

SECURING INDUSTRIAL CONTROL SYSTEMS PROTOCOLS

Eli Biham, Sara Bitan and <u>Alon Dankner</u> Technion – Israel Institute of Technology

3rd Israeli Conference on Hardware and Side-Channel Attacks (ICHSA 2021)

INDUSTRIAL CONTROL SYSTEMS

- ICS systems are designed to manage, monitor and control industrial processes in real-time.
- Widely used in critical infrastructures, such as power plants and water supply.







THE K7 PROTOCOL

- K7 is a protected protocol for ICS systems that fits large organizations.
 - Supports central management of users, keys and permissions
 - Secure and flexible
 - Using tickets
- In this talk, we discuss a few of the problems that K7 solves.

PROBLEM 1: MUTUAL AUTHENTICATION

- The latest versions of the Siemens PLCs introduced integrity and replay protection into their proprietary S7 protocol.
- The S7 protocol lacks client authentication, any TIA can communicate with any PLC.
- In a Black Hat talk in 2019 we presented Rogue7, which is an impersonation attack on the newest model of the S7 PLC.
 - Stealth attack that modifies the program but causes the PLC to present a false display for the HMI.





Rogue Engineering Station

PROBLEM 2: PASSWORD PROTECTION

- S7 offers password protection for specific ICS features (read, write and more).
 - Users must maintain long lists of passwords that complicate their work.
 - Or, even worse, to set the same password to all the PLCs.





PROBLEM 3: AUTHORIZATION

- There is no support for ICS permissions, e.g., program download or upload.
- No policy mechanism.
 - Who can perform which operation on which device.





PROBLEM 4: CENTRAL MANAGEMENT

- Large organizations typically contain many users and many facilities (organizational units).
- None of the current models support central management of a large number of devices.
 - Without requiring the engineers and technicians to handle thousands of passwords manually.
- A central mechanism in essential to manage and control the devices and their permissions.
 - Allows scalable and distributed administration of identities and permissions.





OUR PROTOTYPE

Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

P5 C:\Users\amit.nizri> cd .\Converters_full_code\amit\servers\ P5 C:\Users\amit.nizri\Converters_full_code\amit\servers> python .\Auth_Server1.py

[*] Server has created a connection to 127.0.0.1:2993

TGS_Request: TIA_192.168.0.63 PLC_192.168.0.19

client ticket on server side:

Ticket__sepiration_setup : 2020-12-03 13:54:56, Ticket__server_id: ;PtC_192.108.01.97, __protocol : W, _Ticket__client_id: TTA.192.66.063, _Ticket__authentication_alg : AR A-256, Ticket__authentication_key : 0086dae65931:80/aer.538cg0-11-04/32:00-00__Ticket__ 20-12-03 12:55:50.578000, Ticket__compitation_retroewerneropyton_alg : ARS-726-CBC, _Ticket__ ption_key : 87 aef39bac598412456er#0408100 : set(['Load-SoFTWARE', 'WATCH']) JC_model : S/-YYYY, _Ticket__compisions : set(['Load-SoFTWARE', 'WATCH']) T just resolved a form client: TCS_Request: Drc.192.108.0.19

Connection to 127.0.0.1:29933 was closed







Securing Industrial Control Systems Protocols



- The K7 protocol solves all the problems we described, and more.
- We presented some of the problems solved by K7
 - Mutual authentication.
 - Password-based protection.
 - Authorization and supports granular permissions.
 - Central management of users, privileges and security.
- Easy to upgrade the system gradually, using protocol converters, unlike all current systems.
- We implemented the K7 protocol, our prototype is based on Siemens S7 but can be adapted to other vendor protocols.



THANK YOU FOR LISTENING 🕐