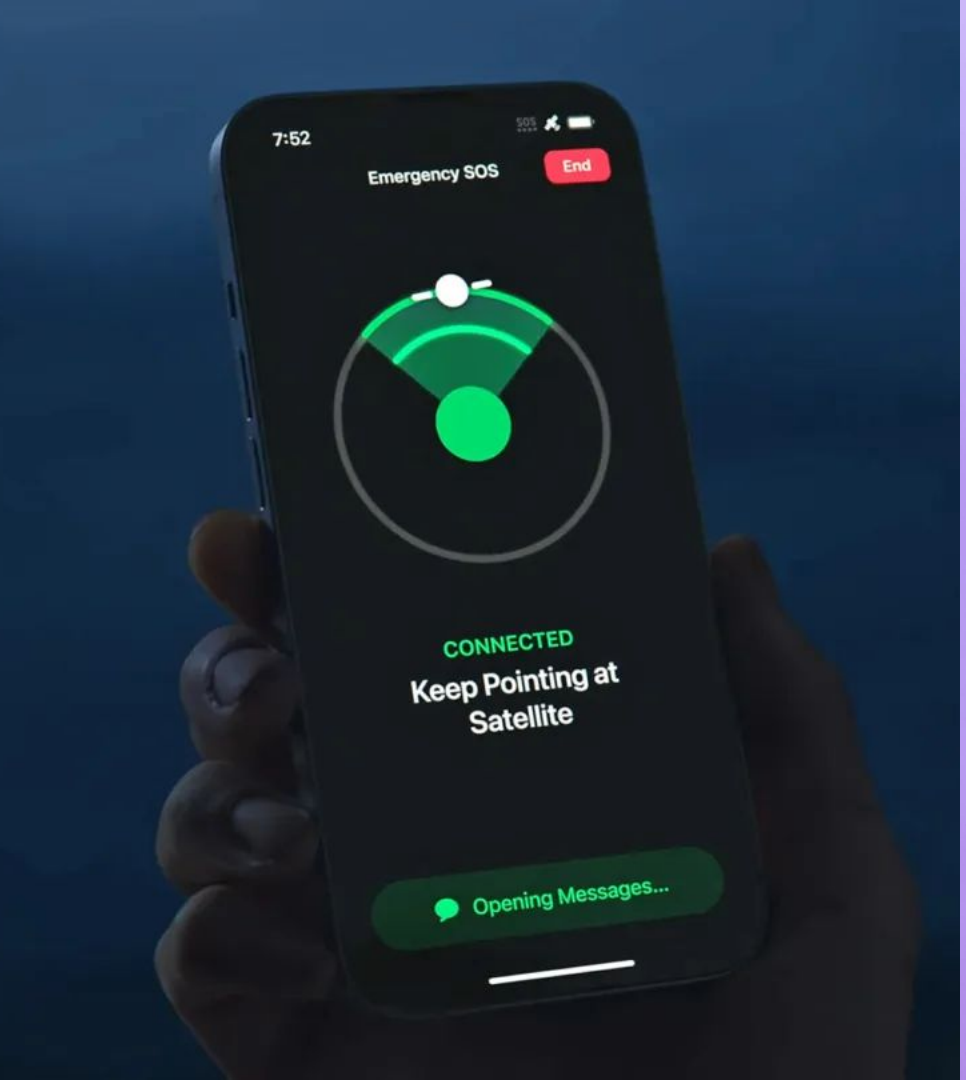
Securing the Next Generation of Cyber-Physical Systems

Efrén López-Morales
PhD Candidate at Texas A&M University-Corpus Christi


7:52
Emergency SOS
End
CONNECTED
Keep Pointing at Satellite
Opening Messages...


DARKREADING
NEWSLETTER SIGN-UP
Cybersecurity Topics
World
The Edge
DR Technology
Events
Resources
Improved, Stuxnet-Like PLC Malware Aims to Disrupt Critical Infrastructure
A newly developed PLC malware does not require physical access to target an ICS environment, is mostly platform neutral, and is more resilient than traditional malware aimed at critical infrastructure.

DARKREADING

NEWSLETTER SIGN-UP

Cybersecurity Topics | World | The Edge | DR Technology | Events | Resources

Improved, Stuxnet-Like PLC Malware Aims to Disrupt Critical Infrastructure

A newly developed PLC malware does not require physical access to target an ICS environment, is mostly platform neutral, and is more resilient than traditional malware aimed at critical infrastructure.

'Crash Override': The Malware That Took Down a Power Grid

In Ukraine, researchers have found the first real-world malware that attacks physical infrastructure since Stuxnet.

DARKREADING

NEWSLETTER SIGN-UP

Cybersecurity Topics | World | The Edge | DR Technology | Events | Resources

Improved, Stuxnet-Like PLC Malware Aims to Disrupt Critical Infrastructure

A newly developed PLC malware does not require physical access to target an ICS environment, is mostly platform neutral, and is more resilient than traditional malware aimed at critical infrastructure.

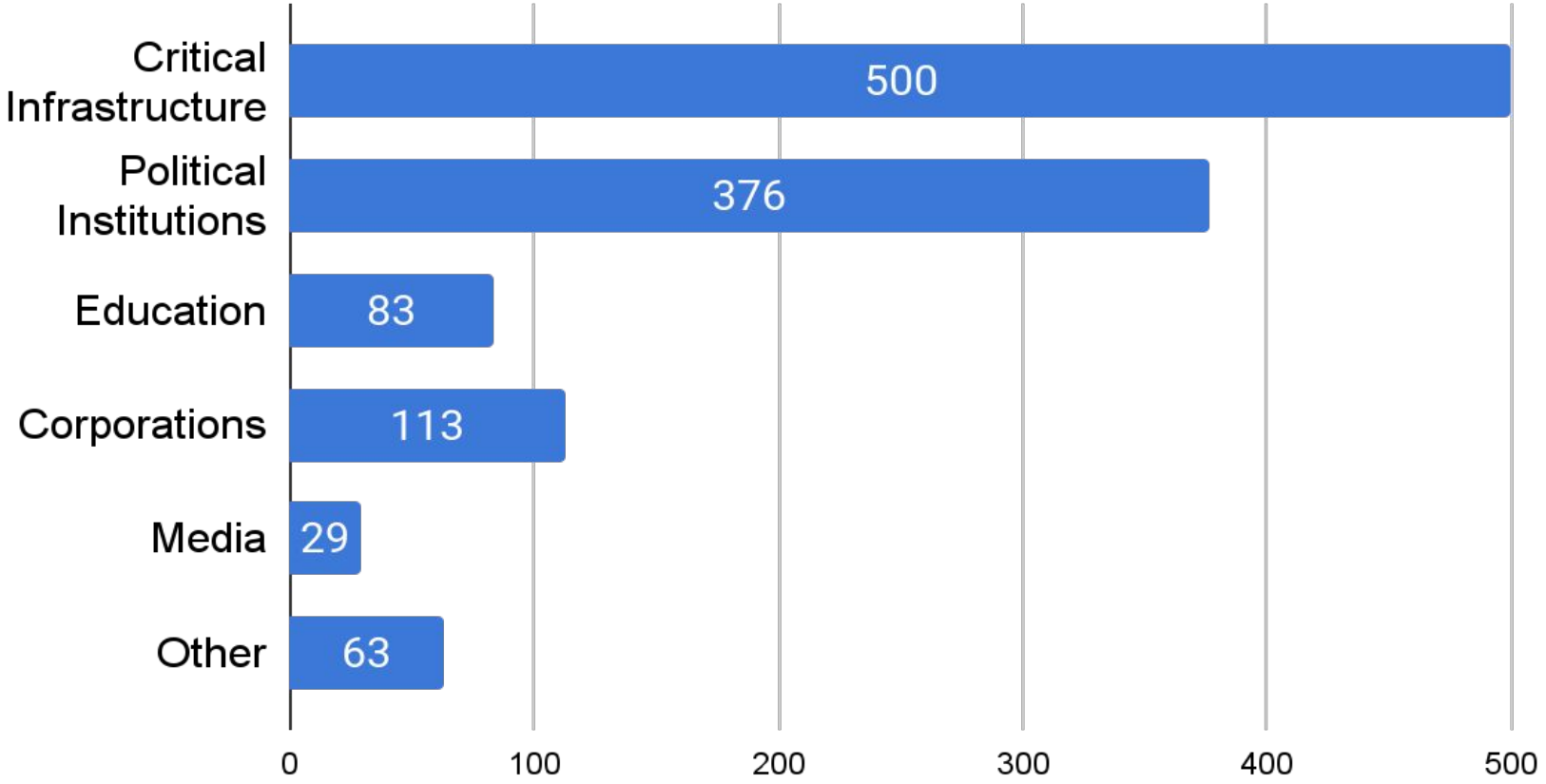
'Crash Override': The Malware That Took Down a Power Grid

In Ukraine, researchers have found the first real-world malware that attacks physical infrastructure since Stuxnet.

The New York Times

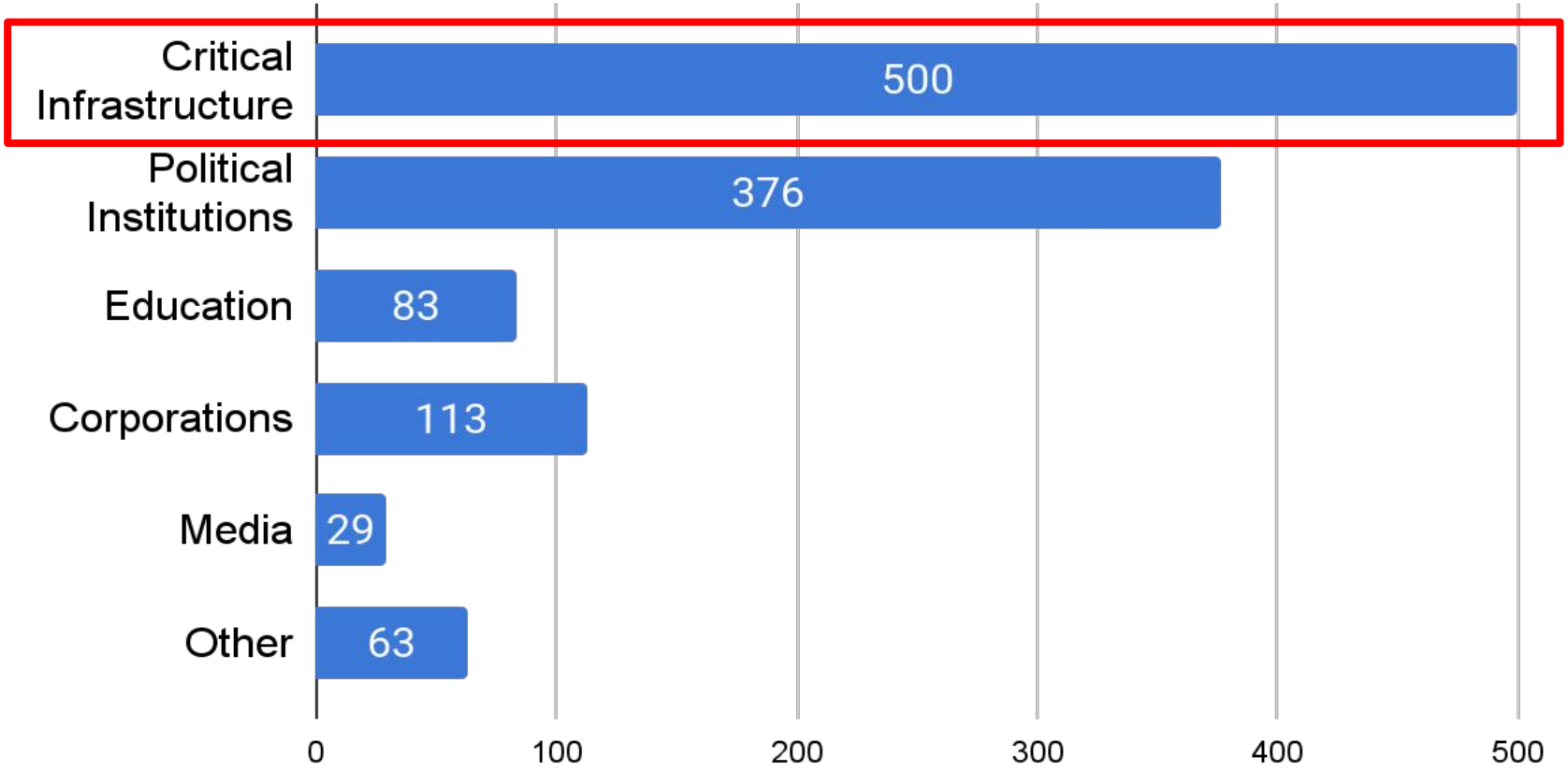
Cyberattack Forces a Shutdown of a Top U.S. Pipeline

The sectors most targeted by cybercrime (2023)



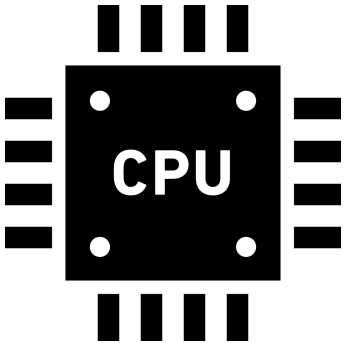
Source: European Repository of Cyber Incidents

The sectors most targeted by cybercrime (2023)

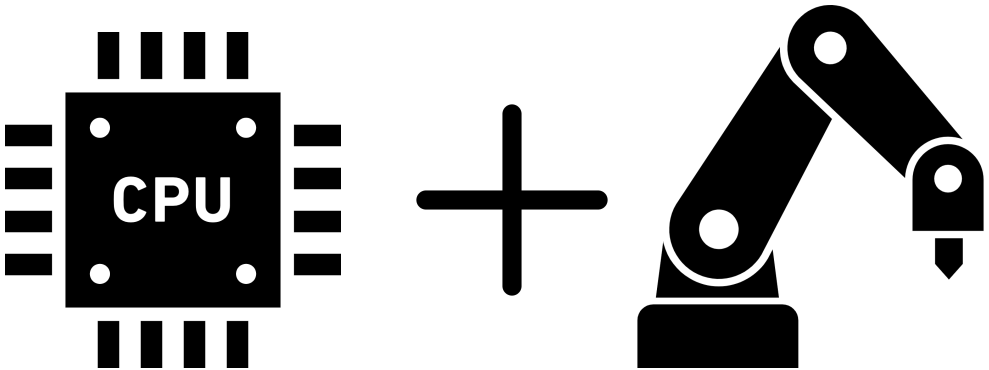


Source: European Repository of Cyber Incidents

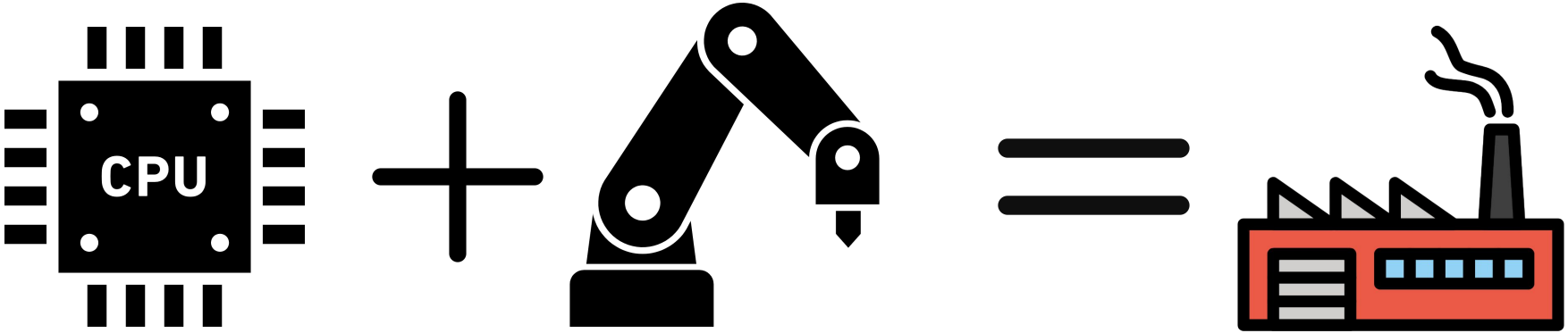
What are Cyber-Physical Systems (CPS)?



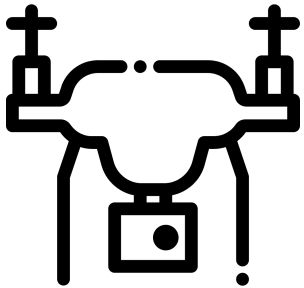
What are Cyber-Physical Systems (CPS)?



What are Cyber-Physical Systems (CPS)?

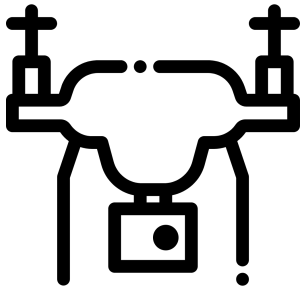


What are the types of CPS?

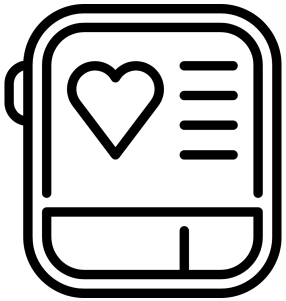


Drones

What are the types of CPS?

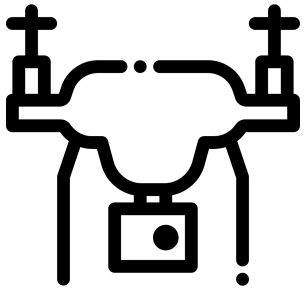


Drones

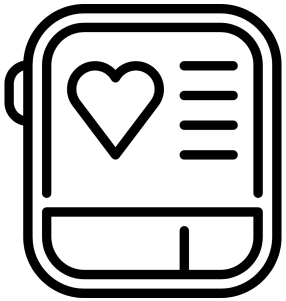


Healthcare

What are the types of CPS?



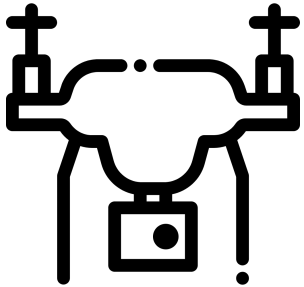
Drones



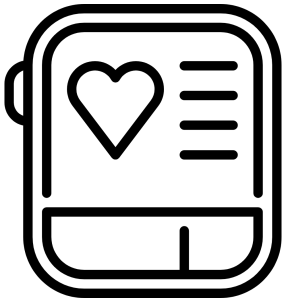
Healthcare

Industrial Control Systems

What are the types of CPS?



Drones

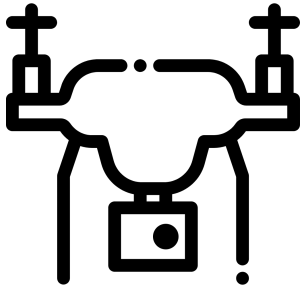


Healthcare

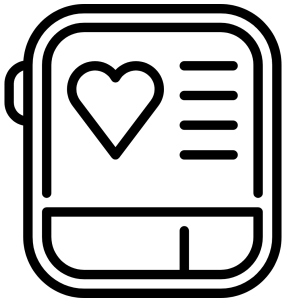
Industrial Control Systems

Connected Vehicles

What are the types of CPS?



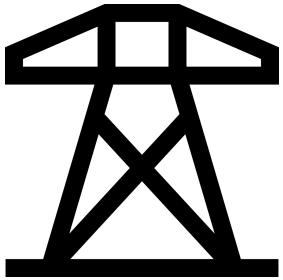
Drones



Healthcare

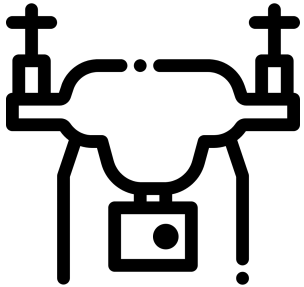
Industrial Control Systems

Connected Vehicles

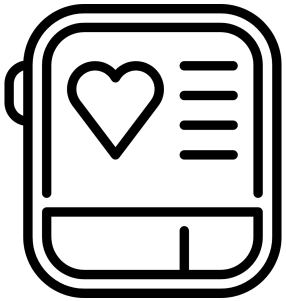


Smart Grid

What are the types of CPS?



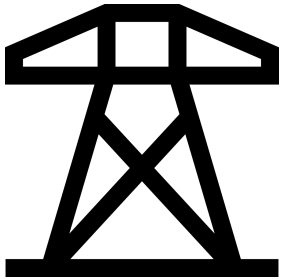
Drones



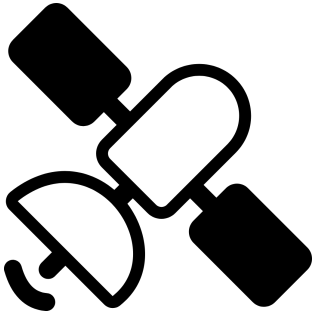
Healthcare

Industrial Control Systems

Connected Vehicles

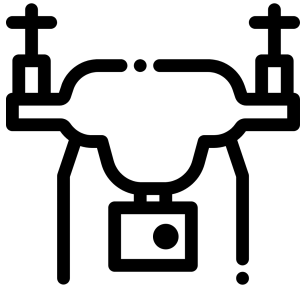


Smart Grid

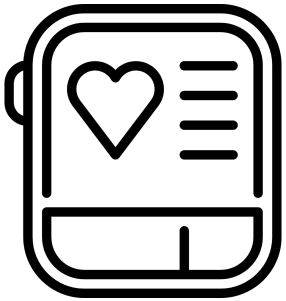


Space Systems

What are the types of CPS?



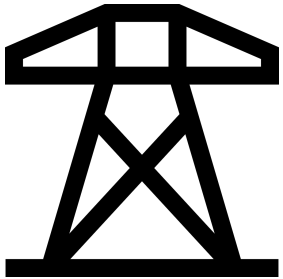
Drones



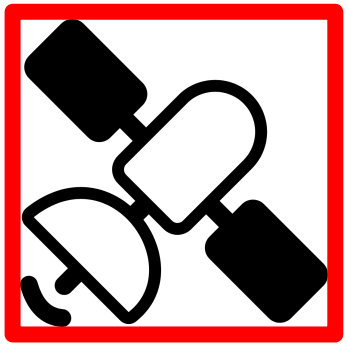
Healthcare

Industrial Control Systems

Connected Vehicles



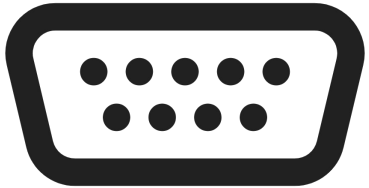
Smart Grid



Space Systems

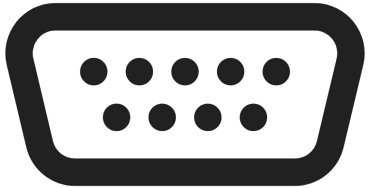
Legacy Cyber-Physical Systems

Legacy Cyber-Physical Systems

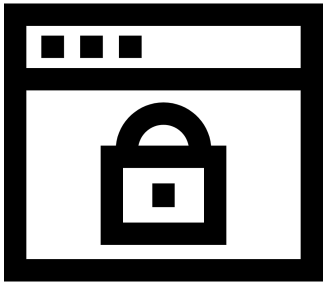


Analog Networks

Legacy Cyber-Physical Systems

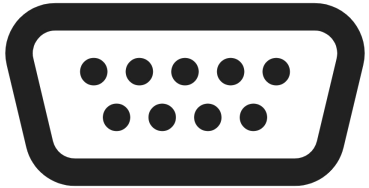


Analog Networks

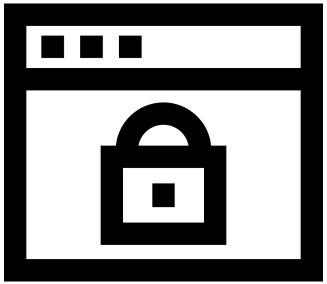


Proprietary Software

Legacy Cyber-Physical Systems



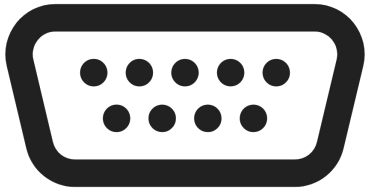
Analog Networks



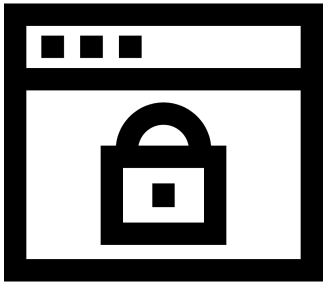
Proprietary Software

Limited Connectivity

Legacy Cyber-Physical Systems

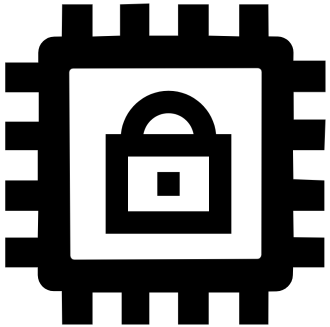


Analog Networks



Proprietary Software

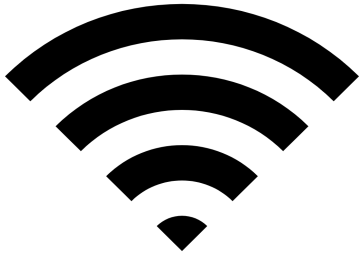
Limited Connectivity



Proprietary Hardware

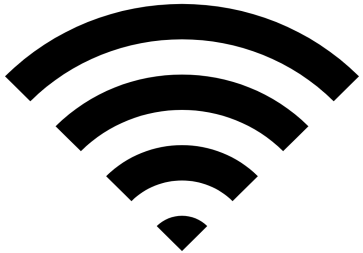
Next Generation of Cyber-Physical Systems

Next Generation of Cyber-Physical Systems

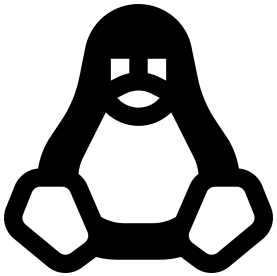


Digital Networks

Next Generation of Cyber-Physical Systems

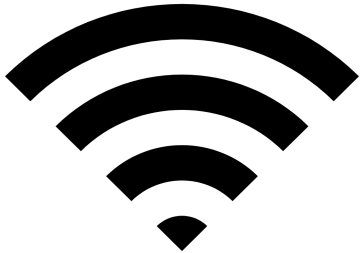


Digital Networks

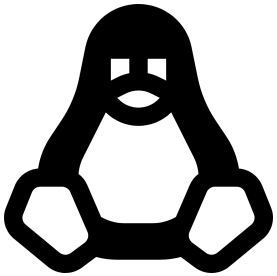


Open Source Software

Next Generation of Cyber-Physical Systems



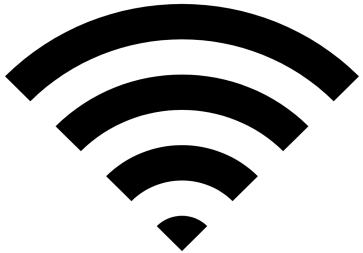
Digital Networks



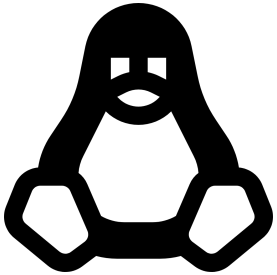
Open Source Software

IoT-Ready

Next Generation of Cyber-Physical Systems

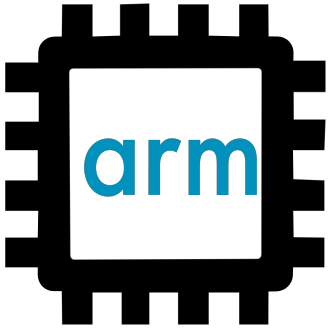


Digital Networks



Open Source Software

IoT-Ready

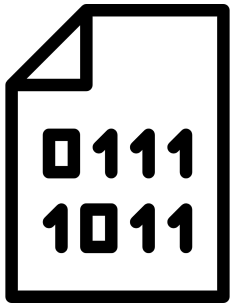


Open Architecture Hardware

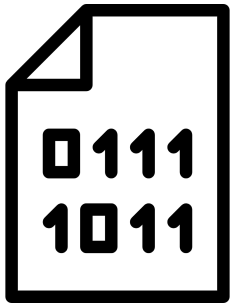
Research Gap in the Cybersecurity of Next Gen CPS

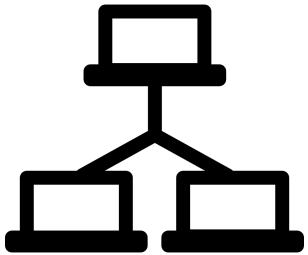
Research Gap in the Cybersecurity of Next Gen CPS

Research Gap in the Cybersecurity of Next Gen CPS

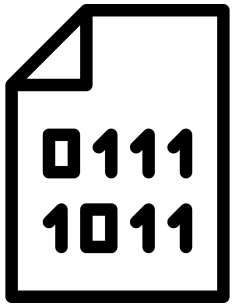


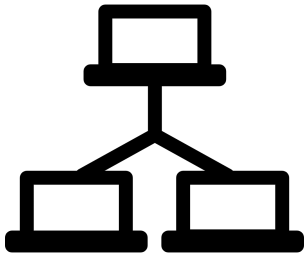
Research Gap in the Cybersecurity of Next Gen CPS

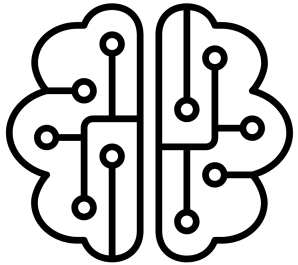




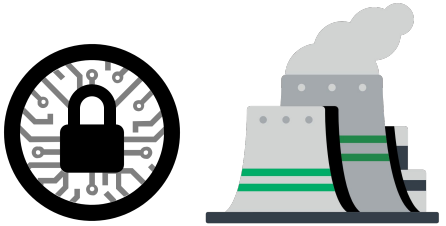
Research Gap in the Cybersecurity of Next Gen CPS





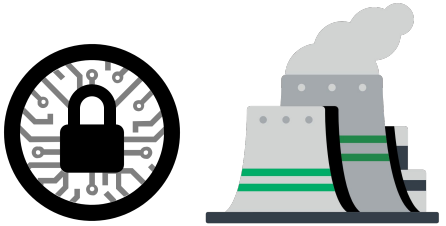


My Research



Develop novel cybersecurity mechanisms to address critical security gaps in next-generation cyber-physical systems.

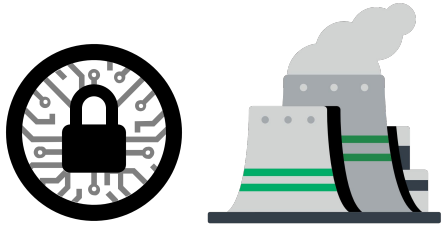
My Research



Develop novel cybersecurity mechanisms to address critical security gaps in next-generation cyber-physical systems.

- Develop end-to-end software solutions to protect critical infrastructure

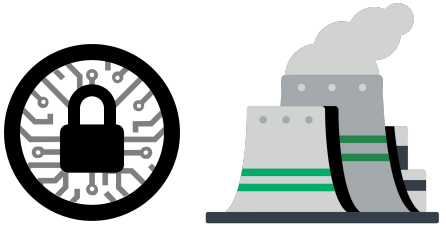
My Research



Develop novel cybersecurity mechanisms to address critical security gaps in next-generation cyber-physical systems.

- Develop end-to-end software solutions to protect critical infrastructure
- Design and conduct experiments involving both systems and human factors

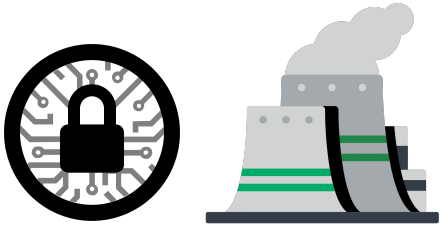
My Research



Develop novel cybersecurity mechanisms to address critical security gaps in next-generation cyber-physical systems.

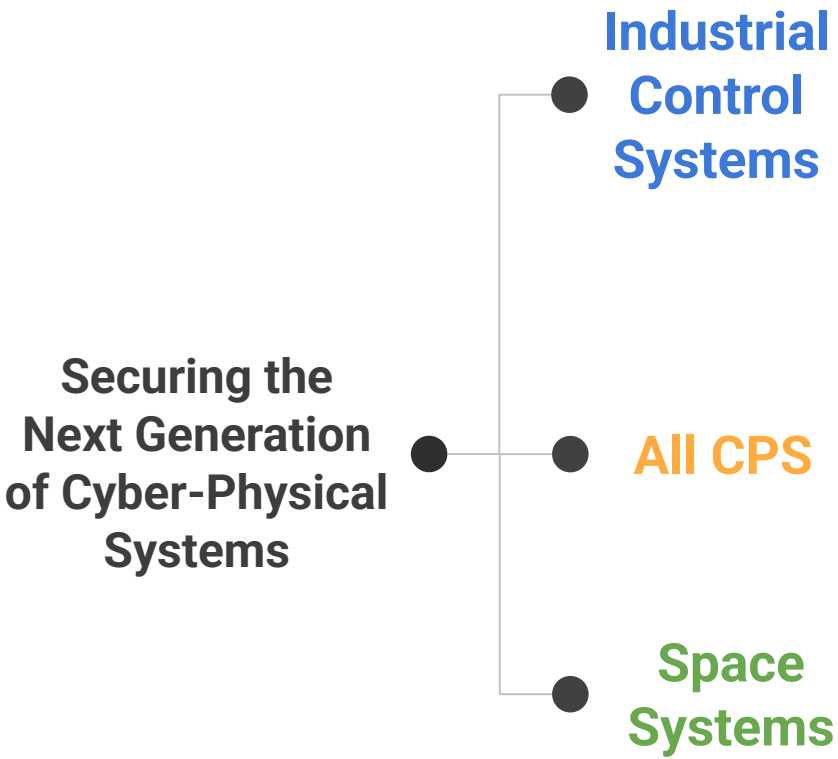
- Develop end-to-end software solutions to protect critical infrastructure
- Design and conduct experiments involving both systems and human factors
- Collaborate with international industry and academia organizations

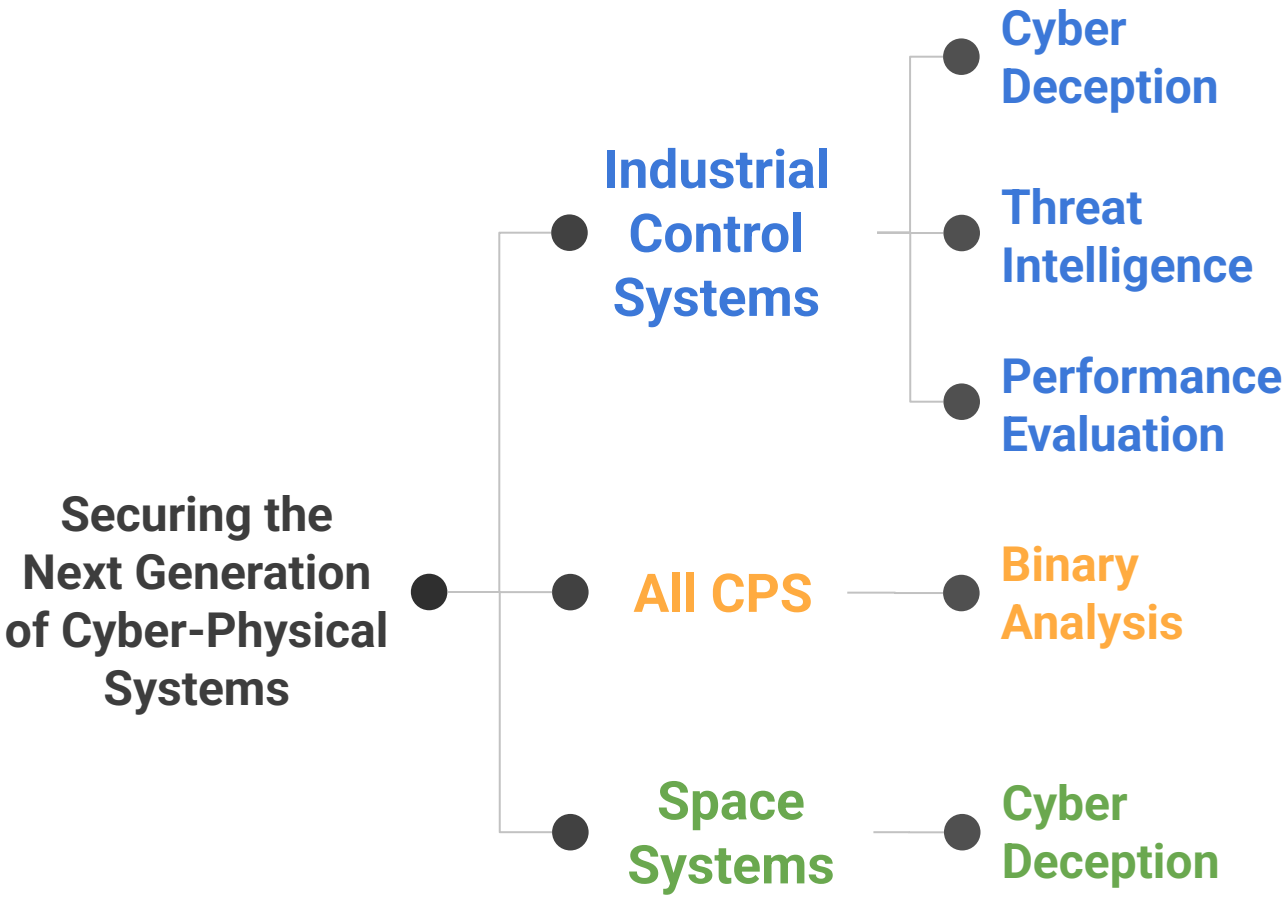
My Research

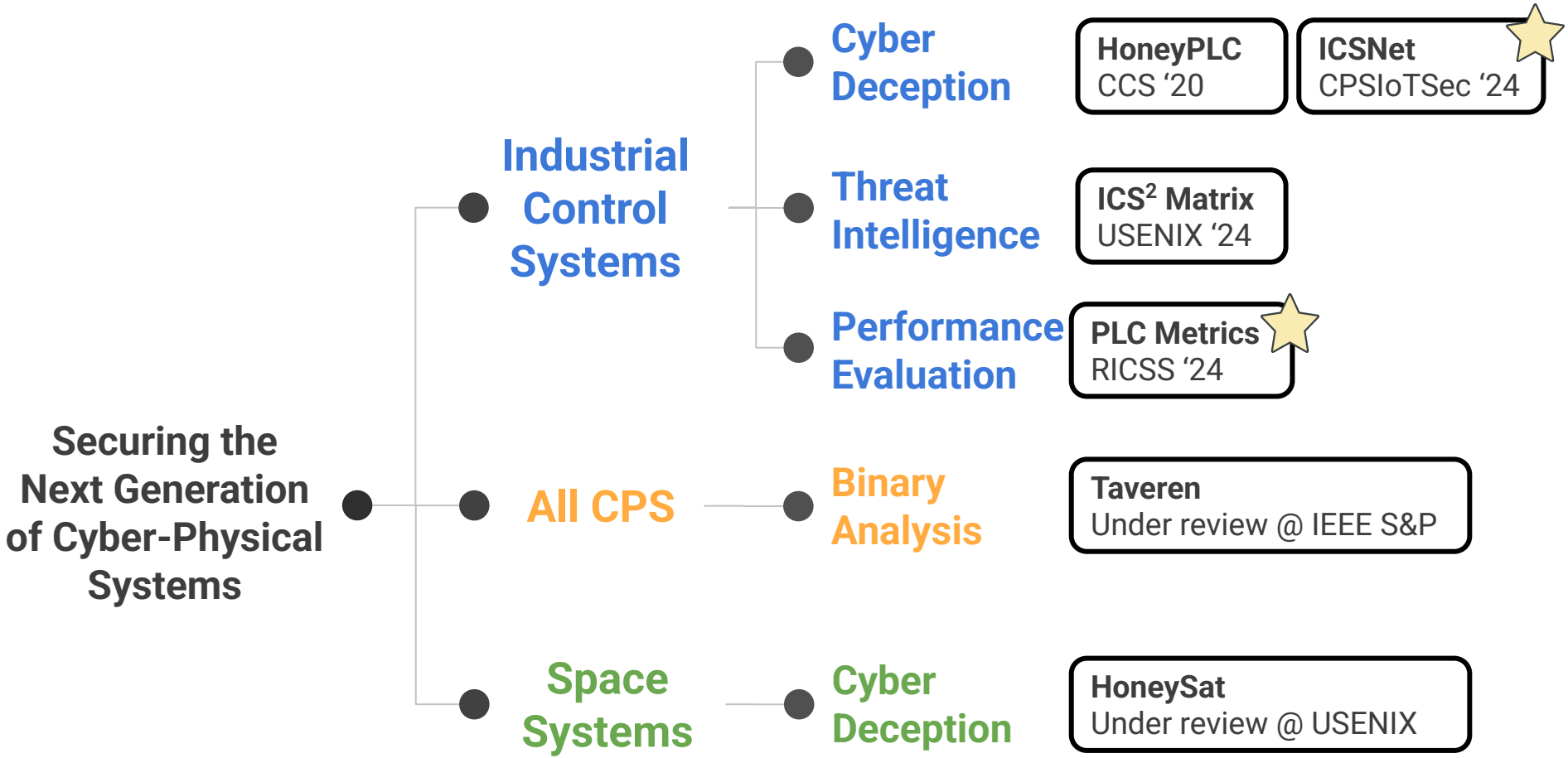


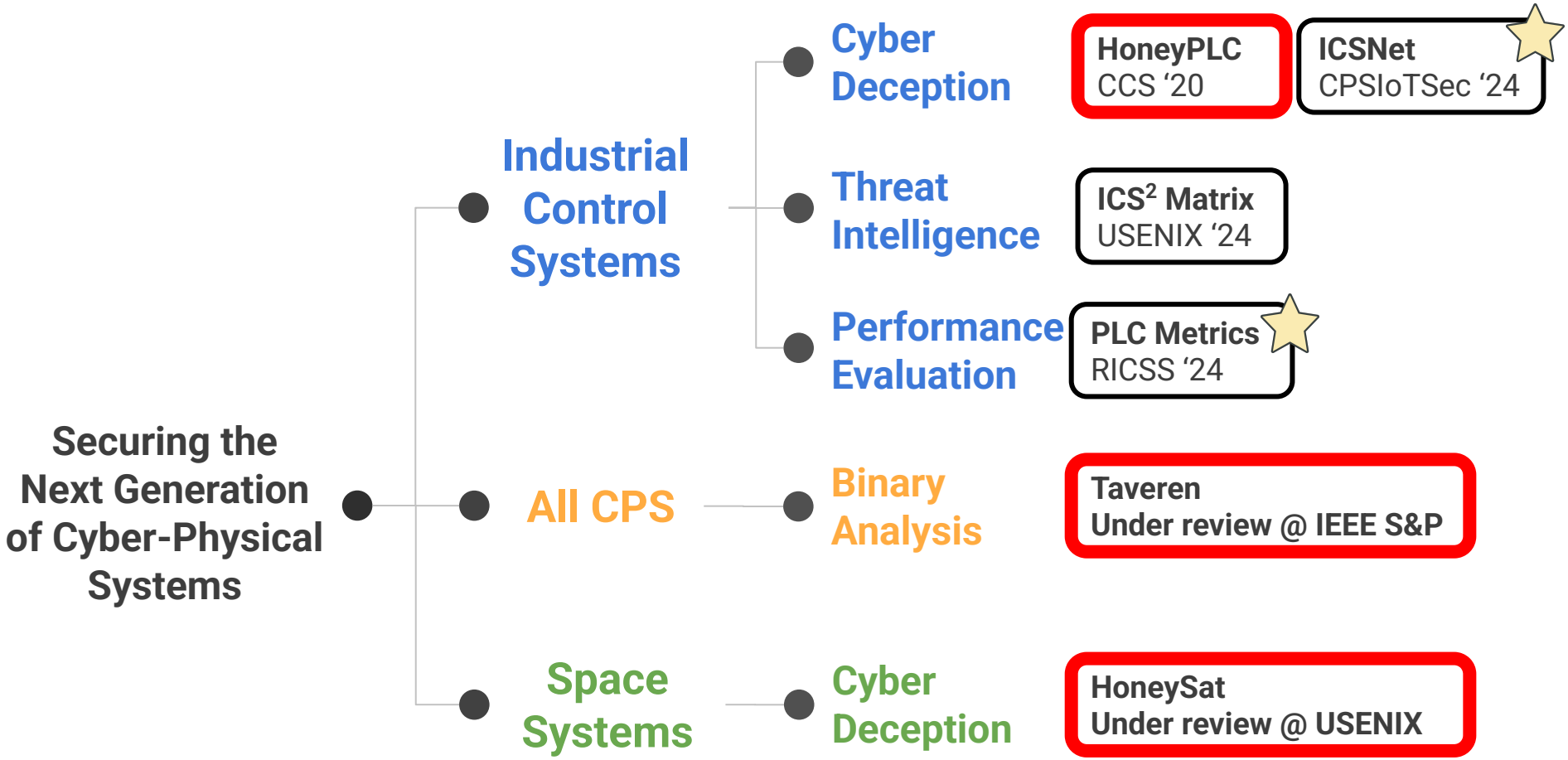
Develop novel cybersecurity mechanisms to address critical security gaps in next-generation cyber-physical systems.

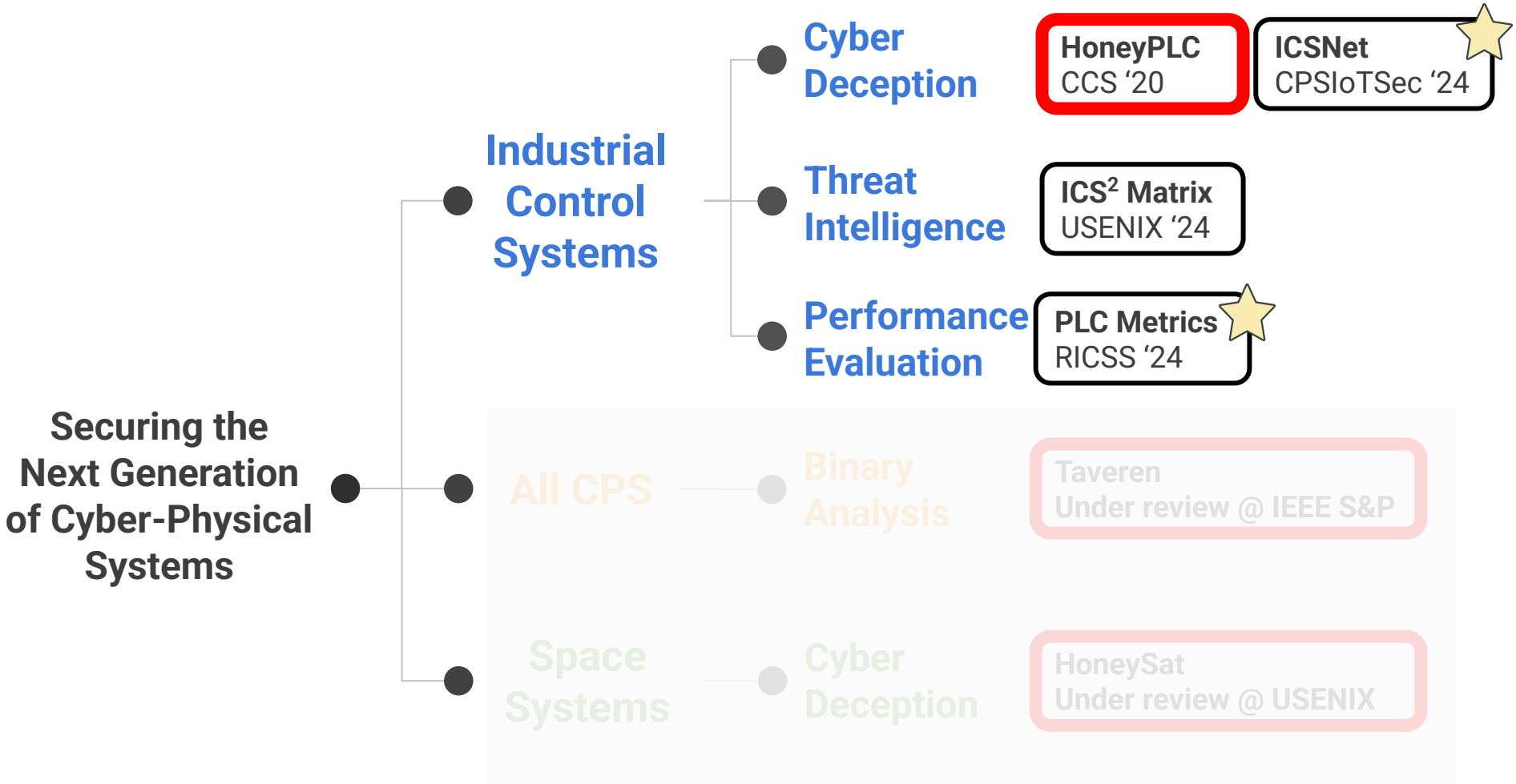
- Develop end-to-end software solutions to protect critical infrastructure
- Design and conduct experiments involving both systems and human factors
- Collaborate with international industry and academia organizations
- Deliver security solutions ready for real-world adoption, and application

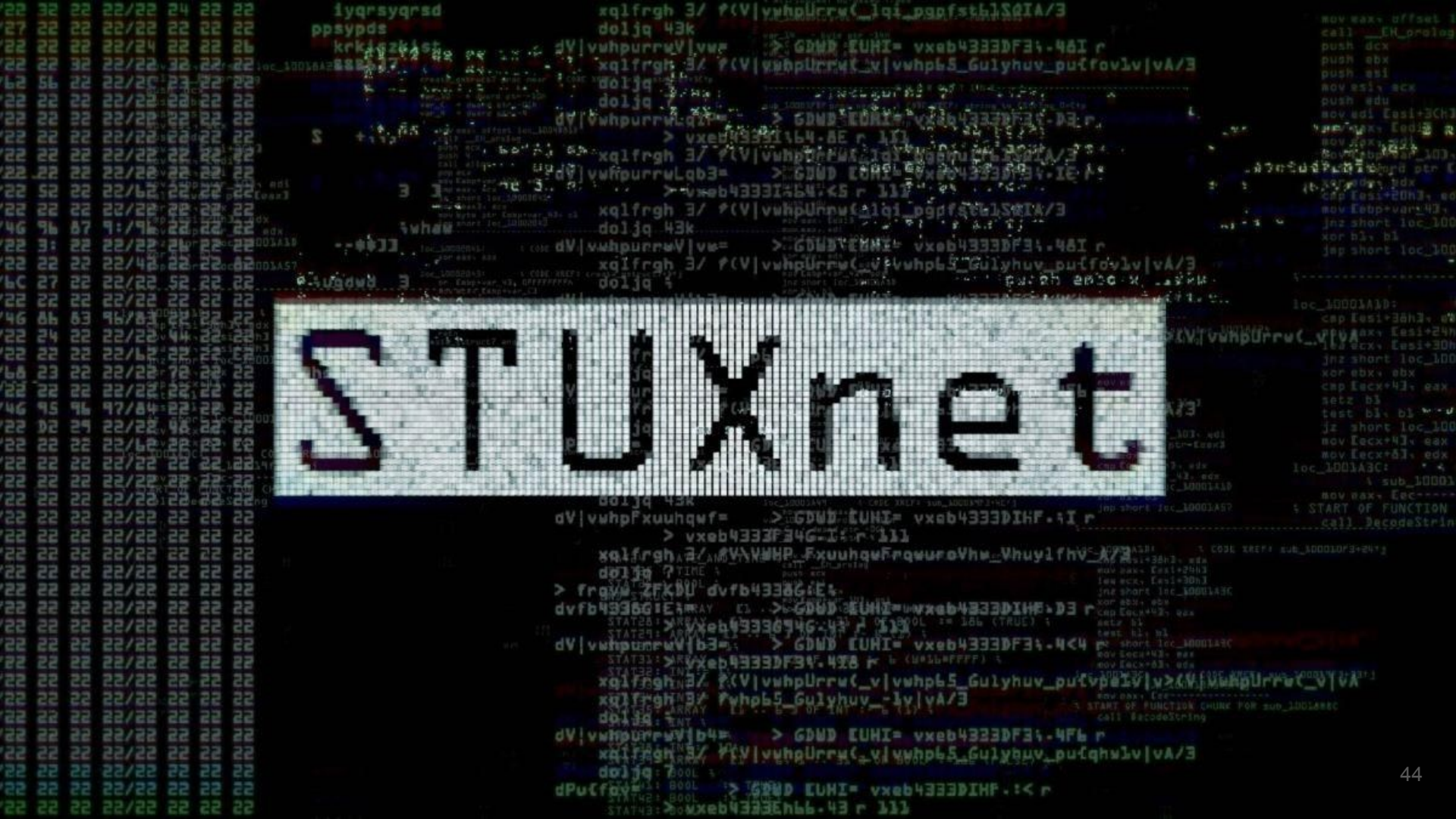

Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
All CPS
Space Systems


Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
Threat Intelligence
Performance Evaluation
All CPS
Binary Analysis
Space Systems
Cyber Deception


Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
Threat Intelligence
ICS² Matrix
USENIX '24
Performance Evaluation
PLC Metrics
RICSS '24
All CPS
Binary Analysis
Taveren
Under review @ IEEE S&P
Space Systems
Cyber Deception
HoneySat
Under review @ USENIX


Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
Threat Intelligence
ICS² Matrix
USENIX '24
Performance Evaluation
PLC Metrics
RICSS '24
All CPS
Binary Analysis
Taveren
Under review @ IEEE S&P
Space Systems
Cyber Deception
HoneySat
Under review @ USENIX


Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
Threat Intelligence
ICS² Matrix
USENIX '24
Performance Evaluation
PLC Metrics
RICSS '24
All CPS
Binary Analysis
Taveren
Under review @ IEEE S&P
Space Systems
Cyber Deception
HoneySat
Under review @ USENIX


STUXnet

Background: What is a Programmable Logic Controller?

- Vital device in ICS

Background: What is a Programmable Logic Controller?

- Vital device in ICS
- Controls physical equipment (nuclear centrifuge)

Background: What is a Programmable Logic Controller?

- Vital device in ICS
- Controls physical equipment (nuclear centrifuge)
- Multiple brands, models, architectures

Background: What is a Programmable Logic Controller?

- Vital device in ICS
- Controls physical equipment (nuclear centrifuge)
- Multiple brands, models, architectures
- Implement different network protocols such as HTTP

Background: What is a honeypot?

- Decoy computer system

Background: What is a honeypot?

- Decoy computer system
- Attracts malicious actors

Background: What is a honeypot?

- Decoy computer system
- Attracts malicious actors
- Record all interaction data

Background: What is a honeypot?

- Decoy computer system
- Attracts malicious actors
- Record all interaction data
- Analyze data to obtain knowledge

Background: What is a honeypot?

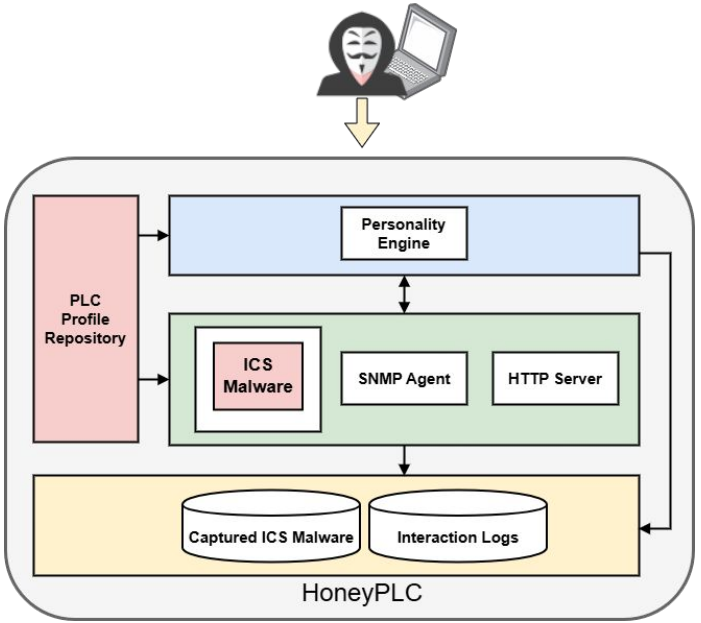
- Decoy computer system
- Attracts malicious actors
- Record all interaction data
- Analyze data to obtain knowledge
- Multiple ICS honeypots (simulate PLCs)

What is the problem?

Current ICS honeypots are limited by the quality of the data they can gather

Our solution: HoneyPLC

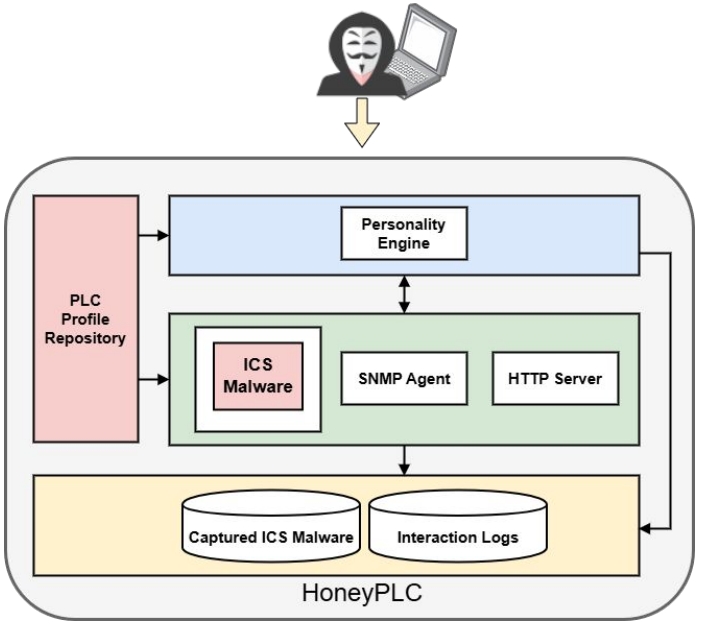
- Honeypot that simulates different PLCs



López-Morales, Efrén, et al. "Honeyplc: A next-generation honeypot for industrial control systems." Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 2020.

Our solution: HoneyPLC

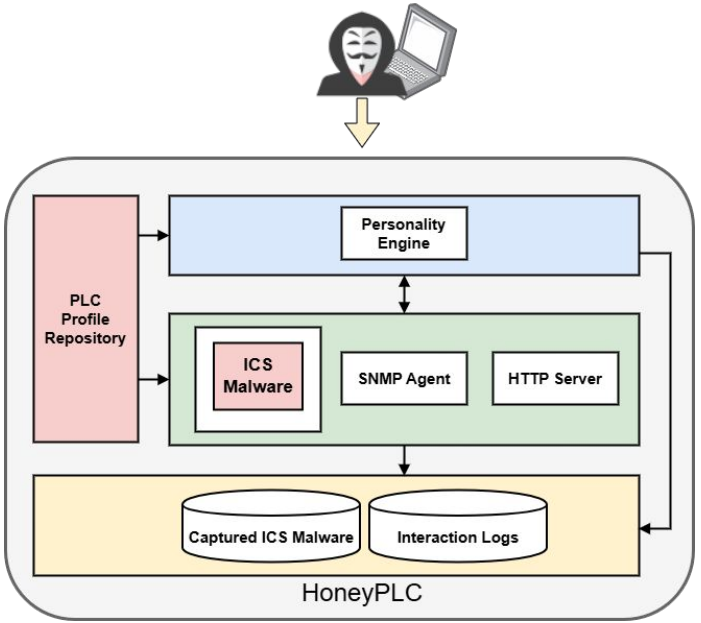
- Honeypot that simulates different PLCs
- Simulates ICS-specific network protocols



López-Morales, Efrén, et al. "Honeyplc: A next-generation honeypot for industrial control systems." Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 2020.

Our solution: HoneyPLC

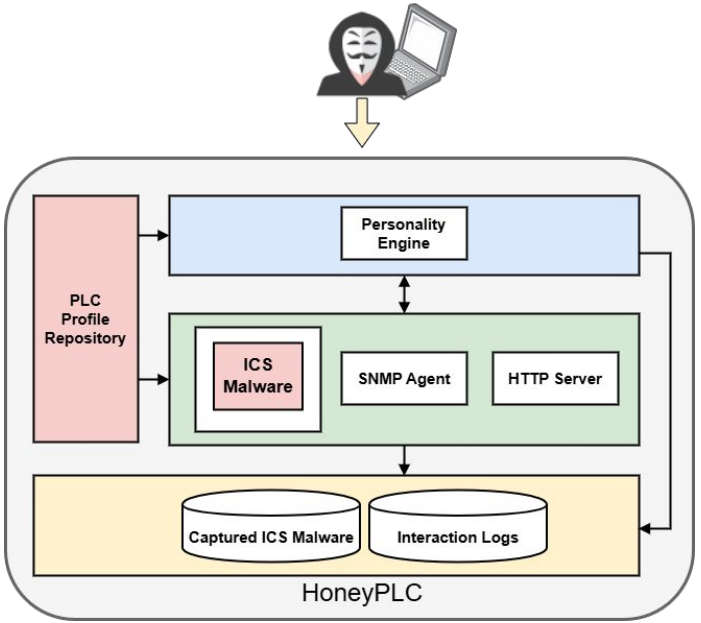
- Honeypot that simulates different PLCs
- Simulates ICS-specific network protocols
- Collects real-world ICS cyberattack data



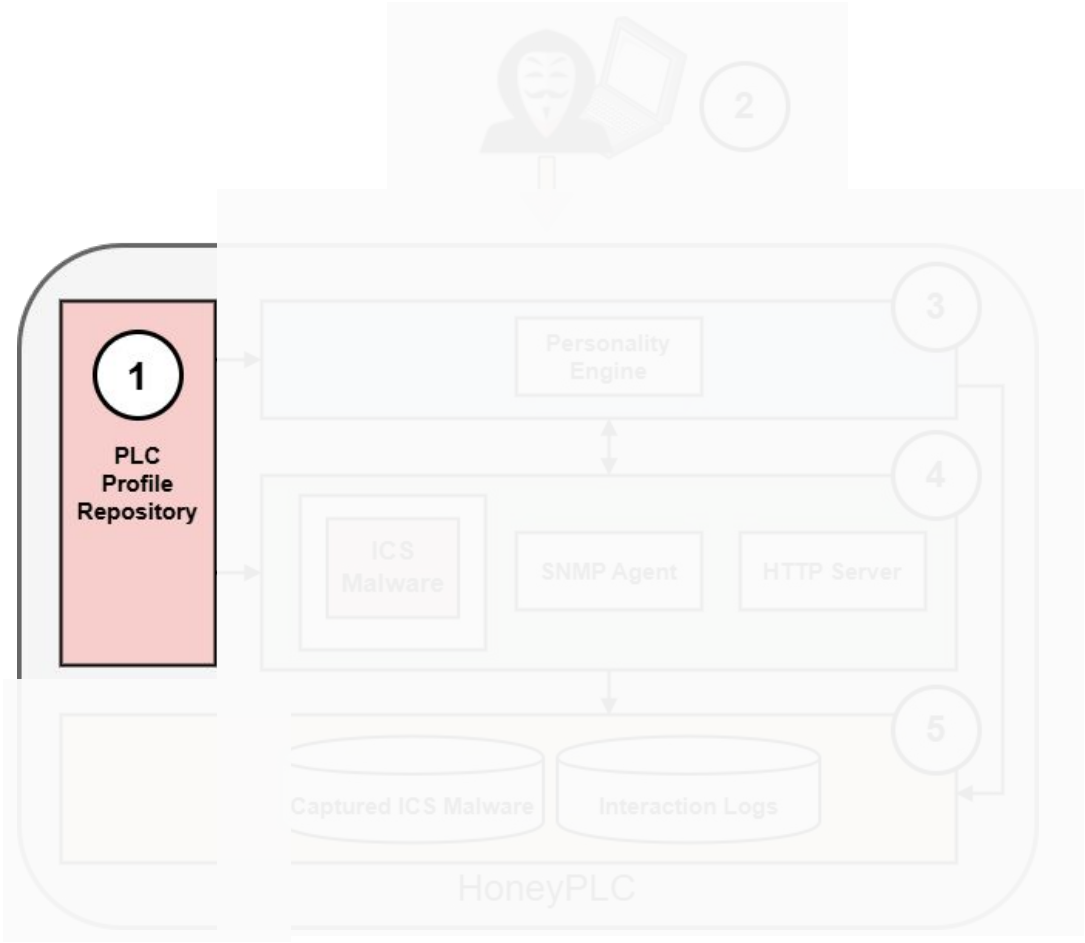
López-Morales, Efrén, et al. "Honeyplc: A next-generation honeypot for industrial control systems." Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 2020.

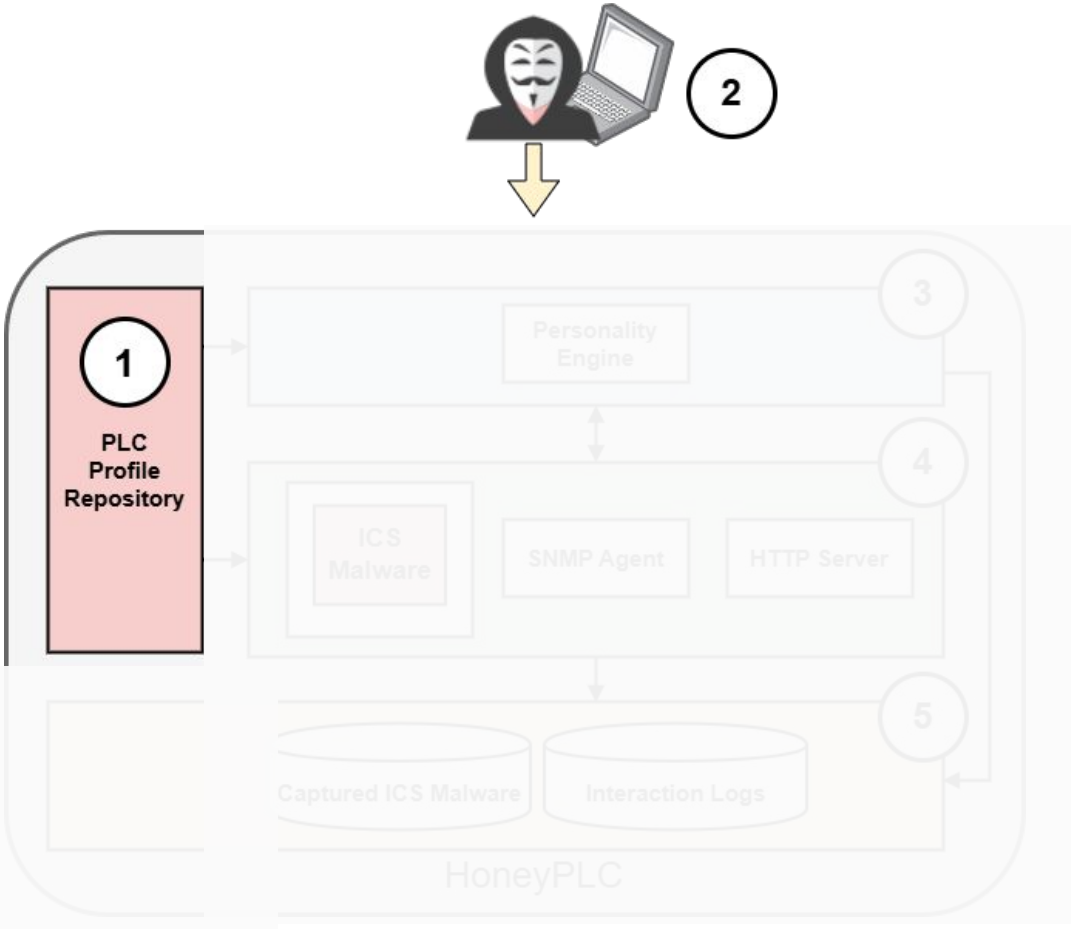
Our solution: HoneyPLC

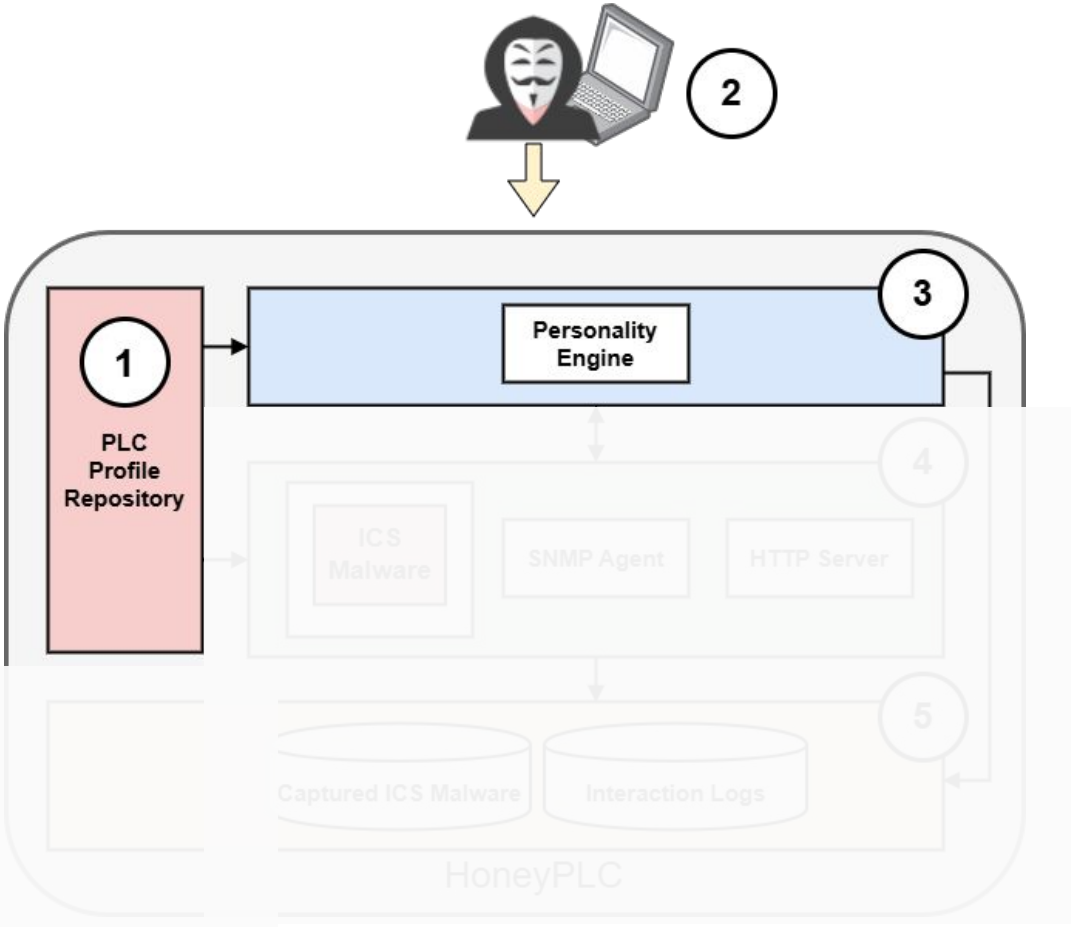
- Honeypot that simulates different PLCs
- Simulates ICS-specific network protocols
- Collects real-world ICS cyberattack data
- Collects ICS-specific malware

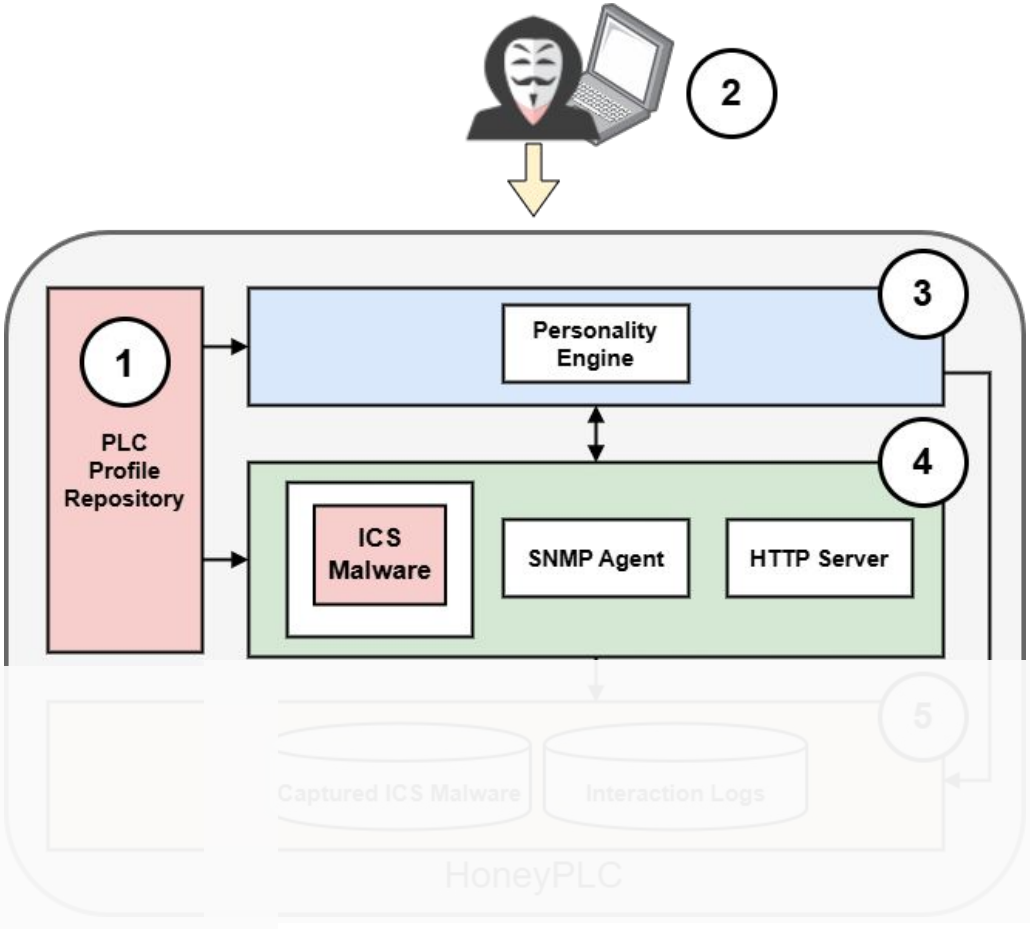


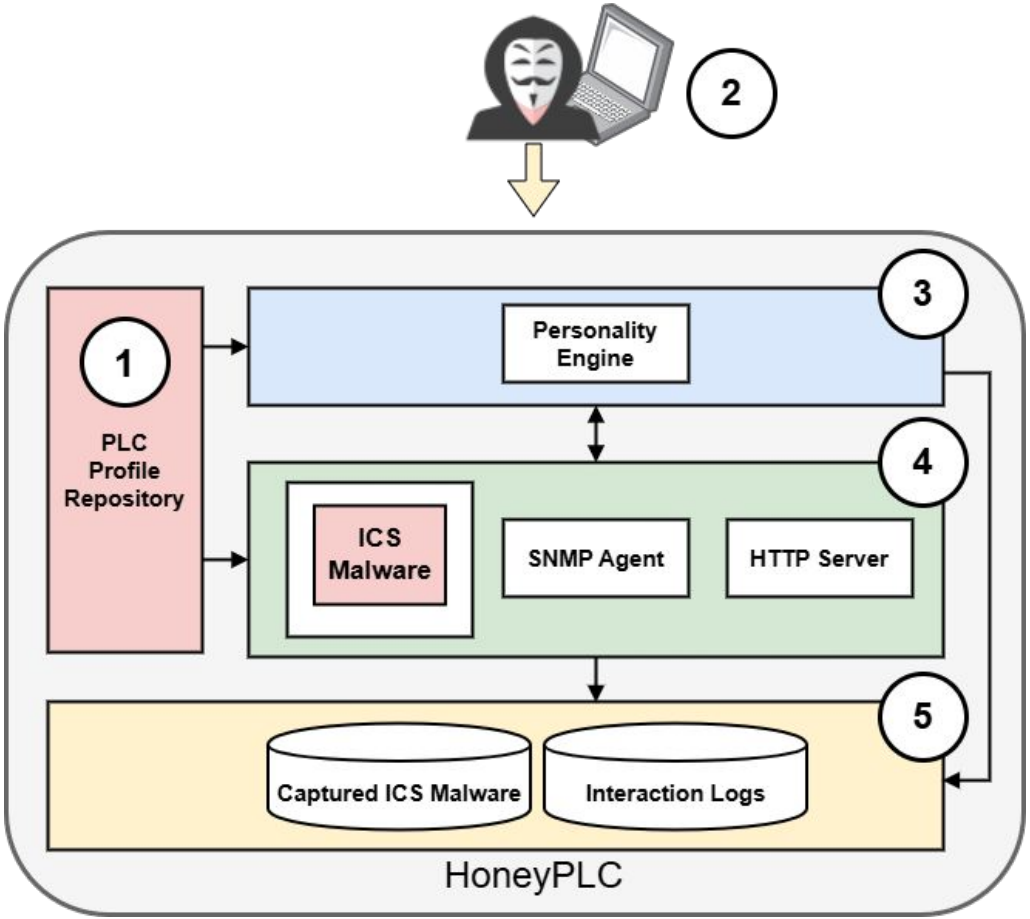
López-Morales, Efrén, et al. "Honeyplc: A next-generation honeypot for industrial control systems." Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 2020.


1
PLC
Profile
Repository
2
3
Personality
Engine
4
ICS
Malware
SNMP Agent
HTTP Server
5
Captured ICS Malware
Interaction Logs
HoneyPLC


2
1
PLC
Profile
Repository
3
Personality
Engine
4
ICS
Malware
SNMP Agent
HTTP Server
5
Captured ICS Malware
Interaction Logs
HoneyPLC

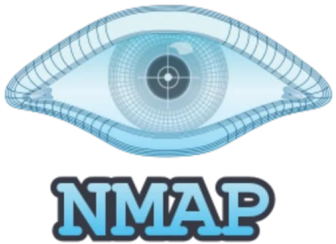

2
1
PLC
Profile
Repository
Personality
Engine
3
4
ICS
Malware
SNMP Agent
HTTP Server
5
Captured ICS Malware
Interaction Logs
HoneyPLC


2
1
PLC
Profile
Repository
3
Personality
Engine
4
ICS
Malware
SNMP Agent
HTTP Server
5
Captured ICS Malware
Interaction Logs
HoneyPLC


2
1
PLC
Profile
Repository
3
Personality
Engine
4
ICS
Malware
SNMP Agent
HTTP Server
5
Captured ICS Malware
Interaction Logs
HoneyPLC

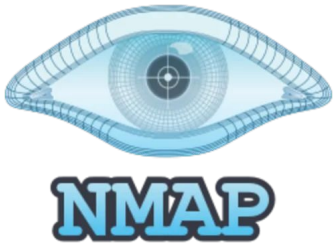
How did we evaluate HoneyPLC?

1. Well-known cybersecurity tools



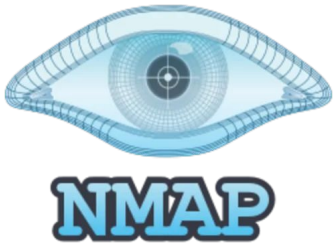
How did we evaluate HoneyPLC?

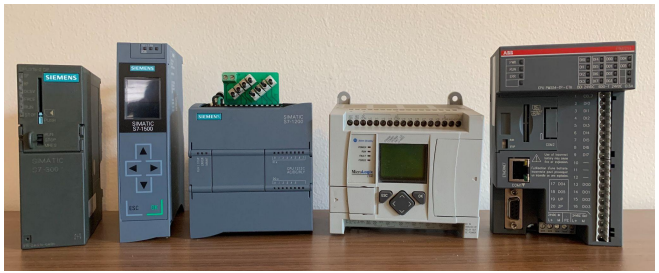
1. Well-known cybersecurity tools
2. Deployment over the Internet



How did we evaluate HoneyPLC?

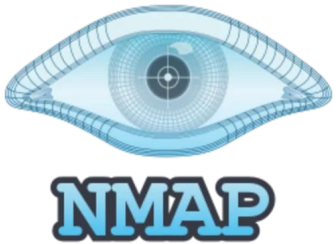
1. Well-known cybersecurity tools
2. Deployment over the Internet
3. Tested multiple PLC models

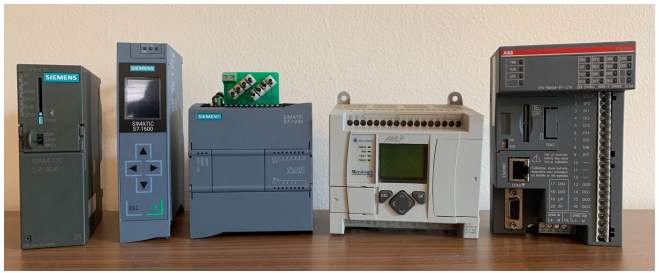




How did we evaluate HoneyPLC?

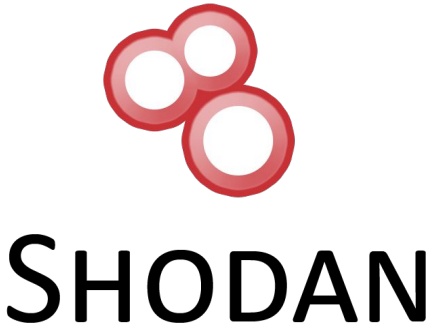
1. **Well-known cybersecurity tools**
2. **Deployment over the Internet**
3. Tested multiple PLC models





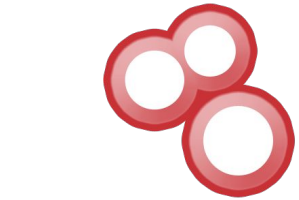
What did we find?

Security Tool
Nmap
Siemens PLC Manager
Shodan
PLCInject
PLCScan



What did we find?

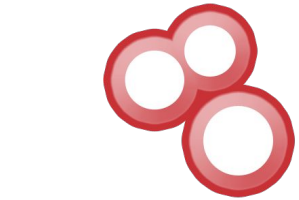
Security Tool	Type
Nmap	Industry
Siemens PLC Manager	Industry
Shodan	Industry
PLCInject	Academia
PLCScan	Academia



SHODAN

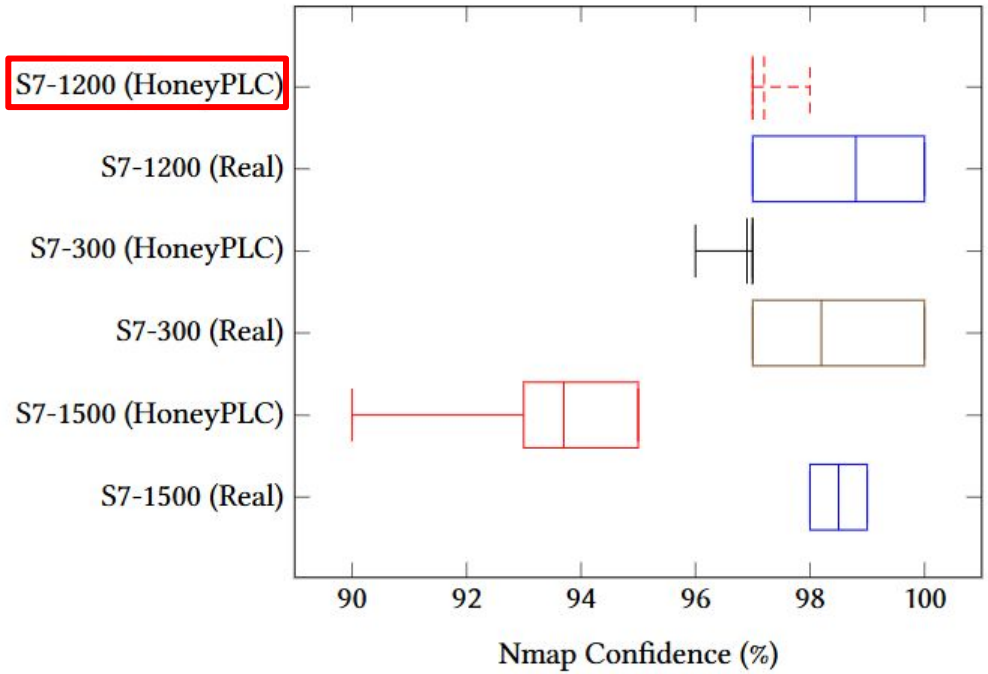
What did we find?

Security Tool	Type	Result
Nmap	Industry	✔
Siemens PLC Manager	Industry	✔
Shodan	Industry	✔
PLCInject	Academia	✔
PLCScan	Academia	✔

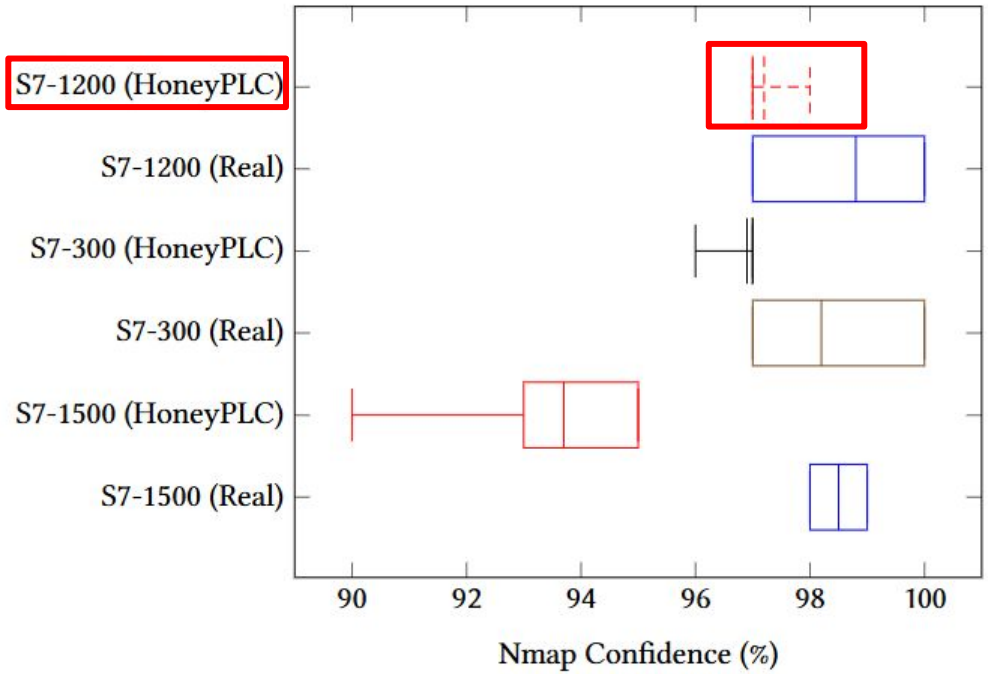


SHODAN

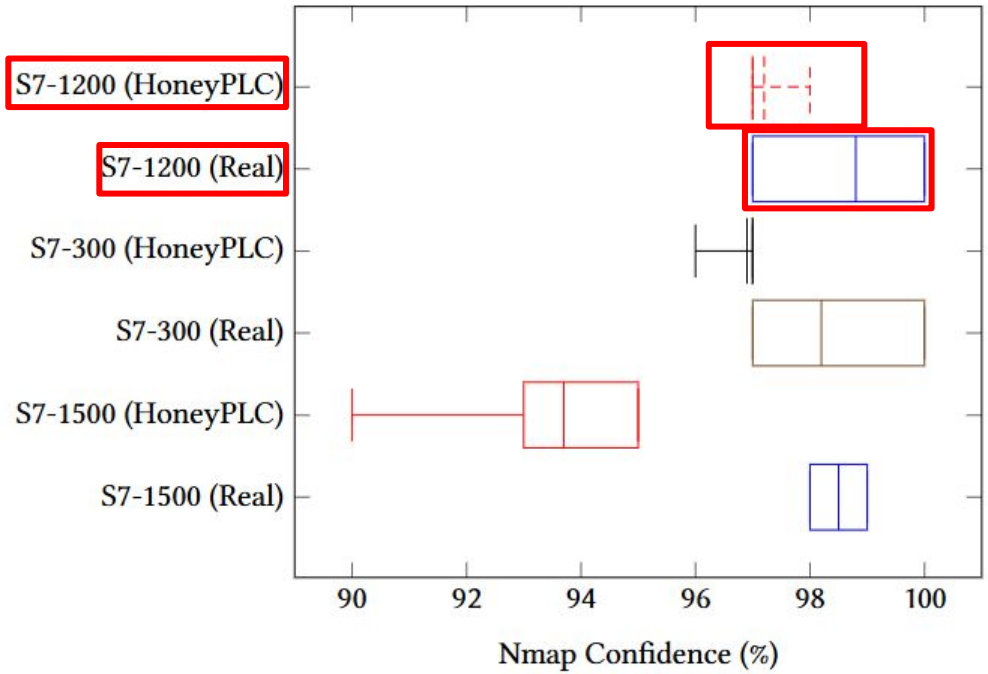
HoneyPLC's Performance versus Nmap



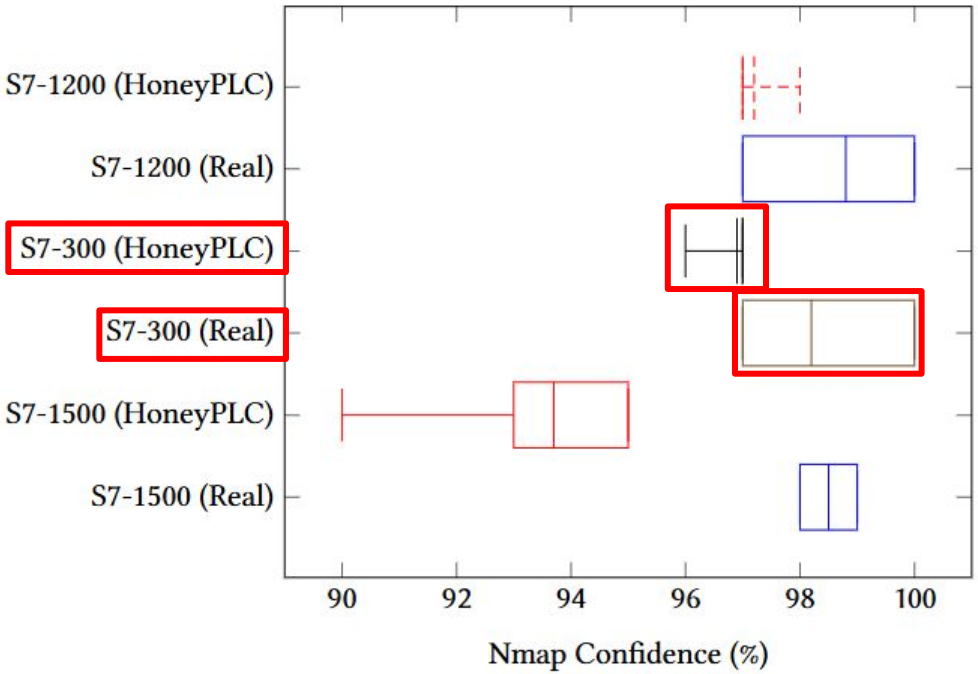
HoneyPLC's Performance versus Nmap



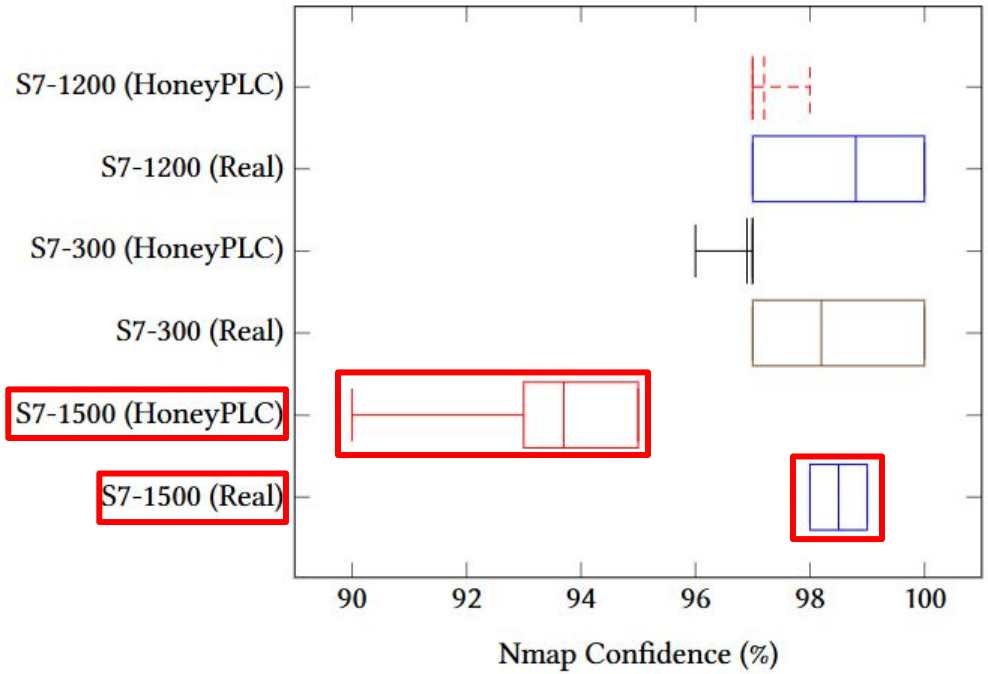
HoneyPLC's Performance versus Nmap



HoneyPLC's Performance versus Nmap



HoneyPLC's Performance versus Nmap



What did we find?

PLC Profile
Siemens S7-300
Siemens S7-1200
Siemens S7-1500

What did we find?

PLC Profile	Connections
Siemens S7-300	600
Siemens S7-1200	202
Siemens S7-1500	292

What did we find?

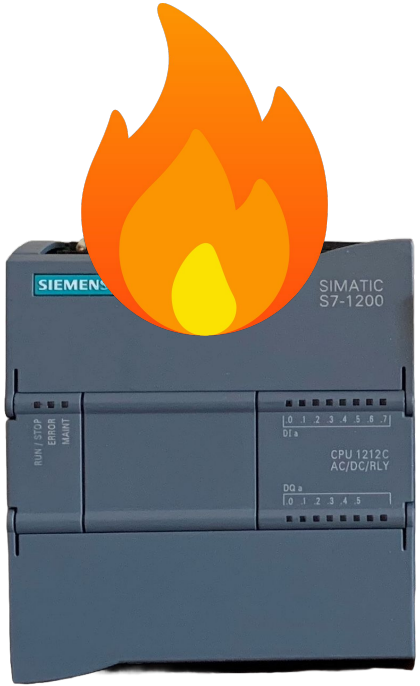
PLC Profile	Connections	Read PLC Memory
Siemens S7-300	600	80
Siemens S7-1200	202	0
Siemens S7-1500	292	0

What did we find?

PLC Profile	Connections	Read PLC Memory	PLC Stop
Siemens S7-300	600	80	4
Siemens S7-1200	202	0	0
Siemens S7-1500	292	0	0

What did we find?

PLC Profile	Connections	Read PLC Memory	PLC Stop
Siemens S7-300	600	80	**4**
Siemens S7-1200	202	0	0
Siemens S7-1500	292	0	0



Conclusion: HoneyPLC

- An extensible, realistic honeypot with advanced simulations

[1] Conti, Mauro, Francesco Trolese, and Federico Turrin. "Icspot: A high-interaction honeypot for industrial control systems." 2022 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2022.

Conclusion: HoneyPLC

- An extensible, realistic honeypot with advanced simulations
- Deceives well-known security tools and remain covert

[1] Conti, Mauro, Francesco Trolese, and Federico Turrin. "Icspot: A high-interaction honeypot for industrial control systems." 2022 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2022.

Conclusion: HoneyPLC

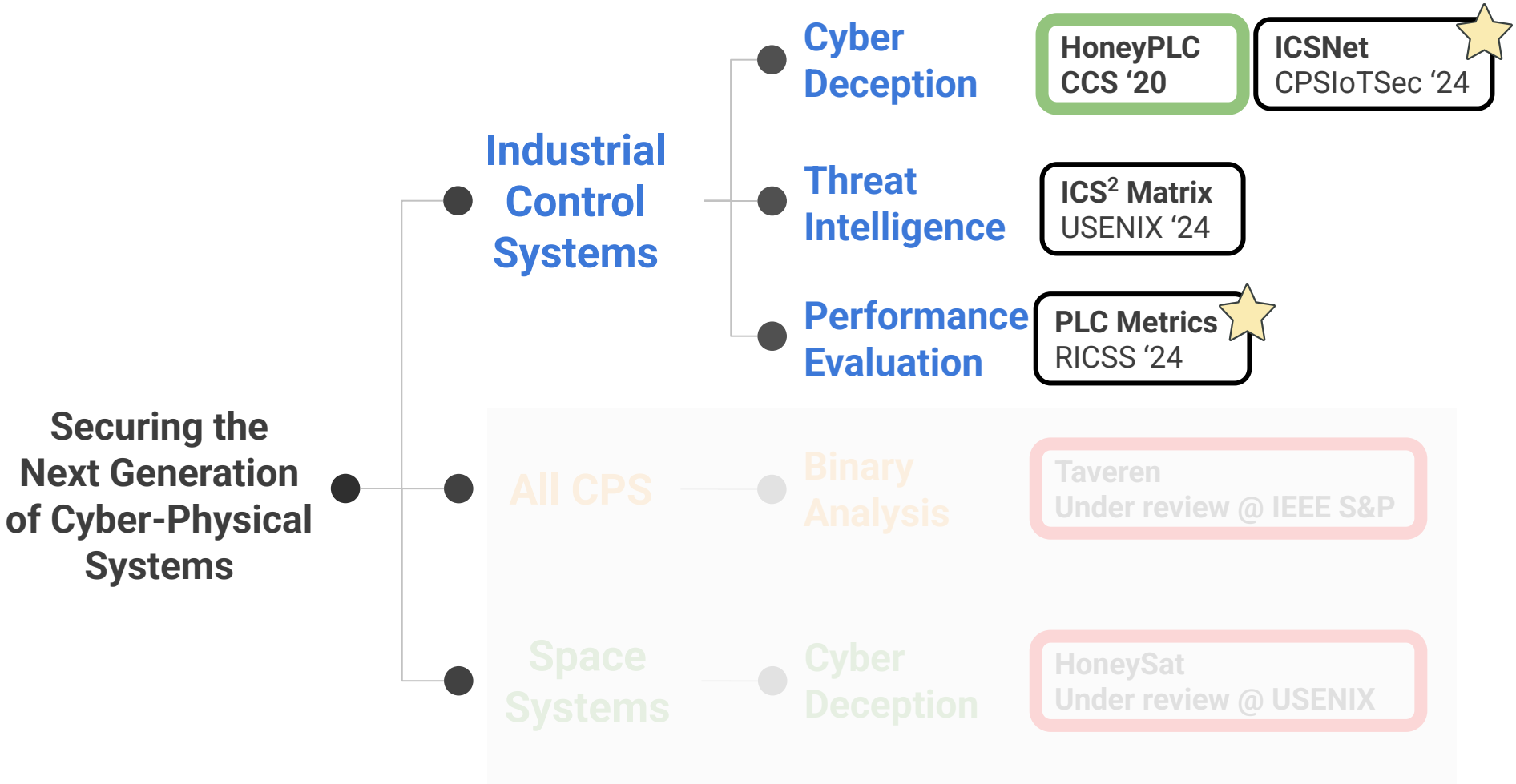
- An extensible, realistic honeypot with advanced simulations
- Deceives well-known security tools and remain covert
- Captures real-world cyberattack data to protect ICS

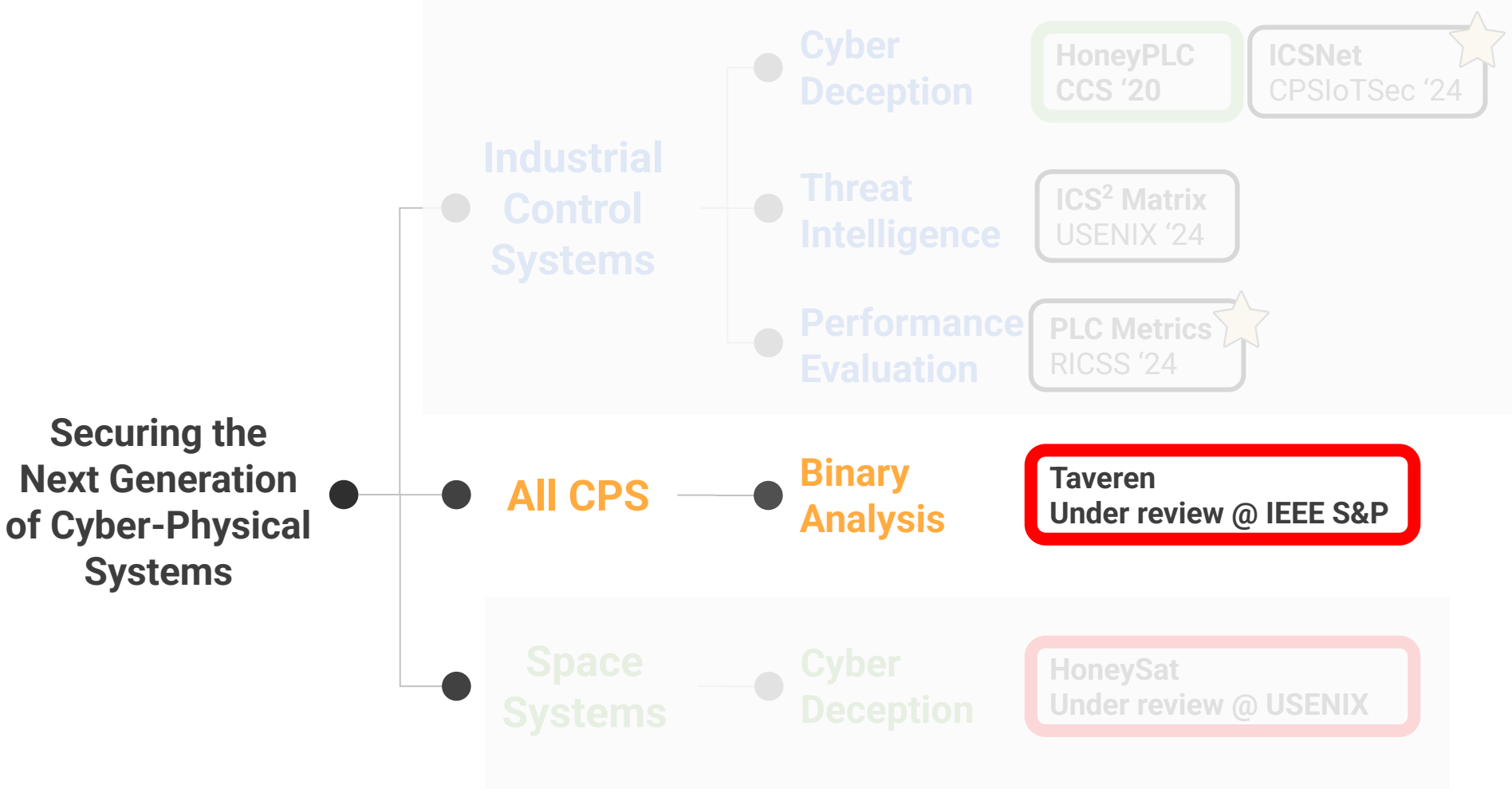
[1] Conti, Mauro, Francesco Trolese, and Federico Turrin. "Icspot: A high-interaction honeypot for industrial control systems." 2022 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2022.

Conclusion: HoneyPLC

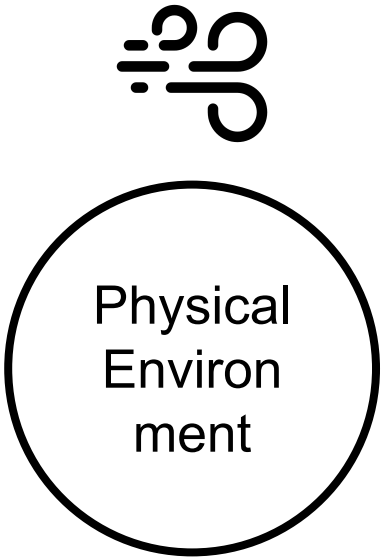
- An extensible, realistic honeypot with advanced simulations
- Deceives well-known security tools and remain covert
- Captures real-world cyberattack data to protect ICS
- *“HoneyPLC, which to the best of our knowledge, represents the most advanced ICS honeypot available.” [1]*

[1] Conti, Mauro, Francesco Trolese, and Federico Turrin. "Icspot: A high-interaction honeypot for industrial control systems." 2022 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2022.

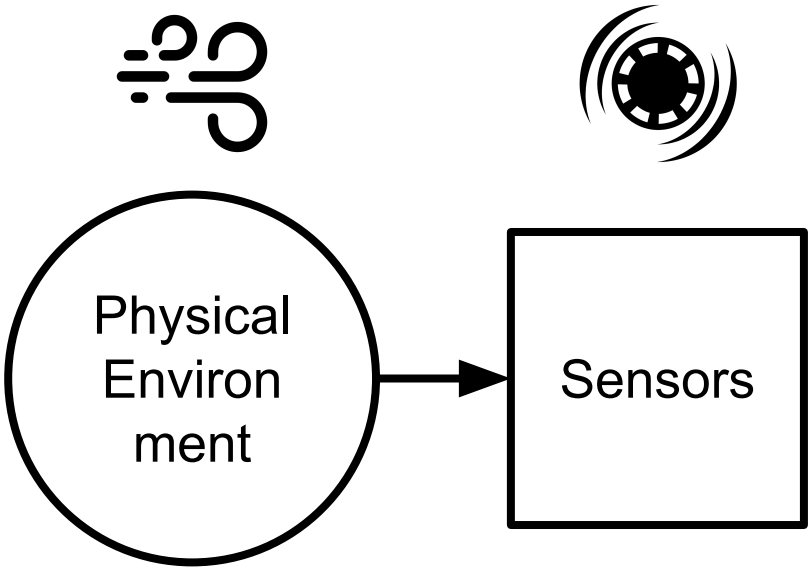

Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
Threat Intelligence
ICS² Matrix
USENIX '24
Performance Evaluation
PLC Metrics
RICSS '24
All CPS
Binary Analysis
Taveren
Under review @ IEEE S&P
Space Systems
Cyber Deception
HoneySat
Under review @ USENIX


Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
Threat Intelligence
ICS² Matrix
USENIX '24
Performance Evaluation
PLC Metrics
RICSS '24
All CPS
Binary Analysis
Taveren
Under review @ IEEE S&P
Space Systems
Cyber Deception
HoneySat
Under review @ USENIX

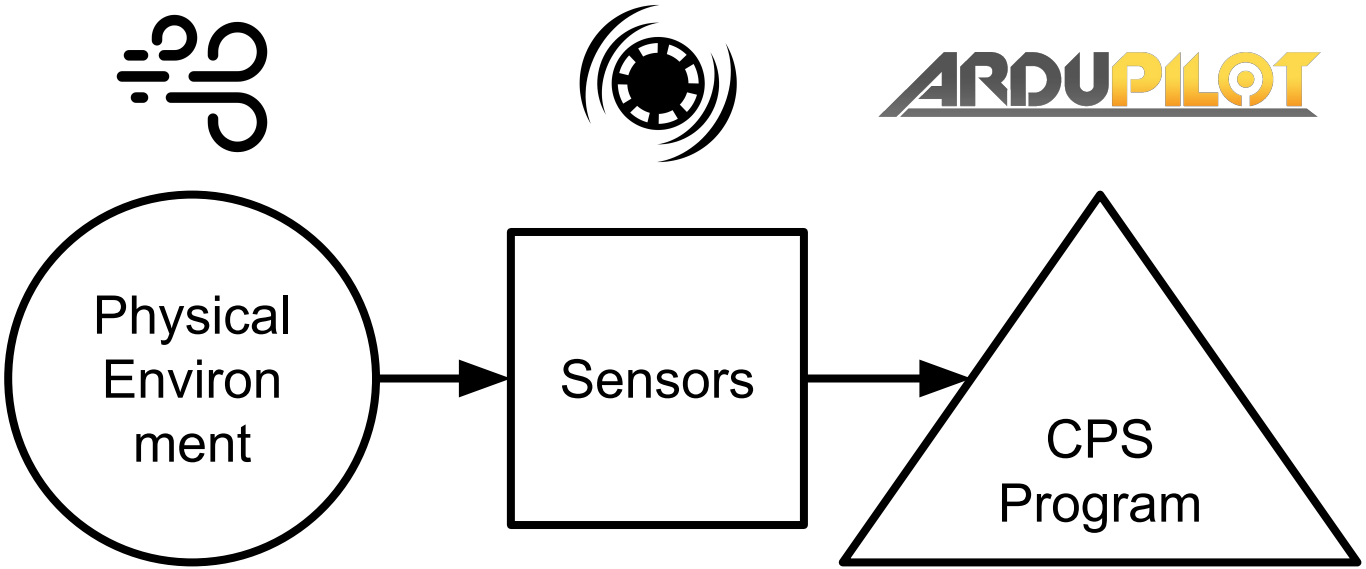
Background: Cyber-Physical Systems' Programs



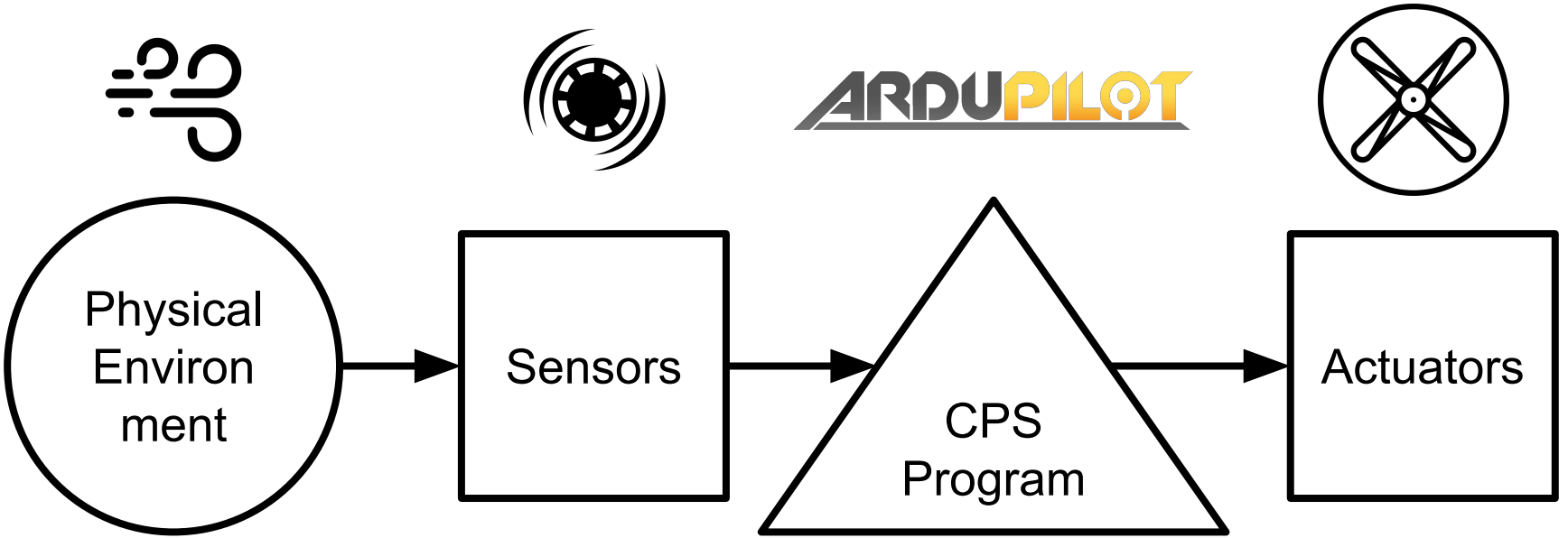
Background: Cyber-Physical Systems' Programs



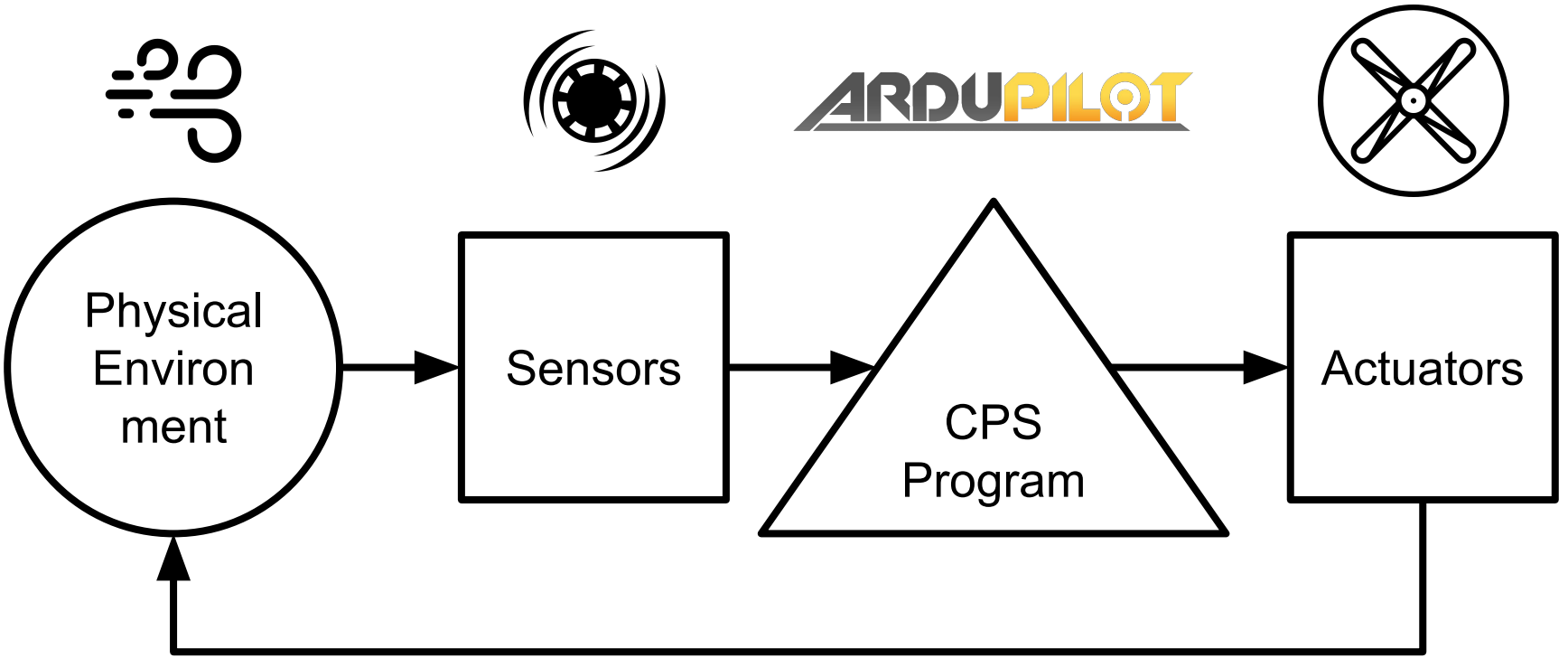
Background: Cyber-Physical Systems' Programs



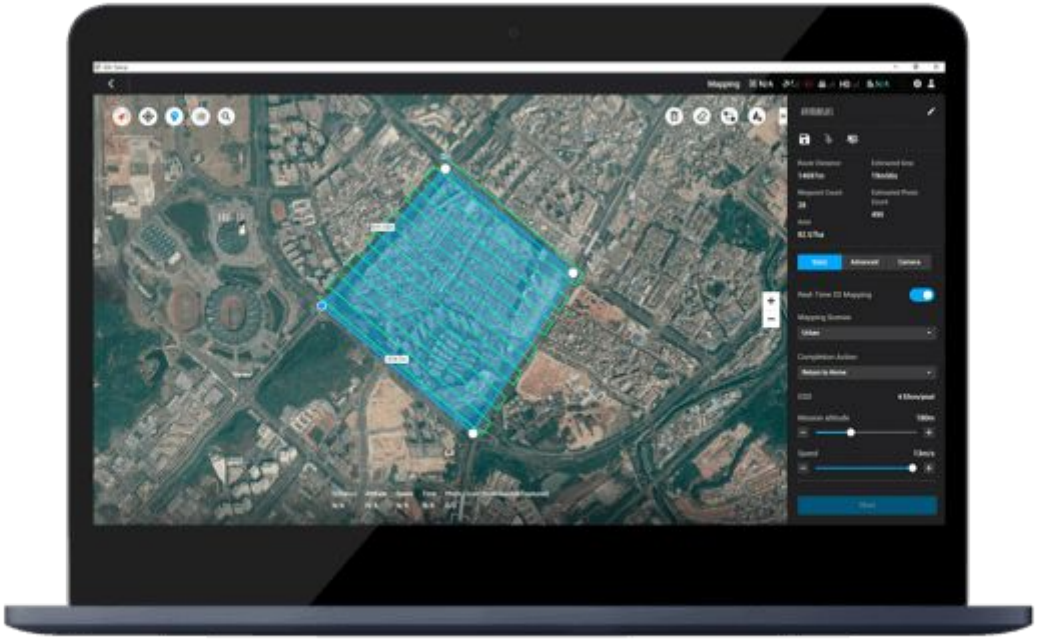
Background: Cyber-Physical Systems' Programs



Background: Cyber-Physical Systems' Programs



Background: CPS Proprietary Programs



Background: What is binary analysis?

- Technique used to analyze and review binary code

Background: What is binary analysis?

- Technique used to analyze and review binary code
- Allows us to find vulnerabilities

Background: What is binary analysis?

- Technique used to analyze and review binary code
- Allows us to find vulnerabilities
- Necessary to analyze software when we do not have the source code

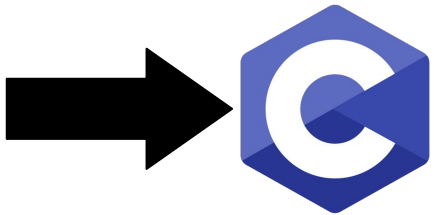
Background: What is binary analysis?

```
int main() {

    printf("Hello, World!\n");

    return 0;
}
```

Human-readable source code

Background: What is binary analysis?

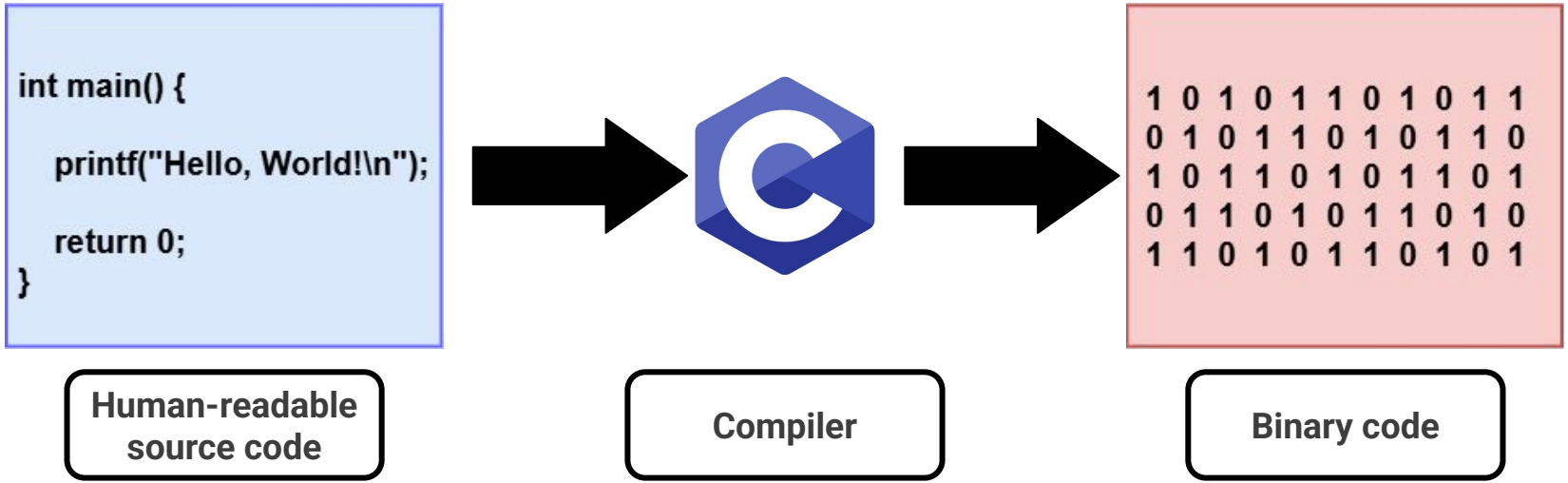
```
int main() {
    printf("Hello, World!\n");
    return 0;
}
```



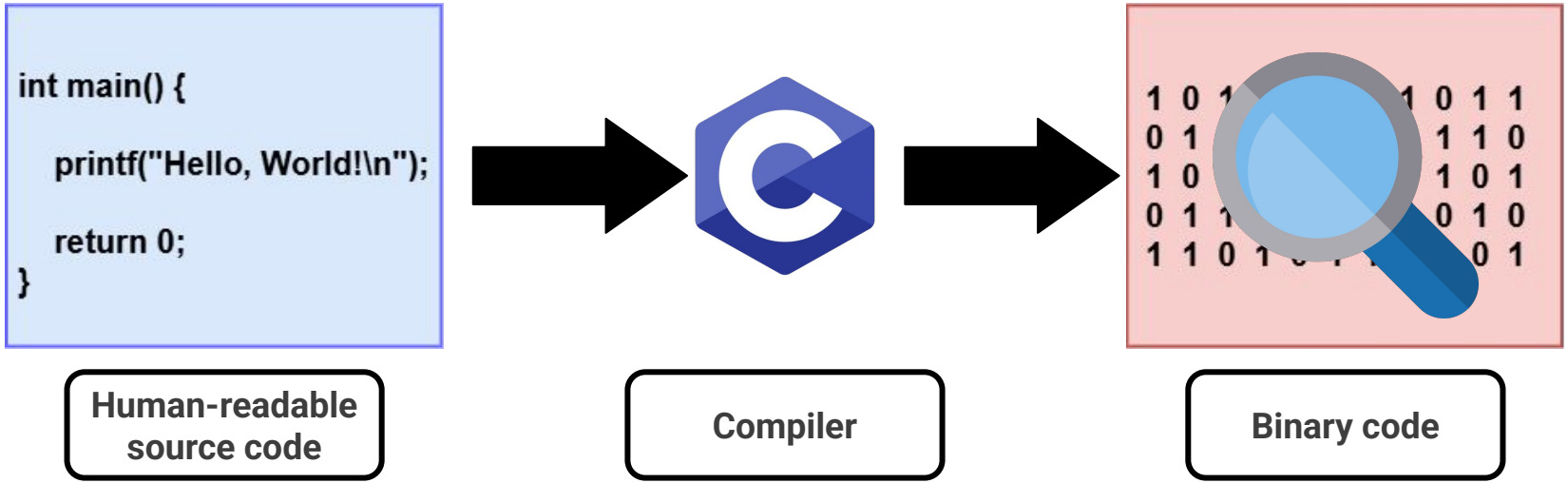
Human-readable source code

Compiler

Background: What is binary analysis?



Background: What is binary analysis?



Background: Security versus Safety

Background: Security versus Safety

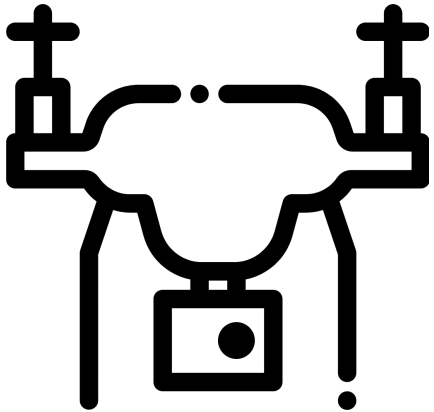
```
#include <string.h>

void foo (char *bar)
{
   char  c[12];

   strcpy(c, bar);  // no bounds
}

int main (int argc, char **argv)
{
   foo(argv[1]);
}
```

Background: Security versus Safety

```
#include <string.h>

void foo (char *bar)
{
   char  c[12];

   strcpy(c, bar);  // no bounds
}

int main (int argc, char **argv)
{
   foo(argv[1]);
}
```

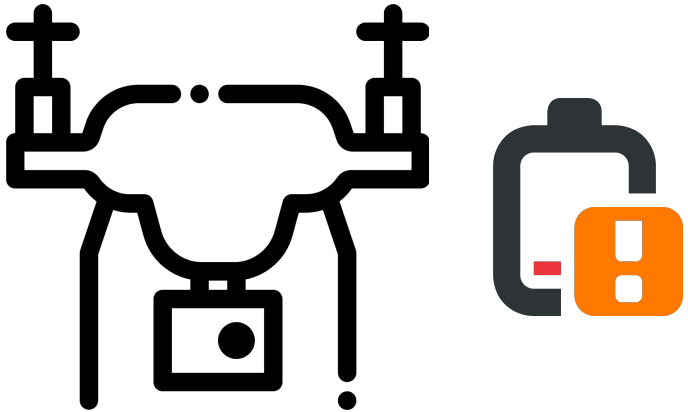
Background: Security versus Safety

```c
#include <string.h>

void foo (char *bar)
{
   char  c[12];

   strcpy(c, bar);  // no bounds
}

int main (int argc, char **argv)
{
   foo(argv[1]);
}
```



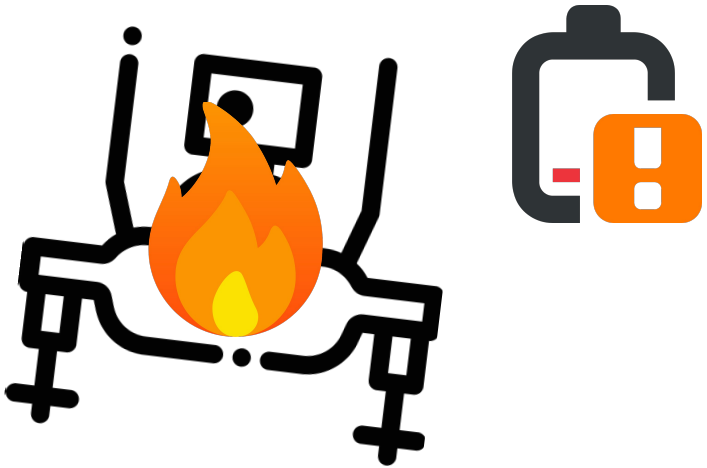
Background: Security versus Safety

```c
#include <string.h>

void foo (char *bar)
{
   char  c[12];

   strcpy(c, bar);  // no bounds
}

int main (int argc, char **argv)
{
   foo(argv[1]);
}
```



Background: Security versus Safety

```c
#include <string.h>

void foo (char *bar)
{
   char  c[12];

   strcpy(c, bar);  // no bounds
}

int main (int argc, char **argv)
{
   foo(argv[1]);
}
```



What is the problem?

Current binary analysis methods to analyze CPS programs focus on *security* and cannot find and remove *safety* vulnerabilities.

Our Solution: Taveren

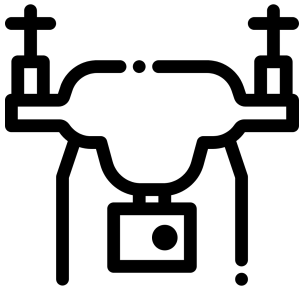
- **Binary analysis tool** for CPS Programs

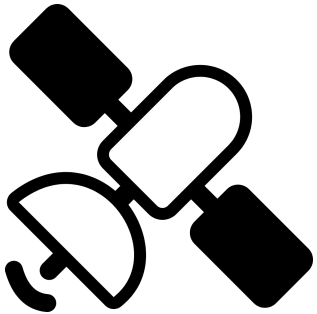
Our Solution: Taveren

- **Binary analysis tool** for CPS Programs
- Enforces **user-generated *safety* policies**

Our Solution: Taveren

- **Binary analysis tool** for CPS Programs
- Enforces **user-generated *safety* policies**
- Works for **multiple CPS programs and architectures**



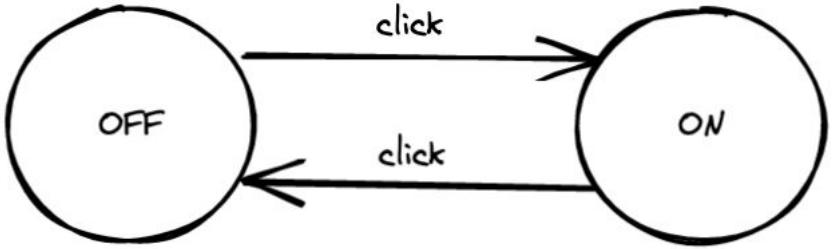


How does Taveren work?

- Built on top of **angr** (open-source binary analysis platform)

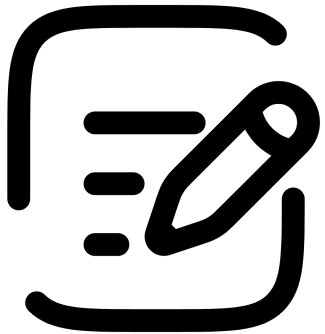
How does Taveren work?

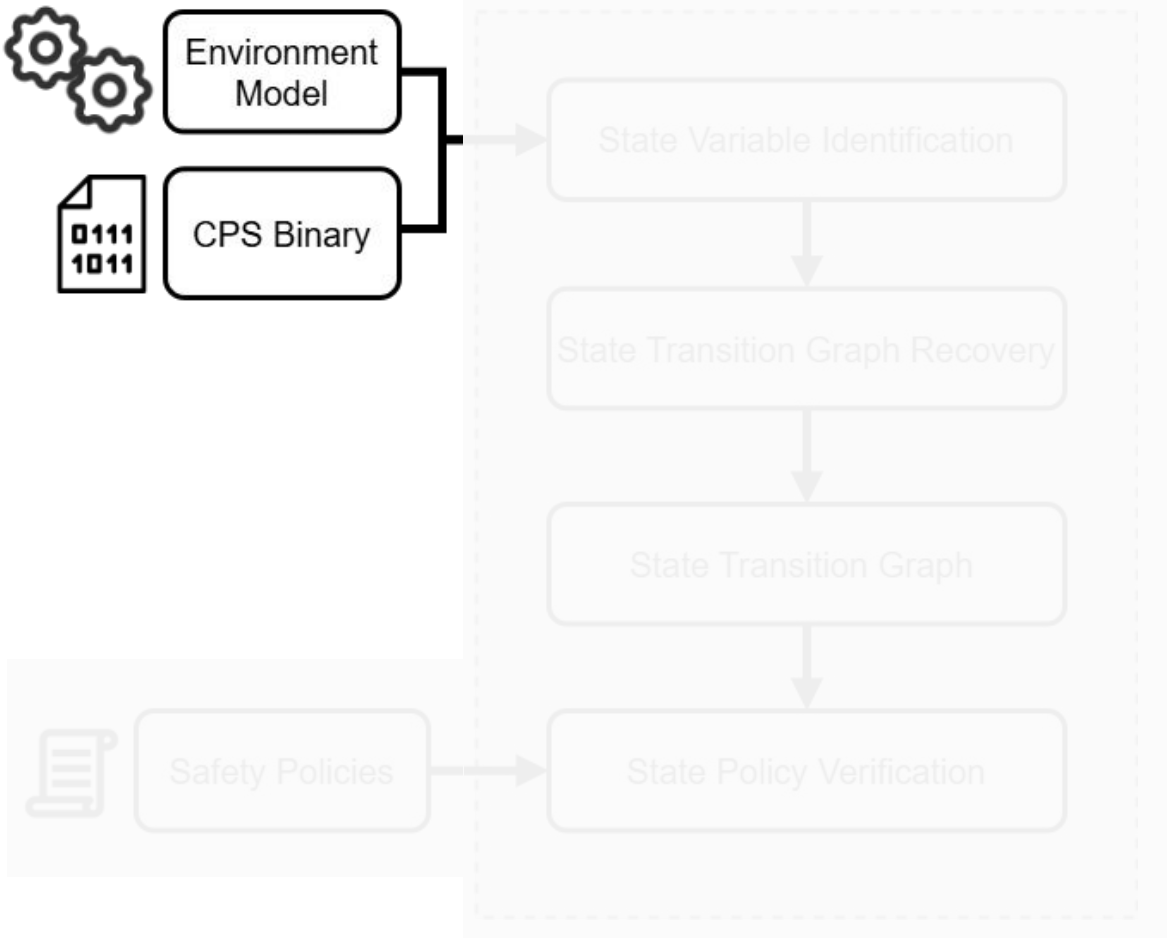
- Built on top of **angr** (open-source binary analysis platform)
- Uses **finite-state machines** to model CPS' complexity

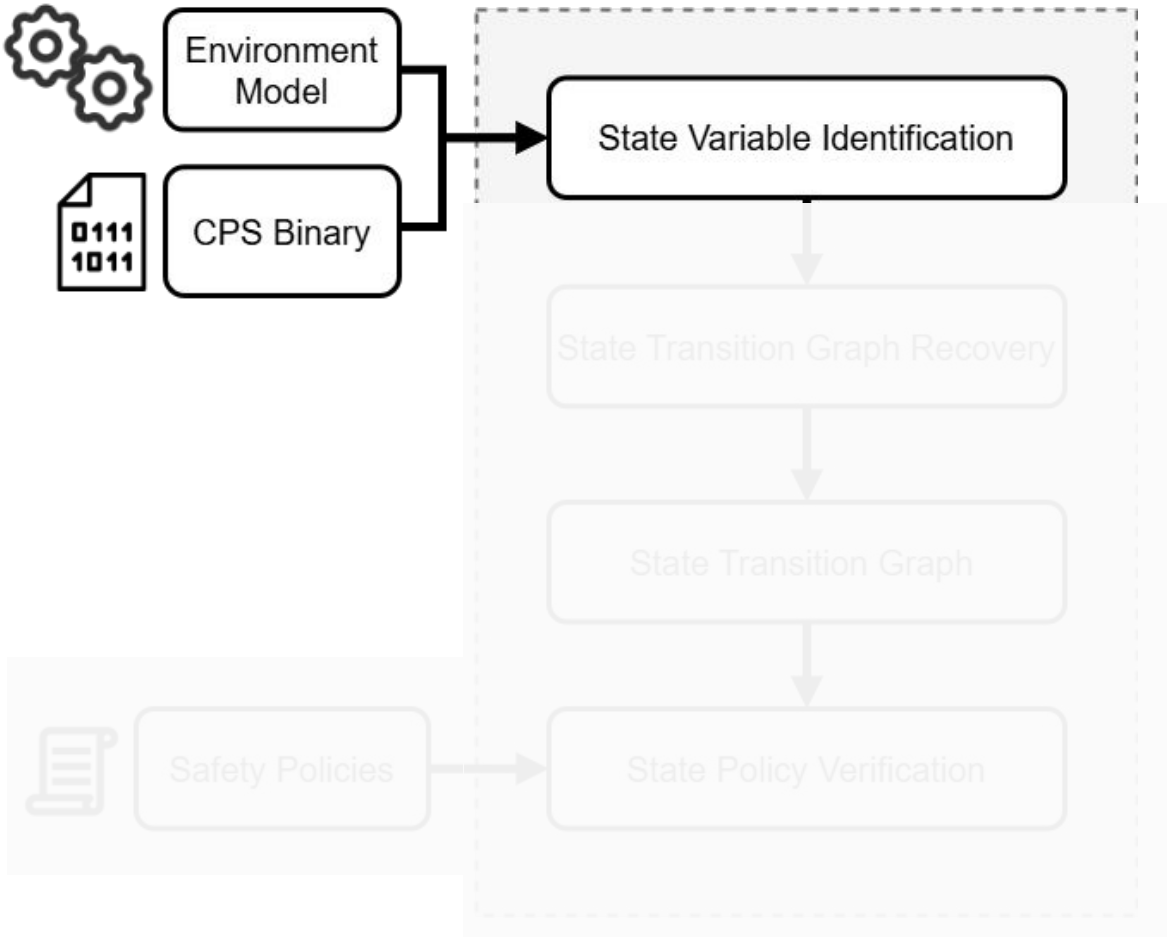


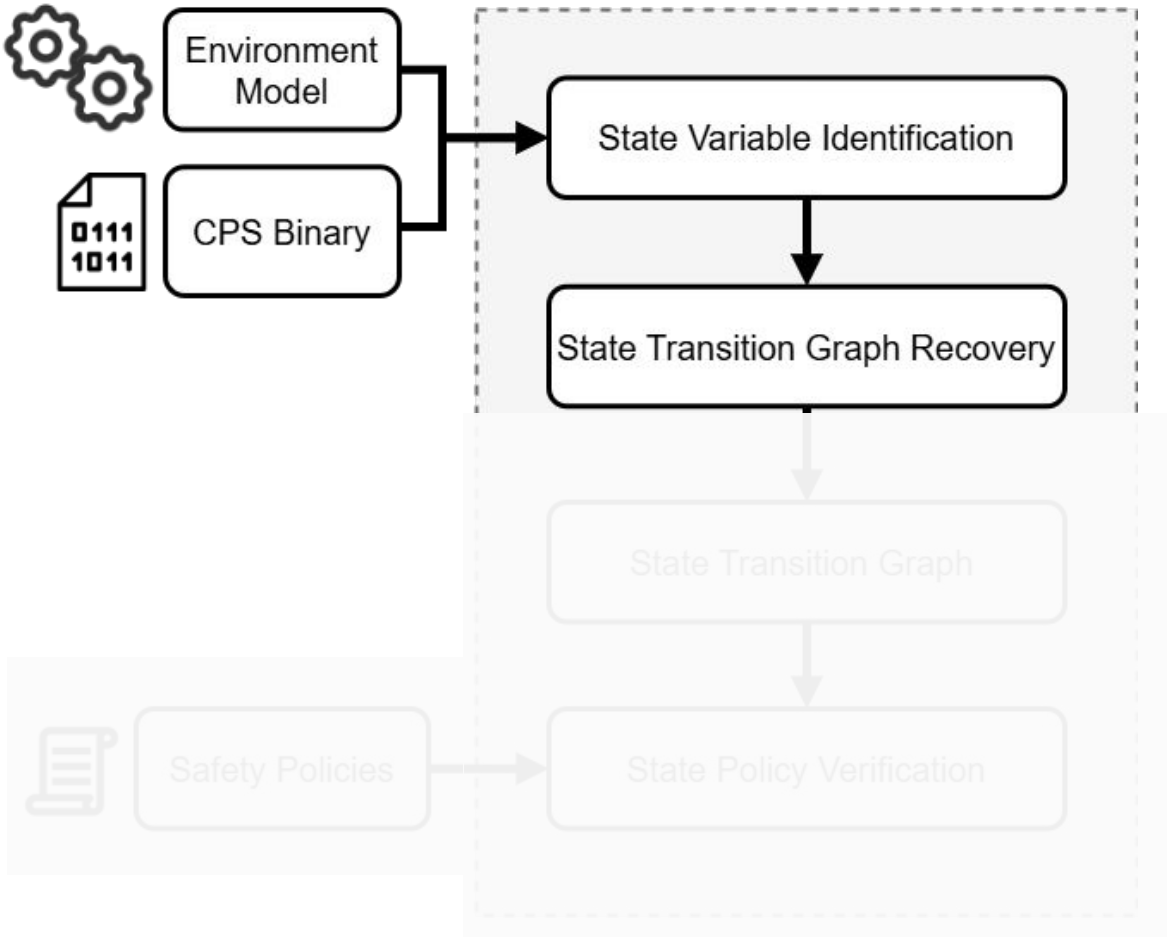
How does Taveren work?

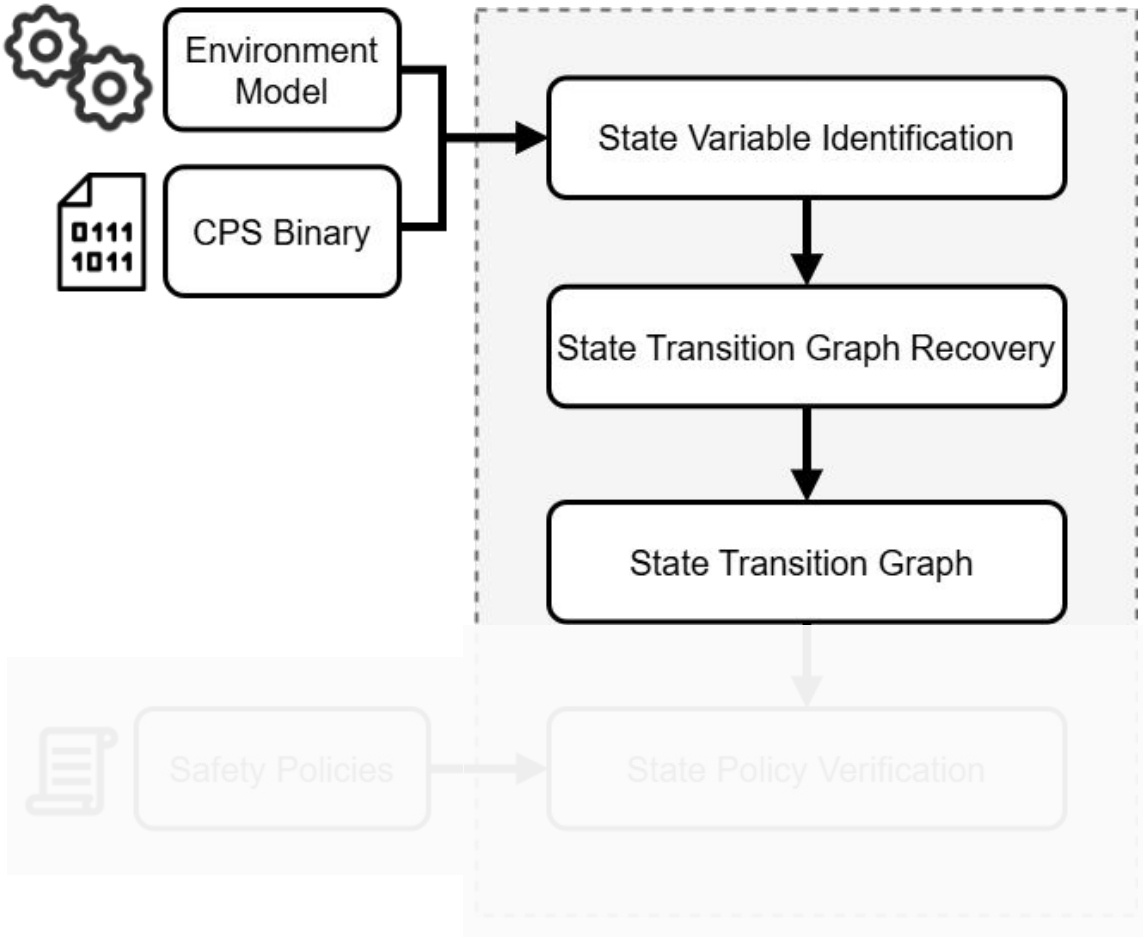
- Built on top of **angr** (open-source binary analysis platform)
- Uses **finite-state machines** to model CPS' complexity
- Requires **CPS program**, ***safety*** **policies,** and **environment model**

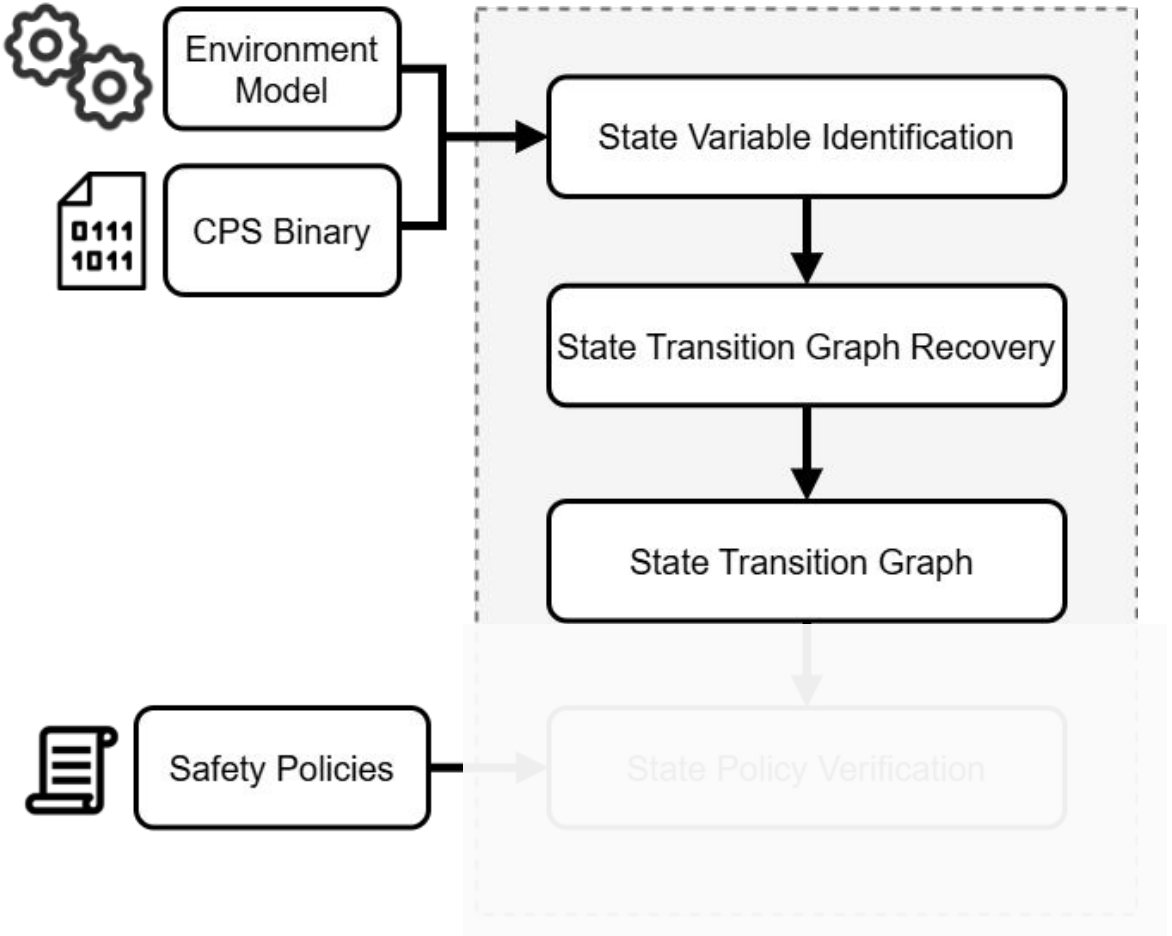


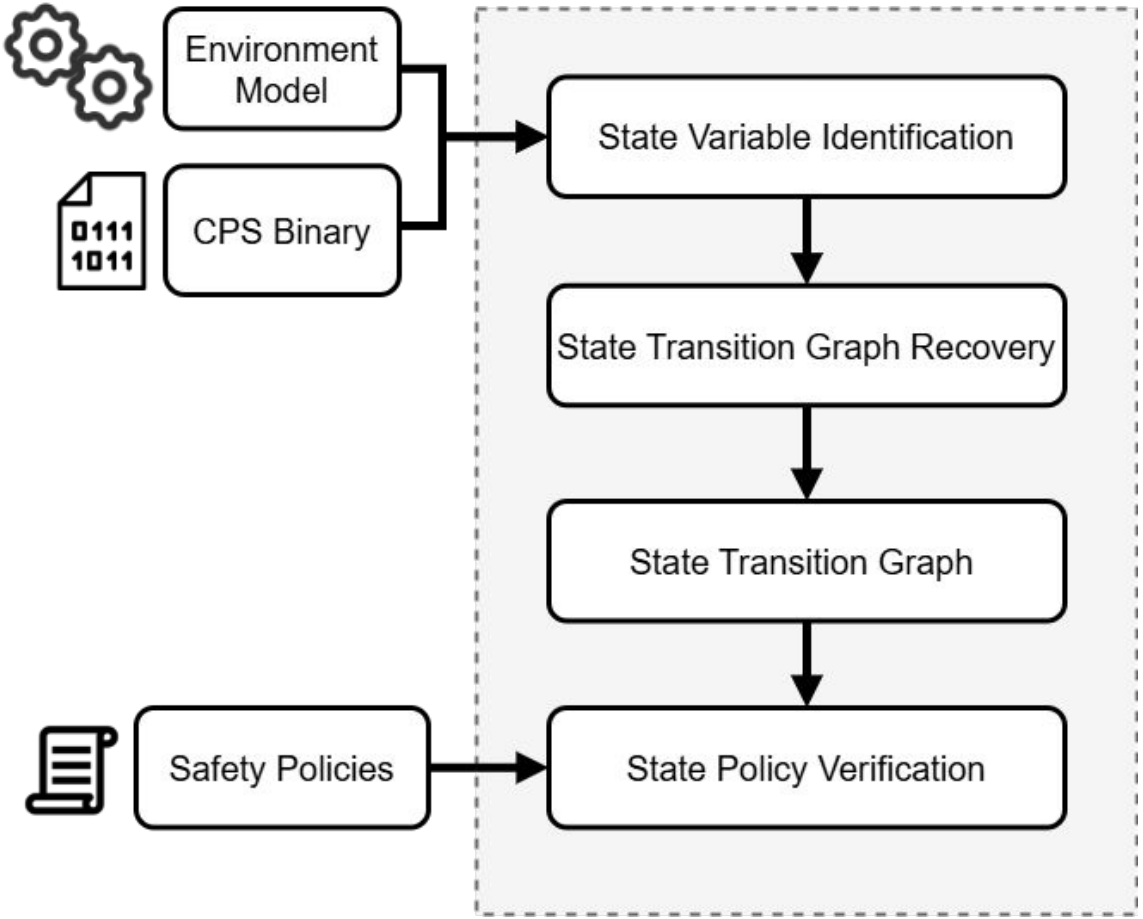

Environment Model
CPS Binary
0111
1011
State Variable Identification
State Transition Graph Recovery
State Transition Graph
Safety Policies
State Policy Verification


Environment Model
CPS Binary
0111
1011
State Variable Identification
State Transition Graph Recovery
State Transition Graph
Safety Policies
State Policy Verification


Environment Model
CPS Binary
0111
1011
State Variable Identification
State Transition Graph Recovery
State Transition Graph
Safety Policies
State Policy Verification

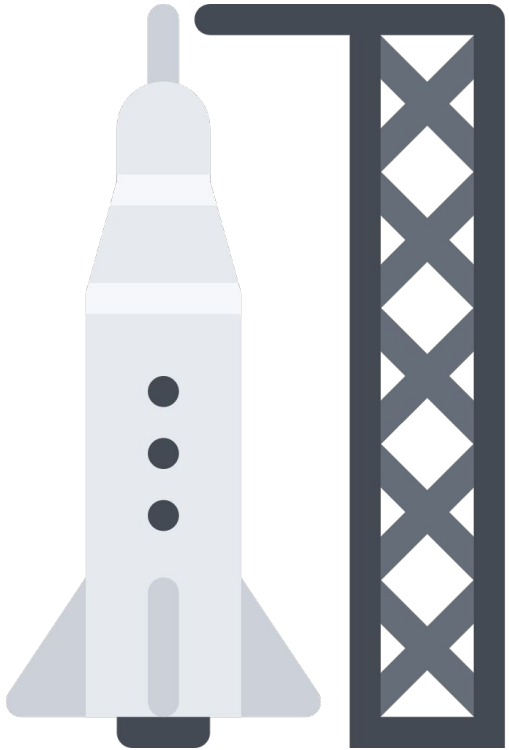

Environment Model
CPS Binary
0111
1011
State Variable Identification
State Transition Graph Recovery
State Transition Graph
Safety Policies
State Policy Verification


Environment Model
CPS Binary
0111
1011
State Variable Identification
State Transition Graph Recovery
State Transition Graph
Safety Policies
State Policy Verification


Environment Model
CPS Binary
0111
1011
State Variable Identification
State Transition Graph Recovery
State Transition Graph
Safety Policies
State Policy Verification

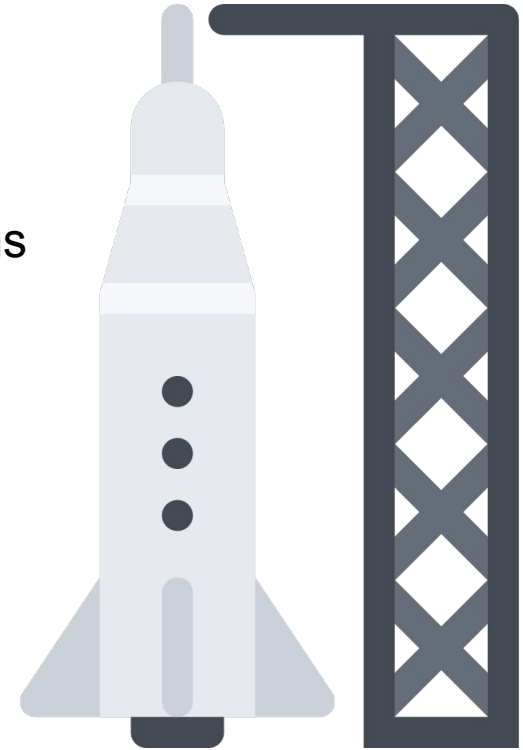
How did we evaluate Taveren?

- Dataset with 19 CPS Program Binaries



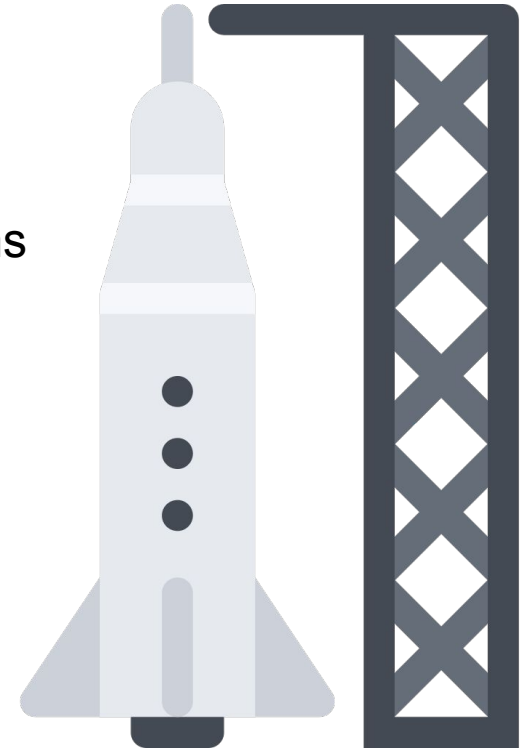
How did we evaluate Taveren?

- Dataset with 19 CPS Program Binaries
- Dataset includes **ICS, UAV, space and vehicle** programs



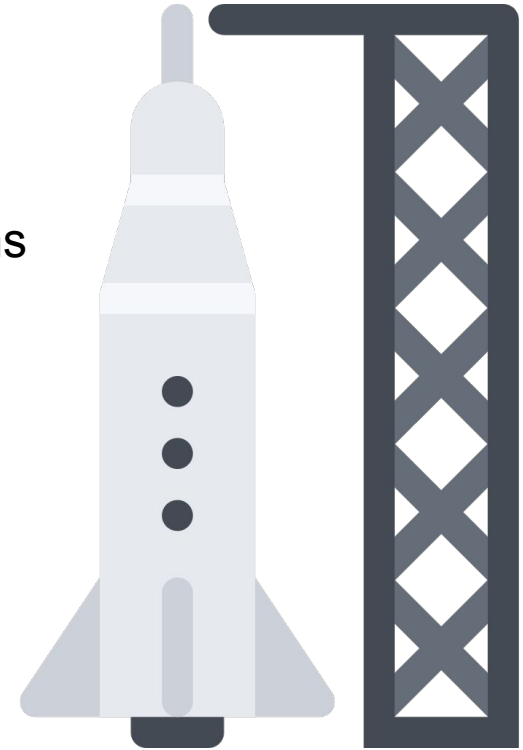
How did we evaluate Taveren?

- Dataset with 19 CPS Program Binaries
- Dataset includes **ICS, UAV, space and vehicle** programs
- ARM and x86 architectures



How did we evaluate Taveren?

- Dataset with 19 CPS Program Binaries
- Dataset includes **ICS, UAV, space and vehicle** programs
- ARM and x86 architectures
- 21 safety policies



What did we find?

- Taveren recovered all **19 CPS programs' transition graphs**
- Taveren has a **95% accuracy** enforcing safety policy

Safety Policy Enforcement Accuracy Results

Safety Policy Enforcement Accuracy Results

#	P.Copter.1	P.Copter.2	Correct?
Copter.1	T	T	Y
Copter.2	T	T	Y
#	**P.Rover.1**		**Correct?**
Rover.1	F		Unknown
#	**P.Lift.1**	**P.Lift.2**	**Correct?**
Lift.1	T	F	N
#	**P.WT.1**	**P.WT.2**	**Correct?**
WT.1	F	F	Y
WT.2	T	T	Y
WT.3	F	F	Y
#	**P.Pack.1**	**P.Pack.2**	**Correct?**
Pack.1	T	F	Y

Safety Policy Enforcement Accuracy Results

#	P.Copter.1	P.Copter.2	Correct?
Copter.1	T	T	Y
Copter.2	T	T	Y
#	**P.Rover.1**		**Correct?**
Rover.1	F		Unknown
#	**P.Lift.1**	**P.Lift.2**	**Correct?**
Lift.1	T	F	N
#	**P.WT.1**	**P.WT.2**	**Correct?**
WT.1	F	F	Y
WT.2	T	T	Y
WT.3	F	F	Y
#	**P.Pack.1**	**P.Pack.2**	**Correct?**
Pack.1	T	F	Y

#	P.TL.1	P.TL.2	P.TL.3	Correct?
TL.4	T	F	T	Y
TL.5	T	F	T	Y
TL.6	T	F	T	Y
TL.7	T	F	F	Y
TL.8	F	F	T	Y
TL.9	T	T	T	Y
TL.10	T	F	F	Y
TL.11	T	T	T	Y
#	**P.Abort.1**	**P.Abort.2**		**Correct?**
Abort.3	F	T		Y
#	**P.Oven.1**	**P.Oven.2**	**P.Oven.3**	**Correct?**
Oven.1	T	T		Y
#	**P.Vend.1**			**Correct?**
Vend.1	F			Y
#	**P.Elev.1**	**P.Elev.2**	**P.Elev.3**	**Correct?**
Elev.1	T	T	T	Y

Safety Policy Enforcement Accuracy Results

#	P.Copter.1	P.Copter.2	Correct?
Copter.1	T	T	Y
Copter.2	T	T	Y
#	P.Rover.1		Correct?
Rover.1	F		Unknown
#	P.Lift.1	P.Lift.2	Correct?
Lift.1	T	F	N
#	P.WT.1	P.WT.2	Correct?
WT.1	F	F	Y
WT.2	T	T	Y
WT.3	F	F	Y
#	P.Pack.1	P.Pack.2	Correct?
Pack.1	T	F	Y

#	P.TL.1	P.TL.2	P.TL.3	Correct?
TL.4	T	F	T	Y
TL.5	T	F	T	Y
TL.6	T	F	T	Y
TL.7	T	F	F	Y
TL.8	F	F	T	Y
TL.9	T	T	T	Y
TL.10	T	F	F	Y
TL.11	T	T	T	Y
#	P.Abort.1	P.Abort.2		Correct?
Abort.3	F	T		Y
#	P.Oven.1	P.Oven.2	P.Oven.3	Correct?
Oven.1	T	T		Y
#	P.Vend.1			Correct?
Vend.1	F			Y
#	P.Elev.1	P.Elev.2	P.Elev.3	Correct?
Elev.1	T	T	T	Y

Safety Policy Enforcement Accuracy Results

CPS Binary
ArduCopter 1
ArduCopter 2

Safety Policy Enforcement Accuracy Results

CPS Binary	**Policy 1:** Do not apply throttle when in unknown position
ArduCopter 1	Patch Applied
ArduCopter 2	Patch Applied

Safety Policy Enforcement Accuracy Results

CPS Binary	**Policy 1:** Do not apply throttle when in unknown position	**Policy 2:** Flip maneuvers cannot last more than 2.5 seconds
ArduCopter 1	Patch Applied	Patch Applied
ArduCopter 2	Patch Applied	Patch Applied

Safety Policy Enforcement Accuracy Results

CPS Binary	**Policy 1:** Do not apply throttle when in unknown position	**Policy 2:** Flip maneuvers cannot last more than 2.5 seconds	**Taveren Result**
ArduCopter 1	Patch Applied	Patch Applied	Correct
ArduCopter 2	Patch Applied	Patch Applied	Correct

Conclusion: Taveren

- First binary analysis tool to find safety vulnerabilities in CPS programs

Conclusion: Taveren

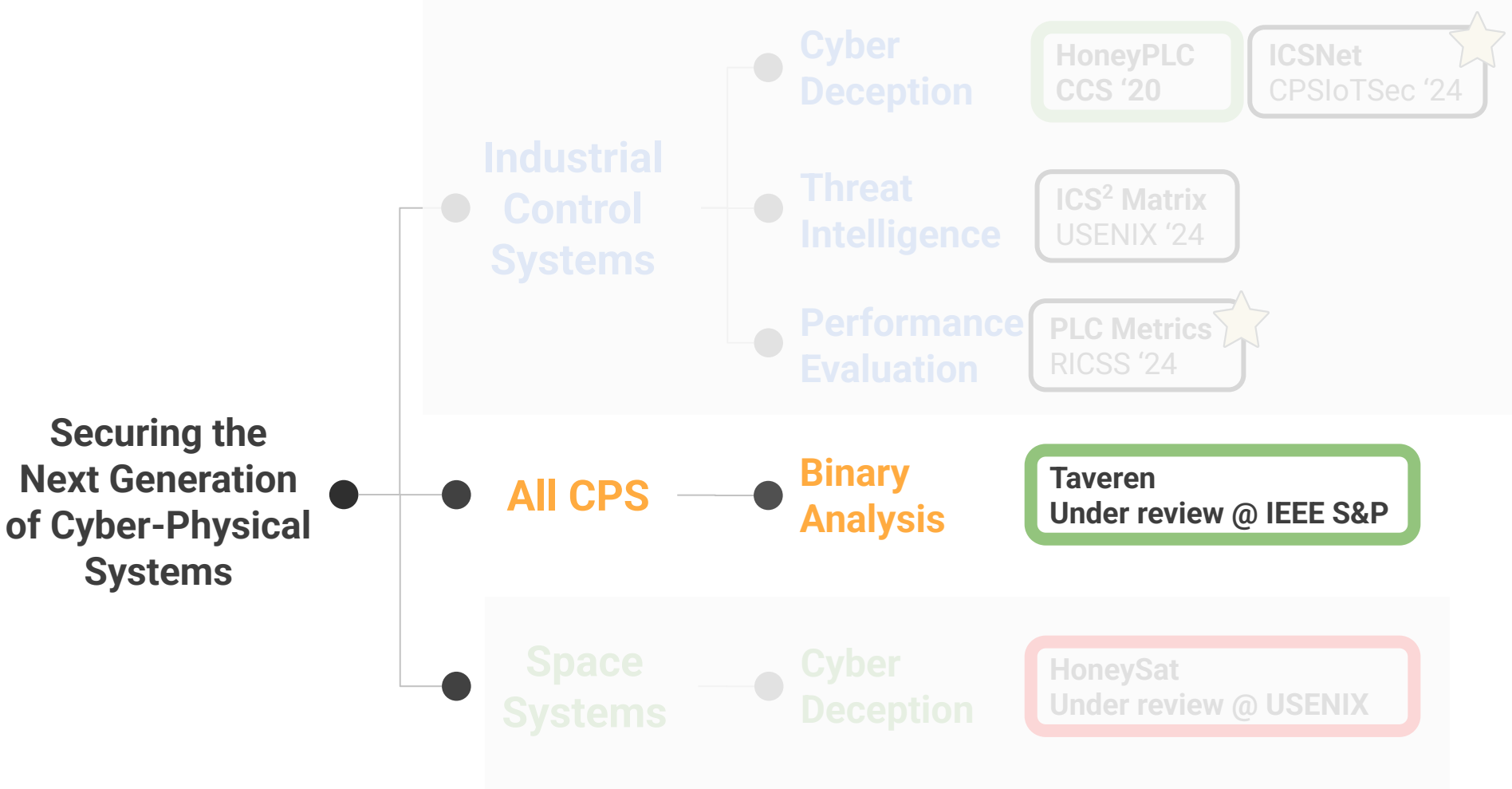
- First binary analysis tool to find safety vulnerabilities in CPS programs
- Works with multiple types of CPS

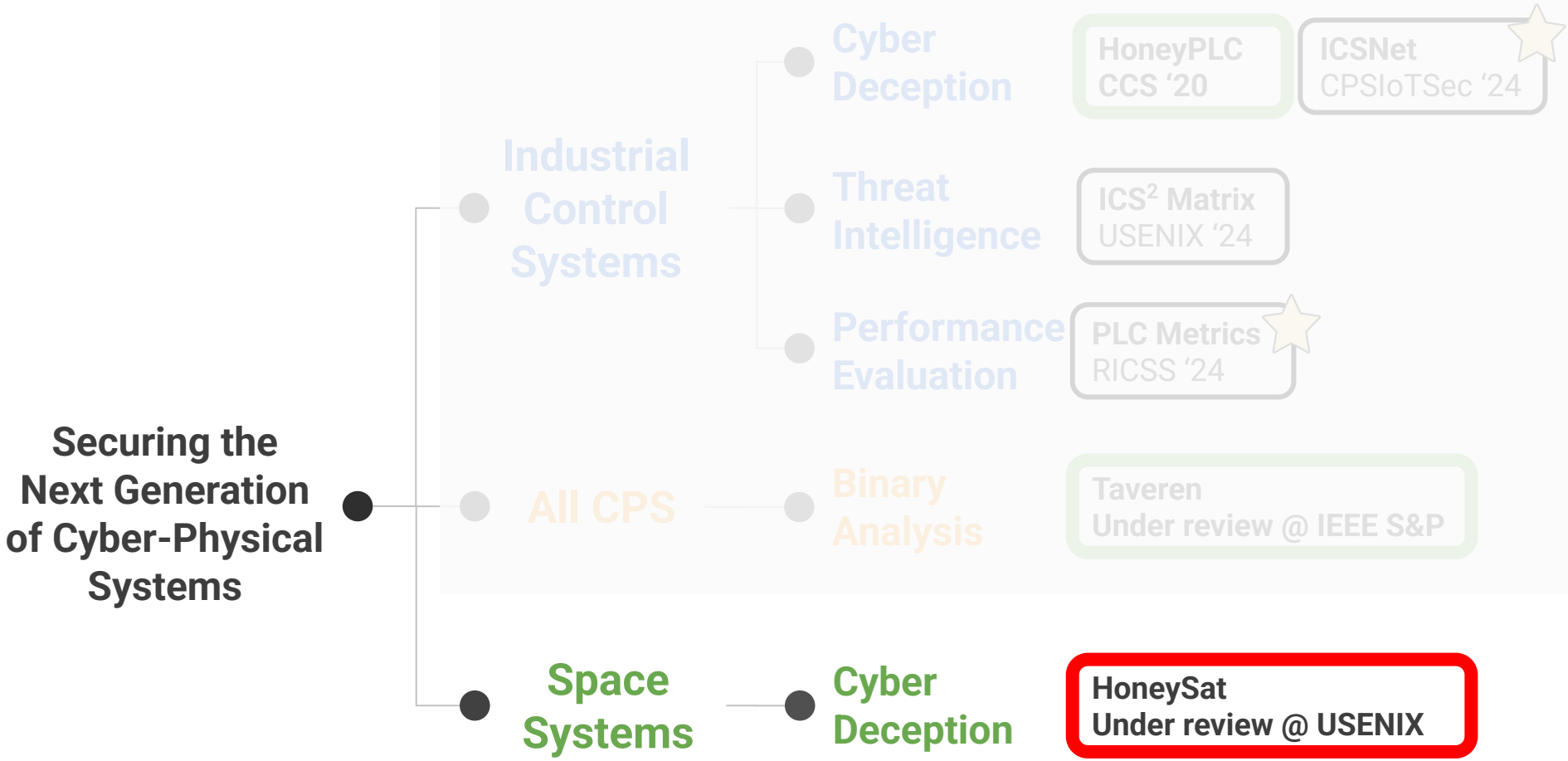
Conclusion: Taveren

- First binary analysis tool to find safety vulnerabilities in CPS programs
- Works with multiple types of CPS
- Evaluated using real-world CPS programs

Conclusion: Taveren

- First binary analysis tool to find safety vulnerabilities in CPS programs
- Works with multiple types of CPS
- Evaluated using real-world CPS programs
- Improves the cybersecurity of CPS by finding previously unknown safety vulnerabilities


Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
HoneyPLC CCS '20
ICSNet CPSIoTSec '24
Threat Intelligence
ICS² Matrix USENIX '24
Performance Evaluation
PLC Metrics RICSS '24
All CPS
Binary Analysis
Taveren Under review @ IEEE S&P
Space Systems
Cyber Deception
HoneySat Under review @ USENIX


Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
Threat Intelligence
ICS² Matrix
USENIX '24
Performance Evaluation
PLC Metrics
RICSS '24
All CPS
Binary Analysis
Taveren
Under review @ IEEE S&P
Space Systems
Cyber Deception
HoneySat
Under review @ USENIX


SPACEX

Space: The Final Frontier for Cyberattacks

A failure to imagine — and prepare for — threats to outer-space related assets could be a huge mistake at a time when nation-states and private companies are rushing to deploy devices in a frantic new space race.

Space: The Final Frontier for Cyberattacks

A failure to imagine — and prepare for — threats to outer-space related assets could be a huge mistake at a time when nation-states and private companies are rushing to deploy devices in a frantic new space race.

Rocket Lab launches 5 'Internet of Things' satellites to orbit

News By Elizabeth Howell published September 18, 2024

Space: The Final Frontier for Cyberattacks

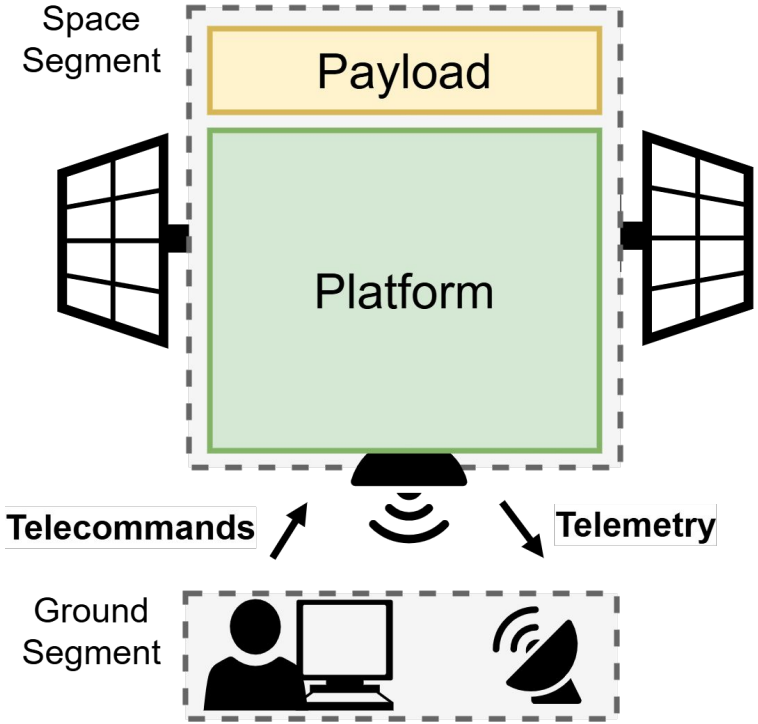
A failure to imagine — and prepare for — threats to outer-space related assets could be a huge mistake at a time when nation-states and private companies are rushing to deploy devices in a frantic new space race.

Rocket Lab launches 5 'Internet of Things' satellites to orbit

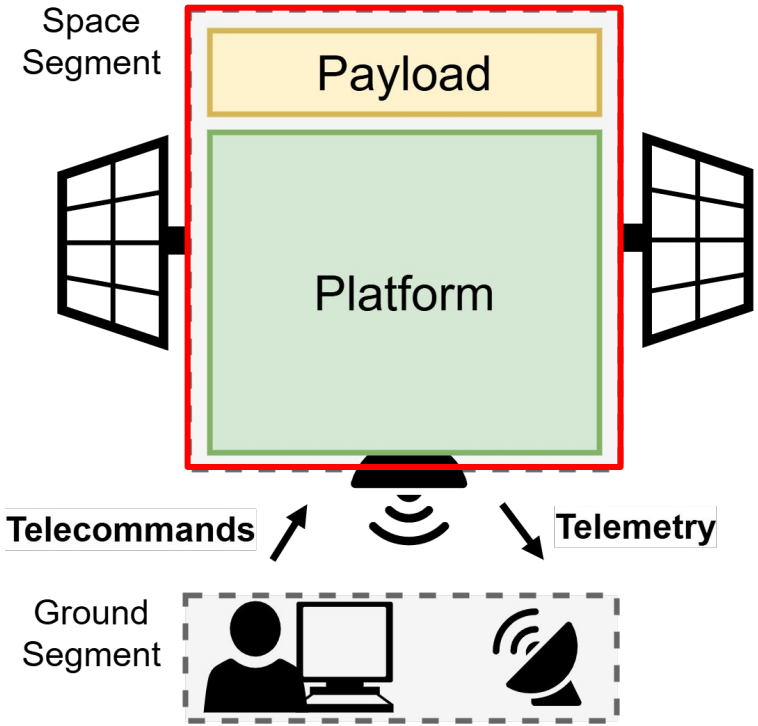
News By Elizabeth Howell published September 18, 2024

New Star Wars Plan: Pentagon Rushes to Counter Threats in Orbit

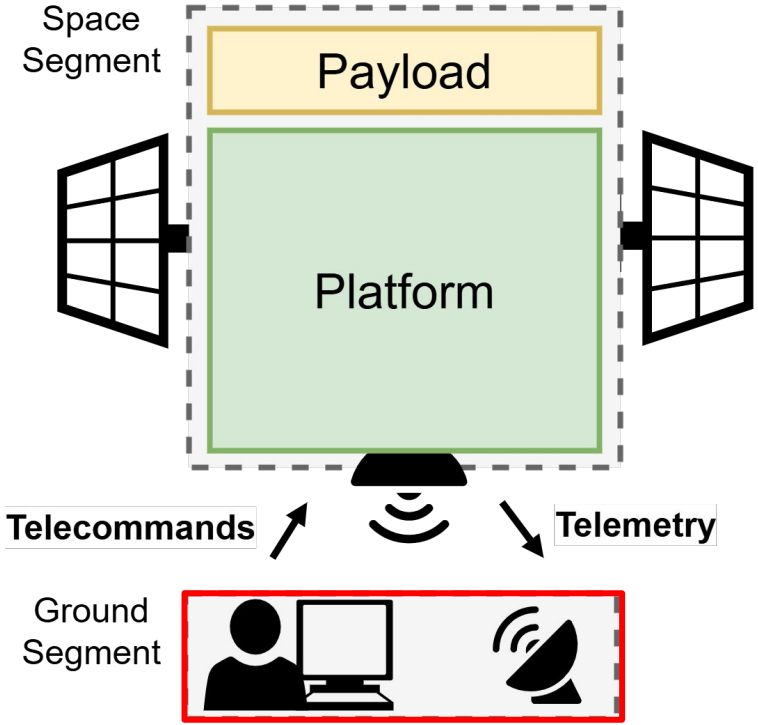
Background: Anatomy of a Satellite Mission



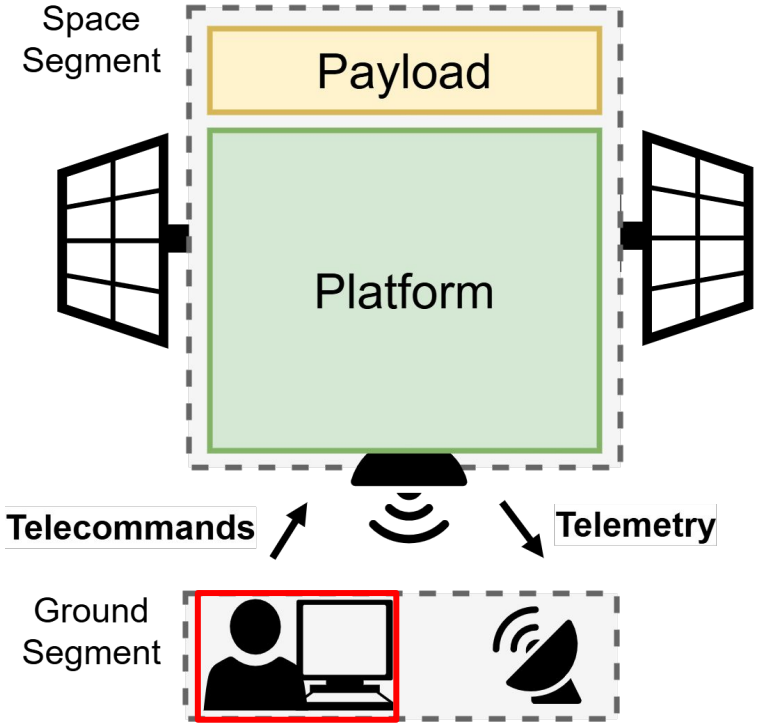
Background: Anatomy of a Satellite Mission



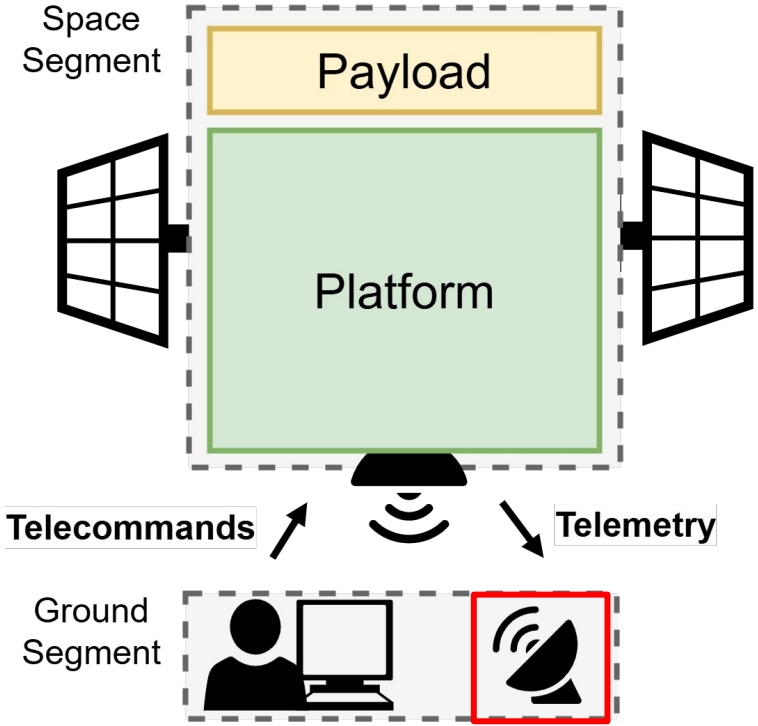
Background: Anatomy of a Satellite Mission



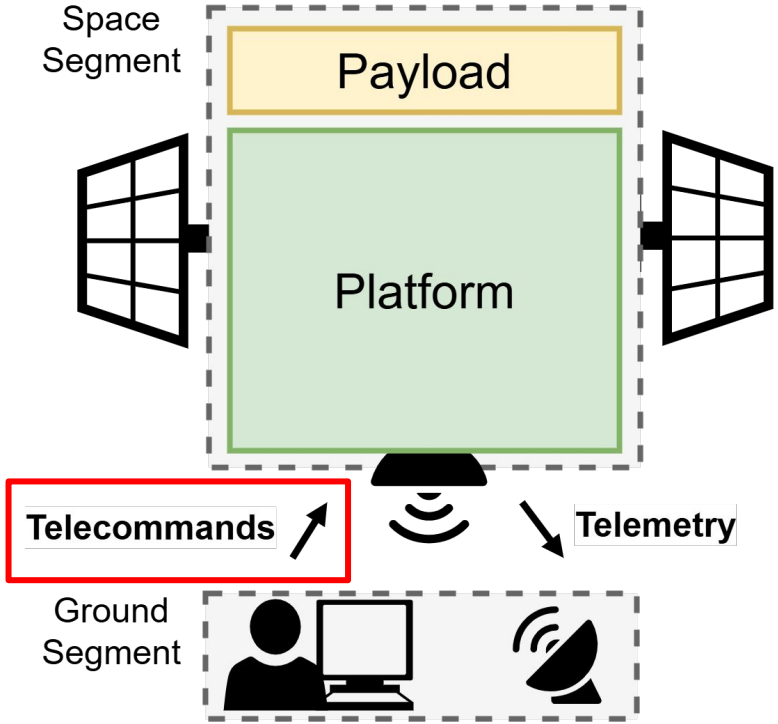
Background: Anatomy of a Satellite Mission



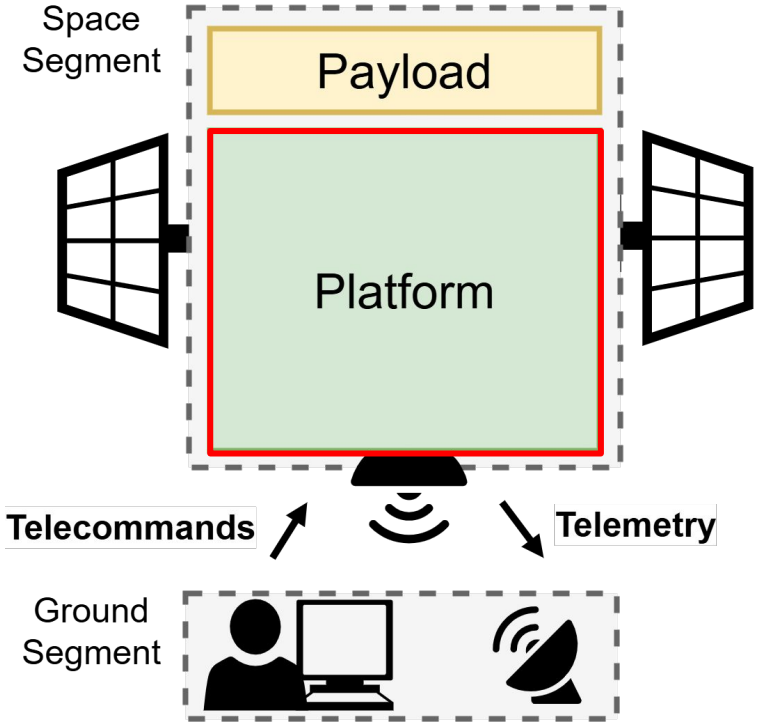
Background: Anatomy of a Satellite Mission



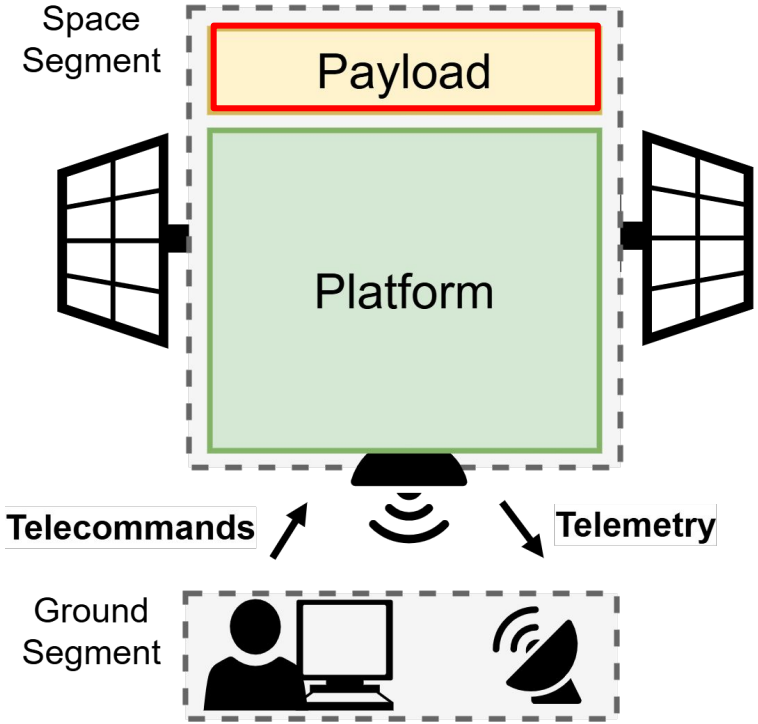
Background: Anatomy of a Satellite Mission



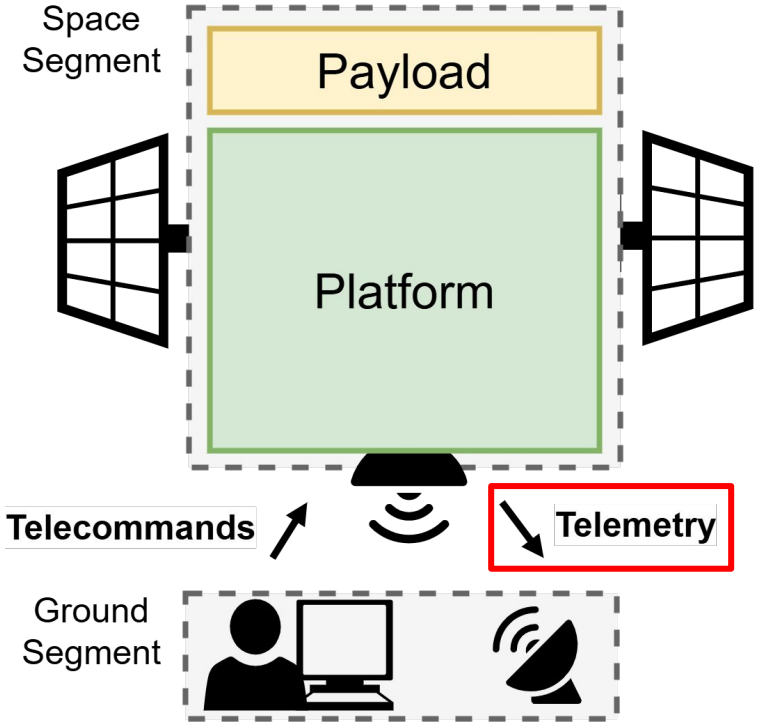
Background: Anatomy of a Satellite Mission



Background: Anatomy of a Satellite Mission



Background: Anatomy of a Satellite Mission



Background: Refresher on Honeypots

- Decoy computer system

Background: Refresher on Honeypots

- Decoy computer system
- Attracts malicious actors

Background: Refresher on Honeypots

- Decoy computer system
- Attracts malicious actors
- Record all interaction data

Background: Refresher on Honeypots

- Decoy computer system
- Attracts malicious actors
- Record all interaction data
- Analyze data to obtain knowledge

Background: Refresher on Honeypots

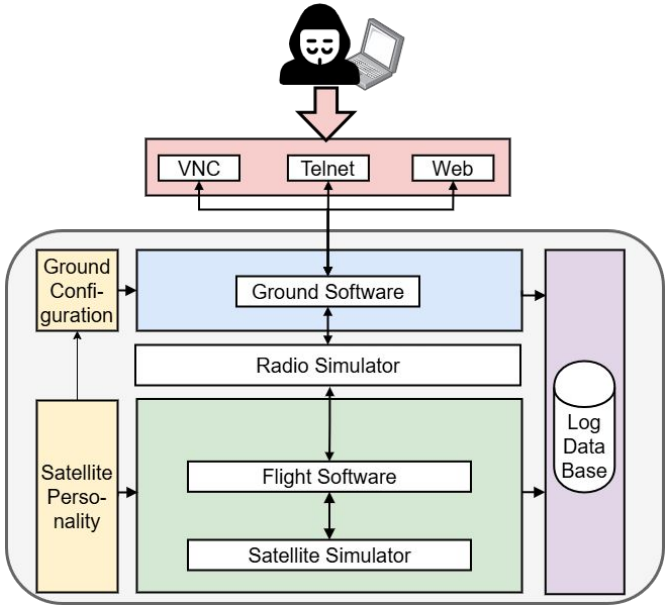
- Decoy computer system
- Attracts malicious actors
- Record all interaction data
- Analyze data to obtain knowledge
- There is no satellite honeypot!

What is the problem?

There is no way to collect data regarding cyberattacks that target satellites.

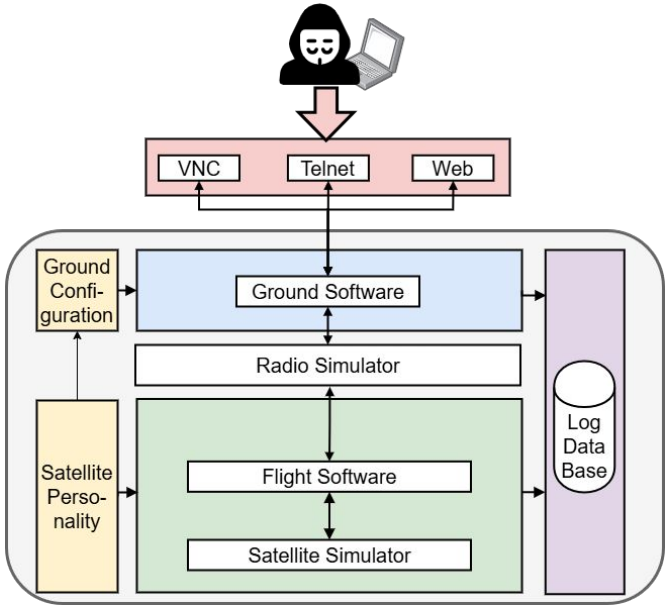
Our solution: HoneySat

- Honeypot that multiple real satellite missions



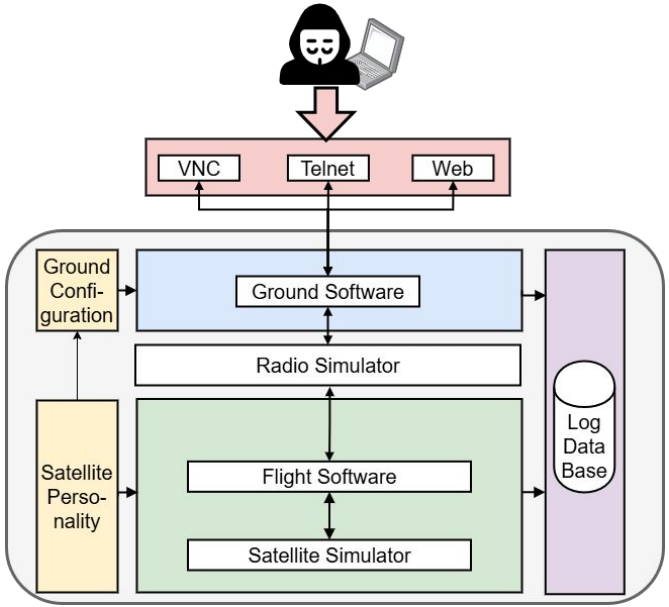
Our solution: HoneySat

- Honeypot that multiple real satellite missions
- Accessible via the Internet



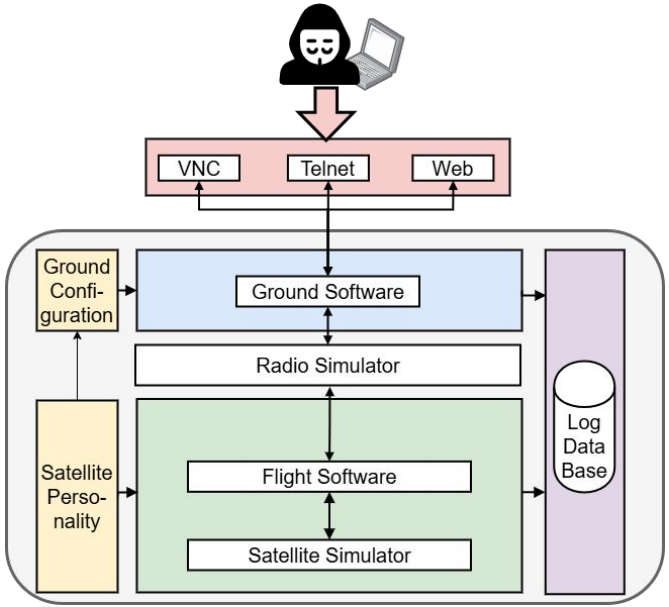
Our solution: HoneySat

- Honeypot that multiple real satellite missions
- Accessible via the Internet
- Uses real satellite software



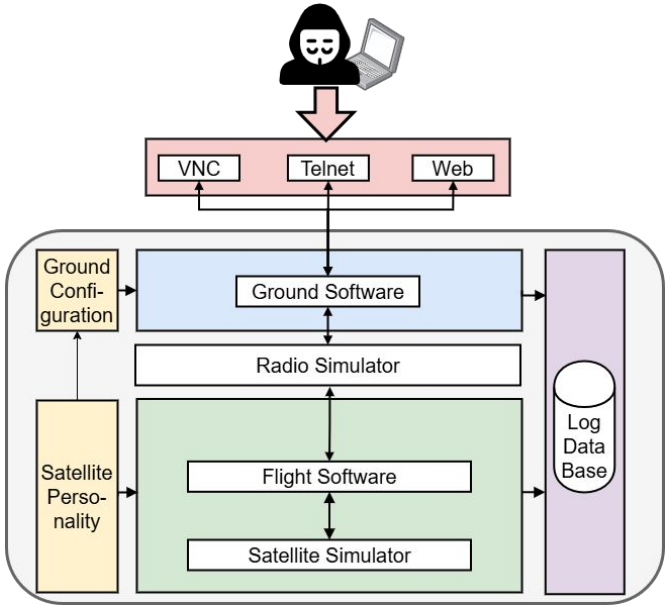
Our solution: HoneySat

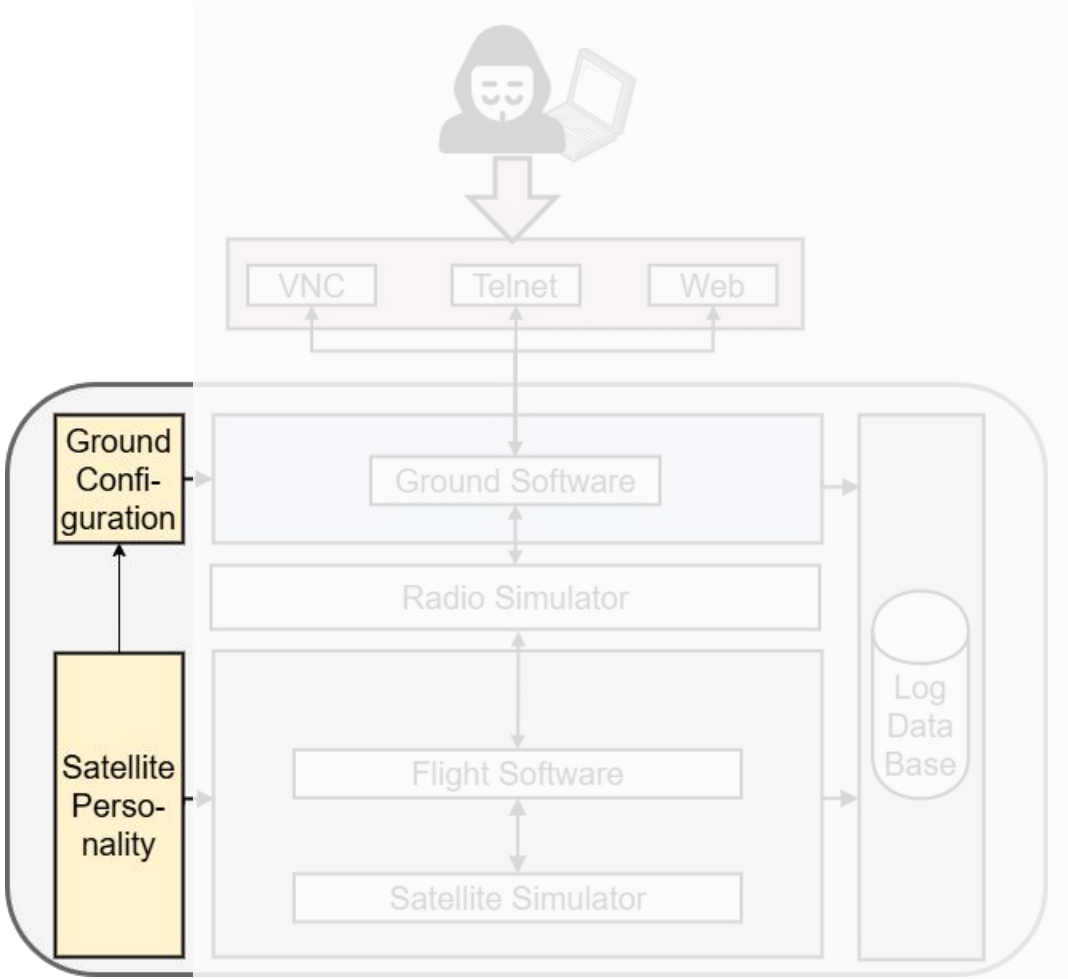
- Honeypot that multiple real satellite missions
- Accessible via the Internet
- Uses real satellite software
- Simulates space physics (orbital mechanics)

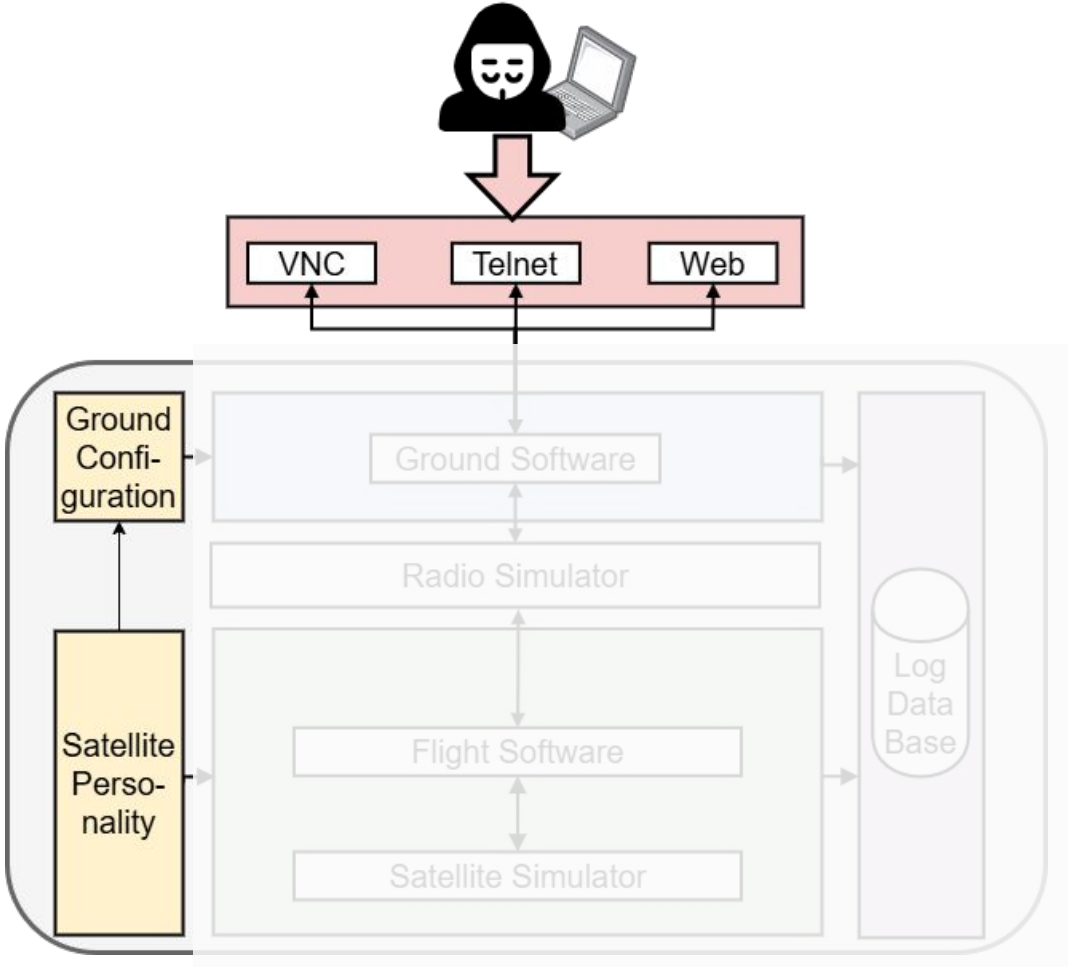


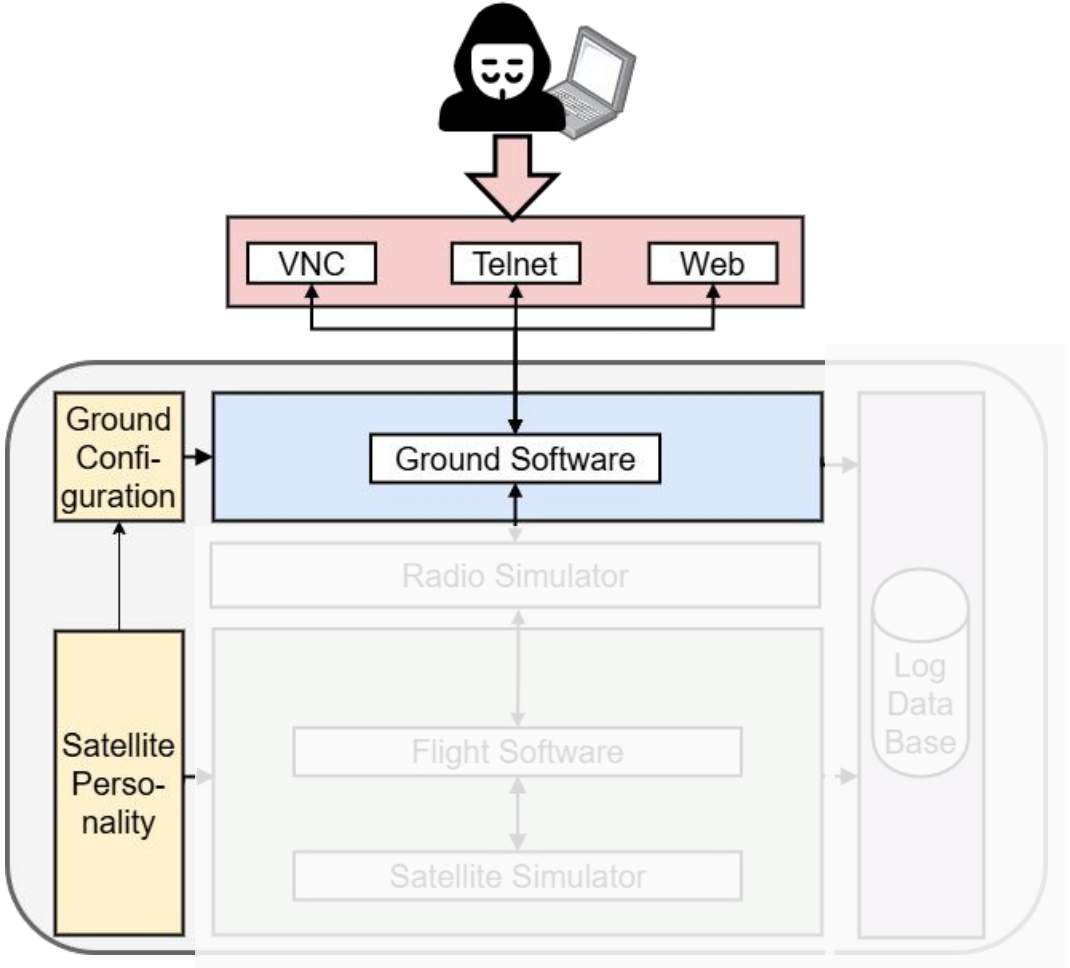
Our solution: HoneySat

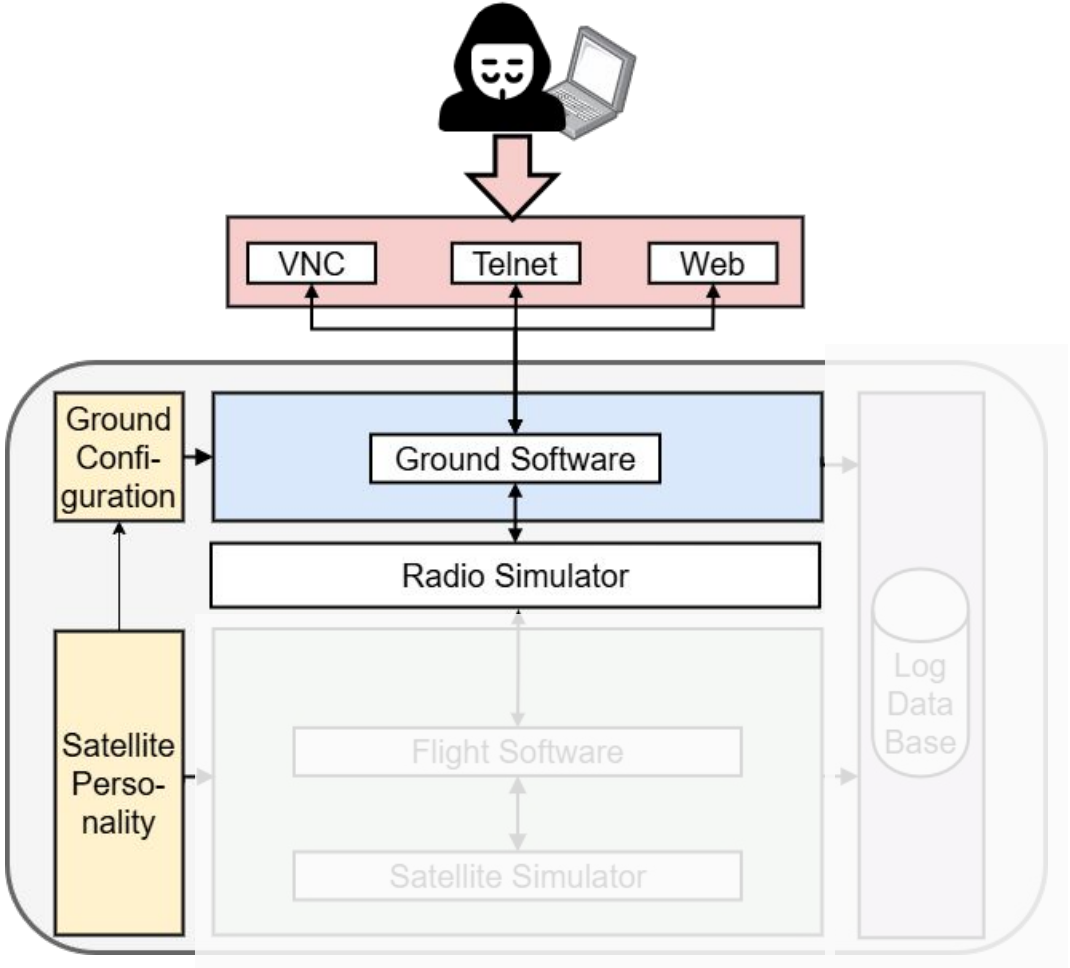
- Honeypot that multiple real satellite missions
- Accessible via the Internet
- Uses real satellite software
- Simulates space physics (orbital mechanics)
- Collects real-world satellite cyberattack data

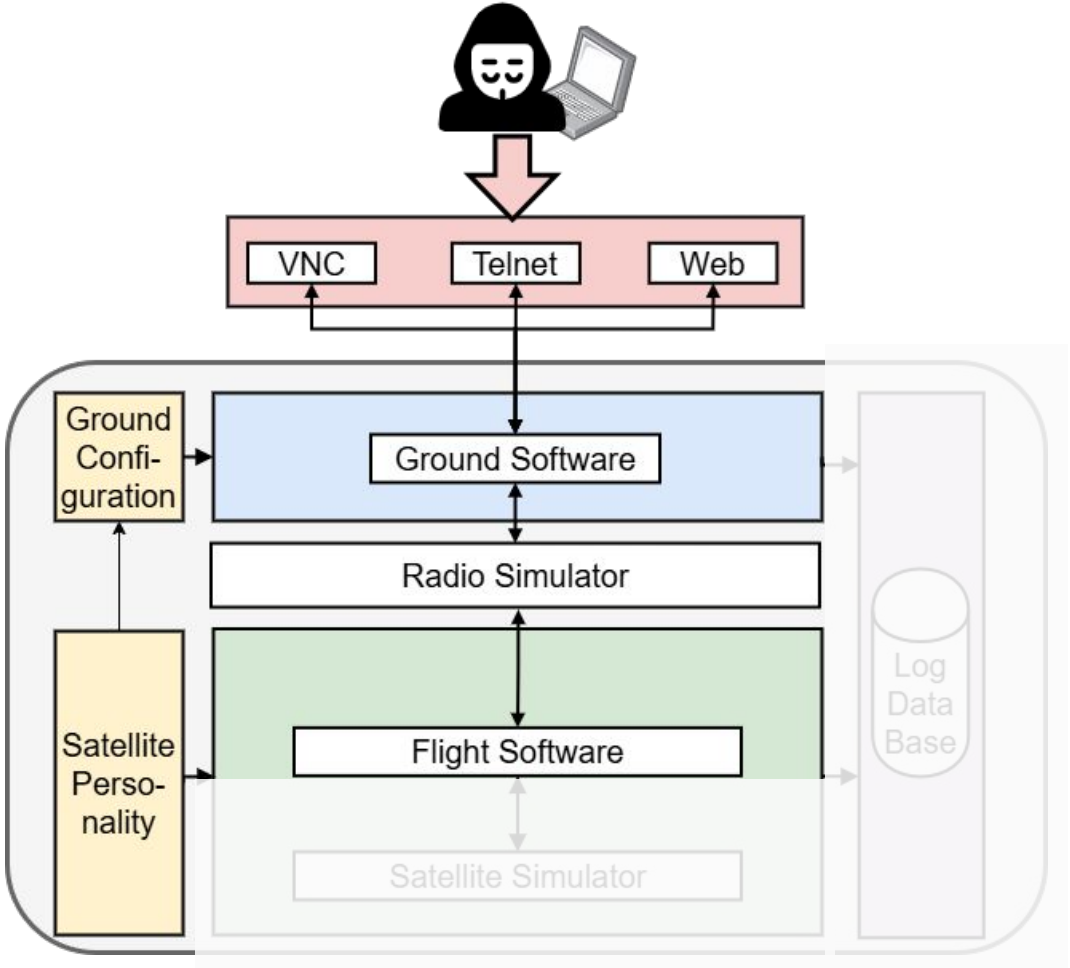


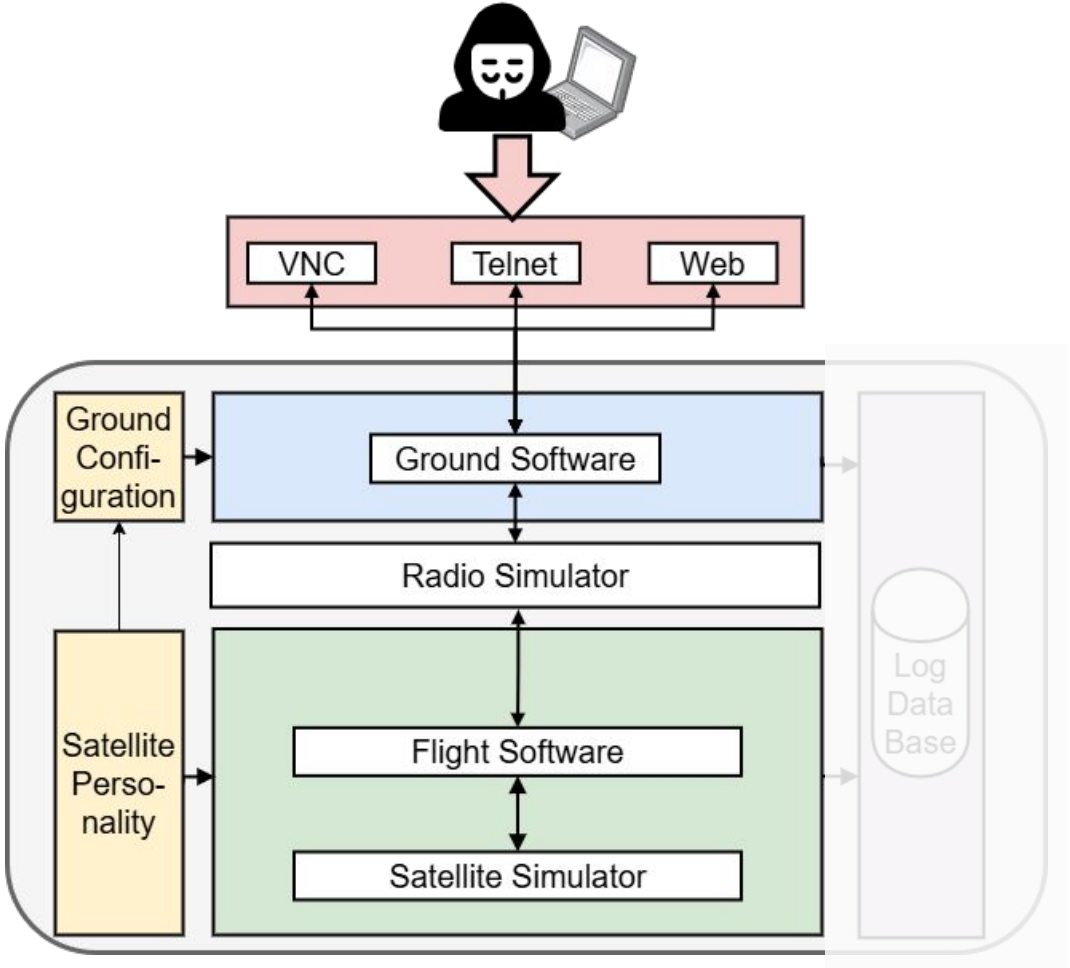

VNC
Telnet
Web
Ground Confi-guration
Ground Software
Radio Simulator
Log Data Base
Satellite Perso-nality
Flight Software
Satellite Simulator

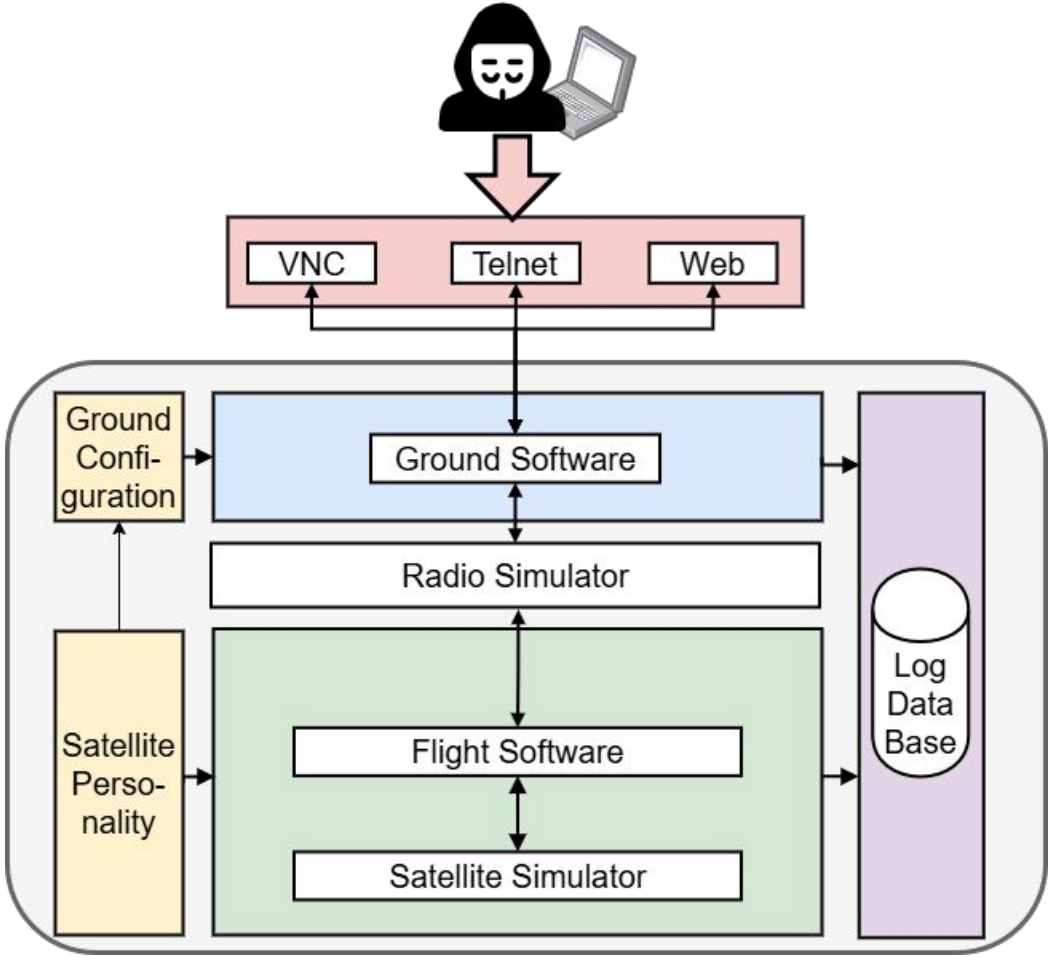

VNC
Telnet
Web
Ground Confi-guration
Satellite Perso-nality
Ground Software
Radio Simulator
Flight Software
Satellite Simulator
Log Data Base


VNC
Telnet
Web
Ground Confi-guration
Ground Software
Radio Simulator
Log Data Base
Satellite Perso-nality
Flight Software
Satellite Simulator


VNC
Telnet
Web
Ground Confi-guration
Ground Software
Radio Simulator
Satellite Perso-nality
Flight Software
Satellite Simulator
Log Data Base


VNC
Telnet
Web
Ground Confi-guration
Ground Software
Radio Simulator
Satellite Perso-nality
Flight Software
Log Data Base
Satellite Simulator


VNC
Telnet
Web
Ground Confi-guration
Ground Software
Radio Simulator
Satellite Perso-nality
Flight Software
Satellite Simulator
Log Data Base


VNC
Telnet
Web
Ground Confi-guration
Ground Software
Radio Simulator
Satellite Perso-nality
Flight Software
Satellite Simulator
Log Data Base

How did we simulate space conditions?

- We developed a Python library: Satellite Simulator

How did we simulate space conditions?

- We developed a Python library: Satellite Simulator
- We use existing data on real satellites' orbital mechanics

How did we simulate space conditions?

- We developed a Python library: Satellite Simulator
- We use existing data on real satellites' orbital mechanics
- We simulate 6 physical processes:

How did we simulate space conditions?

- We developed a Python library: Satellite Simulator
- We use existing data on real satellites' orbital mechanics
- We simulate 6 physical processes:
  - Satellite's orbit
  - Battery
  - 3D-space orientation
  - Temperature
  - Magnetic field
  - Payload

How did we evaluate HoneySat?

1. Surveyed real-world satellite operators

How did we evaluate HoneySat?

1. Surveyed real-world satellite operators
2. Deployment over the Internet to get real-world interactions

How did we evaluate HoneySat?

1. Surveyed real-world satellite operators
2. Deployment over the Internet to get real-world interactions
3. Tested simulating multiple satellites

How did we evaluate HoneySat?

1. **Surveyed real-world satellite operators**
2. **Deployment over the Internet to get real-world interactions**
3. Tested simulating multiple satellites

What did we find?

- We surveyed 14 experienced satellite operators and ask them if our honeypot was realistic

What did we find?

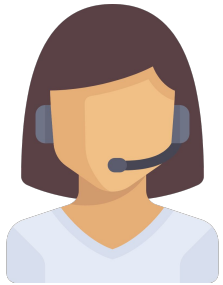
- We surveyed 14 experienced satellite operators and ask them if our honeypot was realistic
- 57.1% said that HoneySat's telemetry is realistic

What did we find?

- We surveyed 14 experienced satellite operators and ask them if our honeypot was realistic
- 57.1% said that HoneySat's telemetry is realistic
- 64.2% said that HoneySat's communication simulation is realistic

What did we find?

- We surveyed 14 experienced satellite operators and ask them if our honeypot was realistic
- 57.1% said that HoneySat's telemetry is realistic
- 64.2% said that HoneySat's communication simulation is realistic
- 71.4% said that HoneySat's overall simulation is realistic and deceiving



What did we find?

- We deployed HoneySat over the Internet to attract adversaries

What did we find?

- We deployed HoneySat over the Internet to attract adversaries
- Deployment lasted 8 months

What did we find?

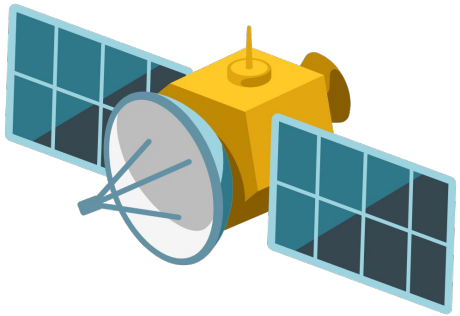
- We deployed HoneySat over the Internet to attract adversaries
- Deployment lasted 8 months
- HoneySat captured 4 real-world telecommands

What did we find?

- We deployed HoneySat over the Internet to attract adversaries
- Deployment lasted 8 months
- HoneySat captured 4 real-world telecommands
- One adversary interacted with HoneySat for 2 hours

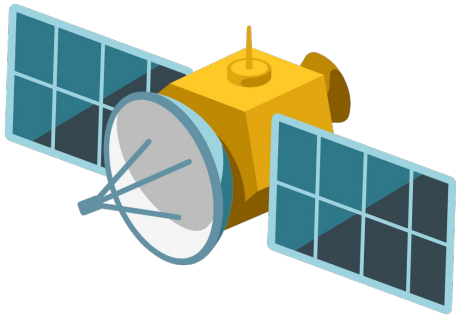
Conclusion: HoneySat

- First satellite honeypot ever



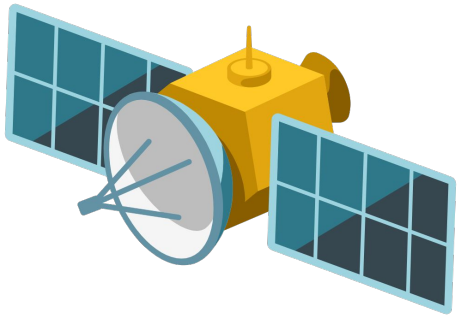
Conclusion: HoneySat

- First satellite honeypot ever
- Simulates multiple types of satellites (e.g. NASA)



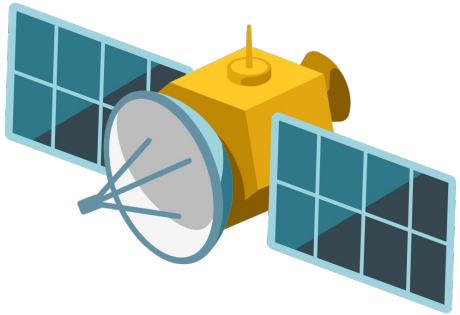
Conclusion: HoneySat

- First satellite honeypot ever
- Simulates multiple types of satellites (e.g. NASA)
- Satellite operators said the simulation is highly realistic



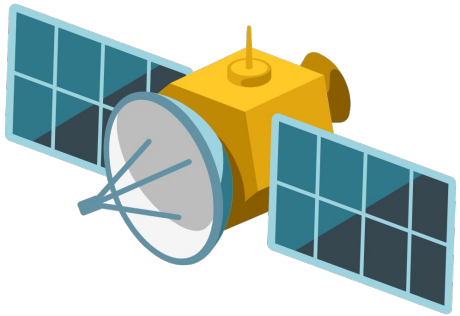
Conclusion: HoneySat

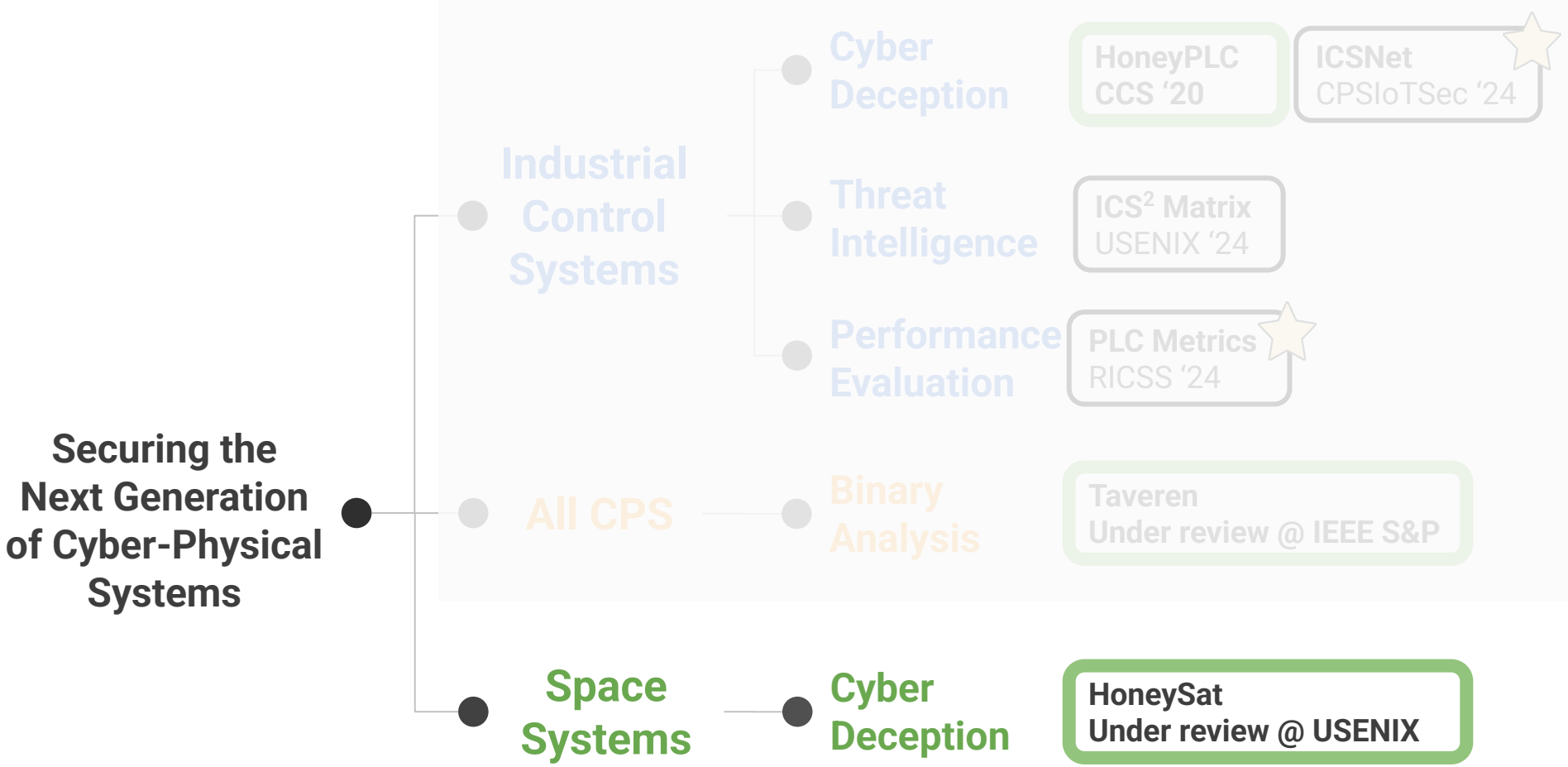
- First satellite honeypot ever
- Simulates multiple types of satellites (e.g. NASA)
- Satellite operators said the simulation is highly realistic
- Captured one of the first-ever data on satellite security

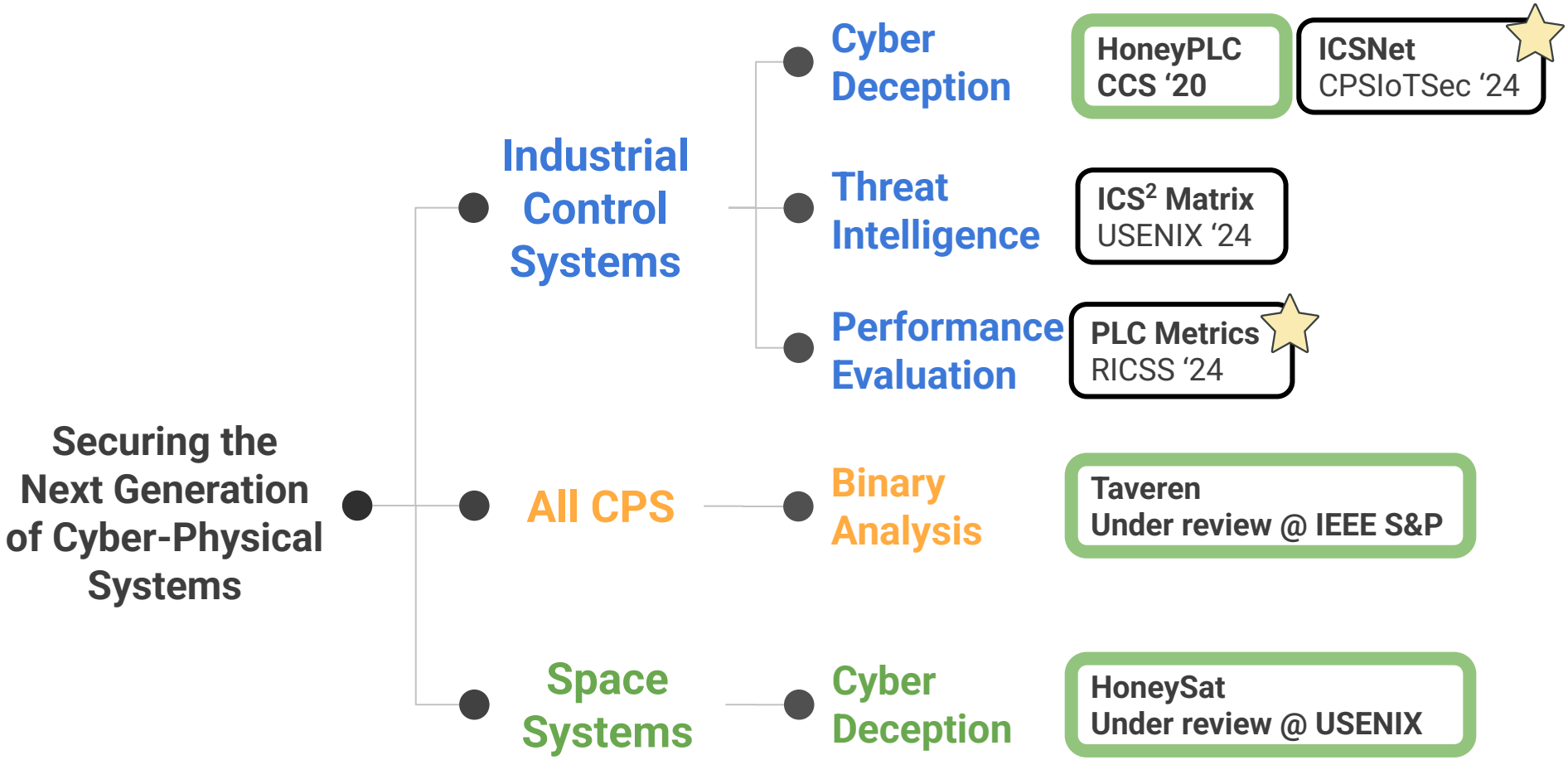


Conclusion: HoneySat

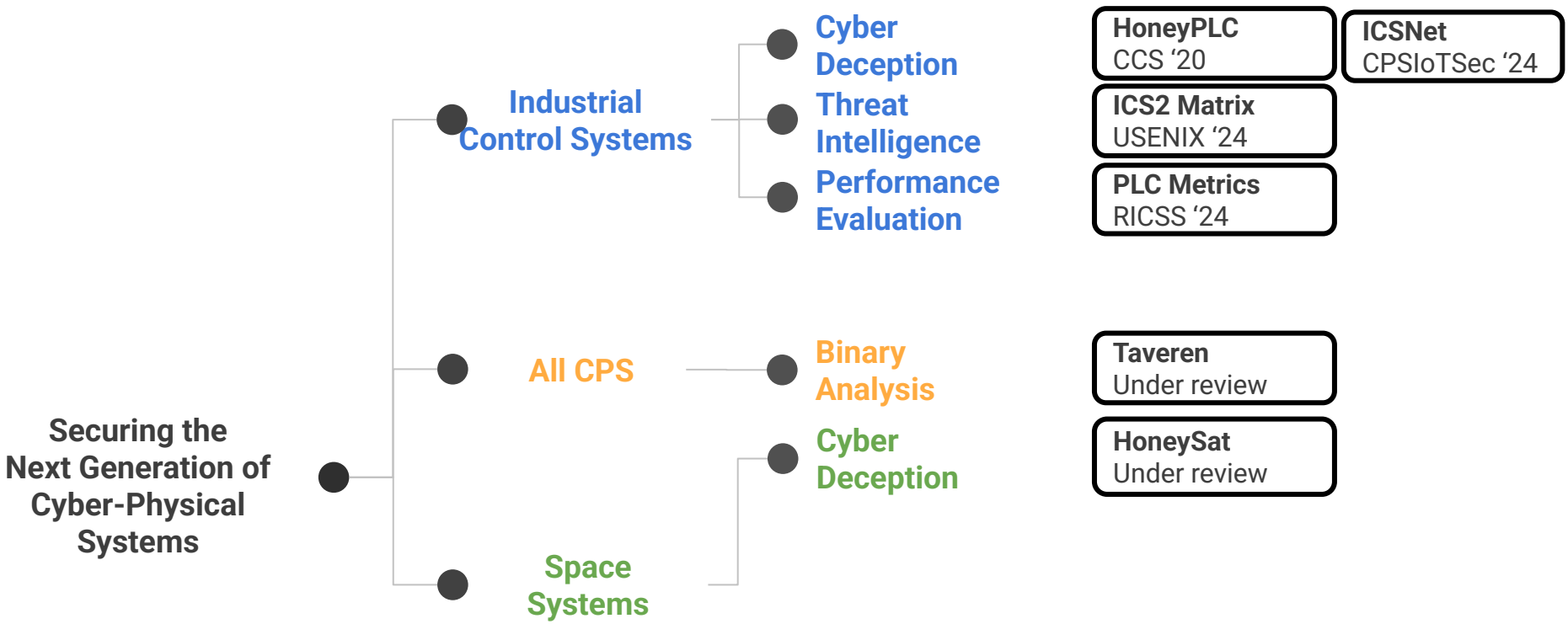
- First satellite honeypot ever
- Simulates multiple types of satellites (e.g. NASA)
- Satellite operators said the simulation is highly realistic
- Captured one of the first-ever data on satellite security
- Deployed by the European Space Agency

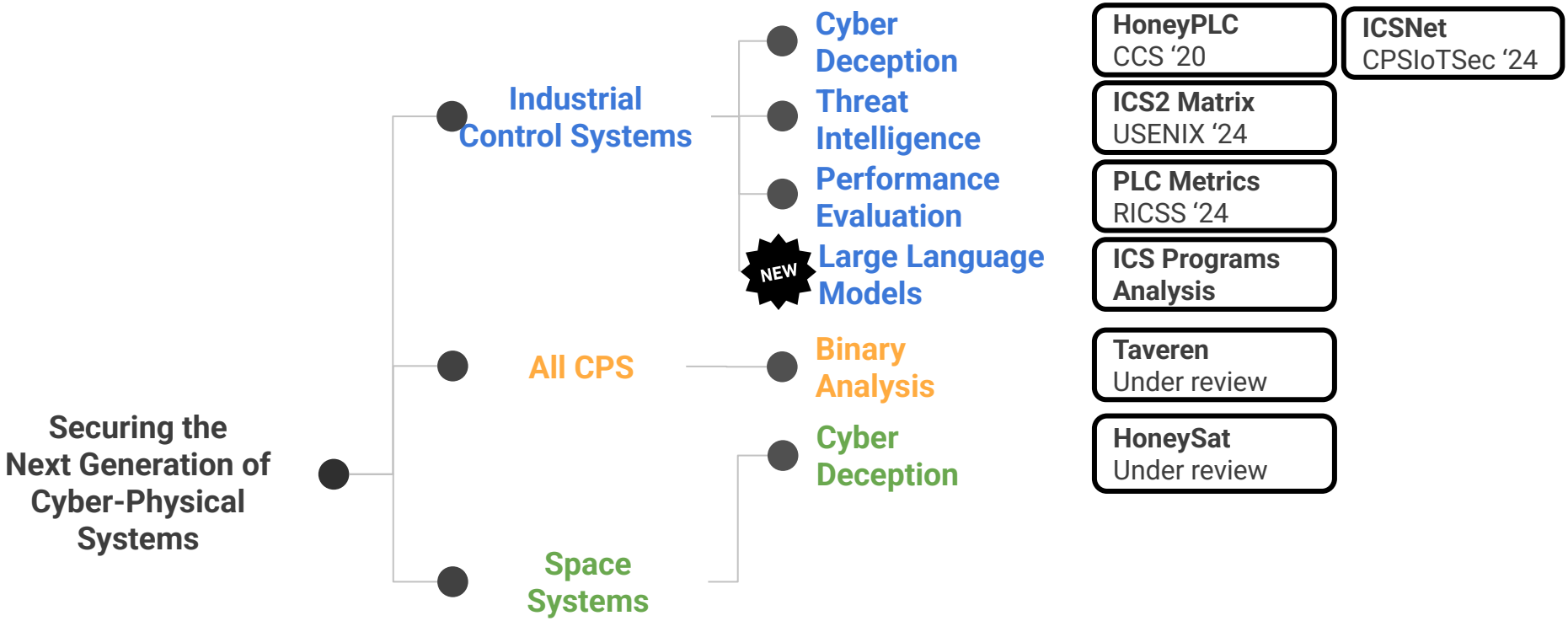


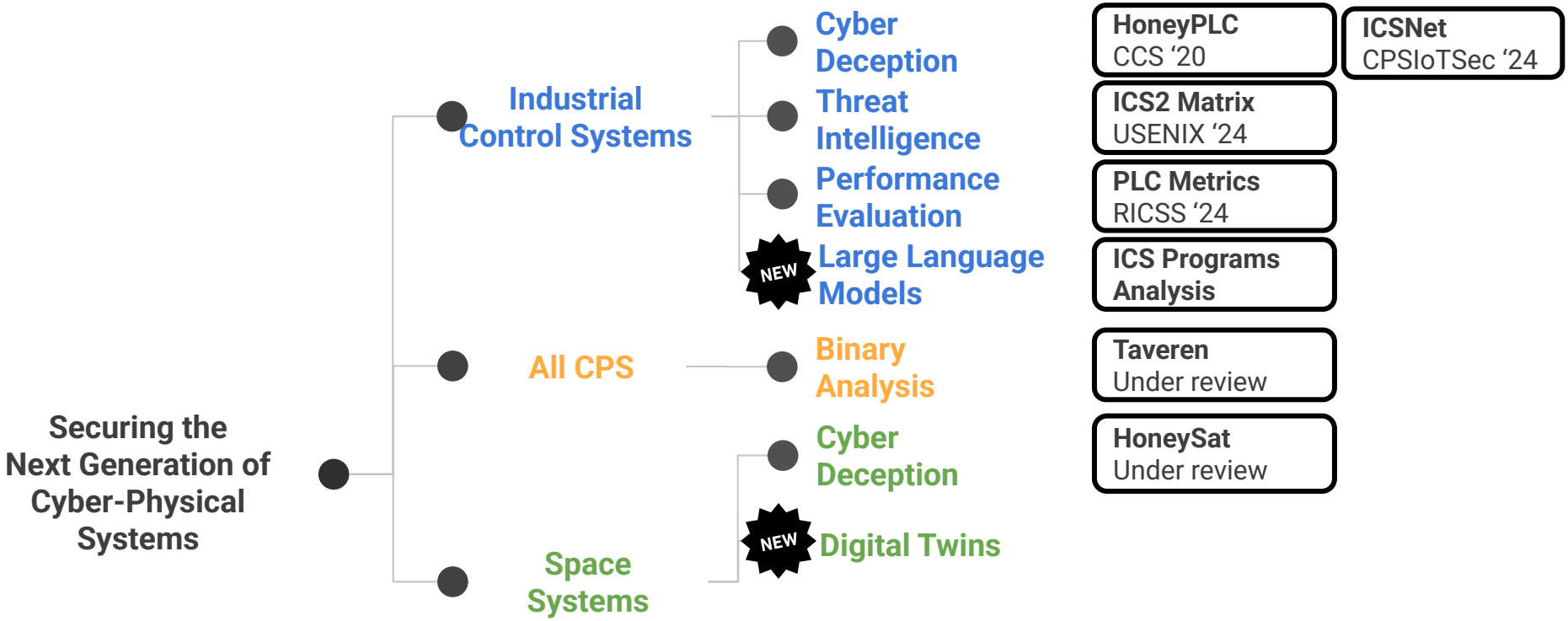

Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
Threat Intelligence
ICS² Matrix
USENIX '24
Performance Evaluation
PLC Metrics
RICSS '24
All CPS
Binary Analysis
Taveren
Under review @ IEEE S&P
Space Systems
Cyber Deception
HoneySat
Under review @ USENIX

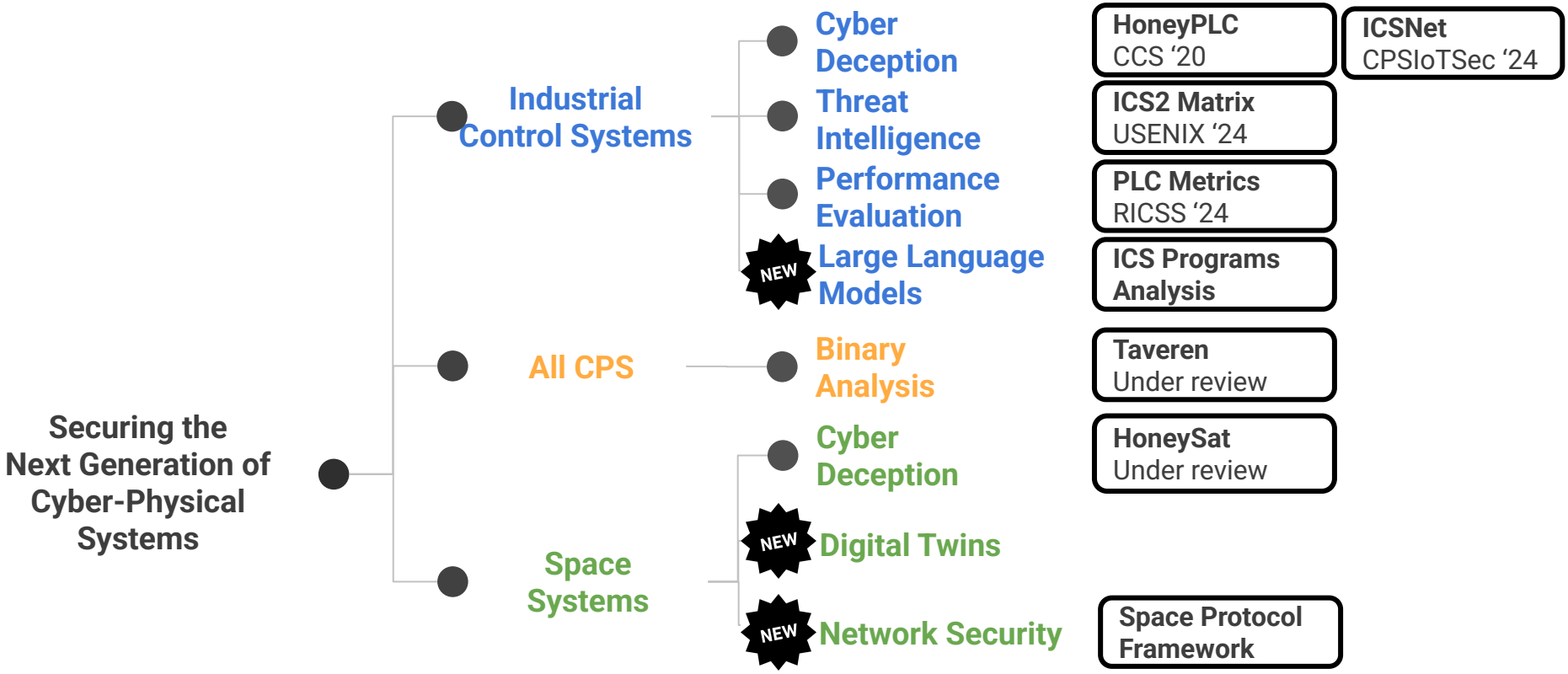

Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
Threat Intelligence
ICS² Matrix
USENIX '24
Performance Evaluation
PLC Metrics
RICSS '24
All CPS
Binary Analysis
Taveren
Under review @ IEEE S&P
Space Systems
Cyber Deception
HoneySat
Under review @ USENIX

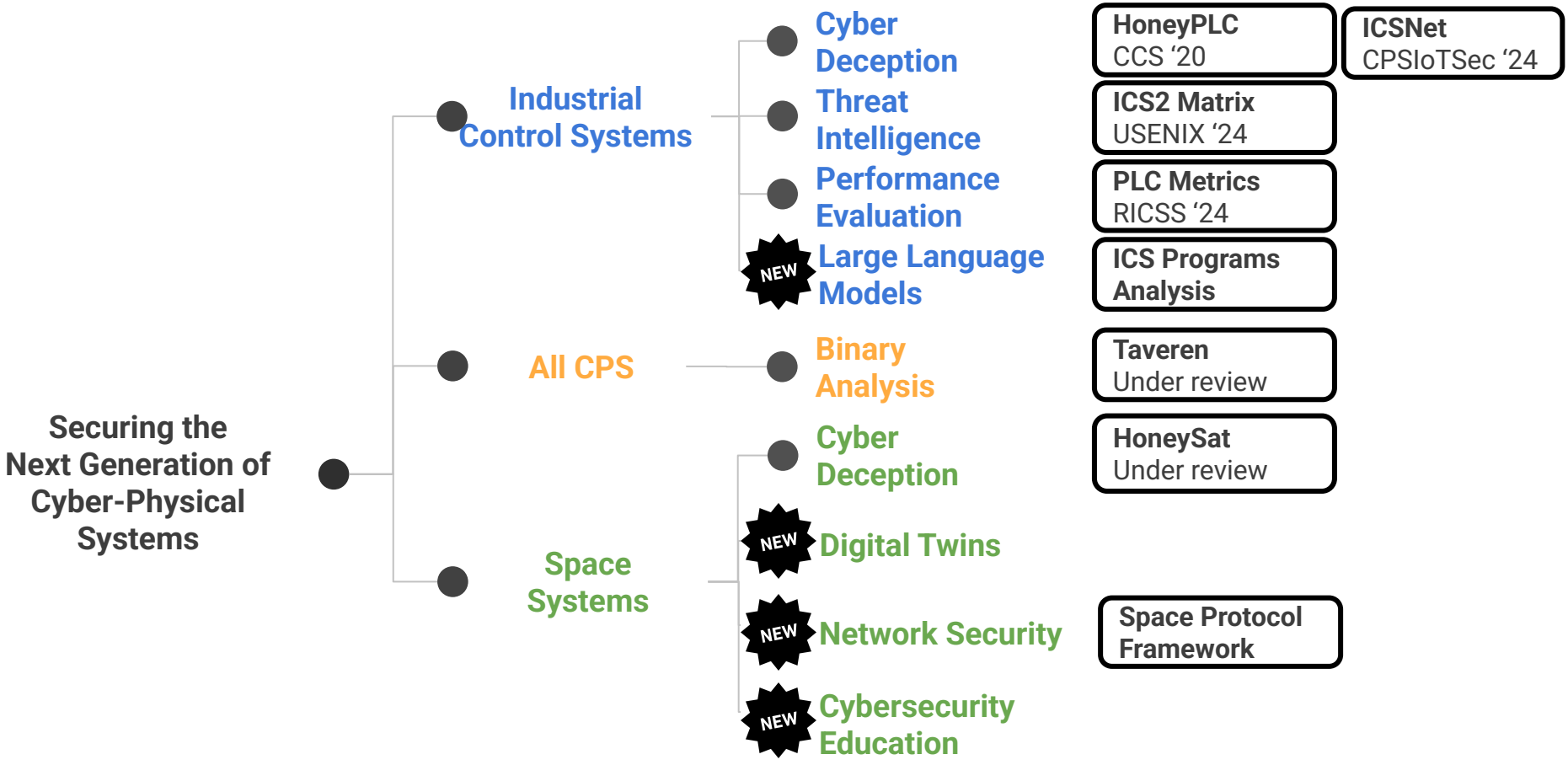
Future Research

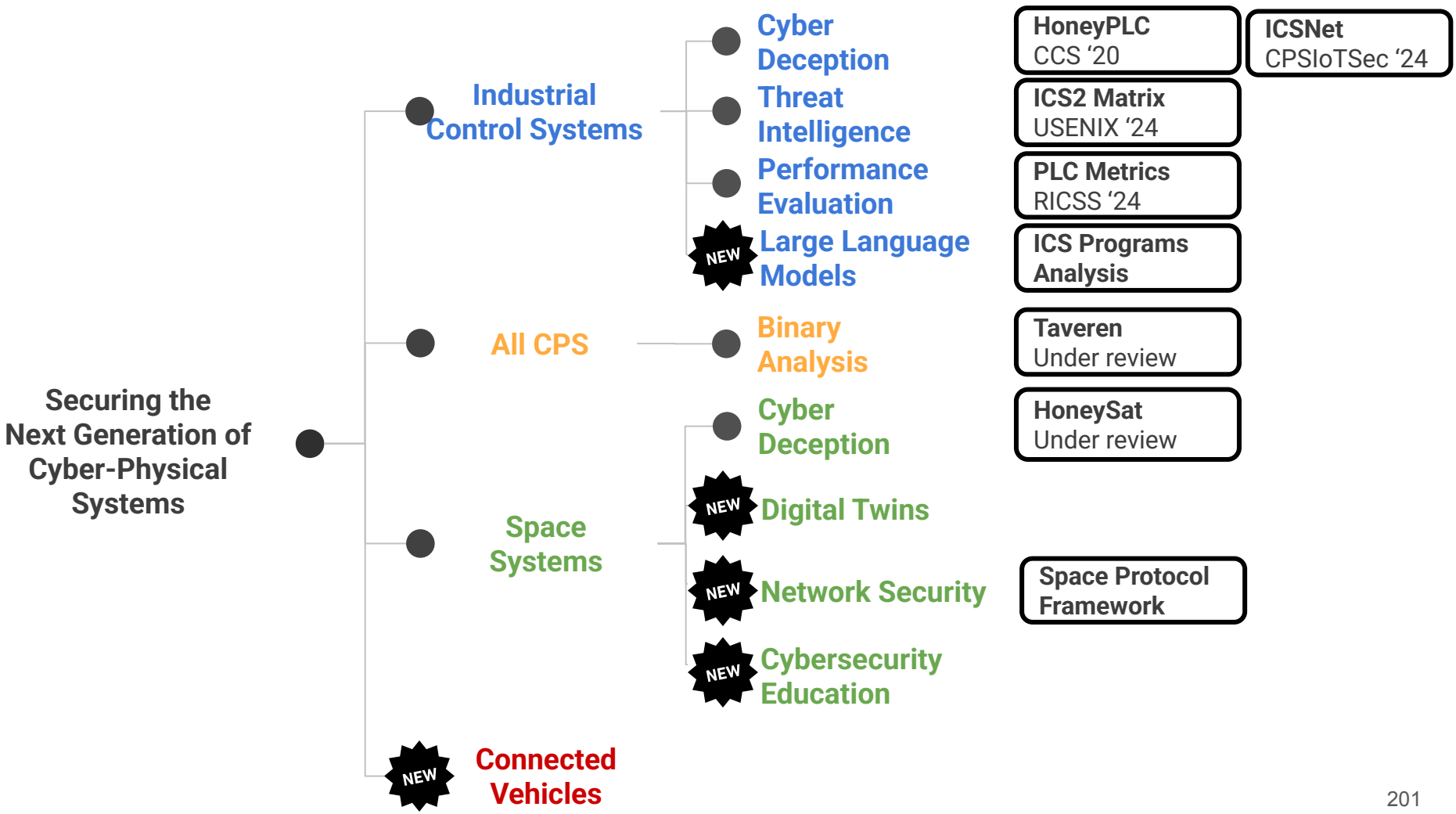

Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
Threat Intelligence
Performance Evaluation
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
ICS2 Matrix
USENIX '24
PLC Metrics
RICSS '24
All CPS
Binary Analysis
Taveren
Under review
Space Systems
Cyber Deception
HoneySat
Under review

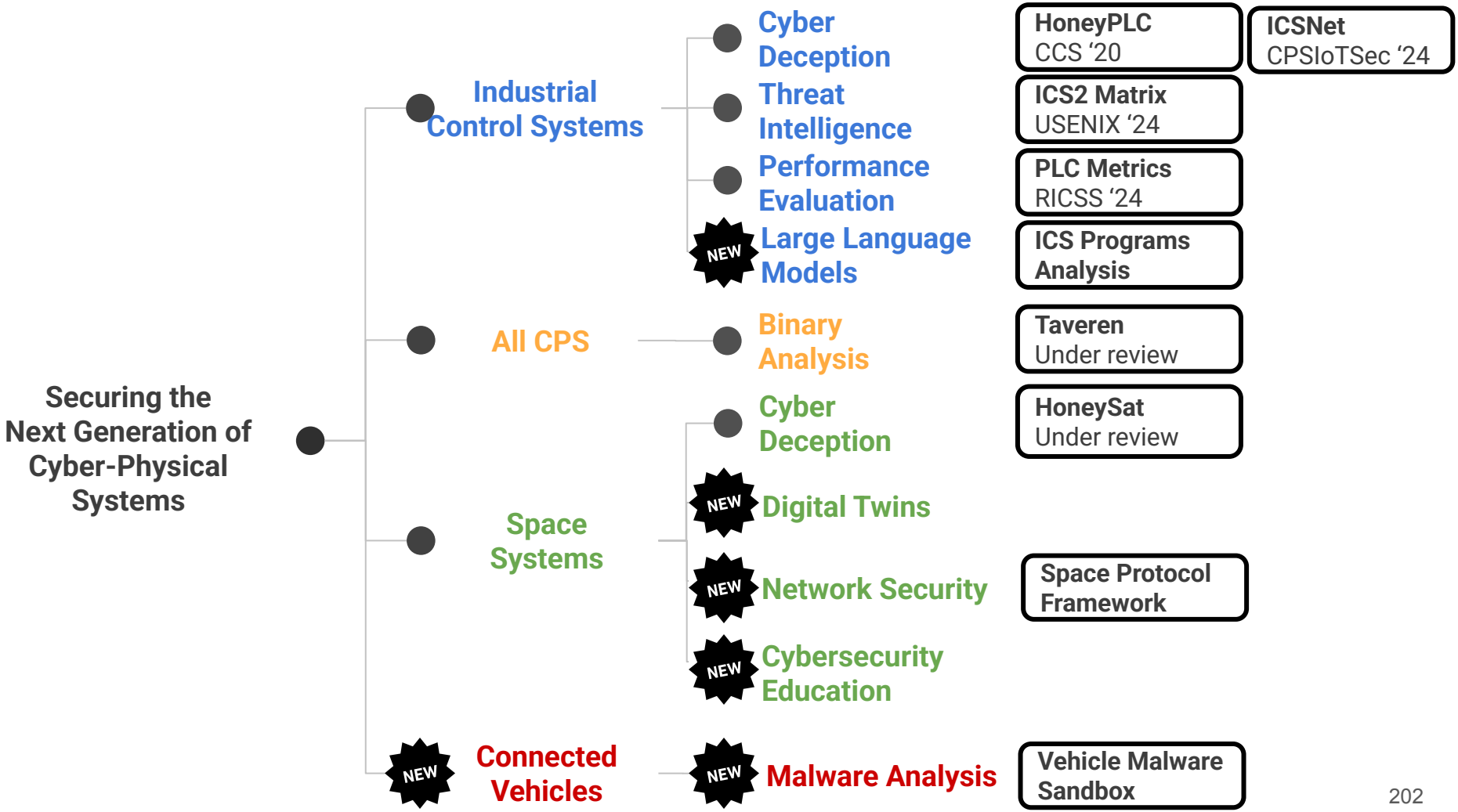

Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
Threat Intelligence
Performance Evaluation
NEW
Large Language Models
All CPS
Binary Analysis
Space Systems
Cyber Deception
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
ICS2 Matrix
USENIX '24
PLC Metrics
RICSS '24
ICS Programs Analysis
Taveren
Under review
HoneySat
Under review

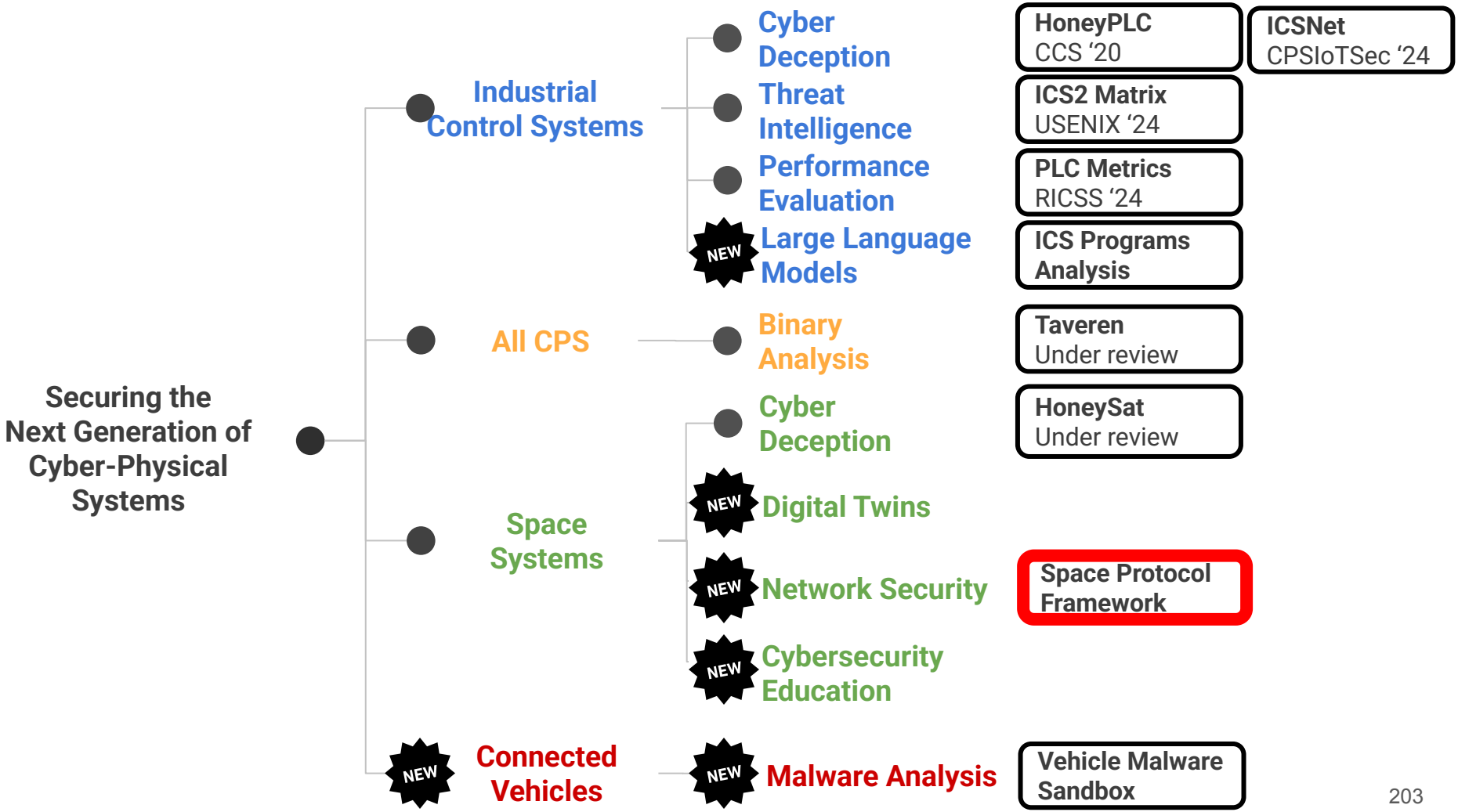

Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
Threat Intelligence
Performance Evaluation
NEW
Large Language Models
All CPS
Binary Analysis
Space Systems
Cyber Deception
NEW
Digital Twins
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
ICS2 Matrix
USENIX '24
PLC Metrics
RICSS '24
ICS Programs Analysis
Taveren
Under review
HoneySat
Under review


Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
Threat Intelligence
Performance Evaluation
NEW
Large Language Models
All CPS
Binary Analysis
Space Systems
Cyber Deception
NEW
Digital Twins
NEW
Network Security
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
ICS2 Matrix
USENIX '24
PLC Metrics
RICSS '24
ICS Programs Analysis
Taveren
Under review
HoneySat
Under review
Space Protocol Framework


Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
Threat Intelligence
Performance Evaluation
NEW
Large Language Models
All CPS
Binary Analysis
Space Systems
Cyber Deception
NEW
Digital Twins
NEW
Network Security
NEW
Cybersecurity Education
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
ICS2 Matrix
USENIX '24
PLC Metrics
RICSS '24
ICS Programs Analysis
Taveren
Under review
HoneySat
Under review
Space Protocol Framework


Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
Threat Intelligence
Performance Evaluation
NEW
Large Language Models
All CPS
Binary Analysis
Space Systems
Cyber Deception
NEW
Digital Twins
NEW
Network Security
NEW
Cybersecurity Education
NEW
Connected Vehicles
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
ICS2 Matrix
USENIX '24
PLC Metrics
RICSS '24
ICS Programs Analysis
Taveren
Under review
HoneySat
Under review
Space Protocol Framework

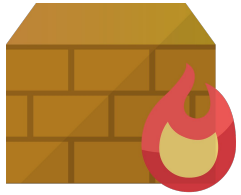

Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
Threat Intelligence
Performance Evaluation
NEW
Large Language Models
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
ICS2 Matrix
USENIX '24
PLC Metrics
RICSS '24
ICS Programs Analysis
All CPS
Binary Analysis
Taveren
Under review
Space Systems
Cyber Deception
HoneySat
Under review
NEW
Digital Twins
NEW
Network Security
Space Protocol Framework
NEW
Cybersecurity Education
NEW
Connected Vehicles
NEW
Malware Analysis
Vehicle Malware Sandbox


Securing the Next Generation of Cyber-Physical Systems
Industrial Control Systems
Cyber Deception
Threat Intelligence
Performance Evaluation
NEW
Large Language Models
HoneyPLC
CCS '20
ICSNet
CPSIoTSec '24
ICS2 Matrix
USENIX '24
PLC Metrics
RICSS '24
ICS Programs Analysis
All CPS
Binary Analysis
Taveren
Under review
Space Systems
Cyber Deception
HoneySat
Under review
NEW
Digital Twins
NEW
Network Security
Space Protocol Framework
NEW
Cybersecurity Education
NEW
Connected Vehicles
NEW
Malware Analysis
Vehicle Malware Sandbox

Space Protocol Security Framework

Space Protocol Security Framework

Space Protocol Security Framework



Space Protocol Security Framework

Space Protocol Security Framework

Collaboration Opportunities

- Gaurav Panwar **(Network Security)**

Collaboration Opportunities

- Gaurav Panwar **(Network Security)**
- Roopa Vishwanathan **(Cryptography)**

Collaboration Opportunities

- Gaurav Panwar **(Network Security)**
- Roopa Vishwanathan **(Cryptography)**
- Jay Misra **(Smart Grid)**

Collaboration Opportunities

- Gaurav Panwar **(Network Security)**
- Roopa Vishwanathan **(Cryptography)**
- Jay Misra **(Smart Grid)**
- Shiva Darian **(Human-Computer Interaction)**

Collaboration Opportunities

- Gaurav Panwar **(Network Security)**
- Roopa Vishwanathan **(Cryptography)**
- Jay Misra **(Smart Grid)**
- Shiva Darian **(Human-Computer Interaction)**
- Huiping Cao (**Machine Learning**)

Funding

- Cyber-Physical Systems (**CPS**)

Funding

- Cyber-Physical Systems (**CPS**)
- Security, Privacy, and Trust in Cyberspace (**SaTC 2.0**)

Funding

- Cyber-Physical Systems (**CPS**)
- Security, Privacy, and Trust in Cyberspace (**SaTC 2.0**)
- Computer and Information Science and Engineering

  Research Expansion Program (**CISE MSI**)

Funding

- Cyber-Physical Systems (**CPS**)
- Security, Privacy, and Trust in Cyberspace (**SaTC 2.0**)
- Computer and Information Science and Engineering Research Expansion Program (**CISE MSI**)
- Faculty Early Career Development Program (**CAREER**)

Funding

- New Mexico Space Grant Consortium

Funding

- New Mexico Space Grant Consortium
- Education Enhancement Grant

Funding

- New Mexico Space Grant Consortium
- Education Enhancement Grant
- Research Initiation Grant (RIG)

Funding

- New Mexico Space Grant Consortium
- Education Enhancement Grant
- Research Initiation Grant (RIG)
- Postdoctoral Fellowship

Funding

- CAHSI-Google Institutional Research Program
- CAHSI REU

Funding

- CAHSI-Google Institutional Research Program
- CAHSI REU

My Research's Broader Impact

Academic Collaborations

Industry Collaborations

DLR Deutsches Zentrum für Luft- und Raumfahrt
German Aerospace Center

MITRE

European Space Agency
Agence spatiale européenne

Open Source Projects

HoneyPLC

HoneySat

ICS^2 Matrix

angr + Taveren

Thank you for listening!

Thank you to all my collaborators and sponsors

Sponsors

CAHSI STUDENT SCHOLARS

CONACYT

SHPE

TEXAS A&M UNIVERSITY CORPUS CHRISTI

Efrén López-Morales

elopezmorales@islander.tamucc.edu

https://efrenlopez.org