Industrial Control Systems
Security Projects

236349

Contact Person:
Dr. Sara Bitan

email: sarab@cs.technion.ac.il

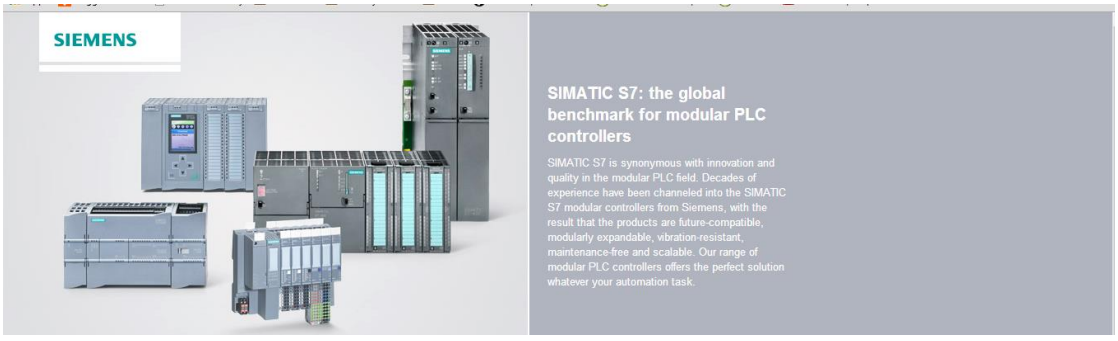
Phone: 04-8295854

Background:

Critical infrastructure such as power plants, chemical plants, railway and other transportation systems and water treatment plants are vital to modern life. These facilities are controlled by industrial control systems which are computerized systems that control equipment such as engines, generators and safety mechanisms.

One of the central devices used for controlling the equipment is the programmable logic controller (PLC) which is a reliable programmable hardware device implementing complex monitoring and control logic of safety-critical and availability-critical systems. This is done by reading and writing to (possibly) hundreds of analog and digital signals according to programmable logic. PLCs are often used as the lowest layer of an industrial control system which contains capabilities such as HMI, non-critical system logic, logging etc. PLCs programming can be done through standard network interface (Ethernet), using proprietary protocols.

Siemens' Simatic S7 is a popular PLC family (almost 20% of the industrial market share in 2010). The Simatic PLC's are programmed through a work station running Siemens' Step7 software.



The goal of the following projects is to ascertain the resiliency of the Simatic S7 programing interface to network based attacks.

The students will work at the cyber lab in the faculty. The lab contains several PLCs (Siemens' S7-1200, S7-1500, VIPA-Silo) and a Step7 programming station.

Project 1: Can one program a PLC from a rouge network station?

Goals:

The goal of this project is to determine whether an attacker, with physical access to a LAN which contains Simatic S7 PLC can modify its programming without running the Step7 software.

Requirements:

- Run the Step 7 software, write a simple program and program the PLC.
- Analyze the network traffic, identify packets containing the program code, and understand the program representation.
- Write packet injection program which modifies the program which was downloaded by the Step7 software.
- Run the packet injection program, and prove that the PLC code was indeed modified.

Pre-requisites:

Programming knowledge.

Deep understating of TCP/IP.

Computer security course.

Project 2: Can one breach the PLC modules access control system

Goals:

The Simatic S7-PLC programming interface has a simple access control system. The programmer can use the Step7 software, to block read/write access to certain modules, or to require authentication. This access control system is designed to protect the PLC from cyber-attacks similar to Stuxnet (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf). The goal of this project is to check whether this newly added access control mechanism can withstand network attacks similar to the ones we seek in Project1.

Requirement:

- Run the Step 7 software, write a simple program and apply various access control settings to its modules.
- Analyze the network traffic, and identify packets containing the access control instructions and authentication/authorization data.
- Determine whether the access control system can be breached; if the answer is positive design an attack
- Implement the attack, and prove that the PLC code was indeed modified.

Pre-requisites:

Programming knowledge.

Deep understating of TCP/IP.

Computer security course