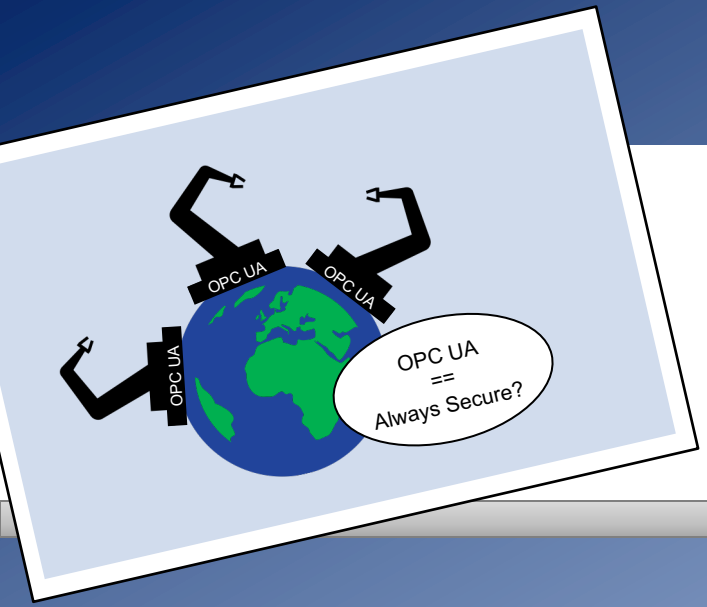


Easing the Conscience with OPC UA

An Internet-Wide Study on Insecure Deployments

Markus Dahlmanns, Johannes Lohmöller, Ina Berenice Fink,
Jan Pennekamp, Klaus Wehrle, and Martin Henze

dahlmanns@comsys.rwth-aachen.de

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC-2023 Internet of Production – 390621612

https://www.comsys.rwth-aachen.de/

OPC UA: Secure by Design Industrial Communication

- **OPC UA: comparably new industrial communication protocol**
  - Secure by design
  - Prime candidate for communication in the Industry 4.0 and IIoT
    - Control of productions via the Internet
  - Extensive configuration required

OPC UA Specification
https://opcfoundation.org/developer-tools/specifications-unified-architecture

- **Official OPC UA security configuration recommendations**

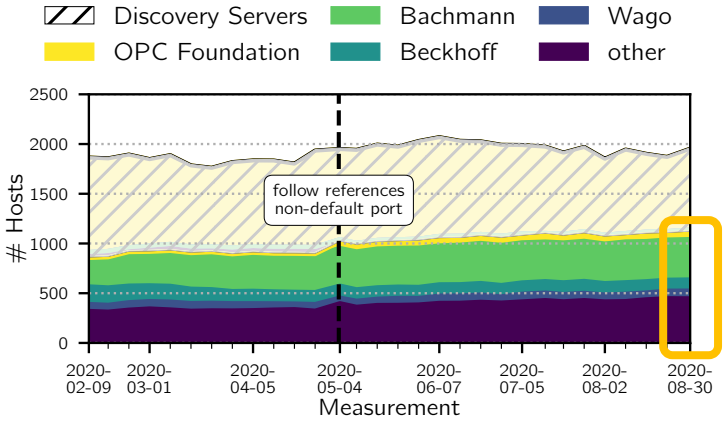
? Are Internet-facing OPC UA deployments configured securely?

OPC UA as key example for deployments using secure-by-design protocols

dahlmanns@comsys.rwth-aachen.de

Measurement Methodology & Found Deployments

- **Active Internet measurements (weekly over 7 months)**
  - TCP SYN scan via `zmap` on port 4840
  - Application layer scan (retrieval of security configurations and payload data)
    - Extension of `zgrab2`, available on github.com/COMSYS/zgrab2



Between 1761 and 2069 deployments discovered in the IPv4 address space

42% being Discovery Servers
- *Only publishing information on other OPC UA deployments*

? Are these Internet-facing OPC UA servers configured securely?

dahlmanns@comsys.rwth-aachen.de

Deficient Security Configurations

Security Mode

1/4 of all found deployments neglect OPC UAs benefits

do not offer communication security at all

Security Policy

1/4 of deployments offering security use deprecated policies

still based on SHA-1

only 1.4% of servers enforce usage of secure policies

as recommended by OPC Foundation

~30% of servers use certificates being too weak for announced policies

impacts communication security

Massive certificate reuse detected

Manufacturer claimed: distributors/operators do not read/understand the product manual

Authentication

44% of deployments do not implement access control

everybody on the Internet can access servers

1/4 of all servers classifiable as production systems

as per mounted namespaces

Simply deploying a secure protocol is not sufficient

How can standardization help?

Dataset available online:
doi.org/10.18154/RWTH-2020-09197

Scanner source code:
github.com/COMSYS/zgrab2

Thank you for your attention!

dahlmanns@comsys.rwth-aachen.de