Colorado State University
Department of Computer Science

Security Hardening of Industrial Control Systems through Attribute Based Access Control

Shwetha Gowdanakatte, Mahmoud Abdelgawad, and Indrakshi Ray

Ninth Annual Industrial Control System Security (ICSS) Workshop

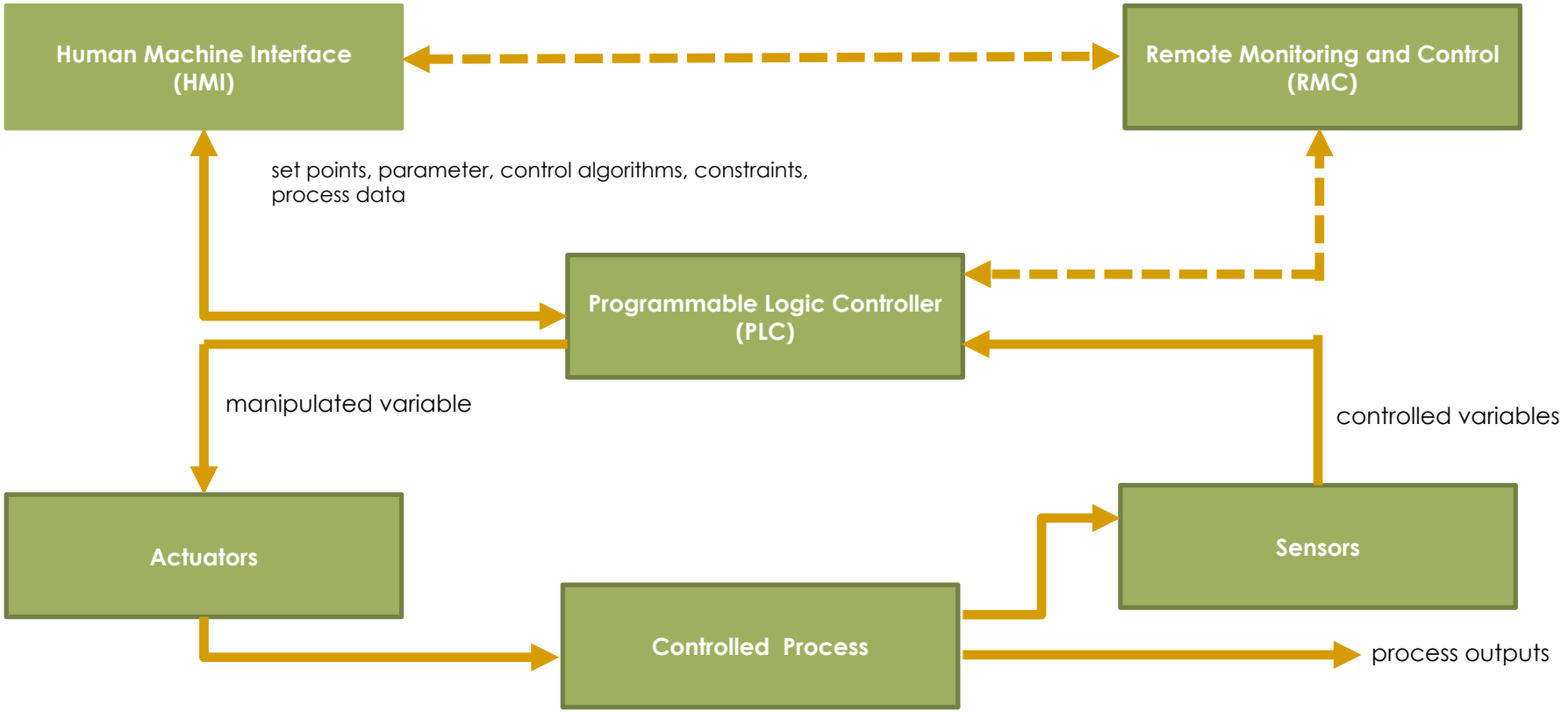
October 2023

Austin, Texas, USA

Outline

- Introduction
- Background
  - PLC and their Security Vulnerabilities
  - NIST NGAC for PLC
- Attack demonstration
  - Attack Model
  - DoS Attack on the PLC
- Security Hardening
  - ABAC Gateway
  - Testbed
  - Prevention of DoS Attack with ABAC Gateway
- Formal Verification
  - Use Case 1: PLC without ABAC Gateway
  - Use Case 2: PLC with ABAC Gateway
- Formal Analysis
- Conclusion & Future work

Industrial Control Systems (ICS)

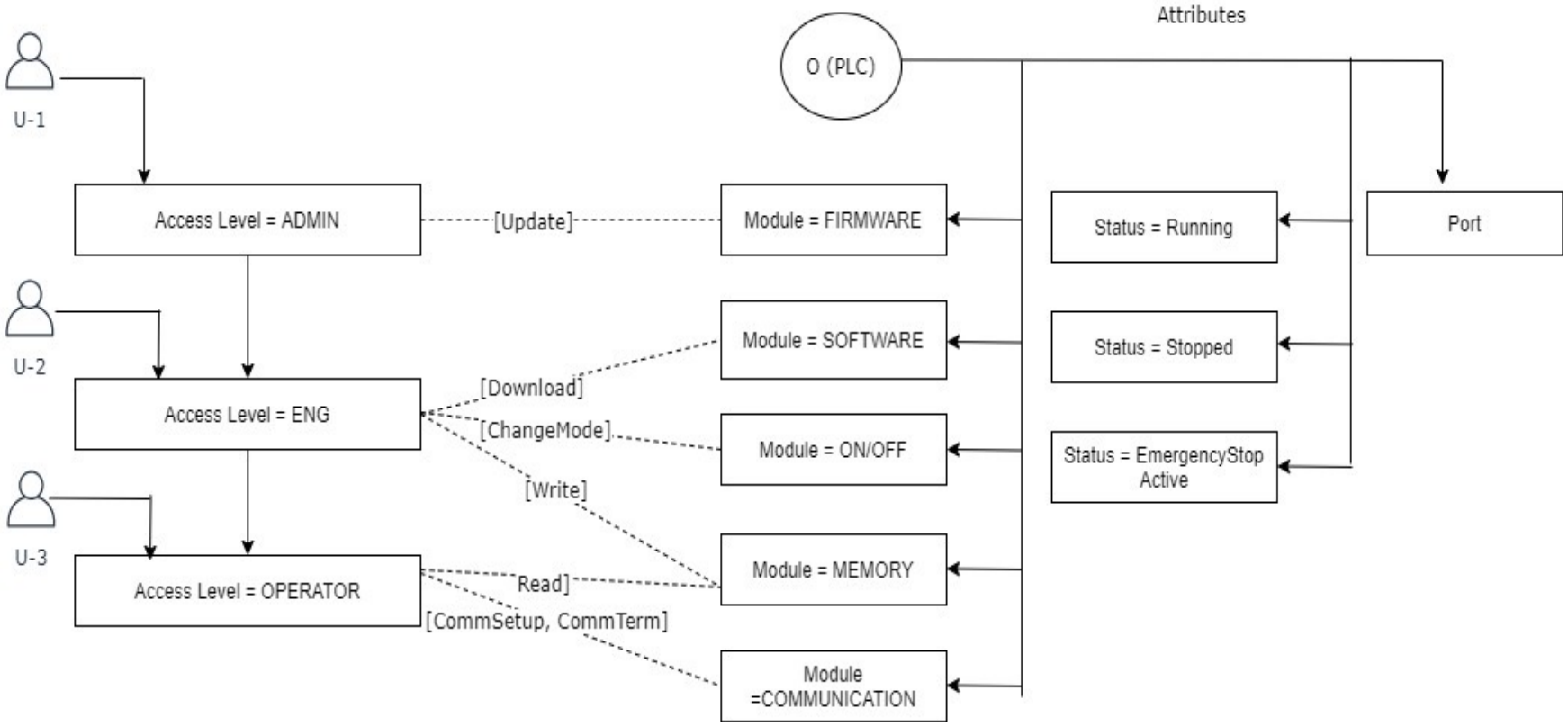


Background: PLC and their Security Vulnerabilities

- Programmable Logic Controllers
  - Rockwell Compact Logix
    - Engineering Framework: Studio 5000
    - Communication Protocol: Common Industrial Protocol (CIP)
  - Siemens S7-1500
    - Engineering Framework: Totally Integrated Automation (TIA) portal
    - Communication Protocol: S7-P3
- Recent Vulnerabilities
  - CVE-2021-1392: Obtain a CIP password and add an authorized admin user
  - CVE-2021-22681: Bypass authentication to impersonate Studio 5000
  - CVE-2016-9342 and CVE -2021-37185: Crafted TCP packets to the PLC

Background: NIST NGAC for PLC

- Attribute-Based Access Control for PLC: Gowdanakatte et al. [1]



[1] Shwetha Gowdanakatte, Indrakshi Ray, and Siv Hilde Houmb. 2022. Attribute Based Access Control Model for Protecting Programmable Logic Controllers. In Proceedings of the ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (CODASPY). ACM, Baltimore, MD, USA, 47–56.

Background: Policy Formalization

- Each policy is expressed as a tuple
  <{User Attribute}, {Resource Attribute},{Environmental Attribute},{operation}>

- User Attributes
  - Access Level = {Operator, Engineer, Administrator}
  - Device ID

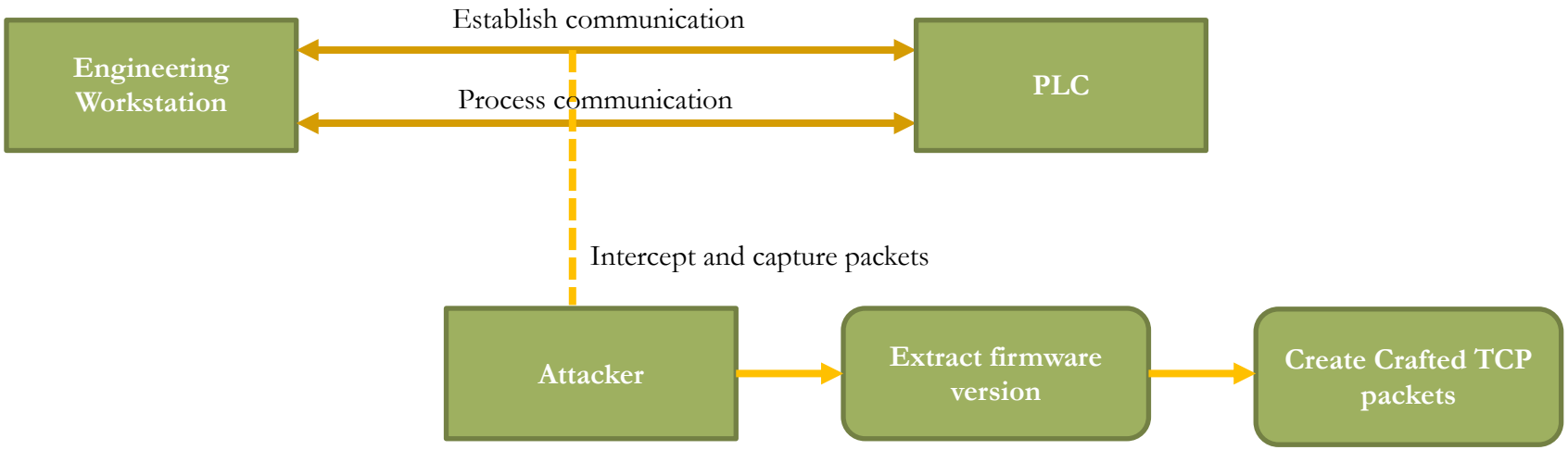
- Resource (PLC) Attributes
  - Module = {Software, Firmware, Communication, Memory}
  - Status= {Stopped, Running, Emergency Stop Active}
  - Operating Mode = {Program, Test, Error, Remote}
  - Port

- Environmental Attributes
  - User Access Time
  - User Access Location

- Example Policy: Communication Setup
  - <{(User.AccessLevel ∈ {Operator, Engineer, Administrator), (User.Device = "Equip 21L OrgABC")}, {(PLC.OperatingMode = Remote)}, {(Env. Access Time = 700 − 16 : 00EST), (Env. Access Loc = OrgABC.local")}, {CommSetup}>

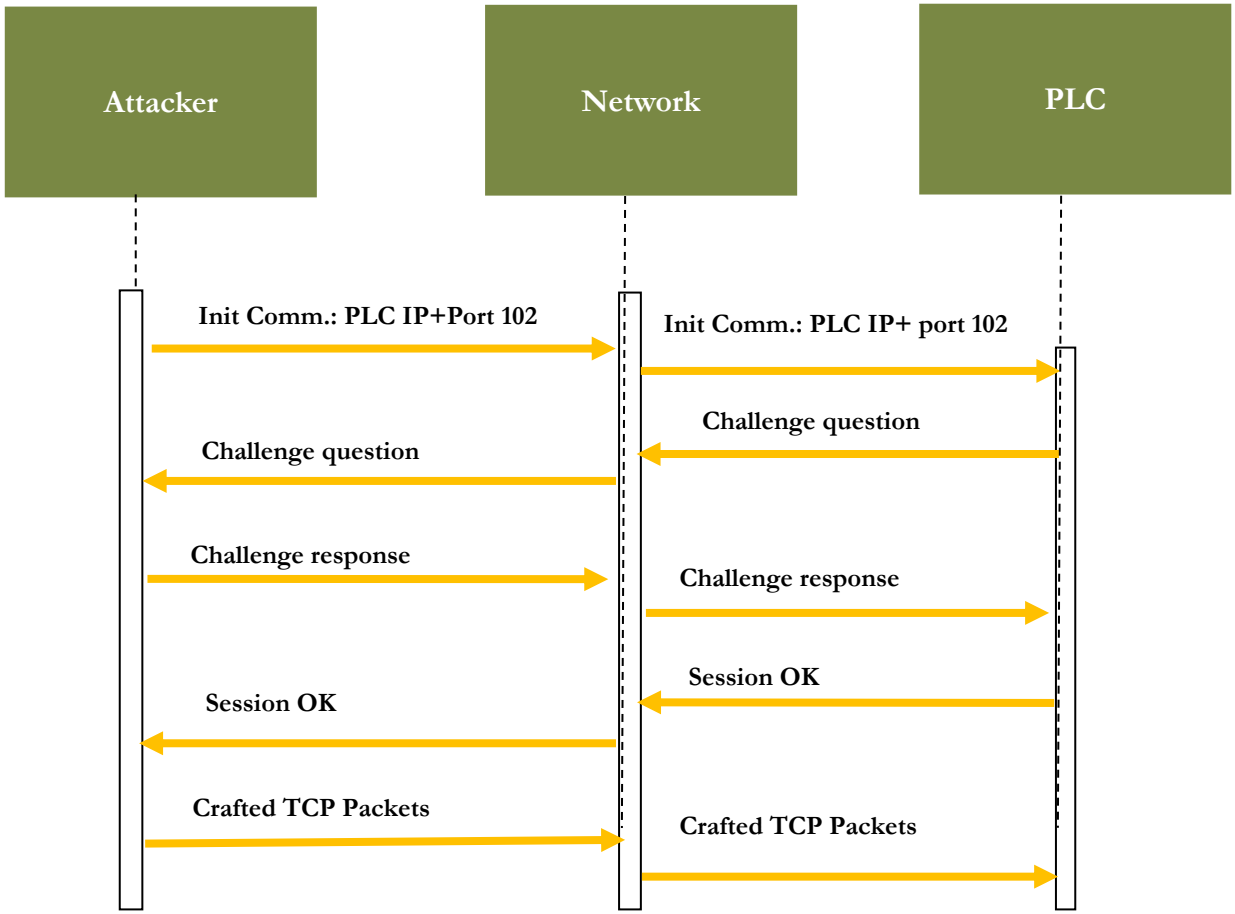
Attack Model

- Phase-1: Man-in-the-Middle (MITM) Attack



Attack Model

- Phase-2: Denial of Service (DoS) Attack



Attack Demonstration

- Attack Setup

- Phase 1: Man-in-the-Middle Attack

```
        Timeout: 10
      > Item Count: 2
        [Response In: 2378]
> Common Industrial Protocol
v CIP Connection Manager
  v Service: Unconnected Send (Request)
      0... .... = Request/Response: Request (0x0)
      .101 0010 = Service: Unconnected Send (0x52)
  v Command Specific Data
      ...0 .... = Priority: 0
      .... 1010 = Tick time: 10
      Time-out ticks: 5
      Actual Time Out: 5120ms
      Message Request Size: 8
    v Message Request
      v Common Industrial Protocol
        > Service: Get Attribute Single (Request)
          Request Path Size: 3 (words)
        v Request Path: Identity, Instance: 0x01, Attribute: 0x05 (Status)
          > Path Segment: 0x20 (8-Bit Class Segment)
          > Path Segment: 0x24 (8-Bit Instance Segment)
          > Path Segment: 0x30 (8-Bit Attribute Segment)
          Get Attribute Single (Request)
```

```
0000  b8 27 eb ab 9f 2c b8 27  eb c6 86 fa 08 00 45 00   .'...,.' ......E.
0010  00 72 cb e2 40 00 40 06  d5 d9 c0 a8 0b 9c c0 a8   .r..@.@. ........
0020  0b dd d0 24 af 12 49 01  06 39 62 65 97 4b 80 18   ...$..I. .9be.K..
0030  01 f6 f1 ec 00 00 01 01  08 0a 6c 13 f1 e3 09 b9   ........ ..l.....
0040  65 3b 6f 00 26 00 01 00  09 00 00 00 00 00 5f 70   e;o.&... ......_p
0050  79 63 6f 6d 6d 5f 00 00  00 00 00 00 00 00 0a 00   ycomm_.. ........
0060  02 00 00 00 00 00 b2 00  16 00 52 02 20 06 24 01   ........ ..R. .$.
0070  0a 05 08 00 0e 03 20 01  24 01 30 05 01 00 01 01   ...... . $ 0 ....
```

Code for requesting status

Get Attribute Single

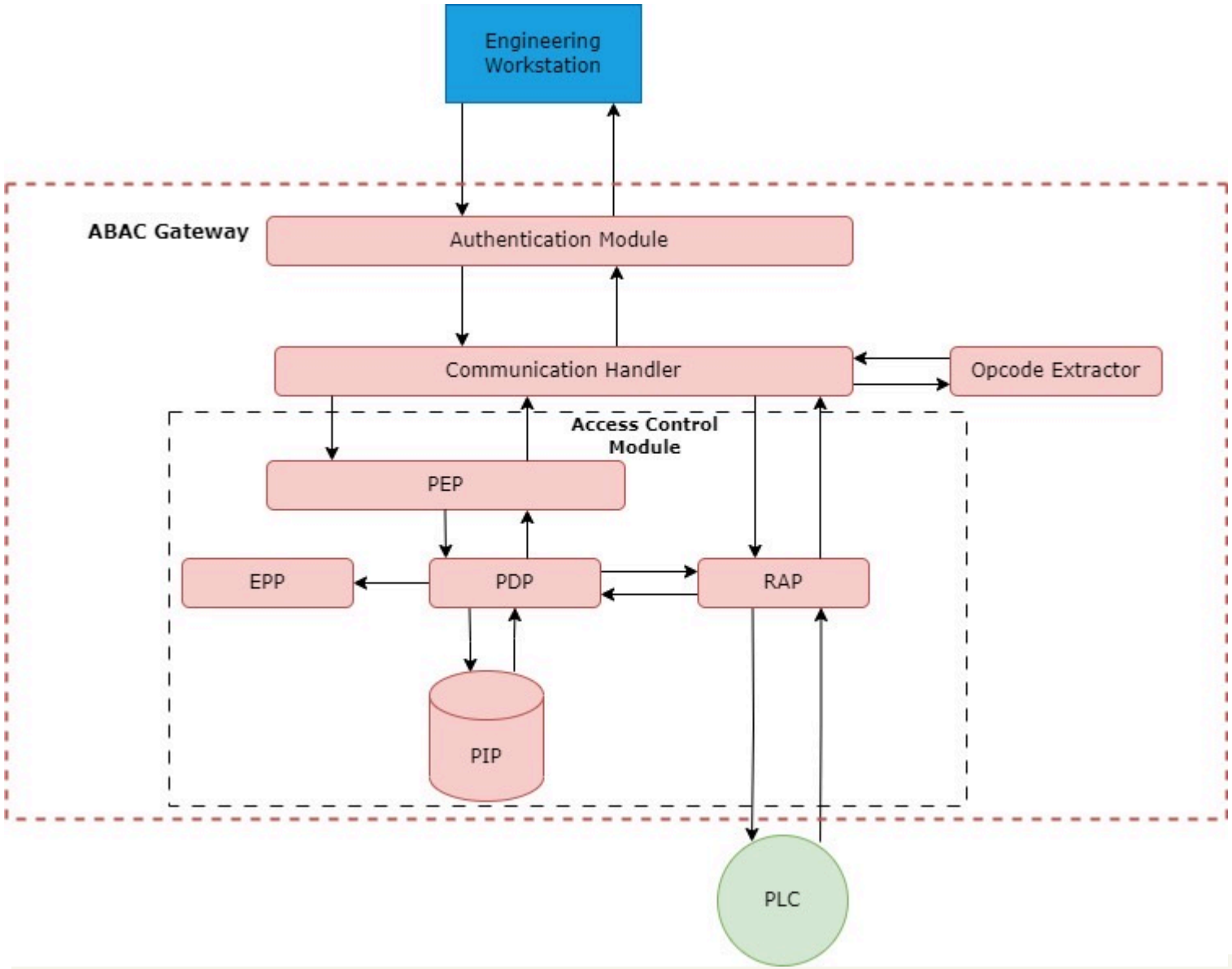
Attack Demonstration

- Phase 2: DoS Attack

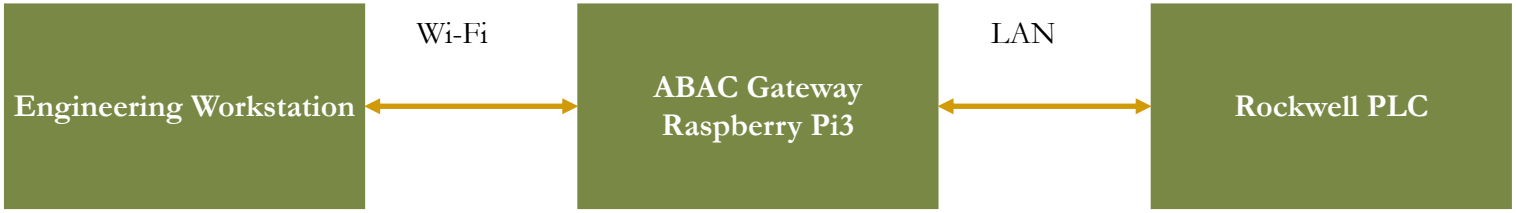
```
(0000) 6f 00 26 00 da 03 03 00 00 00 00 5f 70 79 63    o•&••••••••••_pyc
(0010) 6f 6d 6d 5f 00 00 00 00 00 00 00 00 0a 00 02 00    omm_••••••••••••
(0020) 00 00 00 00 b2 00 16 00 52 02 20 06 24 01 0a 05    ••••••••R• •$•••
(0030) 08 00 0e 03 20 01 24 01 30 90 01 00 01 01          •••• •$•0•••••
```

- Result
  - Recoverable major fault on the PLC
  - Stopping the running process
  - Unavailability of PLC for further online requests
  - Caused DoS attack
- Resolution
  - Manual restarting of the PLC through a power cycle
  - Clear major fault

ABAC Gateway



Test Bed



- NGAC-ABAC Implementation on Raspberry Pi3
  - Python Vakt library
  - Example Policy

```
actions=[Eq('CommSetup')],
subjects=[{'User.AccessLevel' : In('Operator', 'Engineer', 'Administrator'),
           'User.Device' : Eq("Equip21LOrgABC")}],
context={'Env.AccessTime' : And(GreaterOrEqual(7.00), LessOrEqual(16.00)),
         'Env.AccessLoc' : Eq("OrgABC.local"),
         'PLC.OperatingMode' : Eq('Remote')},
resources=[Eq('PLC')],
effect=vakt.ALLOW_ACCESS
```

Test Bed

- Crafted TCP Packet

```
(0000) 6f 00 26 00 da 03 03 00 00 00 00 5f 70 79 63   o•&••••••••_pyc
(0010) 6f 6d 6d 5f 00 00 00 00 00 00 00 00 0a 00 02 00   omm_•••••••••••
(0020) 00 00 00 00 b2 00 16 00 52 02 20 06 24 01 0a 05   ••••••••R• •$•••
(0030) 08 00 0e 03 20 01 24 01 30 90 01 00 01 01         •••• •$•0•••••
```

  - Device ID of Engineering Workstation: 'velpi'
  - Allowed device ID for establishing the communication with Compact Logix: 'Equip21LOrgABC'

- Communication Request Packet

```
e4 90 69 a4 3f 16 b8 27  eb ab 9f 2c 08 00 45 00   ..i.?..' ...,..E.
00 44 79 5c 40 00 40 06  28 f7 c0 a8 0b dd c0 a8   .Dy\@.@. (.......
0b 33 82 40 af 12 87 38  12 90 32 9b 69 6c 50 18   .3.@...8 ..2.ilP.
01 f6 98 97 00 00 65 00  04 00 00 00 00 00 00 00   ......e. ........
00 00 5f 70 79 63 6f 6d  6d 5f 00 00 00 00 01 00   .._pycom m_......
00 00                                              ..
```

Test Bed

Policy Verification for ‘Register Session’ Request

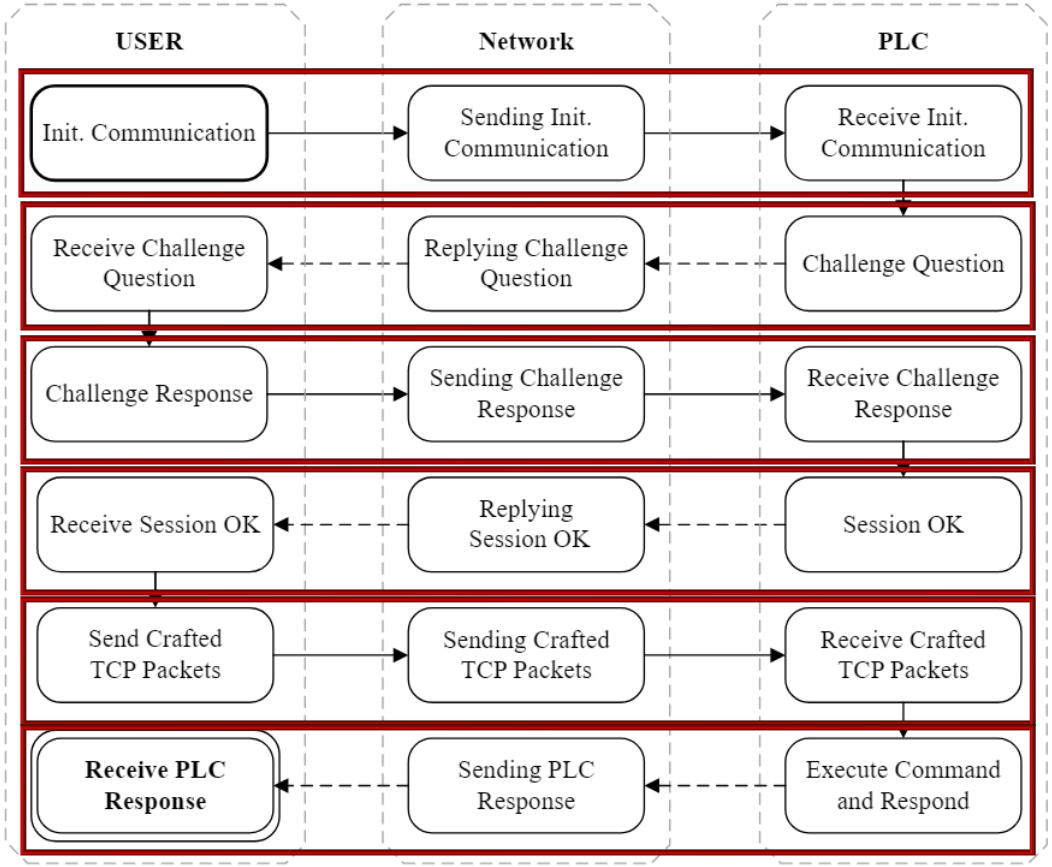
```
Connected by ('192.168.102.14', 36294)
Received from client : b'e\x00\x04\x00\x00\x00\x00\x00\x00\x00\x00\x000.8.6   \x
00\x00\x00\x00\x01\x00\x00\x00'
HexData 650004000000000000000000302e382e362020200000000001000000
Commnad 6500
Command Final CommSetup
Returned Command CommSetup
Verifying Policy
Policy Failed on Device ID and Packets Rejected
```

DoS attack prevented based on invalid device ID

Verification: PLC Operates without ABAC Gateway

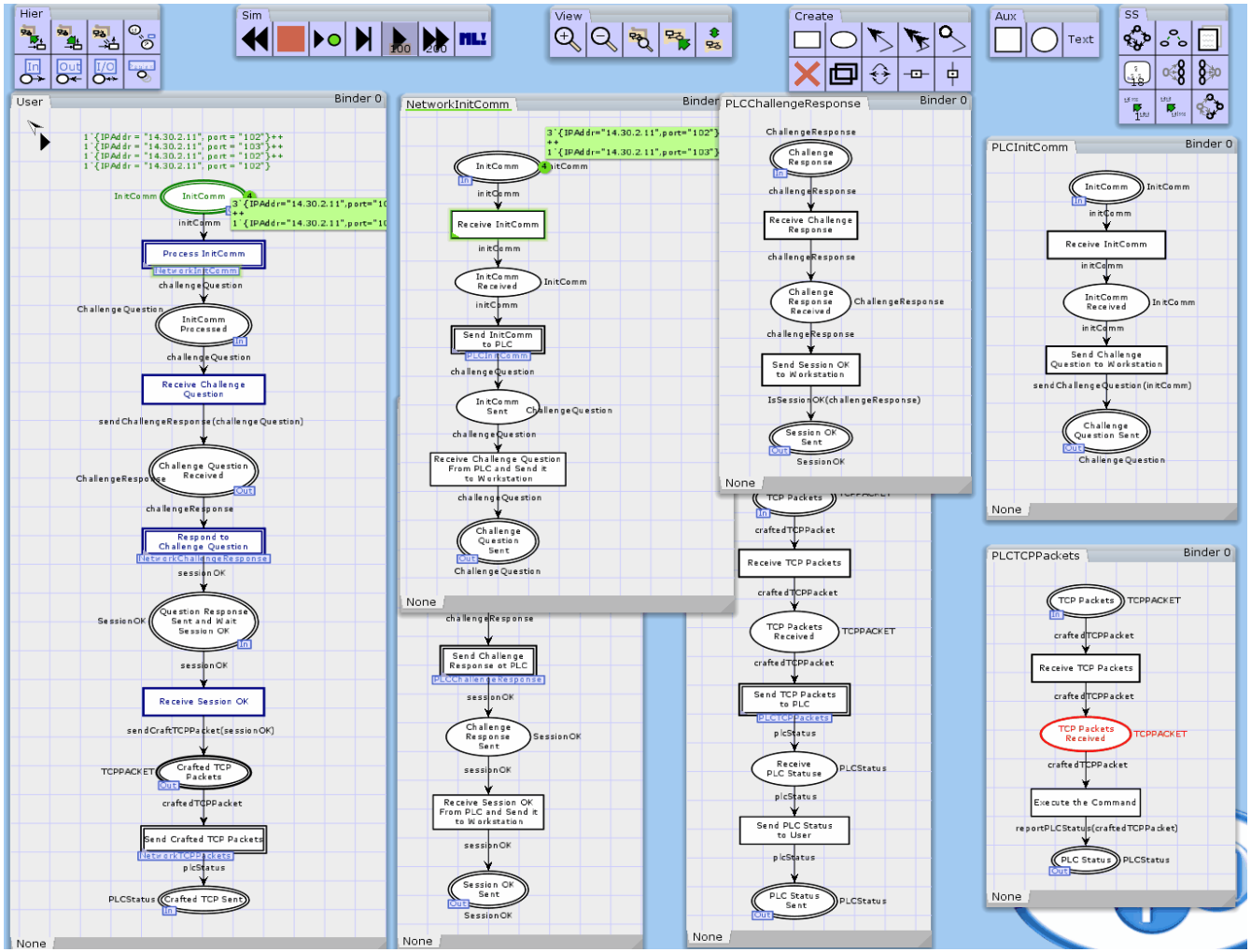
- **CPN Block Diagram**
- **Three CPNs:**
  - **User, Network, and PLC**

1. User sends a request packet to initialize communication with PLC
2. The PLC receives the request and replies with a challenge question
3. The user sends the challenge response.
4. The PLC confirms that the session is *OK* to be established.
5. The user sends a command to PLC to be executed.
6. The PLC executes the command and confirms the user with PLC status



Verification: PLC Operates without ABAC Gateway

CPN Demo: TCP Packets traveling between User and PLC through Network



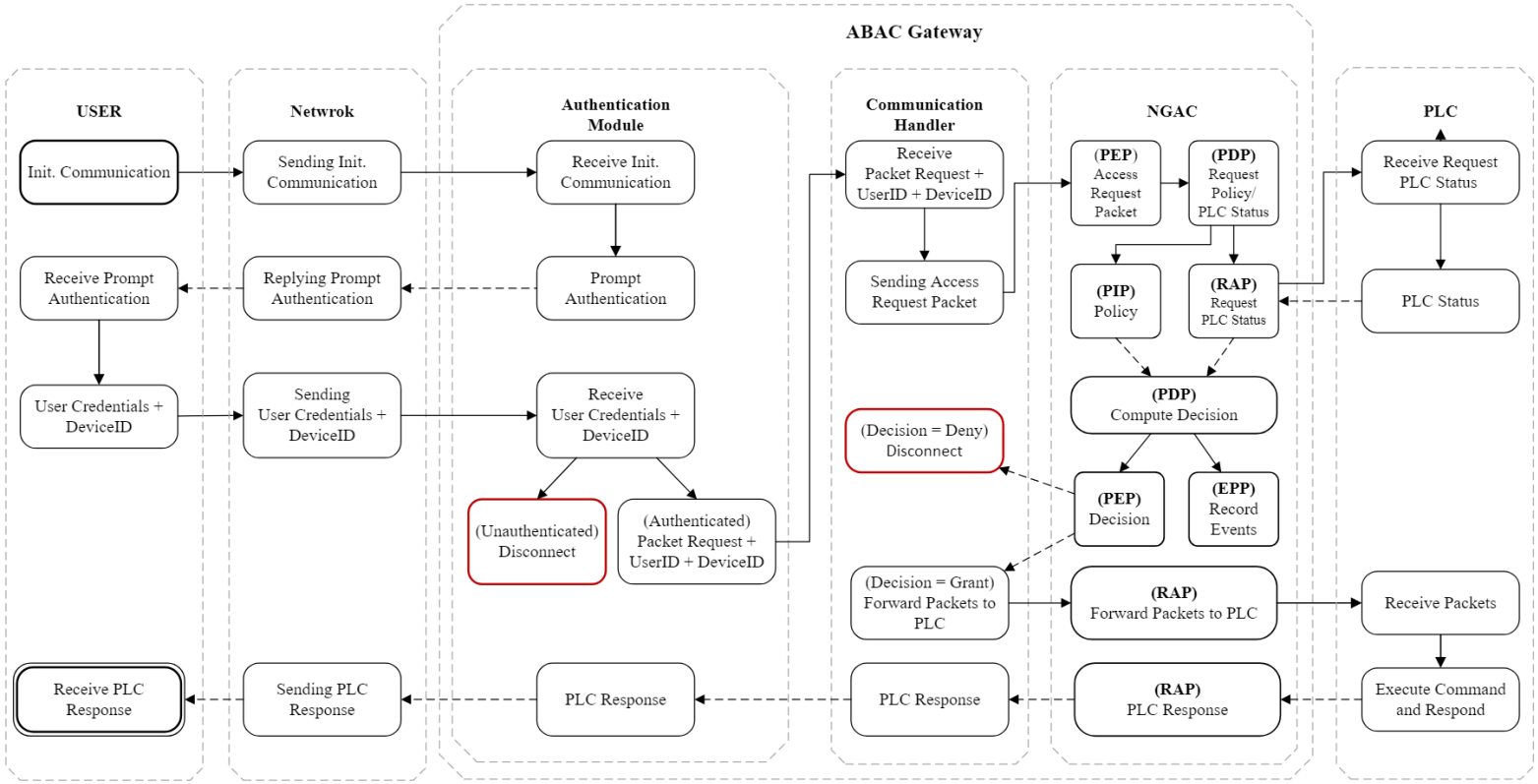
Verification: PLC Operates without ABAC Gateway

Testcases: CPN Tokens demonstrate legal access (first 3 tokens) and attacks (last 2 tokens)

TC#	Description	Input (Token)	Expected Output	Actual Output	Testcase Status
1	ADMIN: A legal user listed in DAC-ACL and has privilege to setup PLC communication	{IP = {srcIPAddr = "10.255.10.7", dstIPAddr = "129.10.1.3"}, TCP = {srcPort = "5357", dstPort = "44818", CIP = {Command = Comm.Setup, SessionHandle = "established"}}}	PLC Status Running	PLC Status Running	Passed
2	ADMIN: A legal user listed in DAC-ACL privilege to stop PLC communication	{IP = {srcIPAddr = "10.255.10.7", dstIPAddr = "129.10.1.3"}, TCP = {srcPort = "5357", dstPort = "44818", CIP = {Command = Comm.Stop, SessionHandle = "established"}}}	PLC Status Stopped	PLC Status Stopped	Passed
3	USER: A legal user listed in DAC-ACL but does not have privilege to stop PLC communication	{IP = {srcIPAddr = "10.255.10.23", dstIPAddr = "129.10.1.3"}, TCP = {srcPort = "5357", dstPort = "44818", CIP = {Command = Comm.Stop, SessionHandle = "established"}}}	PLC Status Stopped	TCP Packet Rejected	Failed
4	ATTACKER-1: An attacker impersonates USER to stop PLC communication	{IP = {srcIPAddr = "13.255.255.1", dstIPAddr = "129.10.1.3"}, TCP = {srcPort = "5357", dstPort = "44818", CIP = {Command = Comm.Stop, SessionHandle = "established"}}}	PLC Status Stopped	TCP Packet Rejected	Failed
5	ATTACKER-2: An attacker impersonates ADMIN to setup PLC communication	{IP = {srcIPAddr = "13.255.255.3", dstIPAddr = "129.10.1.3"}, TCP = {srcPort = "5357", dstPort = "44818", CIP = {Command = Comm.Stop, SessionHandle = "established"}}}	PLC Status Stopped	PLC Status Stopped	Passed

- TC#4: ATTACKER-1 impersonates USER and obtained the same access discretion, but DAC blocked its TCP request packet. (Testcase failed)
- TC#5: ATTACKER-2 impersonates ADMIN, gained its discretion, and stopped the PLC. (Testcase passed)

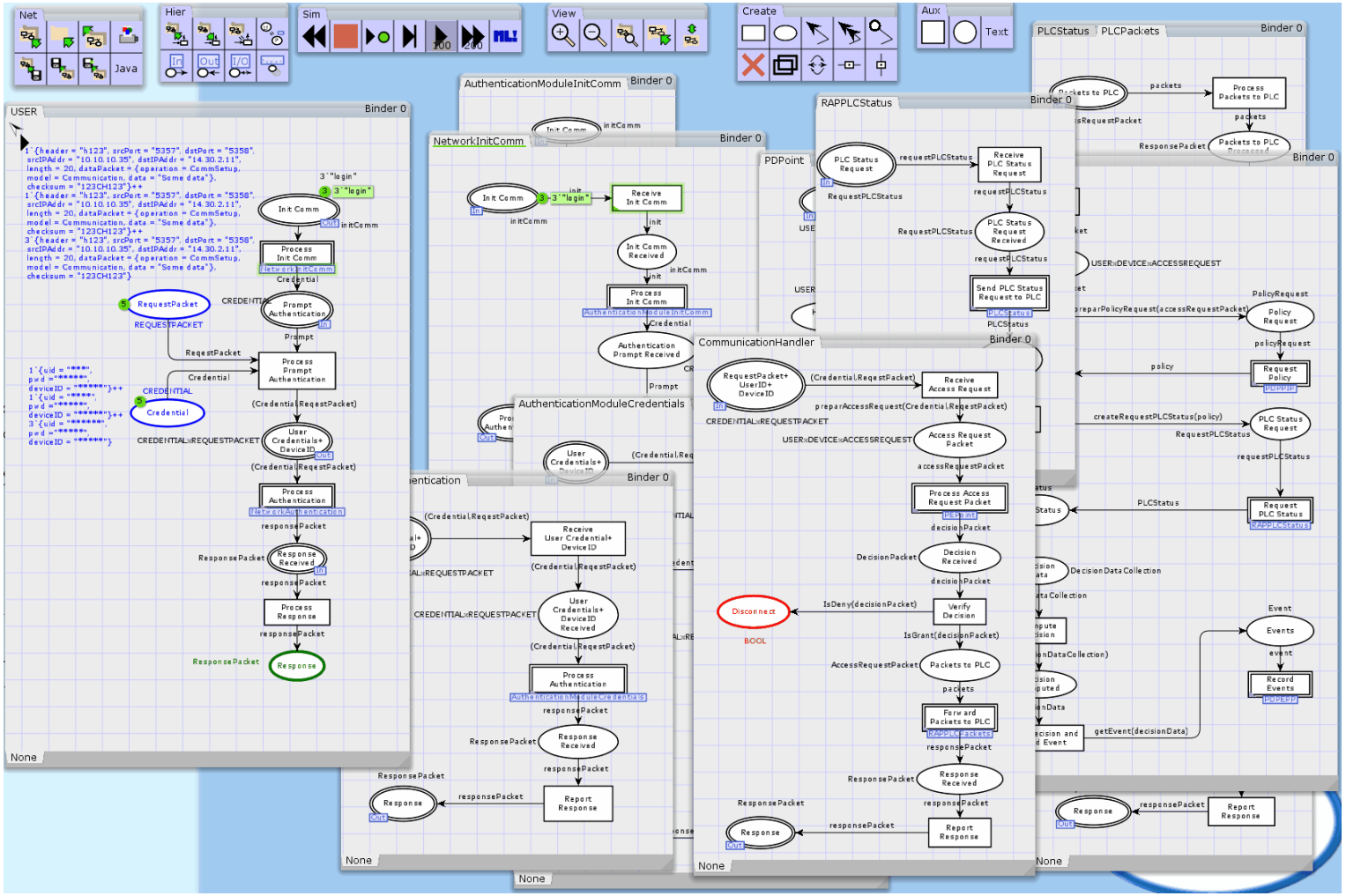
Verification: PLC Operates with ABAC Gateway



- **CPN Block Diagram:** Four CPNs (User, Network, ABAC Gateway, and PLC)
- **ABAC Gateway:** contains three sub CPN blocks: Authentication Module, Comm. Handler, and Access Control Module (NGAC)
- Any TCP Packet sent from User to PLC must go through the ABAC Gateway

Verification: PLC Operates with ABAC Gateway

CPN Demo: TCP Packets traveling between User and PLC through Network and **ABAC Gateway**



Verification: PLC Operates with ABAC Gateway

Testcases: CPN Tokens demonstrate legal access (first 3 tokens) and attacks (last 3 tokens)

TC#	Description	Input (Token)	Expected Output	Actual Output	Testcase Status
1	ADMIN: a legal user assigned in NGAC Comm.Setup policy	{IP = {srcIPAddr = "10.255.10.7", dstIPAddr = "129.10.1.3"}, TCP = {srcPort = "5357", dstPort = "44818", UserID = "ADMIN-01", EncPWD = "PWD123", DeviceID = "SR123", AccessTime = "13:10EST", CIP = {Command = Comm.Setup, SessionHandle = "established"}}}	PLC Status Running	PLC Status Running	Passed
2	ADMIN: a legal user assigned in NGAC Comm.Stop policy	{IP = {srcIPAddr = "10.255.10.7", dstIPAddr = "129.10.1.3"}, TCP = {srcPort = "5357", dstPort = "44818", UserID = "ADMIN-01", EncPWD = "PWD123", DeviceID = "SR123", AccessTime = "13:15EST", CIP = {Command = Comm.Stop, SessionHandle = "established"}}}	PLC Status Stopped	PLC Status Stopped	Passed
3	USER: a legal user has not assigned in NGAC Comm.Setup policy	{IP = {srcIPAddr = "10.255.10.23", dstIPAddr = "129.10.1.3"}, TCP = {srcPort = "5357", dstPort = "44818", UserID = "USER-01", EncPWD = "PWD567", DeviceID = "SR567", AccessTime = "13:25EST", CIP = {Command = Comm.Stop, SessionHandle = "established"}}}	PLC Status Stopped	Access Denied & User Disconnected	Failed
4	ATTACKER-1: an attacker impersonates USER to stop PLC communication	{IP = {srcIPAddr = "13.255.255.1", dstIPAddr = "129.10.1.3"}, TCP = {srcPort = "5357", dstPort = "44818", UserID = "USER-01", EncPWD = "PWD567", DeviceID = "SR999", AccessTime = "13:35EST", CIP = {Command = Comm.Stop, SessionHandle = "established"}}}	PLC Status Stopped	Authentication fails & User Disconnected	Failed
5	ATTACKER-1: an attacker impersonates USER to stop PLC communication	{IP = {srcIPAddr = "13.255.255.1", dstIPAddr = "129.10.1.3"}, TCP = {srcPort = "5357", dstPort = "44818", UserID = "USER-01", EncPWD = "PWD567", DeviceID = "SR567", AccessTime = "13:40EST", CIP = {Command = Comm.Stop, SessionHandle = "established"}}}	PLC Status Stopped	Access Denied & User Disconnected	Failed
6	ATTACKER-2: an attacker impersonates ADMIN to setup PLC communication	{IP = {srcIPAddr = "13.255.255.3", dstIPAddr = "129.10.1.3"}, TCP = {srcPort = "5357", dstPort = "44818", UserID = "ADMIN-01", EncPWD = "PWD123", DeviceID = "SR123", AccessTime = "13:45EST", CIP = {Command = Comm.Stop, SessionHandle = "established"}}}	PLC Status Stopped	Access denied & User Disconnected	Failed

- TC#6: ATTACKER-2 impersonates ADMIN, sends setup command, but it is denied by the ABAC Gateway. (Testcase failed)

Formal Analysis

State Space		SCC Graph		Status
#State	#Transition	#State	#Transition	Full
1820	5733	1820	5733	
Home State		Dead State		#Dead Transitions
[1653]		[1378,1745]		2

State-Space Analysis for Use Case 1

State Space		SCC Graph		Status
#State	#Transition	#State	#Transition	Full
4876	18057	4876	18057	
Home State		Dead State		#Dead Transitions
[683]		[722,723,3156,3157,3158,3159, 3160,3161,3162,3163,3164,3165, 3166,3167]		27

State-Space Analysis for Use Case 2

- State Space- Total number of states and transitions during the communication between the user and the PLC
- Strongly Connected Graphs (SCC)- Verifies the correctness of the model
- Dead State – Represent the state at which the communication is terminated between the user and the PLC

Conclusion

- It may be impossible to patch all the vulnerabilities of ICS.
- The solution is to protect against authentication vulnerabilities in PLC
- We developed NIST NGAC Attribute-Based Access Control for PLC protection.
- We built a testbed to demonstrate the ABAC Gateway
- Formal Verification is executed to verify the PLC system in Use Cases
  1) PLC operates without ABAC Gateway
  2) PLC operates with ABAC Gateway
- Result shows ABAC Gateway effectively hardens the PLC security

Future Work

- Currently, we are investigating the use of NIST NGAC for the security hardening of other devices in an ICS environment.
- Next, we will analyze the latency, performance, and throughput of the ICS due to the incorporation of the ABAC module

Acknowledgement

- NSF
- NIST
- Cyber Risk Research
- Statnett
- AMI
- ARL
- New Push

Thank you!

Questions?