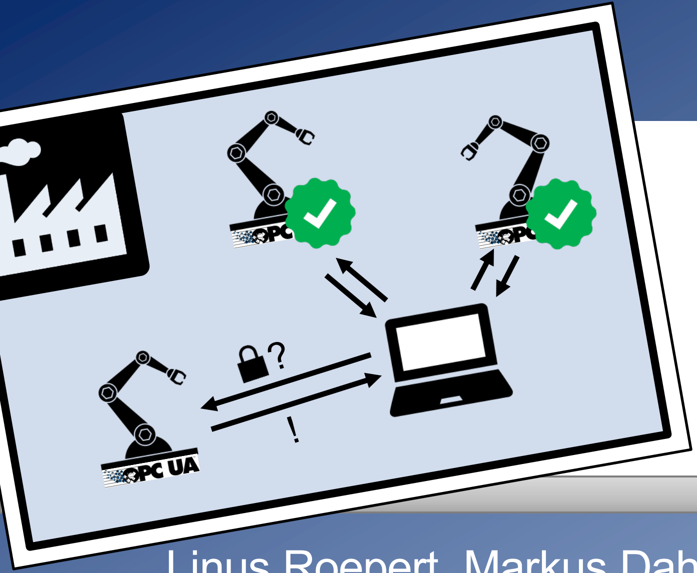


Assessing the Security of OPC UA Deployments

Linus Roepert, Markus Dahlmanns, Ina Fink, Jan Pennekamp, Martin Henze

dahlmanns@comsys.rwth-aachen.de

Contribution of our Research Focus Class on Cyber-Physical System Security
(https://www.comsys.rwth-aachen.de/teaching/ws-19/20/rfc-on-cyber-physical-system-security)

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

1st ITG IT Security Workshop, April 2020

Fraunhofer FKIE

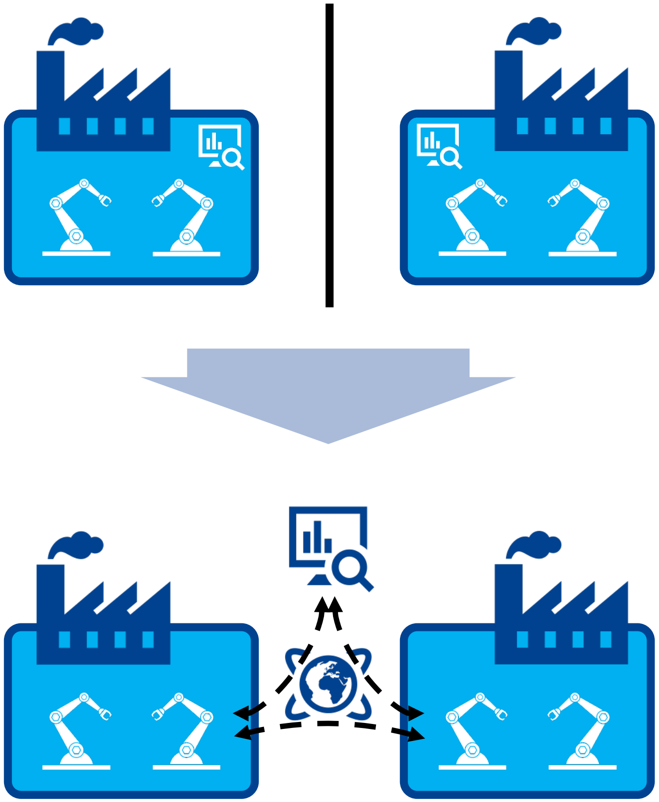
COM SYS

RWTH AACHEN UNIVERSITY

Industrial Networks Move Closer to the Internet

- **Industrial networks were isolated in past**
  - No security requirements
  - Rather simple protocols, e.g., Modbus
- **Convergence with IT networks**
  - Introduction of attack vectors
    - Exploited in past, e.g., Stuxnet or NotPetya
- **Industry 4.0 and IIoT**
  - Control of productions via the Internet
  - Data exchange between production lines

Need for secure industrial communication

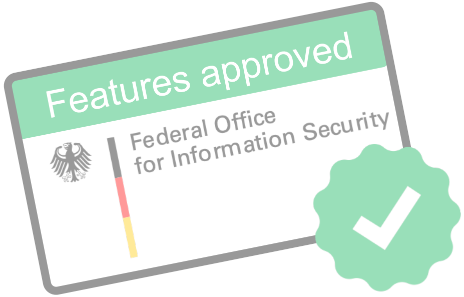


OPC UA: Prime Candidate for Secure Industrial Communication

- **Enables communication from the field up to the cloud**
  - Representation of objects, functions, and relationships as a graph (address space)
  - Abstraction allows communication between devices of different manufacturers

Checks for secure configurations neccessary

- **Integrates security measures**
  - Authentication
    - Anonymous access, username/password, certificate, or authentication token
    - Allows access control for every node in address space
  - Integrity and confidentiality
    - Three Security Modes: enable/disable integrity and confidentiality
    - Seven Security Policies: define algorithms and key lengths
      - One disables security; two are deprecated



Security Assessment of Industrial Devices

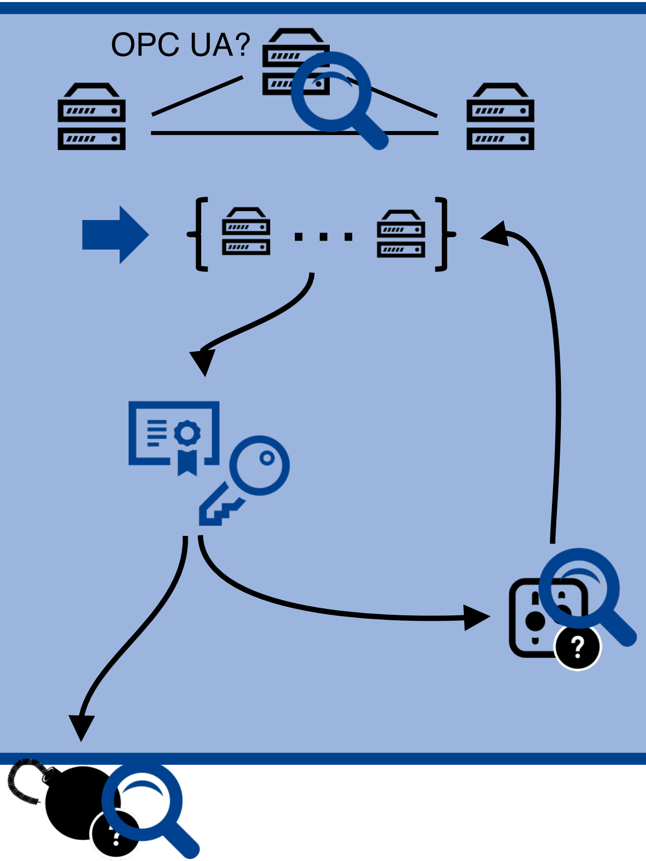
- **Tools such as the Metasploit Framework have proven to be useful**
  - Modules available to test specific PLCs, …
    - Schneider Modicon
    - Siemens SIMATIC
  - … SCADA software, …
    - Sielco Sistemi
    - Winlog
    - Measuresoft ScadaPro
  - … and industrial protocols
    - Modbus
    - Profinet
    - IEC 60870-5-104

⚠ OPC UA support missing

- **How to detect configuration errors?**
  - Anonymous access to sensitive functions
  - Wrongly chosen security modes
  - Weak acceptance of security policies

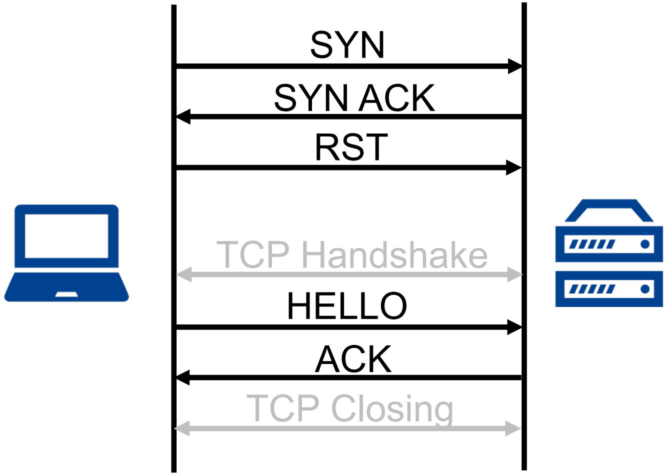
Our Metasploit Module: Assessment of OPC UA Deployments

- **Metasploit module to check configuration**
  - A. Detection of OPC UA servers
    - Scan network for OPC UA appliances
    - Generate set of proven OPC UA servers
  - B. Test authentication methods
    - Try to log in to the found servers
      - Detect disabled authentication / weak credentials
  - C. Derive further configuration
    - Get general device information
    - Evaluate security configuration
  - D. Ability to check for vulnerabilities



Discovery of OPC UA Deployments

- **Metasploit Framework already includes `nmap`**
  - TCP SYN scan on specified network
  - Detect hosts offering a service on specified port
- **Module to prove for running OPC UA instance**
  - Perform initial part of OPC UA handshake



IPs of hosts running OPC UA on specified port

```
[*] Running for 195.254.227.245...
[+] 195.254.227.245:4840 - Success
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Test Login Credentials

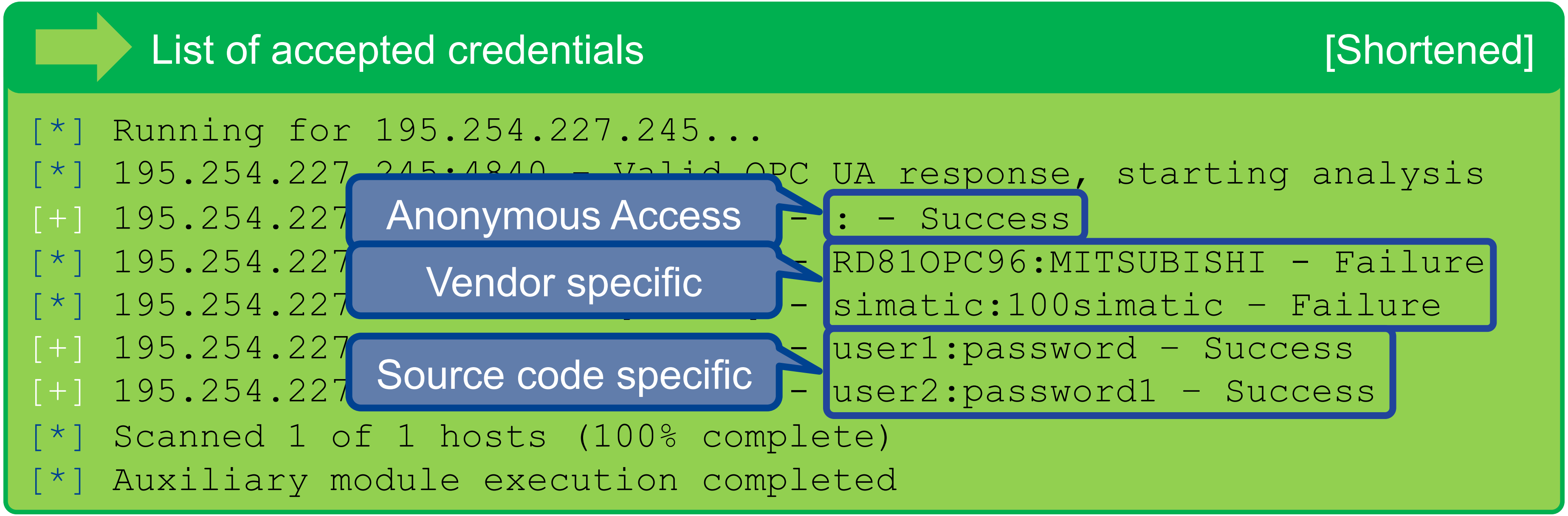
- **Check for anonymous access**
  - Empty username and password
- **Brute force for weak credentials**
  - Gathered from user manuals, …
  - List available: /COMSYS/msf-opcua

List of accepted credentials [Shortened]

```
[*] Running for 195.254.227.245...
[*] 195.254.227.245:4840 - Valid OPC UA response, starting analysis
[+] 195.254.227.245:4840 - [ 1/27] - : - Success
[*] 195.254.227.245:4840 - [ 9/27] - RD81OPC96:MITSUBISHI - Failure
[*] 195.254.227.245:4840 - [10/27] - simatic:100simatic - Failure
[+] 195.254.227.245:4840 - [20/27] - user1:password - Success
[+] 195.254.227.245:4840 - [21/27] - user2:password1 - Success
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Test Login Credentials

- **Check for anonymous access**
  - Empty username and password
- **Brute force for weak credentials**
  - Gathered from user manuals, …
  - List available: /COMSYS/msf-opcua



List of accepted credentials [Shortened]

```
[*] Running for 195.254.227.245...
[*] 195.254.227.245:4840 – Valid OPC UA response, starting analysis
[+] 195.254.227                    – : – Success
[*] 195.254.227                    – RD81OPC96:MITSUBISHI – Failure
[*] 195.254.227                    – simatic:100simatic – Failure
[+] 195.254.227                    – user1:password – Success
[+] 195.254.227                    – user2:password1 – Success
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Configuration Check

- **Get General OPC UA Deployment Information**
  - `ServerName`: String for identification
  - `ProductUri`: Product information, e.g., PLC model
  - `ApplicationUri`: Application information, e.g., version
- **Get Security Parameters**
  - Security Level: Manual security rating
  - Message Security Mode: Integrity and confidentiality
  - Security Policy: Specification of algorithms
  - Authentication mechanism
  - Access control per node
- **Get list of known OPC UA services (Endpoints)**
  - Possibility to get addresses of other deployments

Configuration Check

- **Get General OPC UA Deployment Information**
  - `ServerName`: String for identification
  - `ProductUri`:
  - `ApplicationUri`:

Evaluate deployed products, patch level, update availability, …

- **Get Security Parameters**
  - Security Level: Reevaluate classification
  - Message Security Mode: Security adherence
  - Security Policy: Check selected algorithms
  - Authentication mechanism
  - Access control per node

Check protection of data

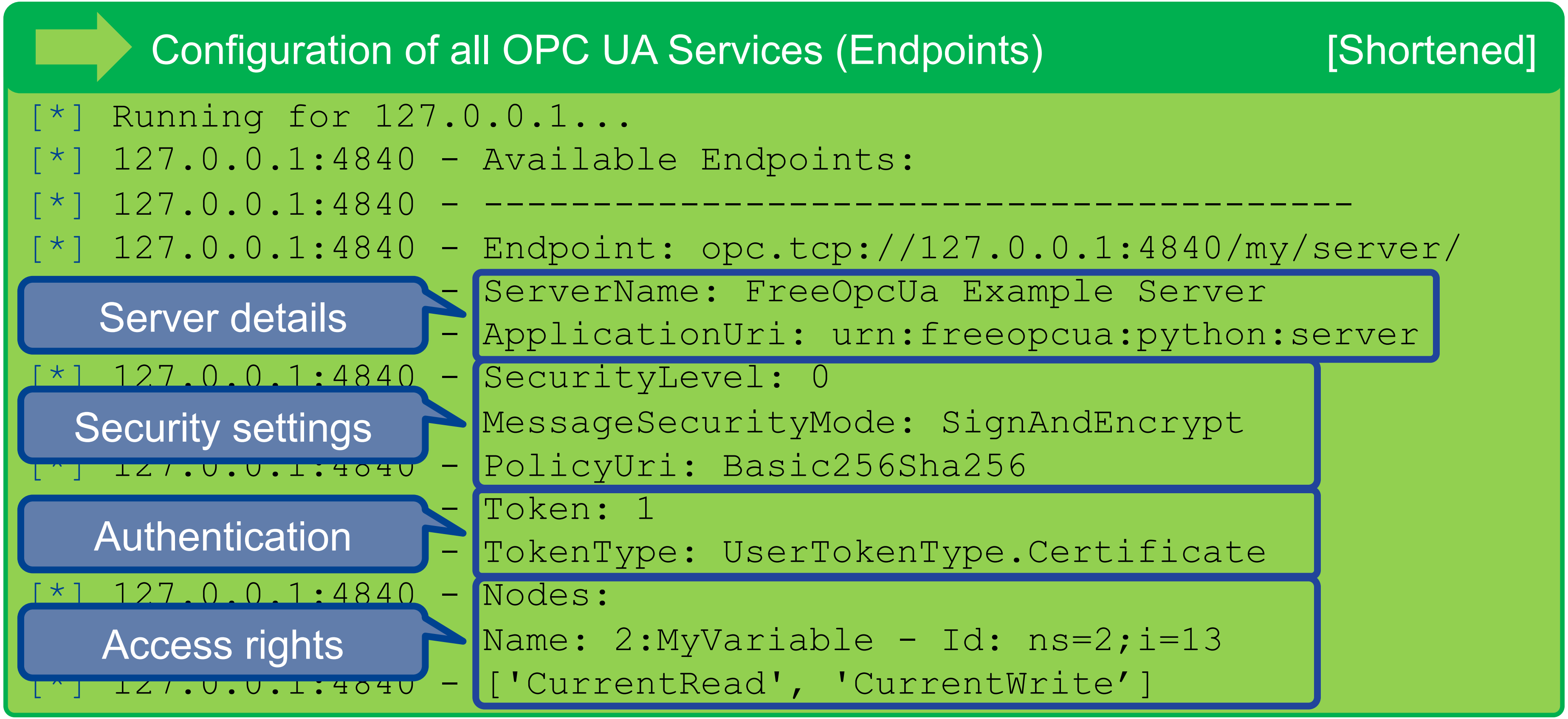
- **Get list of known OPC UA services (Endpoints)**
  - Possibility to get addresses of other deployments Restart assessment

Configuration Check: Output

Configuration of all OPC UA Services (Endpoints) [Shortened]

```
[*] Running for 127.0.0.1...
[*] 127.0.0.1:4840 - Available Endpoints:
[*] 127.0.0.1:4840 - ----------------------------------------
[*] 127.0.0.1:4840 - Endpoint: opc.tcp://127.0.0.1:4840/my/server/
[*] 127.0.0.1:4840 - ServerName: FreeOpcUa Example Server
[*] 127.0.0.1:4840 - ApplicationUri: urn:freeopcua:python:server
[*] 127.0.0.1:4840 - SecurityLevel: 0
[*] 127.0.0.1:4840 - MessageSecurityMode: SignAndEncrypt
[*] 127.0.0.1:4840 - PolicyUri: Basic256Sha256
[*] 127.0.0.1:4840 - Token: 1
[*] 127.0.0.1:4840 - TokenType: UserTokenType.Certificate
[*] 127.0.0.1:4840 - Nodes:
[*] 127.0.0.1:4840 - Name: 2:MyVariable - Id: ns=2;i=13
[*] 127.0.0.1:4840 - ['CurrentRead', 'CurrentWrite’]
```

Configuration Check: Output



Configuration of all OPC UA Services (Endpoints) [Shortened]

```
[*] Running for 127.0.0.1...
[*] 127.0.0.1:4840 - Available Endpoints:
[*] 127.0.0.1:4840 - ----------------------------------------
[*] 127.0.0.1:4840 - Endpoint: opc.tcp://127.0.0.1:4840/my/server/
                   - ServerName: FreeOpcUa Example Server
                   - ApplicationUri: urn:freeopcua:python:server
[*] 127.0.0.1:4840 - SecurityLevel: 0
                     MessageSecurityMode: SignAndEncrypt
[*] 127.0.0.1:4840 - PolicyUri: Basic256Sha256
                   - Token: 1
                   - TokenType: UserTokenType.Certificate
[*] 127.0.0.1:4840 - Nodes:
                     Name: 2:MyVariable - Id: ns=2;i=13
[*] 127.0.0.1:4840 - ['CurrentRead', 'CurrentWrite’]
```

Server details

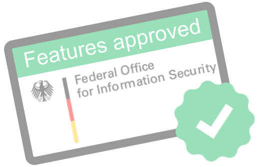
Security settings

Authentication

Access rights

Conclusion

- **OPC UA prime candidate for secure industrial communication**
  - ▶ Security attested by the Federal Office for Information Security in Germany
  - ▶ Only secure if configured correctly
    - ■ Large variety of security settings



- **Our work: Metasploit Framework module to assess OPC UA deployments**
  - ▶ Find deployments
  - ▶ Check for weak authentication parameters
    - ■ Protect deployments from malicious access
  - ▶ Get configuration for further inspection
    - ■ Ensure secure communication to avoid eavesdropping, MitM attacks, …
  - ▶ Available on github.com/COMSYS/msf-opcua

Thank you for your attention!