UCIrvine | The Henry Samueli School of Engineering

Autonomous and Intelligent
Cyber-Physical Systems Laboratory

BayesImposter: Bayesian Estimation Based .bss Imposter Attack on Industrial Control System

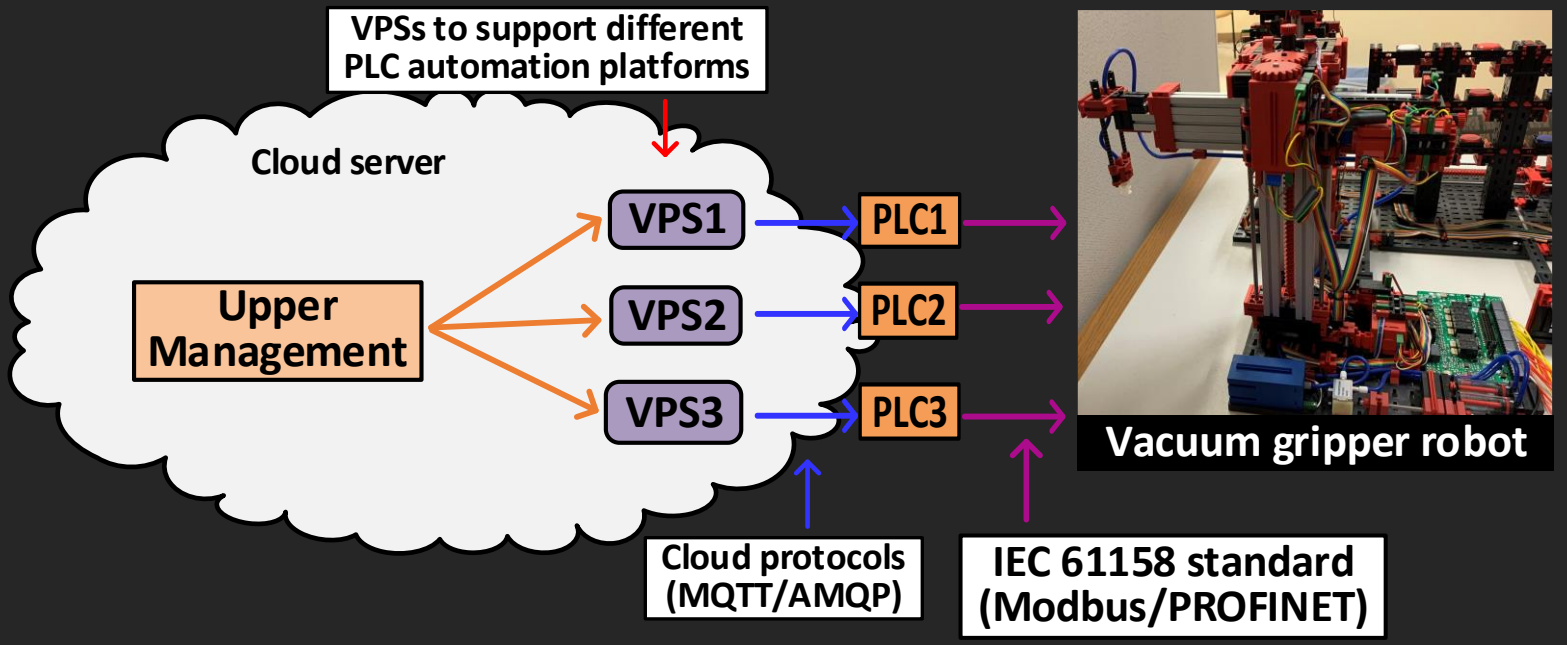
Anomadarshi Barua, Lelin Pan, Mohammad Abdullah Al Faruque

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

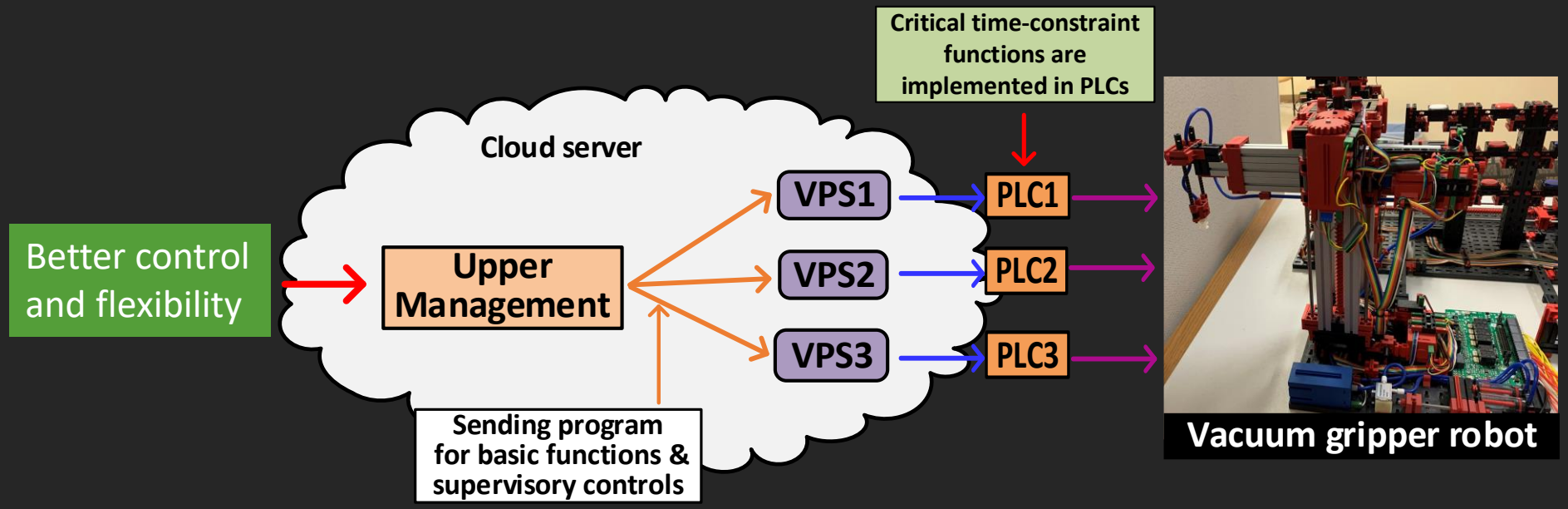


Industries evidently use VPSs to reduce the number of required physical machines to reduce cost

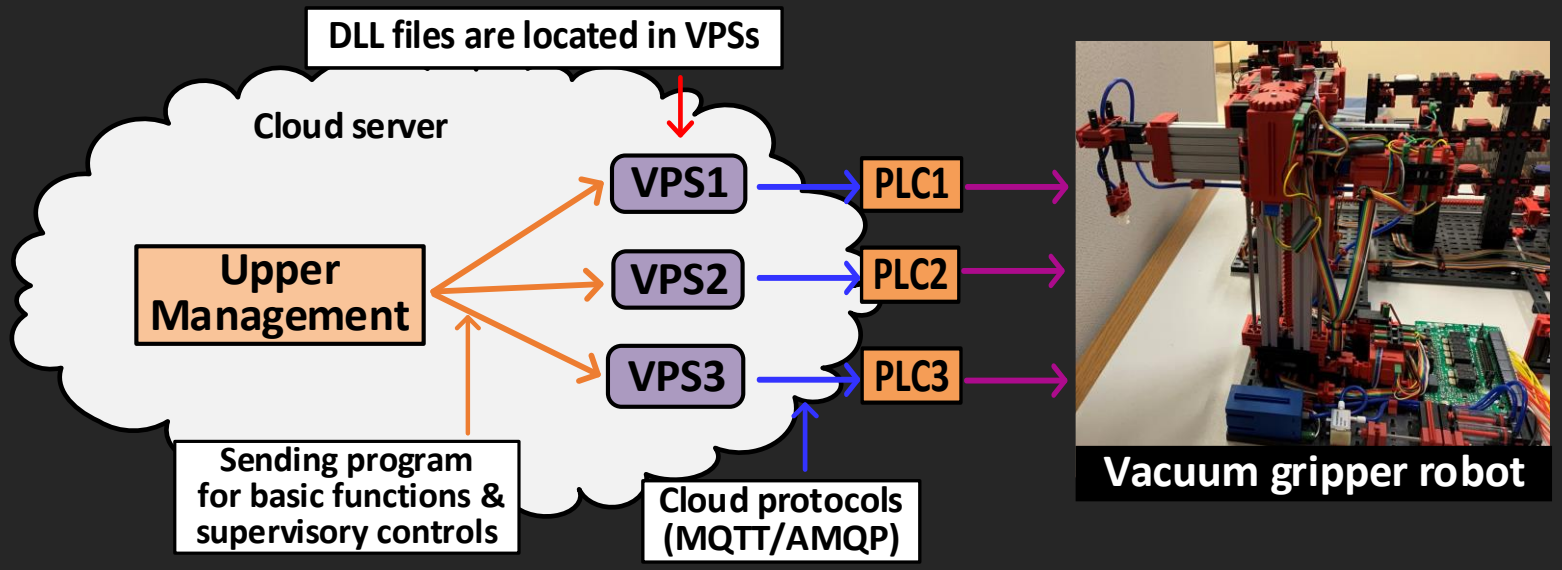
Programs for PLCs

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.)



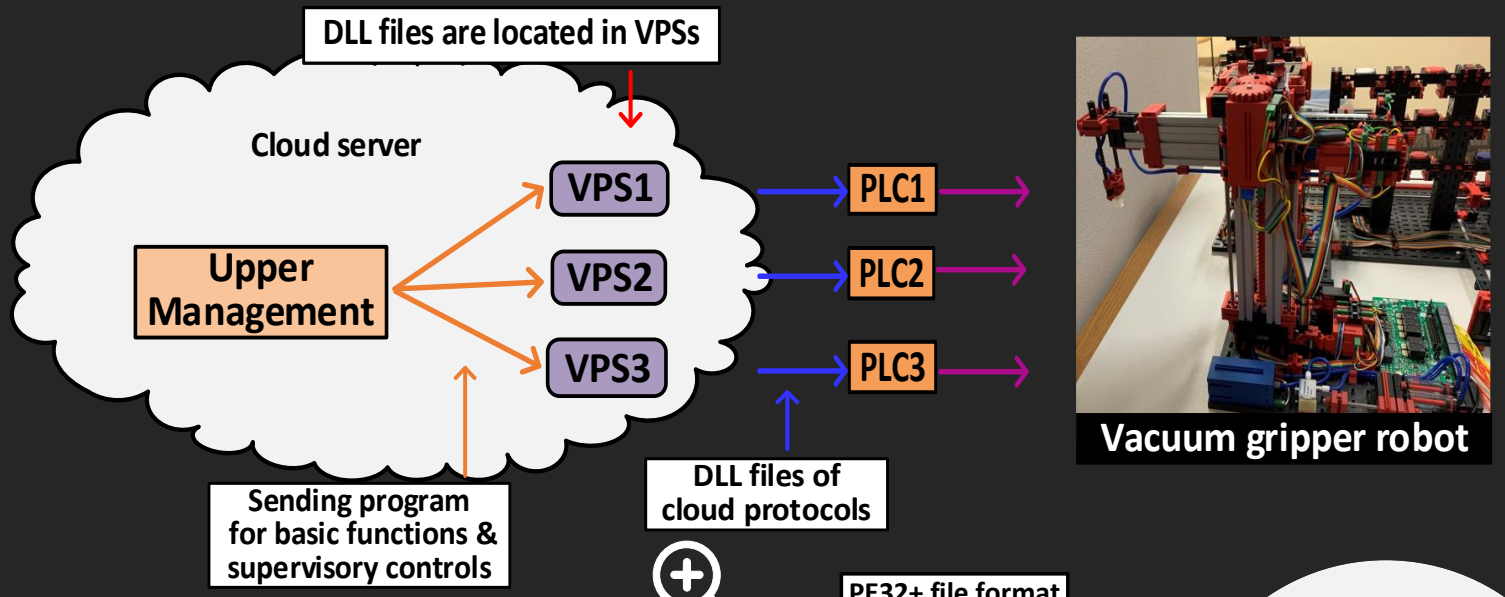
DLL Flies of Cloud Protocols Carry Supervisory Commands



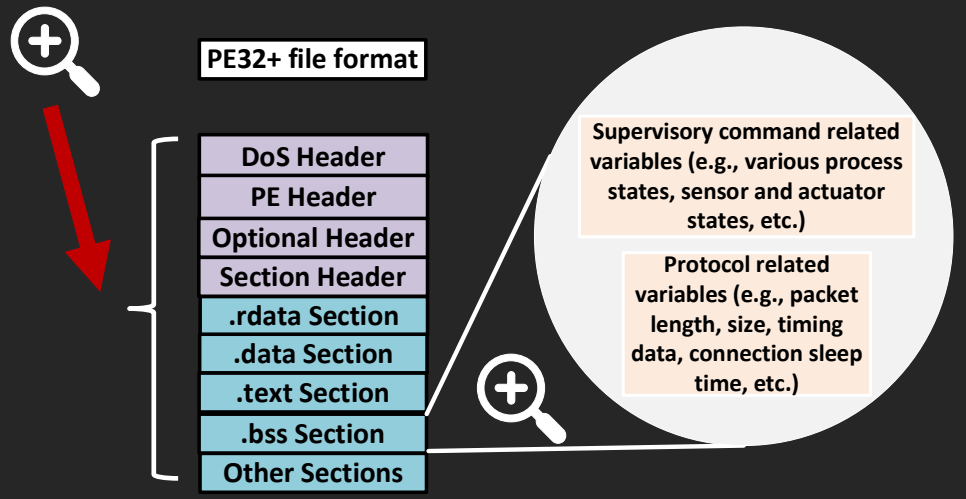
SL	Cloud protocol variants	Target control DLL
1	EMQ X Broker	erlexec.dll
2	Mosquitto	mosquitto.dll
3	MQTT-C	mqtt_pal.dll
4	eMQTT5	MQTT_client.dll
5	wolfMQTT	MqttMessage.dll

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



Vacuum gripper robot



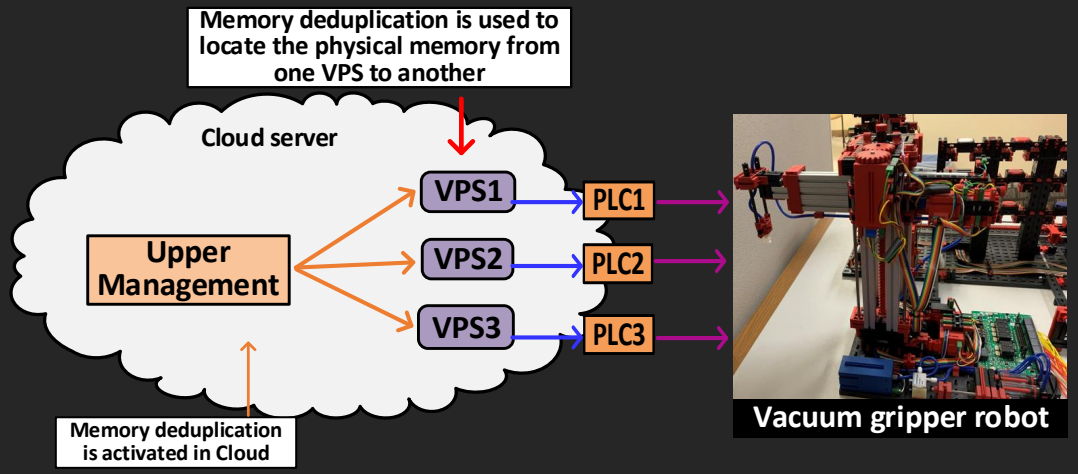
Page aligned in Physical memory

Pages are mapped in physical memory at load time by the operating system

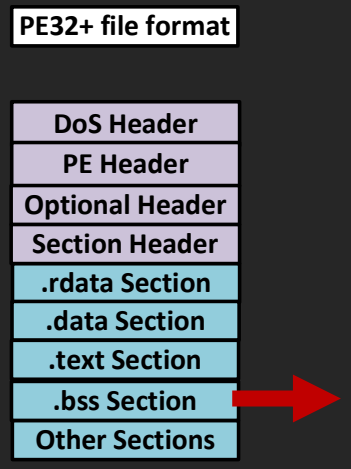
Why Memory Deduplication

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

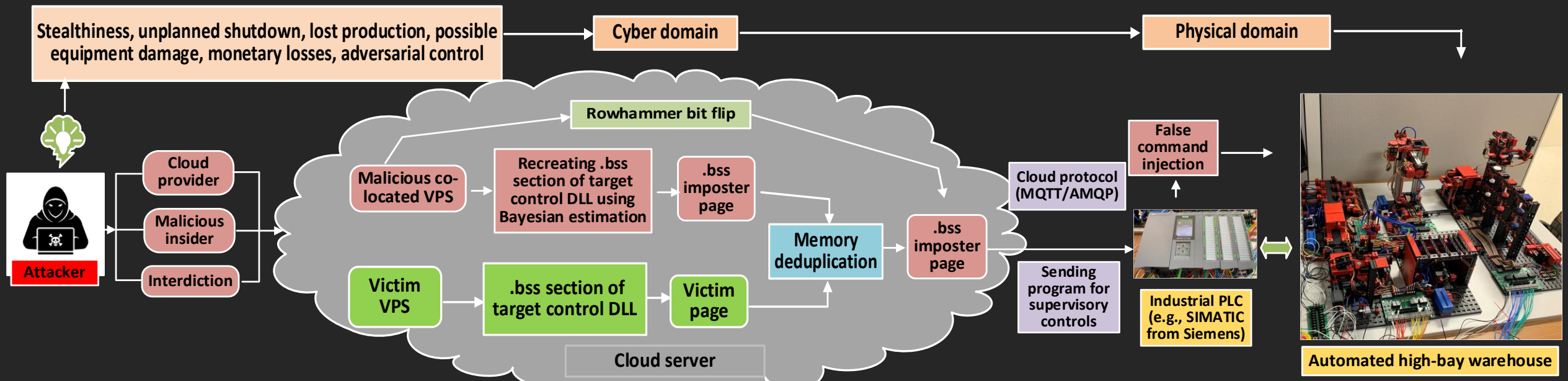


Vacuum gripper robot

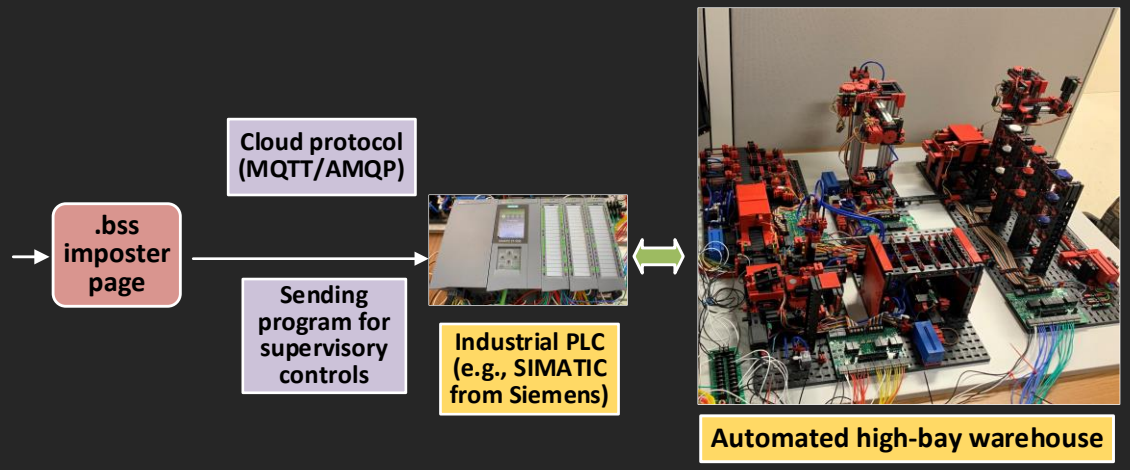


Duplicate the .bss section and can use memory deduplication to locate the .bss section in the physical memory

Attack Model: BayesImposter

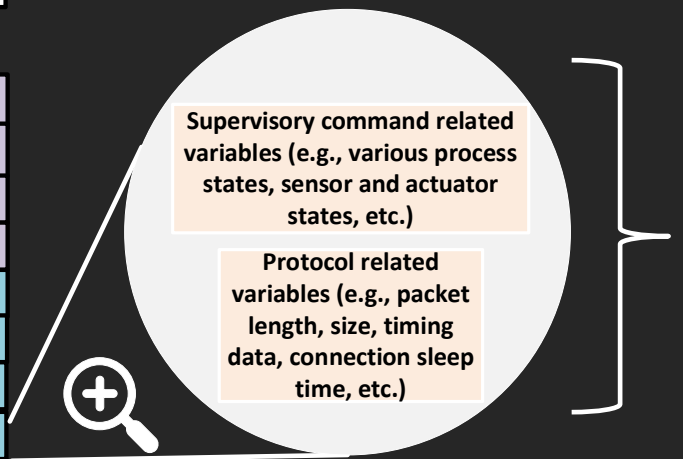


An Example: What the .bss Section Carry



PE32+ file format

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



Tag values in Tag table

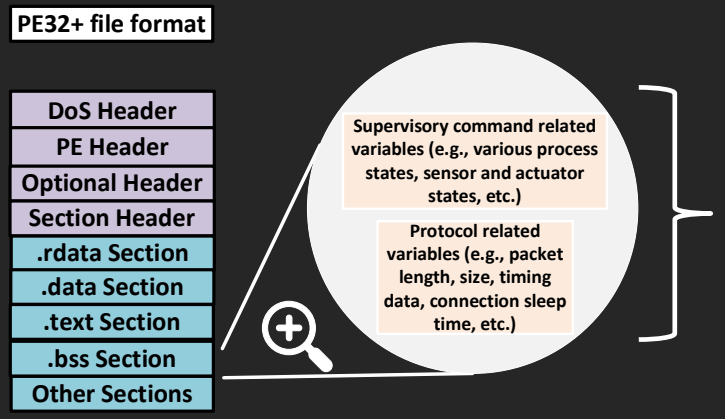
Boolean type

Non-boolean type

	Name	Path	Data Type	Logical Addr	Comment
2	RUN state	able	Bool		state started by start button 1 time
3	SL belt motor	Default tag table	Bool	%Q0.0	Q1
4	SL process white block	Default tag table	Bool	%M0.1	sorting line, processing white block
5	SL process blue block	Default tag table	Bool	%M0.3	sorting line, processing blue block
6	SL process red block	Default tag table	Bool	%M0.4	sorting line, processing red block
7	SL light barrier inlet	Default tag table	Bool		ng line light barrier inlet state, start
8	SL eject the block	Default tag table	Bool	%M0.7	sorting line ejecting a block
9	SL block detected	Default tag table	Bool	%M40.0	sorting line detected a block
10	SL colour sensor	Default tag table	Int	%IW4	I4: sorting line analog colour sensor
11	SL compressor	Default tag table	Bool	%Q0.1	Q2: sorting line vacuum compressor
12	SL white block ejector valve	Default tag table	Bool	%Q0.2	Q3: ejector valve for white block
13	SL blue block ejector valve	Default tag table	Bool	%Q0.4	Q5: ejector valve for blue block
14	SL red block ejector valve	Default tag table	Bool	%Q0.3	Q4: ejector valve for red block

Challenge to Duplicate the .bss Section

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



	Name	Path	Data Type	Logical Addr	Comment
2	RUN state	Default tag table	Bool	%Q0.0	state started by start button 1 time
3	SL belt motor	Default tag table	Bool	%Q0.0	Q1
4	SL process white block	Default tag table	Bool	%M0.1	sorting line, processing white block
5	SL process blue block	Default tag table	Bool	%M0.3	sorting line, processing blue block
6	SL process red block	Default tag table	Bool	%M0.4	sorting line, processing red block
7	SL light barrier inlet	Default tag table	Bool		ng line light barrier inlet state, start
8	SL eject the block	Default tag table	Bool	%M0.7	sorting line ejecting a block
9	SL block detected	Default tag table	Bool	%M40.0	sorting line detected a block
10	SL colour sensor	Default tag table	Int	%IW4	I4: sorting line analog colour sensor
11	SL compressor	Default tag table	Bool	%Q0.1	Q2: sorting line vacuum compressor
12	SL white block ejector valve	Default tag table	Bool	%Q0.2	Q3: ejector valve for white block
13	SL blue block ejector valve	Default tag table	Bool	%Q0.4	Q5: ejector valve for blue block
14	SL red block ejector valve	Default tag table	Bool	%Q0.3	Q4: ejector valve for red block

Tag values in Tag table

Boolean type

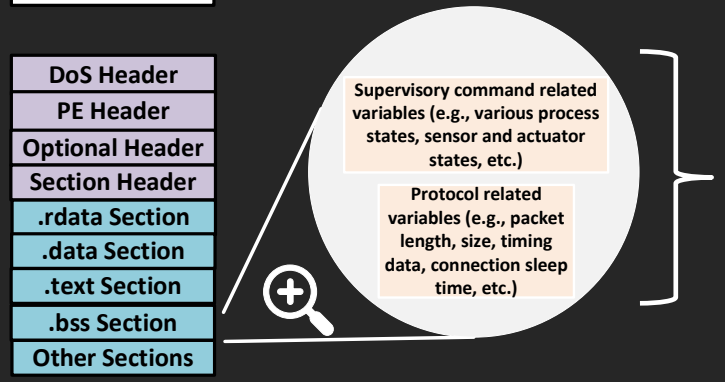
Non-boolean type

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?

PE32+ file format



	Name	Path	Data Type	Logical Addr	Comment
2	RUN state	Default tag table	Bool	%Q0.0	state started by start button 1 time
3	SL belt motor	Default tag table	Bool	%Q0.0	Q1
4	SL process white block	Default tag table	Bool	%M0.1	sorting line, processing white block
5	SL process blue block	Default tag table	Bool	%M0.3	sorting line, processing blue block
6	SL process red block	Default tag table	Bool	%M0.4	sorting line, processing red block
7	SL light barrier inlet	Default tag table	Bool		ng line light barrier inlet state, start
8	SL eject the block	Default tag table	Bool	%M0.7	sorting line ejecting a block
9	SL block detected	Default tag table	Bool	%M40.0	sorting line detected a block
10	SL colour sensor	Default tag table	Int	%IW4	I4: sorting line analog colour sensor
11	SL compressor	Default tag table	Bool	%Q0.1	Q2: sorting line vacuum compressor
12	SL white block ejector valve	Default tag table	Bool	%Q0.2	Q3: ejector valve for white block
13	SL blue block ejector valve	Default tag table	Bool	%Q0.4	Q5: ejector valve for blue block
14	SL red block ejector valve	Default tag table	Bool	%Q0.3	Q4: ejector valve for red block

Tag values in Tag table

Boolean type

Non-boolean type

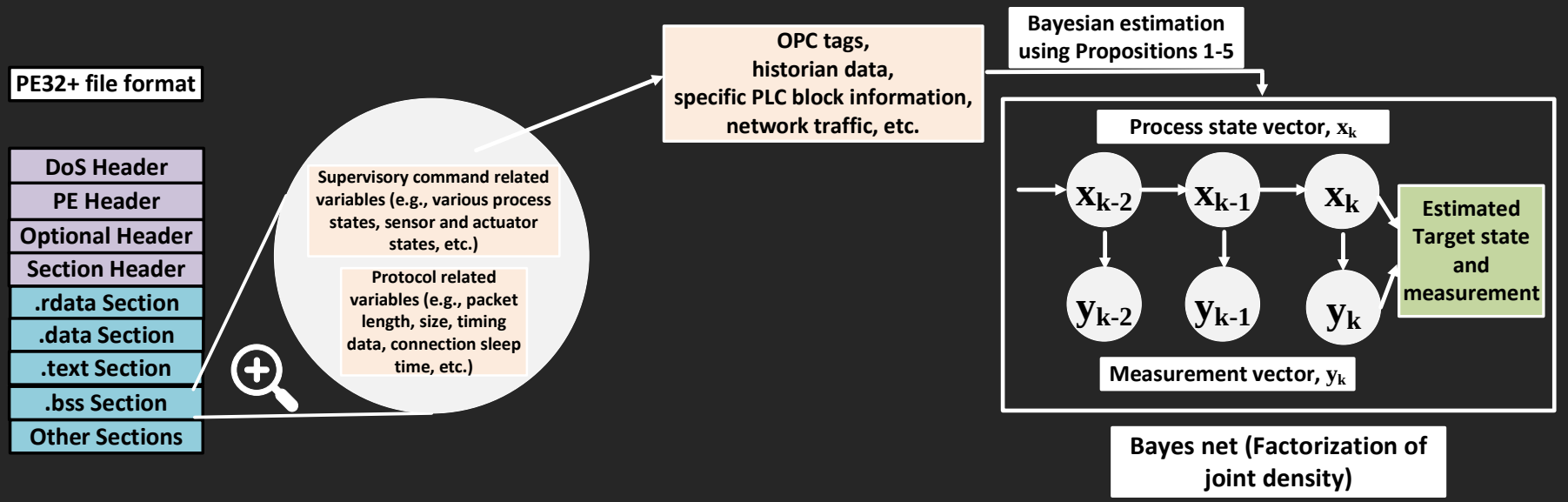
ICS is dynamic in nature and can be expressed as a state-space model
And Supervisory commands corresponds to a particular state

$$x_k = f_{k-1}(x_{k-1}, q_{k-1}) = p(x_k \mid x_{k-1})$$ -> x_k is the current state

$$y_k = h_k(x_k, r_k) = p(y_k \mid x_k)$$ -> y_k is the current measurement

Bayesian Estimation..(continued)

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



$x_k = f_{k-1}(x_{k-1}, q_{k-1}) = p(x_k \mid x_{k-1})$ -> x_k is the current state

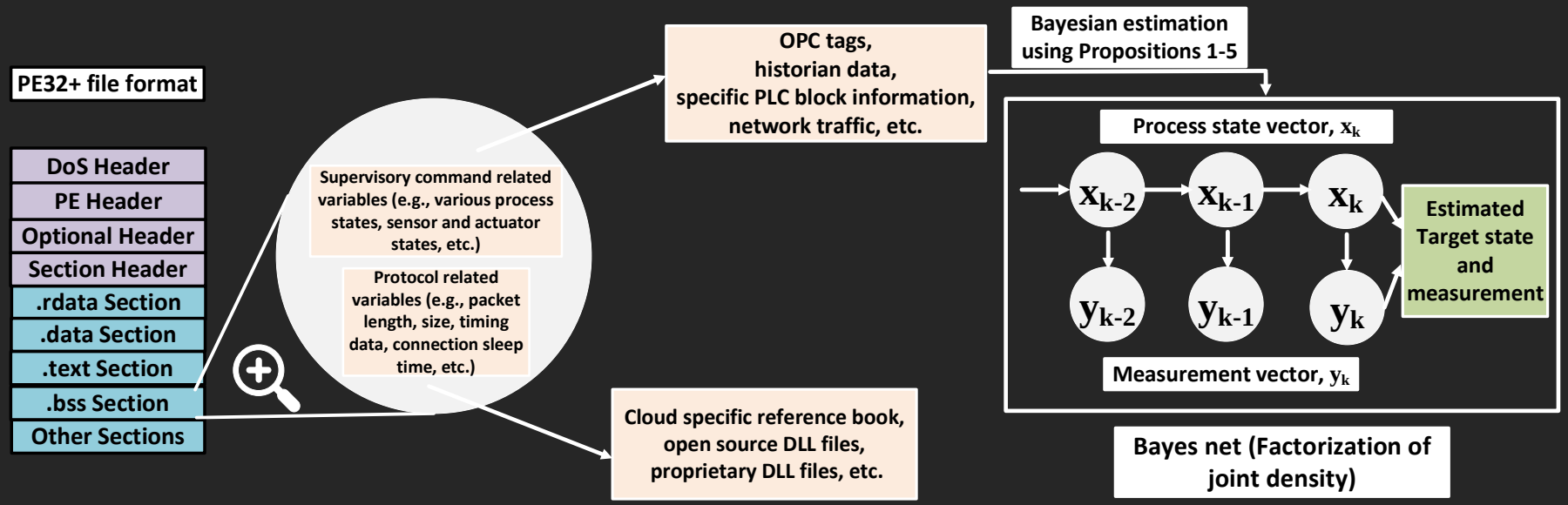
$y_k = h_k(x_k, r_k) = p(y_k \mid x_k)$ -> y_k is the current measurement

$p(x_k \mid y_{1:k-1}) = \int p(x_k \mid x_{k-1})\, p(x_{k-1} \mid y_{1:k-1})\, dx_{k-1}$ -> Chapman-Kolmogorov equation

$$p(y_k = z \mid x_k) = \frac{p(x_k \mid y_k = z)\, p(y_k = z)}{\sum p(y_k)\, p(x_k \mid y_k)}$$ ->Estimating y_k for univariate and multivariate system

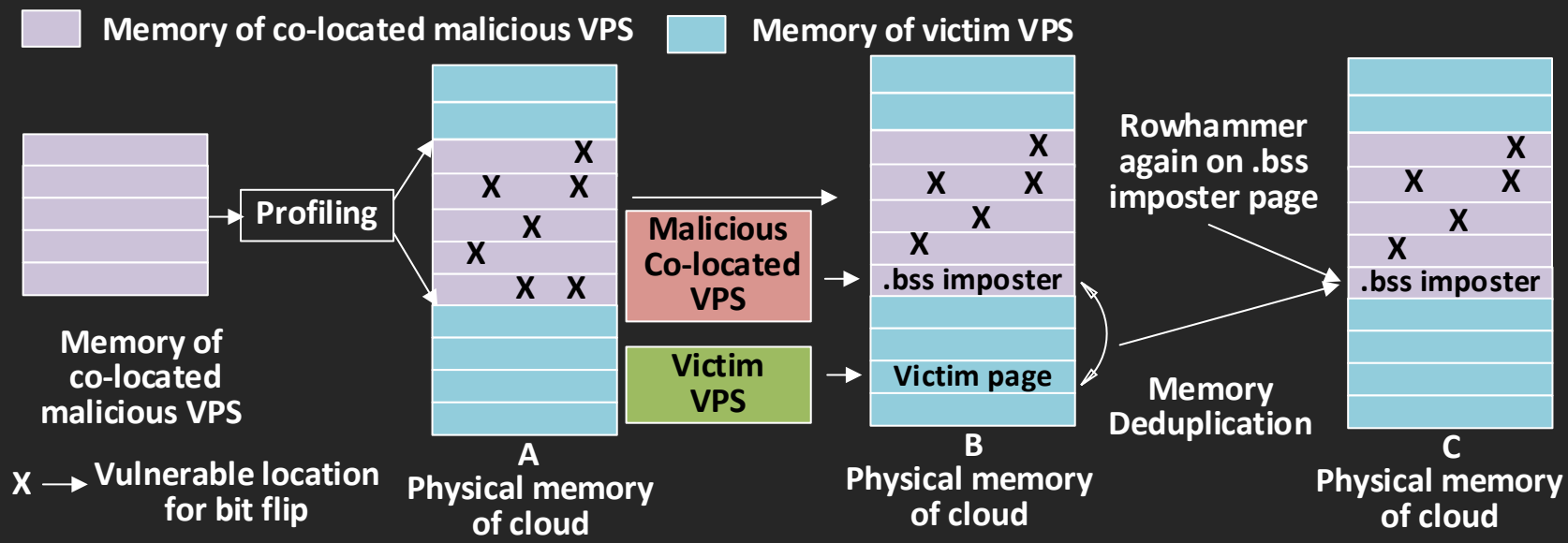
Bayesian Estimation..(continued)

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

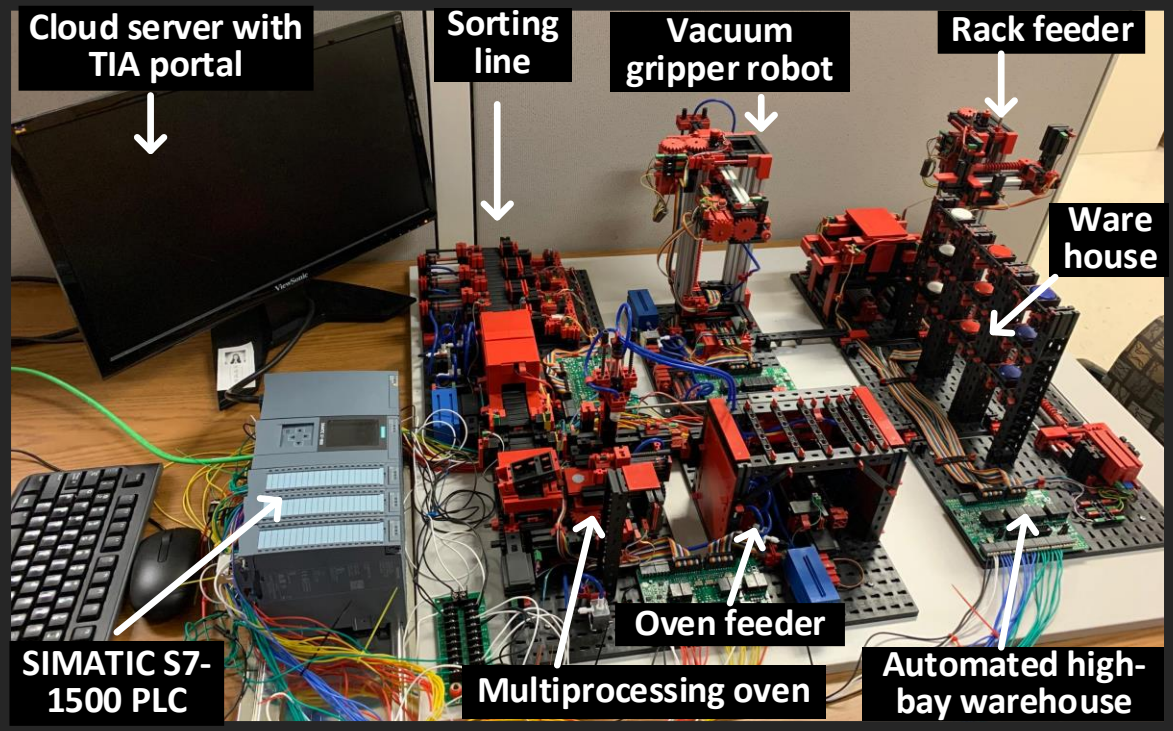


Memory Deduplication + Rowhammer

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



Attack Model Evaluation



Bit-Flip in the .bss Imposter Page

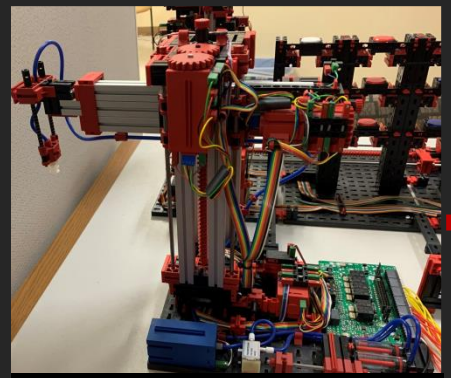
```
809 (0 0 1 7 383b   0) (0 0 1 7 3b5d   0) :
810 (0 0 1 7 3b72   0) (0 0 1 7 3b5d   0) :
811 (0 0 1 7 3b73   0) (0 0 1 7 3b5d   0) :
812 (0 0 1 7 3baf   0) (0 0 1 7 3b5d   0) :
813 (0 0 1 7 3bde   0) (0 0 1 7 3b5d   0) :
814 (0 0 1 7 3c96   0) (0 0 1 7 3b5d   0) : (0 0 1 7 3c97   0) 0743|f7|ff
815 (0 0 1 7 3c97   0) (0 0 1 7 3b5d   0) :
816 (0 0 1 7 3c98   0) (0 0 1 7 3b5d   0) :
817 (0 0 1 7 3e03   0) (0 0 1 7 3b5d   0) :
818 (0 0 1 7 3fdc   0) (0 0 1 7 3b5d   0) :
819 (0 0 1 7 456d   0) (0 0 1 7 3b5d   0) :
820 (0 0 1 7 4f4c   0) (0 0 1 7 3b5d   0) :
```

Format: <channel><dimm><rank> <bank><row><column>

Row offset

After bit-flip

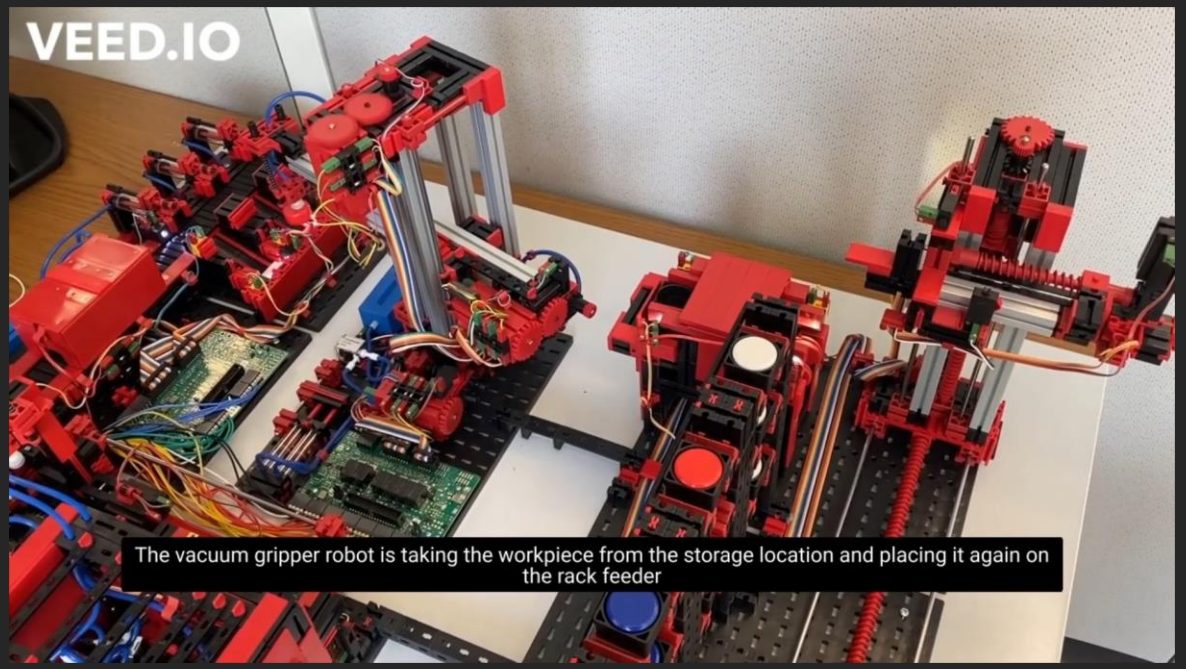
Expected fill pattern



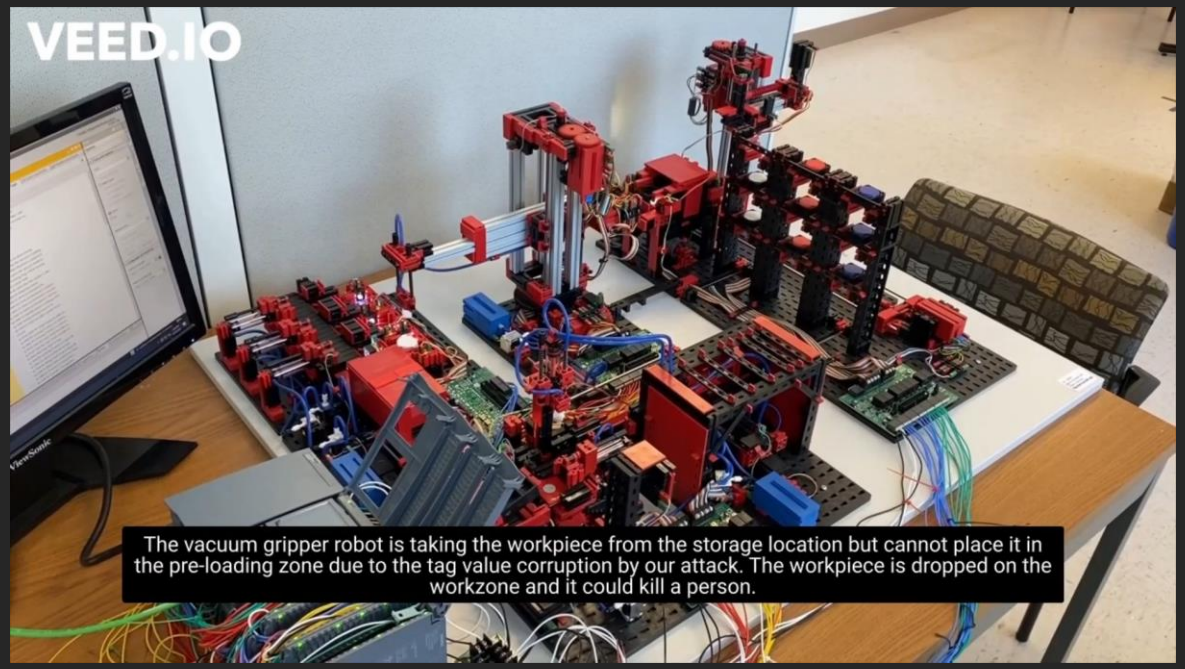
Vacuum gripper robot

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

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 .bss Imposter Attack on Industrial Control System

Contact Email: anomadab@uci.edu