**ID: 70 H**

**Cyber Protection for Infrastructure**

**Cyber Security of OT Controllers**

**הגנת סייבר לבקרים במערכות תפעוליות**

**Raz Balas,** Havier Roasso, Elroei Damri, Amir Ellenbogen

NRCN, Israel

Razbalas412@gmail.com 052-6467778

Programmable Logic Controllers (PLCs) control valuable assets all around the world. Cyberattacks on such assets can cause system unavailability, leak of information, financial losses and most important - fatality. PLC security is therefore very important.

Cyber security is like a game of "cat and mouse" that takes place between attackers who wish to harm and defenders who are determined to defend. This work regards the defenders' side of cyber security and presents what can be done in order to protect

PLCs from cyberattacks.

One method of securing PLCs includes hardening the PLC, i.e. making them harder to penetrate and harder for cyberattackers to harm. Four aspects of PLC hardening are

presented [1] [2] [3].

First, PLC hardening comprises securing the PLC's IDE (Integrated Development Environment) from where the PLC program can be accessed and changed, which isa vulnerable territory for attackers. IDE securing can be achieved mainly by making it harder to penetrate. This can be accomplished by numerous security operations such as user authentication and splitting the code into sections.

Other aspects include physical and logical hardening. Physical hardening mainly includes preventing physical access, while adding physical isolation, and physical devices to defend the PLC such as circuit breakers. Logical hardening includes firmware and software operations, such as authentications and deactivating unused

features and unused communication protocols.

Yet another aspect of PLC hardening comprises integrating security in PLC program codes, i.e. development of a secure code. This aspect mainly includes instructions to code developers, e.g. avoiding miscalculations and loose ends in the code, thereby making the code harder to exploit by cyberattackers.

This presentation will demonstrate best practices and discuss demands for PLC code security and hardening. The presentation is intended for code developers and project managers.

REFERENCES

[l] PLC Device Security - Tailoring needs, Wen Chinn Yew, February 15, 2017. https://sansorg.egnyte.com/dl/aN9oVirLPG

[2] NIST 800-82r2, Guide to Industrial Control Systems (JCS) Security May 2015. http://dx.doi.org/10.6028/NIST.SP.800-82r2

[3] Secure PLC coding practices: "Top 20 List", 15 June 2021. https://plc-security.com



**השכלה**

2016-2020 .הנדסת חשמל ואלקטרוניקה - המכללה האקדמית סמי שמעון - ממוצע 88 B.Sc

.התמחות - מערכות תקשורת

.פרויקט הנדסי - מערכת לבדיקות רכיבי תקשורת אופטית

2011-2013 תעודת הנדסאי אלקטרוניקה - מכללת עמ״ל 1 - ממוצע 85

.התמחות-מחשבים

.פרויקט הנדסי - מערכת עזר אלקטרונית ללקוי שמיעה

**ניסיון תעסוקתי**

2021-היום OT קמ״ג - מהנדס סייבר

מוביל נושא הגנת בקרים וציוד תעשייתי - קביעת שיטות עבודה, החדרת טכנולוגיות, הערכת סיכונים, התאמה ושילוב של מוצרי הגנה. .חלק מצוות התגובה

2019-2021 אירונאוטיקס - פיתוח תכן אלקטרומכאני, משרת סטודנט.

,פיתוח תכן אלקטרומכאני לרתמות חשמליות כולל ניתוח צרכים הנדסיים

.הגדרת מפרטי כבילה ומאפייני תקשורת