Investigating Cyber-Physical Attacks against IEC 61850 Photovoltaic Inverter Installations

BooJoong Kang, Peter Maynard, Kieran McLaughlin, Sakir Sezer
CSIT Centre for Secure Information Technologies
Queen's University Belfast
Northern Ireland, United Kingdom
{b.kang, pmaynard01, kieran.mclaughlin, s.sezer}@qub.ac.uk

Filip Andrén, Christian Seitl, Friederich Kupzog, Thomas Strasser
AIT Austrian Institute of Technology Energy Department - Electric Energy Systems
Vienna, Austria
{filip.andren, christian.seitl, friederich.kupzog, thomas.strasser}@ait.ac.at

***Abstract*—Cyber-attacks against Smart Grids have been found in the real world. Malware such as Havex and BlackEnergy have been found targeting industrial control systems (ICS) and researchers have shown that cyber-attacks can exploit vulnerabilities in widely used Smart Grid communication standards. This paper addresses a deep investigation of attacks against the manufacturing message specification of IEC 61850, which is expected to become one of the most widely used communication services in Smart Grids. We investigate how an attacker can build a custom tool to execute man-in-the-middle attacks, manipulate data, and affect the physical system. Attack capabilities are demonstrated based on NESCOR scenarios to make it possible to thoroughly test these scenarios in a real system. The goal is to help understand the potential for such attacks, and to aid the development and testing of cyber security solutions. An attack use-case is presented that focuses on the standard for power utility automation, IEC 61850 in the context of inverter-based distributed energy resource devices; especially photovoltaics (PV) generators.**

Keywords—Smart Grid security, IEC 61850, man-in-the-middle attack, photovoltaics

I. INTRODUCTION

The emerging cyber threats facing Smart Grids can be illustrated through a trend of recently discovered cyber-attacks. Havex is a remote access Trojan (RAT) which targets the open platform communication (OPC) standard widely used in process control systems. One of the Havex payloads enumerates all connected network resources, and uses the classic distributed component object model (DCOM) based version of the OPC standard to gather information about connected control system resources within the network [1]. In Dec. 2014, the United States Computer Emergency Response Team (US-CERT) had identified BlackEnergy malware which compromised industrial control systems in the US for at least three years [2]. BlackEnergy discovered on internet-connected HMIs including those from GE Cimplicity, Advantech/ Broadwin WebAccess, and Siemens WinCC. According to a report from Germany's Federal Office for Information Security [3], an advanced persistent threat (APT) group attacked an unnamed steel plant in Germany, resulting in significant damage. Login credentials were obtained via 'spear phishing' emails and social engineering techniques. Access was gained to the office network, then to the production systems, where a situation was initiated where a blast furnace could not shut down as normal, causing significant physical damage. Across these publicized examples, there is a trend towards the use and repurposing of crime-ware with new payload modules and functionalities specifically tailored towards intrusions in ICS environments. The resulting challenge is to understand and address the security gaps, where attackers understand the underlying physical systems, and appear to have the capability and intent to affect the operation of physical processes.

In this paper we conduct experiments regarding the cyber-security and physical effects of attacks conducted in the Smart Grid, against equipment using IEC 61850. This is an object oriented substation automation standard defining how to describe the devices in an electrical substation and how to exchange the information about these devices [4]. IEC 61850 also standardizes the set of abstract communication services allowing for compatible exchange of information among components of a power system. IEC 61850 offers three types of communication models: client/server type communication services model, a publisher-subscriber model and sample values model for multicast measurement values. The generic object oriented substation event (GOOSE) is a multicast message containing information that allows the receiving device to know that a status has changed and the time of the last status is changed. Because GOOSE does not support any authentication or encryption techniques, it is vulnerable to many cyber-attacks [9], [10], [11]. Manufacturing message specification (MMS) is one of the communication services widely used in IEC 61850. A TCP/IP connection is vulnerable to the man-in-the-middle (MITM) attack and MMS is also vulnerable to the MITM attack because MMS operates over standard TCP/IP and has no encryption [12].

In our experiments, a test environment comprising a photovoltaic (PV) installation is used to investigate and demonstrate a custom attack payload that can execute MITM attacks, manipulate data, and affect the physical system. The experiments are motivated by a set of National Electric Sector

978-1-4673-7929-8/15/$31.00 ©2015 IEEE

Cybersecurity Organization Resource (NESCOR) failure scenarios [16], which are applied to the physical test-bed.

The remainder of this paper is organized as follows. Section II summarizes the related work. Section III describes attack capabilities based on the MITM attack. Section IV presents a case study at the physical test-bed and Section V discusses some issues. Finally, Section VI concludes the paper and outlines avenues for future work.

II. Related Work

Much of the existing published work investigating the insecurity and exploitation of ICS communications focuses on Modbus, DNP3, IEC 60870-5 and IEC 61850. A key vulnerability for most systems is the lack of authentication or validation mechanisms. Although standards and mechanisms exist to address these issues (e.g. IEC 62351), their use in the real world is relatively uncommon at present.

M. Robinson [5] covers possible attack vectors such as lack of protocol security in MODBUS and DNP3. It discusses potential attacks like replay, MITM and spoofing. T. Morris et al. [6] investigates attacks such as response and measurement injection, and command injection using the MODBUS protocol. The paper details various levels of injection attacks ranging from naive injection which randomly injects values to complex injections, or target specific fields and values based on domain knowledge. Y. Yang et al. [7] details how MITM can be accomplished on smart grids. Gao et al. [8] shows command injection using Ettercap and other techniques. P. Maynard et al. performed the MITM attack against IEC 60870-5-104 which is widely used in control communication for water, gas and electricity and operates over TCP/IP [13].

J. Hoyos et al. [9] demonstrated a practical GOOSE message spoof attack. They identify GOOSE messages by looking for the specific Ether-type, 0x88B8, in Ethernet frames. After decoding GOOSE messages, they overwrite values, e.g., stNum, sqNum and values inside the data sets. They find out the GOOSE message interval by observing legitimate messages and they inject false (spoofed) messages within the observed interval. As a modification attack, they changed a data value to cause the intelligent electronic devices (IED) to trip the relay that could control a circuit breaker or switch in a real substation. N. Kush et al. [10] presented three variants of GOOSE 'poisoning' that: prevent legitimate GOOSE messages from being processed; hijack the communication, which can be used to implement a denial of service (DoS) attack; or manipulate the GOOSE subscriber. In the attacks, they multicast a single or a range of spoofed GOOSE messages with a status number which is high enough to cause the subscriber not to service any legitimate GOOSE messages with status numbers that are equal or less. As a result, they can then control the subscriber.

J. Hong et al. [11] simulated several cyber-attacks targeting IEC 61850-based Supervisory Control and Data Acquisition (SCADA) systems, e.g., replay, packet modification, injection and DoS attacks. They specially targeted GOOSE and sampled values (SV) which are multicast messages of IEC 61850 standard. In their test-bed, an IED subscribes to SV of voltage and current values from a Merging Unit and a circuit breaker subscribes to GOOSE from the IED. By broadcasting previously captured or generated GOOSE and SV messages to the substation LAN, an attacker could open the circuit breaker.

The above attacks are exploiting the lack of authentication and encryption at the data-link layer and GOOSE and SV do not include any of authentication and encryption. MMS is an alternative communication protocol of IEC 61850 but it is also vulnerable to the man-in-the-middle attack because MMS operates over TCP/IP. Published research on MMS is lacking, and this is the area in which this paper now focuses.

III. Attacking IEC 61850

In this section, attacks on power utility automation devices (i.e., IED) and SCADA systems are described. First, the MITM attack will be explained, which will be the basis of further attacks. Then, we will describe what specific attacks are possible against devices and systems that use IEC 61850 MMS communication. Finally, the described attack scenarios are compared against specific scenarios outlined by NESCOR. Our attack capabilities focus on the standard for power utility automation, IEC 61850, in the context of inverter-based distributed energy resource (DER) devices; especially on PV systems [14]. In the experiments here are some assumptions: 1) at least one of hosts in the network is already compromised by an attacker, which may be achieved using a 'typical' combination of phishing, malware, and so on as outlined in the Introduction; 2) target devices are connected to the same network; 3) the attacker is able to sniff traffic and identify the IP addresses and port numbers of target devices using the targeted application-level protocol, e.g. IEC 61850.

A. IEC 61850

IEC 61850 is an object oriented substation automation standard that defines how to describe devices in an electrical substation and how to exchange the information about these devices [4]. The IEC 61850 information model is based on two main levels of modelling: the breakdown of a real device (physical device) into logical devices, and the breakdown of logical device into logical nodes, data objects and data attributes. The approach of IEC 61850 is to decompose the application functions into the smallest entities which are used to exchange information. These entities are called Logical Nodes (LN); for example a virtual representation of a circuit breaker class, with a standardized class name such as XCBR [15]. IEC 61850 also standardizes the set of abstract communication services (Abstract Communication Service Interface–ACSI) allowing for compatible exchange of information among components of a power system. IEC 61850 offers three types of communication models: client/server type communication services model, a publisher-subscriber model and sample values model for multicast measurement values. Fig. 1 shows the communication stack of IEC 61850.

The GOOSE message structure supports the exchange of a wide range of possible common data organized by a dataset. The GOOSE message is multicast and is received by the IEDs which have been configured to subscribe to it. GOOSE messages contain information that allows the receiving device to know that a status has changed and the time of the last status

is changed. IEC 61850 also defines mappings between the abstract services/objects to a specific protocol such as MMS. For the sake of brevity, we will not go into detail of these mappings here, other than to say MMS objects and services can be mapped according to the IEC 61850-8-1 specification.

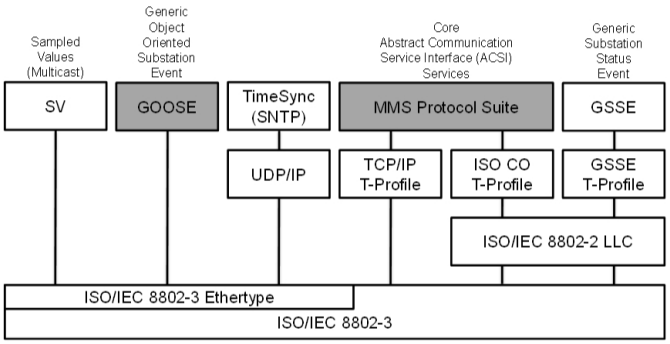


Fig. 1 IEC 61850 communication stack

B. Man-in-the-middle Attack

Our principal interest is the ability to facilitate manipulation of data at Layer 7, the application layer. A MITM attacker is placed in the middle of the connection between victims by hijacking the connection or making independent connections with the victims. The attacker can make the victims believe they are talking directly to each other by relaying messages between them. There are several Layer 2 techniques for MITM network attacks. Address resolution protocol (ARP) is used for resolution of IP addresses into MAC addresses. To resolve the MAC address, an ARP request is sent out on the LAN. The machine with the IP address then responds its MAC address within an ARP reply. ARP is a stateless and trusted protocol, so hosts will cache any ARP replies they receive, regardless of whether they requested information. ARP entries will be overwritten when a new ARP reply is received. ARP has no method to authenticate the origination of the message. This allows ARP spoofing that associates the attacker's MAC address with the IP address of a victim by sending spoofed ARP replies onto the LAN. Then, any traffic meant for that IP address will be sent to the attacker instead.

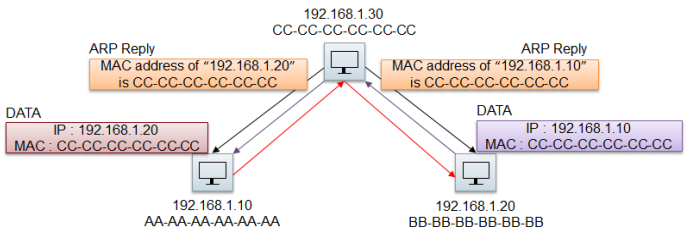


Fig. 2 ARP poisoning

As shown in Fig. 2, an attacker can send spoofed ARP replies to poison the ARP cache of each victim. The spoofed ARP entry will be stored in the ARP cache. When two victims send any messages to each other, the messages will contain the attacker's MAC address so the messages will be delivered to the attacker. The attacker will relay the messages to the original destination to make the victims believe that their messages are well delivered.

C. Attack Capabilities

MMS is one of communication services widely used in IEC 61850 and operates over standard TCP/IP. By ARP spoofing, an attacker can launch the MITM attack on the MMS communications of IEC 61850 devices. There are several types of attacks that the attacker can produce based on the MITM attack, and four types of them will be explained in this section; eavesdropping, modification, injection, and DoS attacks. Even if an attacker successfully achieved the MITM attack on the target, the attacker might want to gather more useful information by eavesdropping the hijacked or tapped communication before carrying out any further attacks. The attacker can observe all traffic between two devices and gather device-level information by decoding MMS messages. This enables attacks to be executed at Layer 7, the application layer.

During the MITM attack, the attacker will get messages from one device, modify them, and then relay the messages to the intended destination. Modification attacks can be used for example to hide or falsify measurements about the devices, and hence the underlying physical system, or to send undesired commands to the devices. After modification, checksum fields in the message should be recalculated before forwarding. MMS used for the client/server communication in IEC 61850 doesn't have any checksum field but TCP has a checksum field in the header. If the length of the message is changed, the sequence and acknowledgement fields of the messages should be adjusted as well as for all the following messages to maintain the communication between the devices.

After any injection is complete on the communication, the attacker will need to manage some side-effects of the injection. First, there might be some responses from the target machine, due the injected message, that the attacker needs to drop or alter. Second, any sequence and acknowledgement information needs to be corrected during the rest of communication. This includes sequence and acknowledgement fields in the TCP header, and the invoke ID field in MMS messages. Without this adjustment, the communication between devices will be terminated or reset. There are also several DoS attacks to be perpetrated against IEC 61850 devices, based on the MITM attack. First, an attacker can skip the relay step of the MITM attack, effectively blocking all messages to the original destination. Second, the attacker can modify all data in messages so devices never get the correct data. Lastly, the attacker can inject termination commands to devices.

D. Implementation

To implement the attacks, Ettercap is used along with a customized plug-in designed for targeted attacks against IEC 61850 MMS communications. The ability and expertise to develop such a payload, which can successfully interact with the ICS commands, is the key aspect differentiates the skills of an average attacker from one that can realize a physical effect on a target system. For obvious reasons, the detailed design of this attack plug-in is not discussed here. Using Ettercap and this custom plug-in the MITM attack can be launched on the communication between two machines, A and B, by running Ettercap with '*-M arp /IP address of A/ /IP address of B/*' options that will execute ARP poisoning targeting two given IP addresses. The custom attack is loaded by giving another

option '*-P mitm_61850*' when we run Ettercap, where '*mitm_61850*' is the name of the plug-in (see Fig. 3).

```
ettercap 0.8.1 copyright 2001-2014 Ettercap Development Team

Listening on:
  eth0 -> 7A:
          10.55.55.130/255.255.255.0
          fe80::

  35 plugins
  42 protocol dissectors
  57 ports monitored
19839 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services

Scanning for merged targets (2 hosts)...

* |==================================================>| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 10.55.55.111 0E:

 GROUP 2 : 10.55.55.121 8A:
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help

Activating mitm_61850 plugin...
```

Fig. 3 Ettercap execution

Once the MITM attack is launched, and the customized plug-in loaded, the tool receives all packets between targets and the plug-in can modify the packets. It can decode MMS packets by using the Abstract Syntax Notation One (ASN.1) Basic Encoding Rules (BER) to get detailed information of devices. It is designed to modify packets before forwarding them and can drop packets or inject craft packets as shown in Fig. 4. To maintain the connection, it recalculates the checksum of modified packets and adjusts sequence and acknowledgement numbers if a packet is injected or dropped. Checksum recalculation is supported in Ettercap but sequence and acknowledgement adjustment is done independently.

```
[1] 10.55.55.121 -> 10.55.55.111
[2] 10.55.55.111 -> 10.55.55.121
[3] 10.55.55.121 -> 10.55.55.111
[4] 10.55.55.111 -> 10.55.55.121

!!!Injection : 10.55.55.121 -> 10.55.55.111

[5] 10.55.55.111 -> 10.55.55.121

!!!Packet Drop


!!!Injection : 10.55.55.121 -> 10.55.55.111

[6] 10.55.55.111 -> 10.55.55.121

!!!Packet Drop

[7] 10.55.55.121 -> 10.55.55.111
[8] 10.55.55.111 -> 10.55.55.121
```

Fig. 4 Customized Ettercap plug-in outputs: two injections and two drops

IV. Case Study : PV Inverter

A. Remote Commands for DER Units

State-of-the art DER installations feature a power grid operator interface for external control commands. The minimum size of installations from which such an interface is required, as well as protocols and command sets used depend on local grid codes. A typical application of such SCADA connections to DER units is power shedding. This is necessary when generation is significantly higher, or load is significantly lower, than planned. It can also be necessary in case of emergency situations such as a split of the interconnected transmission grid in larger sub-systems (see e.g. [17]). Although in practice, heterogeneous solutions for remote control of DER units are used, we selected a likely near-future scenario in which a PV inverter is equipped with an IEC 61850 interface [18], [19]. The effect of attacking a single DER unit is of course low. However, assuming that a large number of units are involved, e.g. the NECOR scenarios as discussed later, consequences can range from monetary losses for DER and grid operator up to physical damage and power failures.

B. Laboratory Setup

The demonstration of the attack capability is carried out in a defined environment, the AIT SmartEST laboratory. The SmartEST lab offers an environment for testing, verification and R&D in the field of large scale distributed energy system integration and smart grids applications. The laboratory infrastructure accommodates DER components as inverters, storage systems, combined heat and power (CHP) units, voltage regulators/controllers, and other types of related electrical equipment. Powerful controllable AC and DC sources allow full-power testing capability up to 1 MVA (AC), including a high-performance PV array simulation (DC).

The laboratory setup includes a commercial off-the-shelf 20 kW PV inverter connected to a PV simulator as power source and a laboratory current sink as model for the power grid connection. The inverter itself has no IEC 61850 capabilities. These are added by a gateway component on the basis of Raspberry Pi (R-Pi) hardware, which essentially serves as a programmable gateway between an IEC 61850 SCADA network and the inverters in-built Modbus interface (see Fig. 5) [14]. The programmable functions of the gateway controller are realized using the IEC 61499 reference model for distributed automation. For the purposes of experimentation the communications network that is externally accessible ends at the IEC 61850 interface of the R-Pi controller.

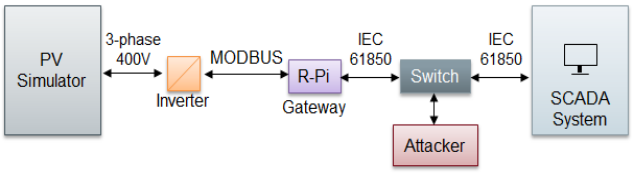


Fig. 5 Lab setup used to demonstrate the MITM attack on a PV inverter

C. Attacks to PV Inverter

For the purpose of the experiments we assume that an attacker has already compromised a machine which is connected to the same LAN and identified the IP addresses of the target inverter and controller devices. In the compromised machine, the attacker can easily execute the MITM attack on the target devices by using ARP poisoning as described in the previous Section III-A. Once the attacker executes the MITM attack with target IP addresses, the attacker can get all packets between the target devices. In our demonstration, Ettercap is used to execute ARP poisoning for the MITM attack and a customized plug-in is implemented and loaded to execute further attacks on the communication between the target devices. As shown in Fig. 5, the R-Pi is the translator between MODBUS and IEC 61850 for the PV inverter and its IP

address ends with 111. A SCADA system is a monitoring client to the PV inverter via the R-Pi and its IP address ends with 121. Note it is assumed an attacker has already compromised a machine in the same LAN.

Fig. 6 shows packet captures of our attack demonstration at the client-side, which is a SCADA system. 'No.' is the sequence number of packet and 'Source' and 'Destination' are source and destination IP addresses. Protocol and the length of packet are also shown and a short information of packet is shown in the 'Info' column. We used Wireshark to capture the packets at the client, which is controlled by a legitimate operator. The operator at the client behaves a predefined normal scenario controlling the power limitation of PV inverter. The first seven packets are initialization packets for a new MMS connection and the operator made seven confirmed-requests and got seven responses for the requests.

No.	Source	Destination	Protocol	Length	Info
505	10..121	10..111	TCP	66	49481→102 [SYN] Seq=0 Win=8192 L
506	10..111	10..121	TCP	66	102→49481 [SYN, ACK] Seq=0 Ack=1
507	10..121	10..111	TCP	54	49481→102 [ACK] Seq=1 Ack=1 Win=
508	10..121	10..111	COTP	76	CR TPDU src-ref: 0x0002 dst-ref:
509	10..111	10..121	COTP	76	CC TPDU src-ref: 0x0002 dst-ref:
510	10..121	10..111	MMS	245	initiate-RequestPDU
511	10..111	10..121	MMS	201	initiate-ResponsePDU
526	10..121	10..111	TCP	54	49481→102 [ACK] Seq=214 Ack=170
1060	10..121	10..111	MMS	133	confirmed-RequestPDU
1061	10..111	10..121	MMS	94	confirmed-ResponsePDU
1062	10..121	10..111	MMS	146	confirmed-RequestPDU
1063	10..111	10..121	MMS	83	confirmed-ResponsePDU
1082	10..121	10..111	TCP	54	49481→102 [ACK] Seq=385 Ack=239
1335	10..121	10..111	MMS	139	confirmed-RequestPDU
1336	10..111	10..121	MMS	90	confirmed-ResponsePDU
1346	10..121	10..111	TCP	54	49481→102 [ACK] Seq=470 Ack=275
1699	10..121	10..111	MMS	133	confirmed-RequestPDU
1700	10..111	10..121	MMS	94	confirmed-ResponsePDU
1701	10..111	10..121	MMS	146	confirmed-RequestPDU
1703	10..111	10..121	MMS	83	confirmed-ResponsePDU
1713	10..121	10..111	TCP	54	49481→102 [ACK] Seq=641 Ack=344
1986	10..121	10..111	MMS	139	confirmed-RequestPDU
1987	10..111	10..121	MMS	90	confirmed-ResponsePDU
1999	10..121	10..111	TCP	54	49481→102 [ACK] Seq=726 Ack=380
2806	10..121	10..111	MMS	139	confirmed-RequestPDU
2807	10..111	10..121	MMS	90	confirmed-ResponsePDU
2822	10..121	10..111	TCP	54	49481→102 [ACK] Seq=811 Ack=416

Fig. 6 Packer captures at client-side (SCADA system)

The first confirmed-request (#1060) is a 'getVariableAccessAttributes' request to get the type of a given data attribute and the second confirmed-request (#1062) is a write request to change the value of 'MaxWLim' as '0x082C80000' which is the floating value of '100' as shown in Fig. 7. (Note that the actual attribute names are intentionally partially redacted). This write request sets the power limitation of the PV inverter to 100%.

```
Frame 1062: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on int
Ethernet II, Src: 8a:[redacted] (8a:[redacted]), Dst: 0e:[redacted]
Internet Protocol Version 4, Src: 10.55.55.121 (10.55.55.121), Dst: 10.55.55.111
Transmission Control Protocol, Src Port: 49481 (49481), Dst Port: 102 (102), Seq
MMS
  confirmed-RequestPDU
    invokeID: 2
    confirmedServiceRequest: write (5)
      write
        variableAccessSpecificatn: listOfVariable (0)
          listOfVariable: 1 item
            listOfVariable item
              variableSpecification: name (0)
                name: domain-specific (1)
                  domain-specific
                    domainId: FORTE_GWLDevice1
                    itemId: [redacted]MaxWLim[redacted]
        listOfData: 1 item
          Data: floating-point (7)
            floating-point: 0842c80000
```

Fig. 7 Write request to 100% of power limitation (by operator)

A read request (#1335) for the same data attribute, 'MaxWLim' has been sent and the value of 'MaxWLim' is set as requested by the previous write request as shown in Fig. 8(b). After another 'getVariableAccessAttributes' request (#1699), there is another write request (#1701) to change the value of 'MaxWLim' as '0x084270000' which is the floating value of '60' as shown in Fig. 9. At this time the operation has been to set the maximum power limit to 60% of possible power output. The operator also checked the value of 'MaxWLim' by sending a read request (#1986) and Fig. 10 shows that it is set as requested.

```
Frame 1335: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on int
Ethernet II, Src: 8a:[redacted] (8a:[redacted]), Dst: 0e:[redacted]
Internet Protocol Version 4, Src: 10.55.55.121 (10.55.55.121), Dst: 10.55.55.111
Transmission Control Protocol, Src Port: 49481 (49481), Dst Port: 102 (102), Seq
MMS
  confirmed-RequestPDU
    invokeID: 3
    confirmedServiceRequest: read (4)
      read
        variableAccessSpecificatn: listOfVariable (0)
          listOfVariable: 1 item
            listOfVariable item
              variableSpecification: name (0)
                name: domain-specific (1)
                  domain-specific
                    domainId: FORTE_GWLDevice1
                    itemId: [redacted]MaxWLim[redacted]
```

(a) Read request

```
Frame 1336: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interfa
Ethernet II, Src: 0e:[redacted] (0e:[redacted]), Dst: 8a:[redacted]
Internet Protocol Version 4, Src: 10.55.55.111 (10.55.55.111), Dst: 10.55.55.121
Transmission Control Protocol, Src Port: 102 (102), Dst Port: 49481 (49481), Seq
MMS
  confirmed-ResponsePDU
    invokeID: 3
    confirmedServiceResponse: read (4)
      read
        listOfAccessResult: 1 item
          AccessResult: success (1)
            success: floating-point (7)
              floating-point: 0842c80000
```

(b) Read response

Fig. 8 Read request (a) and response (b) with 100% of power limitation

```
Frame 1701: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on int
Ethernet II, Src: 8a:[redacted] (8a:[redacted]), Dst: 7a:[redacted]
Internet Protocol Version 4, Src: 10.55.55.121 (10.55.55.121), Dst: 10.55.55.111
Transmission Control Protocol, Src Port: 49481 (49481), Dst Port: 102 (102), Seq
MMS
  confirmed-RequestPDU
    invokeID: 5
    confirmedServiceRequest: write (5)
      write
        variableAccessSpecificatn: listOfVariable (0)
          listOfVariable: 1 item
            listOfVariable item
              variableSpecification: name (0)
                name: domain-specific (1)
                  domain-specific
                    domainId: FORTE_GWLDevice1
                    itemId: [redacted]MaxWLim[redacted]
        listOfData: 1 item
          Data: floating-point (7)
            floating-point: 0842700000
```

Fig. 9 Write request to 60% of power limitation (by operator)

```
Frame 1987: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interfa
Ethernet II, Src: 7a:[redacted] (7a:[redacted]), Dst: 8a:[redacted]
Internet Protocol Version 4, Src: 10.55.55.111 (10.55.55.111), Dst: 10.55.55.121
Transmission Control Protocol, Src Port: 102 (102), Dst Port: 49481 (49481), Seq
MMS
  confirmed-ResponsePDU
    invokeID: 6
    confirmedServiceResponse: read (4)
      read
        listOfAccessResult: 1 item
          AccessResult: success (1)
            success: floating-point (7)
              floating-point: 0842700000
```

Fig. 10 Read response with 60% of power limitation at client-side

As shown in Fig. 11, the power limitation has been changed to '0x084120000', which is '10', when the operate checks the power limitation by sending a read request (#2806). There is no write request between two read requests (#1986 and #2806). Without any action from the operator, the power limitation has

been changed to 10%. Fig. 12 shows the packet captures at the server-side, R-Pi. The first seven packets are for MMS initialization and the R-Pi got nine confirmed-requests and made nine responses for the requests. Note that there are two more requests in the packet captures at the R-Pi. The first six pairs of confirmed-request and response are the same packets that we've seen in the packet captures at the client-side.

As shown in Fig. 13, the power limitation is '0x0842700000' which is the same value as shown in Fig. 9.

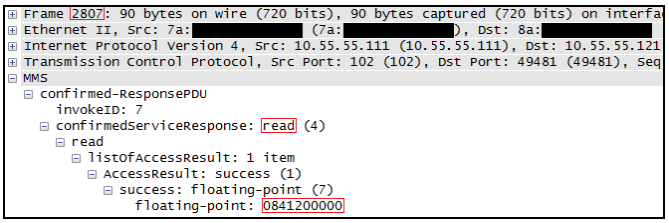


Fig. 11 Read response with 10% of power limitation at client-side

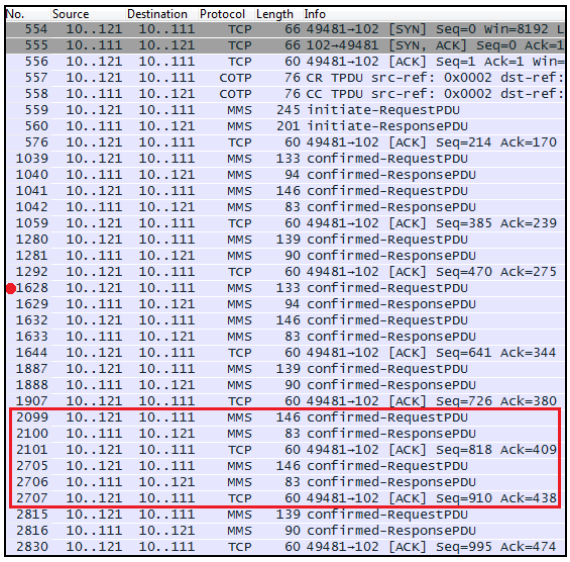


Fig. 12 Packet captures at server-side (R-Pi)

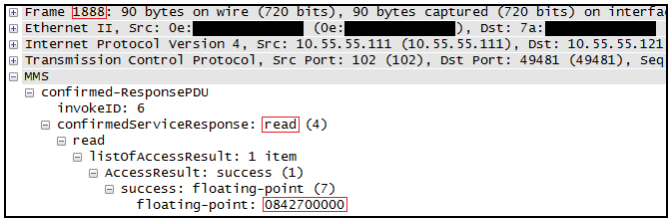


Fig. 13 Read response with 60% of power limitation at server-side

The last pair of confirmed-request and response is also same with the last pair in the packet captures at the client side (see Fig. 11 and Fig. 14). However, two confirmed-requests (#2099 and #2705) and two confirmed-responses (#2100 and #2706) cannot be found in the packet captures at the client-side but those packets don't have any different IP address. Those packets are highlighted by a red rectangle in the Fig. 15.

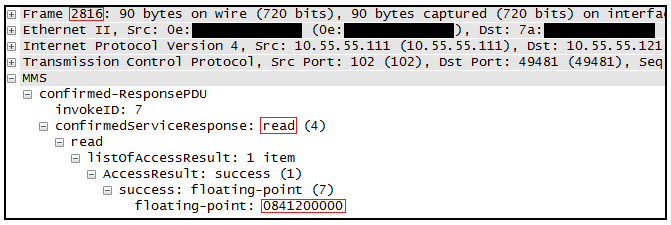
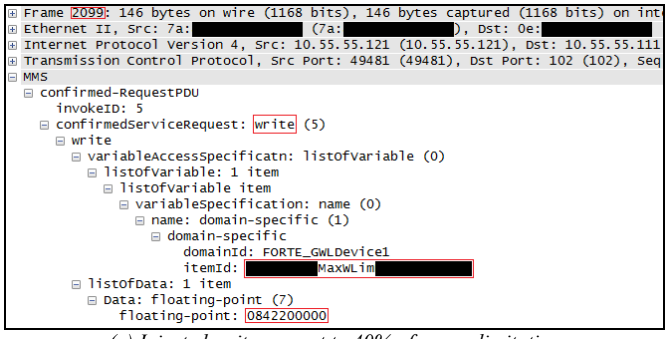
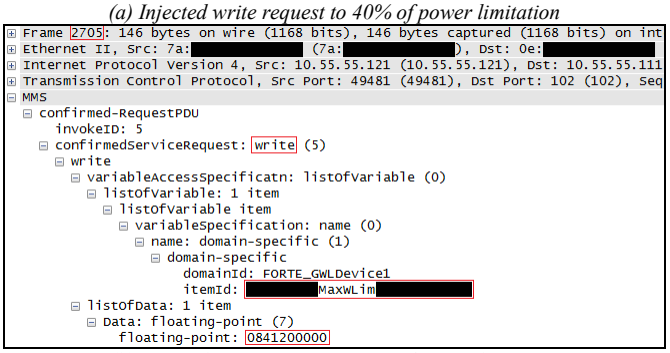


Fig. 14 Read response with 10% of power limitation at server-side



(a) Injected write request to 40% of power limitation



(b) Injected write request to 10% of power limitation

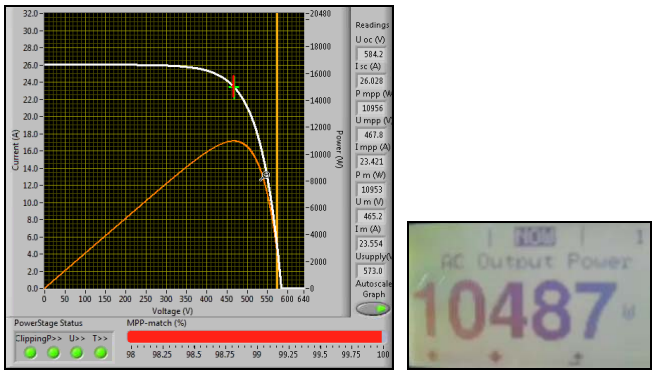
Fig. 15 Two injected write requests by the attacker

The new two confirmed-requests (#2099, #2705) are write requests to change the data attribute 'MaxWLim' to '0x0842200000' and '0x0841200000', respectively. The latter value is the value seen in the last read response in the packer captures at the client-side. These two requests have been injected by the attacker and the responses of the two requests have been dropped to prevent being sent to the legitimate client, (the operator) as shown in Fig. 4. As a summary, the attacker can eavesdrop, modify, inject and drop packets based on the MITM attack. As a case study, false MMS packets which can maliciously set the power limitation to any desired values. Note that no packet which is captured at the client-side, so the controlling system is not aware of such changes.

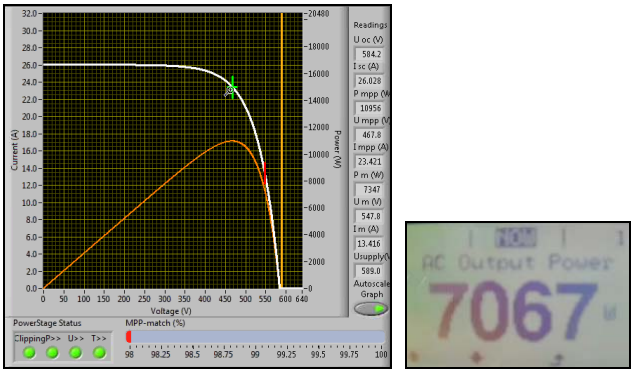
D. Physical Impact on PV Inverter

In this section, we will highlight the physical impact of the attacks on the PV inverter. In the experiments there are two ways to record and observe the electrical output of the PV inverter system. Fig. 16 shows the PV simulated panel on the left (it is worth noting the "simulated" panel produces real physical electrical outputs and responses). The graph shows the characteristic voltage vs. current curve, and power output, for the PV panel. A green cross shows the maximum power

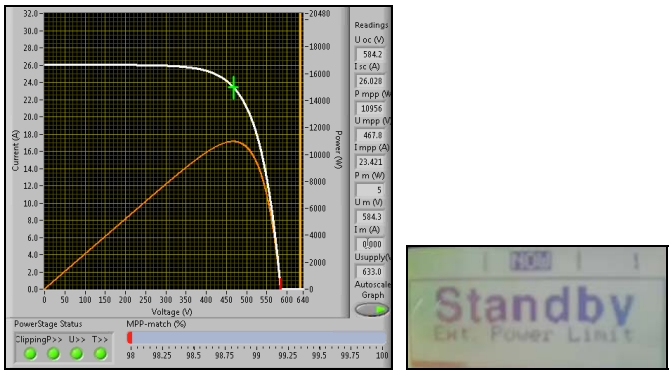
point, i.e. the theoretical maximum power output of the PV panel. The red cross shows the real power point at which the system is currently operating. Normally the inverter tries to operate at the maximum power point, as shown in Fig. 16-(a), where the red and green crosses overlap. The PV inverter can be programmed with different power limitation set-points, such that the power output is limited (up to100%). In such a case the operating point (red cross) moves away from the maximum power point.



(a) 100% of power limitation by the operator



(b) 60% of power limitation by the operator



(c) 10% of power limitation by the attacker

Fig. 16 Status changes of PV inverter: (a) 100% power limitation, (b) 60% power limitation, and (c) 10% power limitation, causing a standby state

Before executing any cyber-attacks, the operator has set the power limitation to 100% and the PV inverter generates AC output power of 10,487 W as shown in Fig. 16-(a). When the operator set the power limitation to 60%, the PV inverter generates 7,067 W of the AC output power as shown in Fig. 16-(b). After capturing and analyzing the communications during this valid operation, as described in the previous section, an attacker is now able to craft malicious packets and execute an attack to set the power limitation to a value of their choice. The Ettercap tool presented in this paper allows any vale to be selected. In the example shown Fig. 16-(c) the attacker sets this value to 10%. As the result of this new set-point, the PV inverter is forced to physically switched off, and it can be seen that in Fig. 16-(c) the LCD display shows it has fallen into standby mode. At this point the device is non-operational and requires several minutes to restart.

V. Discussion

Plain text transmissions that lack encryption and authentication make the underlying physical systems vulnerable to various types of cyber-attacks. IEC 61850 itself does not specify security aspects and does not enforce any authentication or encryption in GOOSE and SV. MMS has authentication and access control functionalities but MMS itself is not designed with information security in mind [14]. The MITM attack can be launched even in the presence of such authentication and the attacker can read all packets in a typical implementation where there is no encryption.

IEC 62351 is a set of standards handling information security for communication protocols including IEC 61580, IEC 60870-5-104 and DNP3 [20]. IEC 62351-4 [21] specifies procedures, protocol extensions, and algorithms to facilitate securing MMS based applications. It recommends to use Transport Layer Security (TLS) to secure the MMS communications. However one reason for lack of adoption, as M. Chowdhury et al. [22] point out, is that legacy embedded systems may have concerns such as high run-time memory usage and considerable increase of data read and write times because of the limited resources.

A. NESCOR Mappings

The experiments and attack scenarios presented in this work have been designed to map to a number of NESCOR failure scenarios [16] that defines several DER scenarios. The attacker capabilities in the following scenarios map directly to the capabilities demonstrated in our experiments:

DER.14 defines a threat agent that spoofs DER control commands to perform emergency shutdowns of a large number of DER systems simultaneously. A threat agent (the attacker) can use the MITM attack to perform modification on DER SCADA control commands. The attacker can capture all messages from and to the target DER systems, and can therefore modify captured control commands causing emergency shutdowns or stops of the target DER systems. The number of DER systems is not a problem as long as the DER systems are connected in the same network. This attack scenario could make the target power system unstable and cause outages and power quality problems.

DER.15 identifies a threat agent that modifies data being monitored by the utility distribution DER SCADA system in real-time, altering the load value so that it is higher than the actual value. An attacker can use the MITM attack to perform modification on DER data. The attacker can capture messages

to the target DER SCADA systems and the attacker can alter captured data to predefined or random values. The attacker can also observe the data over a period of time to figure out appropriate values for this modification. *DER.15*, suggests this attack scenario could increase utility costs for unnecessary ancillary services, as just one of many possible outcomes.

DER.16 describes a threat agent that breaches a DER SCADA system and causes the DER SCADA system to issue an invalid command to all DER systems. An attacker can use a MITM attack to perform modification and injection attacks on the connections of the target system. The attacker can capture some messages, modify them to include invalid commands, and then relay the invalid commands to DER systems. Invalid commands could be chosen at random. *DER.16* suggests this scenario could make the power system experience immediate and rapid fluctuations as some DER systems shut down while others go into default mode, with no Volt/VAR support, others revert to full output, and a few become islanded micro-girds. It might also cause equipment damage due to power system surges and sags and transmission power quality problem.

VI. Conclusion

IEC 61850 is becoming increasingly widely adopted in Smart Grids to support power automation systems. GOOSE, SV and MMS are communication services which can be used to exchange information among IEC 61850 devices. Previous published works have investigated attack capabilities against GOOSE and SV, but not MMS. In this paper, we derived and implemented cyber-attack capabilities based on MITM attacks in an electrical system which uses MMS communications. This work has been verified in a test-bed environment using real physical PV devices and communications. Most other publications also tend to lack extensive verification in realistic environments. The experiments have demonstrated the capability to cause a physical effect on the electrical devices and underlying system operation. This was achieved via malicious manipulation of power limits, thus changing the physical operation of PV inverter devices, or indeed to cause them to switch off, without the knowledge of the operator at the SCADA system. The operations of the described custom Ettercap attack payload, and the resulting physical consequences, have proven consistent with the attack capabilities, scenarios and consequences outlined by NESCOR. A significant contribution of this work is the development of a Havex-like malware payload that can be used for continued research into threat modelling, penetration testing, and designing security approaches for the described IEC 61850 PV environment, consistent with the priorities described by NESCOR.

Acknowledgment

The research presented in this paper has been supported by the SPARKS project, funded by EU 7th Framework Programme (FP7/2007-2013, grant agreement no. 608224). (www.project-sparks.eu).

References

[1] ICS-CERT, "ICS focuses malware (update A)," ICS-ALERT-14-176-02A, June 2014.

[2] ICS-CERT, "Ongoing sophisticated malware campaign compromising ICS (update B)," ICS-ALERT-14-281-01B, December 2014.

[3] Bundesamt für Sicherheit in der Information (BSI), "Die Lage der IT-sicherheit in Deutschland 2014," November 2014.

[4] R.E. Mackiewicz, "Overview of IEC 61850 and benefits," in Proc. IEE Power Systems Conference and Exposition (PSCE), pp. 623-630, 2006.

[5] M. Robinson, "The SCADA threat landscape," in Proc. first International Symposium for ICS & SADA Cyber Security Research, pp. 30-41, September 2013.

[6] T.H. Morris and W. Gao, "Industrial control system cyber attacks," in Proc. first Internation Symposium for ICS & SCADA Cyber Security Research, pp. 22-29, September 2013.

[7] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E.G. Im, Z.Q. Yao, B. Pranggono, H.F. Wang, "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems,", in Proc. International Conference on Sustainable Power Generation and Supply (SUPERGEN), pp. 1-8, 2012.

[8] W. Gao, T. Morris, B. Reaves, D. Richey, "On SCADA control system command and response injection and intrusion detection,", eCrime Researchers Summit (eCrime), pp. 1-9, 2010.

[9] J. Hoyos, M. Dehus, T.X. Brown, "Exploiting the GOOSE protocl: a practical attack on cyber-infrastructgure," GC'12 Workshop: Smart Grid Communication: Design for Performance, 2012.

[10] N. Kush, E. Ahmed, M. Branagan, E. Foo, "Poisoned GOOSE: exploiting the GOOSE prtocol," ACSW-AISC 2014, Auckland, New Zealand, January 2014.

[11] J. Hong, C. Liu, M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," IEEE Transactions on Smart Grid, vol.5, no.4, pp. 1643-1653, 2014.

[12] J.T. Sorensen and M.G. Jaatun, "An analysis of the manufacturing messaging specification protocol," in Proc. 5th Internation Conference on Ubiquitous Intelligence in Computing, Oslo, Norway, June 2008.

[13] P. Maynard, K. McLaughlin, B. Haberler, "Towards understanding man-in-the-middle attacks on IEC 60870-5-104 SCADA networks," in Proc. 2nd Internation Symposium for ICS & SCADA Cyber Security Research, 2014.

[14] R. Bründlinger, T. Strasser, G. Lauss, A. Hoke, S. Chakraborty, G. Martin, B. Kroposki, J. Johnson, E. de Jong, "Lab tests: verifying that smart grid power converters are truly smart," IEEE Power and Energy Magazine, vol. 13, no. 2, pp. 30-42, 2015.

[15] R. Zurawski, "The industrial information technology handbook," CRC Press, 2004.

[16] National Electric Sector Cybersecurity Organization Resource (NESCOR), "Electric sector failure scenarios and impact analyses version 1.0," Technical Paper, Electric Power Research Institute (EPRI), September 2013.

[17] Union for the Co-ordination of Tranmission of Electricity (UCTE), "Final report system disturbance on 4 November 2006," 2007

[18] A. Gaviano, K. Weber, C. Dirmeier, "Challenges and integration of PV and wind energy facilities from a smart grid point of view," Energy Procedia, vol. 25, pp. 118-125, 2012.

[19] F. Andren, R. Bründlinger, T. Strasser, "IEC 61850/61499 control of distributed energy resources: concept, guidelines, and implementation," IEEE Transactions on Energy Conversion, vol. 29, no. 4, pp. 1008-1017, 2014.

[20] F. Cleveland, "IEC 62351 security standards for the power system information infrastructure," IEC TC57 WG15 Security Standards ver 14, June 2012.

[21] IEC TS 62351-4, "Power systems management and associated information exchange Data and communications security, Part 4: profiles including MMS," June 2007.

[22] M.M.R. Chowdhury, H. Raddatz, J.E.Y. Rossebo, "Challenges when securing manufacturing message service in legacy industrial control system," IEEE Emerging Technology and Factory Automation, 2014.