black hat EUROPE 2021
november 10-11, 2021
BRIEFINGS

Resting on Feet of Clay: Securely Bootstrapping OPC UA Deployments

Alessandro Erba, Anne Müller, Nils Ole Tippenhauer

CISPA — Helmholtz Center for Information Security
Saarbrücken, Germany

Industrial Control Systems security

Industrial Control Systems and Critical infrastructures are a valuable assets.

Process disruption may cause:

- Arm human beings
- Monetary loss

Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra
June 4, 2021, 9:58 PM GMT+2

ICS and Industrial Protocols security

- Popular industrial protocols often do not support security features by design.
  - E.g., Ethernet/IP, Modbus/TCP, PROFINET
- Legacy Hardware and Software
  - Missing support to security features
- Sensors and actuators can drive the system to unsafe states
  - Sensors and actuator commands are not authenticated

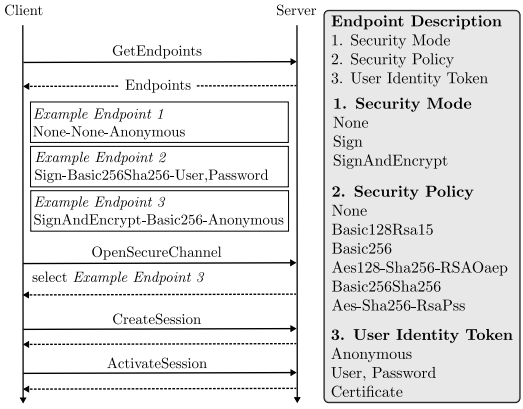
OPC Unified Architecture (UA)

- Industrial M2M protocol
- Platform-independent
- Secure communication
  - Authentication, encryption (different modes)
- Developed by OPC foundation, current version 1.04 released in 2018

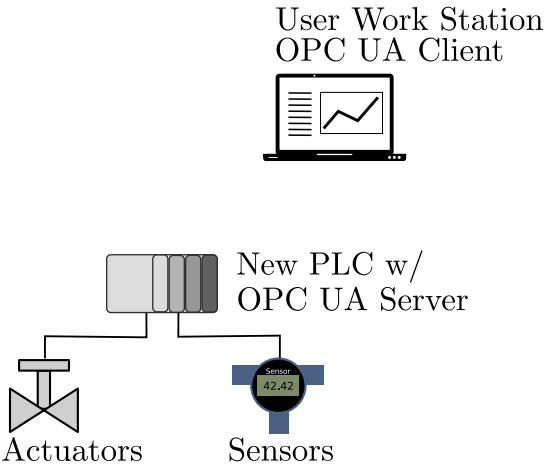
German BSI reviewed OPC UA security and found no systematic errors
Dahlmanns et al. (2020) found large numbers of insecure OPC UA systems online

Introduction to OPC UA security

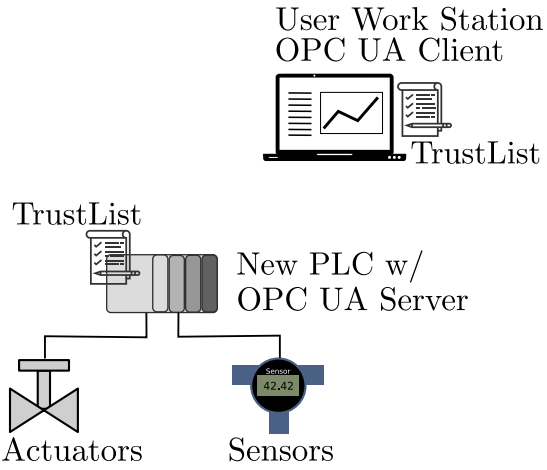
- Servers offer endpoints
- Each endpoint can have own security mode, security policy, and user identity
- Security modes
  - None, Sign, SingAndEncrypt
- Security policies
  - Concrete scheme, e.g., Basic256Sha256
- User identity, authentication
  - User and Password
  - Certificate based



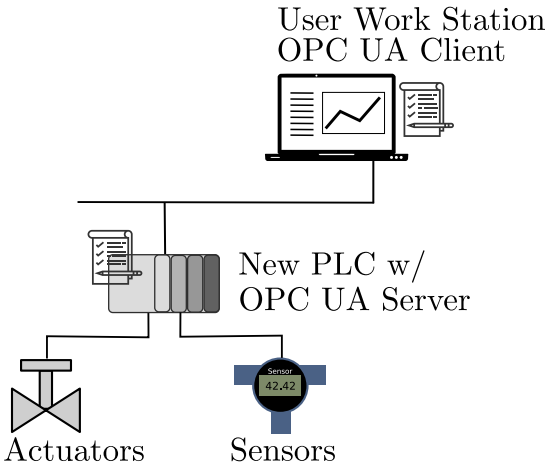
Example Addition of New Device



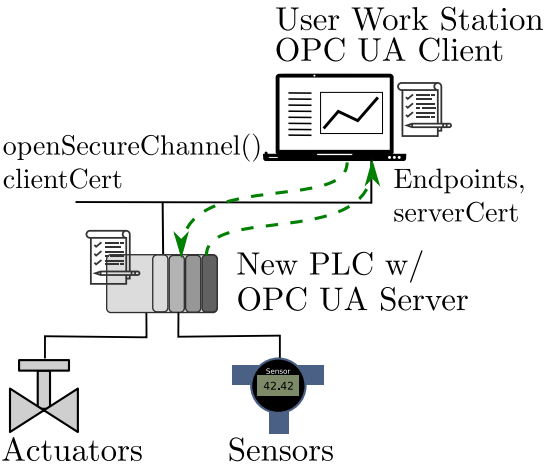
Example Addition of New Device



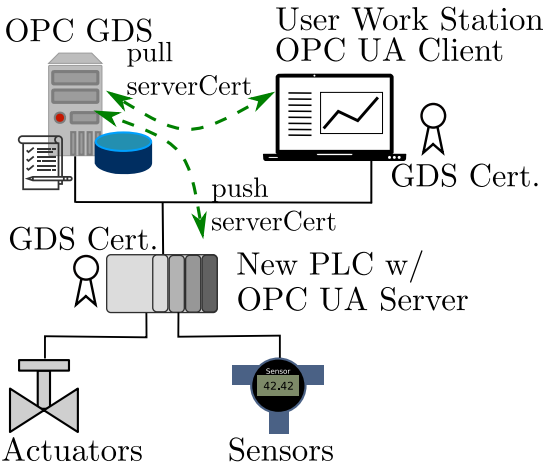
Example Addition of New Device



Example Addition of New Device



Example Addition of New Device



How is the Trust Bootstrapped?

- How does the new device get the trust root (e.g., cert of GDS)?
- On Internet, root CAs have their certs shipped in clients
  - Not possible for ICS setting (self-signed certs, no Internet)
- *How is this solved in practise?*
- *What are challenges to set up OPC UA security?*
- How do libraries and OPC products
  - Recommend security configurations?
  - Address this trust root issue?

Review of artifacts' OPC UA security features

We reviewed 48 OPC UA enabled products, to verify how and which security features are implemented.

Review of artifacts' OPC UA security features

Table: ●/○ product supports/not supports a feature. ◐ problems with feature configuration.

+After a preprint release of this manuscript, the documentation related to the product was updated. Now it supports security and it is certified.

Vendor	Platform	OPC Cert.	Pub-Sub	GDS	Security	Trust List	Recommended Policy
B&R	ADI OPC UA	●	○	○	●	●	Not specified
Bachmann	OPC UA Client/Serv.	○	○	○	◐	◐	Not specified
Beckoff	TC3 OPC UA	○	○	○	◐	◐	Deprecated policy
Beijer	iX Developer	○	○	○	○	○	None
Bosch Rexroth	ctrlX CORE	○	○	○	●	◐	None not supported
General Electric	iFIX	○	○	●	●	◐	Basic256Sha256
Honeywell	ControlEdge Builder	○+	○	○	○	○	None
Lenze	Easy Starter	○	○	○	◐	◐	Deprecated policy
Mitsubishi	MX Configurator-R	●	○	○	●	●	None
National Instr.	InsightCM	○	○	○	●	●	None
Omron	SYSMAC-SE2	●	○	○	●	●	Not specified
Panasonic	HMWIN Studio	○	○	●	●	◐	Not specified
Rockwell	Factory talk linx	○	○	○	●	●	Not specified
Schneider	Control Expert	●	○	○	●	●	Basic256Sha256
Siemens	STEP 7	●	○	●	●	◐	Not specified
Weidmüller	u-create studio	○	○	○	●	●	Basic256Sha256
Yokogawa	SMARTDAC+	○	○	○	○	○	None
Codesys based platforms							
Codesys	Codesys V3.5	○	●	○	●	◐	Not specified
ABB	Automation Builder	○	○	○	●	◐	Basic256Sha256
Eaton	XSOFT-CODESYS	○	○	○	●	◐	Not specified
Hitachi	HX Codesys	○	○	○	●	◐	Not specified
Wago	e!cockpit	●	○	●	●	◐	Not specified

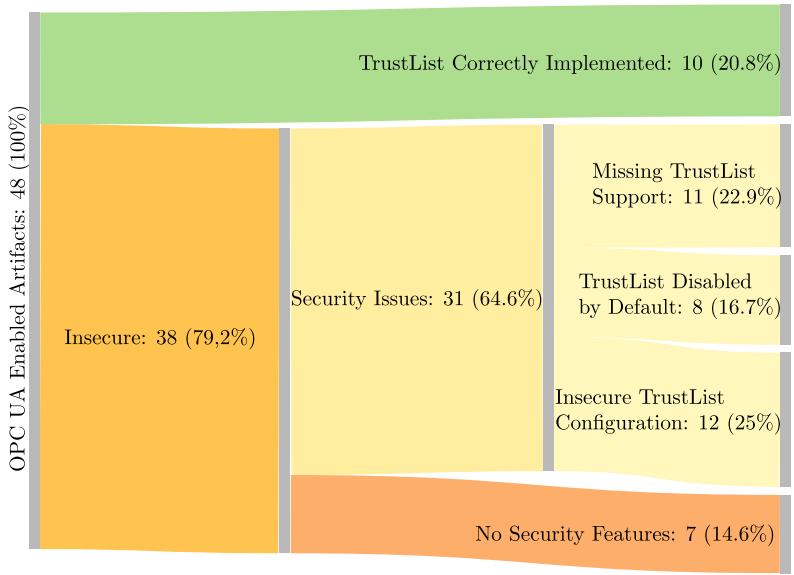
Review of artifacts' OPC UA security features

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

+Server certified, client not certified. *Denotes that the feature is going to be introduced in the next release

Name	Lang.	OPC Cert.	Pub Sub	GDS	Server Security	Server Trust List	Server Demo App.	Client Security	Client Trust List	Client Demo App.
ASNeG	C++	○	○*	○	●	○	-	○*	-	-
Eclipse Milo	Java	○	○	○	●	●	●	●	◐	○
Free OpcUA	C++	○	○	○	-	-	-	○	-	-
LibUA	C#	○	○	○	●	○	○	●	○	○
node-opcua	.js	○	○*	○	●	●	◐	●	○	○
opc-ua-client	C#	○	○	-	-	-	-	●	●	◐
opcua	Rust	○	○	○	●	●	◐	●	●	◐
opcua	Golang	○	○	○	-	-	-	●	-	-
opcua	TypeScript	○	○	-	-	-	-	○	-	-
opcua4j	Java	○	○	○	○	-	-	-	-	-
open62541	C	◐+	●	○	●	●	◐	●	●	◐
OpenScada UA	C++	○	○	○	●	○	○	●	○	○
Python-opcua	Python	○	○	○	●	○	○	●	○	○
S2OPC	C	◐+	●	○	●	●	●	●	◐	◐
UA.NET	C#	●	○	●	●	●	●	●	●	◐
UAexpert	C++	●	○	○	-	-	-	●	●	◐

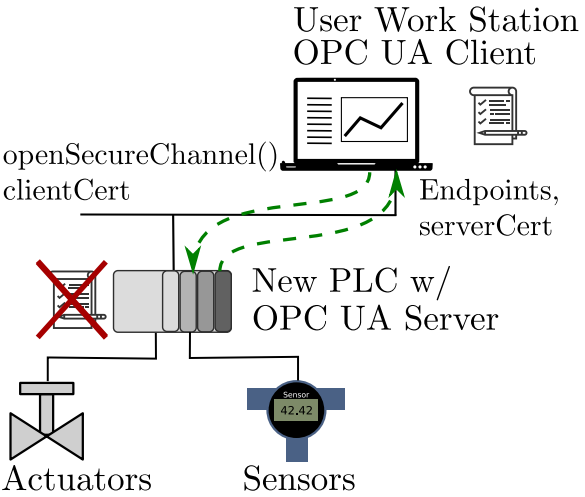
Review of artifacts' OPC UA security features



Review of artifacts' OPC UA security features

Security issues: Missing Support to Trust List

Exchange encrypted messages with untrusted parties



Review of artifacts' OPC UA security features

Security issues: Trust List disabled by default

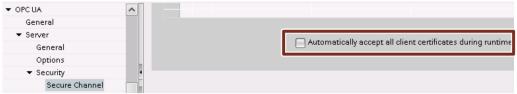
2.1.4 Security via certificate management (optional)

The following prerequisites have to be fulfilled for these settings:

- Global security settings are enabled
- You are logged in to the global security settings
- Client certificates are available.

The following instruction shows you what you have to configure, in order to only allow OPC UA clients with defined software certificates to connect to the OPC UA server:

1. Navigate to the "Properties" of the configured S7-1500 CPU in the TIA Portal.
2. Navigate to the "OPC UA" > "Server" > "Security" > "Secure Channel" inspector window and disable the "Automatically accept all client certificates during runtime" check box in "Trusted clients".



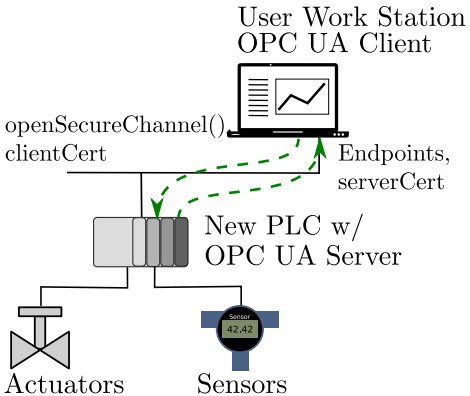
Source: SIEMENS S7-1500 OPC UA Server User Manual

Review of artifacts' OPC UA security features

Security issues: Insecure Trust List configuration

The OPC UA standard allows this behavior:

- New certificates are stored in a quarantine list
- Assumes that trained personnel is authorized to trust incoming certificates.

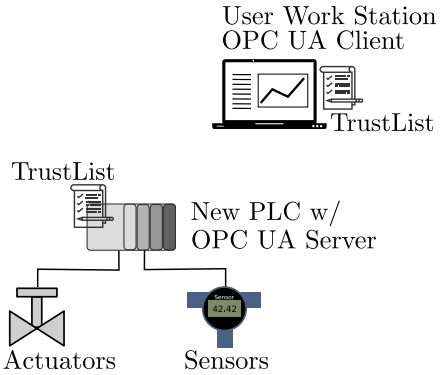


Review of artifacts' OPC UA security features

Security issues: Insecure Trust List configuration

The OPC UA standard allows this behavior:

- New certificates are stored in a quarantine list
- Assumes that trained personnel is authorized to trust incoming certificates.

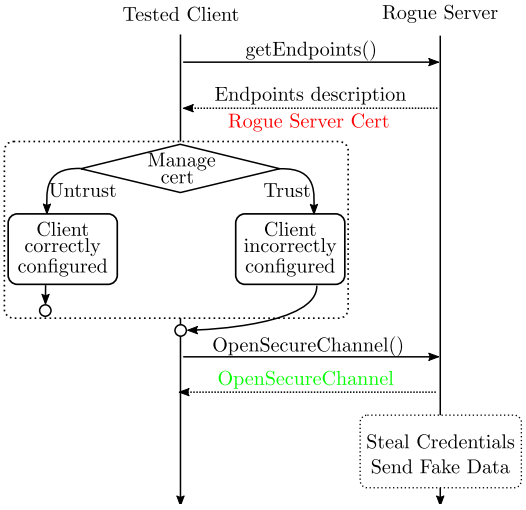


This is Fine

Attacks against OPC UA deployments

Rogue Server

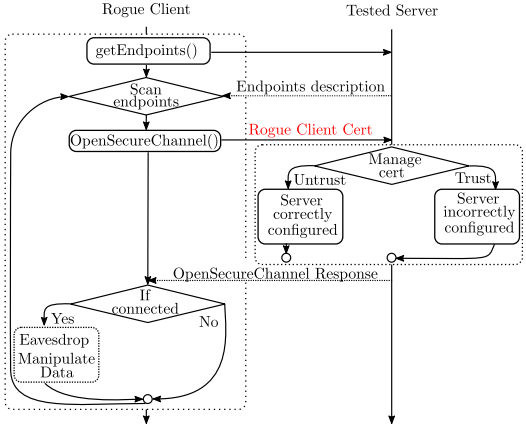
- The attacker impersonates a server on the network
- A new client is installed in the network
- The benign client shares credentials with the untrusted server
- The benign client is fed with erroneous sensor data



Attacks against OPC UA deployments

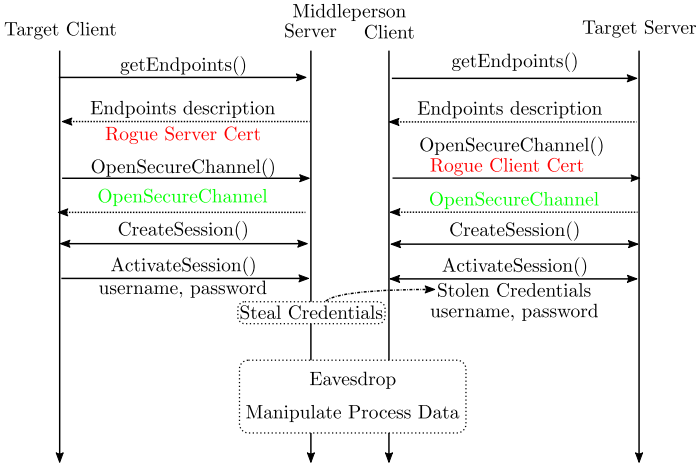
Rogue Client

- The attacker impersonates a legitimate client on the network
- The malicious client is installed in the network
- The malicious client reads sensor readings and process information
- The malicious client issues commands to the PLC



Attacks against OPC UA deployments

Middleperson attack



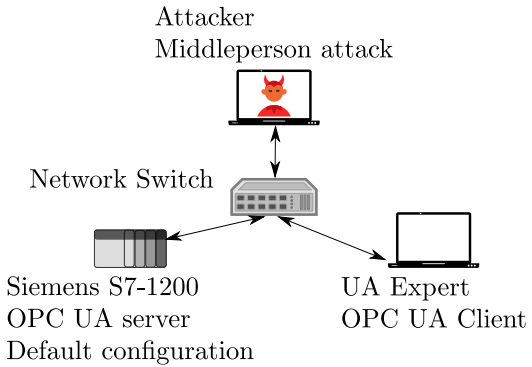
POC implementation

- Implemented in Python
  - Python OPC UA library
- CLI

Features:

- Rogue Server
- Rogue Client
- Middle-person attack
- Steal user credentials
- Clone legitimate certificates

Available at `https://github.com/scy-phy/OPC-UA-attacks-POC`



Discussion of possible countermeasures

- Enable secure behaviors by default
  - From opt-in security to security by default
- Distribute certificates upon connection (Out-of-band)
  - Avoid server and client to start until the Trust List is populated
- Add support for the missing security features

Conclusions

- OPC UA offers security features
- We have reviewed OPC UA enabled products
  - 38/48 of the considered products present some security issues
- Configuration of OPC UA deployments is challenging
  - Erroneous configuration enables attacks.
  - We have practically demonstrated them.
  - An attacker can steal user credentials in plain text.
- Impact: as reaction to our pre-print `https://arxiv.org/abs/2104.06051`
  - Several libraries/vendors already updated documentation
  - OPC UA documentation will likely be updated
  - Certification process might also be reviewed

Conclusions

- OPC UA offers security features
- We have reviewed OPC UA enabled products
  - 38/48 of the considered products present some security issues
- Configuration of OPC UA deployments is challenging
  - Erroneous configuration enables attacks.
  - We have practically demonstrated them.
  - An attacker can steal user credentials in plain text.
- Impact: as reaction to our pre-print `https://arxiv.org/abs/2104.06051`
  - Several libraries/vendors already updated documentation
  - OPC UA documentation will likely be updated
  - Certification process might also be reviewed

Thank you for your attention - Questions?