SoK: Security of Programmable Logic Controllers

Efrén López-Morales, *Texas A&M University-Corpus Christi;* Ulysse Planta, *CISPA Helmholtz Center for Information Security;* Carlos Rubio-Medrano, *Texas A&M University-Corpus Christi;* Ali Abbasi, *CISPA Helmholtz Center for Information Security;* Alvaro A. Cardenas, *University of California, Santa Cruz*

https://www.usenix.org/conference/usenixsecurity24/presentation/lopez-morales

This artifact appendix is included in the Artifact Appendices to the Proceedings of the 33rd USENIX Security Symposium and appends to the paper of the same name that appears in the Proceedings of the 33rd USENIX Security Symposium.

August 14–16, 2024 • Philadelphia, PA, USA

978-1-939133-44-1

Open access to the Artifact Appendices to the Proceedings of the 33rd USENIX Security Symposium is sponsored by USENIX.

USENIX Security '24 Artifact Appendix: SoK: Security of Programmable Logic Controllers

Efrén López-Morales
Texas A&M University-Corpus Christi

Ulysse Planta
CISPA Helmholtz Center for Information Security

Carlos Rubio-Medrano
Texas A&M University-Corpus Christi

Ali Abbasi
CISPA Helmholtz Center for Information Security

Alvaro A. Cardenas
University of California, Santa Cruz

A Artifact Appendix

A.1 Abstract

In our paper, we provide a systematization of knowledge that covers 133 research papers that account for 17 years of research on the security of PLCs. This SoK produced two artifacts. A systematic literature review dataset and a threat taxonomy called *ICS*^{2} *Matrix*. The dataset is available at https://github.com/efrenlopezm/plc-sok-dataset and the threat taxonomy is available at https://github.com/efrenlopezm/ics2matrix.

A.2 Description & Requirements

A.2.1 Security, privacy, and ethical concerns

Our artifacts do not pose any security or privacy risks because they do not include any code.

A.2.2 How to access

The systematic literature review dataset is available at https://github.com/efrenlopezm/plc-sok-dataset/tree/ebeb195e5969d99061302950bb173c6d997be30e.

The threat taxonomy *ICS*^{2} *Matrix* is available at https://github.com/efrenlopezm/ics2matrix/tree/e60ba236a45483bec81b16677b8c71314267f235.

A.2.3 Hardware dependencies

None.

A.2.4 Software dependencies

The dataset is available as a *.csv* file with no software dependencies. The *ICS*^{2} *Matrix* is available as a *.xlsx* file which requires a spreadsheet software such as Microsoft Excel or Apache OpenOffice.

A.2.5 Benchmarks

None.

A.3 Set-up

A.3.1 Installation

No installation required.

A.3.2 Basic Test

Please see the instructions provided here on how to use the *ICS*^{2} *Matrix*.

A.4 Notes on Reusability

We hope other researchers will use the systematic literature review data to further explore the security of PLCs by analyzing it for purposes other than those discussed in our paper. We also hope that the *ICS*^{2} *Matrix* will be used by other researchers to classify TTPs used to target Industrial Control Systems. We welcome pull requests on both of these artifacts' GitHub repositories.

A.5 Version

Based on the LaTeX template for Artifact Evaluation V20231005. Submission, reviewing and badging methodology followed for the evaluation of this artifact can be found at https://secartifacts.github.io/usenixsec2024/.