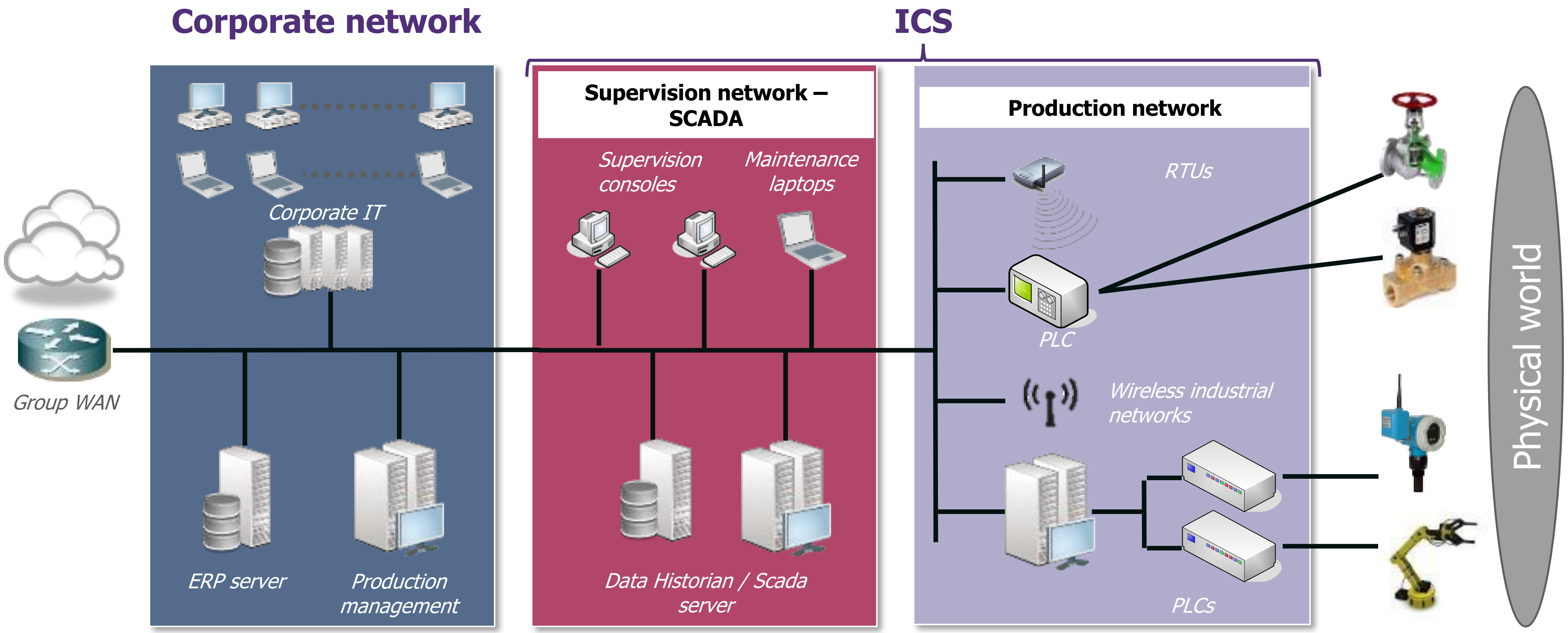
WAVESTONE

OPC-UA: A secure ICS protocol

June 2023

Arnaud Soullié
Senior Manager
@arnaudsoullie

What is an Industrial Control System (ICS)?



Legacy ICS protocols

Most widespread ICS protocols include:

/ Modbus

/ Profinet

/ Ethernet/IP

/ CIP

Most legacy ICS protocols don’t offer any security at all:

/ *No authentication*

/ *No encryption*

/ *Replayable*

OPC

The OPC suite of protocols was developed in the 90s to allow easier integration of IT and ICS

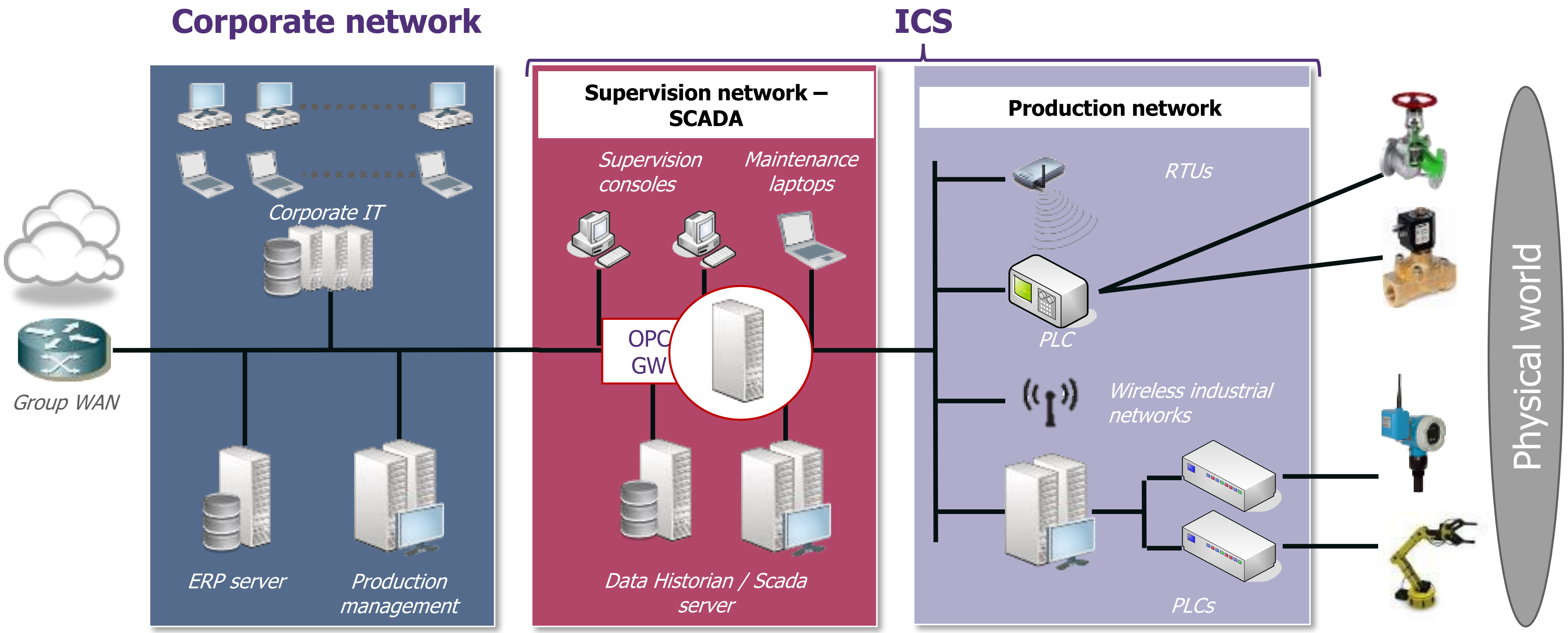
/ Protocols were based on COM/DCOM (Microsoft) technologies

/ Several variants (OPC-DA / OPC A&E / OPC HAD / OPC-DX)

➔ Limited to Microsoft world

➔ Doesn’t play nice with firewalls

What is an Industrial Control System (ICS)?



Confidential

OPC-UA

OPC-UA is a brand-new protocol created in 2006

/ *Cross-platform*

/ *Available for free*

/ *Provides security features!*

Available over several transport layers: TCP, HTTP, MQTT

You can subscribe to “data change” instead of polling

Use of data models to precisely describe data and allow better interoperability

Concept of namespaces and nodes: everything is a node

A *very* complex protocol: 70 pages of specifications for Modbus, thousands for OPC-UA

OPC-UA security features

OPC-UA provides both signature & encryption, through:

A Security Mode:

- None
- Sign
- Sign & Encrypt

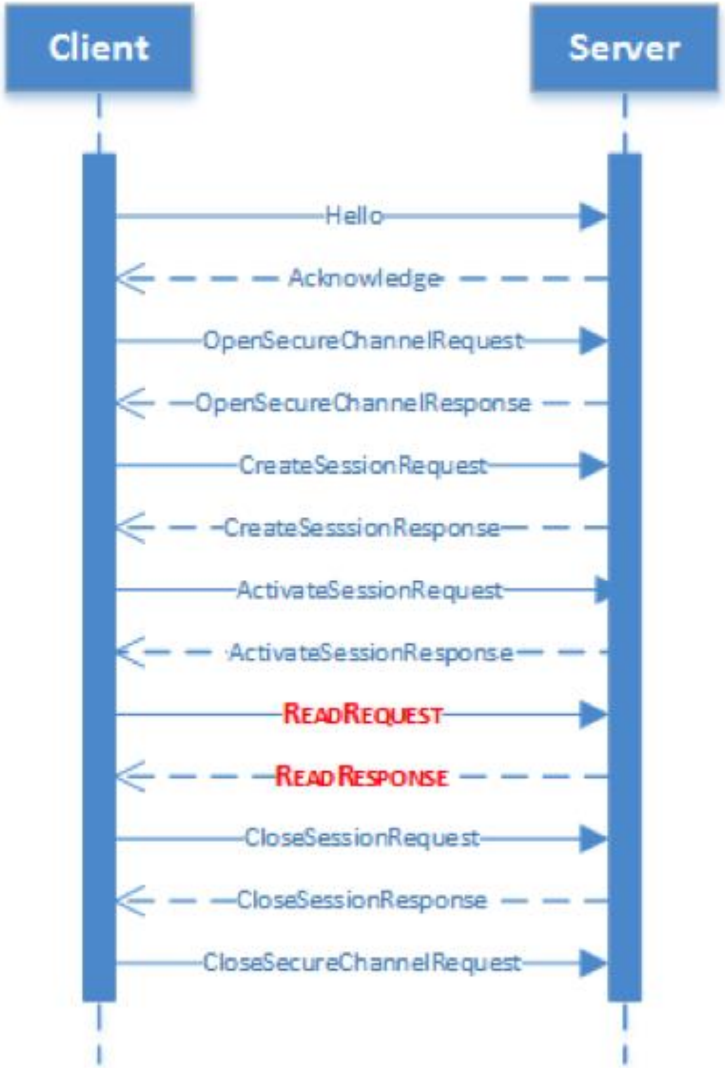
A Security Policy:

- Basic128RSA128
- Basic256
- Basic256SHA256
- AES128SHA256RSAOAEP
- AES256SHA256RSAPSS

In addition, authentication & authorization can be performed through certificates or login/passwords (*and even SAML when used with HTTP transport if I'm correct*)

➔ Huge improvement over legacy ICS protocols !
However, technical implementations are not flawless

OPC-UA security features



OPC-UA session workflow

1 – Hello

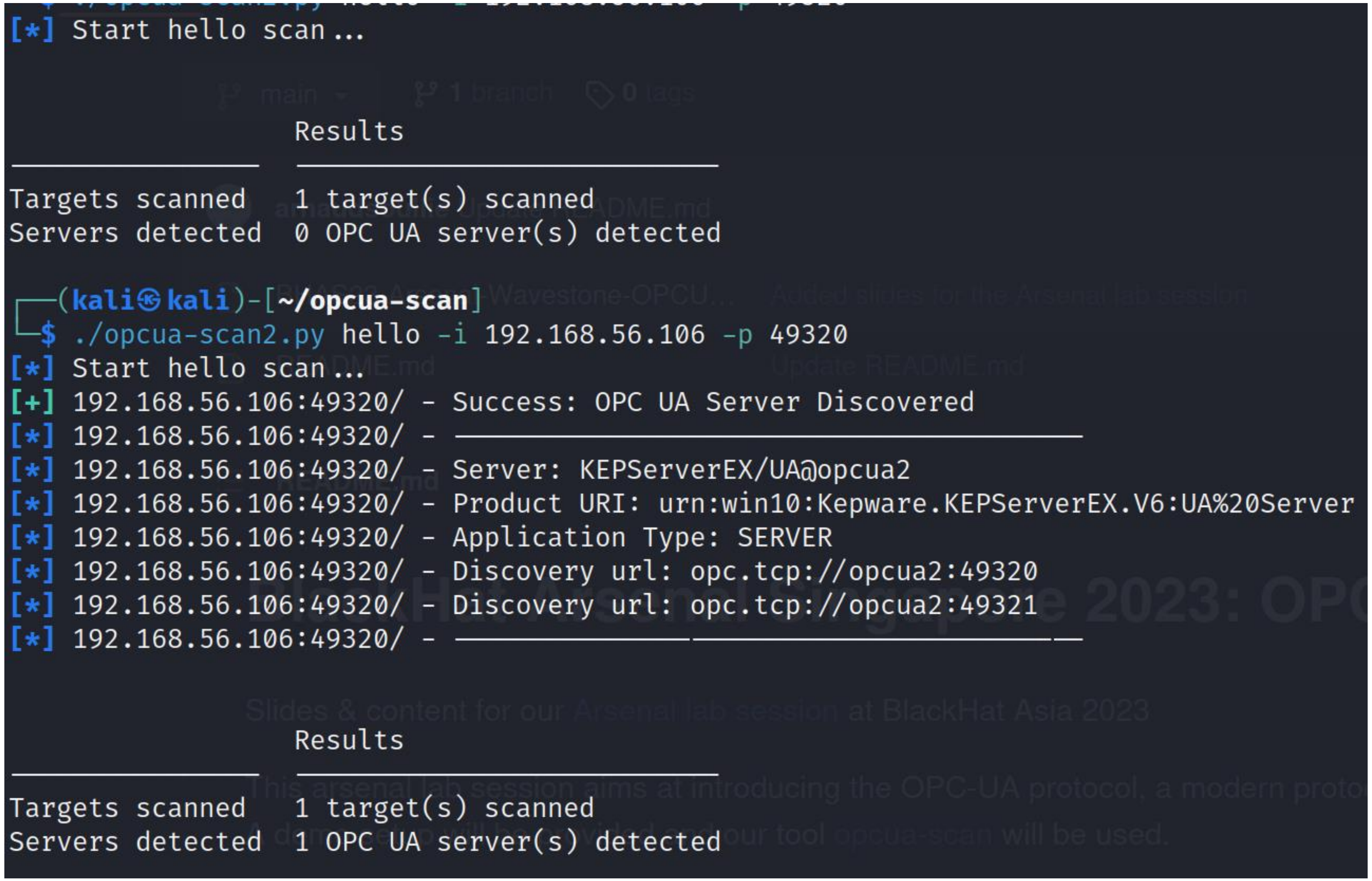
2 – SecureChannel

3 - Session

Opcua-scan: a tool for OPC-UA discovery and information gathering

Basic recon

```
./opcua_scan.py hello -i IP_ADRESS -p ‘PORT1, PORT2, PORT3’
```

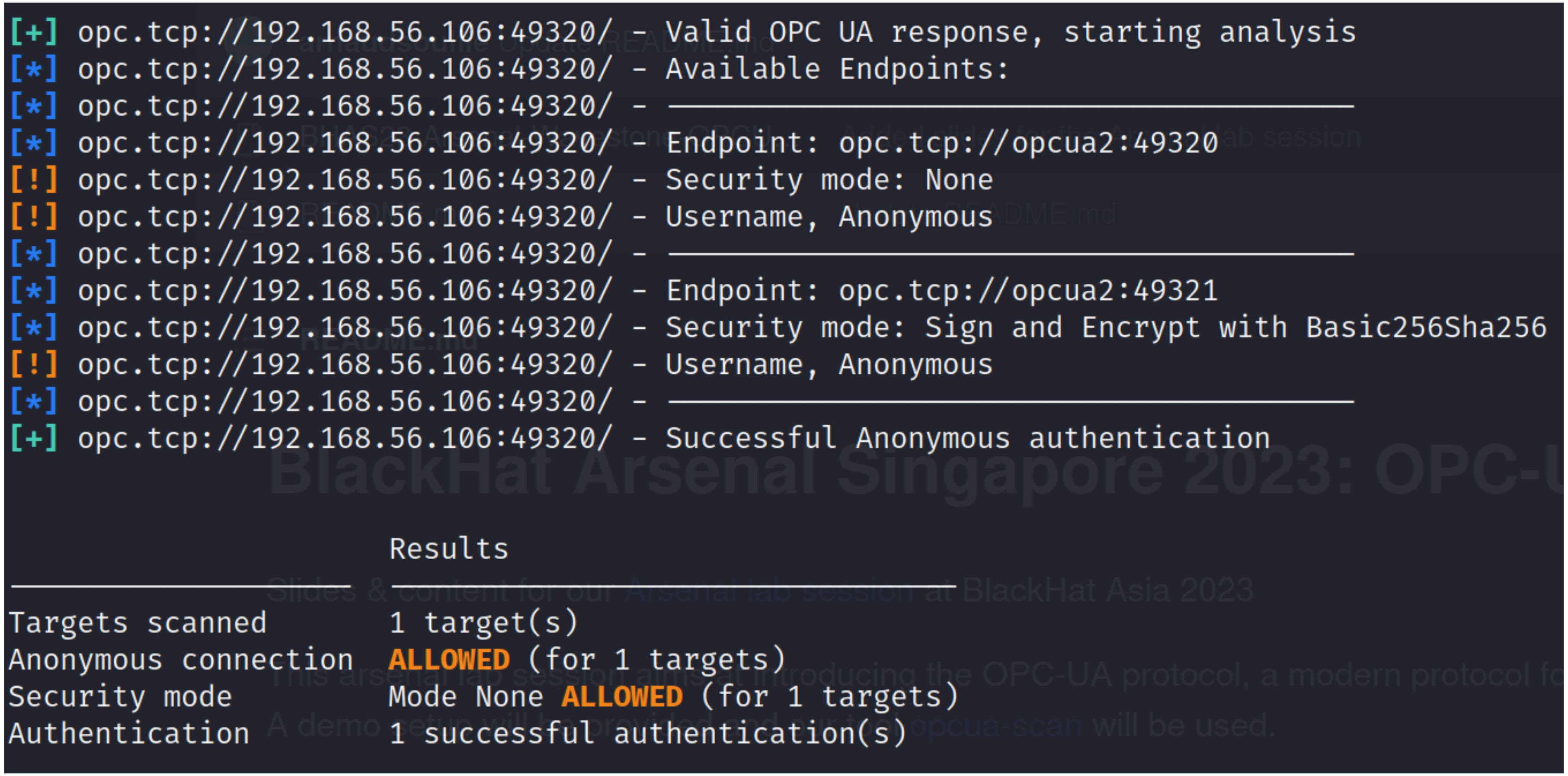


```
[*] Start hello scan ...

                 Results
___________________   _______________________________
Targets scanned    1 target(s) scanned
Servers detected   0 OPC UA server(s) detected

┌──(kali㉿kali)-[~/opcua-scan]
└─$ ./opcua-scan2.py hello -i 192.168.56.106 -p 49320
[*] Start hello scan ...
[+] 192.168.56.106:49320/ - Success: OPC UA Server Discovered
[*] 192.168.56.106:49320/ - ______________________________________________
[*] 192.168.56.106:49320/ - Server: KEPServerEX/UA@opcua2
[*] 192.168.56.106:49320/ - Product URI: urn:win10:Kepware.KEPServerEX.V6:UA%20Server
[*] 192.168.56.106:49320/ - Application Type: SERVER
[*] 192.168.56.106:49320/ - Discovery url: opc.tcp://opcua2:49320
[*] 192.168.56.106:49320/ - Discovery url: opc.tcp://opcua2:49321
[*] 192.168.56.106:49320/ - ______________________________________________

                 Results
___________________   _______________________________
Targets scanned    1 target(s) scanned
Servers detected   1 OPC UA server(s) detected
```

Opcua-scan: a tool for OPC-UA discovery and information gathering

Getting information from an endpoint

```
./opcua-scan2.py server_config -t'opc.tcp://192.168.56.104:49320/'
```

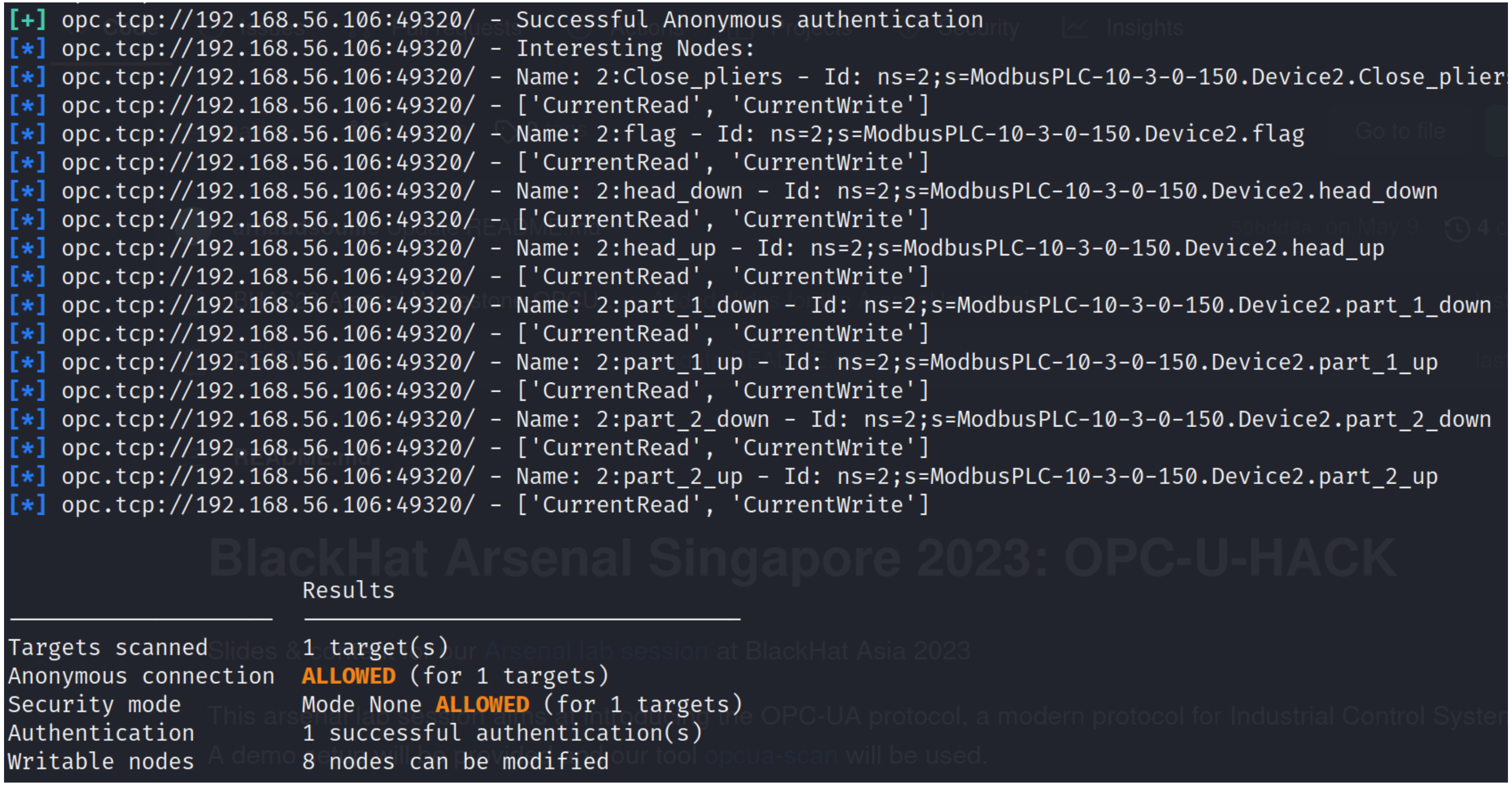


```
[+] opc.tcp://192.168.56.106:49320/ - Valid OPC UA response, starting analysis
[*] opc.tcp://192.168.56.106:49320/ - Available Endpoints:
[*] opc.tcp://192.168.56.106:49320/ - ────────────────────────────────────────
[*] opc.tcp://192.168.56.106:49320/ - Endpoint: opc.tcp://opcua2:49320
[!] opc.tcp://192.168.56.106:49320/ - Security mode: None
[!] opc.tcp://192.168.56.106:49320/ - Username, Anonymous
[*] opc.tcp://192.168.56.106:49320/ - ────────────────────────────────────────
[*] opc.tcp://192.168.56.106:49320/ - Endpoint: opc.tcp://opcua2:49321
[*] opc.tcp://192.168.56.106:49320/ - Security mode: Sign and Encrypt with Basic256Sha256
[!] opc.tcp://192.168.56.106:49320/ - Username, Anonymous
[*] opc.tcp://192.168.56.106:49320/ - ────────────────────────────────────────
[+] opc.tcp://192.168.56.106:49320/ - Successful Anonymous authentication


                      Results
────────────────────  ─────────────────────────────────
Targets scanned       1 target(s)
Anonymous connection  ALLOWED (for 1 targets)
Security mode         Mode None ALLOWED (for 1 targets)
Authentication        1 successful authentication(s)
```

Opcua-scan: a tool for OPC-UA discovery and information gathering

Finding writable nodes

```
./opcua-scan2.py server_config -t'opc.tcp://192.168.56.104:49320/' -nw
```

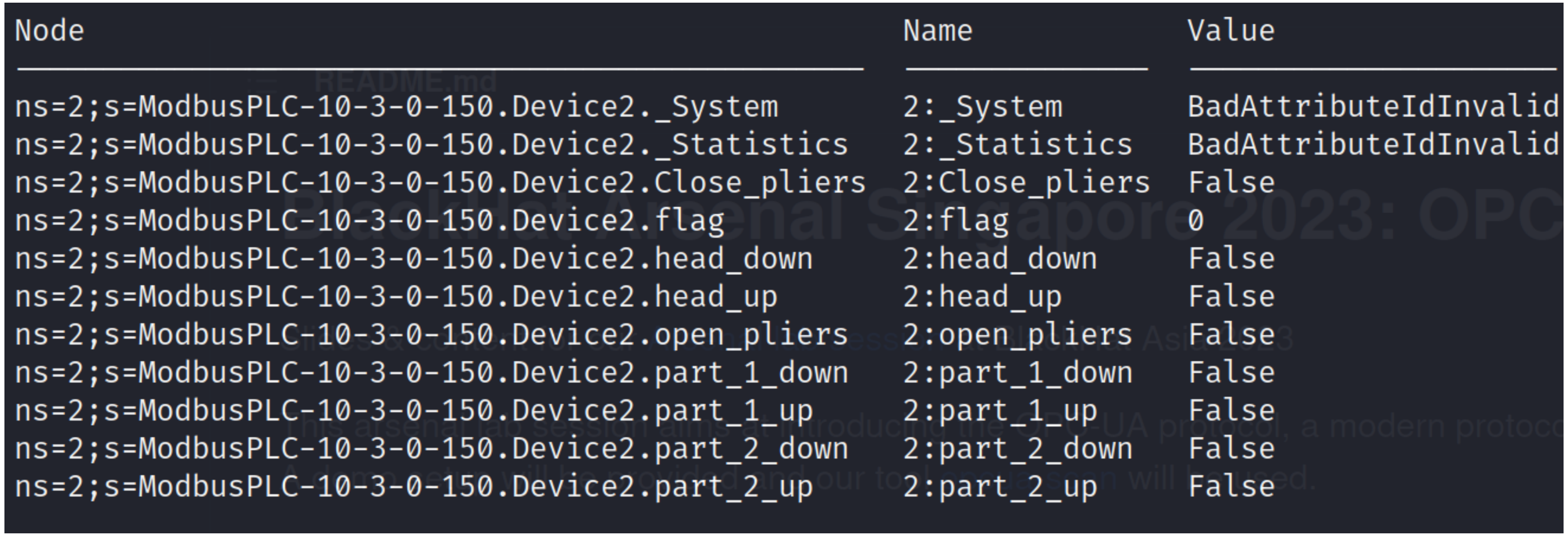


```
[+] opc.tcp://192.168.56.106:49320/ - Successful Anonymous authentication
[*] opc.tcp://192.168.56.106:49320/ - Interesting Nodes:
[*] opc.tcp://192.168.56.106:49320/ - Name: 2:Close_pliers - Id: ns=2;s=ModbusPLC-10-3-0-150.Device2.Close_plier
[*] opc.tcp://192.168.56.106:49320/ - ['CurrentRead', 'CurrentWrite']
[*] opc.tcp://192.168.56.106:49320/ - Name: 2:flag - Id: ns=2;s=ModbusPLC-10-3-0-150.Device2.flag
[*] opc.tcp://192.168.56.106:49320/ - ['CurrentRead', 'CurrentWrite']
[*] opc.tcp://192.168.56.106:49320/ - Name: 2:head_down - Id: ns=2;s=ModbusPLC-10-3-0-150.Device2.head_down
[*] opc.tcp://192.168.56.106:49320/ - ['CurrentRead', 'CurrentWrite']
[*] opc.tcp://192.168.56.106:49320/ - Name: 2:head_up - Id: ns=2;s=ModbusPLC-10-3-0-150.Device2.head_up
[*] opc.tcp://192.168.56.106:49320/ - ['CurrentRead', 'CurrentWrite']
[*] opc.tcp://192.168.56.106:49320/ - Name: 2:part_1_down - Id: ns=2;s=ModbusPLC-10-3-0-150.Device2.part_1_down
[*] opc.tcp://192.168.56.106:49320/ - ['CurrentRead', 'CurrentWrite']
[*] opc.tcp://192.168.56.106:49320/ - Name: 2:part_1_up - Id: ns=2;s=ModbusPLC-10-3-0-150.Device2.part_1_up
[*] opc.tcp://192.168.56.106:49320/ - ['CurrentRead', 'CurrentWrite']
[*] opc.tcp://192.168.56.106:49320/ - Name: 2:part_2_down - Id: ns=2;s=ModbusPLC-10-3-0-150.Device2.part_2_down
[*] opc.tcp://192.168.56.106:49320/ - ['CurrentRead', 'CurrentWrite']
[*] opc.tcp://192.168.56.106:49320/ - Name: 2:part_2_up - Id: ns=2;s=ModbusPLC-10-3-0-150.Device2.part_2_up
[*] opc.tcp://192.168.56.106:49320/ - ['CurrentRead', 'CurrentWrite']


                      Results
 ───────────────────  ────────────────────────────────
 Targets scanned      1 target(s)
 Anonymous connection ALLOWED (for 1 targets)
 Security mode        Mode None ALLOWED (for 1 targets)
 Authentication       1 successful authentication(s)
 Writable nodes       8 nodes can be modified
```

Opcua-scan: a tool for OPC-UA discovery and information gathering

Browsing content

```
./opcua-scan2.py read_data -t 'opc.tcp://192.168.56.106:49320’

./opcua-scan2.py read_data -t 'opc.tcp://192.168.56.106:49320’ -r ‘i=85’
-single True
```

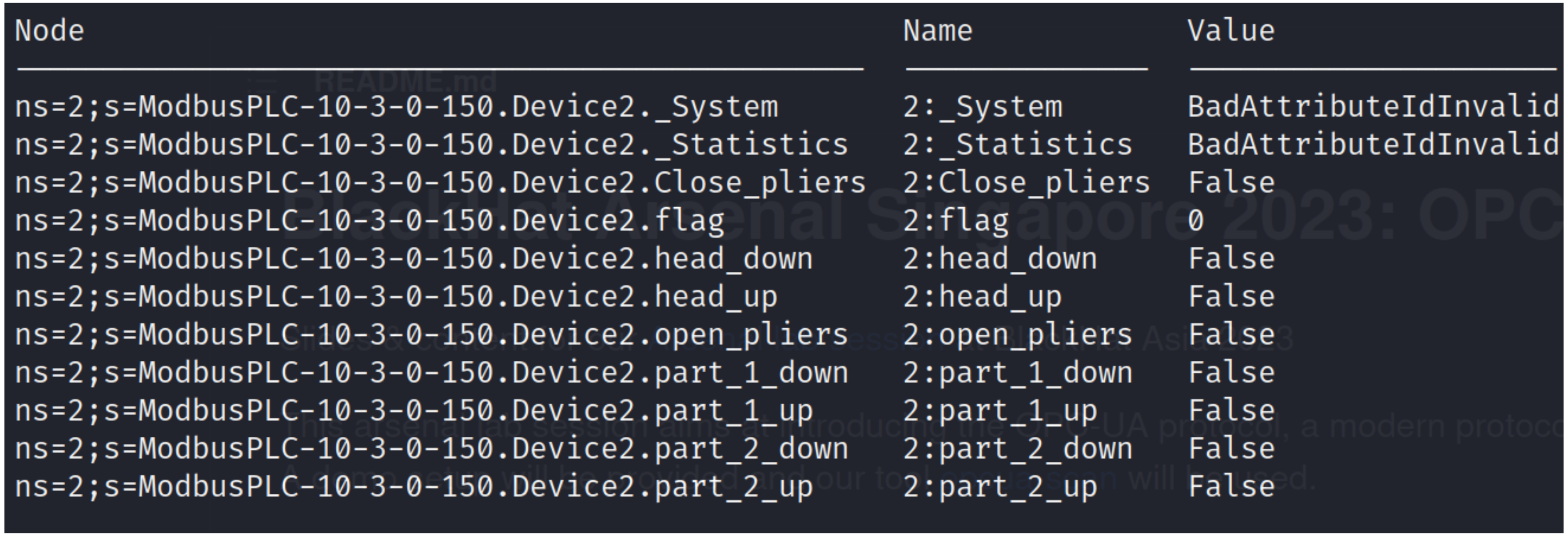


```
Node                                              Name            Value
────────────────────────────────────────────────  ──────────────  ─────────────────────
ns=2;s=ModbusPLC-10-3-0-150.Device2._System       2:_System       BadAttributeIdInvalid
ns=2;s=ModbusPLC-10-3-0-150.Device2._Statistics   2:_Statistics   BadAttributeIdInvalid
ns=2;s=ModbusPLC-10-3-0-150.Device2.Close_pliers  2:Close_pliers  False
ns=2;s=ModbusPLC-10-3-0-150.Device2.flag          2:flag          0
ns=2;s=ModbusPLC-10-3-0-150.Device2.head_down     2:head_down     False
ns=2;s=ModbusPLC-10-3-0-150.Device2.head_up       2:head_up       False
ns=2;s=ModbusPLC-10-3-0-150.Device2.open_pliers   2:open_pliers   False
ns=2;s=ModbusPLC-10-3-0-150.Device2.part_1_down   2:part_1_down   False
ns=2;s=ModbusPLC-10-3-0-150.Device2.part_1_up     2:part_1_up     False
ns=2;s=ModbusPLC-10-3-0-150.Device2.part_2_down   2:part_2_down   False
ns=2;s=ModbusPLC-10-3-0-150.Device2.part_2_up     2:part_2_up     False
```

Opcua-scan: a tool for OPC-UA discovery and information gathering

Browsing content authenticated

```
./opcua-scan2.py read_data -t 'opc.tcp://192.168.56.106:49320’

./opcua-scan2.py read_data -t 'opc.tcp://192.168.56.106:49320’ –r ‘i=85’
–a Username –u user –p password
```



```
Node                                                Name             Value
-----------------------------------------------     --------------   ---------------------
ns=2;s=ModbusPLC-10-3-0-150.Device2._System         2:_System        BadAttributeIdInvalid
ns=2;s=ModbusPLC-10-3-0-150.Device2._Statistics     2:_Statistics    BadAttributeIdInvalid
ns=2;s=ModbusPLC-10-3-0-150.Device2.Close_pliers    2:Close_pliers   False
ns=2;s=ModbusPLC-10-3-0-150.Device2.flag            2:flag           0
ns=2;s=ModbusPLC-10-3-0-150.Device2.head_down       2:head_down      False
ns=2;s=ModbusPLC-10-3-0-150.Device2.head_up         2:head_up        False
ns=2;s=ModbusPLC-10-3-0-150.Device2.open_pliers     2:open_pliers    False
ns=2;s=ModbusPLC-10-3-0-150.Device2.part_1_down     2:part_1_down    False
ns=2;s=ModbusPLC-10-3-0-150.Device2.part_1_up       2:part_1_up      False
ns=2;s=ModbusPLC-10-3-0-150.Device2.part_2_down     2:part_2_down    False
ns=2;s=ModbusPLC-10-3-0-150.Device2.part_2_up       2:part_2_up      False
```

Opcua-scan: a tool for OPC-UA discovery and information gathering

Dynamic tags

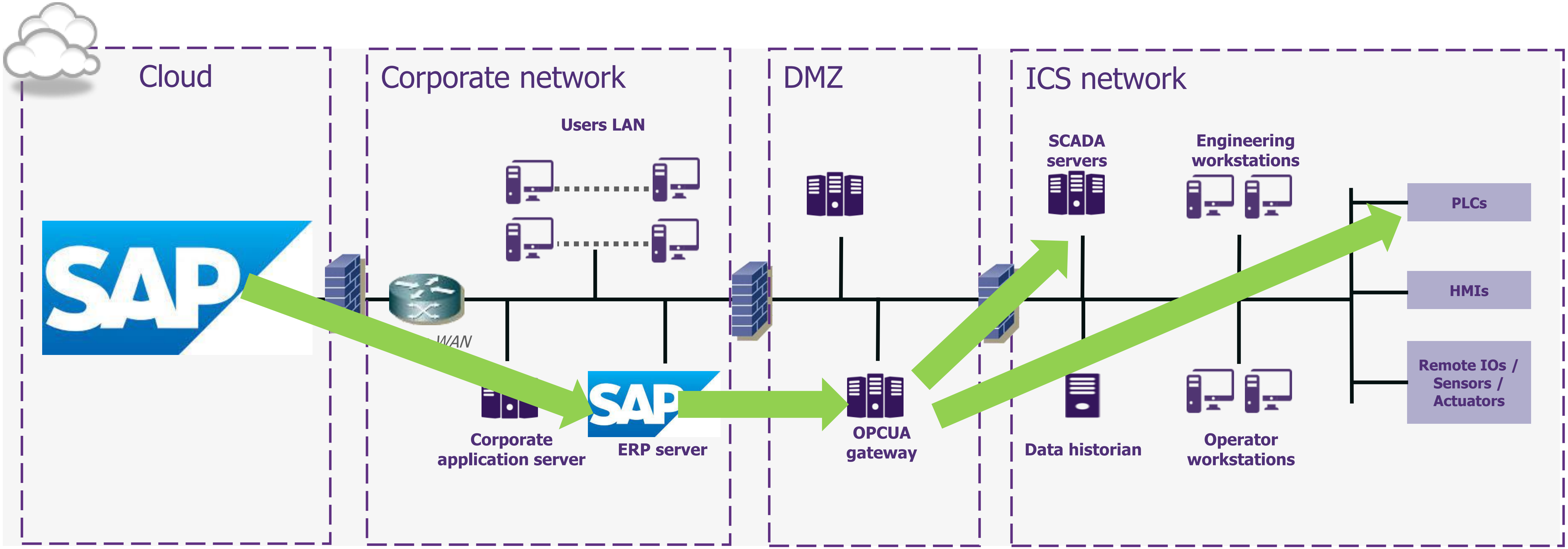
A « tag » is like a variable. It is mapped to a device (PLC) memory address

Example : « valve_34 » could correspond to the state (OPEN or CLOSED) and be mapped to the register 25432 of the PLC at address 10.23.0.67

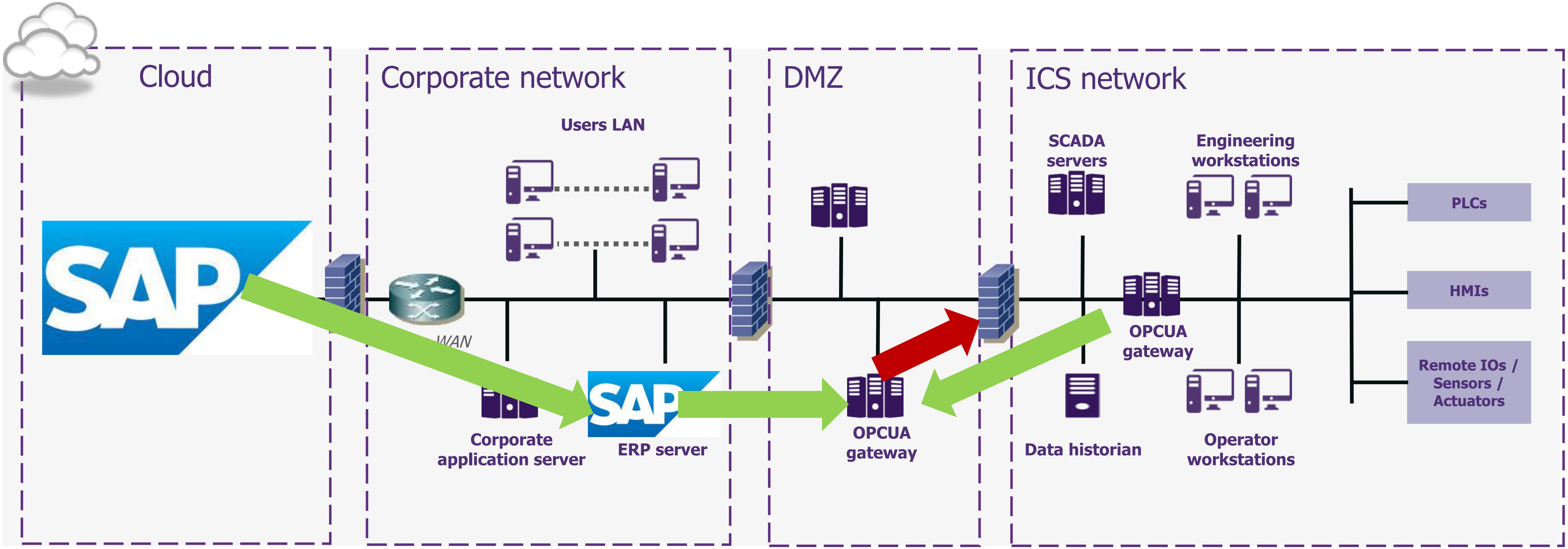
Dynamic tags allow to directly query data from the PLC without having to create the tag

```
./opcua-scan2.py read_data -t 'opc.tcp://192.168.56.106:49320' -r
'ns=2;s=ModbusPLC-10-3-0-150.NewPLC.00005' -a Username -u user -p
passwordpassword --single True
```

Real-life architectures (1/2)



Real-life architectures (1/2)



OPC-UA

OPC-UA is more and more deployed

- Not only gateways
- SCADA systems
- Directly into low-level devices (like PLCs), so it could replace insecure legacy protocols

Still some hard problems to solve

- It’s a standard but not everything is interoperable
- Distribution and renewal of certificates is hard
- Not a lot of implementations for the GDS (*Global Discovery Service*), a kind of directory to get certificates

To go further

Our ressources

- ‘opcua-scan’ tool: https://github.com/wavestone-cdt/opcua-scan
- BlackHat Asia Arsenal write-up: https://github.com/wavestone-cdt/bhasia23-opcuhack

Excellent articles by Claroty

- Part 1: https://claroty.com/team82/research/opc-ua-deep-dive-history-of-the-opc-ua-protocol
- Part 2: https://claroty.com/team82/research/opc-deep-dive-part-2-what-is-opc-ua
- Part 3: https://claroty.com/team82/research/opc-ua-deep-dive-part-3-exploring-the-opc-ua-protocol

The Positive Way

WAVESTONE

Arnaud SOULLIE
Senior Manager

arnaud.soullie@wavestone.com

wavestone.com
@wavestone_