SoK: Security of Programmable Logic Controllers

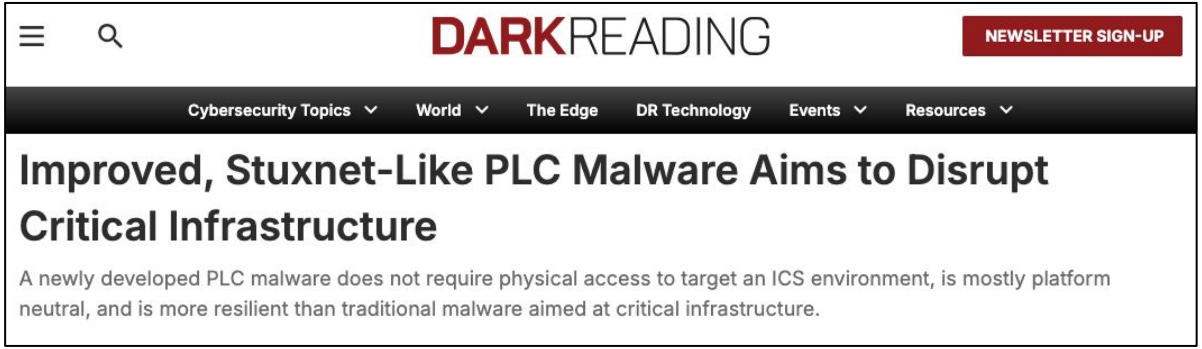
Efrén López-Morales*, Ulysse Planta[†],
Carlos Rubio-Medrano*, Ali Abbasi[†], Alvaro Cardenas[§]

Texas A&M University - Corpus Christi*,
CISPA Helmholtz Center for Information Security[†],
University of California, Santa Cruz[§]

33rd USENIX Security Symposium

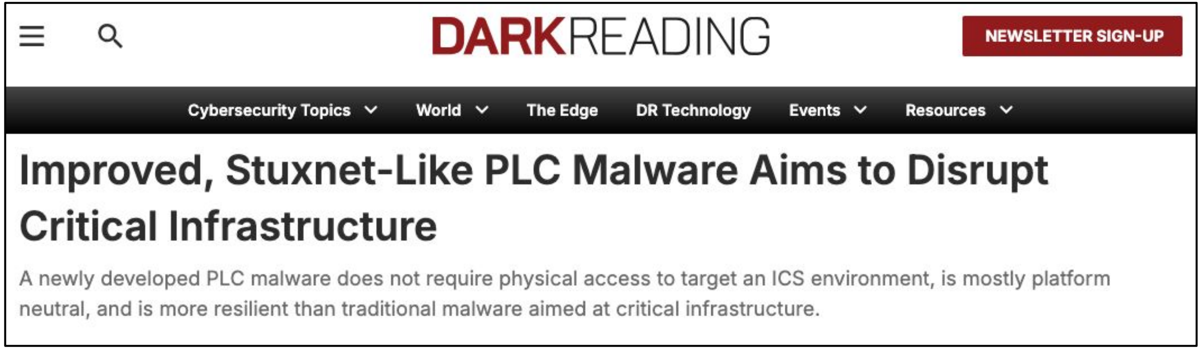
August 16th, 2024

145B
SWEET DEAL
METRO
NO TRESPASSING



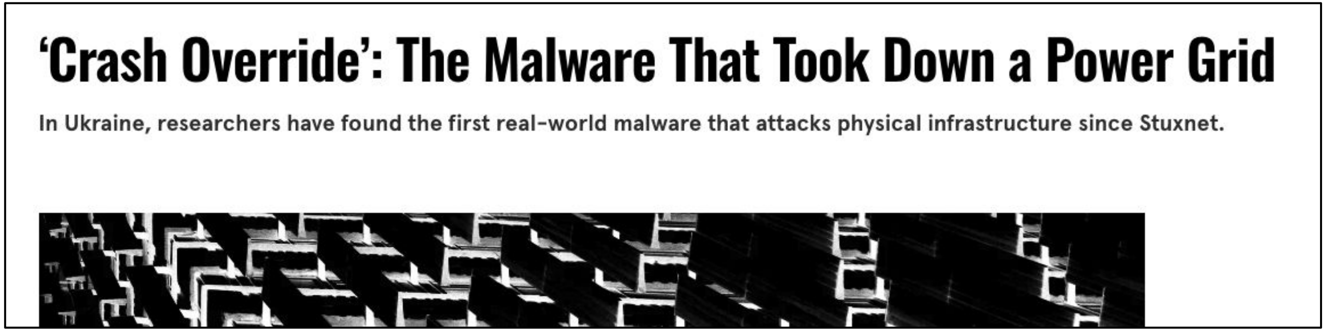
Improved, Stuxnet-Like PLC Malware Aims to Disrupt Critical Infrastructure

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.



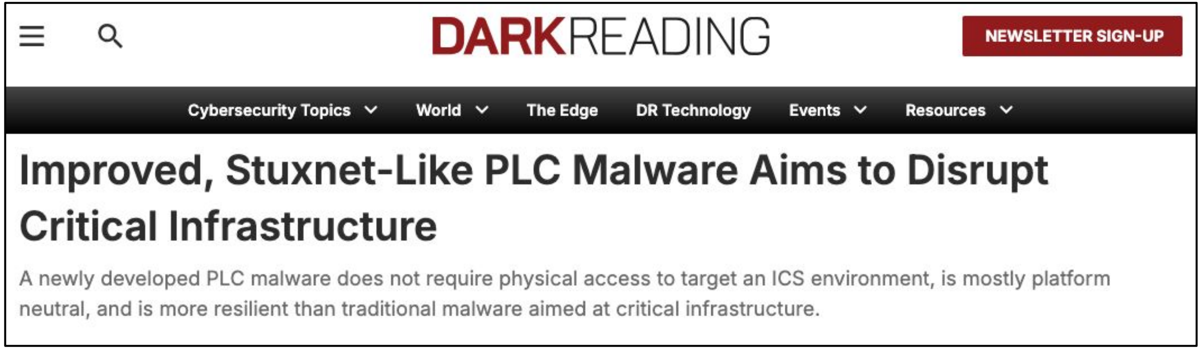
Improved, Stuxnet-Like PLC Malware Aims to Disrupt Critical Infrastructure

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.



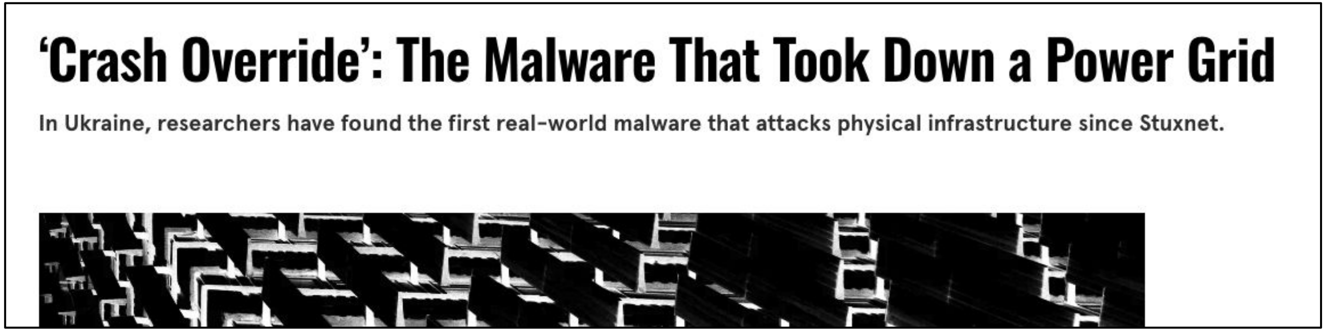
‘Crash Override’: The Malware That Took Down a Power Grid

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



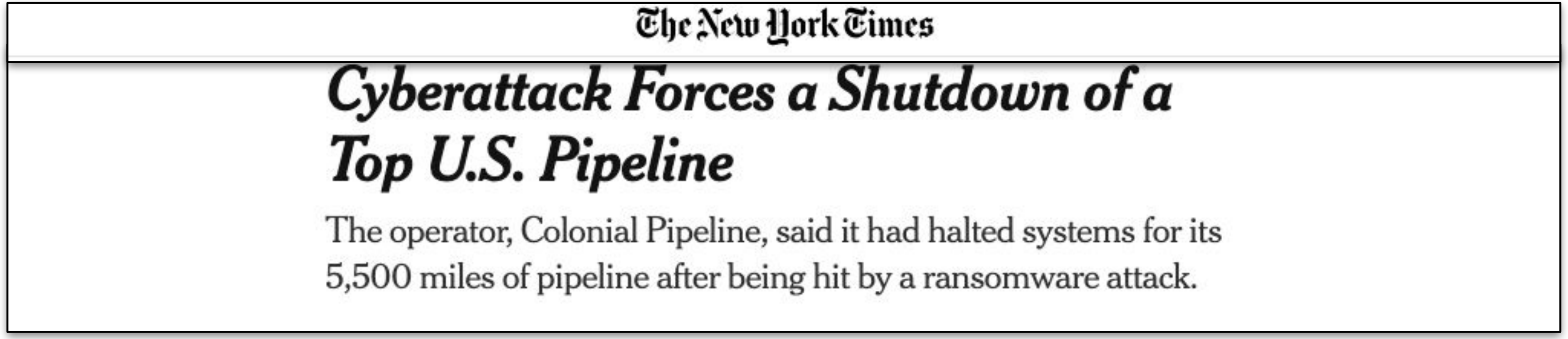
Improved, Stuxnet-Like PLC Malware Aims to Disrupt Critical Infrastructure

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.



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

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.

Background

Programmable Logic Controllers (PLC)

Programmable Logic Controllers (PLC)

- Control physical industrial equipment, e.g., pumps.

Programmable Logic Controllers (PLC)

- Control physical industrial equipment, e.g., pumps.
- Proprietary software and hardware architectures.

Programmable Logic Controllers (PLC)

- Control physical industrial equipment, e.g., pumps.
- Proprietary software and hardware architectures.
- Increasingly interconnected, e.g., cloud.

Programmable Logic Controllers (PLC)

- Control physical industrial equipment, e.g., pumps.
- Proprietary software and hardware architectures.
- Increasingly interconnected, e.g., cloud.
- Yet, little to no built-in security features.

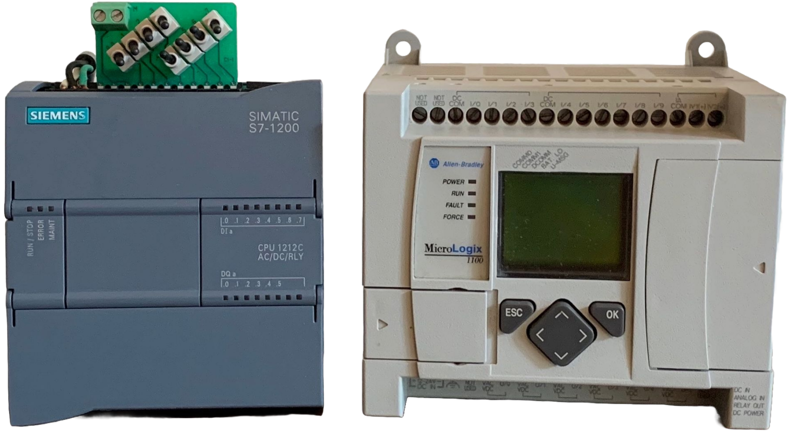
HardPLCs VS SoftPLCs

HardPLCs

SoftPLCs

HardPLCs VS SoftPLCs

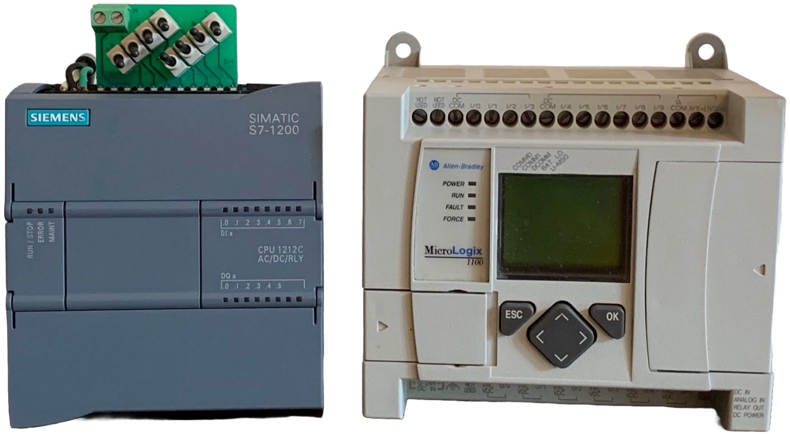
HardPLCs



SoftPLCs

HardPLCs VS SoftPLCs

HardPLCs



SoftPLCs

OPENPLC

TO A MORE
OPEN FUTURE

CODESYS

Problem Statement

Plenty of PLC security research has been produced.

Plenty of PLC security research has been produced.

<u>However, we do not know where the security of PLCs stands and what research directions should (or should not) be taken in the future</u>.

Research Questions

Research Questions

1. What are the available **attack** methods against PLCs?

⚔️

Research Questions

1. What are the available **attack** methods against PLCs?

⚔️

2. What are the available **defense** methods to protect PLCs?

🛡️

Research Questions

1. What are the available **attack** methods against PLCs?

⚔️

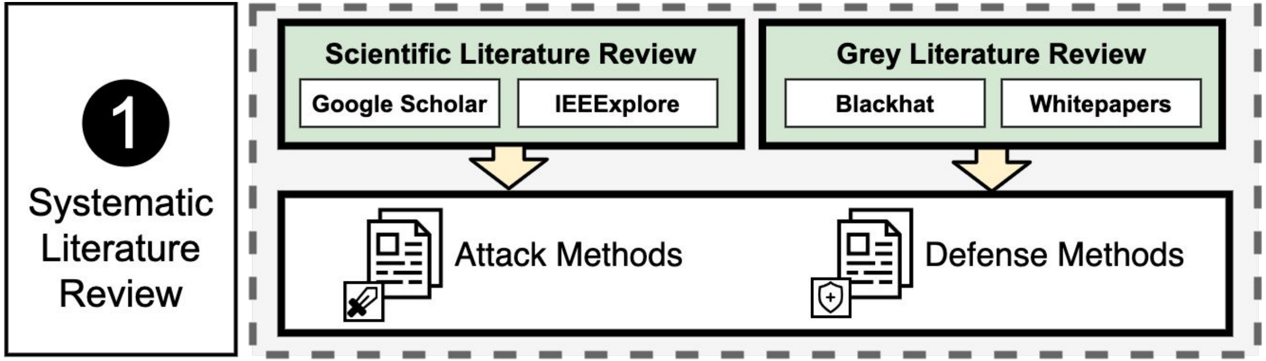
2. What are the available **defense** methods to protect PLCs?

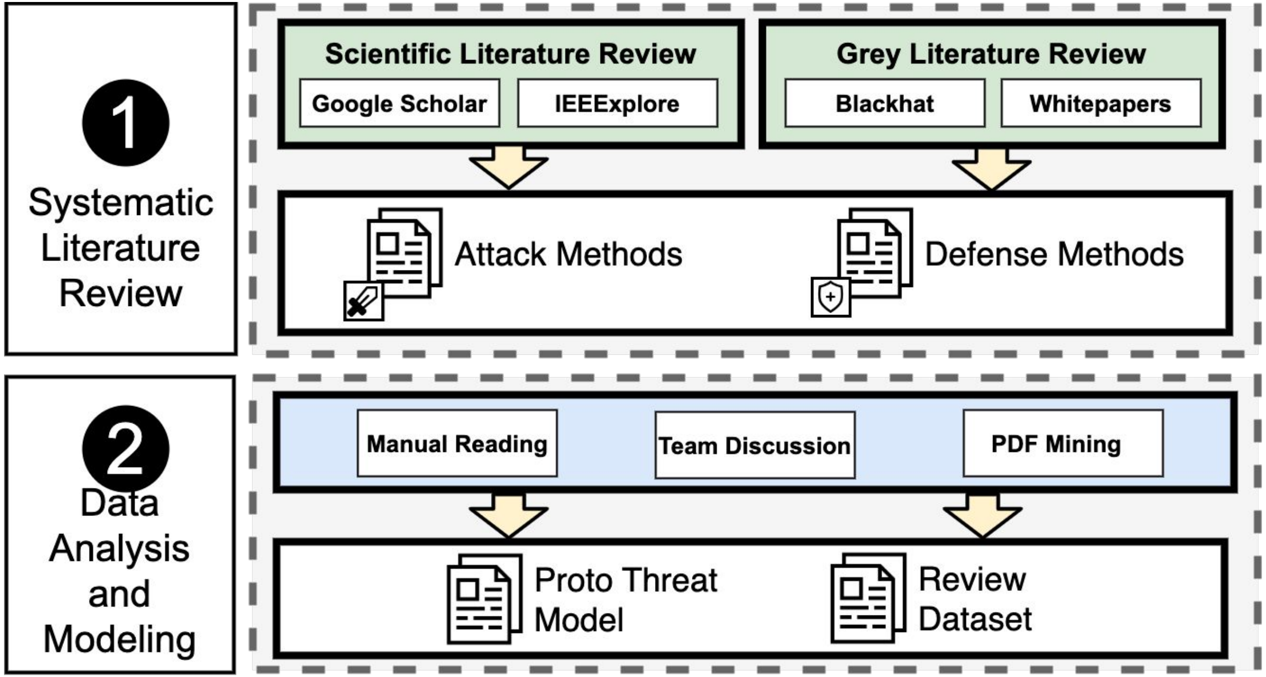
🛡️

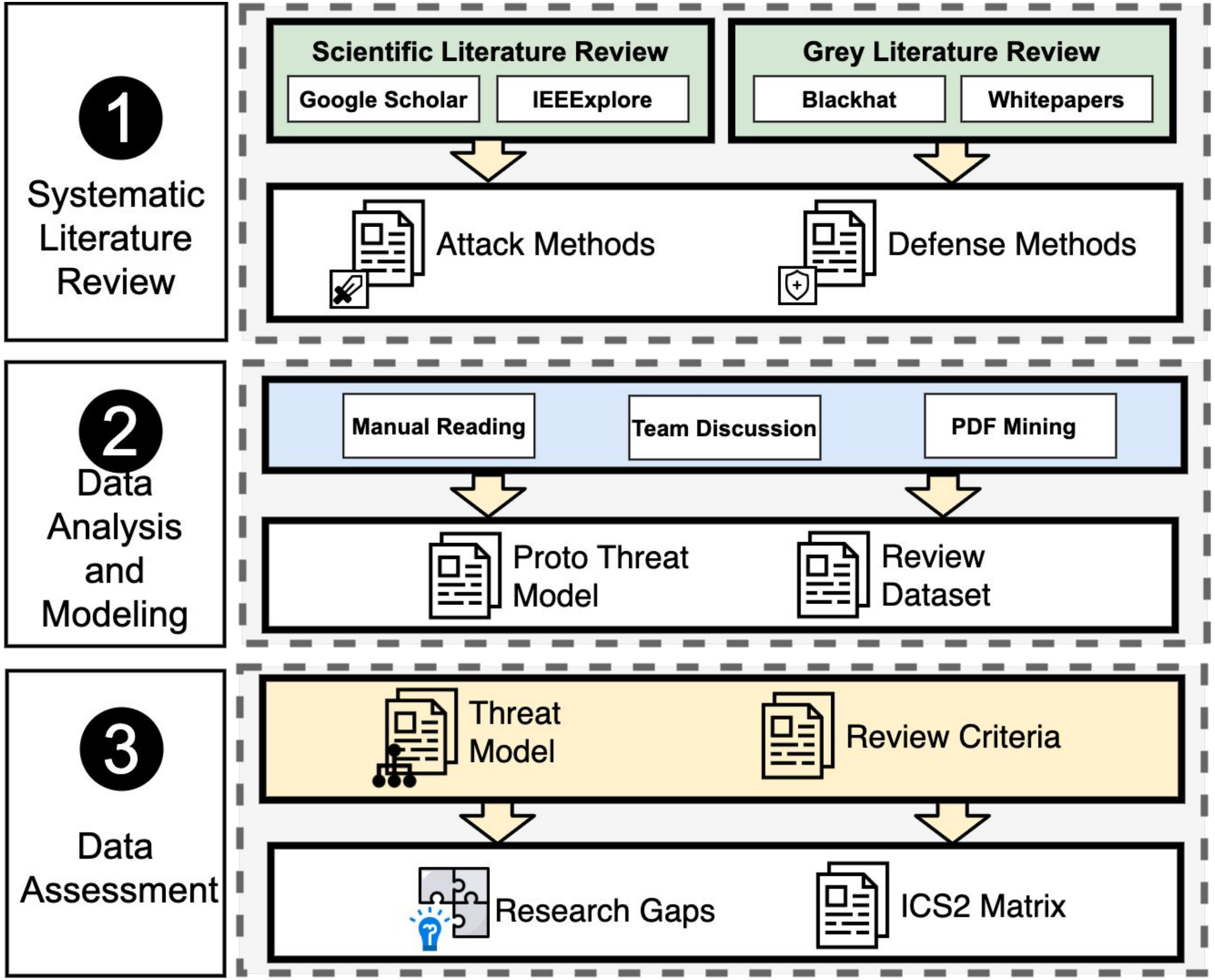
3. Are the current defenses **enough** to address the existing attack methods?

⚔️🛡️

Methodology


1
Systematic Literature Review
Scientific Literature Review
Google Scholar
IEEExplore
Grey Literature Review
Blackhat
Whitepapers
Attack Methods
Defense Methods


1
Systematic Literature Review
Scientific Literature Review
Google Scholar
IEEExplore
Grey Literature Review
Blackhat
Whitepapers
Attack Methods
Defense Methods
2
Data Analysis and Modeling
Manual Reading
Team Discussion
PDF Mining
Proto Threat Model
Review Dataset



1 Systematic Literature Review

Scientific Literature Review

Google Scholar

IEEExplore

Grey Literature Review

Blackhat

Whitepapers

Attack Methods

Defense Methods

2 Data Analysis and Modeling

Manual Reading

Team Discussion

PDF Mining

Proto Threat Model

Review Dataset

3 Data Assessment

Threat Model

Review Criteria

Research Gaps

ICS2 Matrix

Final SoK Scope

- 133 papers

Final SoK Scope

- 133 papers
- 119 attack methods

Final SoK Scope

- 133 papers
- 119 attack methods
- 70 defense methods

Final SoK Scope

- 133 papers
- 119 attack methods
- 70 defense methods
- 20 evaluation criteria

Final SoK Scope

- 133 papers
- 119 attack methods
- 70 defense methods
- 20 evaluation criteria
- 17 years of research

Final SoK Scope

- 133 papers
- 119 attack methods
- 70 defense methods

- 20 evaluation criteria
- 17 years of research
- From 2007 to 2023

Results

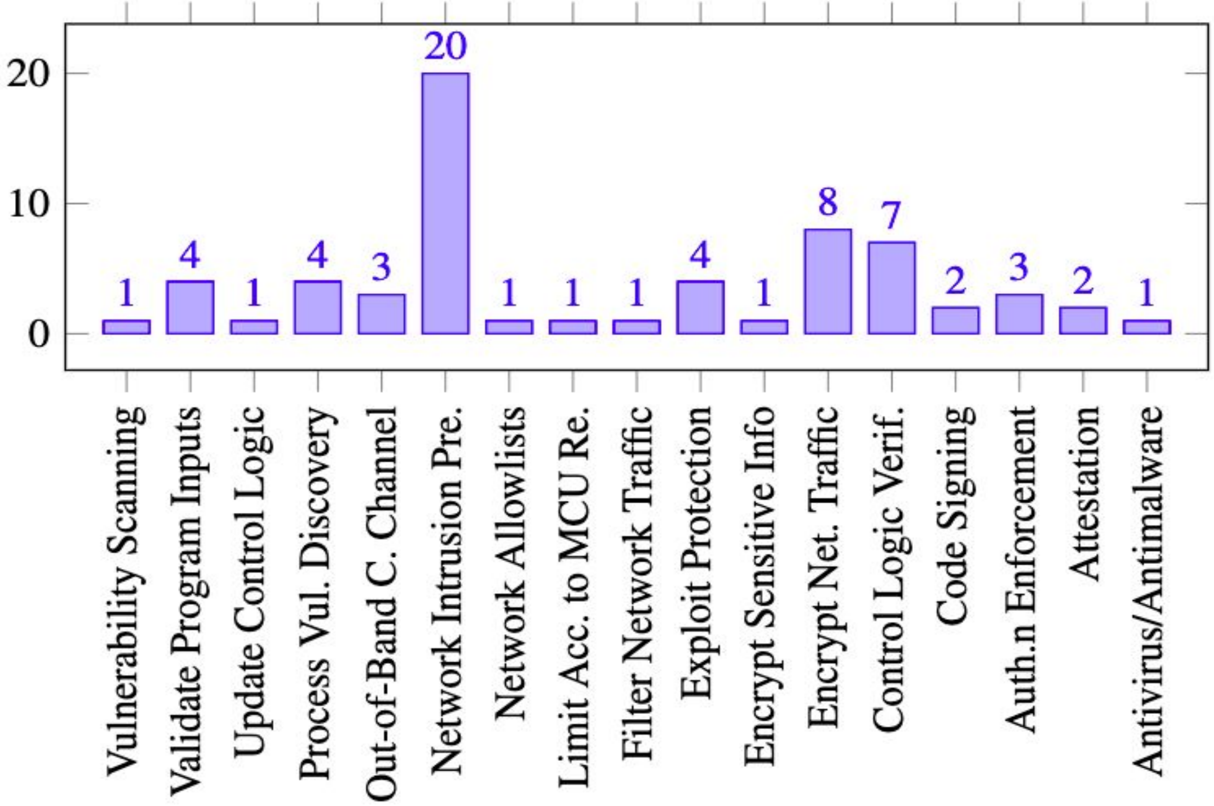
Summary of Results

1. Most of the Attacks Require Zero Environment Knowledge.
2. The Security of Important PLC Brands Has Not Been Explored.
3. Lack of Defenses at the Recovery Stage.
4. Attacks and Defenses are Evaluated on a Small Subset of PLCs
5. Important Tactics have Little to No Research.
6. Most Mitigation Strategies have Little to No Research.
7. Weaknesses of State-of-the-Art Defenses.
8. Reproducible Research Crisis.
9. Transition from HardPLCs to SoftPLCs.
10. We introduce a new threat taxonomy for ICS and PLCs.

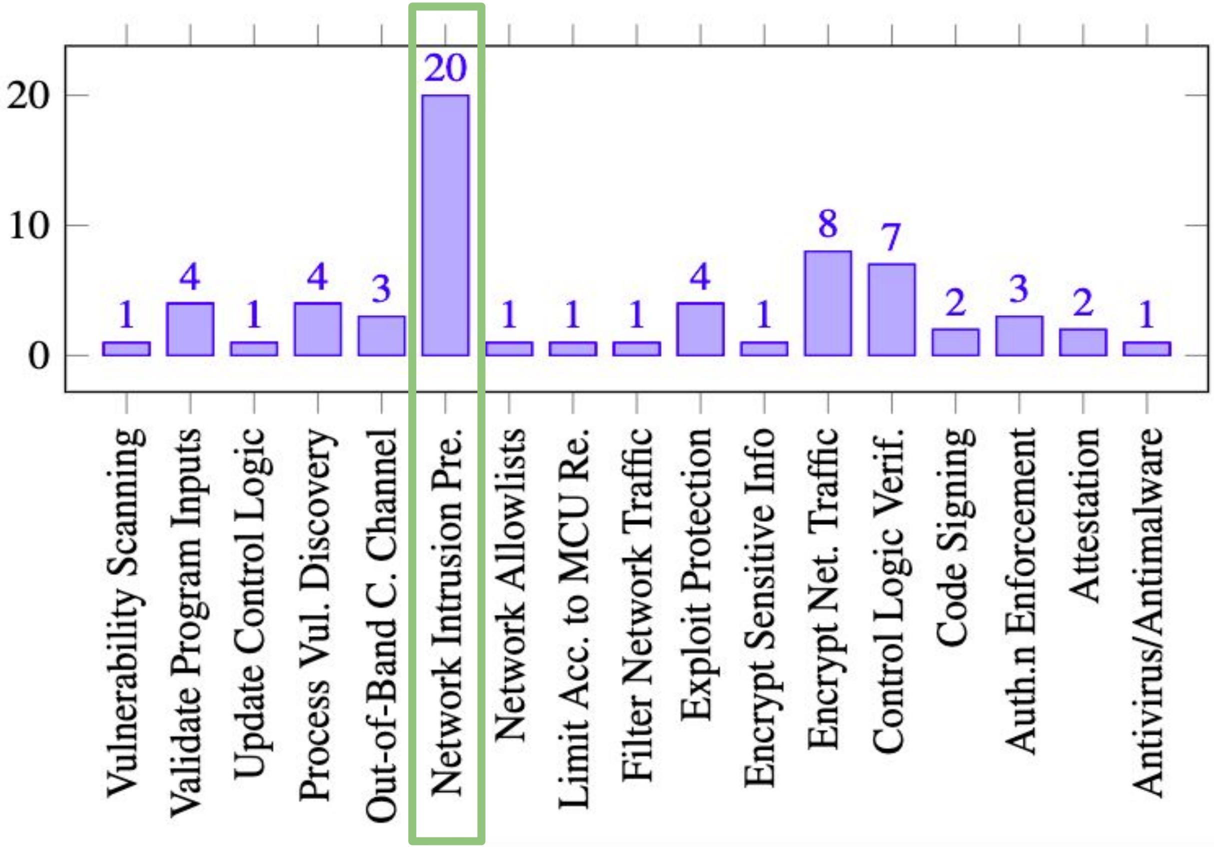
Summary of Results

1. Most of the Attacks Require Zero Environment Knowledge.
2. The Security of Important PLC Brands Has Not Been Explored.
3. Lack of Defenses at the Recovery Stage.
4. Attacks and Defenses are Evaluated on a Small Subset of PLCs
5. Important Tactics have Little to No Research.
6. **Most Mitigation Strategies have Little to No Research.**
7. Weaknesses of State-of-the-Art Defenses.
8. **Reproducible Research Crisis.**
9. **Transition from HardPLCs to SoftPLCs.**
10. We introduce a new threat taxonomy for ICS and PLCs.

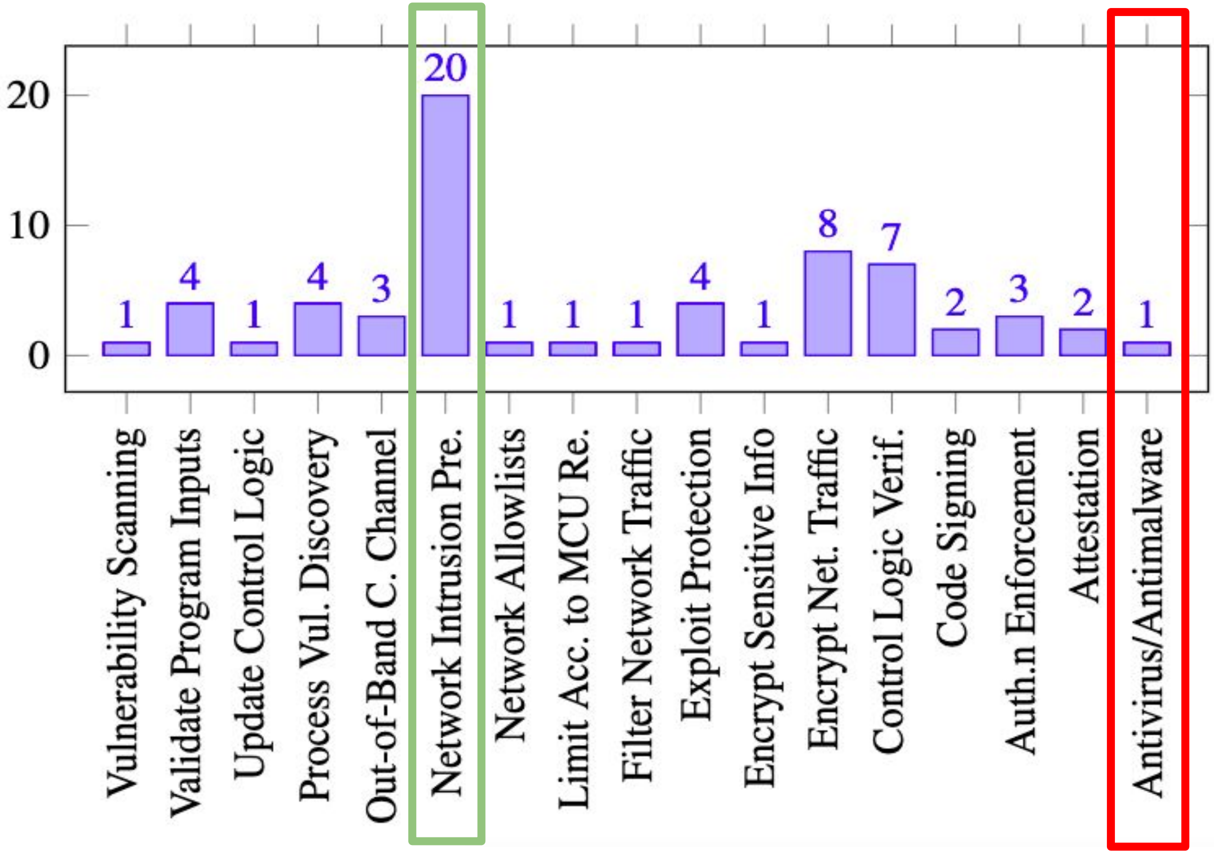
Multiple PLC Defenses Have Almost No Research



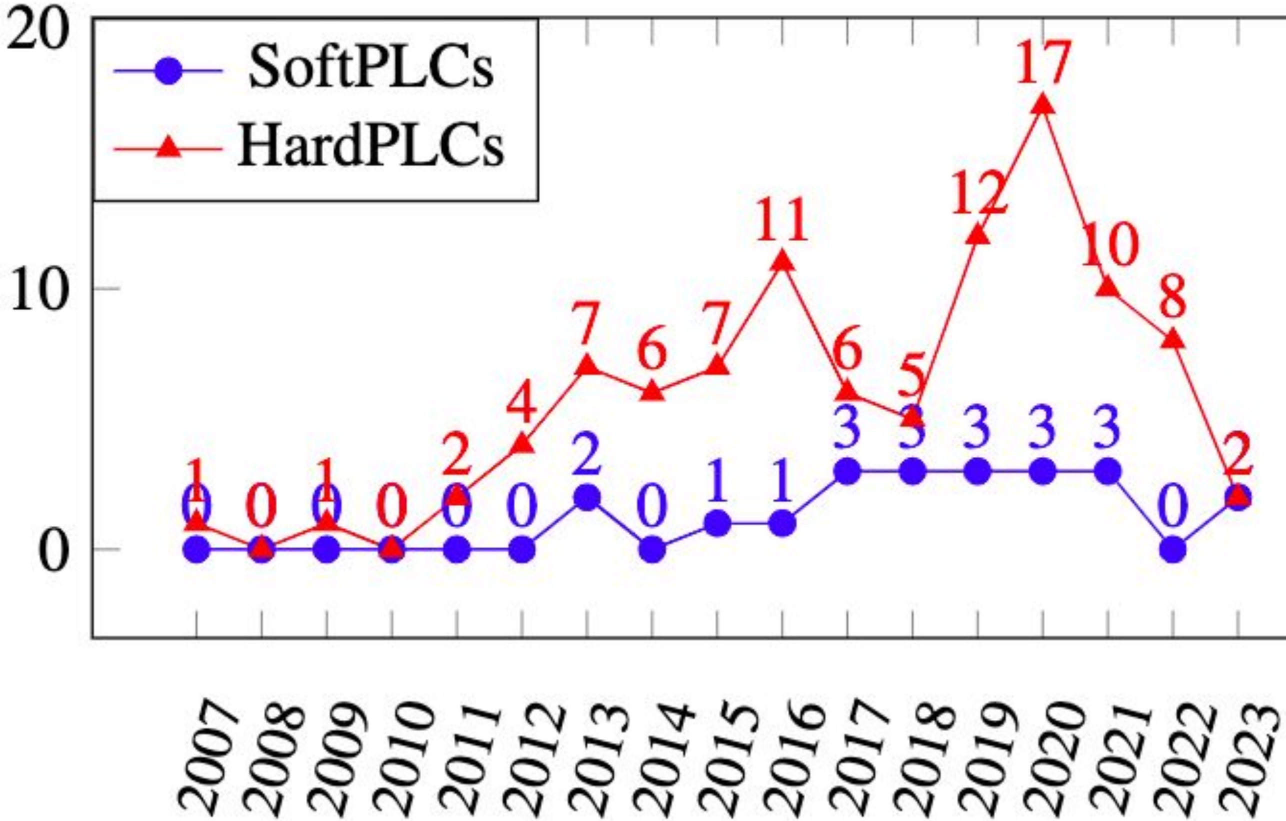
Multiple PLC Defenses Have Almost No Research



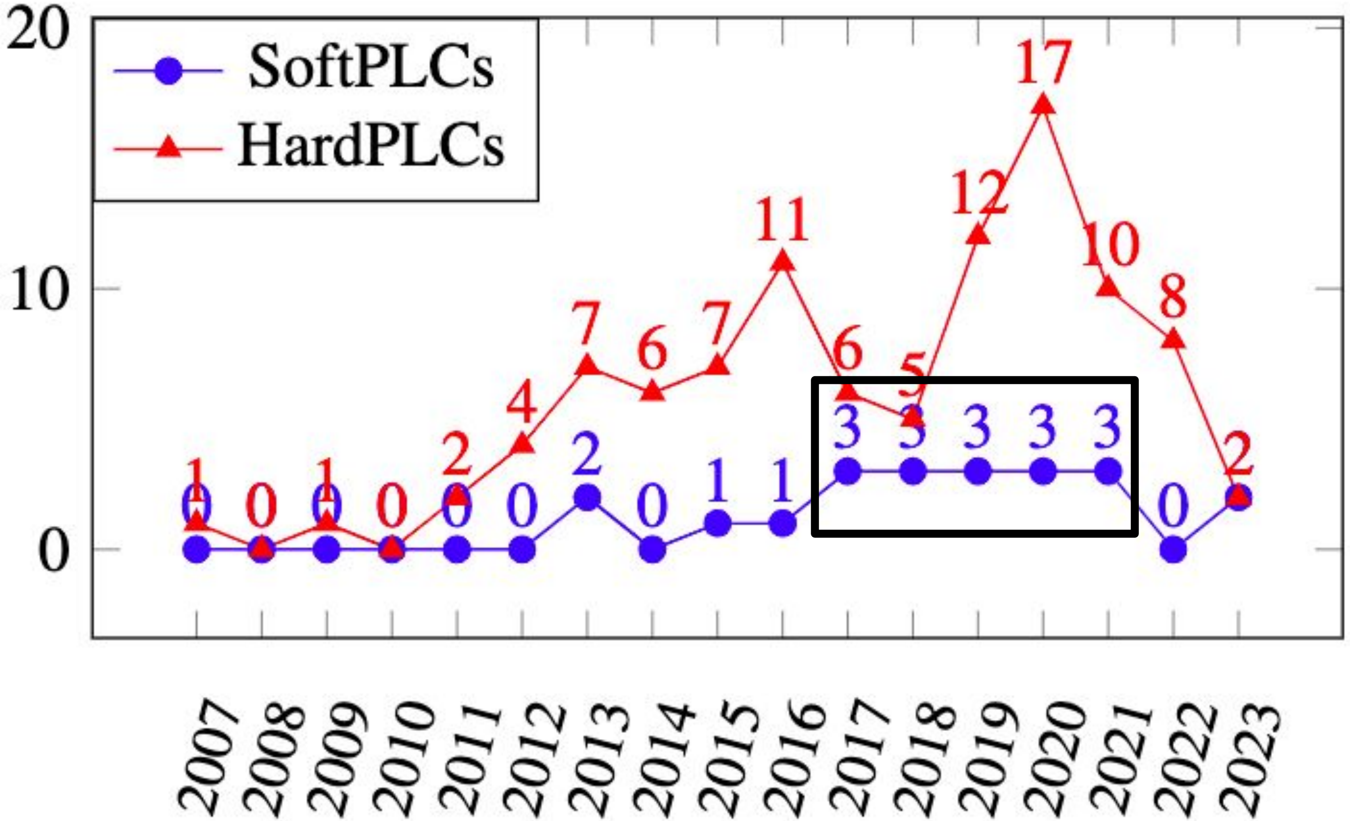
Multiple PLC Defenses Have Almost No Research



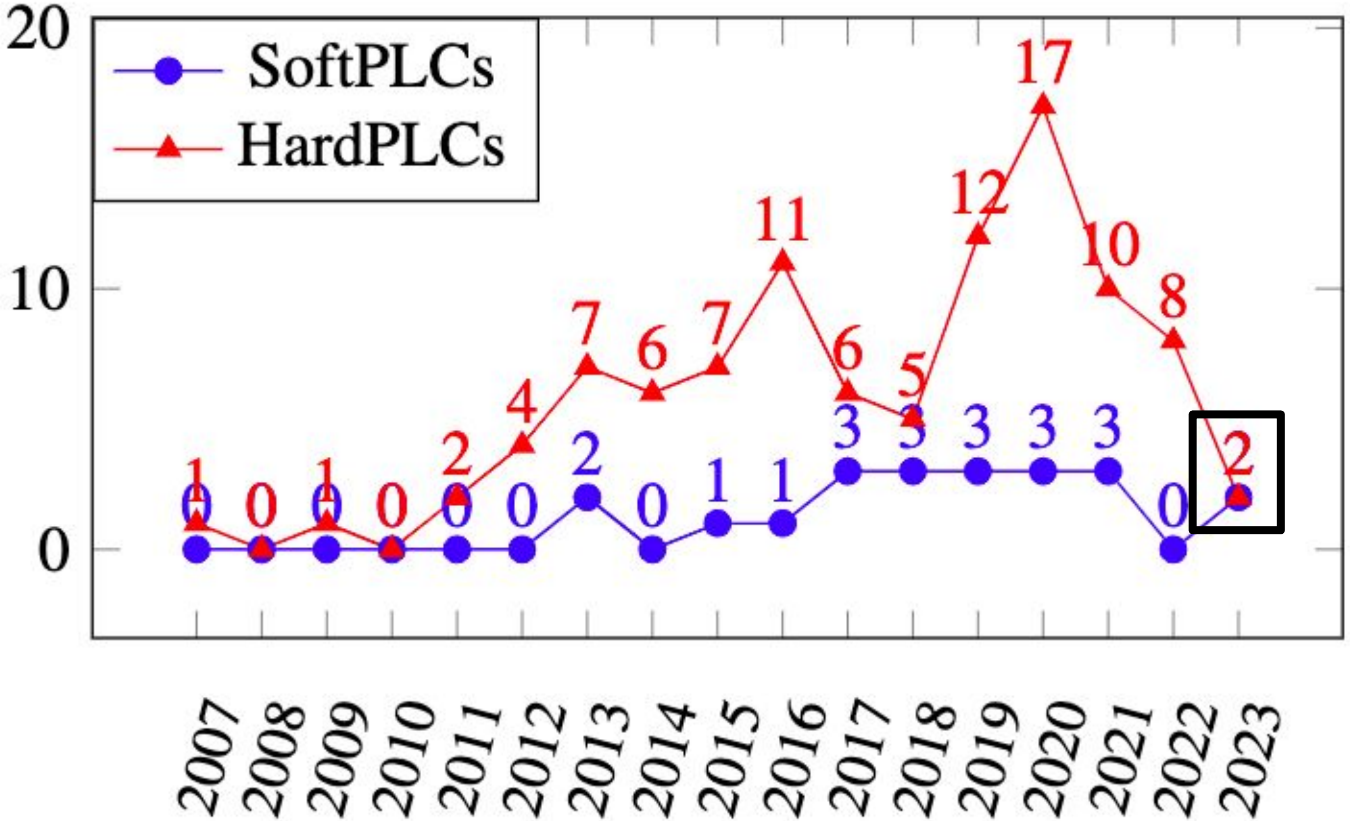
Transition From HardPLCs to SoftPLCs



Transition From HardPLCs to SoftPLCs



Transition From HardPLCs to SoftPLCs



Recommendations For Hard to SoftPLC Transition

- Developing transitional defense methods that **secure both** HardPLCs and SoftPLCs.

Recommendations For Hard to SoftPLC Transition

- Investigating defense mechanisms available for SoftPLCs **previously unavailable** for HardPLCs (*no proprietary restrictions*).

Recommendations For Hard to SoftPLC Transition

- Investigating both attack and defense methods that are **possible only** with SoftPLCs (*use new features such as cloud integration*).

PLC Security Research Reproducibility Crisis

- It is not feasible to reproduce PLC security research for two reasons:

PLC Security Research Reproducibility Crisis

- It is not feasible to reproduce PLC security research for two reasons:
  - Limited Research Artifacts

PLC Security Research Reproducibility Crisis

- It is not feasible to reproduce PLC security research for two reasons:
  - Limited Research Artifacts
  - No Evaluation Metrics

PLC Security Research Reproducibility Crisis

- It is not feasible to reproduce PLC security research for two reasons:
  - **Limited Research Artifacts**
  - No Evaluation Metrics

PLC Research Artifact Survey

- Only 16% of the PLC security papers have any kind of publicly available research artifact.

PLC Research Artifact Survey

- Only 16% of the PLC security papers have any kind of publicly available research artifact.

- What about reaching out to the authors directly?

PLC Research Artifact Survey

- We contacted **91 authors** via email to request access to their papers’ research artifact.

PLC Research Artifact Survey

- We contacted **91 authors** via email to request access to their papers' research artifact.
- We received **16 responses (17.6%).**

PLC Research Artifact Survey

- We contacted **91 authors** via email to request access to their papers’ research artifact.
- We received **16 responses (17.6%).**
- Only **3 authors (3%)** shared their artifacts.

PLC Research Artifact Survey

- Why did the other authors not share their artifacts?

PLC Research Artifact Survey

- Why did the other authors not share their artifacts?
  - **30%** said the project was completed long ago or the first author moved on to a different institution.

PLC Research Artifact Survey

- Why did the other authors not share their artifacts?
  - **30%** said the project was completed long ago or the first author moved on to a different institution.
  - **25%** said there were funding or distribution restrictions.

PLC Research Artifact Survey

- Why did the other authors not share their artifacts?
  - **30%** said the project was completed long ago or the first author moved on to a different institution.
  - **25%** said there were funding or distribution restrictions.
  - **15%** said they were working on it and will publish it later.

PLC Research Artifact Survey

- Why did the other authors not share their artifacts?
    - **30%** said the project was completed long ago or the first author moved on to a different institution.
    - **25%** said there were funding or distribution restrictions.
    - **15%** said they were working on it and will publish it later.
    - **30%** said there were no plans to release it to the public.

Are the current defenses **enough** to address the existing attack methods?

⚔️🛡️

Are the current defenses **enough** to address the existing attack methods?

No

Conclusion

- We systematize **17 years** worth of PLC security literature.

Conclusion

- We systematize **17 years** worth of PLC security literature.
- We provide evidence of important **research gaps**

Conclusion

- We systematize **17 years** worth of PLC security literature.
- We provide evidence of important **research gaps**
- We provide **recommendations** on how PLC security research should go in the future

Conclusion

- We systematize **17 years** worth of PLC security literature.
- We provide evidence of important **research gaps**
- We provide **recommendations** on how PLC security research should go in the future
- We introduce a **new threat taxonomy** for ICS and PLCs.

Thank you for your attention!

ARTIFACT EVALUATED

usenix ASSOCIATION

AVAILABLE

Contact me!

efrenlopez.org

I am on the job market