

Easing the Conscience with OPC UA: An Internet-Wide Study on Insecure Deployments

Markus Dahlmanns*, Johannes Lohmöller*, Ina Berenice Fink*,
Jan Pennekamp*, Klaus Wehrle*, Martin Henze[‡]

*Communication and Distributed Systems, RWTH Aachen University, Aachen, Germany

[‡]Cyber Analysis & Defense, Fraunhofer FKIE, Wachtberg, Germany

{dahlmanns, lohmoeller, fink, pennekamp, wehrle}@comsys.rwth-aachen.de · martin.henze@fkie.fraunhofer.de

ABSTRACT

Due to increasing digitalization, formerly isolated industrial networks, e.g., for factory and process automation, move closer and closer to the Internet, mandating secure communication. However, securely setting up OPC UA, the prime candidate for secure industrial communication, is challenging due to a large variety of insecure options. To study whether Internet-facing OPC UA appliances are configured securely, we actively scan the IPv4 address space for publicly reachable OPC UA systems and assess the security of their configurations. We observe problematic security configurations such as missing access control (on 24% of hosts), disabled security functionality (24%), or use of deprecated cryptographic primitives (25%) on in total 92% of the reachable deployments. Furthermore, we discover several hundred devices in multiple autonomous systems sharing the same security certificate, opening the door for impersonation attacks. Overall, in this paper, we highlight commonly found security misconfigurations and underline the importance of appropriate configuration for security-featuring protocols.

CCS CONCEPTS

• Networks → Security protocols; • Security and privacy → Security protocols;

KEYWORDS

industrial communication, network security, security configuration

ACM Reference Format:

Markus Dahlmanns, Johannes Lohmöller, Ina Berenice Fink, Jan Pennekamp, Klaus Wehrle, Martin Henze. 2020. Easing the Conscience with OPC UA: An Internet-Wide Study on Insecure Deployments. In *ACM Internet Measurement Conference (IMC '20)*, October 27–29, 2020, Virtual Event, USA. ACM, New York, NY, USA, 10 pages. <https://doi.org/10.1145/3419394.3423666>

1 INTRODUCTION

Industrial networks, e.g., used for factory and process automation, traditionally were designed as isolated networks with no connections to, e.g., office networks or the Internet [6, 44]. Consequently,

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

IMC '20, October 27–29, 2020, Virtual Event, USA

© 2020 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM ISBN 978-1-4503-8138-3/20/10...\$15.00

<https://doi.org/10.1145/3419394.3423666>

industrial protocols, such as Modbus or ProfiNet, do not implement any security functionality. However, with an increasing interconnection of industrial networks, serious security threats arise as evidenced by incidents such as NotPetya or manipulation attacks on several industrial devices [26]. These threats, coupled with an increase in industrial communication (e.g., driven by Industry 4.0), highlight the need for secure industrial protocols.

OPC UA, a comparatively new industrial protocol, released in 2008, was designed from scratch with security in mind [19] and is attested secure (e.g., by the German Federal Office for Information Security [19]). However, OPC UA requires an active configuration of numerous security settings, where incautious decisions lead to weakly or even unsecured systems. In industrial deployments, such configurations not only allow for well-known attacks, e.g., eavesdropping and theft of confidential data, but also facilitate to control production lines, cause physical damage, and harm humans [28]. Configuration recommendations [52], e.g., on the use of ciphers, attempt to confine the spread of insecure deployments.

However, until now, it is unclear whether system operators adhere to such security recommendations and therefore prevent unauthorized access to modern industrial deployments. In other domains, active Internet-wide scanning has proven to be a valuable and accepted method to perform this task [23, 31, 57, 61]. Likewise, different works identify the risks of Internet-connected industrial devices using legacy protocols without security functionality [3, 20, 44]. This motivates us to combine these two streams of research to analyze the security configurations of industrial deployments.

In this paper, we study whether Internet-connected OPC UA deployments and their configurations capitalize on the strong level of security theoretically provided by the underlying protocol design [19]. To this end, we actively scan the complete IPv4 address space for publicly reachable OPC UA systems and subsequently assess the security configurations of found deployments.

Contributions. Our main contributions are as follows.

- We perform weekly measurements of the complete IPv4 address space over seven months to detect OPC UA devices, which we can attribute to well-known industrial manufacturers and sectors, e.g., building automation and power systems.
- We assess the security configurations of Internet-facing OPC UA devices following official security guidelines and recommendations. Our results show that 92% of OPC UA systems are configured deficiently, e.g., due to missing access control, disabled security functionality, use of deprecated cryptographic primitives, or certificate reuse.
- We release our anonymized dataset [11] and our OPC UA extensions of `zgrab2` [9] to allow for reproducibility of our results.

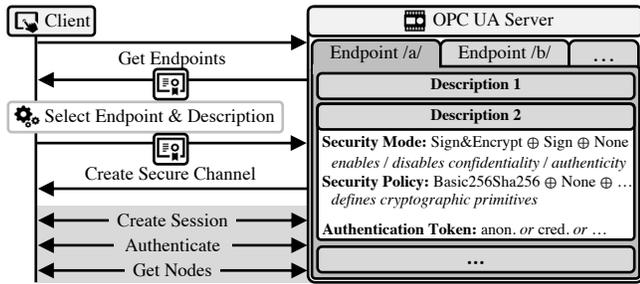


Figure 1: OPC UA server configuration and communication steps with clients selecting one of multiple endpoints with different descriptions a server offers (according to [48–50]).

2 A PRIMER ON OPC UA AND SECURITY

Besides many functional improvements over prior industrial protocols, e.g., cross-vendor communication and platform independence, OPC UA is the first widely-deployed industrial protocol with built-in and attested security [19], allowing for secure remote access.

To enable platform-independent communication between industrial devices of different manufacturers, OPC UA servers represent device functions, sensor values, and other variables as well as their relationships as a set of nodes in an address space, where namespaces provide semantic information about nodes [41]. From this address space, clients can dynamically request the execution of functions or data of variables. While OPC UA offers a variety of different communication paradigms and interfaces, e.g., publish/subscribe or HTTP(S), we focus on the binary interface (standard port 4840 via TCP) as it is a mandatory feature of all OPC UA devices [49]. It implements security-specific mechanisms, such as authentication, access control, as well as integrity protection and confidentiality [50].

Figure 1 illustrates the establishment of a (secure) connection in OPC UA, specifically focusing on information such as security primitives that an OPC UA server provides to clients. First, as OPC UA servers can provide data via different endpoints, clients request a list of endpoints with a description of their security configurations. Apart from this list, the response includes a certificate that authenticates the server. After choosing one of the available endpoints, the client starts to establish a *secure channel* using the channel parameters in the endpoint description.

Thereby, the *security mode* in the endpoint description enables or disables confidentiality and/or authentication for communication. Notably, establishing a secure channel already allows the client to authenticate to the server via a certificate, optionally realizing the first level of access control. Table 1 lists the *security policies* defining the cryptographic primitives for the secure channel establishment in the endpoint description, e.g., hash function and key length.

After establishing a secure channel, clients create a *session* for subsequent data transmissions. To access a server’s address space, clients need to authenticate (using user credentials, a certificate, or an authentication token) unless anonymous access is enabled. Depending on the authenticated user, OPC UA servers can enforce different access control rules at the granularity of single nodes.

Although OPC UA’s protocol design is secure [19], its various configuration options can significantly impact security. Official recommendations attempt to improve this situation [52]: First, communication security should never be disabled, i.e., signed and

Policy	Sig. Hash	Cert. Hash	Key Len. [bit]	A
None	—	—	—	N
Basic128Rsa15	SHA1	SHA1	[1024; 2048]	D1
Basic256	SHA1	SHA1, SHA256	[1024; 2048]	D2
Aes128_Sha256_RsaOaep	SHA256	SHA256	[2048; 4096]	S1
Basic256Sha256	SHA256	SHA256	[2048; 4096]	S2
Aes256_Sha256_RsaPss	SHA256	SHA256	[2048; 4096]	S3

A: abbreviations for policies in the remainder of this paper

Table 1: OPC UA security policies define used ciphers and key lengths (insecure and deprecated polices marked gray).

encrypted communication should be used whenever possible. Likewise, anonymous authentication should be forbidden. Finally, only three of the six available security policies should be used, as one provides no security and two have been deprecated due to the use of SHA-1 (cf. Table 1). Consequently, it is important to verify that OPC UA deployments follow these recommendations.

3 RELATED WORK

The benefits of a global view on the security configuration of OPC UA deployments are emphasized by research on the security of Internet-facing industrial appliances as well as Internet-wide security analyses for Web protocols.

Security of Industrial Deployments: Different works identify security issues of industrial deployments [6, 26, 33, 53, 56, 62]. While actual security incidents are seldom [43], already a single incident can be catastrophic [45]. Remarkably, Mirian et al. [44] still found ten-thousands of industrial devices connected to the Internet via legacy and insecure protocols. These devices can be classified, e.g., as programmable logic controllers [20]. Other research found robots controllable via the Internet [13].

Internet scan projects, e.g., Censys [15] or Shodan [59], offer meta-information about all Internet-connected devices, including industrial deployments [25, 40], detecting new industrial devices within one month [3]. Several studies analyzed Shodan’s data on industrial devices to assess their security and found a vast amount of devices affected by known software vulnerabilities, e.g., in the Netherlands [5], in Finland [37], and worldwide [24]. These works only consider industrial devices using legacy industrial protocols.

Devices using these legacy and insecure industrial protocols are often subject to scanning activities [4, 17, 35]. While standard scanning tools, e.g., zmap [16], not necessarily influence normal operations of industrial devices [8], malicious activities can compromise such unprotected devices.

Nawrocki et al. observe communication over legacy industrial protocols on IXP level and show that 96% of messages originate from industrial devices [45], emphasizing the need for secure industrial communication. Assessment guidelines and tools assist operators in correctly configuring secure industrial protocols such as OPC UA [30, 52, 55].

However, until now, it is an open question whether OPC UA deployments actually capitalize on increased security functionality compared to legacy industrial protocols that provide no security.

Internet Security Measurements: Active and passive measurements have proven useful for insights on the deployment and (mis-)configuration of security protocols.

Different works examine TLS deployments, i.e., the TLS and certificate configuration of Internet-facing embedded devices [57],

the spread of flaws in key generation [27] or TLS implementations [61], and the shift to newer versions and features [1]. Further, related work analyzed security certificates regarding configuration [32], validity [7], wrong issuance [38], and certificate transparency logs [22]. Besides HTTPS deployments, also communication services [31] and SSH were examined [23].

In addition, Internet measurements have been utilized to find insecurely configured embedded devices [10], detect compromised IoT devices [42, 46, 58], and study cloud usage as well as communication security of IoT devices [54]. Motivated by these observations, we set out to study whether modern Internet-facing industrial appliances that use the OPC UA protocol capitalize on the promised increases in security.

4 OPC UA SCANNING & DATASET

Our methodology to analyze the security configuration of Internet-facing OPC UA deployments relies on weekly scans of the complete IPv4 address space on the default OPC UA binary protocol port (TCP, 4840), as implementing the binary protocol is mandatory for all OPC UA instances [49]. By performing weekly scans, we can observe situation changes, e.g., software updates and certificate renewals. During both, design and execution, we follow principles of ethical research and established best practices for Internet-wide active measurements (cf. Appendix A). Whenever possible, we inform operators of insecure systems to prevent future harm.

Scanner: We rely on `zmap` to detect Internet-facing systems with an open TCP port 4840 and `zgrab2`, which we extended with OPC UA functionality based on `gopcua`, to connect to the found servers (0.5% of hosts with an open TCP port 4840 actually run OPC UA). Subsequently, we retrieve information on the provided endpoints, their security configuration, i.e., available security modes, security policies, and authentication tokens, as well as establish a secure channel. Whenever a server offers the security policy `Sign` or `SignAndEncrypt`, we send a self-signed certificate during the secure channel handshake. Furthermore, we also connect to other host / port combinations listed as endpoints on scanned OPC UA servers (as of 2020-05-04). For each server with anonymous access enabled, we traverse through the offered address space to retrieve all nodes and their access rights.

We use the collected information to (i) validate compliance of security configurations with security recommendations [52], (ii) compare the conformance of advertised security configurations with used cryptographic ciphers, and (iii) discover devices neglecting security best practices [2, 12].

Dataset Overview: In Figure 2, we detail the number of publicly reachable OPC UA servers over time (seven months between 2020-02-09 and 2020-08-30), grouped by manufacturers of the software resp. industrial device (we manually clustered the values of the `ApplicationURI` field provided by servers). We discovered between 1761 and 2069 deployments in the IPv4 address space.

The found OPC UA servers can be broadly classified into two categories. First, *discovery servers* (hatched in Figure 2, 42% of hosts in our latest measurement) only announcing OPC UA endpoints running on other host / port combinations. These systems mainly rely on the OPC UA reference implementation [47] and their number varies slightly from measurement to measurement. The second

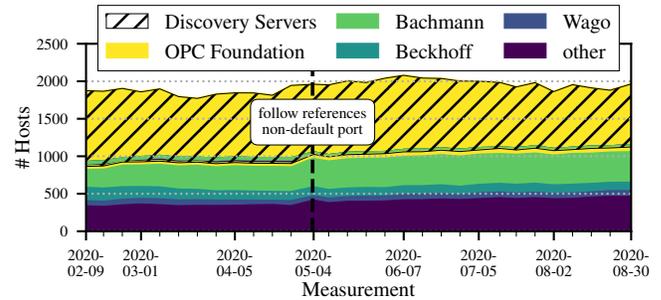


Figure 2: OPC UA servers found by our measurements can often be assigned to well-known manufacturers.

class comprises *full OPC UA servers* (“servers” from here on), mostly on industrial devices, which we could attribute to well-known industrial device manufacturers, most prominently Bachmann (406 devices in our last measurement), Beckhoff (112), and Wago (78). Their number marginally increased during the time of our measurements. Since the security configuration of OPC UA servers is only relevant for data transmission and not for the unprotected retrieval of endpoints, we focus on non-discovery servers below (1114).

To enable reproducibility of our results, we make our anonymized dataset [11] and extensions of `zgrab2` [9] publicly available.

5 SECURITY OF OPC UA DEPLOYMENTS

While, in principle a secure protocol, OPC UA requires complex and correct configuration to achieve a secure deployment [19]. Configuration recommendations [52] as well as general security advice for industrial control systems [63] and generic security guidelines, e.g., on the use of certificates [2, 52] and hash functions [12, 18], aid this task. However, it is unclear whether operators follow these recommendations to secure their deployments. To overcome this gap of knowledge, we analyze and assess all reachable OPC UA servers’ security configurations w.r.t. communication security, authorization, and access control. Unless stated otherwise, we rely on our latest measurement (2020-08-30) for our analysis. In Appendix B we elaborate on the distribution of security configurations over device manufacturers and autonomous systems.

5.1 Advertised Security Properties

Using their endpoint descriptions, OPC UA servers advertise different security modes and security policies and thus define foundational security settings and cryptographic primitives.

Message Security Mode: The client-chosen message security mode determines whether the communication is authenticated and confidential (mode `SignAndEncrypt`), authenticated (`Sign`), or insecure (`None`) (cf. Section 2). To enable clients to benefit from secure connections, it is fundamental that servers provide the corresponding security modes. Hence, it is essential to assess both the strongest (maximum security level that a client can enforce) and the weakest security mode (minimum security level) servers offer.

Figure 3 (left) shows the number of hosts supporting a specific security mode and further marks the number of hosts where a security mode is the least resp. most secure mode available, e.g., the security mode `Sign` (S) is supported by 588 hosts but is the least secure mode available on only 28 hosts and the most secure mode

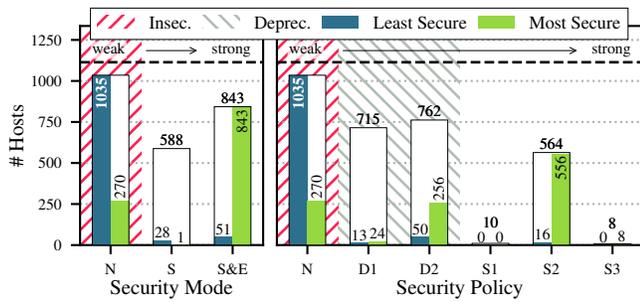


Figure 3: Number of hosts providing security modes (None (N), Sign (S), SignAndEncrypt (S&E)) and policies (cf. Table 1) as well as number of hosts offering these as their least and most secure option (dashed line = all hosts).

on only one host, indicating that most of the hosts also support the security modes None (N) and SignAndEncrypt (S&E). Overall, 844 servers (75%) follow the recommendation and provide support for at least one of the security modes SignAndEncrypt or Sign, i.e., authenticated communication (visible in Figure 3 by summing up hosts supporting one of these modes as their most secure option). However, 270 servers (26%) only support the security mode None and, therefore, fail to enable secure communication [52] rendering the security benefits of OPC UA inaccessible.

Security Policies: While message security modes define whether communication security is enabled, security policies define the selected cryptographic primitives (cf. Section 2). Here, two out of five specified security policies other than None are marked as deprecated due to the use of SHA-1 (Basic128Rsa15 (D1), Basic256 (D2); cf. Table 1). Therefore, these policies should not be supported whenever the use of stronger policies is technically possible [52].

Figure 3 (right) details the number of servers offering security policies and the number of servers providing a specific policy as their least and most secure option. While the security policy None is only offered in combination with security mode None, the other policies are announced together with the security modes Sign and SignAndEncrypt. While 564 servers support one of the policies with a sufficient level of security (S1, S2, S3) (visible in Figure 3 by summing up hosts supporting these policies as their most secure option), only 16 enforce the use of these policies, i.e., do not provide a less secure alternative. In contrast, 786 hosts still support SHA-1-based policies that have been deprecated in 2017 (D1, D2). A subset of 280 servers support these policies as their most secure option and thus lack an adequate security level for connecting clients.

To summarize, while only 1.4% of all servers enforce the use of strong cryptographic policies, 70% of all servers still support deprecated and insecure policies. Despite using OPC UA, a principally secure protocol, these numbers indicate that the security configurations are not updated as fast as basic cryptographic primitives lose their security guarantees. Given the long lifetime of industrial components [63], exposing such devices to the Internet and not updating their configuration is (potentially) dangerous.

Takeaway: Already for elementary security settings, we uncover 270 servers (24%) offering no security at all and 280 servers (25%) supporting only deprecated cryptographic ciphers. Summing up, 49% of the servers do not fully utilize the security benefits of OPC UA, i.e., do not allow clients to connect securely according to today’s standards.

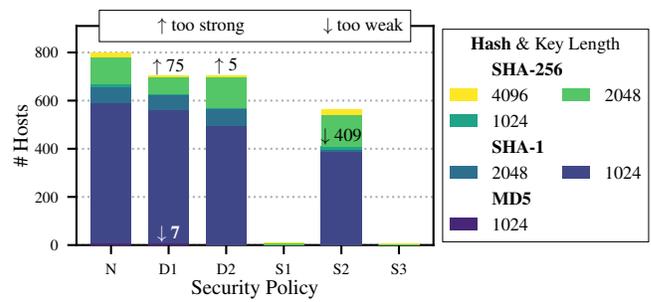


Figure 4: Number of servers sending a certificate to implement announced policies (separated by signature hash function and key length).

5.2 Actually Used Security Parameters

While security policies define mandatory cryptographic primitives, so far, it was an open question whether OPC UA servers implement the security parameters determined in their announced policies. To study the effective implementation of the security policies, we analyze all servers’ certificates (99% self-signed, 2 CA signed), focussing on their used cryptographic algorithms and key lengths, for conformance with the announced security policies.

In Figure 4, we present for each security policy the number of received certificates that servers delivered, highlighting the cryptographic hash function and key length. Most notably, out of the servers offering the recommended Basic256Sha256 (S2) policy, 409 servers provide certificates that do not match the specified security parameters, i.e., using MD5 or SHA-1 and/or a too-short key, weakening the built-in security of OPC UA. Contrary, out of the servers announcing the weakest and deprecated security policy (Basic128Rsa15 (D1)), 75 servers provide certificates using cryptographic primitives being too “strong”. In most cases, these certificates use SHA-256 instead of SHA-1 (as required by D1) as signature hash function. Although too strong primitives do not weaken the security, the specification does not allow such behavior, i.e., such settings potentially hinder clients from connecting.

In general, OPC UA implementations do not check compliance to security policies or do not sufficiently alert operators when inappropriate certificates are provided. The use of weaker primitives than defined by the policy causes the gained communication security to be weaker than expected, rendering the security benefits advertised by the security policies ineffective. Contrary, certificates using too strong primitives nullify the alleged compatibility with legacy clients, which might not be able to operate with these primitives [29, 34]. In case the certificate includes a longer key than the client is able to handle, e.g., due to memory limitations, the client is not able to connect. However, when the certificate is created using a hash function that the client does not support, the client might abort the connection or continues without verifying the certificate.

Takeaway: Out of the 844 servers, which in theory provide sufficient security, 70% actually realize a weaker security level in practice than specified, e.g., due to the use of SHA-1. In combination with the 280 servers already announcing deprecated security options, this leads to 60% of servers with deprecated configurations. Adding the 26% of servers offering no security, 85% of found servers are affected by configuration deficits.

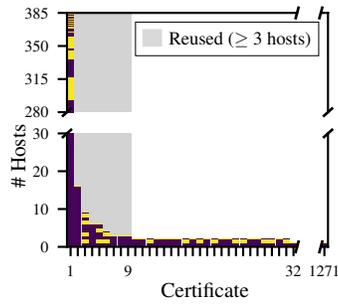


Figure 5: Number of hosts using the same certificate to authenticate (alternating colors indicate distinct autonomous systems).

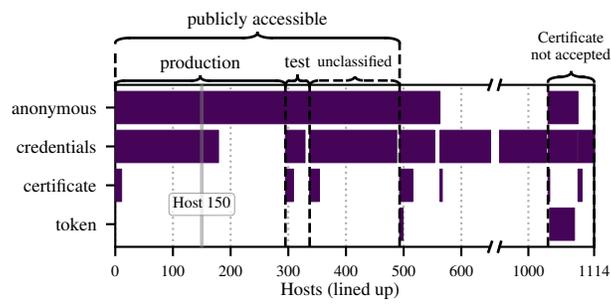


Figure 6: All hosts lined up marking offered authentication methods, accessible hosts and our classification results, e.g., Host 150 was accessible, classified as production system and provided anon. and cred. as auth. types.

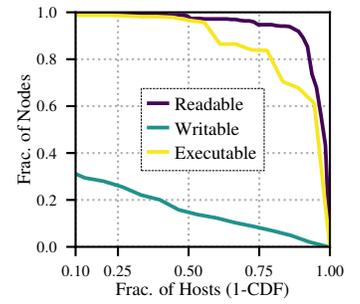


Figure 7: Fraction of read- and writable nodes as well as executable functions on all 493 publicly accessible hosts.

5.3 Secrets Not Meant to be Shared

Apart from the correct configuration and use of security parameters, the handling of secrets is also crucial for the security of Internet-facing deployments. Most important, cryptographic secrets must remain private to avert impersonation and eavesdropping [2].

To assess whether operators adhere to foundational security best-practices, we check whether different servers authenticate using the same security certificate. Figure 5 lines up all received certificates and shows the number of hosts announcing it to authenticate. Notably, we encounter 9 certificates of which each is deployed on at least three devices (to account for devices changing their IP address during our measurements, highlighted in Figure 5), most likely deployed at different operators. Although the OPC UA protocol does not allow the client to verify that the certificate’s private key is indeed installed on the server whenever the client certificate is rejected (due to an ambiguous error response), we still assume so as it is a fundamental requirement for the secure channel handshake (needed for the decryption of the request) [48].

From available meta-information, we can derive that certificate reuse concerns systems encompassing automation systems, amongst others, for energy technology and parking guidance. In one extreme case, we found a single certificate issued by a manufacturer of industrial control systems (as per the subject field) deployed on 385 hosts in 24 different autonomous systems. Two additional certificates of the same manufacturer show the same practice (on 9 resp. 6 devices in 8 resp. 5 autonomous systems). We informed the manufacturer about our observations at the end of April 2020, whereupon the manufacturer claimed that distributors and/or operators do not read or understand the product manual which emphasizes the risks of certificate reuse. As a countermeasure, the manufacturer targeted to sensitize its distributors w.r.t. security and sent security information to all its customers in early June 2020. However, even three months after the manufacturer sent the security information, we were not able to see any differences in the configuration strategy of the affected hosts.

From the discussion with the manufacturer we can, furthermore, assume that these devices indeed are installed at different operators since a distributor is responsible for the configuration of the devices and sells it to the operators. Even if not installed at different operators, the usage of the same certificate and key material

over hundreds of devices installed in the field, connected to many different ASSs, increases the number of attack vectors significantly.

Next to proper handling, the correct creation of secrets is also important for secure deployments, i.e., cryptographic keys often need to be chosen uniformly at random [27]. While the handling of some secrets is questionable, we have not found any evidence of key material that is subject to insufficient randomness by pairwise checking the keys of all received certificates for shared primes.

Takeaway: Numerous OPC UA systems disregard fundamental security recommendations and reuse security certificates across devices, making these susceptible to impersonation and eavesdropping. As this only affects 5 devices otherwise configured securely, it has no significant effect on our previous assessment of 85% of servers being configured deficiently.

5.4 Unprotected OPC UA Address Spaces

Access control to protect the information in the address space is an essential part of the OPC UA security concept, consisting of two steps (cf. Section 2): certificate validation during the secure channel establishment, and authorization during the session establishment. The latter especially means that anonymous access should be disabled, requiring connecting clients to authenticate [52, 60].

Available Authorization Methods: Figure 6 shows all found OPC UA servers and details the resp. available authentication options¹. We sort servers by the authentication options they support and further separate (to the right) servers that abort the creation of a secure channel rejecting our self-signed certificate (cf. Section 4). Out of the 1034 servers that allow anyone to establish a secure channel, 563 servers (50% of all Internet-reachable OPC UA systems) also offer anonymous access. Notably, this number encompasses 71 servers that otherwise force clients to communicate securely.

System Classification: To evaluate whether systems with insufficient access control indeed are production systems, we access all servers that offer anonymous access not rejecting our session request (493 servers, cf. Figure 6), e.g., due to invalid configurations. To not interfere with any process, we never change the system’s state, e.g., by write operations or function executions. Further, we handle the received data responsibly and reach out to operators whenever we are able to identify them to inform them about their openly accessible system (cf. Appendix A).

¹We further detail on available authentication methods in Appendix B.2.

We heuristically classify accessible OPC UA systems into production or test systems by analyzing the supported namespaces (cf. Section 2). Although we cannot label 156 systems (standard namespace only), our approach classifies 295 production systems based on namespaces relating to industrial manufacturers or standards, e.g., IEC 61131-3 [36]. Likewise, we categorize 42 systems as test systems as they use namespaces of example applications, e.g., [21].

Overall, our classification points out that a significant ratio of insecure configurations can be linked to production systems allowing control by unauthorized users without any countermeasures.

Address Space Access Control: To assess the severity of allowing anonymous access, we also analyze the access rights of the anonymous user, i.e., whether servers allow clients reading or writing nodes and executing functions anonymously.

Figure 7 shows to which extent a share of hosts enables the anonymous user to read or write nodes and execute functions. 90% of all servers allow clients to read more than 97% of available nodes anonymously, e.g., variables called `m3InflowPerHour`, indicating that attackers can monitor the device’s behavior. Manual examination of the data the readable nodes contain allowed us to identify a few systems such as parking guidance systems including license plate and video surveillance data. Further, 33% of hosts allow anonymous writes to >10% of their nodes, e.g., `rSetFillLevel`, enabling attackers to inject various data into the OPC UA appliance. 61% of the systems enable anonymous users to execute over 86% of functions provided, allowing to change the server configuration, e.g., `AddEndpoint`. Based on our judgment, none of the function names suggest that the execution of the function would directly alter the physical state of a machine. Furthermore, there might be other parts of the production deployment which are under access control. Still, we find it risky that at least a part of production systems are accessible anonymously enabling attackers to read and write values as well as to execute various functions.

Takeaway: 44% of OPC UA systems, many classified as production systems, do not realize access control and thus allow anyone to read and write data as well as execute functions. This issue concerns 71 servers implementing communication security increasing the share of servers leaving out security opportunities from 24% to 30%. In total, 92% of all OPC UA servers show configuration deficits.

5.5 A Lack of Longitudinal Improvements

To assess whether the security of OPC UA configurations improves over time, we (i) perform analyzes on weekly data and (ii) analyze the distribution of security certificates using included time information covering time beyond the seven months of our measurements.

During seven months (February to August 2020), we are unable to detect any significant change in the fraction of deficiently configured systems (avg: 92%, std: 0.8%, min: 91%, max: 94%). Still, in 84 cases, we detect certificate renewals on servers with static IP addresses and can investigate whether operators change certificates as part of software updates or use this opportunity to switch to secure ciphers. In nine cases, we observed a simultaneous software update (as per OPC UA’s `SoftwareVersion` field). While all renewed certificates were self-signed and valid, only in seven cases security increased by replacing SHA-1. Surprisingly, one certificate renewal even resulted in a downgrade from SHA-256 to SHA-1.

Analyzing the combined 4296 certificates retrieved over all measurements, we observe that 2174 (50%) SHA-1 certificates were generated after the deprecation of the corresponding security policies in 2017 (NotBefore field), with 1923 SHA-1 certificates still being created and deployed since the beginning of 2019.

Furthermore, we observe continuing deployments of devices from the same manufacturer where multiple devices use the identical certificate (cf. Section 5.3), noticeably increasing from 263 devices on 2020-02-09 to 387 devices on 2020-08-09 indicating that the distributor still installs devices by copying certificates.

Takeaway: Weekly scans over seven months and the analysis of certificates generated in a longer timespan show that the security of OPC UA deployments did not improve over time, e.g., by certificate exchange. We even observe continuous insecure deployments of systems relying on deprecated ciphers and/or sharing the same certificate.

6 CONCLUSION

OPC UA is the prime candidate to realize standardized and secure industrial communication for an increasing industrial digitalization [55]. In this paper, we study whether the general security of OPC UA’s design [19] leads to secure Internet-facing deployments.

Using Internet-wide active measurements, we show that 92% of all 1114 Internet-reachable OPC UA deployments are configured deficiently: First, we reveal servers completely disabling communication security (26%) or relying on deprecated cryptographic primitives (25%) such as SHA-1. Second, we discover the incorrect application of theoretically secure configurations on additional 35% of systems. Partly, these systems are also affected by a systematic reuse of security-critical certificates on hundreds of systems across various autonomous systems. Finally, we find that 44% of all servers allow unauthenticated users to read and write values from industrial devices and even execute system functionality.

Our analysis in this paper uncovers configuration deficits of OPC UA devices reachable via IPv4. It might be possible that various OPC UA devices are connected via IPv6 only and therefore are not captured in our scans. We do not anticipate that these devices are configured more securely, but leave this analysis for future research.

To conclude, our results underpin that secure protocols, in general, are no guarantee for secure deployments if they need to be configured correctly following regularly updated guidelines that account for basic primitives losing their security promises. Thus, we are strongly convinced that it is imperative to reduce configuration complexity in security protocols and demand secure defaults for all configuration options, eventually transitioning from security by design to security by default. Given the overall still comparatively small number of Internet-connected OPC UA appliances at the beginning of the uptake of the fourth industrial revolution [39, 51], now is the perfect time to rethink and reinforce the security configuration of OPC UA deployments and thus eventually realize secure industrial Internet-wide communication.

ACKNOWLEDGMENTS

We would like to thank the anonymous reviewers and our shepherd Mirja Kühlewind for their fruitful comments. This work is funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany’s Excellence Strategy – EXC-2023 Internet of Production – 390621612.

REFERENCES

- [1] Johanna Amann, Oliver Gasser, Quirin Scheitle, Lexi Brent, Georg Carle, and Ralph Holz. 2017. Mission Accomplished? HTTPS Security after Diginotar. In *Proceedings of the 2017 Internet Measurement Conference (IMC '17)*. ACM, 325–340. <https://doi.org/10.1145/3131365.3131401>
- [2] Elaine Barker and Allen Roginsky. 2019. Recommendation for Cryptographic Key Generation. NIST SP 800-133 Rev. 1. (2019).
- [3] Roland Bodenheimer, Jonathan Butts, Stephen Dunlap, and Barry Mullins. 2014. Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. *International Journal of Critical Infrastructure Protection* 7, 2 (2014), 114–123. <https://doi.org/10.1016/j.ijcip.2014.03.001>
- [4] Olivier Cabana, Amr M. Youssef, Mourad Debbabi, Bernard Lebel, Marthe Kassouf, and Basile L. Agba. 2019. Detecting, Fingerprinting and Tracking Reconnaissance Campaigns Targeting Industrial Control Systems. In *Proceedings of the 16th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA '19)*. Springer, 89–108. https://doi.org/10.1007/978-3-030-22038-9_5
- [5] Jorge Martin Ceron, Justyna Joanna Chromik, José Jair Cardoso de Santanna, and Aiko Pras. 2019. *Online Discoverability and Vulnerabilities of ICS/SCADA Devices in the Netherlands*. Technical Report. University of Twente.
- [6] Manuel Cheminod, Luca Durante, and Adriano Valenzano. 2013. Review of Security Issues in Industrial Networks. *IEEE Transactions on Industrial Informatics* 9, 1 (2013), 277–293. <https://doi.org/10.1109/TII.2012.2198666>
- [7] Taejoong Chung, Yabing Liu, David Choffines, Dave Levin, Bruce MacDowell Maggs, Alan Mislove, and Christo Wilson. 2016. Measuring and Applying Invalid SSL Certificates: The Silent Majority. In *Proceedings of the 2016 Internet Measurement Conference (IMC '16)*. ACM, 527–541. <https://doi.org/10.1145/2987443.2987454>
- [8] Kyle Coffey, Richard Smith, Leandros Maglaras, and Helge Janicke. 2018. Vulnerability Analysis of Network Scanning on SCADA Systems. *Security and Communication Networks* 2018 (2018). <https://doi.org/10.1155/2018/3794603>
- [9] COMSYS. 2020. zgrab2 OPC UA scanner plugin. (2020). <https://github.com/COMSYS/zgrab2>
- [10] Ang Cui and Salvatore J. Stolfo. 2010. A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan. In *Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC '10)*. ACM, 97–106. <https://doi.org/10.1145/1920261.1920276>
- [11] Markus Dahlmans, Johannes Lohmöller, Ina Bernice Fink, Jan Pennekamp, Klaus Wehrle, and Martin Henze. 2020. Dataset to "Easing the Conscience with OPC UA: An Internet-Wide Study on Insecure Deployments". (2020). <https://doi.org/10.18154/RWTH-2020-09197>
- [12] Quynh H. Dang. 2012. Recommendation for Applications Using Approved Hash Algorithms. NIST SP 800-107 Rev. 1. (2012).
- [13] Nicholas DeMarinis, Stefanie Tellex, Vasileios P. Kemerlis, George Konidaris, and Rodrigo Fonseca. 2019. Scanning the Internet for ROS: A View of Security in Robotics Research. In *Proceedings of the 2019 International Conference on Robotics and Automation (ICRA '19)*. IEEE, 8514–8521. <https://doi.org/10.1109/ICRA.2019.8794451>
- [14] David Dittrich and Erin Kenneally. 2012. *The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research*. Technical Report. U.S. Department of Homeland Security.
- [15] Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, and J Alex Halderman. 2015. A Search Engine Backed by Internet-Wide Scanning. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15)*. ACM, 542–553. <https://doi.org/10.1145/2810103.2813703>
- [16] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. 2013. ZMap: Fast Internet-wide Scanning and Its Security Applications. In *Proceedings of the 22nd USENIX Security Symposium (SEC '14)*. USENIX Association, 605–620.
- [17] Claude Fachkha, Elias Bou-Harb, Anastasis Keliris, Nasir Memon, and Mustaque Ahamad. 2017. Internet-scale Probing of CPS: Inference, Characterization and Orchestration Analysis. In *Proceedings of the 24th Annual Network and Distributed System Security Symposium (NDSS '17)*. Internet Society. <https://doi.org/10.14722/ndss.2017.23149>
- [18] Federal Office for Information Security. 2020. Cryptographic Mechanisms. BSI TR-02102. (2020).
- [19] Federal Office for Information Security. 2017. *OPC UA Security Analysis*. Technical Report. Federal Office for Information Security (BSI).
- [20] Xuan Feng, Qiang Li, Haining Wang, and Limin Sun. 2016. Characterizing industrial control system devices on the Internet. In *Proceedings of the 2016 IEEE 24th International Conference on Network Protocols (ICNP '16)*. IEEE. <https://doi.org/10.1109/ICNP.2016.7784407>
- [21] FreeOpCUA. 2016 (accessed June 2, 2020). FreeOpCUA Example Implementation. <https://github.com/FreeOpCUA/python-opcua/tree/master/examples>. (2016 (accessed June 2, 2020)).
- [22] Oliver Gasser, Benjamin Hof, Max Helm, Maciej Korczynski, Ralph Holz, and Georg Carle. 2018. In Log We Trust: Revealing Poor Security Practices with Certificate Transparency Logs and Internet Measurements. In *Proceedings of the 19th International Conference on Passive and Active Measurement (PAM '18)*. Springer, 173–185. https://doi.org/10.1007/978-3-319-76481-8_13
- [23] Oliver Gasser, Ralph Holz, and Georg Carle. 2014. A deeper understanding of SSH: Results from Internet-wide scans. In *Proceedings of the 2014 IEEE Network Operations and Management Symposium (NOMS '14)*. IEEE. <https://doi.org/10.1109/NOMS.2014.6838249>
- [24] Béla Genge and Călin Enăchescu. 2016. ShoVAT: Shodan-Based Vulnerability Assessment Tool for Internet-Facing Services. *Security and Communication Networks* 9, 15 (2016), 2696–2714. <https://doi.org/10.1002/sec.1262>
- [25] Adam Hansson, Mohammad Khodari, and Andrei Gurtov. 2018. Analyzing Internet-connected industrial equipment. In *Proceedings of the 2018 International Conference on Signals and Systems (ICSSigs '18)*. IEEE, 29–35. <https://doi.org/10.1109/ICSSIGSYS.2018.8372775>
- [26] Kevin E. Hemsley and Ronald E. Fisher. 2018. *History of Industrial Control System Cyber Incidents*. Technical Report. Idaho National Laboratory. <https://doi.org/10.2172/1505628>
- [27] Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. 2012. Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices. In *21st USENIX Security Symposium (USENIX Security 12)*. USENIX Association, Bellevue, WA, 205–220. <https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/heninger>
- [28] Martin Henze. 2020. The Quest for Secure and Privacy-preserving Cloud-based Industrial Cooperation. In *Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS '20)*. IEEE.
- [29] Jens Hiller, Jan Pennekamp, Markus Dahlmans, Martin Henze, Andriy Panchenko, and Klaus Wehrle. 2019. Tailoring Onion Routing to the Internet of Things: Security and Privacy in Untrusted Environments. In *Proceedings of the 2019 IEEE 27th International Conference on Network Protocols (ICNP '19)*. IEEE. <https://doi.org/10.1109/ICNP.2019.8888033>
- [30] Filip Holik, Josef Horalek, Ondrej Marik, Sona Neradova, and Stanislav Zitta. 2014. Effective penetration testing with Metasploit framework and methodologies. In *Proceedings of the 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI '14)*. IEEE, 237–242. <https://doi.org/10.1109/CINTI.2014.7028682>
- [31] Ralph Holz, Johanna Amann, Olivier Mehani, Matthias Wachs, and Mohamed Ali Kaafar. 2016. TLS in the Wild: An Internet-wide Analysis of TLS-based Protocols for Electronic Communication. *Proceedings 23rd Annual Network and Distributed System Security Symposium (NDSS '16)* (2016). <https://doi.org/10.14722/ndss.2016.23055>
- [32] Ralph Holz, Lothar Braun, Nils Kammenhuber, and Georg Carle. 2011. The SSL Landscape: A Thorough Analysis of the x.509 PKI Using Active and Passive Measurements. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference (IMC '11)*. ACM, 427–444. <https://doi.org/10.1145/2068816.2068856>
- [33] Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo. 2017. Cyber-Physical Systems Security—A Survey. *IEEE Internet of Things Journal* 4, 6 (2017), 1802–1831. <https://doi.org/10.1109/JIOT.2017.2703172>
- [34] René Hummen, Hanno Wirtz, Jan Henrik Ziegeldorf, Jens Hiller, and Klaus Wehrle. 2013. Tailoring end-to-end IP security protocols to the Internet of Things. In *Proceedings of the 2013 21st IEEE International Conference on Network Protocols (ICNP '13)*. IEEE. <https://doi.org/10.1109/ICNP.2013.6733571>
- [35] Martin Husák, Nataliia Neshenko, Morteza Safaei Pour, Elias Bou-Harb, and Pavel Čeleda. 2018. Assessing Internet-Wide Cyber Situational Awareness of Critical Sectors. In *Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES '18)*. ACM. <https://doi.org/10.1145/3230833.3230837>
- [36] Karl-Heinz John and Michael Tiegelkamp. 2010. *IEC 61131-3: Programming Industrial Automation Systems Concepts and Programming Languages, Requirements for Programming Systems, Decision-Making Aids* (2nd ed.). Springer. <https://doi.org/10.1007/978-3-642-12015-2>
- [37] Timo Kiravuo, Seppo Tiilikainen, Mikko Särelä, and Jukka Manner. 2015. Peeking Under the Skirts of a Nation: Finding ICS Vulnerabilities in the Critical Digital Infrastructure. In *Proceedings of the 14th European Conference on Cyber Warfare and Security (ECCWS '15)*. ACPI, 137–144.
- [38] Deepak Kumar, Zhengping Wang, Matthew Hyder, Joseph Dickinson, Gabrielle Beck, David Adrian, Joshua Mason, Zakir Durumeric, J. Alex Halderman, and Michael Bailey. 2018. Tracking Certificate Misissuance in the Wild. In *Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 785–798. <https://doi.org/10.1109/SP.2018.00015>
- [39] Heiner Lasi, Peter Fettek, Hans-Georg Kemper, Thomas Feld, and Michael Hoffmann. 2014. Industry 4.0. *Business & Information Systems Engineering* 6, 4 (2014), 239–242. <https://doi.org/10.1007/s12599-014-0334-4>
- [40] Éireann P. Leverett. 2011. *Quantitatively Assessing and Visualising Industrial System Attack Surfaces*. Master's thesis. University of Cambridge.
- [41] Wolfgang Mahnke, Stefan-Helmut Leitner, and Matthias Damm. 2009. *OPC Unified Architecture*. Springer. <https://doi.org/10.1007/978-3-540-68899-0>
- [42] Antonio Mangino, Morteza Safaei Pour, and Elias Bou-Harb. 2020. Internet-Scale Insecurity of Consumer Internet of Things: An Empirical Measurements

- Perspective. *ACM Transactions on Management Information Systems* (2020). <https://doi.org/10.1145/3394504>
- [43] Bill Miller and Dale Rowe. 2012. A survey SCADA of and critical infrastructure incidents. In *Proceedings of the 1st Annual Conference on Research in Information Technology (RIIT '12)*. ACM, 51–56. <https://doi.org/10.1145/2380790.2380805>
- [44] Ariana Mirian, Zane Ma, David Adrian, Matthew Tischer, Thasphon Chuenchujit, Tim Yardley, Robin Berthier, Joshua Mason, Zakir Durumeric, J. Alex Halderman, and Michael Bailey. 2016. An Internet-wide view of ICS devices. In *Proceedings of the 2016 14th Annual Conference on Privacy, Security and Trust (PST '16)*. IEEE, 96–103. <https://doi.org/10.1109/PST.2016.7906943>
- [45] Marcin Nawrocki, Thomas C. Schmidt, and Matthias Wählisch. 2020. Uncovering Vulnerable Industrial Control Systems from the Internet Core. In *Proceedings of the 2020 IEEE/IFIP Network Operations and Management Symposium (NOMS '20)*. IEEE.
- [46] Nataliia Neshenko, Elias Bou-Harb, Jorge Crichigno, Georges Kaddoum, and Nasir Ghani. 2019. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Communications Surveys & Tutorials* 21, 3 (2019), 2702–2733. <https://doi.org/10.1109/COMST.2019.2910750>
- [47] OPC Foundation. 2016. OPC UA LDS-ME! The official UA Local Discovery Server with Multicast Extensions from the OPC Foundation. <https://opcfoundation.github.io/UA-LDS/>. (2016).
- [48] OPC Foundation. 2017. OPC Unified Architecture – Part 4: Services. OPC 10000-4: OPC Unified Architecture. (2017).
- [49] OPC Foundation. 2017. OPC Unified Architecture – Part 7: Profiles. OPC 10000-7: OPC Unified Architecture. (2017).
- [50] OPC Foundation. 2018. OPC Unified Architecture – Part 2: Security Model. OPC 10000-2: OPC Unified Architecture. (2018).
- [51] Jan Pennekamp, René Glebke, Martin Henze, Tobias Meisen, Christoph Quix, Rihan Hai, Lars Gleim, Philipp Niemiets, Maximilian Rudack, Simon Knappe, Alexander Epple, Daniel Trauth, Uwe Vroomen, Thomas Bergs, Christian Brecher, Andreas Bührig-Polaczek, Matthias Jarke, and Klaus Wehrle. 2019. Towards an Infrastructure Enabling the Internet of Production. In *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*. 31–37.
- [52] Uwe Pohlmann and Axel Sikora. 2018. Practical Security Recommendations for building OPC UA Applications. *Industrial Ethernet Book* 106 (2018).
- [53] Davide Quarta, Marcello Pogliani, Mario Polino, Federico Maggi, Andrea Maria Zanchettin, and Stefano Zanero. 2017. An Experimental Security Analysis of an Industrial Robot Controller. In *Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP '17)*. IEEE, 268–286. <https://doi.org/10.1109/SP.2017.20>
- [54] Jingjing Ren, Daniel J. Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. 2019. Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach. In *Proceedings of the 2019 Internet Measurement Conference (IMC '19)*. ACM, 267–279. <https://doi.org/10.1145/3355369.3355577>
- [55] Linus Roepert, Markus Dahlmanns, Ina Berenice Fink, Jan Pennekamp, and Martin Henze. 2020. Assessing the Security of OPC UA Deployments. In *Proceedings of the 1st ITG Workshop on IT Security (ITSec '20)*. University of Tübingen. <https://doi.org/10.15496/publikation-41813>
- [56] Ahmad-Reza Sadeghi, Christian Wachsmann, and Michael Waidner. 2015. Security and Privacy Challenges in Industrial Internet of Things. In *Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC '15)*. ACM. <https://doi.org/10.1145/2744769.2747942>
- [57] Nayanamana Samarasinghe and Mohammad Mannan. 2019. Another look at TLS ecosystems in networked devices vs. Web servers. *Computers & Security* 80 (2019), 1–13. <https://doi.org/10.1016/j.cose.2018.09.001>
- [58] Farooq Shaikh, Elias Bou-Harb, Nataliia Neshenko, Andrea P. Wright, and Nasir Ghani. 2018. Internet of Malicious Things: Correlating Active and Passive Measurements for Inferring and Characterizing Internet-Scale Unsolicited IoT Devices. *IEEE Communications Magazine* 56, 9 (2018), 170–177. <https://doi.org/10.1109/MCOM.2018.1700685>
- [59] Shodan. 2013. Shodan. <https://www.shodan.io>. (2013).
- [60] Siemens AG – Division Digital Factory. 2018. *SINUMERIK 840D sl/828D / OPC UA – Projektierungshandbuch*. Technical Report. Siemens AG.
- [61] Drew Springall, Zakir Durumeric, and J. Alex Halderman. 2016. Measuring the Security Harm of TLS Crypto Shortcuts. In *Proceedings of the 2016 Internet Measurement Conference (IMC '16)*. ACM, 33–47. <https://doi.org/10.1145/2987443.2987480>
- [62] Ioannis Stelios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcaraz, and Javier Lopez. 2018. A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services. *IEEE Communications Surveys & Tutorials* 20, 4 (2018), 3453–3495. <https://doi.org/10.1109/COMST.2018.2855563>
- [63] Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. 2015. Guide to Industrial Control Systems (ICS) Security. NIST SP 800-82 Rev. 2. (2015).

A ETHICS

While not involving human subjects, our research still warrants ethical considerations, as measurements of industrial systems could have unintended implications, for example, concerning information security, privacy, or safety.

During the design, execution, and analysis of our research, we thus follow basic ethical research guidelines [14] as well as practices and procedures imposed by our institutions. Most importantly, we carefully handle all collected data (cf. Appendix A.1) and further adhere to standard measurement guidelines [16] to reduce the impact of our measurements (cf. Appendix A.2).

A.1 Responsible Handling of Data

As part of our measurements, we only request publicly available data from OPC UA servers, i.e., data for which no authorization is required. Thereby, we never bypass any security mechanisms and never alter the state of a server, i.e., we never write to any variable in an OPC UA server’s address space nor execute any functions. Still, our dataset might contain very sensitive data for those servers that do not implement or do not correctly configure access control for their address space (cf. Section 5.4). Consequently, we store all data solely on secured systems and exclude collected payload data from our dataset release. Hence, our results on address space access control in Section 5.4 cannot be independently reproduced by others. Still, to protect potentially sensitive data, we consider this decision an appropriate trade-off. To prevent attackers using our dataset to find insecure OPC UA deployments, we further replace IP addresses and autonomous system IDs by consecutive numbers as well as blacken fields in certificates containing equivalent address information (e.g., FQDNs).

Identifying Operators: Besides using the collected data for our research, especially for the classification of systems and analysis of access control (cf. Section 5.4), we analyzed the collected data to identify server operators to inform them about their accessible systems where possible. To this end, we automatically searched the address space for nodes containing email addresses and, furthermore, invested manual effort to identify the operators of additional systems (where we could not find contact data in the address space).

Operator Feedback: Overall, out of 493 systems that provide unprotected access to potentially sensitive data and functionality, we were able to retrieve contact information for 50 systems, including systems for water sewerage, parking lot management, and hotel management. Subsequently, we reached out to the operators via email (and in one case by phone) to inform them about potential security problems and provided them with pointers to information on how to correctly secure their systems to prevent any potential harm caused by attackers, such as executing system functions as well as stealing or changing data. We received only two replies to our contact attempts, one promising to forward our information notice to the responsible IT department and one asking for security advice. At the time of writing (four months after our initial contact attempts), both systems, as well as all but three of the other systems for which we could derive contact information, are still online. However, the device where the operator asked for security advice now implements access control.

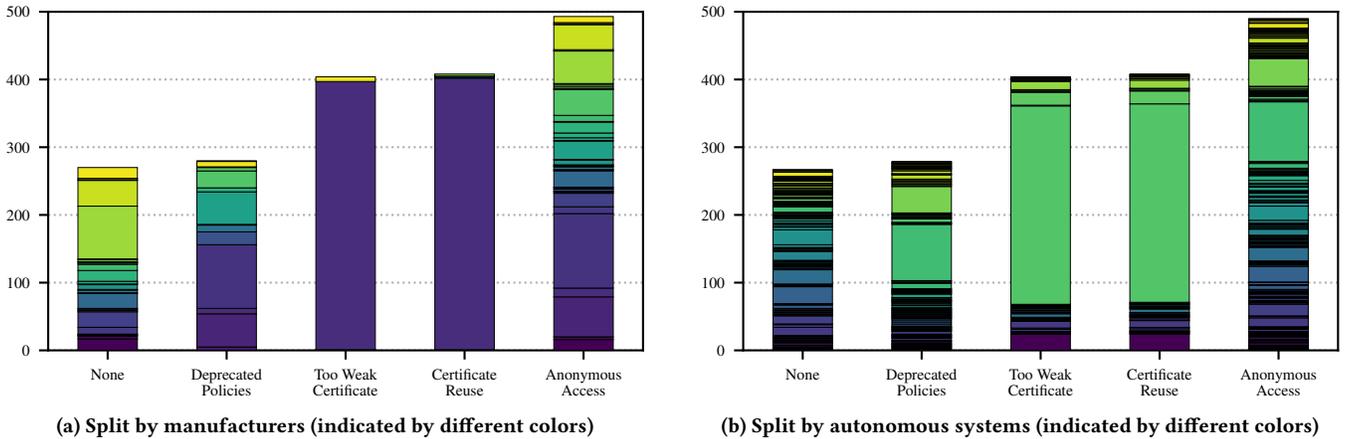


Figure 8: Number of hosts only providing security mode and policy None, only deprecated policies (D1, D2, cf. Table 1), too weak certificates, affected by certificate reuse, and allow anonymous access.

Manufacturer Feedback: Likewise, we reached out to the manufacturer listed in the subject field of (i) a security certificate used identically on more than 350 hosts as well as (ii) two additional certificates used on fewer hosts (cf. Section 5.3). The manufacturer claimed that the issue of certificate reuse likely results from customers/distributors copying system images and/or configuration files containing automatically generated security certificates. As a consequence, the manufacturer reached out to its customers to sensitize them for the risks resulting from copying security certificates in June 2020. However, three months after the information was sent, we do not observe any decline in systems using these certificates in our measurements. Instead, our data suggests that new systems using one of these certificates continue to get deployed as we observe an increase of 24 devices since their first reply and 3 devices in the week between our latest measurements.

A.2 Reducing Impact of Measurements

While related work claims that measurements with `zmap` not necessarily impact industrial devices [8], we still set out to minimize the implication of our weekly OPC UA active Internet measurements to the largest extent possible by following well-established Internet measurement guidelines [16].

Restricted Measurements: We closely coordinate our measurement study with RWTH Aachen University’s Network Operation Center to reduce the impact on our Internet uplink and the Internet as a whole and to handle potential inquiries or abuse requests as fast as possible. Additionally, we exclude systems from our measurements that requested so.

Contact Information: To prominently display the intent of our scans, we provide rDNS records for the IP address used for scanning and provide contact information both in the certificate and the `ApplicationName` field of our client. Furthermore, we provide a website at the IP address used for scanning with detailed explanations on the scope and purpose of our research. Additionally, to allow for exclusion in future scans, we list opt-out instructions on the website. Based on such requests, we exclude 5.79 M IP addresses (0.13% of the IPv4 address space) from our measurements.

Measurement Load: To not overload any autonomous system, we spread our scans over a timeframe of approximately 24 hours and rely on `zmap`’s address randomization. More importantly, to not overload potentially resource-constrained industrial devices during our traversal of their OPC UA address space, we instruct our scanner module to wait 500 ms between subsequent requests to one server. We further set a scanning time (60 min) and outgoing traffic (50 MB) limit per host, forcing our scanner to disconnect whenever the limit exceeds. On average, our scanner was connected to an OPC UA server for 110 s (std: 461 s, min: 31 ms, max: 5393 s) causing 352 kB of outgoing traffic (std: 2 MB, min: 28 B, max: 50 MB). In some rare cases, our scanner exceeds the set time limit due to side effects caused by parallel scanning of different hosts.

Overall, as OPC UA does not realize security by default, we consider it essential to know whether modern OPC UA deployments take advantage of the built-in security features. To answer this question, we have taken sensible measures to reduce the risks introduced by active Internet measurements of industrial appliances, aiming to influence the security of OPC UA deployments positively.

B A CLOSER LOOK AT OUR RESULTS

During our research on the security configurations of Internet-facing OPC UA deployments, we calculated much more extensive statistics than presented in the body of this paper. Here, we give detailed insight into this data, i.e., we break down our classification of deficiently configured OPC UA deployments by manufacturers and connecting autonomous systems (Appendix B.1) as well as elaborate on the access control of OPC UA devices (Appendix B.2).

B.1 Separating Deficits Into Classes

In this paper, we showed that 92% of Internet-facing OPC UA deployments are affected by different configuration deficits, i.e., disabling built-in communication security, using deprecated security primitives, disregarding secure policies, systematically reusing private key material, and/or disabling access control. In this appendix, we shed light on whether devices of specific manufacturers are more affected than devices of other manufacturers (Appendix B.1.1) and

Authentication Type				Accessible Hosts			Unaccessible Hosts					
anon.	cred.	cert.	token	Class:	Productive	Test	Unclassified	Reason:	Authentication	Secure Channel		
•					116 (10%)	8 (0.7%)	5 (0.4%)		9 (0.8%)	1 (0.1%)	139 (12%)	
	•				0 (0.0%)	0 (0.0%)	0 (0.0%)		464 (41%)	21 (1.9%)	485 (43%)	
•	•				168 (15%)	20 (1.8%)	134 (12%)		38 (3.4%)	5 (0.4%)	365 (32%)	
	•	•			0 (0.0%)	0 (0.0%)	0 (0.0%)		4 (0.4%)	7 (0.6%)	11 (1.0%)	
•	•	•			11 (1.0%)	14 (1.3%)	17 (1.5%)		17 (1.5%)	3 (0.3%)	62 (5.6%)	
•	•		•		0 (0.0%)	0 (0.0%)	0 (0.0%)		0 (0.0%)	43 (3.9%)	43 (3.9%)	
•	•	•	•		0 (0.0%)	0 (0.0%)	0 (0.0%)		6 (0.5%)	0 (0.0%)	6 (0.5%)	
					295 (26%)	42 (3.8%)	156 (14%)			541 (48%)	80 (7.2%)	
					493 (44%)					621 (55%)		

Table 2: Number and fraction of hosts supporting different OPC UA authentication types, split by our classification (accessible hosts) and reason for connection reject (unaccessible hosts). Unused combinations of authentication types are omitted.

whether devices in specific autonomous systems are more deficiently configured than devices in other autonomous systems (Appendix B.1.2).

B.1.1 Manufacturers. We already described in this paper that some configuration deficits are limited to a few manufacturers, i.e., certificate reuse mainly affects devices of one manufacturer (cf. Section 5.3). In this section, we give insight in whether the other configuration deficits affect the devices built by specific manufacturers more than others. To determine the device manufacturer of found OPC UA hosts, we use the same classification as used in the body of this paper (cf. Section 4), i.e., we analyzed the ApplicationURL field provided by the servers.

Figure 8a shows for each configuration deficit identified in this paper the number of affected devices and illustrates the distribution over device manufacturers of the hosts. Indeed, some large fractions of devices built by specific manufacturers are affected by the same configuration deficits, e.g., enabling anonymous access or only providing security mode and policy None. In one case, only providing security mode and policy None affects all found devices of this manufacturer. Current product manuals of this manufacturer state that connections relying on this security mode and policy are insecure but do not inform about possible consequences.

The results for too weak security primitives in used certificates and certificate reuse coincides with our results in the main part of the paper, i.e., only a few manufacturers are affected but in one case, these certificates are installed on a large number of devices.

B.1.2 Autonomous Systems. Figure 8b details the same analysis but illustrates the distribution of the devices connected to different

autonomous systems. Regarding hosts with too weak certificates in comparison to the security policy description and reusing certificates, a large fraction is connected via the same autonomous system, an ISP focussed on connecting (I)IoT devices to the Internet. Except for many devices two other autonomous system relying on deprecated policies and allowing anonymous access at the same time (both being regional Internet service providers), the devices affected by security configuration deficits are distributed over the Internet as they are located in different autonomous systems.

B.2 Discovered Access Control Configurations

In Section 5.4 we showed that a large number of OPC UA devices are accessible without any authentication (offering anonymous access) and elucidated which authentication types are how frequently used.

Table 2 details the distribution of access control settings of Internet-facing OPC UA servers. On the one hand, 621 servers (55% of all discovered servers) rejected our access attempts by either rejecting the secure channel channel establishment (7.2%) or denying access based on the authentication method (48%). Note, that this also includes servers initially offering anonymous access but nevertheless aborting the connection due to a faulty or incomplete endpoint configuration. On the other hand, 493 servers (44%) allowed access to their address spaces without any authentication although, in many cases, secure authentication types are offered in parallel. Out of these 493 servers, based on used namespaces in their address space, we classified 295 servers as production and 42 servers as test systems (26% resp. 3.8% of all Internet-facing OPC UA deployments).