hardened testbed considered in this work. The vulnerabilities enable common IT system attacks, such as SQL injection, to be launched against electric power infrastructures, corroborating recent reports about attacks against power grids [16,31].

This paper seeks to raise awareness about current and future threats and about the importance of incorporating cyber security requirements when designing, developing and

deploying smart grid data collection infrastructures. Just as important is training practitioners with strong security backgrounds who can grapple with the challenging problems created by the increasing adoption of IT in smart grids, in particular, and critical infrastructures, in general. We emphasize that major vendors and power grid operators take security very seriously, which is why a plethora of products are available to enhance the security of smart grid data collection infrastructure deployments. But these solutions primarily focus on security at the system level instead of the individual device or component level.

Electric power grid security is an open issue, one that requires continuous attention and improvement. Great strides have been made, but much more work remains to be done. Interested readers are referred to [2,3,13,17,22–25,27,29,30] for details about commercial products and best practices that can help address some of the security issues raised in this paper.

Acknowledgements

The research leading to these results has received funding from the European Commission's FP7-SECURITY Programme (SEC-2012.2.5-1) under Grant Agreement no.313034 (SAWSOC Project). This work has been partially supported by the TENACE PRIN Project (n. 20103P34XC) funded by the Italian Ministry of Education, University and Research. This work has been partially supported by Regione Campania through the research project "Embedded Systems in critical domains", POR Campania FSE 2007/2013.

REFERENCES

- [1] M. Afzaal, C. Di Sarno, L. Coppolino, S. D'Antonio, L. Romano, A resilient architecture for forensic storage of events in critical infrastructures, in: *Proceedings of the Fourteenth IEEE International Symposium on High-Assurance Systems Engineering*, 2012, pp. 48–55.
- [2] M. Braendle, Cyber Security – Effectively and Efficiently Tackling the Challenges Ahead, ABB, Cary, North Carolina, 2011, (<http://www.abb.com/cawp/seitp202/a6a42387602e83828525784200766310.aspx>).
- [3] T. Canals, A. Munsuri, Making Smart Metering Real: Deploying Prime Based Networks, ZIV Metering Solutions, Zamudio, Spain, 2011, (www.meteringsolutions.ziv.es/documentacion/papers/Deploying-PRIME-based-networks-JIEEC2011.pdf).
- [4] L. Coppolino, S. D'Antonio, I. Elia, L. Romano, Security analysis of smart grid data collection technologies, in: *Proceedings of the Thirtieth International Conference on Computer Safety, Reliability and Security*, pp. 143–156, 2011.
- [5] L. Coppolino, S. D'Antonio, M. Esposito, L. Romano, Exploiting diversity and correlation to improve the performance of intrusion detection systems, in: *Proceedings of the International Conference on Network and Service Security*, 2009.
- [6] L. Coppolino, S. D'Antonio, L. Romano and G. Spagnuolo, An intrusion detection system for critical information infrastructures using wireless sensor network technologies, in: *Proceedings of the Fifth International Conference on Critical Infrastructure*, 2010.
- [7] S. Corsi, C. Sabelli, General blackout in Italy Sunday September 28, 2003, h. 03:28:00, in: *Proceedings of the IEEE Power Engineering Society General Meeting*, 2004, pp. 1691–1702.
- [8] J. Dagle, North American SynchroPhasor Initiative, in: *Proceedings of the Forty-First Annual Hawaii International Conference on System Sciences*, 2008.
- [9] J. Eto, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, U. S.-Canada Power System Outage Task Force, Washington, DC and Ottawa, Canada, 2004 (emp.lbl.gov/publications/final-report-august-14-2003-blackout-united-states-and-canada-causes-and-recommendation).
- [10] M. Ficco, L. Coppolino, L. Romano, A weight-based symptom correlation approach to SQL injection attacks, in: *Proceedings of the Fourth Latin-American Symposium on Dependable Computing*, 2009, pp. 9–16.
- [11] M. Ficco, A. Daidone, L. Coppolino, L. Romano, A. Bondavalli, An event correlation approach for fault diagnosis in SCADA infrastructures, in: *Proceedings of the Thirteenth European Workshop on Dependable Computing*, 2011, pp. 15–20.
- [12] R. Gardner, Y. Liu, FNET: A quickly deployable and economic system to monitor the electric grid, in: *Proceedings of the IEEE Conference on Technologies for Homeland Security*, 2007, pp. 209–214.
- [13] M. Hadley, J. McBride, T. Edgar, L. O'Neil, J. Johnson, Securing Wide Area Measurement Systems, Pacific Northwest National Laboratory, Richland, Washington, 2007 (energy.gov/sites/prod/files/oeprod/DocumentsandMedia/8-Securing_WAMS.pdf).
- [14] Institute of Electrical and Electronics Engineers, 1344-1995 IEEE Standard for Synchrophasors for Power Systems, Piscataway, New Jersey, 1995.
- [15] S. Larsson, E. Ek, The black-out in southern Sweden and eastern Denmark, September 23, 2003, in: *Proceedings of the IEEE PES Power Systems Conference and Exposition*, 2004, pp. 1668–1672.
- [16] McAfee, Global Energy Cyberattacks: "Night Dragon," Santa Clara, California, 2011, (www.mcafee.com/au/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf).
- [17] S. Mix, Primer Discussion on Cyber Security: What do the CIP Standards Mean for SynchroPhasors in the Future? North American Electric Reliability Corporation, Washington, DC, 2009, (www.naspi.org/File.aspx?fileID=716).
- [18] North American Electric Reliability Corporation, Washington, DC, (www.nerc.com).
- [19] North American SynchroPhasor Initiative, Pacific Northwest National Laboratory, Richland, Washington, (www.naspi.org).
- [20] OpenPDC Grid Protection Alliance, OpenPDC, (openpdc.codeplex.com).
- [21] A. Phadke, Synchronized phasor measurements in power systems, *IEEE Computer Applications in Power* 6(2) (1993) 10–15.
- [22] RFL Electronics, What's new: eXmux 3500M – IP Access Multiplexer, Boonton, New Jersey, 2012, (www.rflect.com/news-events/what-s-new).
- [23] Schweitzer Engineering Laboratories, Cybersecurity, Pullman, Washington, 2014, (www.selinc.com/cybersecurity).
- [24] Schweitzer Engineering Laboratories, Secure Communications, Pullman, Washington, 2014, (www.selinc.com/securecommunications).
- [25] B. Sikdar, J. Chow, Defending synchrophasor data networks against traffic analysis attacks, *IEEE Transactions on Smart Grid* 2(4) (2011) 819–826.
- [26] Smart Grid Interoperability Panel – Cyber Security Working Group, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture and High-Level Requirements, NIST Interagency Report 7628, National

- Institute of Standards and Technology, Gaithersburg, Maryland, 2010 (csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol11.pdf).
- [27] Smart Grid Interoperability Panel – Cyber Security Working Group, Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security, National Institute of Standards and Technology, Gaithersburg, Maryland, 2010 (www.nist.gov/smartgrid/upload/nistir-7628_total.pdf).
- [28] SmartGrids – European Technology Platform, FAQs about ETP SmartGrids, Brussels, Belgium, 2013 (www.smartgrids.eu/node/56#12).
- [29] R. Smith, Cryptography Concepts and Effects on Control System Communications, Schweitzer Engineering Laboratories, Pullman, Washington, 2009, (www.selinc.com/WorkArea/DownloadAsset.aspx?id=5200).
- [30] J. Stewart, T. Maufer, R. Smith, C. Anderson, E. Ersonmez, Synchrophasor Security Practices, Schweitzer Engineering Laboratories, Pullman, Washington, 2010, (www.selinc.com/WorkArea/DownloadAsset.aspx?id=8502).
- [31] Symantec, Symantec Intelligence Quarterly Report: October–December 2010: Targeted Attacks on Critical Infrastructures, Mountain View, California, 2010, (http://www.symantec.com/content/en/us/enterprise/white_papers/b-symc_intelligence_qtrly_oct_to_dec_WP_21169903.en-us.pdf).
- [32] Tennessee Valley Authority, Knoxville, Tennessee (www.tva.gov).
- [33] D. Wei, Y. Lu, M. Jafari, P. Skare, K. Rohde, Protecting smart grid automation systems against cyberattacks, *IEEE Transactions on Smart Grid*2(4) (2011) 782–795.
- [34] Z. Zhong, C. Xu, B. Billian, L. Zhang, S. Tsai, R. Connors, V. Centeno, A. Phadke, Y. Liu, Power system frequency monitoring network (FNET) implementation, *IEEE Transactions on Power Systems*20(4) (2005) 1914–1921.