Formal verification and risk assessment of an implementation of the OPC-UA Protocol

Enrico Guerra, VR439666

Department of Computer Science
University of Verona

July 14, 2022

Index

1. Introduction
2. OPC-UA Protocol
3. Analysis with VerifPal
4. OPC-UA Protocol Risk Assessment
5. Conclusions

Introduction

Objectives

Risk assessment on an implementation (*asyncua*) of the OPC-UA protocol:

- Assets identification.
- Formal verification of some security properties through a protocol verifier (VerifPal).
- Threats analysis and risk assessment.

Context

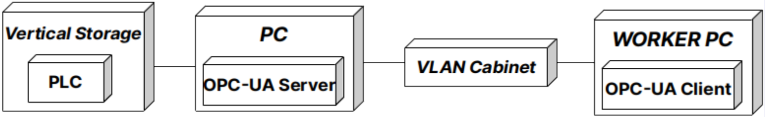
OPC-UA *asyncua* is used in ICE Laboratory, Verona.

Introduction

Analysis method

- Interviews with the staff of the ICE laboratory
- OPC Foundation manuals
- Github source of *asyncua*
- Academic papers on threats to the OPC-UA protocol

Base Component Diagram



The OPC-UA Protocol

Overview

Cross-platform, open source standard developed by the **OPC Foundation**.

Used to exchange data between a **Client** and a **Server**:

- Variables reading and writing
- RPCs calling
- Data saving

Properties we want to be preserved:

- Confidentiality
- Integrity
- Availability
- Authentication
- Non-repudiation

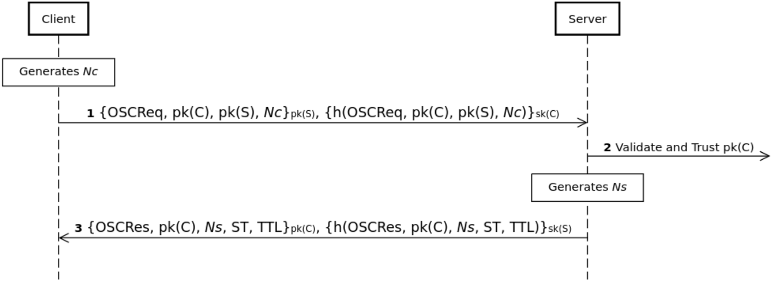
The OPC-UA Protocol

Protocol handshake

Divided in phases:

- Secure Channel establishment.
- Symmetric Keys derivation
- Session creation and activation.

Example of Sequence Diagram


Client
Server
Generates *Nc*
1 $\{\text{OSCReq}, pk(C), pk(S), Nc\}_{pk(S)}, \{h(\text{OSCReq}, pk(C), pk(S), Nc)\}_{sk(C)}$
2 Validate and Trust pk(C)
Generates *Ns*
3 $\{\text{OSCRes}, pk(C), Ns, ST, TTL\}_{pk(C)}, \{h(\text{OSCRes}, pk(C), Ns, ST, TTL)\}_{sk(S)}$

Analysis with VerifPal

Tool able to perform formal analysis of security protocols based on the **Dolev-Yao attacker model**.

Dolev-Yao model

Virtually **all-powerful**, except for cryptographic attacks.

Language

The user only needs to define **agents** and **messages**.

Goals

The tool allows to formally verify **Confidentiality**, **Authentication**, and **Freshness**.

Analysis with VerifPal

Example of an OPC-UA message abstraction in VerifPal language:

```
attacker[active]
principal Client[
 knows C_sk, C_pk, S_pk
 generates SecValue
 sign = SIGN(C_sk,
     HASH(CONCAT(SecValue, C_pk)))
 m1 = PKE_ENC(S_pk,
    CONCAT(SecValue, C_pk, sign))
]

Client -> Server: m1
```

Total messages: 6

Total code lines: 130

Analysis with VerifPal

Results

Preserved in all messages of the protocol:

- **Confidentiality**: encryption.
- **Freshness**: Sequence Numbers.
- **Integrity** and **non-repudiation**: digital signature.

OPC-UA Protocol Risk Assessment

Assets identification

In our case immaterial assets (secret shared keys, passwords, private keys, ..)

Threats identification

Logical and **infrastructural** threats.

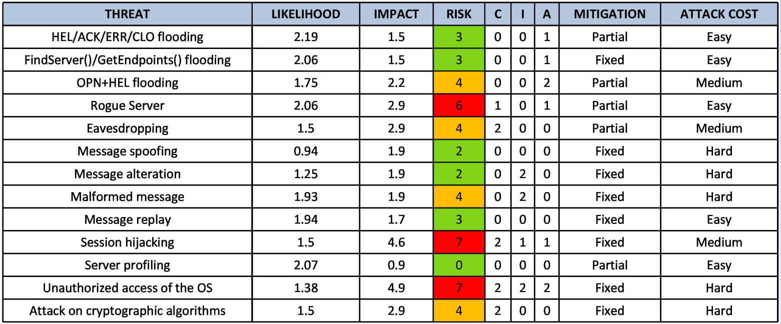
Risk evaluation

For each threat, identification of:

- An impact.
- A likelihood.
- Impacts on Confidentiality, Integrity and Availability.
- A possible mitigation.
- An attack cost.

OPC-UA Protocol Risk Assessment

Risk assessment result table:



THREAT	LIKELIHOOD	IMPACT	RISK	C	I	A	MITIGATION	ATTACK COST
HEL/ACK/ERR/CLO flooding	2.19	1.5	3	0	0	1	Partial	Easy
FindServer()/GetEndpoints() flooding	2.06	1.5	3	0	0	1	Fixed	Easy
OPN+HEL flooding	1.75	2.2	4	0	0	2	Partial	Medium
Rogue Server	2.06	2.9	6	1	0	1	Partial	Easy
Eavesdropping	1.5	2.9	4	2	0	0	Partial	Medium
Message spoofing	0.94	1.9	2	0	0	0	Fixed	Hard
Message alteration	1.25	1.9	2	0	2	0	Fixed	Hard
Malformed message	1.93	1.9	4	0	2	0	Fixed	Hard
Message replay	1.94	1.7	3	0	0	0	Fixed	Easy
Session hijacking	1.5	4.6	7	2	1	1	Fixed	Medium
Server profiling	2.07	0.9	0	0	0	0	Partial	Easy
Unauthorized access of the OS	1.38	4.9	7	2	2	2	Fixed	Hard
Attack on cryptographic algorithms	1.5	2.9	4	2	0	0	Fixed	Hard

Legenda

Likelihood: 0 - 4

Impact: 0 - 5

Risk: 0 - 10

C, **I**, **A**: 0 - 2

Conclusions

This thesis allowed to provide:

- A physical mapping of the ICE laboratory.
- An additional security evidence on the OPC-UA protocol.
- An appropriate risk assessment of OPC-UA to the state of the art.

Future works

May be focused on:

- Analysis of the interoperability of OPC-UA with brokers (Kafka, MQTT, ..).