Business from technology

OPC and MES Day Finland 2014

7 October 2014

OPC UA Security Evaluation

Pasi Ahonen, Senior Scientist, KYBER-TEO Project Manager
VTT Technical Research Centre of Finland

Contents

1.MY PAST WORK IN FINLAND: Improving Industrial Cyber Security & Continuity

- ✓Approach 2008 - 2016

2.TODAY's TOPIC: OPC UA Security Evaluation

- ✓Basics
- ✓CASE: UA Binary Stack Fuzz testing

3.CURRENT WORK: KYBER-TEO "Improving cyber security for industry" Total project (2014-2016)

- ✓ One-slide intro only

1.Improving Industrial Cyber Security

Our approach & past national projects

”to industrial cyber security”

Our Approach to Industrial Cyber Security (Including usage of OPC UA)

Year	Main Idea / Task	Project
2008-2009	1. FIND THE AREAS: – What are the main problems?	TITAN "Data Security for Industrial Automation"
2009-2010	2. STUDY BASICS: –Analyse the Existing Guidelines	TITAN "Data Security for Industrial Automation"
2011-2012	3. OPEN THEMES: –Theme Workshops	TEO-TT "Development of industrial cyber security in national theme workshops"
2011-2012	4. PROCUREMENT: –Common Reqs & Instructions	COREQ-VE "Common REQuirements for VEndors"
2012-2013	5.COMPANY CASES: –Help at the companies	COREQ-ACT "Active industrial cases for information security"
2014-2016	6.MORE COMPANY CASES: –Help in 3 WPs	KYBER-TEO "Improving cyber security for industry"

Our Approach to Industrial Cyber Security

OPC UA Hardening Guide Example

4. PROCUREMENT: –Common Reqs & Instructions

Requirement Base

COREQ-VE: SECURITY REQUIREMENTS FOR INDUSTRIAL AUTOMATION VENDOR MANAGEMENT:

Number	Class	Objective	Security act	Scope G = Gen. M = O&M P = Project	Importance 1 = Minimum 2 = Option 3 = Advanced 4 = N/A (Out)	Requirement	Responsible V=Vendor P=Principal Other=?	Additional requirements	Implementation example
1	Hardening	Hardened systems & applications	Project specific hardening guide	P	1	Vendor's hardening guide shall include: a) software and functionality to be removed, b) protection of diagnostic and configuration ports, c) disabling all unused ports on switches and routers, d) maintenance process to hardened system	V+P	The vendor shall provide an up-to-date list of platform software, licences, applications and protocols required by the system operation. If possible, use only one version of each protocol	Must find an acceptable minimum configuration for each and every device, harden according to guide, verify and apply "hardened" marking to documentation
2	Hardening	Reduced data flows	Documented data flows	P	1	Vendor shall document all data flows and storage points with identification of sensitive information	V+P	For multivendor environments, the vendor shall provide a detailed system integration guide with interface descriptions	Data flow: Source address, destination address, protocol, port, purpose/application, etc.
3	Network segmentation	Separated ICS networks	Define segmentation architecture	P	1	Vendor shall document the segmentation architecture between operative ICS and other domains	V+P	The vendor shall document in detail the used data flows between segments (and between security zones)	Critical vendor- or functional networks inside control system domain shall also be assigned to separate segments and subnetworks
4	Data safekeeping	Planned data safekeeping	Documented system data safekeeping	P	2	Vendor shall document their systems' data safekeeping capability (incl. data reduction, timeouts, data purging etc.)	V		System data safekeeping functions are typically system specific and must comply with the Principal's requirements

Instructions | Reqs - Org | **Reqs - Prep & Dev** | Reqs - Test & Comm | Reqs - Maint & Supp | References

2.TODAY's TOPIC: OPC UA Security Evaluation

2.TODAY's TOPIC: OPC UA Security Evaluation

WARNING:

I BELIEVE, WE ARE NOT EVALUATING & TESTING INDUSTRIAL DATA COMMUNICATION ENOUGH TODAY!

2.TODAY's TOPIC: OPC UA Security Evaluation

<u>Learn</u> EARLY the TARGET environment to be tested

Get familiar with the test target & its environment!

Identify areas that have encountered problems before?

Test target

- ✓ Installed Application(s)
- ✓ Used Platforms
- ✓ Settings
- ✓ Relevant Use cases
- ✓ Existing Features,
- ✓ Implemented Modes
- ✓ Etc.

Possible setup for testing?:

- OPC UA Apps
- OS Platforms
- OS & App conf
- Use cases
- Feat. & Modes
- Virtualized test environment

- ✓ **Test automation (restart target…)!**
- ✓ **Flexible test network conf.!**
- ✓ **Filtering, etc.**

2.TODAY's TOPIC: OPC UA Security Evaluation

Technological Threats

✓Vulnerabilities in systems & networks

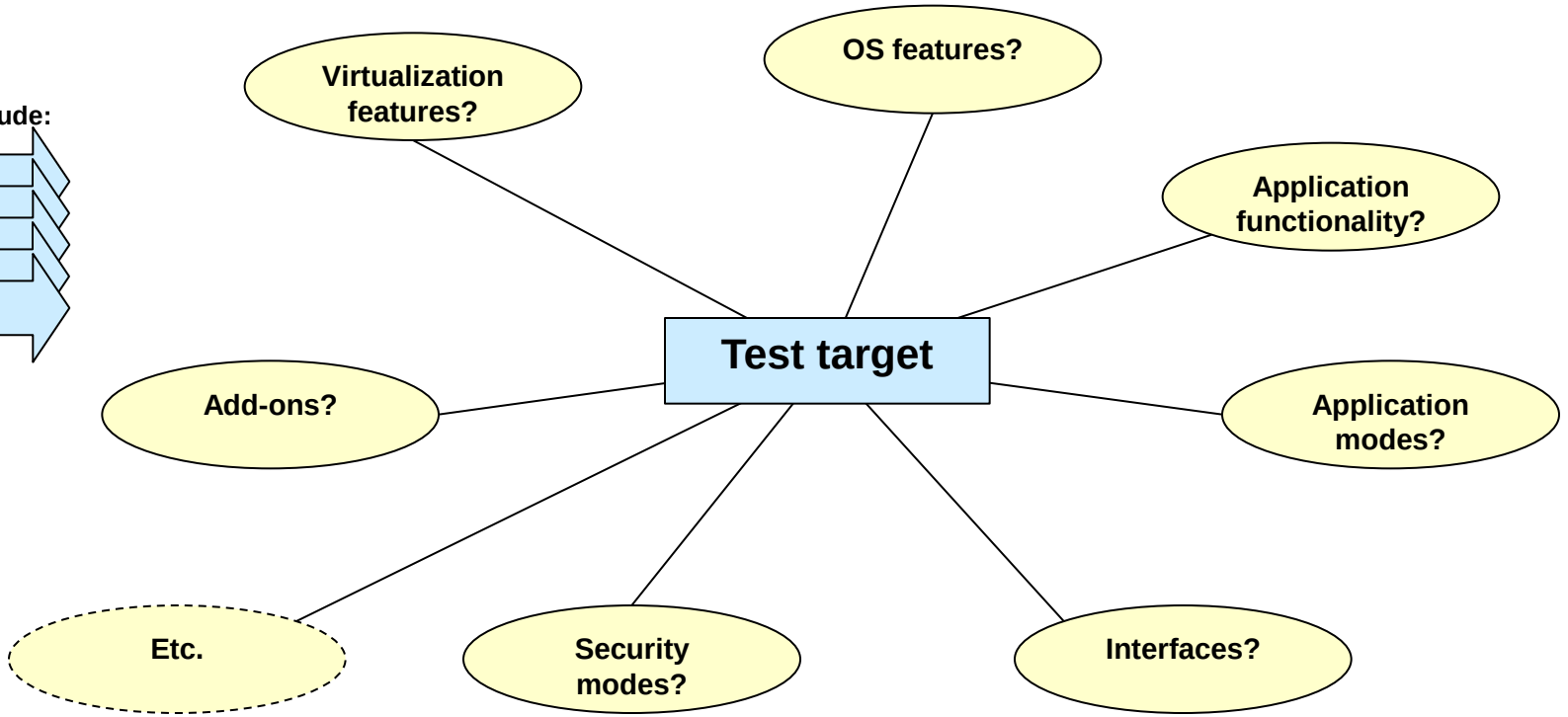
Reasons:

a) **Increased TCP/IP –** Internet type of Risks!
b) **Increased dependency** on networks (e.g. due to Certificates)
c) **Protocol based attacks** against UA XML – which may be vulnerable (attack tools exist) → Insertion of COMMANDS!
d) **System update and maintenance challenges** due to long life cycle of applications

2.TODAY's TOPIC: OPC UA Security Evaluation

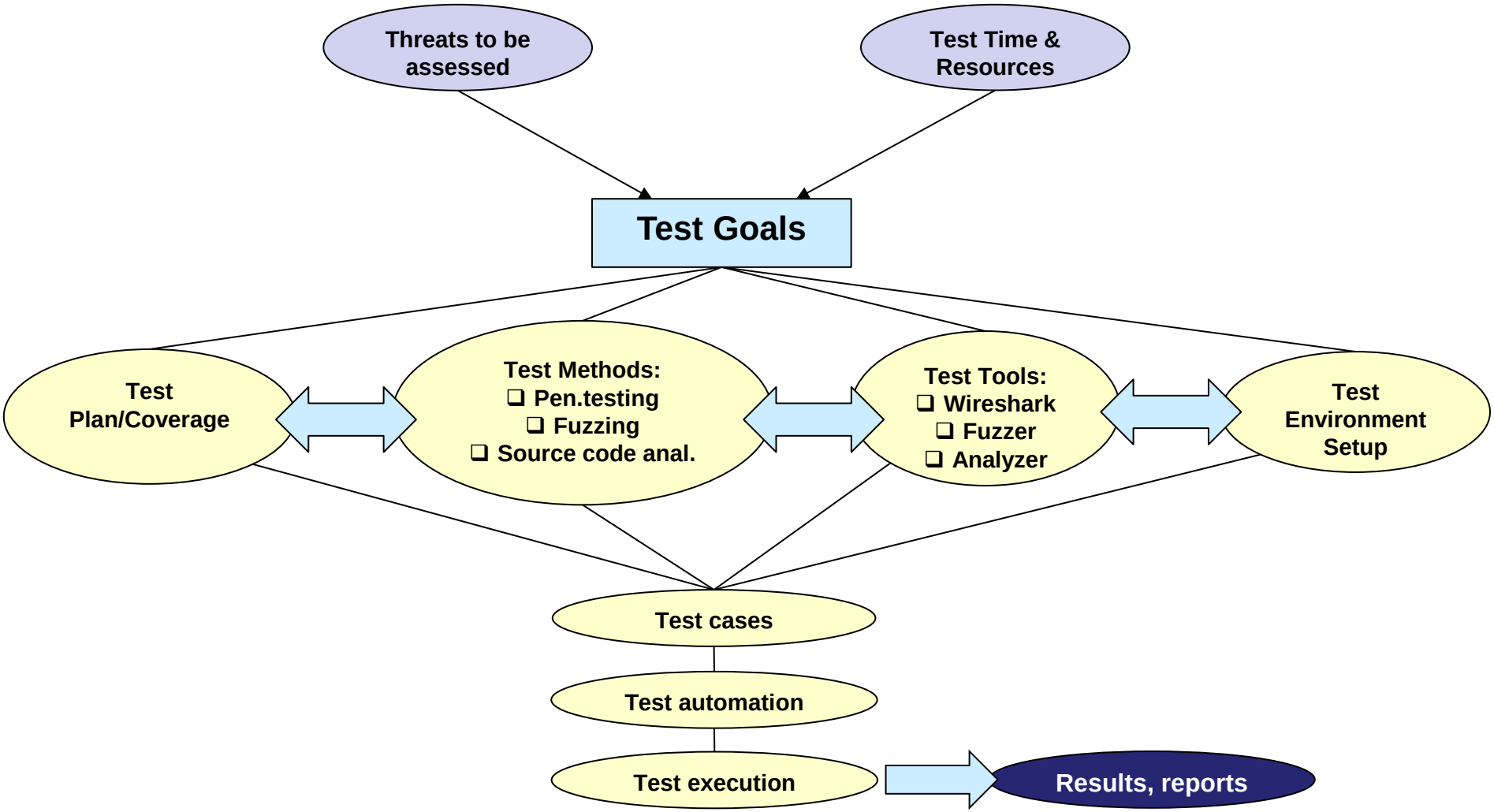
Before test runs: Agree about the SYSTEM features to be tested!

Threats to be tested may include:
Compromized Credentials?
Message Flooding?
Message Replay?
Message Header Modification?
Message Data Modification?
Rogue OPC UA node?
Etc.



2.TODAY's TOPIC: OPC UA Security Evaluation

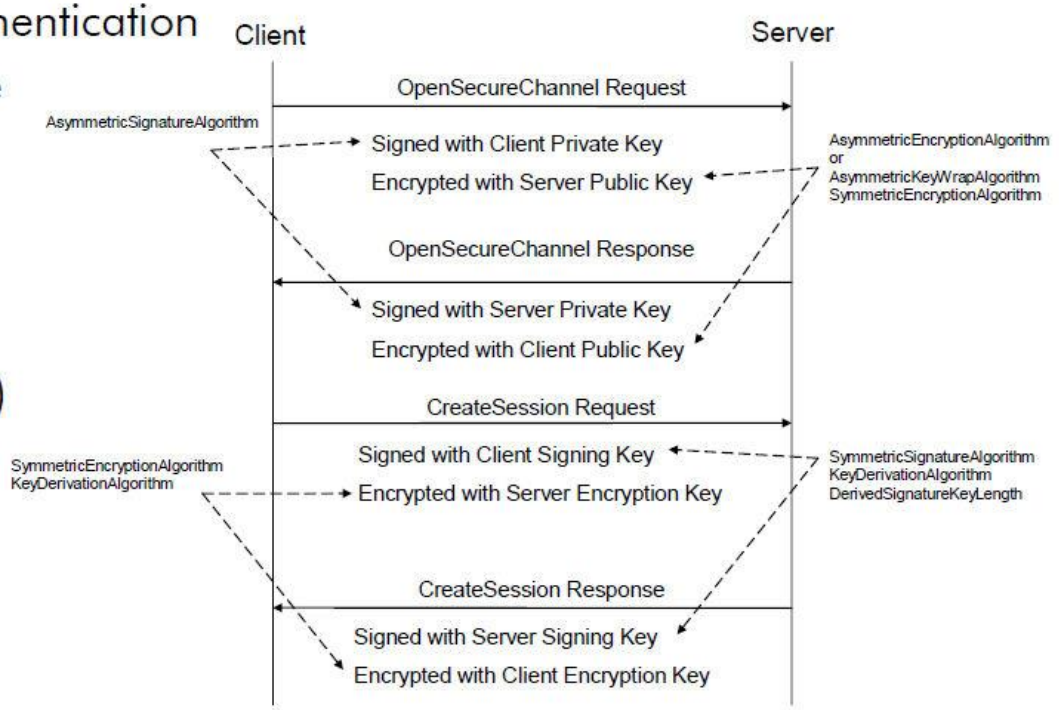
Focus on Test Goals



2.TODAY's TOPIC: OPC UA Security Evaluation

OPC UA Connection Security

- OpenSecureChannel
  - Asymmetric encryption (RSA) with ApplicationInstance Certificates (X.509v3)
  - Application authentication
  - Exchange of the symmetric encryption key
- CreateSession
  - Symmetric encryption (AES)
- ActivateSession
  - User authentication

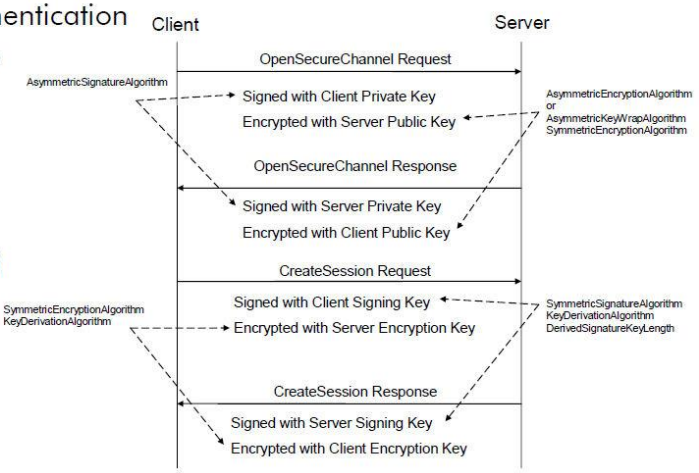


Reference/Figure: http://www.prosys.fi

2.TODAY's TOPIC: OPC UA Security Evaluation

OPC UA Authentication & Security Modes

- OpenSecureChannel
  - Asymmetric encryption (RSA) with ApplicationInstance Certificates (X.509v3)
  - Application authentication
  - Exchange of the symmetric encryption key
- CreateSession
  - Symmetric encryption (AES)
- ActivateSession
  - User authentication



Authentication

- User Authentication
  - –Anonymous
  - –User Name & Password
  - –User Certificate (X.509)
  - –External Tokens (e.g. Kerberos)
- Application Authentication
  - –Application Instance Certificate

SecurityModes

- **MessageSecurityMode**
  - **– None**
  - **– Sign**
  - **– Sign & Encrypt**
- SecurityPolicy
  - – Basic128Rsa15
  - – Basic256
  - – Basic256Sha256 (new, 1.02)
  - – New policies can be defined
- Client application defines the used security mode

Apply these modes to easely record the OPC UA message sequences!

Reference/Figure: http://www.prosys.fi

Include PKI Certificate Mgmt testing?
-Example: GDS-

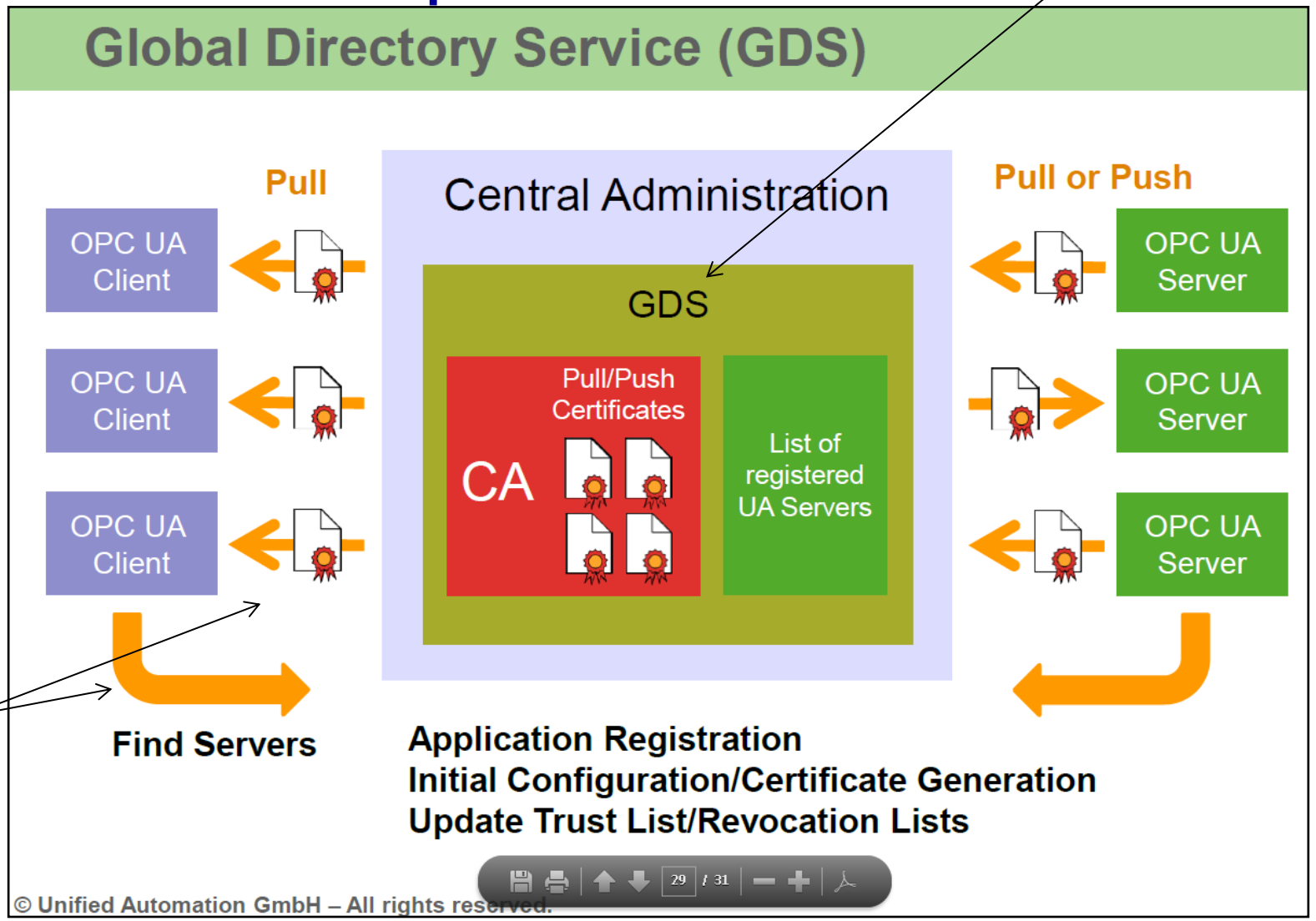
OPC UA Discovery options
- ✓ Discover on known port 4840 of a network node
- ✓ Use mDNS for ad-hoc discovery in local network
- ✓ Use GDS as central discovery server:
  - ❑ RequestCertificate
  - ❑ SignCertificate
  - ❑ RenewCertificate
  - ❑ CheckRequestStatus
  - ❑ GetTrustList

All OPC UA applications to use Certificate trust list

X.509 based **Certificate management (PKI)** messaging
- Using HTTPS Certificates for the mgmt messaging

GDS as OPC UA wrapper around any directory or CA

GDS Services as test target?



REF: https://opcfoundation.org/wp-content/uploads/2014/08/12_UA_Discovery.pdf

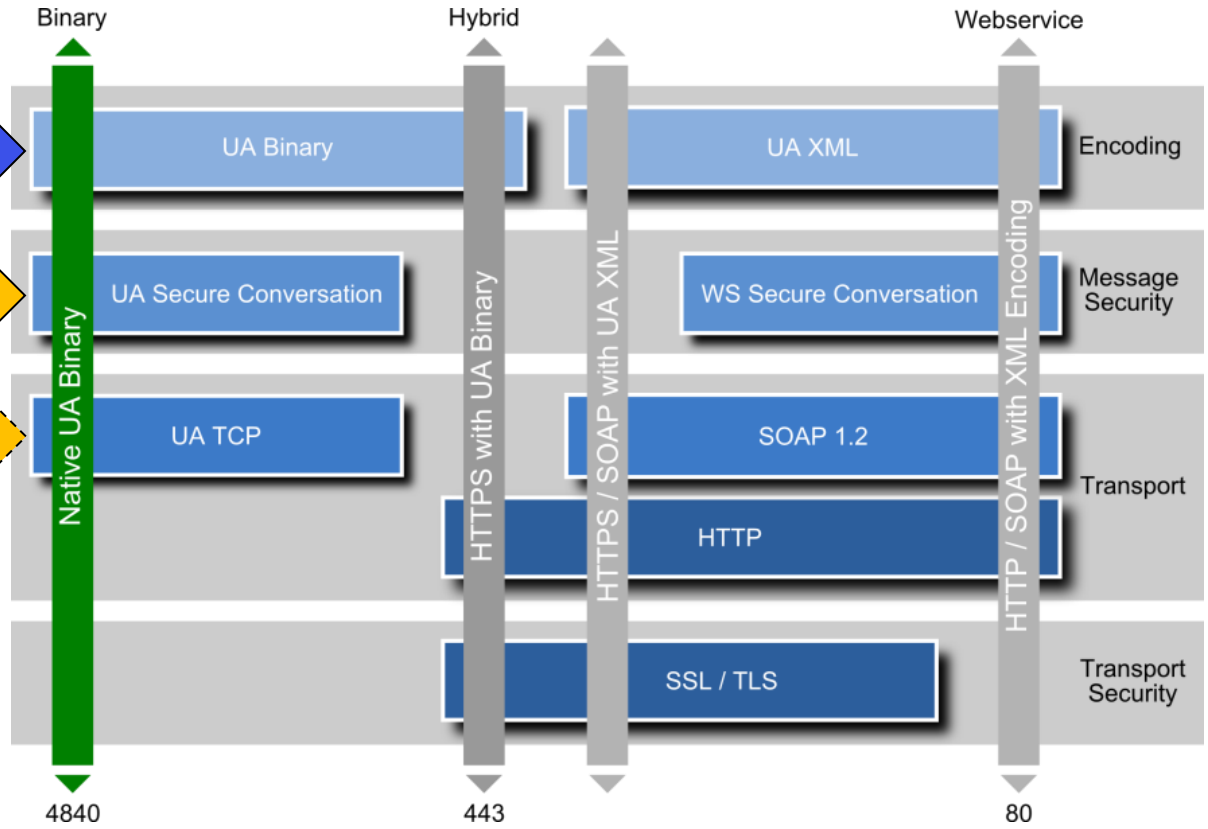
OPC UA Protocols
-Binary stack testing-

NOTE: OPC UA Security testing tools are under development right now!

Binary stack! testing:

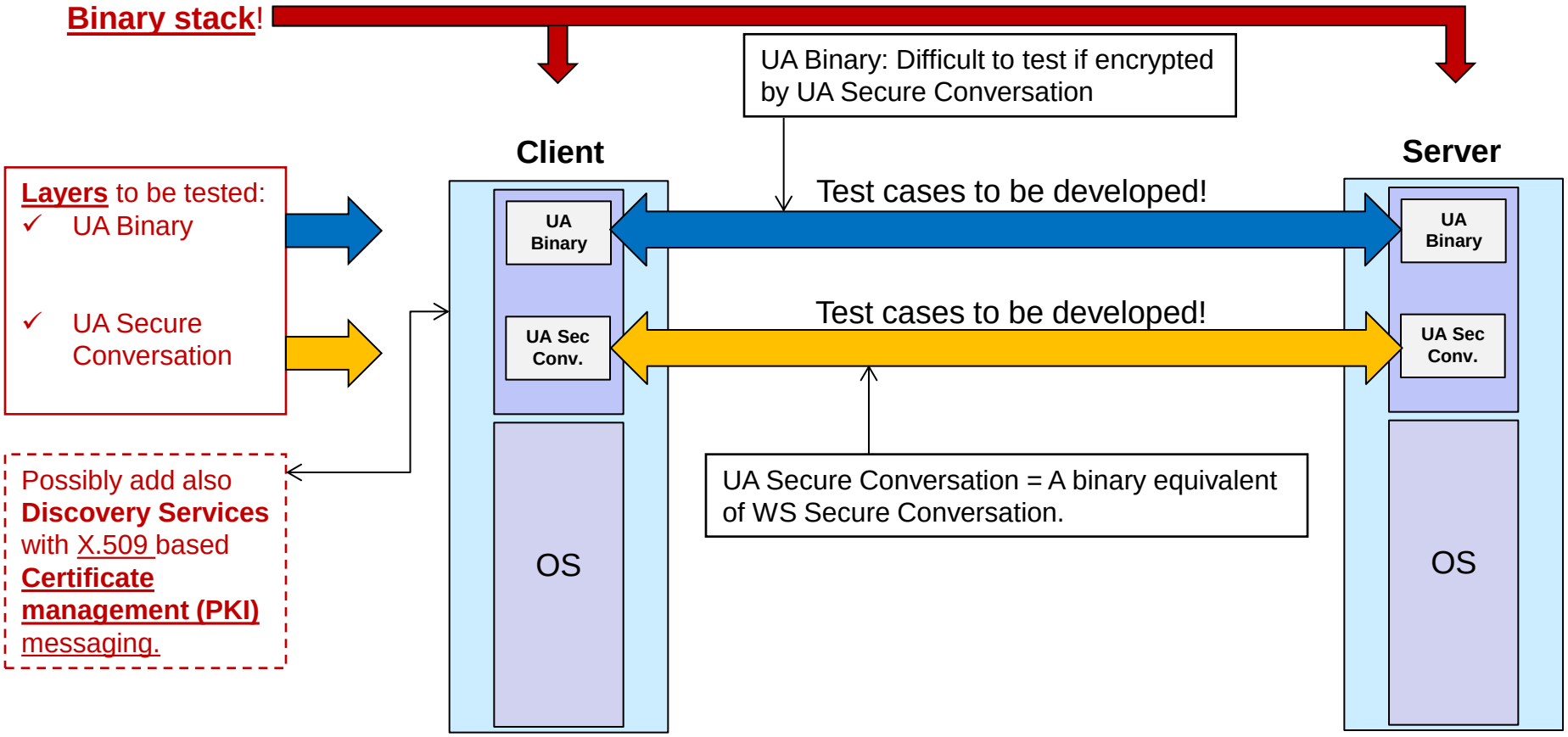
Layers to be tested:
- ✓ UA Binary
- ✓ UA Secure Conversation
- ✓ UA TCP

Test each of the three layers separately!

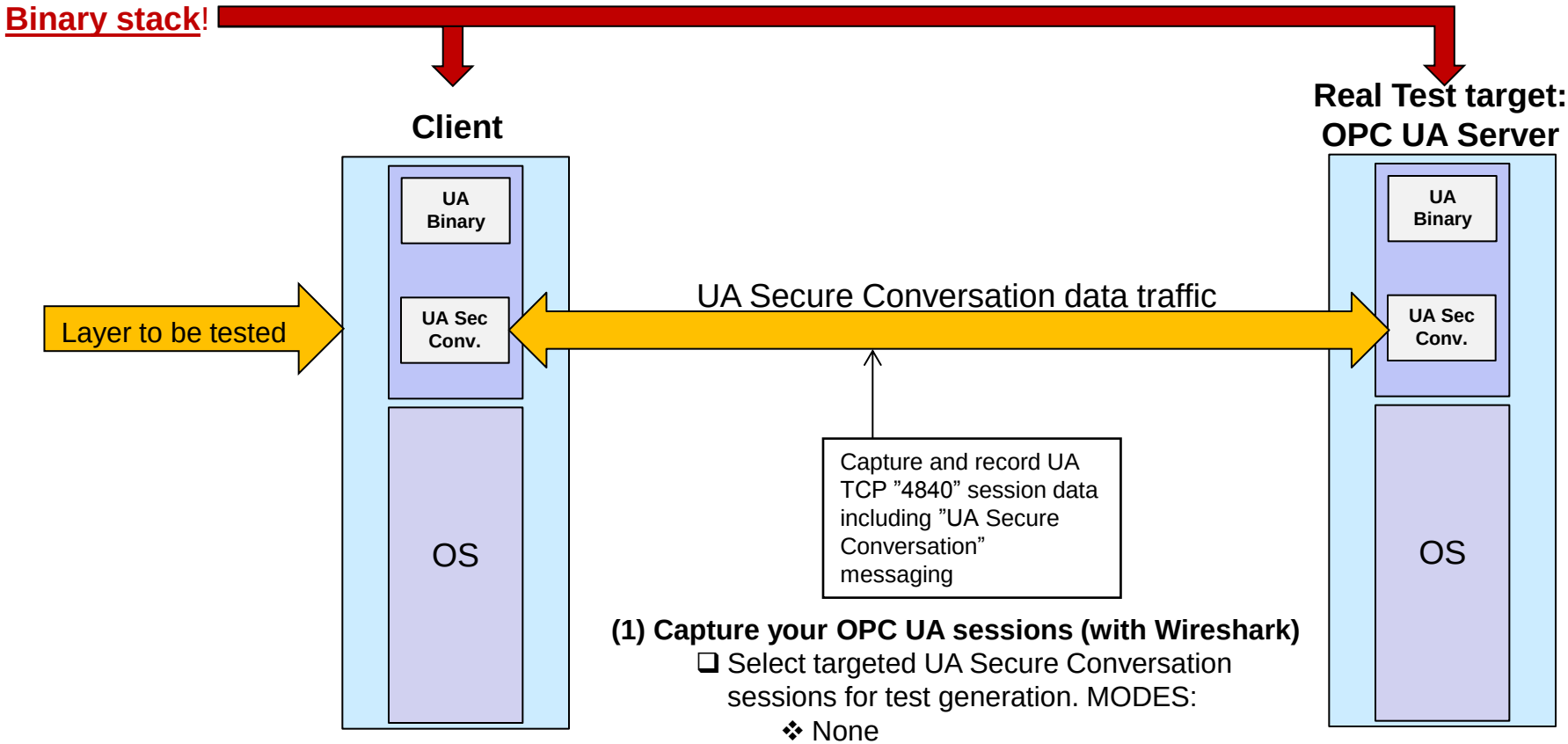


Layer figure is from: http://www.ascolab.com/en/technology-unified-architecture.html

Set Up and Configure the Test System -OPC UA Binary Stack-



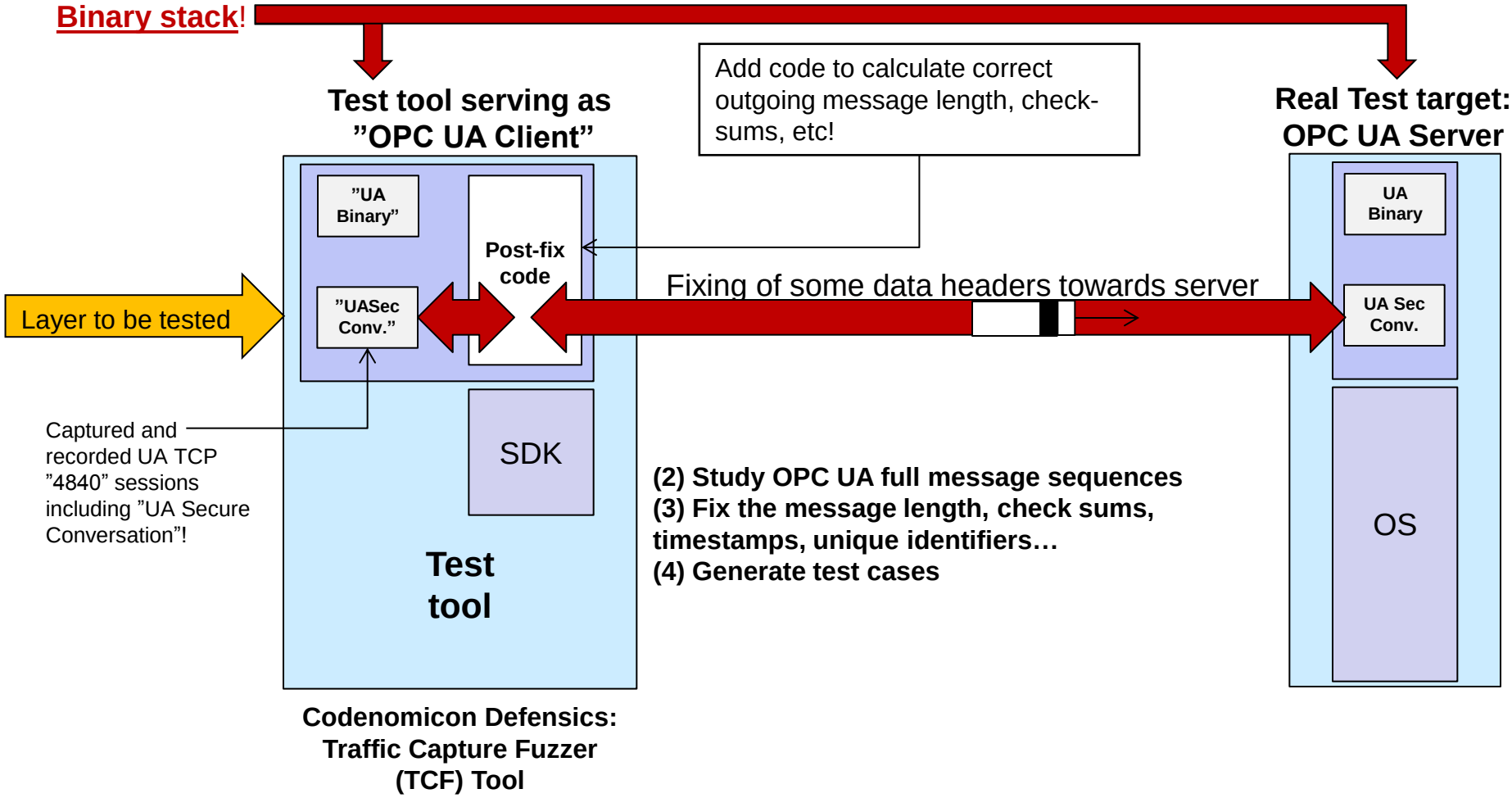
CASE: Setting Up the Fuzz testing for OPC UA Server



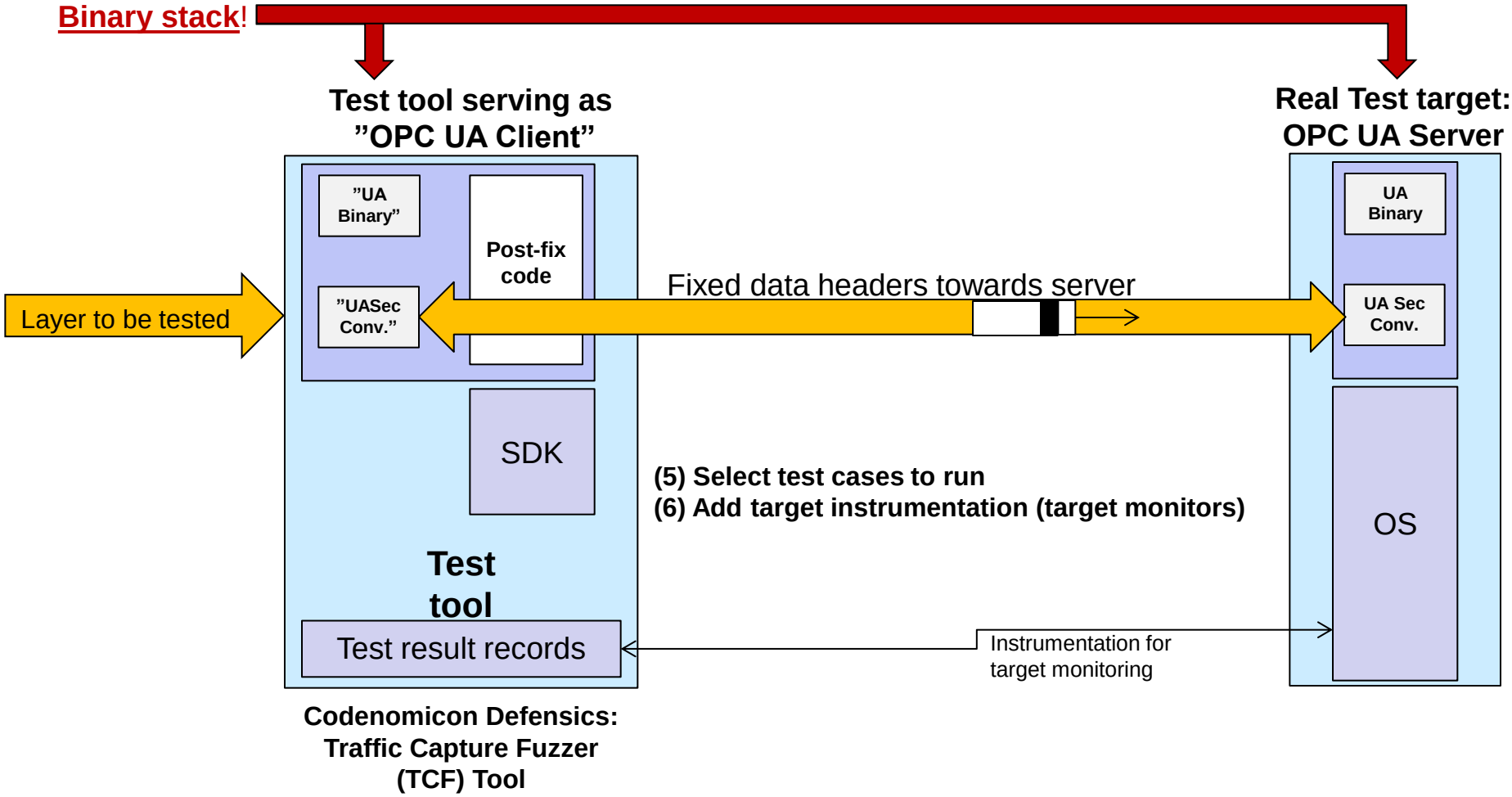
(1) Capture your OPC UA sessions (with Wireshark)

- ❑ Select targeted UA Secure Conversation sessions for test generation. MODES:
  - ❖ None
  - ❖ Sign
  - ❖ Sign & Encrypt
- ❑ Utilize e.g. filtering of sessions, etc.

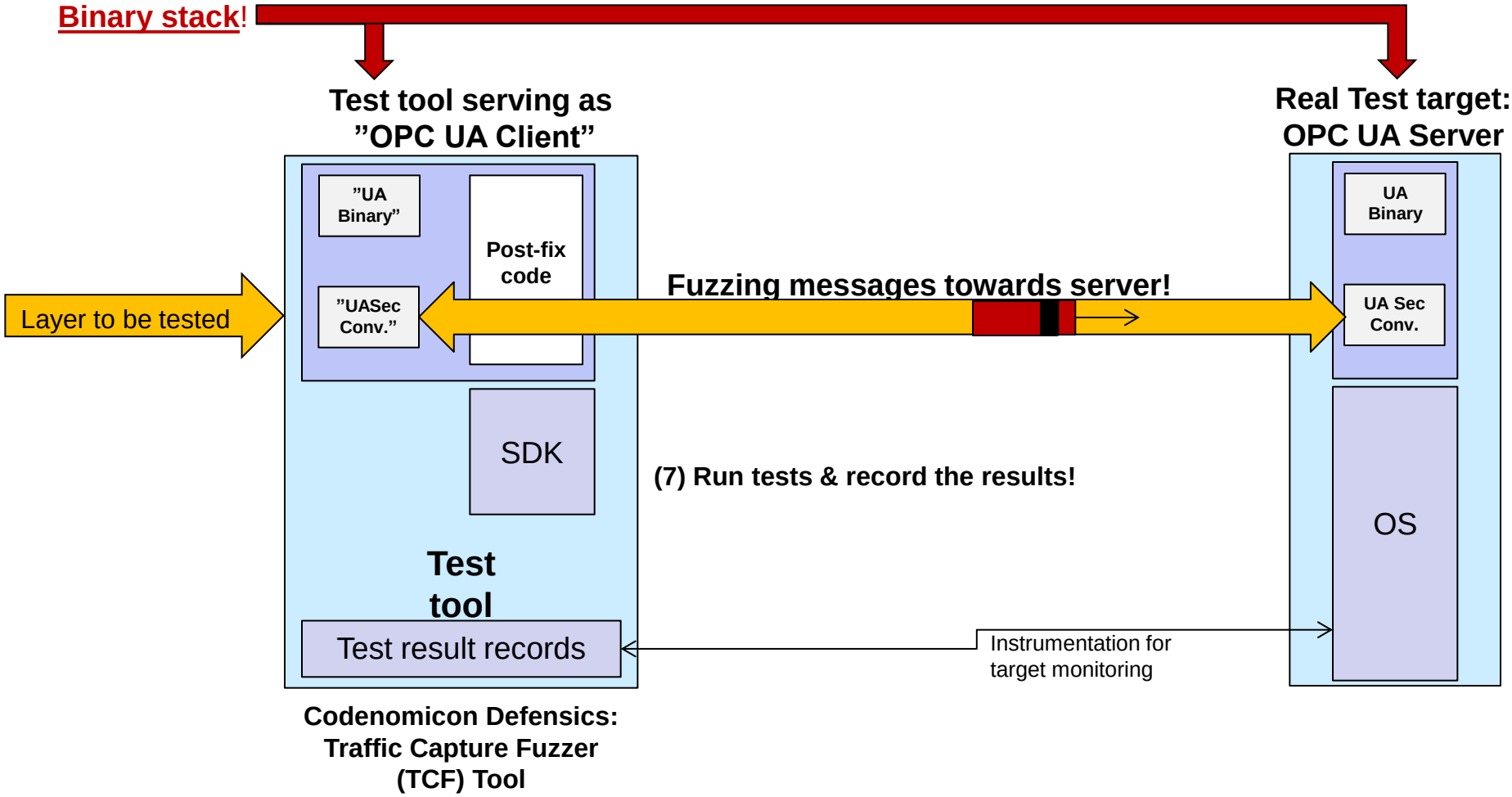
CASE: Setting Up the Fuzz testing for OPC UA Server



CASE: Setting Up the Fuzz testing for OPC UA Server

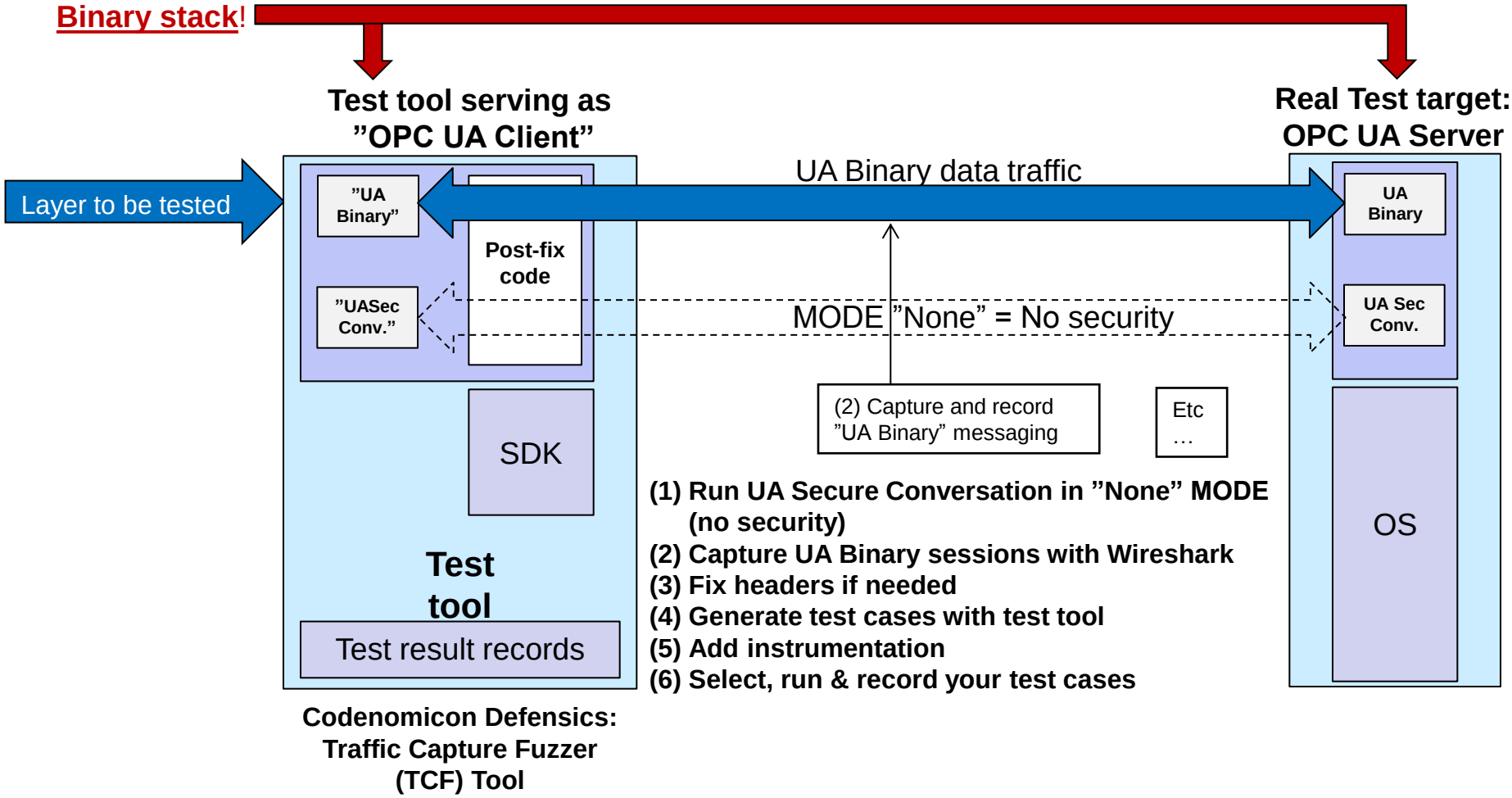


CASE: Setting Up the Fuzz testing for OPC UA Server



Codenomicon Defensics: Traffic Capture Fuzzer (TCF) Tool

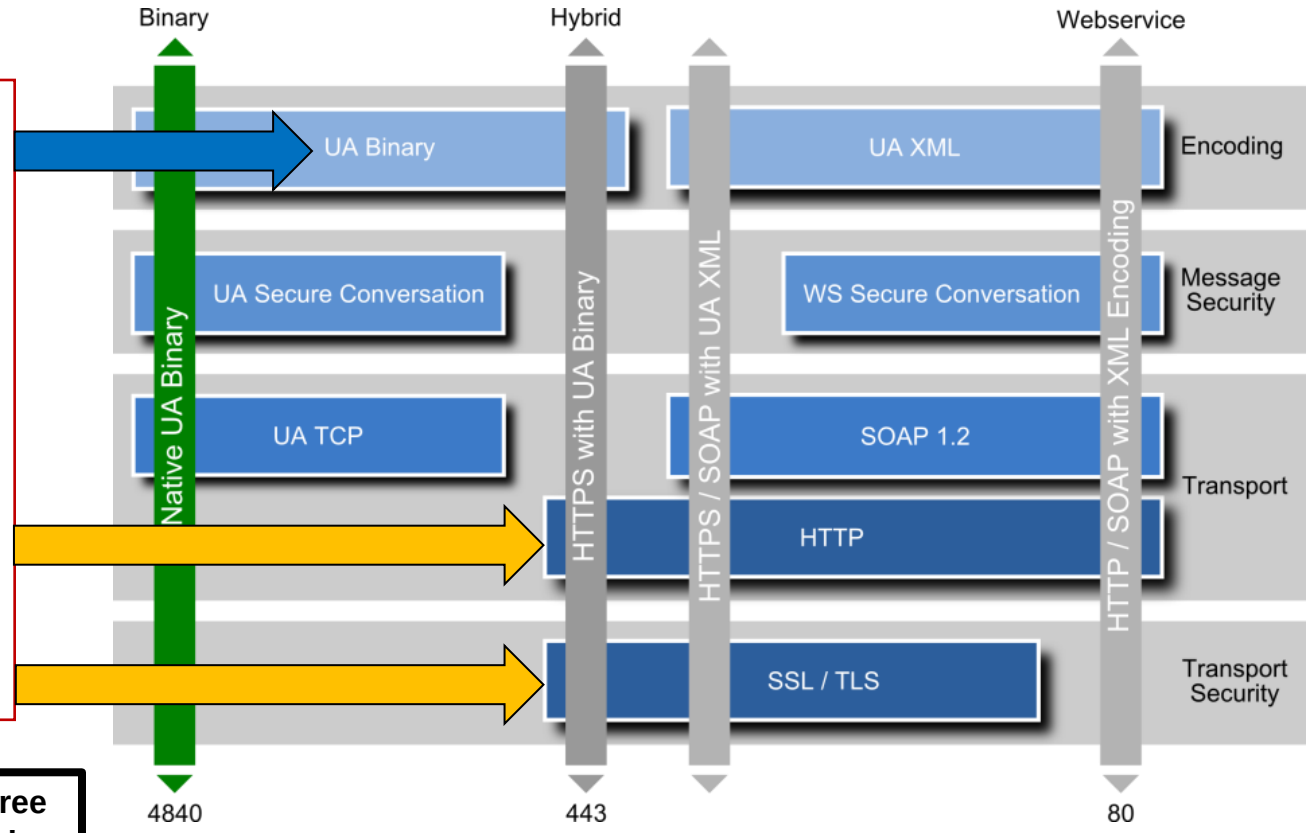
CASE: Setting Up the Fuzz testing for OPC UA Server



OPC UA Protocols
-Hybrid stack testing-

Hybrid stack! testing:

Layers to be tested:
- ✓ UA Binary
- ✓ HTTP
- ✓ SSL/TLS



Build your Test cases?

Utilize HTTP Test Suite

Utilize SSL Test Suite

Test each of the three layers separately!

Layer figure is from: http://www.ascolab.com/en/technology-unified-architecture.html

2.TODAY's TOPIC: OPC UA Security Evaluation

Main challenges in OPC UA System's Security Protection:

- Management of – OPC UA Systems & Configurations
- Establishment of – OPC UA Vendors' security evaluation activities
- System & Communication security – E.g. OPC UA Certificate management!
- Etc.

2.TODAY's TOPIC: OPC UA Security Evaluation

Technological PROTECTION

ENSURE THE AVAILABILITY OF KEYS

- ✓ Planning for long PKI Certificate life-cycles
- ✓ PKI Certificate management systems
- ✓ PKI Certificate maintenance processes

SECURE THE ACCESS TO OPC UA SYSTEMS

- ✓ Layered Defense: Frontend FW + Backend FW + Segments
- ✓ Separate: Mgt. Access / Security services maintenance / Data access
- ✓ Secure Gateway solutions (OPC UA Gateway), Monitoring
- ✓ VPN tunneling of OPC UA connections
- ✓ External Audits!

3. KYBER-TEO Project
”Improving cyber security for industry” (2014-2016)

Part of Implementing the national Cyber Security strategy 2014-2016
(see: http://www.turvallisuuskomitea.fi)

KYBER-TEO ”Improving cyber security for industry” (National NESA program 2014 - 2016)

Developing and testing SERVICES in the participating companies to ensure the cyber security and continuity of Finnish industrial production

WP 1: Cyber security practices and mappings
WP 2: Deploying the cyber security to industrial production
WP 3: Cyber security monitoring services for automation networks

GOAL: To disseminate results and experiences between companies.

Focus on co-operation

- **Participating companies**
  - ✓ **Company specific cases**
  - ✓ **Project work (technology, services)**
- **Other industrial companies (e.g. through dedicated NESA HUOVI-portal project area)**
  - ✓ **Wide company reviews**
  - ✓ **Result dissemination seminars**
- **State authority & Research co-operation: (Advice, quality, development, dissemination, education)**
  - ✓ **National Emergency Supply Agency (Project owner)**
  - ✓ **VTT (Project lead & execution)**
  - ✓ **TUT - Tampere University of Technology (Project subcontractor)**
  - ✓ **Finnish Communications Regulatory Authority - The National Cyber Security Centre (NCSC)**

Detail Information & participation to KYBER-TEO project, please contact:
Pasi Ahonen, VTT Senior Scientist, KYBER-TEO Project Manager
pasi.ahonen@vtt.fi

Contact point

Pasi Ahonen, Senior Scientist, VTT

Project Manager: TITAN, TEO-TT, COREQ-VE, COREQ-ACT, TEO-SUMMARY, KYBER-TEO…

pasi.ahonen@vtt.fi

GSM: 044-730 7152.