Conference on Information Technology and Data Science

Attacking IEC 60870-5-104 Protocol*

Péter György, Tamás Holczer

CrySyS Lab, Department of Networked Systems and Services,
Budapest University of Technology and Economics
pgyorgy@crysys.hu
holczer@crysys.hu

Proceedings of the 1st Conference on Information Technology and Data Science
Debrecen, Hungary, November 6–8, 2020
published at http://ceur-ws.org

Abstract

IEC 60870-5-104 is a widely used protocol for telecontrol in European power systems. Despite its wide usage, security was not a priority when the protocol was created in 2000. The IEC-104 protocol lacks important security features such as encryption, integrity protection, or authentication. In this paper, our goal is to show the risks of using this insecure protocol. To demonstrate it, we designed and implemented a wide range of different attacks. We also rated the stealthiness of these attacks in order to show that detection of an intruder is not always obvious. Our stealthy and successful attacks were carried out in a test environment with several virtual machines running an open-source implementation of the protocol.

Keywords: IEC-104, attack, security, power grid

1. Introduction

IEC 60870-5-104 (a.k.a IEC-104) is part of the IEC 60870 set of standards [1]. IEC 60870 defines how telecontrol systems work in power transmission and control applications.

*This work was partially performed in the frame of the FIEK_16-1-2016-0007 project, implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the FIEK_16 funding scheme.

IEC 60870-5-101 (a.k.a IEC-101) is a standard for power system monitoring, control, and associated communications for telecontrol, teleprotection, and associated telecommunications for electric power systems. IEC-104 protocol is an extension of the IEC-101 protocol with the changes in transport, network, link, and physical layer services to suit the complete network access. The standard uses TCP/IP. The application layer of IEC-104 is preserved the same as that of IEC-101 with some of the data types and facilities not used.

The security of IEC 104, by design, has been proven to be problematic. Though the IEC technical committee has published a security standard IEC 62351, which implements end-to-end encryption which would prevent such attacks as a replay, man-in-the-middle (MitM), and packet injection. Unfortunately, due to the increase in complexity vendors are reluctant to roll this out on their networks. The insecure IEC 104 designed in the '90s is still used widespread in European power systems.

In this paper, our goal was to show the possible consequences of using an insecure protocol with known flaws.

The remainder of this paper is organized as follows. Section 2 provides a brief introduction to the IEC-104 protocol. Section 3 presents the overview of already existing attacks against the protocol. Section 4 describes the architecture of our simulator. In Section 5 the attack scenarios are described in detail. In Section 6 the attacks are evaluated. Finally, in Section 7 we summarize our work.

2. IEC 60870-5-104

As we have mentioned earlier IEC-104 is widely used for telecontrolling in Europe. DNP3 is used for the same purpose in North America. This paper focuses on the former protocol. IEC-104 follows the client-server architecture. The protocol has 2 message types APCI (Application Protocol Control Information) and ASDU (Application Service Data Unit). In the following, we will give a brief overview of these message types, to make understanding of the attacks easier. An in-depth analysis of IEC-104 was published by Petr Matoušek [5], which describes the protocol in more detail.

2.1. Application Protocol Control Information

Each APCI (Application Protocol Control Information) starts with a start byte with value 0x68 followed by the 8-bit length of APDU (Application Protocol Data Unit) and four 8-bit control fields(CF). APDU contains an APCI or an APCI with ASDU. Generally, the length of the APCI is 6 bytes.

The frame format is determined by the two last bits of the first control field. The standard defines three frame formats, I-format, U-format, and S-format. The S and I format stores the sequence numbers about the messages sent. If this counter is invalid then the connection is terminated, this behaviour will be used in one of the attacks. Figure 1 shows the structure of different frames.

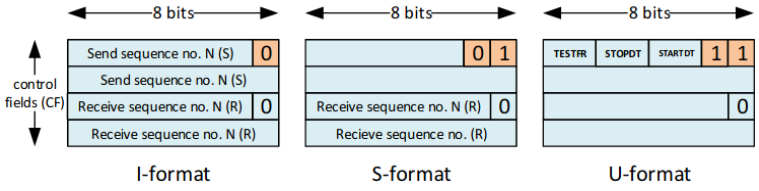

Figure 1. The frame formats of APCI.

2.2. Application Service Data Unit

The ASDU contains two main sections: the data unit identifier and the data itself. It starts with a type of identification, which specifies the command. It also stores the address of the originator. The information object address and the information element (value).

The information object address (IOA) is used as a selector, this specifies which object we need to interact with. It is a 3 bytes long address. The information element is a 2-byte long integer value, it stores the value of the IOA.

There are 127 different messages used in IEC-104. There are commands for both monitoring and controlling. When a server receives a command from the client, it responds with the values requested by the client or by an acknowledgment. Figure 2 shows the structure of the ASDU.

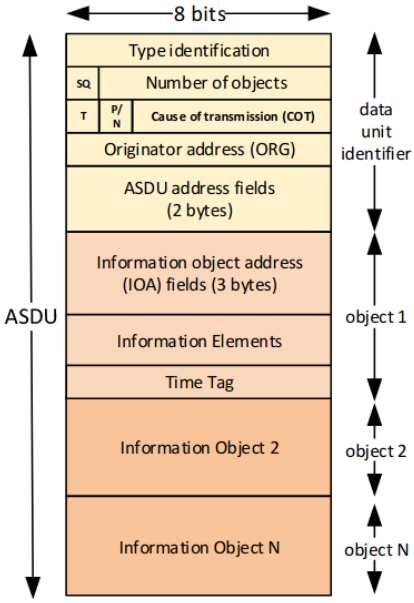

Figure 2. The structure of ASDU.

The APCI lacks integrity protection therefore tampering with the packet will

not be noticed by the communicating parties. The lack of integrity protection will be abused by several attacks described in Section 5.

3. State of the Art

The security of power systems is a well-researched topic [4, 11]. The security of IEC-104 lead to numerous publications. There are papers about attacking the protocol, hardening the protocol, and detecting attacks in networks where IEC-104 is used.

3.1. Flaws of the Protocol

Numerous flaws are described in [9]. The authors of the paper tried DoS attacks and exploited the lack of authentication of the IEC-104 protocol. They also successfully carried out a MitM attack where they could isolate the PLC and the MTU by dropping packages.

A more in-depth attack is described in [8]. The writers of the paper simulated a complete attack from penetrating the SCADA to injecting packet in the IEC communication. They reset the original connection and initiated a persistent connection for the attacker.

A very detailed description of MitM attacks is presented in [6]. The creators of the paper tried packet replay attacks and packet modification attacks.

During our research we used techniques from the previously mentioned papers. The attacks described in these papers are fairly easy to detect because each of the attacks reset the TCP stream. We wanted to avoid detection therefore we used more stealthy methods to achieve full control over the power grid. Therefore, instead of restarting the TCP stream like the authors of the mentioned papers, we achieved the MitM position without terminating the original connection. This method is far harder to notice since no log messages were generated by the communicating parties unlike the attacks described in the mentioned papers.

Before introducing our attack toolkit, we introduce the testbed we used in our work.

4. Architecture of the Testbed

To test the security aspects of IEC-104, we required an implementation of the protocol. The possible candidates were the following.

- MasterOPC - IEC-104 [7]
- OpenMUC - IEC-104 [2]
- FreyrSCADA - IEC-104 [3]

Out of the three candidates, we decided to work with the OpenMUC implementation of the protocol. The main reason behind the decision was that the implementation is open-source and it was written in Java, therefore it can be customized to fit our needs.

As we have mentioned earlier in Section 2 the protocol follows the client-server architecture. Therefore we need two machines, one of them for the client and the other one for the server. We also wanted to test MitM attacks, therefore we put in a router machine between the client and the server. The machines were virtualized in vCenter. The network architecture is presented in Figure 3.

We assume that the attacker already penetrated the network where IEC-104 is used, but neither the servers nor the clients are exploited. The attacker is present in the network with a device which can put itself in the middle of the communication. This kind of attacks are well known from the past, thus not described in this paper. The interested reader can understand the basics of such attacks from various sources such as [10].

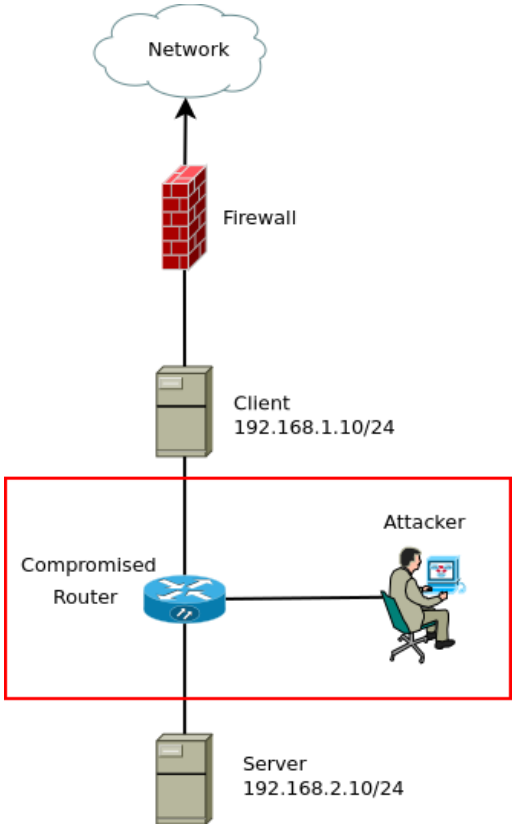

Figure 3. IEC Network where attacker is inside.

We designed a small power grid with a few stations. This grid was controlled by the IEC client. The topology of the grid is presented in Figure 4.

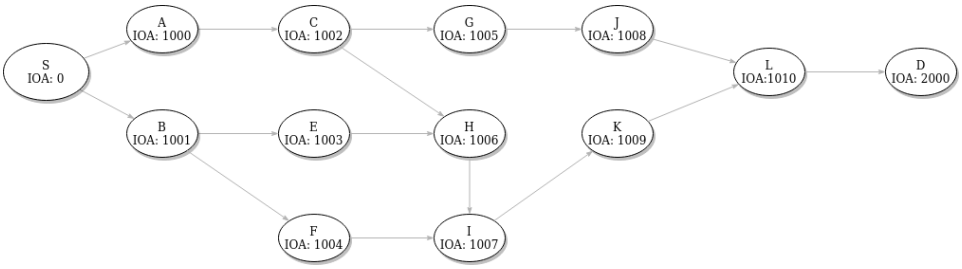

Figure 4. The topology of the stations.

The client periodically sends control commands to the server to generate network traffic.

For better visualization, we created a small web app, that holds the value of each station, the app is presented in Figure 5.

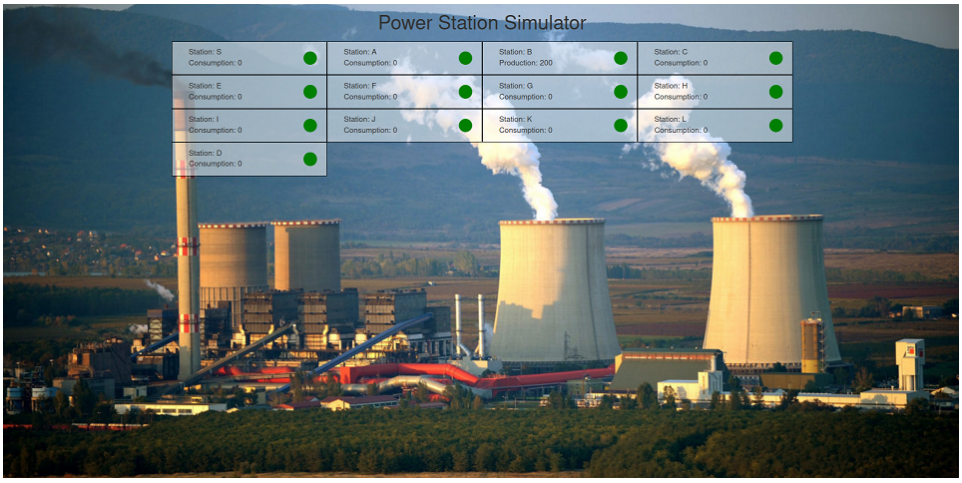

Figure 5. The visualization of the stations.

As the main components of the test environment is introduced, we may proceed to the attacks against the protocol.

5. Attacking the Protocol

In this section, we introduce the attacks. The attacks we designed vary in severity and complexity. We will start with simple attacks, and move forward to more complex scenarios.

5.1. Unauthorized Access

The protocol lacks authentication therefore an attacker can connect to a server and send commands. For example, an attacker could send an interrogation command to learn the IOAs used by the server. The steps of the attacks are the following:

- Discover the IP address and port of the IEC Server.
- The attacker has to impersonate an IEC Client and send a connection request to the IEC Server.
- Since the protocol lacks authentication, the connection request of the attacker will be accepted.
- The attacker can send arbitrary commands to the IEC Server.

Figure 6 shows the output of the IEC Server.

```
A client has connected using TCP/IP. Will listen for a StartDT request. Connection ID: 2
Started data transfer on connection (2) Will listen for incoming commands.
```

Figure 6. The log messages of the IEC Server.

As it is shown in Figure 6 the IEC Server logs every connection, therefore it is fairly easy for an operator to detect unauthorized access attacks if log analysis is done properly.

5.2. Tampering with IEC APCI Sequence Numbers

An unexpected sequence number in the APCI field of the packet results in the termination of the connection. This behavior can be used to cause Denial of Service (DoS). An attacker with Man in the Middle (MitM) capabilities can exploit this behavior using the following steps:

- Pass the routing of packets to a user space program. For example, use NetfilterQueue[1]
- Capture a packet
- Modify the sequence number of the IEC APCI
- Recalculate TCP checksum and modify it
- Release the packet

[1] `https://www.netfilter.org/projects/libnetfilter_queue/doxygen/html/`

Figure 7 shows the output of the IEC Server.

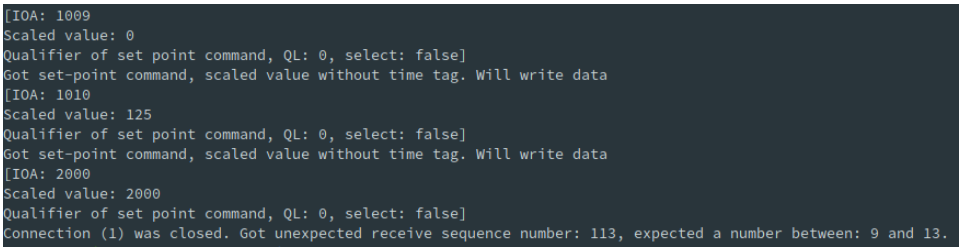

Figure 7. The log messages of the IEC Server.

As it is shown in Figure 7 the IEC Server logs the unexpected sequence number, therefore it is fairly easy for an operator to detect this attack.

5.3. Poison TCP Stream

The communication between the server and the client is carried out in a single TCP stream which is constantly kept alive. If the attacker can modify or insert a packet with an incorrect TCP sequence number, or send a FIN while impersonating a valid party, then the communication is terminated. This behavior can be used to cause DoS. An attacker with MitM capabilities can exploit this behavior using the following steps:

- Pass the routing of packets to a user space program. For example, use NetfilterQueue
- Capture a packet
- Modify the TCP sequence number and acknowledgment number
- Recalculate TCP checksum and modify it
- Release the packet

Figure 8 shows the output of the IEC Server.

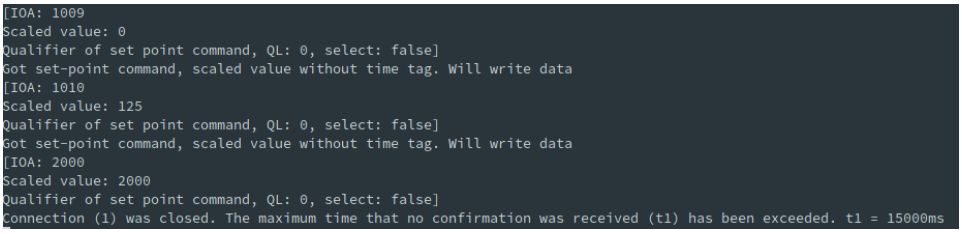

Figure 8. The log messages of the IEC Server.

As it is shown in Figure 8 the IEC Server logs the loss of connection but does not log the reason, therefore it is much harder for an operator to detect this attack.

5.4. Packet Injection

An attacker can inject packets to the communication, however simply injecting a packet will result in the termination of the connection, because it will cause a sequence number (both APCI and TCP) miss-match between the server and the client. Therefore after injecting a packet the attacker needs to patch the sequence number of every other packet. Not just the sequence number can be modified but also the values of the ASDU field. Therefore, this can lead to taking over the control of the power grid. An attacker needs to be in a MitM position to carry out this attack. The steps of the attack are the following:

- Pass the routing of packets to a user space program. For example, use NetfilterQueue.
- Read every packet that passes through and learns the TCP and IEC sequence numbers (Learning Phase).
- As the attacker learned every sequence number he can inject a new packet to the communication (Inject Phase).
- Keep track of the sequence numbers using sequence number offsets.
- Capture every other packet and patch the sequence numbers so the connection will not terminate due to incorrect sequence numbers (Patch Phase).

Figure 9 shows the visual representation of the attack, it is important to note that in "Patch Phase" the attacker has to correct the sequence number, to avoid termination of connection and therefore be detected.

This attack is much harder to detect because the connection is not terminated. The attacker can spoof the values that are seen by the operator, which makes detecting even harder.

6. Evaluation

The difficulty of detection and the severity of the attacks described in Section 5 is different.

The attack described in Section 5.1 has a very high severity because the attacker can send arbitrary commands to the server. The attack does not require a skilled attacker, which makes it even more dangerous. The operator and the attacker are simultaneously controlling the stations. New connections are logged by the server therefore it is easy to detect this attack.

The attacks described in Section 5.2 and 5.3 are similar. The severity of these attacks is medium because they can prevent the client from controlling the server.

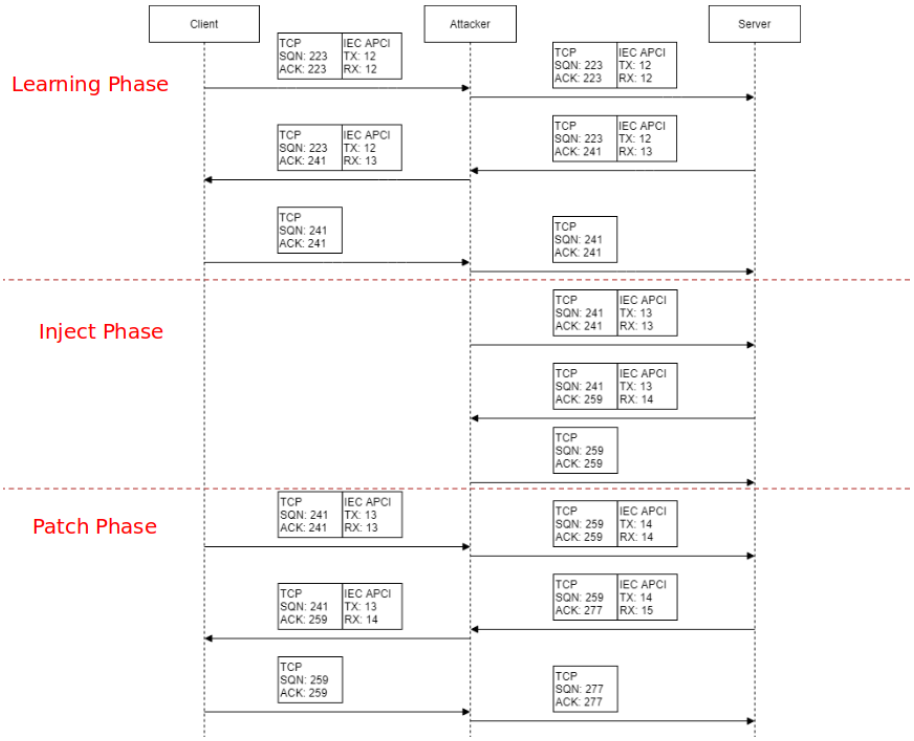

Figure 9. Flow of the packet injection attack.

However, these attacks can be used combined with the attack described in Section 5.1 to hinder the operator even more.

The attack described in section 5.4 has a critical severity because the attacker can send arbitrary commands and can also stop the client from communicating with the server. The attacker can also spoof values for the client, to make the operator believe everything is working properly. No log message is generated during this attack, therefore the detection is also hard.

7. Summary and Future Works

We created numerous attacks against the IEC-104 protocol. Our goal was to show that even an attacker with limited skills can cause severe damage in a network where an insecure protocol is used. The possible consequences can range from DoS attack to complete takeover of the power grid.

In our opinion, it worth the extra complexity to switch to the secure variant of the protocol because using the insecure version can lead to unnecessary harmful events.

If an attacker wants to get full control over the grid, he also requires the IOA and Station ID pairs. Without the pairs, the attacker can just blindly send control and monitor command to the IOAs, without exactly knowing what he is doing. With the pairing, the attacker can precisely target his commands to manipulate the power grid in his own will. To achieve a full control attack scenario we are working on an algorithm that can pair the Station IDs to the corresponding IOAs.

The attacks which are introduced in this paper were carried out in a simulator. We also want to test in a real-world environment in the near future.

Acknowledgements. We want to thank Csatár János from BME VET for helping us with the simulator.

References

[1] IEC: *Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles (Second Edition)*, International Electrotechnical Commission, 2006.

[2] *IEC 60870-5-104*, `https://www.openmuc.org/iec-60870-5-104/`.

[3] *IEC 60870-5-104 Master Client Simulator*, `http://www.freyrscada.com/iec-60870-5-104-Client-Simulator.php`.

[4] W.-W. Li, W.-X. You, X.-P. Wang: *Survey of cyber security research in power system*, Power System Protection and Control 39.10 (2011), pp. 140–147.

[5] P. Matoušek: *Description and analysis of IEC 104 Protocol*, Faculty of Information Technology, Brno University of Technology, Tech. Rep (2017).

[6] P. Maynard, K. McLaughlin, B. Haberler: *Towards understanding man-in-the-middle attacks on iec 60870-5-104 scada networks*, in: 2nd International Symposium for ICS & SCADA Cyber Security Research 2014 (ICS-CSR 2014) 2, 2014, pp. 30–42.

[7] *OPC Client for IEC 60870-5-104*, `https://https://www.opcti.com/iec-60870-5-104-scada-master.aspx`.

[8] Q. S. Qassim, N. Jamil, M. Daud, N. Ja'affar, S. Yussof, R. Ismail, W. A. W. Kamarulzaman: *Simulating command injection attacks on iec 60870-5-104 protocol in scada system*, International Journal of Engineering & Technology 7.2.14 (2018), pp. 153–159.

[9] P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis, E. Panaousis: *Attacking IEC-60870-5-104 SCADA Systems*, in: 2019 IEEE World Congress on Services (SERVICES), vol. 2642, IEEE, 2019, pp. 41–46.

[10] T. M. Thomas, D. Stoddard: *Network Security First-Step*, Cisco Press, 2011.

[11] W. Wang, Z. Lu: *Cyber security in the smart grid: Survey and challenges*, Computer networks 57.5 (2013), pp. 1344–1371.