Analisi formale delle vulnerabilità di sicurezza nei sistemi e nelle reti industriali

Il progetto di ricerca consiste nell'implementazione di un Framework di analisi a tre livelli per la detection di attacchi a PLC di tipo Ladder Logic Bomb [1] e Control Logic Injection Attack [2-4]. Il framework dovrà automaticamente eseguire il parsing del programma di controllo dei PLC, sia scritto in Ladder Logic che in testo strutturato, ed eseguire i seguenti tre passi di analisi volti al rilevamento degli attacchi sopra menzionati:

1) Analisi statica con algoritmi di Machine Learning: il primo passo consiste nell'analisi statica del programma di controllo del PLC, in modo da estrarre un set di feature che verrà utilizzato da algoritmi di machine learning supervisionato, come linear Support Vector Machines, con l'obiettivo di identificare la presenza di pattern sospetti e caratteristici degli attacchi di Ladder Logic Bomb e di Control Logic Injection.

2) Verifica formale dei programmi di controllo su cui sono stati rilevati pattern sospetti: il framework dovrà essere in grado di tradurre il programma di controllo parsato in un formato compatibile con quello del verificatore formale Intrepyd. In questo passo, verranno definite query specifiche per gli attacchi in analisi da dare in input al verificatore formale.

3) Analisi dinamica su PLC virtualizzato (Open PLC): nel caso in cui la verifica formale confermi la presenza di attacchi, l'ultimo passo permette di capire il tipo di attacco in questione tramite l'analisi dinamica del programma di controllo eseguita su un PLC virtualizzato inserito in un environment di un digital twin che rappresenta l'architettura di una rete industriale secondo lo standard IEC 62443 [5]. Questo terzo step non solo avrà come obiettivo la detection accurata degli attacchi, ma consentirà anche di stimare i danni che tali attacchi causerebbero se realmente eseguiti su una rete industriale reale.

Dovranno essere svolti esperimenti sulle soluzioni realizzate per elaborare considerazioni in merito ad ogni meccanismo di detection utilizzato, individuare punti di forza e debolezza dei tre metodi, al fine di elaborare procedimenti di difesa e analisi alternativi più accurati e precisi.

Il piano delle attività prevede

- *M1 :* studio della letteratura utile ad individuare le feature più rappresentative e gli algoritmi più efficaci per lo svolgimento del passo (1)
- *M2–M8 :* realizzazione del software di analisi descritto al passo (2)
- *M6–M12 :* integrazione del software nel digital twin (esistente) per ampliarne le capacità di analisi dinamica
- *M10-M12 :* raccolta e analisi quantitativa dei dati rappresentativi dell'efficacia della soluzione, specificamente per i tre livelli di difesa, tramite il calcolo dei falsi positivi, falsi negativi, precisione e accuratezza.

BIBLIOGRAFIA:

[1] Govil, Naman, Anand Agrawal, and Nils Ole Tippenhauer. "On ladder logic bombs in industrial control systems." Computer Security: ESORICS 2017 International Workshops, CyberICPS 2017 and SECPRE 2017, Oslo, Norway, September 14-15, 2017, Revised Selected Papers 3. Springer International Publishing, 2018.

[2] Yoo, Hyunguk, and Irfan Ahmed. "Control logic injection attacks on industrial control systems." ICT Systems Security and Privacy Protection: 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings 34. Springer International Publishing, 2019.

[3] Yoo, Hyunguk, et al. "Overshadow PLC to detect remote control-logic injection attacks." Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden, June 19–20, 2019, Proceedings 16. Springer International Publishing, 2019.

[4] Alsabbagh, Wael, and Peter Langendörfer. "A Flashback on Control Logic Injection Attacks against Programmable Logic Controllers." Automation 3.4 (2022): 596-621.

[5] DesRuisseaux, Daniel. "Practical overview of implementing IEC 62443 security levels in industrial control applications." USA: Schneider Electric (2018).