Software Techniques for Cyber-Physical Systems

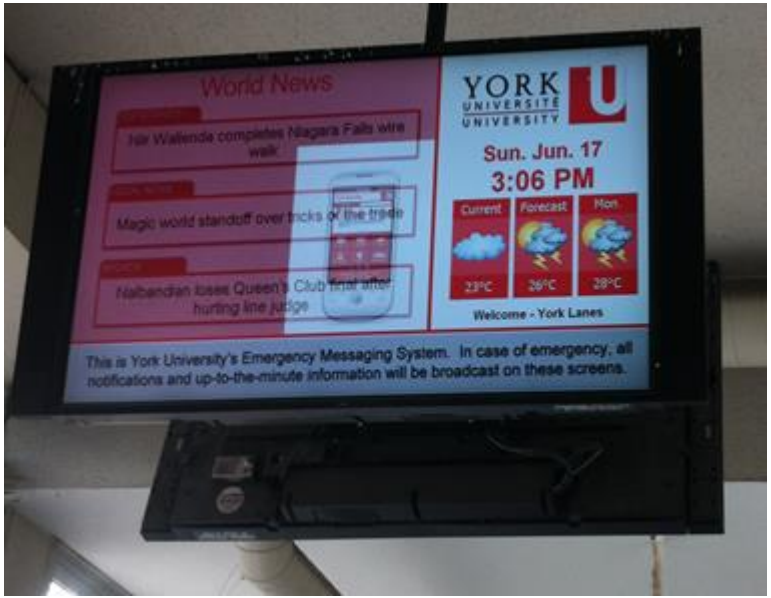
SUN, Jun

Associate Professor @ SUTD

Research Areas

- Software Engineering: How to engineer correct and reliable software?
- Cyber-Security: How to engineer secure software-based systems?
- Formal Methods: How to mathematically show that a piece of software is correct?

http://people.sutd.edu.sg/~sunjun/



The Challenge

How do we make sure Cyber-Physical Systems (CPS) like SWaT are safe and secure?

The Problems

The Attestation Problem

How to make sure that the program in the PLCs of CPS are not tampered?

The Testing Problem

How to test the control programs in PLCs to identify safety and security problems?

The Attestation Problem

Hardware-based Attestation

Execute PLC programs with specially designed hardware.

No such hardware in existing PLCs

Software-based Attestation

Compute a hashcode of the entire memory at runtime and compare it with a predicted one in the controller room.

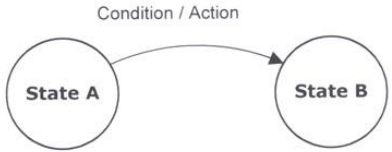
Existing PLCs do not allow direct memory access.

Physical Attestation

Check whether a system behaves as expected according to a model or not.

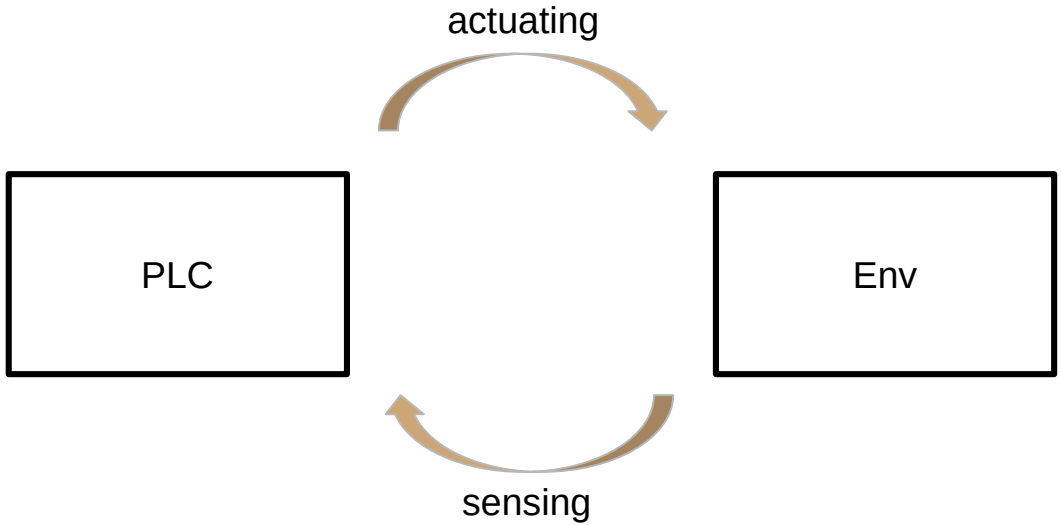
System

=?



How do we obtain a model then?

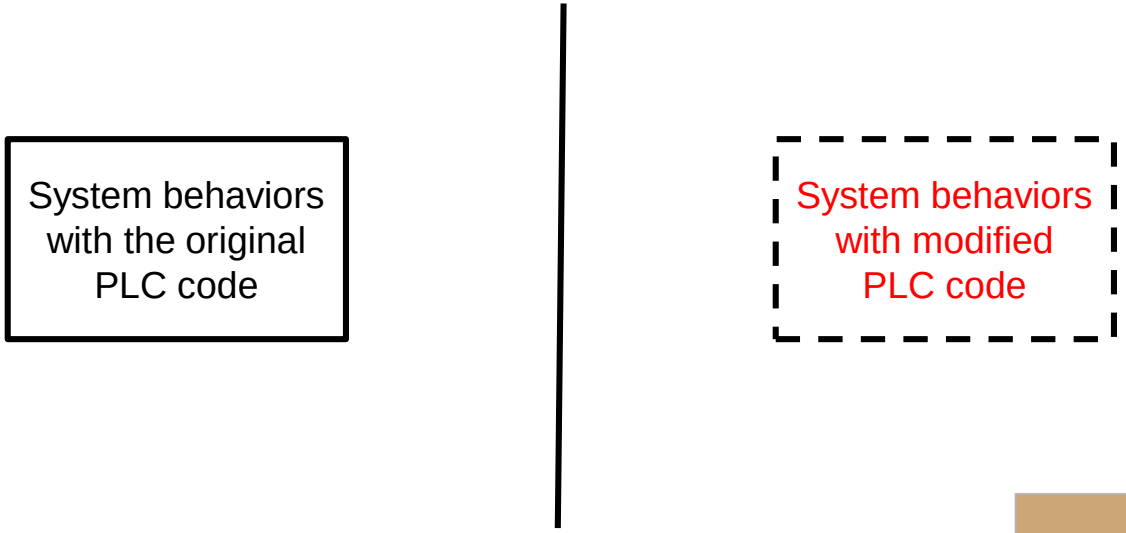
Modeling CPS



PLC code is easy to model

Env is almost impossible to model

Machine Learning



Code Mutation

Apply code mutation techniques to generate mutated PLC codes; and run the system with the modified PLC codes to collect .

Listing 1
SNIPPET OF UNMODIFIED CONTROL CODE FROM PLC #3

```
1 if Sec_P:
2   MI.Cy_P3.CIP_CLEANING_SEC=HMI.Cy_P3.
        CIP_CLEANING_SEC+1
3   if HMI.Cy_P3.CIP_CLEANING_SEC>HMI.
        Cy_P3.CIP_CLEANING_SEC_SP or self
        .Mid_NEXT:
4         self.Mid_NEXT=0
5         HMI.P3.State=19
6 break
```

Listing 2
A POSSIBLE MUTANT OBTAINED FROM LISTING 1

```
1 if Sec_P:
2   MI.Cy_P3.CIP_CLEANING_SEC=HMI.Cy_P3.
        CIP_CLEANING_SEC+1
3   if HMI.Cy_P3.CIP_CLEANING_SEC>HMI.
        Cy_P3.CIP_CLEANING_SEC_SP or self
        .Mid_NEXT:
4         self.Mid_NEXT=0
5         HMI.P3.State=14
6 break
```

Classification

System behaviors with the original PLC code

System behaviors with modified PLC code

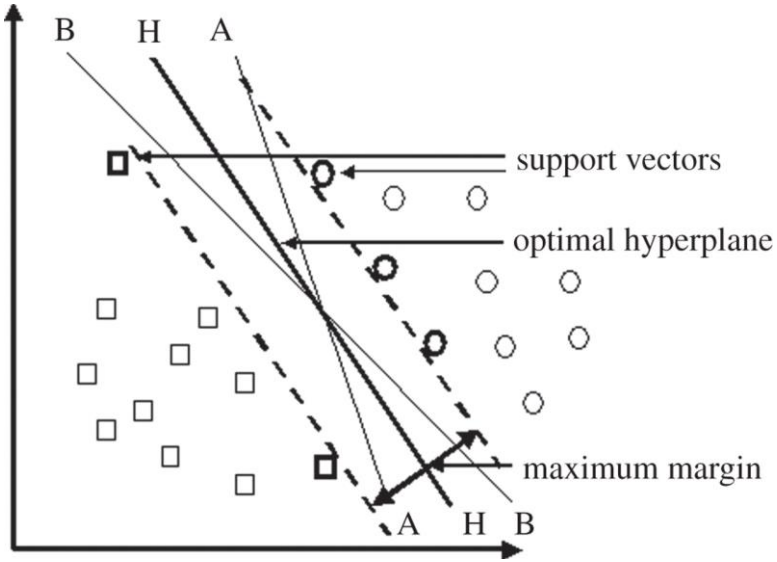
How do obtain the classifier between the two sets of behaviors?

Support Vector Machine

Automatic

Linear or polynomial or arbitrary classifier

Relatively scalable



Correctness

How do we validate the learned classifier is “correct”?

N-fold cross validation

Statistical model checking

Experiments on SWaT

What kind of classifiers shall we use?

type	accuracy	cross-validation accuracy	sensitivity	specificity
SVM-linear	63.34%	64.12%	66.44%	60.23%
SVM-polynomial	67.10%	68.32%	74.92%	51.67%
SVM-RBF	91.05%	90.99%	99.28%	82.82%

Experiments on SWaT

How many mutants are enough?

#mutants	#effective mutants	accuracy	cross-validation accuracy
300	23	63.01%	81.91%
400	31	83.01%	89.01%
500	62	90.07%	89.08%
600	76	91.04%	90.89%
700	91	91.05%	90.99%

Experiments on SWaT

Are the learned model good for physical attestation?

attack stage	# effective mutants	# detected	accuracy (detected)	accuracy (all)
PLC 1	8	5	99.82%	71.54%
PLC 3	20	17	99.89%	92.12%
PLC 4	4	4	99.29%	99.29%
PLC 5	5	3	99.43%	81.20%
PLC 6	3	3	99.87%	99.87%
summary	40	32	99.84%	88.20%

#detected: negative with accuracy >= 85%

Experiments on SWaT

Are the learned model good for detecting other attacks?

attack #	attack point	start state	attack	detected	accuracy
1	MV101	MV101 is closed	Open MV101	yes	89.67%
2	P102	P101 is on whereas P102 is off	Turn on P102	yes	90.01%
3	LIT101	Water level between L and H	Increase by 1mm every second	eventually	63.11%
4	LIT301	Water level between L and H	Water level increased above HH	yes	99.86%
5	MV504	MV504 is closed	Open MV504	yes	92.11%
6	MV304	MV304 is open	Close MV304	yes	88.01%
7	LIT301	Water level between L and H	Decrease water level by 1mm each second	eventually	56.97%
8	MV304	MV304 is open	Close MV304	yes	90.16%
9	LIT401	Water level between L and H	Set LIT401 to less than L	yes	89.36%
10	LIT301	Water level between L and H	Set LIT301 to above HH	yes	99.07%
11	LIT101	Water level between L and H	Set LIT101 to above H	yes	91.12%
12	P101	P101 is on	Turn P101 off	yes	92.06%
13	P101; P102	P101 is on; P102 is off	Turn P101 off; keep P102 off	yes	91.62%
14	P302	P302 is on	Close P302	yes	90.91%
15	LIT101	Water level between L and H	Set LIT101 to less than LL	yes	89.37%

Summary

The Attestation Problem

How to make sure that the program in the PLCs of CPS are not tampered?

Answer

Yuqi Chen, Christ Poskitt, and Jun Sun: “Learning from Mutants: Using Code Mutation to Learn and Monitor Invariants of a Cyber-Physical System”, *IEEE S&P 2018*.

Ongoing Effort

How to test the control programs in PLCs to identify safety and security problems?

How if the CPS (or software systems in general) are smart (evolves over time through machine learning)?

How if an attacker is smart (evolves over time through learning)?