Contribution ID: **526** Type: **Paper**

Breaking Siemens Protocol and Cheating on Distributed Control Systems

With the effort of industrial control system vendors, industrial network protocols are getting hardened and seems secure for last several years. Based on secured industrial network protocols, most of control system have getting updated. Especially, Siemens products widely used in industrial control system have well-made protection and security. However, the number of threats against Siemens products has been increased by cyber criminal. They have been working on vulnerability hunting on these products so that they could targeting most advanced facilities as many as they want.

Siemens s7comm Plus protocol presented with improvements on security such as against replay attack. A few cyber security researchers already analyzed this latest protocol then announced there might be another threat still existed. In this cyber security field like irresistible force paradox, vendors are always trying to update the security flaw. In 2019, however, this well-crafted and secured protocol's mechanism is figured out in final. Its weak point could be used for logic tampering, man in the middle and replay attack between human-machine interface and Siemens S7-1500 programmable logic controller which is latest version.

The purpose of this paper is to inform how this well-made protocol could be analyzed and how it could affect to industrial control system. To conduct experiment for proving the research, physical condenser system was built as part of coordinated research projects. With this set-up, Siemens s7comm plus has been analyzed and tested security flaws that affect to other industrial control system in the same network zone. This paper will give an overview of how it's possible to tamper memory of programmable logic controller and deface screen of human-machine interface with newly founded vulnerability of s7comm plus, and eventually turned to deceive all systems communicating in the same network. As like this, several feasible attack scenarios caused by this vulnerability and each step from the beginning of analysis to deceiving distributed control systems in nuclear power plants.

To abridge technical part, present research is done with vulnerability of s7comm plus protocol and frame a hypothesis how it affects TIA portal which is a software to develop control system and WinCC advanced which is human-machine interface from Siemens and other control system. The encryption mechanism of s7comm plus has been analyzed with debuggers and custom script codes. Main dynamic-link library of encryption algorithm to secure network traffic of s7comm plus has been figured out as well as specific functions in program. Only left part of this research is writing attack code with this vulnerability then deploy to any industrial control system to compromise it in the same network area.

Gender

Male

State

Republic of Korea

Authors: Mr LEE, Seungjun (NSHC Inc.); Mr MOON, Heaeun (NSHC Inc.); Ms KIM, Youngsun (NSHC Inc.)

Presenters: Mr LEE, Seungjun (NSHC Inc.); Mr MOON, Heaeun (NSHC Inc.); Ms KIM, Youngsun (NSHC Inc.)

Track Classification: CC: Information and computer security considerations for nuclear security