1000 - The spear to break the security wall of S7CommPlus

Saturday at 10:00 in Track 4

20 minutes | Exploit

Cheng*ICS Security Researcher, NSFOCUS*

In the past few years, attacks against industrial control systems (ICS) have increased year over year. Stuxnet in 2010 exploited the insecurity of the S7Comm protocol, the communication protocol used between Siemens Simatic S7 PLCs to cause serious damage in nuclear power facilities. After the exposure of Stuxnet, Siemens has implemented some security reinforcements into the S7Comm protocol. The current S7CommPlus protocol implementing encryption has been used in S7-1200 V4.0 and above, as well as S7-1500, to prevent attackers from controlling and damaging the PLC devices.

Is the current S7CommPlus a real high security protocol? This talk will demonstrate a spear that can break the security wall of the S7CommPlus protocol. First, we use software like Wireshark to analyze the communications between the Siemens TIA Portal and PLC devices. Then, using reverse debugging software like WinDbg and IDA we can break the encryption in the S7CommPlus protocol. Finally, we write a MFC program which can control the start and the stop of the PLC, as well as value changes of PLC's digital and analog inputs & outputs. Based on the research above, we present two security proposals at both code level and protocol level to improve the security of Siemens PLC devices.

Cheng

Cheng Lei is an Industrial Control System Security researcher at NSFOCUS. His interest is mainly about PLC and DCS vulnerability exploitation and security enhancement. Over the years he has released three Siemens CVE vulnerability

#defcon25/by_track/track4/saturday #defcon25/By_Day/_saturday