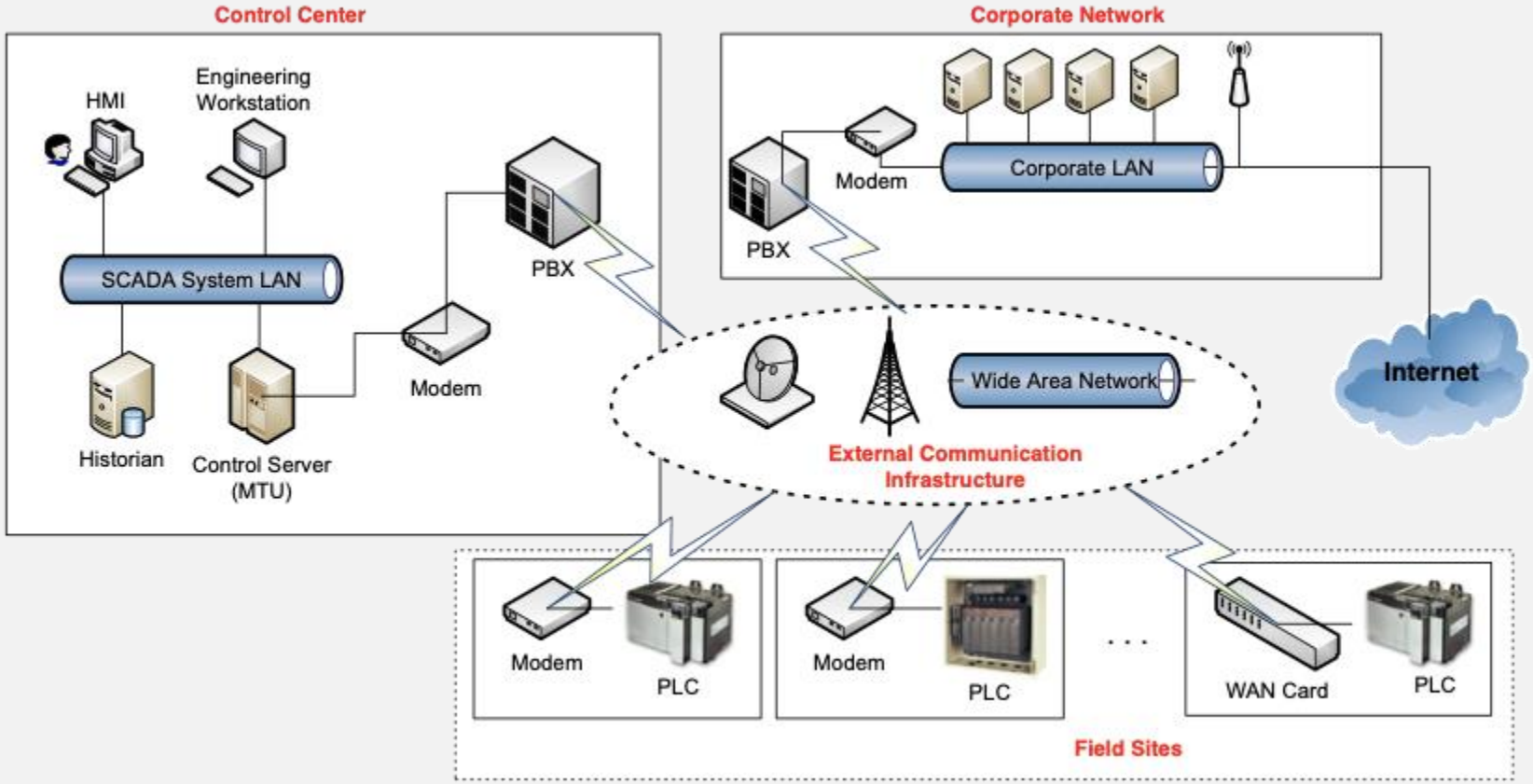
# EMPIRICAL STUDY OF PLC AUTHENTICATION PROTOCOLS IN INDUSTRIAL CONTROL SYSTEMS

**Adeen Ayub**[1], Hyunguk Yoo[2], and Irfan Ahmed[1]

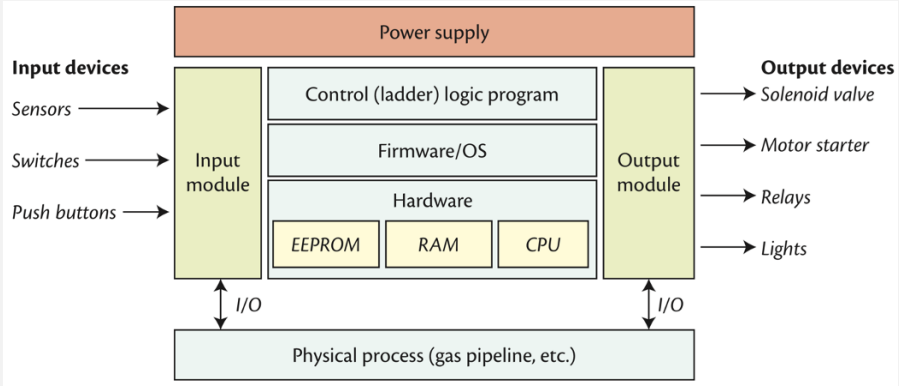
[1] Virginia Commonwealth University
[2] University of New Orleans

# INDUSTRIAL CONTROL SYSTEM (ICS)

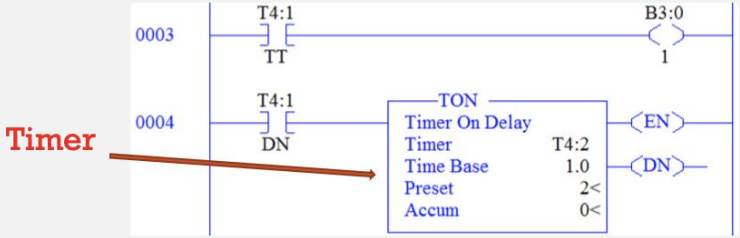


# PROGRAMMABLE LOGIC CONTROLLERS (PLCS)

- Monitor and Control physical processes e.g., nuclear plant, and gas pipeline
- Run a control logic program
- Vendor-supplied engineering software
- Proprietary ICS protocol
- ***Download*** – write a control logic program on a PLC's memory
- ***Upload*** – read a control logic program from a PLC's memory




Ladder Logic Code Snippet



# EMPIRICAL STUDY OF PLC AUTHENTICATION PROTOCOLS

- Utilize Password-based user authentication
  - to protect control logic from unauthorised access

- Study the security design practices in authentication mechanisms of five PLC
  - Sole reliance on network traffic

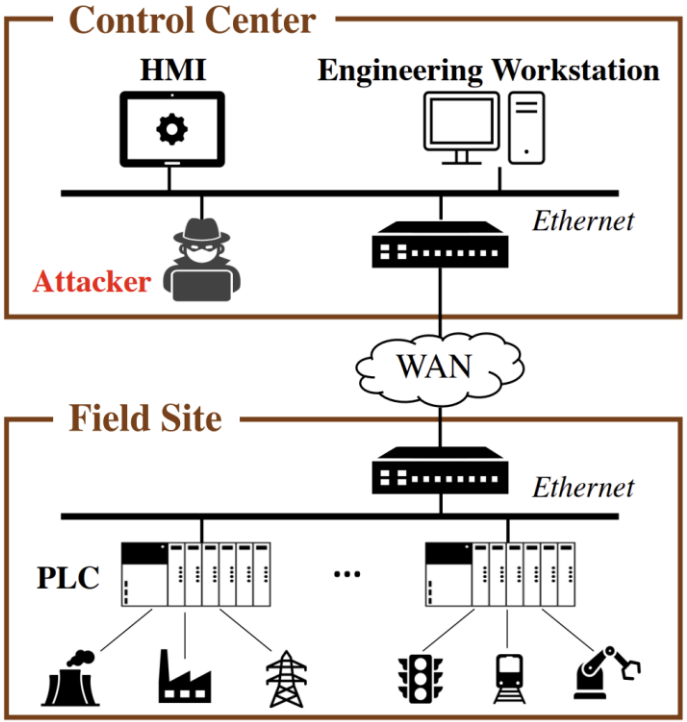
| Vendors | PLCs | Engr. Software |
|---|---|---|
| Schneider Electric | Modicon M221 | SoMachine Basic |
| Allen-Bradley | MicroLogix 1100 & 1400 | RSLogix 500 |
| AutomationDirect | CLICK | CLICK Software |
| Siemens | S7-300 | SIMATIC STEP 7 |

# ADVERSARY MODEL

**Assumptions**:
Access to Level 3 network of Purdue Model (i.e control center network)

**Goal:**
Bypass the authentication mechanism of a password protected PLC over the network
Goal achieved if any of the following tasks are accomplished
1- gain plaintext password
2- read control logic
3- modify control logic of a PLC
4- change the password

**Capabilities:**
Defined using the classic Dolev-Yao model
i.e eavesdropping, fabrication, interception



# STUDY METHOD AND FINDINGS

1. Understanding authentication protocol internals

2. Identifying protocol vulnerabilities
   - Eight exploitable vulnerabilities discovered

3. Mapping an identified vulnerability to the MITRE ATT&CK framework

| CVEs issued | |
|---|---|
| CVE-2021-32978 | CVE-2021-32926 |
| CVE-2021-32980 | CVE-2020-15791 |
| CVE-2021-32982 | CVE-2018-7790 |
| CVE-2021-32984 | CVE-2018-7791 |
| CVE-2021-32986 | CVE-2018-7792 |

# VULNERABILITIES DISCOVERED

| Vul ID | Vulnerability | M221 | MicroLogix 1100 | MicroLogix 1400 | CLICK | Siemens S7-300 |
|---|---|---|---|---|---|---|
| V1 | **Information Disclosure** | n/a | Ver <= 16.0 | Ver <= 21.2 | Ver 2.6 | n/a |
| V2 | **Client side authentication** | n/a | Ver <= 16.0 | Ver <= 21.1 | n/a | n/a |
| V3 | **Weak encryption scheme** | Ver < 1.6.2 | n/a | Ver 21.6 | n/a | All versions |
| V4 | **Small key space** | Ver < 1.6.2 | n/a | n/a | n/a | All versions |
| V5 | **Lack of nonces** | n/a | n/a | n/a | n/a | All versions |
| V6 | **Use of same keys** | n/a | n/a | n/a | n/a | All versions |
| V7 | **Improper session management** | n/a | n/a | n/a | Ver 2.6 | n/a |
| V8 | **No write protection** | Ver <= 1.6.2 | n/a | n/a | n/a | n/a |

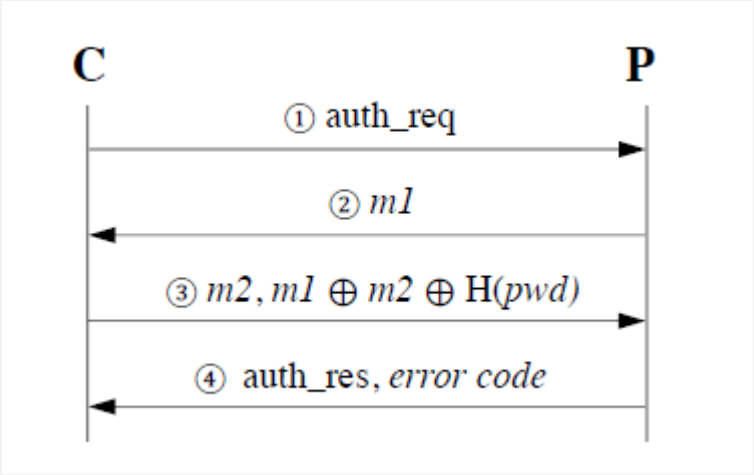
# MITRE ATT&CKS LAUNCHED

| MITRE ATT&CK ID | Attack Name | Modicon M221 | MicroLogix 1100 | MicroLogix 1400 | CLICK | S7-300/400 |
|---|---|---|---|---|---|---|
| T1555 | **Credentials from Password Stores** | n/a | V1, V2 | V1, V2 | V1 | n/a |
| T1040 | **Network Sniffing** | n/a | V1 | V1 | V1 | n/a |
| T1098 | **Unauthorised Password Reset** | V3, V4, V5, V8 | V2, V5 | V2, V5 | n/a | n/a |
| T1562 | **Impair Defenses** | n/a | V2 | V2 | V7 | n/a |
| T1110.002 | **Password Cracking** | n/a | n/a | n/a | n/a | V3, V4, V5, V6 |
| T0830 | **Man in the Middle** | n/a | n/a | V3 | n/a | n/a |
| T1565.002 | **Transmitted Data Manipulation** | n/a | n/a | V3 | n/a | n/a |
| T1499 | **Endpoint Denial of Service** | n/a | n/a | V3 | n/a | n/a |

# CASE STUDY 1: MODICON M221

- Compact controller introduced in August 2014
- Replaced Twido controllers
- Meet the requirements of the Industry 4.0
- Engineering software - SoMachine Basic
- Proprietary protocol embedded in the Modbus protocol

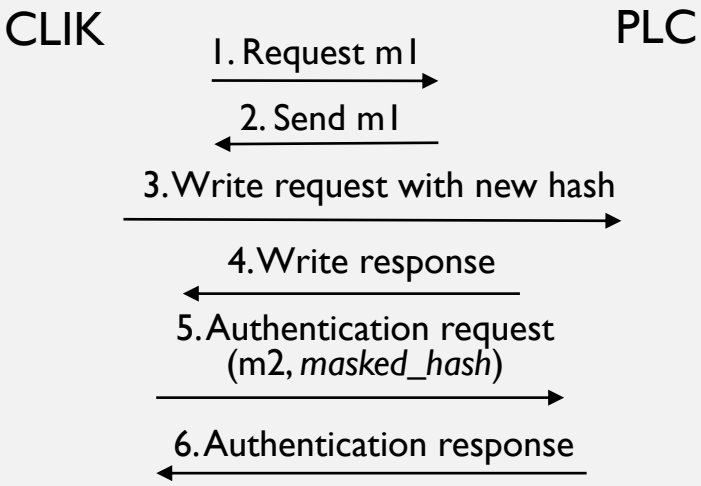
## Authentication Protocol

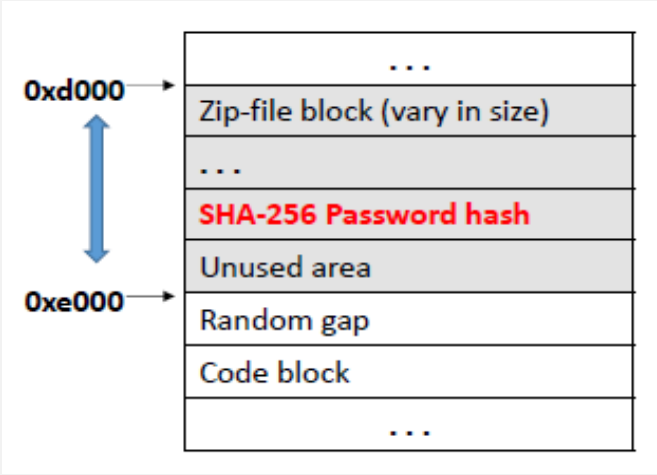


# MITRE ATT&CK

## Unauthorised password reset (T1098)

1) Kalle et al.'s password reset attack




Modicon M221 Memory Layout

| Total block size(KB) | # of project files | Max size zipHash (byates) | Lowest addr. of code block (hex) | Avg. # of write | Max # of write | Avg. time (sec) | Max time (sec) | Attack success rate |
|---|---|---|---|---|---|---|---|---|
| 6 ~ 7 | 5 | 831 | 0xe088 | 3325 | 3413 | 13.48 | 13.88 | 100% |
| 7 ~ 8 | 19 | 1712 | 0xe08c | 2943 | 3266 | 11.89 | 13.31 | 100% |
| 8 ~ 9 | 25 | 2261 | 0xe08c | 2034 | 2385 | 8.21 | 9.64 | 100% |
| >9 | 3 | 3103 | 0xe26c | 1468 | 2379 | 5.89 | 9.42 | 100% |
| Total | 52 | 3103 | 0xe088 | 2458 | 3413 | 9.93 | 13.88 | 100% |

Attacker's footprints

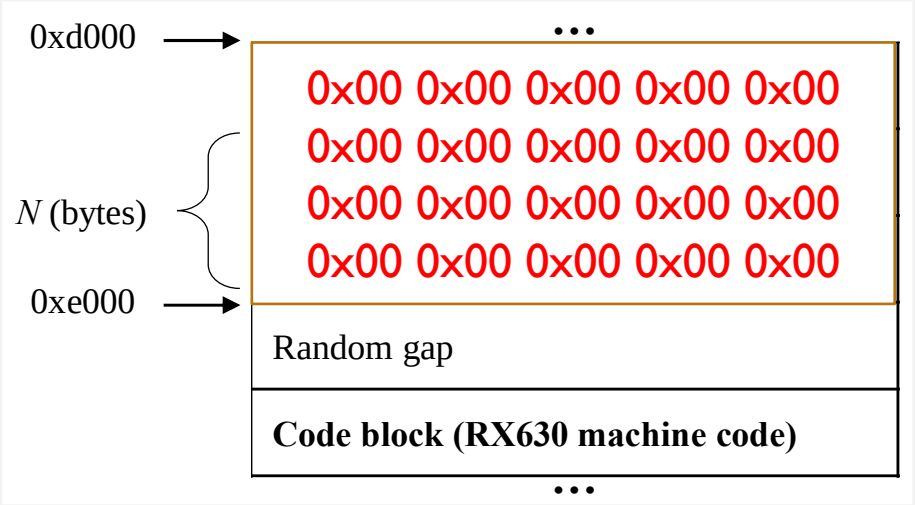
- Additional write packets
- Several failed authentication attempts

# MITRE ATT&CK

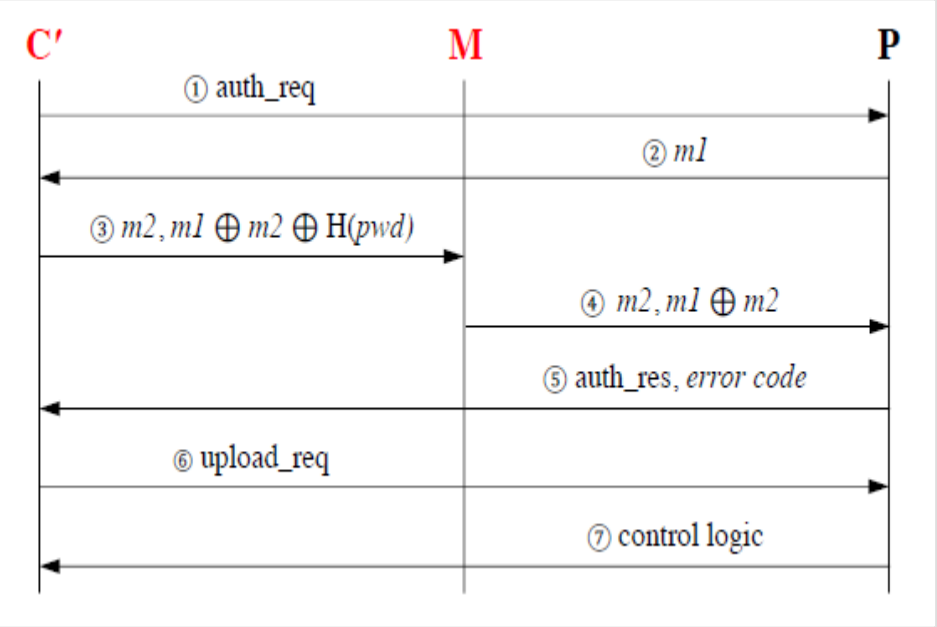
2) 0x00ed (efficient) password reset

**Algorithm 1** Pseudocode for Password Reset Attack

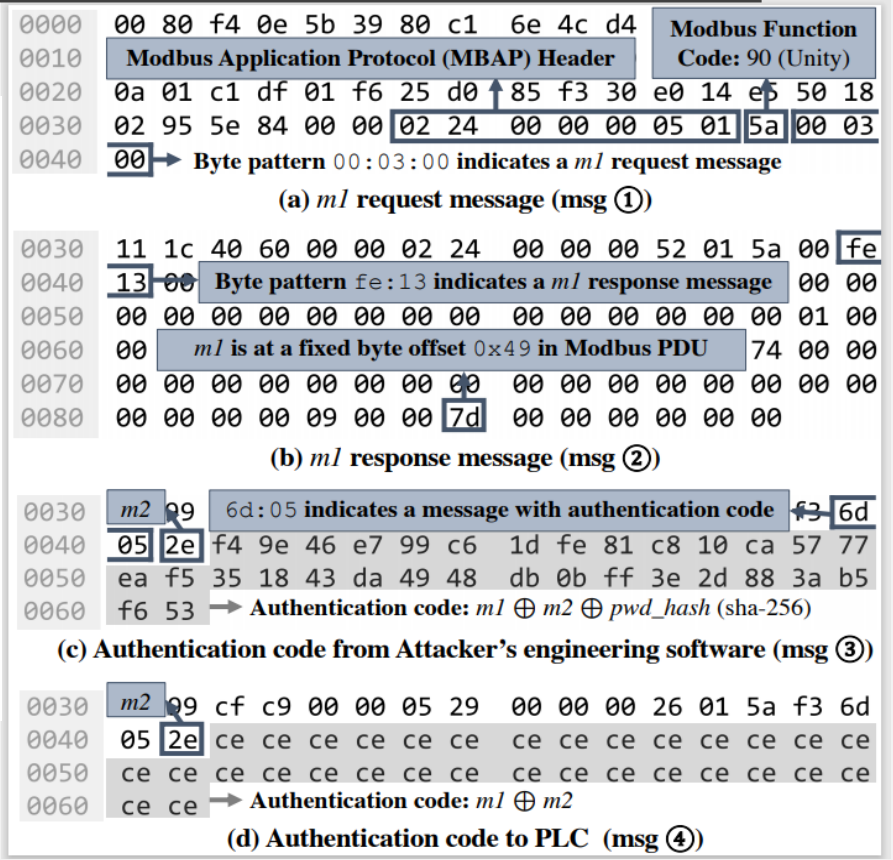
```
zero ← 128 byte array of 0x00
startAddress ← 0xd000
endAddress ← 0xe000
offset ← startAddress
maxSize ← 128 // maximum payload length of M221
while offset ≠ endAddress do
    Send a write request(addr:offset, size:maxSize, payload:zero)
    offset ← offset + maxSize
end while
m1 ← Request m1 from PLC
m2 ← Random number between 0-255
hashSize ← 32 // SHA-256
for i = 0 to hashSize-1 do
    maskedHash[i] ← m1 ⊕ m2
end for
Send an authentication request(m2,maskedHash) to PLC
```



# 0X00ED (EFFICIENT) PASSWORD RESET ATTACK




Upload a control logic into attacker's ES



# EVALUATION

**Experimental settings:**

- Schneider Electric's Modicon M221 (firmware v1.5.1.0 and v1.6.0.1)
- SoMachine Basic (version 1.5 and version 1.6)
- Windows 7 VM to run the engineering software
- Ubuntu 16.04 VM to run attack scripts
- Python and Scapy

| Attack type | Run time/sec | Write requests | Payload size | Failed Auth. Attempts | Attack success rate |
|---|---|---|---|---|---|
| 0x00ed | 0.06571 | 32 | 128 | 0 | 100% |
| Password resetting attack | 9.93 | 2458 | 32 | 2457 | 100% |

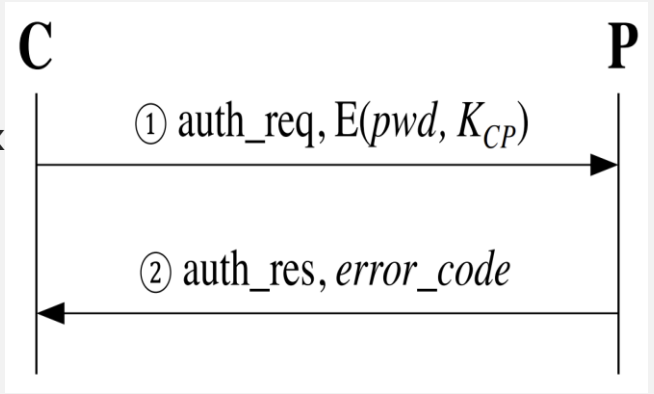
Attacker's footprints

# CASE STUDY 2: SIEMENS S7-300

- Engineering Software - SIMATIC STEP 7(TIA Portal)
- PLC has two modes of protection:
  - Write protection
  - Read/Write protection
- Seven different types of blocks which compose the control logic
  - **(OB (Organization blocks), FC (Functions), FB (Function blocks)**
    - Contain a user's control logic code (i.e., MC7 bytecode)
    - OB comparable to the main() function in C/C++
  - **DB (Data blocks)**
    - The data section of a PLC program
  - **SFC (System function), SFB (System function block**
    - Built-in functions implemented in the PLC firmware
  - **SDB (System data block**)
    - Contains current PLC configurations
    - encrypted password stored in SDBO
      - found through differential analysis

Siemens S7-300

**Authentication Protocol**



# ENCRYPTION ALGORITHM

- Eight-byte password & one-byte secret key
- Substitute each password character $P_i$ with a substitution table entry $N_i$
- XORed with the key K for the first two characters
- XORed the rest with K and $E_{i-2}$

**Algorithm 2** Pseudocode of the weak encryption algorithm

**Input:** password ($P_0$...$P_7$), $K$ (where $K$ is one-byte secret key)
**Output:** encrypted_password ($E_0$...$E_7$)

1: **for** $i$ = 0 to 7 **do**
2: $N_i$ = Substitute($P_i$)
3: **if** $i$ ¡ 2 **then**
4: $E_i = K \oplus N_i$
5: **else**
6: $E_i = K \oplus E_{i-2} \oplus N_i$
7: **end if**
8: **end for**

ENCODING METHOD USED IN SIEMENS S7-300 ENCRYPTION ALGORITHM

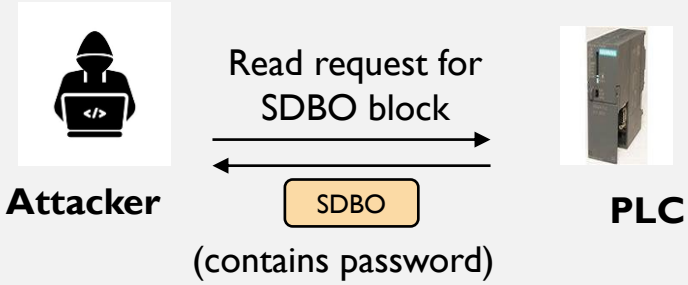
| Character | Encoded (hex) | Character | Encoded (Hex) | Character | Encoded (Hex) | Character | Encoded (Hex) |
|---|---|---|---|---|---|---|---|
| @ | 70 | ‘ | 50 | 0 | 0 | P | 60 |
| A | 71 | a | 51 | 1 | 1 | Q | 61 |
| B | 72 | b | 52 | 2 | 2 | R | 62 |
| C | 73 | c | 53 | 3 | 3 | S | 63 |
| D | 74 | d | 54 | 4 | 4 | T | 64 |
| E | 75 | e | 55 | 5 | 5 | U | 65 |
| F | 76 | f | 56 | 6 | 6 | V | 66 |
| G | 77 | g | 57 | 7 | 7 | W | 67 |
| H | 78 | h | 58 | 8 | 8 | X | 68 |
| I | 79 | i | 59 | 9 | 9 | Y | 69 |
| J | 7a | j | 5a | : | a | Z | 6a |
| K | 7b | k | 5b | ; | b | [ | 6b |
| L | 7c | l | 5c | < | c | \ | 6c |
| M | 7d | m | 5d | = | d | ] | 6d |
| N | 7e | n | 5e | > | e | ^ | 6e |
| O | 7f | o | 5f | ? | f | _ | 6f |

# MITRE ATT&CK

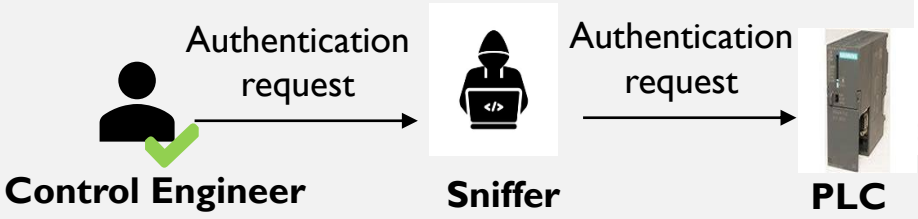
## Password Cracking (T1110.002)

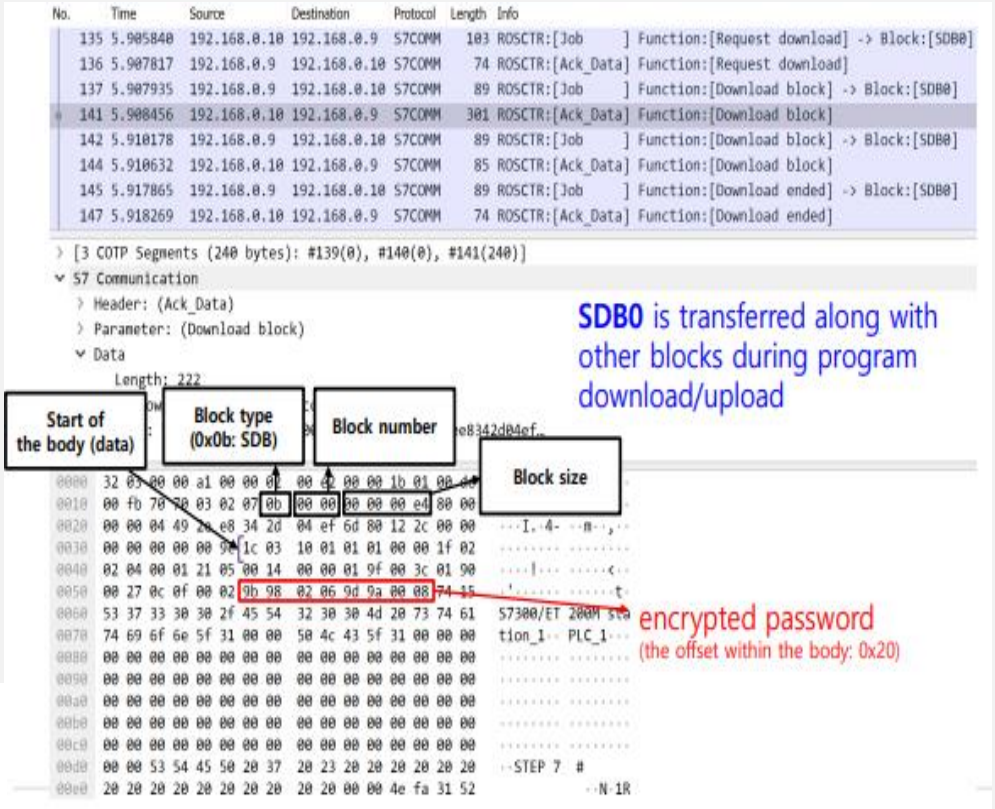
Two scenarios

1- Subverting write protection




2- Subverting read/write protection



# ATTACK EVALUATION

**Experimental Settings:**

- Siemens S7-300 (6ES7 315-2EH14-0AB0) firmware v3.2.8 and v3.2.17
- TIA Portal version v13, v15, and v16.
- Attack scripts in Python using the Snap7 library
- ***CVE-2020-15791***

```
hyunguk@ubuntu:~/s7plc$ python3 s7_attack_pwd1.py 192.168.0.9
Read SDB0 block (228 bytes): 70700302070b0000000000e4800000002978360342e04ef6d8
0122c000000000000009c1c03100101010000 1f020204000121050014000001 9f003c019000270c0
f000280eb1323e7a1296a7415533733303 02f45543230304d2073746174696f6e5f310000504c435
f3100000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000005354455020372023202020202020202020202020202020000016d031524814000
00000
==================================================
Encrypted password (hex):  80eb1323e7a1296a
Before decoding:  ['1a', '71', '9', '52', '6e', '18', '54', '51']
Decrypted password:  *A9b^(da
```

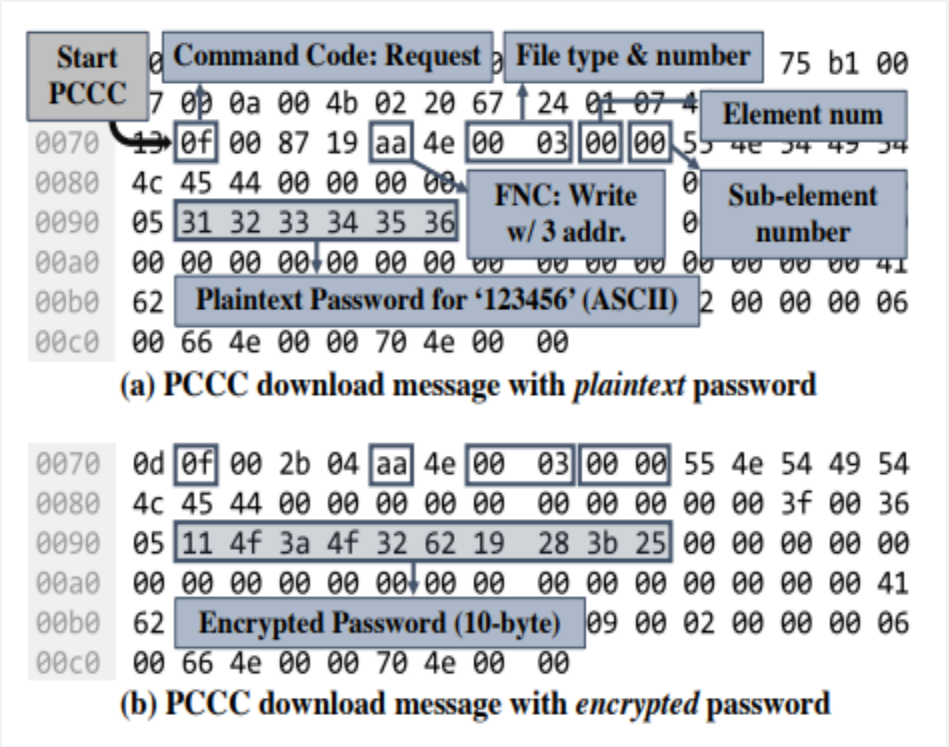
# CASE STUDY 3: MICROLOGIX 1100 AND 1400

- Both are from the same vendor, Allen-Bradley
- Engineering software: RSLogix 500
- ML 1400 has two controller types
  - Default
  - Enhanced Password Security
- ES allows a user to set
  - Password
  - Master password
  - Subroutine Password

# AUTHENTICATION PROTOCOL

**Programmable Controller Communication Commands (PCCC) network protocol**

- PCCC transported over EtherNet/IP (ENIP) which is an adaption of Common Industrial Protocol (CIP)
- PCCC consists of Function Code (FNC) and PCCC data
- Client-side authentication



# MITRE ATT&CK

1. Impair defenses (T1562)

2. Unauthorised password reset (T1098)

3. Network sniffing (T1040)

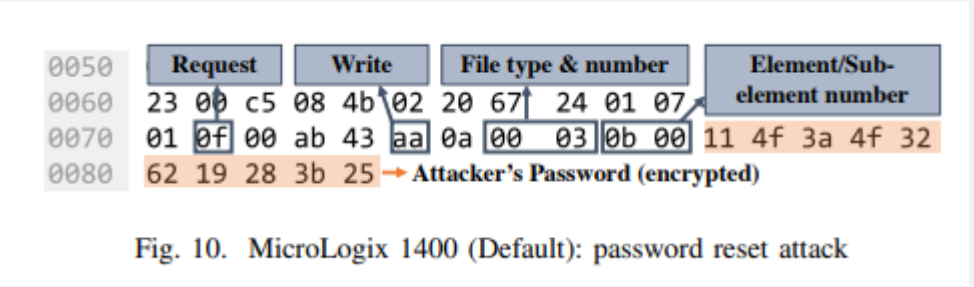



Fig. 10. MicroLogix 1400 (Default): password reset attack

4. Credentials from password stores (T1555)

# ATTACK EVALUATION

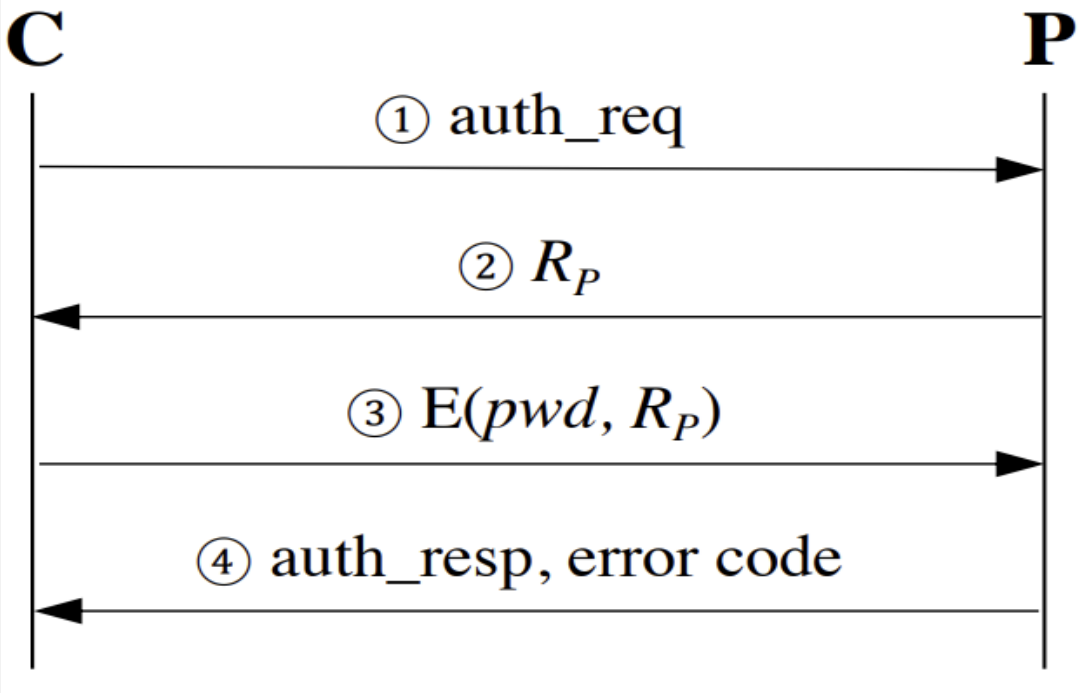
**Experimental Settings:**

- MicroLogix 1400 Series B (firmware version 15.000 and version 21.006)
- MicroLogix 1100 Series B (firmware version 16.000)
- RSLogix 500 (version 9.05.01 and version 12.00.01)
- RSLogix 500 v9.05.01 and RSLogix 500 v12.00.01 run on Windows 7 VM and Windows 10 VM, respectively
- Attacks run on Ubuntu 16.04 VM

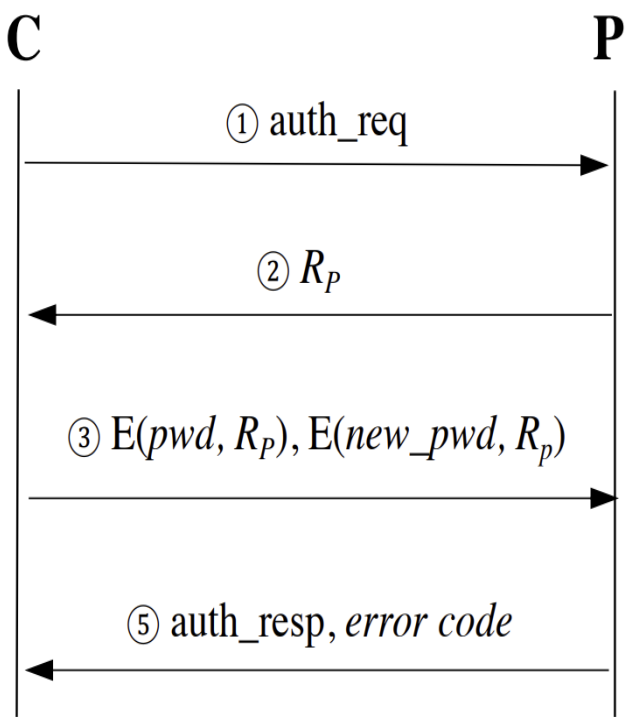
# CASE STUDY 4: MICROLOGIX 1400(ENHANCED PASSWORD SECURITY)

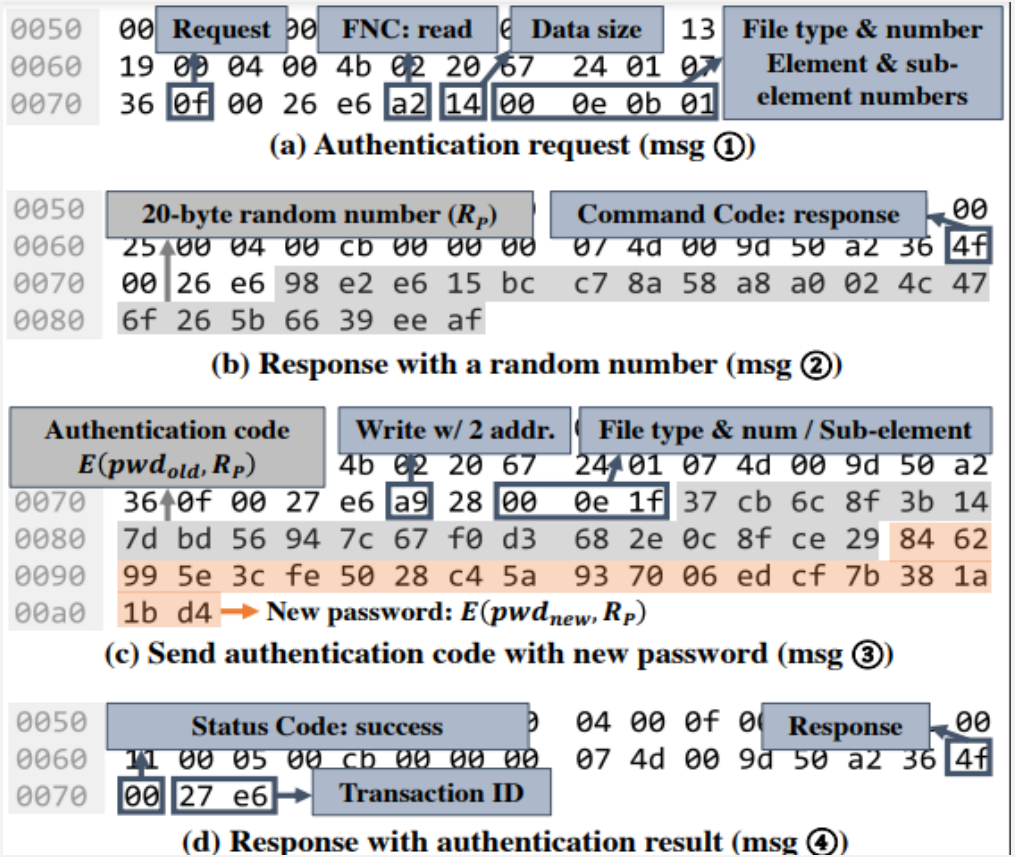
- Latest controller
- Server side authentication

**Authentication Protocol**



# PASSWORD SET/RESET PROTOCOL

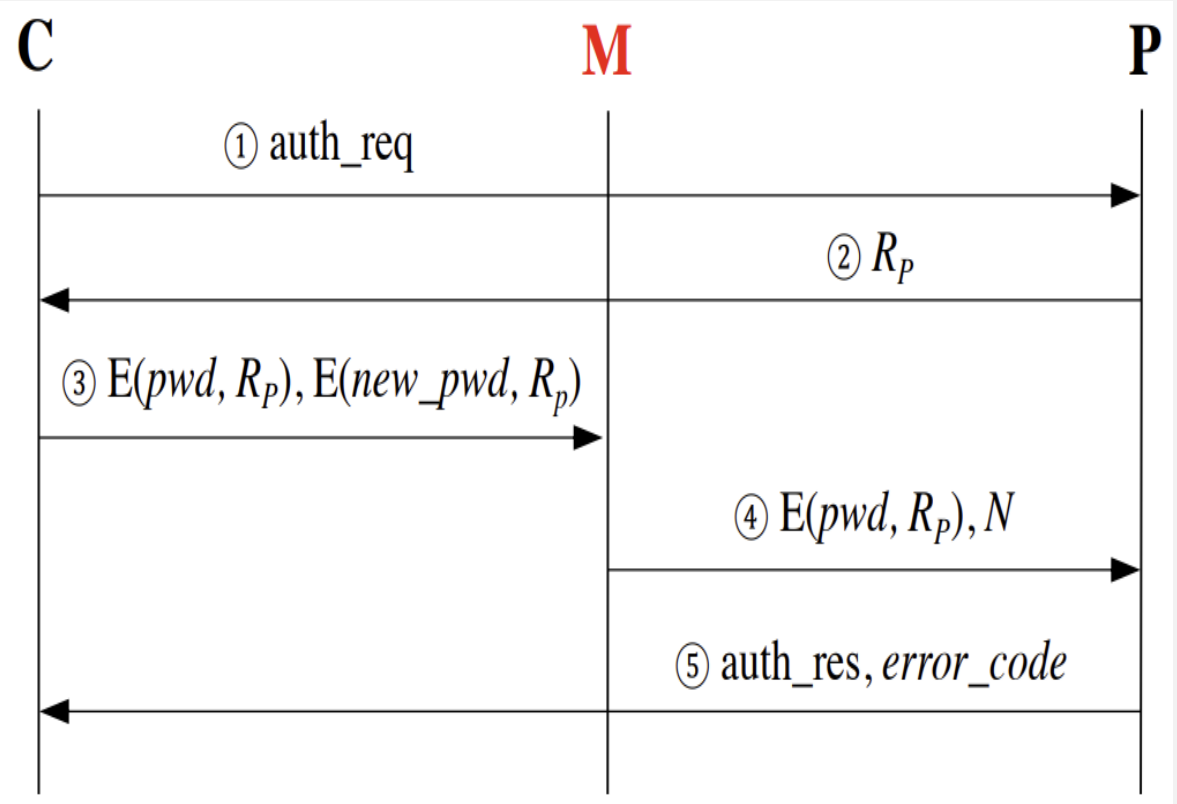


# MITRE ATT&CK

- Man in the Middle (T0830)
- Transmitted Data Manipulation (T1565.002)
- Endpoint Denial of Service (T1499)

**Denial of Service Attack**



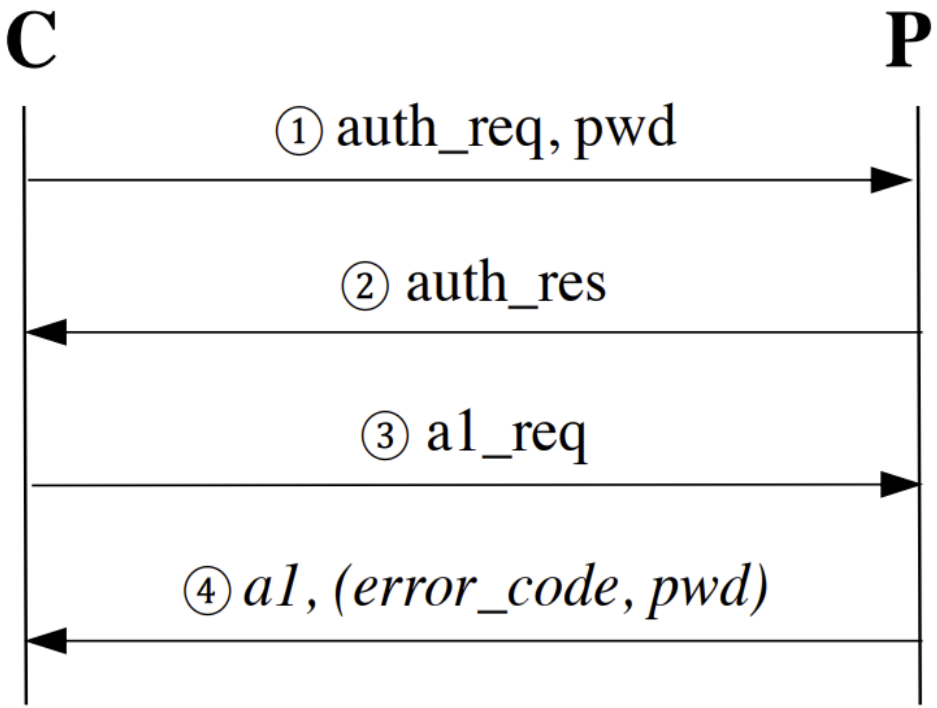
# ATTACK EVALUATION

**Experimental Settings**

- MicroLogix 1400 (firmware version 21.006)
- RSLogix 500 (version 12.00.01)
- Engineering software runs on Windows 10
- Attack scripts run on Ubuntu 16.04 VM
- ***CVE-2021-32926***

# CASE STUDY 6: CLICK PLC

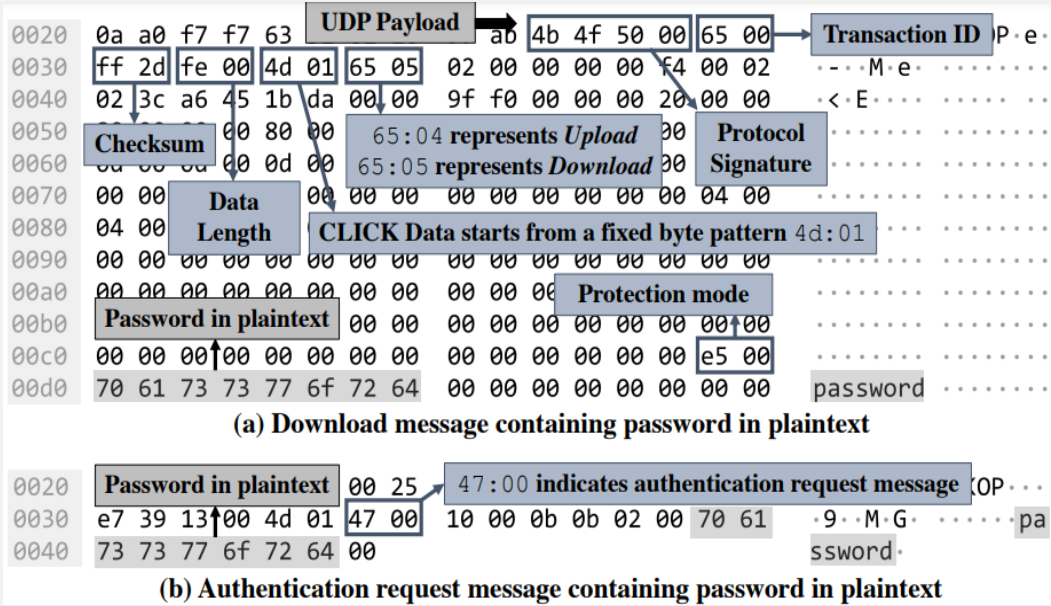
- CLICK Programming software
- User Datagram Protocol

# PROTOCOL VULNERABILITIES

1) Information Disclosure (V1)

- The password gets transmitted in clear text to the PLC
- The PLC stores sensitive information (e.g., last entered password) in credential stores



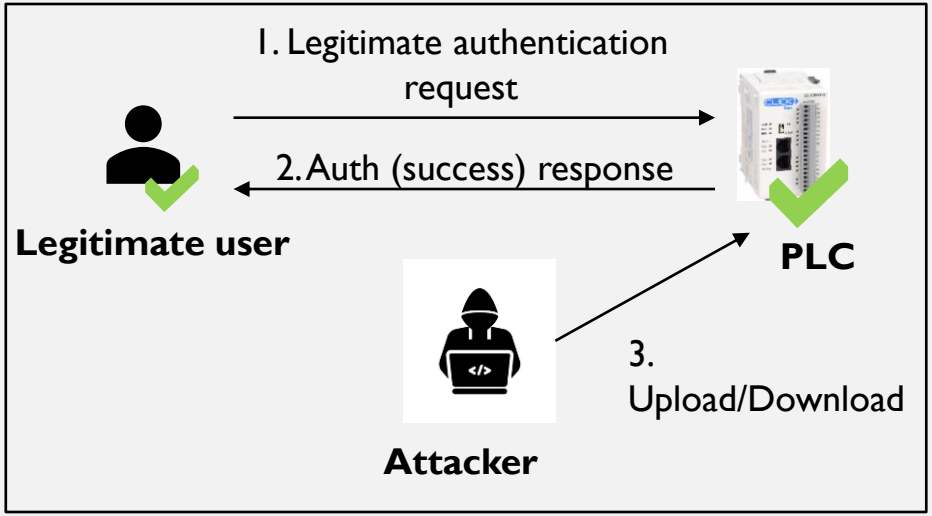

(a) Download message containing password in plaintext

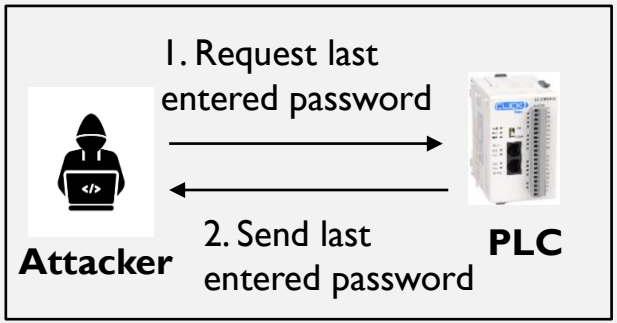
(b) Authentication request message containing password in plaintext

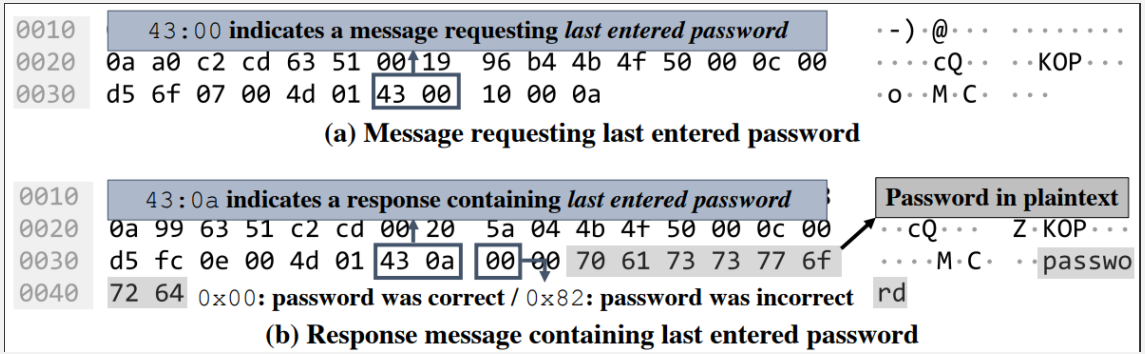
2) Improper session management (V7)

# MITRE ATT&CK

1. Network Sniffing (T1040)
2. Impair defenses (T1562)
3. Credentials from Password Stores (T1555)



# ATTACK EVALUATION

**Experimental Settings:**

- CLICK PLC (v2.60)
- CLICK Programming software (v2.60)
- The programming software runs on Windows 7 VM
- The attacker scripts run on Ubuntu 16.04 VM
- Python and/or Scapy to implement attacker scripts
- ***CVE-2021-32980***
- ***CVE-2021-32984***
- ***CVE-2021-32986***
- ***CVE-2021-32982***
- ***CVE-2021-32978***

# FUNDAMENTAL DESIGN ISSUES

1) Single user authentication
   - Shared password (no username)

2) One-way authentication
   - PLCs as a server do not authenticate client (engineering software) applications

3) Read-protection only
   - Write protection not supported

# CONCLUSION

- Studied five PLCs from four different vendors
- Serious design issues in authentication protocols revealed just by network traffic examination
- Completely redesign – backward compatibility issues, expensive, not feasible
- Network detection, control logic verification
- Partitioning the memory space
- Increasing the key length
- DMZs

# Questions?

Adeen Ayub
ayuba2@vcu.edu
VCU, Richmond, VA

Hyunguk Yoo
hyoo1@uno.edu
UNO, New Orleans, LA

Irfan Ahmed
iahmed3@vcu.edu
VCU, Richmond, VA