Gesellschaft für Informatik e.V. (GI) GI. (Hrsg.): INFORMATIK 2021,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021 1753

Secure OPC UA Server configuration for smart charging stations

Josef Schindler[1], Erkin Kirdan[2], Karl Waedt[3]

Abstract: Direct-To-Consumer (D2C) marketing recently gains popularity in society by bypassing unnecessary mediators and thus avoiding cost. In Information and Communication Technology (ICT) terms, it is comparable with Machine-To-Machine (M2M) communication overcoming additional mediators, i.e. remote servers. In this paper, we research M2M communication for battery boosted charging station. Therefore, we consider a setup comprising an OPC Unified Architecture (OPC UA) Client and OPC UA Server. The server represents the smart charging station, where the client can reserve time slots for charging sessions.

In this paper, we answer how to facilitate this using the different services provided by OPC UA. Additionally, we apply an OPC UA Metasploit module on two differently - according to the function manuals - configured OPC UA Servers. Afterwards, we validate the results.

Keywords: Machine-To-Machine; OPC Unified Architecture; cybersecurity; penetration testing; charging station

1 Introduction

In previous work [SWW19], we demonstrated the standardisation of OPC UA Server interfaces with OPC UA Namespaces. Therefore, we exemplary considered a boosted charging station. A battery helped to overcome insufficient electricity grid connection for high power charging there. Between two charging sessions, the power grid recharges the battery. That refreshes the battery so it can boost the following charging process. In figure 1, yellow arrows depict the power flows by pointing from one component to another. As can be seen, the grid connection is weak (thin line), while the power flow into the Electric Vehicle (EV) is greater. For reservation (customer), organisation (with nearby charging entities) and remote maintenance purposes, there is an OPC UA Server on-site, listening to OPC UA Clients (see figure 1).

According to Erba et al. [EMT21], a secure configuration is crucial, and a remarkable share of vendors do not provide explicit recommendation in their manuals for it. We want to

[1] Friedrich-Alexander-University (FAU) Erlangen-Nuremberg, Chair of Electrical Energy Systems (EES), Cauerstraße 4, 91058, Erlangen, Germany josef.s.schindler@fau.de
[2] Technical University Munich erkin.kirdan@tum.de
[3] Framatome GmbH, ICETA-G Department, Paul-Gossen-Straße 100, 91052, Erlangen, Germany karl.waedt@framatome.com

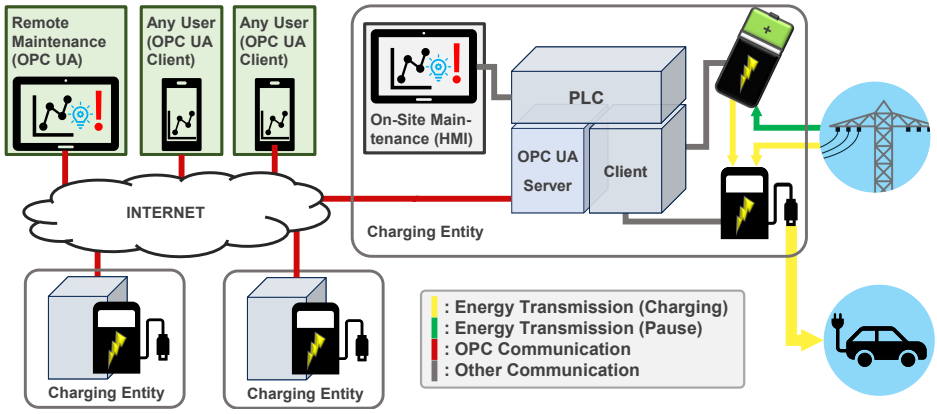

Fig. 1: system communication and power flow overview

look a little bit deeper into the security of Siemens' PLC platform, which is used widely in automation. Our contributions are:

1. Cybersecurity consideration of the boosted EV charger with reservation system (according to [SWW19])
2. A comparison of the manuals concerning OPC UA provided by Siemens [Si18, Si21] and their alignment with a secure configuration
3. Penetration test of the OPC UA Server hosted by the S7-1518 with Metasploit OPC UA-extension [Ro20]

In the following sections, we do a literature review (section 2). Next, in section 3, we depict the hardware configuration (subsection 3.1) and the penetration testing environment and setup (subsection 3.2). Sections 4 & 5 depict the results & conclusion, respectively.

2 Related Work

The security models of the four most commonly used open-source implementations are analyzed in [Mu20a]. According to the results, they comply with the standard's security model with a few vulnerabilities in 2 of the implementations. Furthermore, their scalability is compared for an increasing number of OPC UA Clients and nodes. Scalabilities vary considerably based on the programming language of the OPC UA stack. The same implementations are also analyzed in [Mu20b] with respect to their features and interoperability. According to the results, they can work together seamlessly being deployed as client and servers.

Erba et al. study practical challenges to configure OPC UA securely [EMT21]. Their results show considerable security deficiencies in the implementations that inevitably lead to insecure configurations and deployments.

Roepert et al. assess the security of OPC UA deployments in [Ro20]. As part of their work, they develop a Metasploit module for assisting network-based security assessments of OPC UA deployments. This module is also used to test our setup.

3 System Overview

3.1 Hardware Configuration

The OPC UA Server at the charging entity is reachable from the internet (see section 1 and figure 1). Therefore, a secure configuration is crucial, according to Erba et al. [EMT21]. Additionally, the authors attest Siemens to fail in guiding users to a secure PLC configuration with the OPC UA manual [Si18]. Indeed, Siemens does not give explicit recommendation for a secure configuration there. As users might not be punctual or have time issues, this could lead to weak configurations. Accordingly, one tested configuration is the default one:

- Security Policy: Basic256, Basic256Sha256 (both 'sign' or 'sign and encrypt'), but also None!
- Accept any client certificate!
- Guest authentication!

Recently, Siemens updated manuals dedicated to secure communication. One chapter dedicates to the OPC UA Server configuration and applies to the PLC S7 1518 [Si21]. Accordingly, we employed a second configuration:

- allow only signed and encrypted communication, algorithm: Basic256Sha256
- do not allow guest-authentication
- do not allow access to PLC tags and Data Block (DB) components
- use a specific set or list of trusted clients (certificates) on the PLC

3.2 Metasploit for OPC UA

We wanted to test different cybersecurity configurations for the OPC UA Server described in the previous subsection 3.1. A recently published module for Metasploit dedicates to OPC UA [Ra21, Ro20]. Roepert et al. outline four steps for the assessment of security, which are [Ro20]:

1. Discovery: searching for potential targets, i.e. OPC UA Servers
2. Authentication: testing for different weak authentication methods, such as anonymous, easy-to-know credentials or default credentials. Check whether the server accepts self-signed client certificates.
3. Configuration Check: Deriving OPC UA Server information & configuration
4. Vulnerability Check: Checking for potential exploits such as known Common Vulnerabilities and Exposures (CVE) or Denial-of-Service (DoS).

During our tests, we only performed phases 1-3 (see figure 2). The vulnerability check is out of scope. For phase 4, Roepert et al. refer to existing Metasploit exploits, too [Ro20].

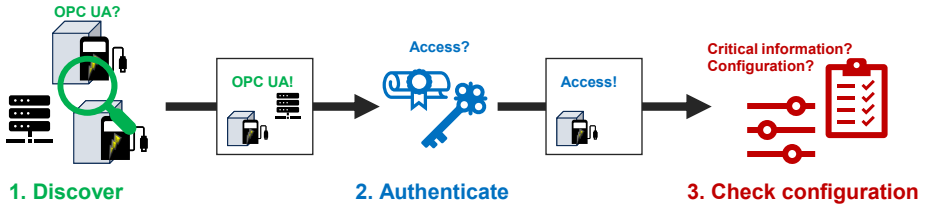

Fig. 2: Security assessment scheme for OPC UA Servers with three steps, according [Ro20]

4 Results

Table 1 depicts the test results for the different phases and configurations. As can be seen, the default configuration revealed information to potential attackers. A login was initially possible without providing credentials. Later on, during the configuration check, one could gather sensitive information. That includes read- and write-able nodes.

With the strict configuration according to the secure communication's manual [Si21], no login was possible. Consequently, no sensitive data could be derived from the OPC UA Server in this test.

5 Conclusion

In this research, we showed that a cyber-secure configuration for respective hardware is crucial. Differently than Erba et al. [EMT21] stated, there is secure guidance for Siemens PLC S7-1500 OPC UA Servers, but one has to look for and find it. That highlights the importance of dedicated policies and training for engineers configuring such hardware. The recently released Metasploit module for OPC UA provides a good option for configuration and penetration testing. Future research could focus on other implementations and vendors than the here considered one, too.

Tab. 1: Security assessment results for PLC S7-1518, with two different configurations

Phase	Configuration	
	Default	**According to security manuals** [Si21]
1. Discovery	Found server	Found server
2. Authentication	Login with empty credentials was possible	No login possible (no fitting credentials found and not possible with self-signed certificate)
3. Configuration	Revealed unencrypted communication (MessageSecurityMode: MessageSecurityMode.None_) Revealed all nodes, even writeable ones and those reserved for privileged users!	Login was not possible, hence no configuration could be derived

References

[EMT21] Erba, Alessandro; Müller, Anne; Tippenhauer, Nils Ole: Practical Pitfalls for Security in OPC UA. arXiv preprint arXiv:2104.06051, 4 2021.

[Mu20a] Muehlbauer, Nikolas; Kirdan, Erkin; Pahl, Marc-Oliver; Carle, Georg: Open-Source OPC UA Security and Scalability. In: 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). pp. 262–269, 2020.

[Mu20b] Muehlbauer, Nikolas; Kirdan, Erkin; Pahl, Marc-Oliver; Waedt, Karl: Feature-based Comparison of Open Source OPC-UA Implementations. GI-Jahrestagung, pp. 367–377, 2020.

[Ra21] Metasploit-framework. `https://github.com/rapid7/metasploit-framework`, Accessed: 2021-06-12.

[Ro20] Roepert, Linus; Dahlmanns, Markus; Fink, Ina Berenice; Pennekamp, Jan; Henze, Martin: Assessing the Security of OPC UA Deployments. In: Proceedings of the 1st ITG Workshop on IT Security (ITSec). 2020.

[Si18] Siemens AG: OPC UA .NET Client for the SIMATIC S7-1500 OPC UA Server. Function manual, Siemens AG, 02 2018.

[Si21] Siemens AG: S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro, ET 200eco PN Communication. Function manual, Siemens AG, 05 2021.

[SWW19] Schindler, Josef; Watson, Venesa; Waedt, Karl: Interoperability of fast charging station with battery booster. GI-Jahrestagung (Workshops), pp. 295–307, 2019.