How to hack an IEC 61850 system (or protect one)

Conference Paper · September 2017

CITATIONS
0

READS
545

1 author:

Dylan Jenkins
ABB
4 PUBLICATIONS **13** CITATIONS

SEE PROFILE

PS1.117

Study Committee B5 Colloquium
September 11-15, 2017
Auckland, New Zealand

How to hack an IEC 61850 system (or protect one)

D. L. P. JENKINS
GE Grid Solutions
Germany

Summary

The threat of cyberattacks on power grids is no longer something that can be disregarded, and the challenge that this poses to IEC 61850 systems in particular presents unique difficulties. To demonstrate how vulnerable these systems are when they are not properly designed or maintained, a mock attack is presented using publicly available hacking tools on various unidentified typical IEC 61850 Intelligent Electronic Devices (IEDs).

The purpose of this exercise is not to actually enable such an attack to occur, but rather to highlight how easy one can be. In fact, the methods that are described are quite unsophisticated, already published in the public domain and indeed already in the hands of would-be attackers.

Many of us have a good understanding of protection and control systems but can consider cybersecurity somewhat of a “black art” that belongs more to the information technology domain. We know that cyber risks exist, but may not necessarily understand how hackers exploit systems and carry out attacks. By showing specifically how a hack on an IEC 61850 based system is performed we can better understand how to defend ourselves against one in the real world, including what countermeasures and processes make such attacks more difficult.

In this example the hacker carries out his[1] attack in the following distinct stages:

1. Reconnaissance:
Here the attacker seeks to gather information on the target system. The ultimate aim is to identify a way to gain access to the substation network and to understand what elements compose the IEC 61850 system. Several technologies and tools are available for this purpose and the attacker may also employ what is known as social engineering: a method of psychological manipulation of employees belonging to the electric utility to have them divulge confidential information or perform actions on the target system.

2. Exploiting Vulnerabilities:
Once inside the target system, the hacker must identify a way of achieving the objective: to cause an outage in the substation and prevent the utility from restoring supply for as long as possible. To do this the hacker will exploit one or more vulnerabilities.
Specific exploit examples that are used in this example attack are:

[1] For the sake of readability, the masculine singular is used in this paper. In reality many hackers do not to act alone but rather in groups [1].

- Manipulating IEC 61850 MMS communication using “man-in-the-middle” attacks
- Injecting ‘spoof’ GOOSE messages into the system
- Corrupting configuration files in protection and control devices

Commonly used tools to carry out such vulnerability exploits attacks are discussed.

3. Covering Tracks:

After successfully carrying out the attack, the hacker will try to destroy any evidence that can be used to be tracked down and caught. This will include erasing traces of activity before and after the attack such as log files.

Countermeasures and best-practices are described that detail what we can do to prevent the attacker from exploiting our system.

Keywords

Cybersecurity, IEC 61850, Digital substations, substation communication networks.

1. Introduction

In this hypothetical attack a hacker seeks to cause a high profile power outage in order to promote his political agenda.

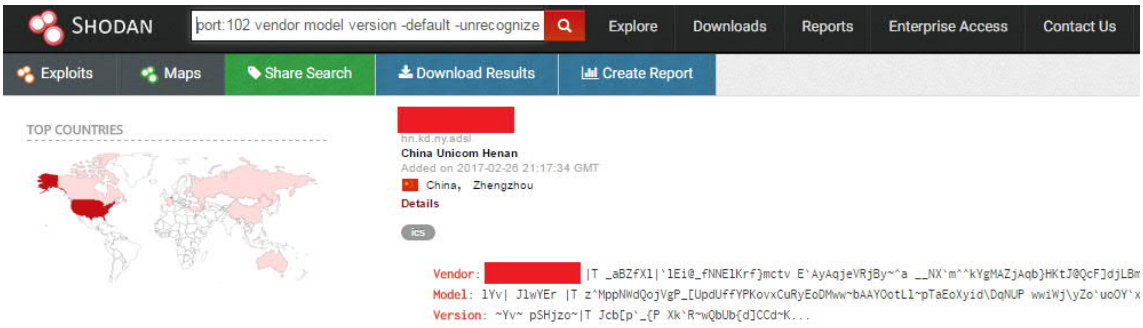
All systems, no matter how well designed can have what are known as called security vulnerabilities. These vulnerabilities may be publicly known[2] or they may be undocumented, in which case they are often referred to “zero day” vulnerabilities. A hacker may use his skills to discover vulnerabilities himself, or he may simply buy them from other security researches. Some publicly available software tools make use of these exploits as a sort of “Hacker Toolkit” an example of which is MetaSploit[3] that supports freely available software to hack SCADA equipment with little technical expertise.

To exploit the substation IEC 61850 based system in this example attack, the hacker will take advantage of some of the inherent vulnerabilities within the standard’s communication protocols, specifically their lack of authentication. Authentication is defined as being able to verify the source of a message, this is important in a security context as without it an attacker can manipulate devices by sending specially crafted messages that may look legitimate, but cause unwanted behaviour.

2. Reconnaissance and breaking in

The hacker searches for a substation that is connected to the internet[4], he finds one using a search engine called SHODAN[5] which can be used to scan for internet connected devices. The identified substation has this connection unbeknownst to the utility (a technician has installed an unauthorised cellular modem to allow for downloading of log files remotely).

[2] See: https://ics-cert.us-cert.gov/advisories
[3] See: https://scadahacker.com/resources/msf-scada.html for examples
[4] We make this simplification in order to focus on IEC 61850 vulnerabilities, if no internet connection is available then the hacker must first break into the utility SCADA network – a much more difficult yet not impossible task.
[5] See: https://www.shodan.io/explore/category/industrial-control-systems



Search using SHODAN showing an internet facing IEC 61850 device (connection details erased)

Before accessing the substation, the attacker employs a technique known as social engineering to manipulate employees to provide documentation files relating to the substation he wishes to attack. After a quick internet search, he finds the name of an engineer responsible for substation maintenance on a list of attendees at a recent technical conference. The engineer is called and the hacker pretends to work for a local design consultancy in need of project documentation. The utility engineer in response, who is convinced by the fake story, wilfully sends the hacker the information that he requires, unaware that this has the potential to cause harm. The hacker receives information and files required for the next stage of the attack including system communication architecture, lists of devices installed at the substation, and the substation IEC 61850 SCL configuration files.

The hacker now quietly infects an engineering workstation that is directly connected to the substation Local Area Network with the Trojans and tools he needs to carry out his attack.

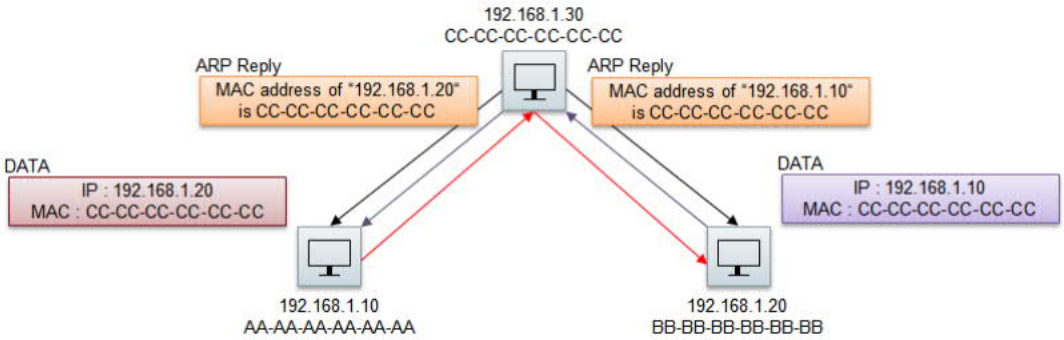
3. Carry out the attack

- MMS protocol “man in the middle” attack

In the first stage a “man in the middle attack” is performed. The objective is to trick the IEC 61850 Client into thinking that it is communicating directly to an IED (an IEC 61850 server) when in reality is communicating via our hijacked workstation. We do this to fool the network operator: they will be unaware that an attack has occurred as all the voltages, currents and switch-gear position values for the attacked bay will be reported as normal, even if in reality the feeder has been tripped.

To implement this attack a tool called Ettercap[6] is used and a process known as ARP poisoning is implemented. ARP is a protocol used by devices on a local area network to determine what MAC address belongs to a specific IP address. The hacker sends poisoned ARP messages to both the IEC 61850 server (a feeder management IED for a bay which reports measurements and switchgear position) and the IEC 61850 client (the substation gateway in this example). Both devices then update the values stored in their memory for MAC addresses associated for each other’s IP address to that of the compromised engineering workstation. Now whenever the client and server try to communicate to each other they will actually send their messages to this workstation which can then modify and relay the messages [2].

[6] See: http://ettercap.sourceforge.net/downloads.html



ARP spoof attack on a IEC 61850 system, as demonstrated by P. McLaughlin et al. [2]

Before relaying MMS reports from the IED to the substation gateway, the compromised workstation modifies the parts of the MMS messages relating to voltage, current and circuit breaker status to that of normal values, so that the utility will have no knowledge of any attack that occurs. Any control commands to the target IED XCBR logical node will also be modified so the client is unable to remotely close the circuit breaker once it has been opened.

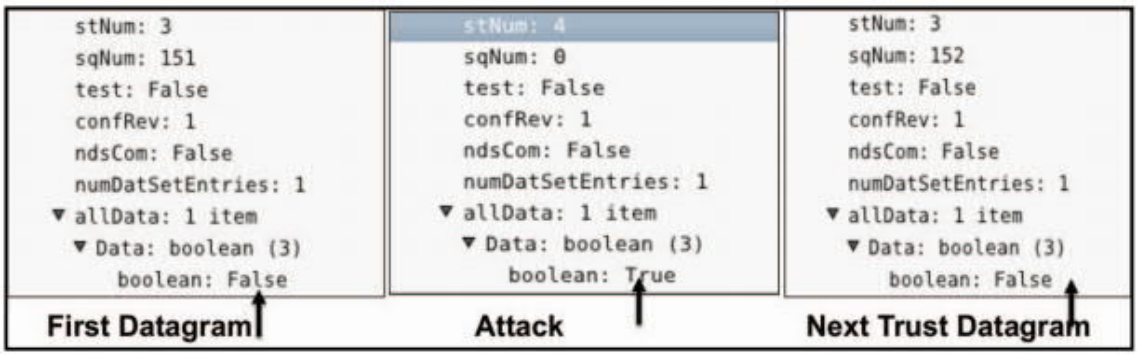
- GOOSE spoof attack to trip feeder circuit breaker

Next, the hacker crafts a spoof GOOSE message using a tool called Scapy[7] that will be used to deliberately trip a feeder circuit breaker and cause a power outage.

By studying the substation design documentation and the IEC 61850 SSD file that was obtained during the reconnaissance phase, the hacker knows that this particular substation implements process bus based tripping between the feeder IEDs and the switchgear control units using GOOSE which he can compromise in order to attack the substation.

Within the substation SCD file the hacker searches for the GOOSE message containing the signal for the protection tripping signal (PTRC.ST.Tr) in its dataset, that is subscribed to by the device associated with the circuit breaker (XCBR). Upon inspection of the in the relevant CID file, the hacker finds the position within the dataset of the GOOSE message for this signal. By sending a spoof GOOSE message with the Boolean value of this data item set to “true” the subscribing switchgear control unit will thus trip its circuit breaker.

Before sending the spoof message however, the hacker’s application employs a script that monitors the publishing IED, so that the message contains the correct MAC source as well as StNum and StVal values that are in the correct sequence. This ensures that any consistency checks that are performed by the subscribing IED are defeated, there is absolutely no way for the subscriber to know that the message is from an illegitimate source [3].



GOOSE exploit attack as demonstrated by J. Hoyos et al. [3]

[7] See: http://www.secdev.org/projects/scapy/

Due to the previous man in the middle attack, the SCADA system is completely unaware that an attack has occurred. The IEC 61850 clients receive compromised reports, indicating that all voltage and current measurements are normal and that the circuit breaker is still in the closed position, when it is in fact open and power to the feeder has been disconnected.

- Covering Tracks

In order to prolong the outage for as long as possible the hacker now sends compromised configuration files to the protection and control devices. For example, the overcurrent pickup setting thresholds are lowered to 0.01Inom. This is easily performed because although the IEDs in the substation are password protected, the utility has left these in their default values. Corrupting the protection settings prolongs the outage for as long as possible, since even if an operator tries to manually close the circuit breaker at the substation, the protection relay will trip immediately as the load current will exceed the pick-up threshold value. The protection relay will need to have its configuration updated, or be taken out of service completely before the circuit can be re-energised. A process that may take several hours due to confusion that have been caused.

With the attack completed the hacker tries to erase the IED event logs (many vendors prevent this action for this very reason) or instead flood the IED log with trivial events, such as LED/target reset commands, until the IED's memory reaches its capacity and the events of the actual attack are overwritten.

4. Conclusions - what could have prevented the attack?

This paper has examined some specific exploits based on the lack of inherent authentication in the IEC 61850 standard. These issues are already well known within the industry and are existing counter-measures that a utility may use to make this type of attack more difficult. In addition, there are new security standards that supplement IEC 61850 its most basic form to provide more effective security.

- NERC CIP for secure internal processes

The North American Electric Reliability Corporation Critical Infrastructure Protection plan (NERC CIP) provides an in depth set of standards to secure the internal processes within a utility. Although the legal requirements are stipulated for North America only, if followed, this standard would have provided secure internal processes and have made it much harder for the hacker to use social engineering to manipulate the utility's employees.

For instance, cyber security would have been taught to relevant personnel and in doing so the utility employee in question would have known to never send internal project documentation to an external party without authorisation (requirement CIP-004-6). The documents should have been classified as 'Sensitive Information' and stipulated that an authorisation process to be followed before this information was disclosed

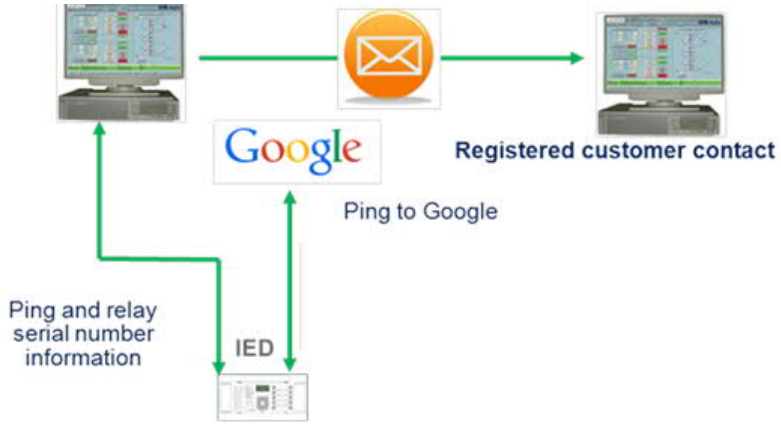
- Intrusion detection

An intrusion detection system can detect abnormal conditions on the substation network that could indicate that a cyber-attack is being performed and respond by notifying the utility. An intrusion detection system, for example could have detected that the hacker was sending poisoned ARP messages on the substation network.

- Internet facing detection

This countermeasure would have detected that an unauthorised connection had been established between the substation to the internet, exposing the substation to an attack, which provided the hacker an easy access point into the network. Had the substation not been internet facing, the attack would have certainly still been possible, but would have required that first the utility SCADA network was breached – a much more difficult task.

The internet facing detection system works by configuring IEDs to send a request (e.g. a ping request) at regular intervals to a host with a fixed internet protocol address (such as 8.8.8.8 for host: google-public-dns-a.google.com) or a predefined server that has been created for this purpose. If a response to the request is received from either the fixed IP address or the server, an alarm notification is raised by the IED and in the case of detection by the server, a message can also be sent to a registered contact at the electric utility.



Internet facing detection

- Authentication of GOOSE and MMS via IEC 62351

The standard IEC 62351 seeks address many of the vulnerabilities within IEC 61850. Because performance is critical in some GOOSE applications the standard specifies authentication of messages only rather than full encryption due to the processing time that would be involved. This means that the receiving IED can verify who has sent the message, thus thwarting the vulnerability was used by the hacker in our example attack.

Authentication is achieved by extending the GOOSE PDU to include an authentication value where the sender can encode a digital signature. The receiver is able to verify that the signature using a public encryption key. The hacker in our example would not be able to generate this signature without access to the sender's secret private encryption key.

In addition to GOOSE authentication the standard IEC 62351, once fully supported by vendors, will offer encryption of client-server communication. Encryption of the sort specified by this standard inherently provides authentication of messages and limits the type of "man in the middle" attack that we have described since the encrypted traffic cannot be modified by a hacker without possession of the MMS server's private encryption key. Any modification of the encrypted message would destroy the integrity of the message, making it totally unusable by the MMS client.

Bibliography

[1]. Snow, G. M. "Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism" 2011 Washington, D.C.

[2]. Kang, B., Maynard, P., McLaughlin, K., Sezer, S., Andrén, F., Seitl, C., ... Strasser, T. "Investigating Cyber-Physical Attacks against IEC 61850 Photovoltaic Inverter Installations." Proceedings of IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA). (pp. 1-8). 2015, Luxembourg.

[3]. Hoyos, J., Dehus, M., Brown, T.X. - "Exploiting the GOOSE Protocol: A Practical Attack on Cyber-infrastructure". GC'12 Workshop: Smart Grid Communications: Design for Performance 2012