BayesImposter: Bayesian Estimation Based Imposter Attack on Industrial Control System

Anomadarshi Barua, Lelin Pan, Mohammad Abdullah Al Faruque
Department of Electrical Engineering and Computer Science,
University of California, Irvine (UCI), USA.
Outline

❖ The ecosystem of cloud-based ICS
❖ An attack using a duplicated DLL file of cloud protocol
❖ A method to duplicate DLL files using Bayesian estimation
❖ Demonstration and evaluation of the attack
❖ Limitations
❖ Countermeasures
Infrastructure: PLCs, Clouds, and Industry 4.0

Industries evidently use VPSs to reduce the number of required physical machines to reduce cost.
Programs for PLCs

IEC 61131 programming standard has three types:
❖ Programs for basic functions
❖ Programs for supervisory controls
❖ Programs for critical time-constraint functions (e.g., security and real-time response etc.)
DLL Flies of Cloud Protocols Carry Supervisory Commands

**Diagram: Cloud server**
- **VPS1**, **VPS2**, **VPS3**
- **Upper Management**
- **PLC1**, **PLC2**, **PLC3**

**Sending program**
- for basic functions & supervisory controls

**Cloud protocols (MQTT/AMQP)**

| SL | Cloud protocol variants | Target control DLL |
|----|-------------------------|--------------------|
| 1  | EMQ X Broker            | erlexec.dll        |
| 2  | Mosquitto               | mosquito.dll       |
| 3  | MQTT-C                  | mqtt_pal.dll       |
| 4  | eMQTTTS                 | MQTT_client.dll    |
| 5  | wolfMQTT                | MqttMessage.dll    |

**Note:** DLL files are located in the parent directory of the installation folder in the VPS/cloud.
The .bss Section of DLL Flies Carry Supervisory Commands

Cloud server

VPS1
VPS2
VPS3

Upper Management

Sending program for basic functions & supervisory controls

DLL files of cloud protocols

Supervisory command related variables (e.g., various process states, sensor and actuator states, etc.)

Protocol related variables (e.g., packet length, size, timing data, connection sleep time, etc.)

Vacuum gripper robot

Page aligned in Physical memory

Pages are mapped in physical memory at load time by the operating system
Memory deduplication in Cloud server:

- It merges identical pages in the physical memory into one page to reduce redundant pages
- It is a widely used feature in cloud servers allowing multiple VPSs to run on less allocated memory in a single physical machine

Duplicate the .bss section and can use memory deduplication to locate the .bss section in the physical memory
Attack Model: BayesImposter

Stealthiness, unplanned shutdown, lost production, possible equipment damage, monetary losses, adversarial control

Cloud provider
Malicious insider
Interdiction

Attacker

Victim VPS
.bss section of target control DLL
Victim page
Cloud server

Malicious co-located VPS
Recreating .bss section of target control DLL using Bayesian estimation
.bss imposter page
Memory deduplication
Rowhammer bit flip

Cyber domain

Physical domain

Cloud protocol (MQTT/AMQP)
Sending program for supervisory controls
Industrial PLC (e.g., SIMATIC from Siemens)
False command injection

Stealthiness, unplanned shutdown, lost production, possible equipment damage, monetary losses, adversarial control

Automated high-bay warehouse
An Example: What the .bss Section Carry

- DoS Header
- PE Header
- Optional Header
- Section Header
- .rdata Section
- .data Section
- .text Section
- .bss Section
- Other Sections

Supervisory command related variables (e.g., various process states, sensor and actuator states, etc.)

Protocol related variables (e.g., packet length, size, timing data, connection sleep time, etc.)

PE32+ file format

Cloud protocol (MQTT/AMQP)

Sending program for supervisory controls

Industrial PLC (e.g., SIMATIC from Siemens)

Automated high-bay warehouse

Tag values in Tag table

- Boolean type

- Non-boolean type

Cloud protocol (MQTT/AMQP)

Sending program for supervisory controls

Industrial PLC (e.g., SIMATIC from Siemens)

Automated high-bay warehouse

Tag values in Tag table

- Boolean type

- Non-boolean type

Cloud protocol (MQTT/AMQP)

Sending program for supervisory controls

Industrial PLC (e.g., SIMATIC from Siemens)

Automated high-bay warehouse

Tag values in Tag table

- Boolean type

- Non-boolean type

Cloud protocol (MQTT/AMQP)

Sending program for supervisory controls

Industrial PLC (e.g., SIMATIC from Siemens)

Automated high-bay warehouse

Tag values in Tag table

- Boolean type

- Non-boolean type

Cloud protocol (MQTT/AMQP)

Sending program for supervisory controls

Industrial PLC (e.g., SIMATIC from Siemens)

Automated high-bay warehouse

Tag values in Tag table

- Boolean type

- Non-boolean type

Cloud protocol (MQTT/AMQP)

Sending program for supervisory controls

Industrial PLC (e.g., SIMATIC from Siemens)

Automated high-bay warehouse

Tag values in Tag table

- Boolean type

- Non-boolean type
Challenge to Duplicate the .bss Section

How to duplicate the .bss section of the DLL files of cloud protocols?

PE32+ file format

Supervisory command related variables (e.g., various process states, sensor and actuator states, etc.)

Protocol related variables (e.g., packet length, size, timing data, connection sleep time, etc.)

Tag values in Tag table
- Boolean type
- Non-boolean type

Lots of unknown values and hence high entropy,
Nearly impossible to guess all these values without any tool,
Success of the attacks depends on the duplication of these tag values
Bayesian Estimation

How to duplicate the .bss section of the DLL files of cloud protocols?

ICS is dynamic in nature and can be expressed as a state-space model
And Supervisory commands corresponds to a particular state

\[ x_k = f_{k-1}(x_{k-1}, q_{k-1}) = p(x_k \mid x_{k-1}) \rightarrow x_k \text{ is the current state} \]
\[ y_k = h_k(x_k, r_k) = p(y_k \mid x_k) \rightarrow y_k \text{ is the current measurement} \]
Bayesian Estimation..(continued)

How to duplicate the .bss section of the DLL files of cloud protocols?

\[ x_k = f_{k-1}(x_{k-1}, q_{k-1}) = p(x_k | x_{k-1}) \]  \( \rightarrow \) \( x_k \) is the current state

\[ y_k = h_k(x_k, r_k) = p(y_k | x_k) \]  \( \rightarrow \) \( y_k \) is the current measurement

\[ p(x_k | y_{1:k-1}) = \int p(x_k | x_{k-1}) p(x_{k-1} | y_{1:k-1}) \, dx_{k-1} \]  \( \rightarrow \) Chapman-Kolmogorov equation

\[ p(y_k = z | x_k) = \frac{p(x_k | y_k = z) p(y_k = z)}{\sum p(y_k) p(x_k | y_k)} \]  \( \rightarrow \) Estimating \( y_k \) for univariate and multivariate system
How to duplicate the .bss section of the DLL files of cloud protocols?

Bayesian Estimation..(continued)

Bayesian estimation using Propositions 1-5

- OPC tags, historian data, specific PLC block information, network traffic, etc.
- Supervisory command related variables (e.g., various process states, sensor and actuator states, etc.)
- Protocol related variables (e.g., packet length, size, timing data, connection sleep time, etc.)
- Cloud specific reference book, open source DLL files, proprietary DLL files, etc.

Cloud specific reference book, open source DLL files, proprietary DLL files, etc.
Memory Deduplication + Rowhammer

After duplicating the .bss section, we use memory deduplication + Rowhammer to cause bit flip in the .bss section.
Attack Model Evaluation

Cloud server with TIA portal

Sorting line

Vacuum gripper robot

Rack feeder

Warehouse

SIMATIC S7-1500 PLC

Multiprocessing oven

Oven feeder

Automated high-bay warehouse
The victim byte f7 is the upper byte of the threshold position being corrupted that changes the 2 cm threshold position to 2050 cm.
Video Demonstration

Before Attack

After Attack

The vacuum gripper robot is taking the workpiece from the storage location and placing it again on the rack feeder.

The vacuum gripper robot is taking the workpiece from the storage location but cannot place it in the pre-loading zone due to the tag value corruption by our attack. The workpiece is dropped on the workzone and it could kill a person.
Limitations

- The attacker needs a collocated VPS with the target VPS in the same cloud.
- The memory deduplication of the cloud machine should be turned on.
- The attacker should have a prior knowledge of the target ICS for Bayesian estimation.
Countermeasures

❖ Increase entropy in the .bss section - This is done using a random variable as a signature in the .bss section

❖ Securing cloud server from the malicious VPS - Any unnecessary or suspicious co-located VPS should be considered as a security breach.

❖ Turning off the KSM – Turning off the memory deduplication will also increase the memory overhead

❖ Use of target Row Refresh (TRR) capability to prevent single-sided and multi-sided Rowhammer attack on cloud networks
Work Summary

❖ Introduce the ecosystem of cloud based industrial control system
❖ Provide an attack using a duplicated .bss section of DLL files of cloud protocols and combination of memory deduplication and rowhammer
❖ Provide a demonstration, justification, and evaluation of the attack
❖ Provide limitations of our attack
❖ Provide countermeasures
Questions

Thank You for Your Attention

BayesImposter: Bayesian Estimation Based Imposter Attack on Industrial Control System

Contact Email: anomadab@uci.edu