Technion researchers decrypt Siemens' smart programmable logic controller firmware

Researchers in the Henry and Marilyn Taub Faculty of Computer Science at the Technion – Israel Institute of Technology will present the decryption of Siemen's programmable logic controller (PLC) firmware at the prestigious Black Hat Hacker Convention in Las Vegas.The findings of the study were forwarded to the company.

The research project was led by the Head of the Technion Hiroshi Fujiwara Cyber Security Research Center, Professor Eli Biham and Dr. Sara Bitan, with master's students Maxim Barsky, Alon Dankner, and Idan Raz.

The group succeeded in hacking the ET200 SP Open Controller, CPU 1515sp, of Siemens' Simatic S7 series, which represents a new concept in controller planning among numerous vendors. The concept is based on the integration of a standard operating system. In this case specifically, the Windows 10 operating system was integrated into the CPU 1515sp. These controllers are used in a variety of civil and military applications, including transportation system, factories, power stations, smart buildings, traffic lights, and others. Their purpose is to provide an automated process control that delivers an optimal, fast response to changing environmental conditions.

Attacks against PLCs have posed a challenge for Siemens, which is considered a vendor that meets the highest of security standards in the industry. The S7 PLC series is perceived as innovative and highly secure, largely thanks to the integration of built-in cryptographic mechanisms, and consequently, attacks against it pose a great challenge.

The Technion researchers attacked the CPU 1515sp and, for the first time, decrypted the firmware which is common to all PLCs in the series. The successful attack enabled the researchers to study the software characteristics. They say that the attack exposed possible vulnerabilities in this PLC, as well as in other controllers in the series, and intensifies the need for improved security of these devices. Considering that they are deployed in critical systems such as power plants, water facilities, transportation system, etc., attacks against them by hostile elements may pose a danger to life.

Dr. Sara Bitan and Alon Dankner will be presenting the research today at the Black Hat Convention in Las Vegas.

Click here for pictures:

Captions:

1. Professor Eli Biham
2. Dr. Sara Bitan
3. master's student Alon Dankner

Photos: Office of the Technion Spokesperson

For more information: Doron Shaham, Technion Spokesperson, +972-50-3109088