Researchers wrest control of one of world's most secure PLCs

August 8 2019

Credit: CC0 Public Domain

Cybersecurity researchers at Tel Aviv University and the Technion Institute of Technology have discovered critical vulnerabilities in the Siemens S7 Simatic programmable logic controller (PLC), one of the world's most secure PLCs that are used to run industrial processes.

Prof. Avishai Wool and M.Sc student Uriel Malin of TAU's School of

Electrical Engineering worked together with Prof. Eli Biham and Dr. Sara Bitan of the Technion to disrupt the PLC's functions and gain control of its operations.

The team is slated to present their findings at Black Hat USA week in Las Vegas this month, revealing the security weaknesses they found in the newest generation of the Siemens systems and how they reverse-engineered the proprietary cryptographic protocol in the S7.

The scientists' rogue engineering workstation posed as a so-called TIA engineering station that interfaced with the Simatic S7-1500 PLC controlling the industrial system. "The station was able to remotely start and stop the PLC via the commandeered Siemens communications architecture, potentially wreaking havoc on an industrial process," Prof. Wool explains. "We were then able to wrest the controls from the TIA and surreptitiously download rogue command logic to the S7-1500 PLC."

The researchers hid the rogue code so that a process engineer could not see it. If the engineer were to examine the code from the PLC, he or she would see only the legitimate PLC source code, unaware of the malicious code running in the background and issuing rogue commands to the PLC.

The research combined deep-dive studies of the Siemens technology by teams at both the Technion and TAU.

Their findings demonstrate how a sophisticated attacker can abuse Siemens' newest generation of industrial controllers that were built with more advanced security features and supposedly more secure communication protocols.

Siemens doubled down on industrial control system (ICS) security in the

aftermath of the Stuxnet attack in 2010, in which its controllers were targeted in a sophisticated attack that ultimately sabotaged centrifuges in the Natanz nuclear facility in Iran.

"This was a complex challenge because of the improvements that Siemens had introduced in newer versions of Simatic controllers," adds Prof. Biham. "Our success is linked to our vast experience in analyzing and securing controllers and integrating our in-depth knowledge into several areas: systems understanding, reverse engineering, and cryptography."

Dr. Bitan noted that the attack emphasizes the need for investment by both manufacturers and customers in the security of industrial control systems. "The attack shows that securing industrial control systems is a more difficult and challenging task than securing information systems," she concludes.

Following the best practices of responsible disclosure, the research findings were shared with Siemens well in advance of the scheduled Black Hat USA presentation, allowing the manufacturer to prepare.

Provided by Tel Aviv University