Assessing the Security of OPC UA Deployments

Linus Roepert*, Markus Dahlmanns*, Ina Berenice Fink*, Jan Pennekamp*, Martin Henze‡
*Communication and Distributed Systems, RWTH Aachen University, Aachen, Germany, {lastname}@comsys.rwth-aachen.de
‡Cyber Analysis & Defense, Fraunhofer FKIE, Wachtberg, Germany, martin.henze@fkie.fraunhofer.de

***Abstract*—To address the increasing security demands of industrial deployments, OPC UA is one of the first industrial protocols explicitly designed with security in mind. However, deploying it securely requires a thorough configuration of a wide range of options. Thus, assessing the security of OPC UA deployments and their configuration is necessary to ensure secure operation, most importantly confidentiality and integrity of industrial processes. In this work, we present extensions to the popular Metasploit Framework to ease network-based security assessments of OPC UA deployments. To this end, we discuss methods to discover OPC UA servers, test their authentication, obtain their configuration, and check for vulnerabilities. Ultimately, our work enables operators to verify the (security) configuration of their systems and identify potential attack vectors.**

I. Introduction

Traditionally, industrial protocols, such as Modbus and Profinet, were designed to operate in isolated networks and thus provide little to no security functionality. However, the increasing interconnection of industrial processes [1] as well as serious security threats, e.g., evidenced by the cyberattack on a German steel mill or NotPetya [2], demand for *secure* industrial protocols. One prime candidate to fill this demand is OPC Unified Architecture (OPC UA) [3], a comparatively new protocol enabling standardized and secure communication across all levels from the field up to the cloud.

OPC UA has been explicitly designed with security in mind as attested by a security analysis performed on behalf of the German Federal Office for Information Security [4]. Still, OPC UA is not secure by default, requiring a thorough configuration [5]. OPC UA's inherent complexity and a wide range of deployment models make this setup a laborious and error-prone task. In fact, several setup instructions for OPC UA servers can result in insecure deployments [4], [6]. Consequently, a need for assessing the security of OPC UA deployments exists, e.g., when integrating them into industrial environments. This is especially crucial for deployments which are (un-)intentionally connected to the Internet, where several thousand probes are searching for exploitable deployments [7].

To aid in performing network-based security assessments of OPC UA deployments, we present approaches to (i) discover OPC UA servers in a network, (ii) test for anonymous, default, or weak login credentials, (iii) retrieve information on the server and security configuration as well as access rights, and (iv) test for susceptibility to certain known CVEs and other potential vulnerabilities. We integrate our tools into the widely used Metasploit Framework and release the source code[1].

[1]Available as open source at https://github.com/COMSYS/msf-opcua

II. OPC UA Security

OPC UA servers represent objects and their relationships as a set of nodes in an address space. To realize security, OPC UA provides authentication, authorization, as well as integrity and confidentiality protection [8]. For client authentication, OPC UA allows anonymous access, a combination of username and password, a certificate, or an authentication token. Furthermore, OPC UA servers can enforce access control for each node. Correct configuration of authentication is indispensable, e.g., restricting anonymous access to non-critical servers [5]. Besides, default credentials of manufacturers must be changed.

To secure communication, OPC UA provides different message security modes (no security, integrity only, or integrity and confidentiality) as well as security policies predefining cryptographic algorithms for encryption and signatures [8]. Depending on the message security mode, the client selects a security policy during the handshake to protect exchanged messages. Notably, out of the seven available security policies, one provides no security, and two have been deprecated because of now insecure underlying cryptographic primitives.

Overall, while OPC UA provides strong security features [4], correct configuration of these security mechanisms is essential. Otherwise, attackers might be able to access confidential data or compromise the OPC UA server.

III. Assessing Security of Industrial Deployments

The need to provide support for assessing the security of industrial deployments is emphasized by efforts for other industrial protocols. Most prominently, different respective modules for the Metasploit Framework are available [9], ranging from modules for specific PLCs, e.g., Schneider Modicon or Siemens S7, over SCADA software, e.g., Sielco Sistemi Winlog or Measuresoft ScadaPro, to industrial protocols, e.g., Modbus, Profinet, or IEC 60870-5-104. Furthermore, Masood et al. [10] recreated Stuxnet's attack vectors in Metasploit.

Consequently, Metasploit is widely used for security assessments in industrial settings, e.g., in the production line of a pharmaceutical company [11], to evaluate perimeter security effectiveness in supervisory and process control zones [12], or to test industrial firewalls of a natural gas compressor [13]. Likewise, NIST used Metasploit to assess the performance of industrial systems with security measures in place [14].

IV. OPC UA Security Assessment

While OPC UA promises a high security level, actually achieving a secure OPC UA deployment depends on correct

Authors' version of a paper accepted for publication in the proceedings of the 1st ITG Workshop on IT Security. Cite as: L. Roepert, M. Dahlmanns, I. B. Fink, J. Pennekamp, and M. Henze, "Assessing the Security of OPC UA Deployments", in *Proceedings of the 1st ITG Workshop on IT Security (ITSec)*, 2020.

manual configuration (cf. Section II). Ensuring this for (own) OPC UA deployments requires network-based security assessments. We use and extend the popular Metasploit Framework to aid in performing such tasks. As illustrated in Figure 1, such an assessment requires several sequential steps.

A. Discovery of OPC UA Servers

As the first step of a network-based security assessment, we need to discover OPC UA servers in a local network. By default, OPC UA uses TCP port 4840 for its binary protocol as well as TCP ports 80 (HTTP) and 443 (HTTPS) when acting as SOAP web service. We extended the network scan functionality of Metasploit by an OPC UA handshake to verify that the discovered devices run OPC UA on said ports, thus obtaining a list of servers for subsequent assessment steps.

B. Testing OPC UA Authentication & Login Credentials

Once an OPC UA server has been discovered, the next step is to test whether authentication is configured securely. OPC UA allows for different modes of authentication (cf. Section II). Out of these modes, especially anonymous access and the widely-used username/password authentication are prone to configuration errors. First, anonymous access (empty login credentials) might give away sensitive information on the server's configuration (see below) and imposes the risk of misconfigured access rights, leading to information leakage or even the risk of unauthorized write operations. Second, username/password-based logins come with the risk of default (documented in manuals) or weak (easily guessable) login credentials. To test for such problems, we added functionality to Metasploit to use the built-in `login_scanner` for OPC UA deployments. Furthermore, we created a list of OPC UA specific default credentials from openly accessible setup instructions and manuals. Following a similar route, we provide functionality to check whether the server accepts a self-signed client certificate without further validation.

C. Deriving OPC UA Server Information & Configuration

If login to an OPC UA server is possible (either anonymous, using username/password, or certificate-based), we can connect to said server to obtain security-related information using our extension of Metasploit. First, information on available and known OPC UA servers can be used to broaden the scope of the assessment (cf. Figure 1). Second, information such as `ApplicationUri` and `ProductUri` provide information on the used software and its version, easing the verification of patch policies and the check for potential vulnerabilities. Third, different security-related configurations can be assessed, e.g., the use of an appropriate `SecurityLevel`, `MessageSecurityMode` enforcing encryption, security policy specified by the `PolicyUri`, and `TokenType` for authentication (cf. Section II). Finally, iterating through the server namespace of readable and writable nodes allows to identify misconfigured permissions (especially for anonymous authentication). Combined, the information queryable after (anonymous) login to an OPC UA server allows to assess security of the underlying server configuration.

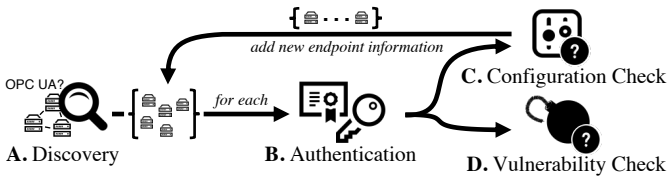

Fig. 1. Our approach for a network-based security assessment of OPC UA deployments (A) discovers OPC UA servers, (B) tests authentication, (C) derives server configuration, and (D) checks for vulnerabilities.

D. Checking for Potential Vulnerabilities

Besides configuration-based security assessment of an OPC UA deployment, we could actively test for susceptibility to known CVEs and other potential vulnerabilities. To this end, Metasploit allows to run exploits for specific CVEs against a server. Furthermore, some OPC UA servers (especially with anonymous access) are prone to a denial-of-service, i.e., attackers can exhaust the number of allowed active sessions.

V. Outlook & Conclusion

To assist operators of OPC UA deployments in performing security assessments, we presented a network-based approach specific to OPC UA and extended the Metasploit Framework accordingly. We verified our approach using both local test installations of different OPC UA implementations as well as public test servers. Currently, we are further extending our toolset, especially by integrating more vulnerability checks. In the future, we plan to validate our methods within industrial deployments and also cover other communication (e.g., publish/subscribe) and deployment (e.g., global discovery and proxy servers) paradigms. With our work, we empower operators of OPC UA deployments to verify the security configuration of their systems and detect potential weaknesses.

Acknowledgments: This work has partly been funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC-2023 Internet of Production – 390621612.

References

[1] J. Pennekamp *et al.*, "Towards an Infrastructure Enabling the Internet of Production," in *IEEE ICPS*, 2019.
[2] K. E. Hemsley and R. E. Fisher, "History of Industrial Control System Cyber Incidents," Tech. Rep. INL/CON-18-44411-Revision-2, 2018.
[3] OPC Foundation, "OPC Unified Architecture Specification – Part 1: Overview and Concepts," Version 1.04, 2017.
[4] Federal Office for Inform. Security, "OPC UA Security Analysis," 2017.
[5] OPC Foundation, "Practical Security Recommendations for building OPC UA Applications," Whitepaper, Version 3, 2018.
[6] C. Angeli *et al.*, "Secure implementation of OPC UA for operators, integrators and manufacturers," Plattform Industrie 4.0, 2018.
[7] C. Fachkha *et al.*, "Internet-scale Probing of CPS: Inference, Characterization and Orchestration Analysis," in *NDSS*, 2017.
[8] OPC Foundation, "OPC Unified Architecture Specification – Part 2: Security Model," Version 1.04, 2017.
[9] M. Caselli and F. Kargl, "A Security Assessment Methodology for Critical Infrastructures," in *CRITIS*, 2014.
[10] R. Masood *et al.*, "Stuxnet Worm Analysis in Metasploit," in *FIT*, 2011.
[11] F. Holik *et al.*, "Effective penetration testing with Metasploit framework and methodologies," in *IEEE CINTI*, 2014.
[12] M. Combs-Ford, "Security Assessment of Industrial Control Supervisory and Process Control Zones," in *SIGITE*, 2016.
[13] T. D. Nguyen *et al.*, "A Strategy for Security Testing Industrial Firewalls," in *ICSS*, 2019.
[14] R. Candell *et al.*, "An Industrial Control System Cybersecurity Performance Testbed," NISTIR 8089, 2015.