# Programmable Logic Controllers – Insecure by Design? A Survey.

Benedikt Geisler

Regensburg University of Applied Sciences, Germany

Authors: Benedikt Geisler, Markus Kucera
Contact: `benedikt1.geisler@st.oth-regensburg.de`

# Presenter

**Benedikt Geisler**

- Pre-university:
  - Apprenticeship in Mechatronics
  - $>$ 5 years of experience in the field of automation
- Bachelor of Engineering in Mechatronics at Regensburg University of Applied Sciences, Germany
- Currently masters student of Computer Science at Regensburg University of Applied Sciences, Germany

# Introduction

Terminology:

- PLC: Programmable Logic Controller
- ICS: Industrial Control System
- OT: Operational Technology
- IT: Information Technology

Major attacks have been carried out against ICSs:

- 2011 – Stuxnet: attack against Iranian uranium enrichment facility [1]
- 2016 – Attack against the Ukrainian power grid, which caused a blackout that affected 225,000 people [2]

# Why is OT different from IT?

- PLCs interact with the physical world.
- Main interest: to reliably run a continuous process.
- Lifespan: 10 – 20 years.
- PLCs hardly ever get patched or updated.
- PLCs use proprietary firmware and operating systems.
- PLCs execute their programs in continuous, real-time cycles.

But: PLCs are often connected to IT networks!

# Siemens

- Reverse-engineering of the password encoding scheme (8 bytes XOR) [3].
- Capturing session data & replaying it to the PLC [4].
- Use of exhaustive search to brute-force the password [5].
- Use of a PLC-worm that can propagate through the network [6].
- Disguise code changes induced by attacks and thus fooling the engineering station [7].

# Allen Bradley

- Fooling network intrusion detection systems through the fragmentation of data or the modification of the signature of the packet header [8].
- Denial of Engineering Operations [9] by:
  - hiding infected ladder logic from the engineering station
  - crashing the engineering station upon retrieving code from the PLC
  - injecting a crafted ladder logic program into the PLC that crashes the PLC upon retrieval

# Schneider

- Single point of failure on triple-modular redundant Schneider Tricon PLC [10]:
  - *latent attack*, which downloads valid, but incorrect PLC code
  - *immediate failure attack*, which transfers invalid data to the PLC, causing an error and a denial of engineering
- Use of the fully automated attack tool CLIK [11], which works in four stages:
  1. stealing control logic binary from the PLC
  2. decompiling the binary to source code
  3. infecting the source code in the PLC
  4. concealment of the infection using a virtual PLC

# Beckhoff

Beckhoff PLCs do not use a proprietary operating system, but are based on Windows. This allows for the use of standard tools to attack the PLCs.

Bonney et al. [12] show the following vulnerabilities on Beckhoff PLCs:

- connection setups are transmitted in plaintext, including username and password
- web server is enabled by default
- insecure default username and password for Virtual Private Network (VPN)

# Modbus

Modbus is a popular, vendor-agnostic protocol used in ICS.

Morris et al. [13] show four attack classes on Modbus:

- reconnaissance
- response and measurement injection
- command injection
- denial of service

# OPC UA

Open Platform Communications Unified Architecture (OPC UA) is a platform-independent service-oriented architecture that is widely used in the industry and supported by all major vendors.

It has been designed with a strong focus on security by integrating the following mechanisms:

- user security by using a user security token,
- application security by using digitally signed X.509 certificates
- transport-level security by signing and encrypting each message

However,

- trust on first use (TOFU) is used for provisioning, thus undermining the security guarantees of OPC UA if the adversary gains access during this first phase [14]
- OPC UA security can also be weakened by major security flaws in its artifacts [15]

# Guidelines & Advisories

To help secure ICSs, several guidelines have been published:

- Guide to Industrial Control Systems Security (NIST) [16]
- ICS Security Compendium (BSI) [17]

From a technical perspective, secure coding practices for ICSs are emerging and collected in an open-source effort [18].

In addition, the US Computer Emergency Response Team (CERT), as well as manufacturers of ICSs, publish advisories on vulnerabilities in their products [19] [20] [21] [22].

# Conclusion

- The notion of PLCs being insecure by design is a recurrent theme in all presented work, the weakest links being a lack of authentication mechanisms and insecure protocols.
- OPC UA, when properly implemented and set up, is the exception to the rule.
- As of today, many of the PLCs in the field are not or are insufficiently protected.

# References I

[1] R. Langner, “Stuxnet: Dissecting a Cyberwarfare Weapon,” *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[2] R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid,” SANS Industrial Control Systems, Tech. Rep., 2016.

[3] H. Wardak, S. Zhioua, and A. Almulhem, “PLC access control: a security analysis,” in *2016 World Congress on Industrial Control Systems Security (WCICSS)*, Dec 2016, pp. 1–6.

[4] D. Beresford, “Exploiting Siemens Simatic S7 PLCs,” *Black Hat USA*, vol. 16, no. 2, pp. 723–733, 2011.

[5] A. Ayub, H. Yoo, and I. Ahmed, “Empirical Study of PLC Authentication Protocols in Industrial Control Systems,” in *Fifteenth IEEE Workshop on Offensive Technologies (WOOT)*, 2021.

[6] R. Spenneberg, M. Brüggemann, and H. Schwartke, “Plc-blaster: A worm living solely in the plc,” *Black Hat Asia*, vol. 16, pp. 1–16, 2016.

[7] E. Biham, S. Bitan, A. Carmel, A. Dankner, U. Malin, and A. Wool, “Rogue7: Rogue engineering-station attacks on S7 Simatic PLCs,” *Black Hat USA*, 2019.

[8] K. Wang, J. J. Parekh, and S. J. Stolfo, “Anagram: A content anomaly detector resistant to mimicry attack,” in *International workshop on recent advances in intrusion detection*. Springer, 2006, pp. 226–248.

[9] S. Senthivel, S. Dhungana, H. Yoo, I. Ahmed, and V. Roussev, “Denial of engineering operations attacks in industrial control systems,” in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, 2018, pp. 319–329.

[10] B. Lim, D. Chen, Y. An, Z. Kalbarczyk, and R. Iyer, “Attack Induced Common-Mode Failures on PLC-Based Safety System in a Nuclear Power Plant: Practical Experience Report,” in *2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC)*, Jan 2017, pp. 205–210.

[11] S. Kalle, N. Ameen, H. Yoo, and I. Ahmed, “CLIK on PLCs! Attacking Control Logic with Decompilation and Virtual PLC,” *Proceedings 2019 Workshop on Binary Analysis Research*, 2019.

# References II

[12] G. Bonney, H. Höfken, B. Paffen, and M. Schuba, “ICS/SCADA security analysis of a Beckhoff CX5020 PLC,” in *2015 International Conference on Information Systems Security and Privacy (ICISSP)*, Feb 2015, pp. 1–6.

[13] T. H. Morris and W. Gao, “Industrial control system cyber attacks,” in *1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013) 1*, 2013, pp. 22–29.

[14] F. Kohnhäuser, D. Meier, F. Patzer, and S. Finster, “On the Security of IIoT Deployments: An Investigation of Secure Provisioning Solutions for OPC UA,” *IEEE Access*, vol. 9, pp. 99 299–99 311, 2021.

[15] A. Erba, A. Müller, and N. O. Tippenhauer, “Security Analysis of Vendor Implementations of the OPC UA Protocol for Industrial Control Systems,” Apr. 2021.

[16] K. A. Stouffer, J. A. Falco, and K. A. Scarfone, “Guide to Industrial Control Systems (ICS) Security,” 2011.

[17] BSI, “ICS Security Compendium,” 2013, accessed: 2021-12-07. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICS-Security_compendium.html

[18] PLC Security, “Top 20 PLC Secure Coding Practices,” accessed: 2021-12-07. [Online]. Available: https://www.plc-security.com

[19] CISA, “Industrial Control Systems,” accessed: 2021-12-07. [Online]. Available: https://us-cert.cisa.gov/ics

[20] Siemens, “Siemens Security News,” 2023, accessed: 2023-02-01. [Online]. Available: https://new.siemens.com/global/en/products/services/cert/news.html#/posts

[21] Beckhoff, “IPC - Security Guideline - Advisories,” 2023, accessed: 2023-02-01. [Online]. Available: https://infosys.beckhoff.com/english.php?content=../content/1033/ipc_security/976057355.html&id=

[22] Schneider, “Cybersecurity support portal,” 2023, accessed: 2023-02-01. [Online]. Available: https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp