King Fahd University of Petroleum & Minerals
College of Computer Science & Engineering
Information and Computer Science Department

PLC Access Control: A Security Analysis

World Congress on Industrial Control Systems Security
(WCICSS 2016)

Haroon Wardak, **Sami Zhioua**, Ahmad Almulhem

Email: zhioua@kfupm.edu.sa

PLC

- A Programmable Logic Controller (PLC) is a control device used to automate industrial processes.
- It works by collecting input data from field devices such as sensors, processing it, then send commands to actuators devices such as motors.

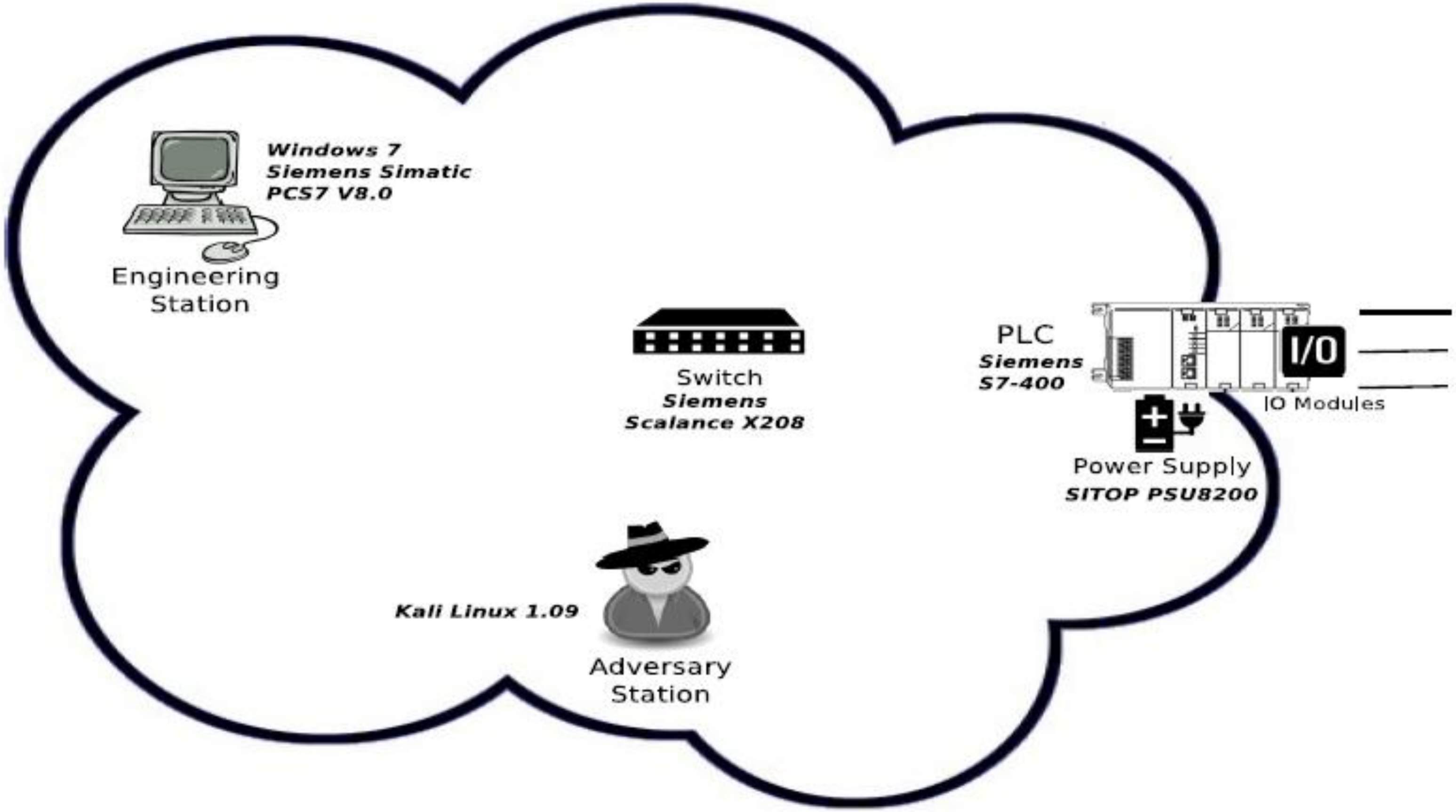
PLC Security

- Being a pivotal device in ICS systems, PLCs are preferred target for cyber security attacks.
- ICS-CERT:
  - out of a total of 589 advisories, 89 target directly PLCs
  - out of a total of 114 alerts, 17 involve PLCs. Another
- Stuxnet malware targeted mainly PLCs

PLC Access Control

- PLC Access Control can be implemented at different levels:
  - Network
  - Physical
  - Firmware
- In this paper, we focus on password based access control

Lab Setup


Windows 7
Siemens Simatic
PCS7 V8.0
Engineering Station
Switch
Siemens
Scalance X208
PLC
Siemens
S7-400
I/O
IO Modules
Power Supply
SITOP PSU8200
Kali Linux 1.09
Adversary Station

PLC Access Control Levels

- Based on S7-400 documentation, there are three access control levels:
  - no protection,
  - write-protection, and
  - read/write-protection.

No Protection Level

- It is the default level.
- Does not provide any form of access control.
- Using this level, any entity (device, station, etc.) can access the PLC processes and data without restriction.
- Access is possible provided that the remote entity “speaks” a PLC supported communication protocol (e.g. COTP, Modbus, Profinet).

Write-Protection Level

- Provides a write protection on PLC data and processes.
- Any attempt to modify data or processes on the PLC (e.g. Load new program, clear data) is password authenticated.

Read/Write Protection Level

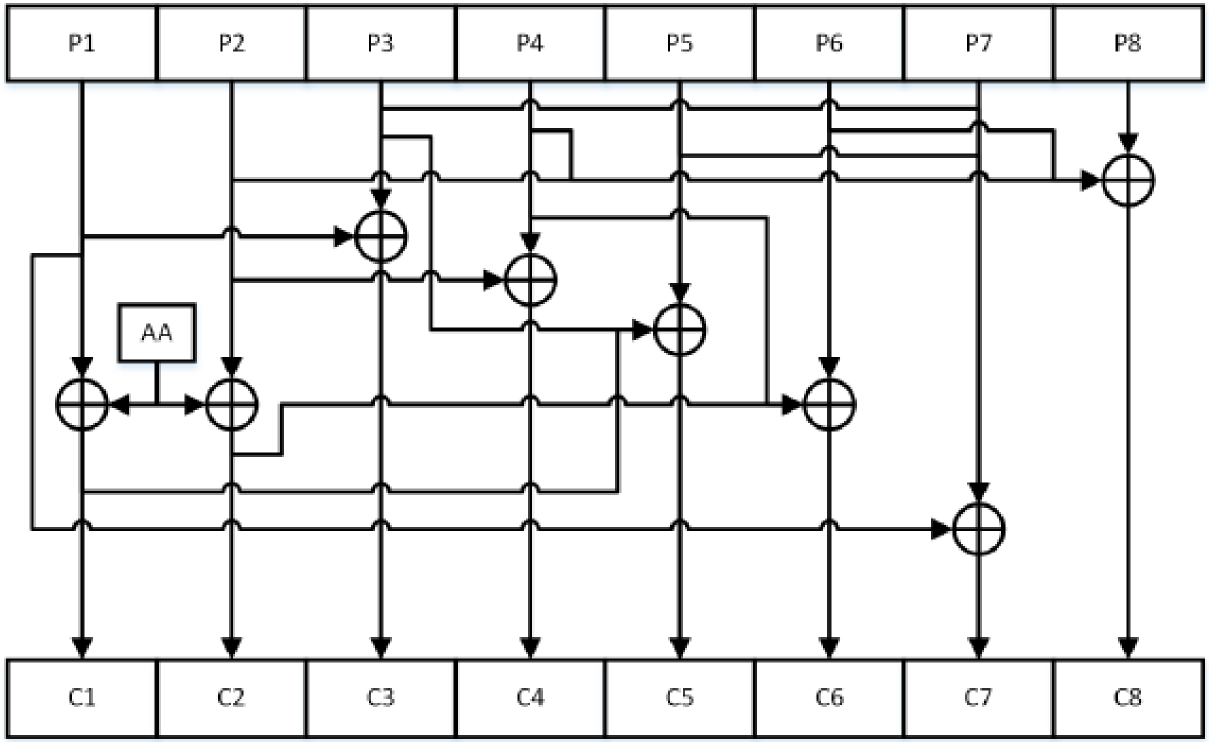
- It is the most restrictive.
- Any interaction, that is, read from or write to the PLC is password authenticated

- We focus on this protection level.

PLC Password Sniffing

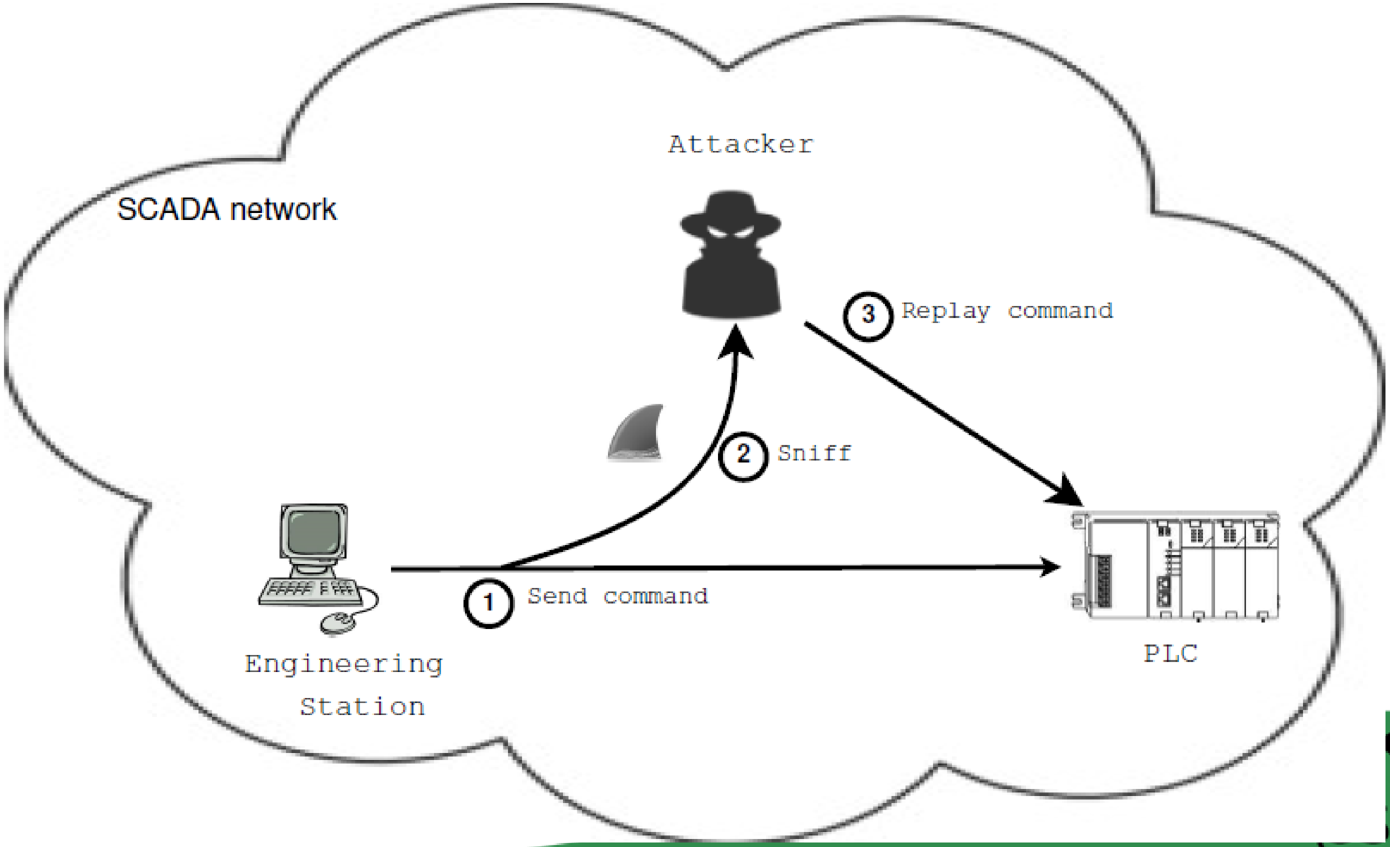
- We collected a large number of communication samples containing the password.
- We could successfully identify the location of the password.
- The password is encoded !

Password Cracking



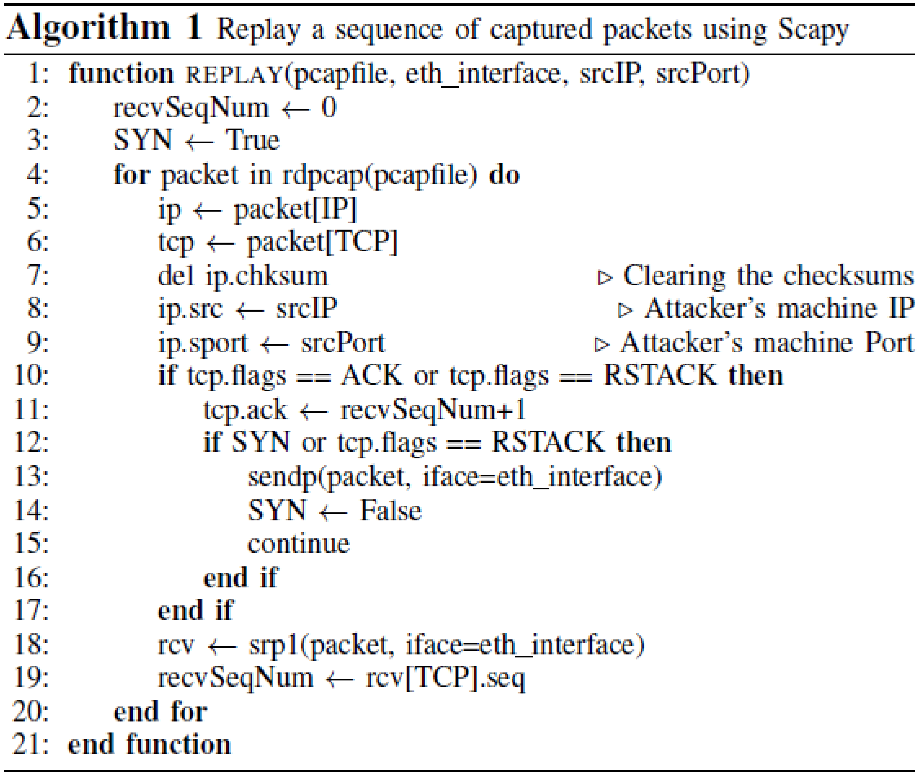
Implemented Attacks

- Replay Attack



Implemented Attacks

- Replay attack algorithm



Algorithm 1 Replay a sequence of captured packets using Scapy

```
function REPLAY(pcapfile, eth_interface, srcIP, srcPort)
    recvSeqNum ← 0
    SYN ← True
    for packet in rdpcap(pcapfile) do
        ip ← packet[IP]
        tcp ← packet[TCP]
        del ip.chksum                              ▷ Clearing the checksums
        ip.src ← srcIP                             ▷ Attacker's machine IP
        ip.sport ← srcPort                         ▷ Attacker's machine Port
        if tcp.flags == ACK or tcp.flags == RSTACK then
            tcp.ack ← recvSeqNum+1
            if SYN or tcp.flags == RSTACK then
                sendp(packet, iface=eth_interface)
                SYN ← False
                continue
            end if
        end if
        rcv ← srp1(packet, iface=eth_interface)
        recvSeqNum ← rcv[TCP].seq
    end for
end function
```

Implemented Attacks

- Password Stealing
- Unauthorized password setting and updating
- Clear PLC memory

Mitigation

- Use encrypted communications
- Use secure devices (Scalance S)
- Use network intrusion detection systems

Conclusion

- PLCs are preferred target for attacks
- PLC Access Control is still relatively weak.
- We showed how to compromise PLC password-based access control:
  - We cracked the password
  - As a consequence, we carried out several attacks
- Future work: Intrusion detection signatures to detect such attacks.

THE END

01 ICS

CSRG

CyberSecurity
Research
Group