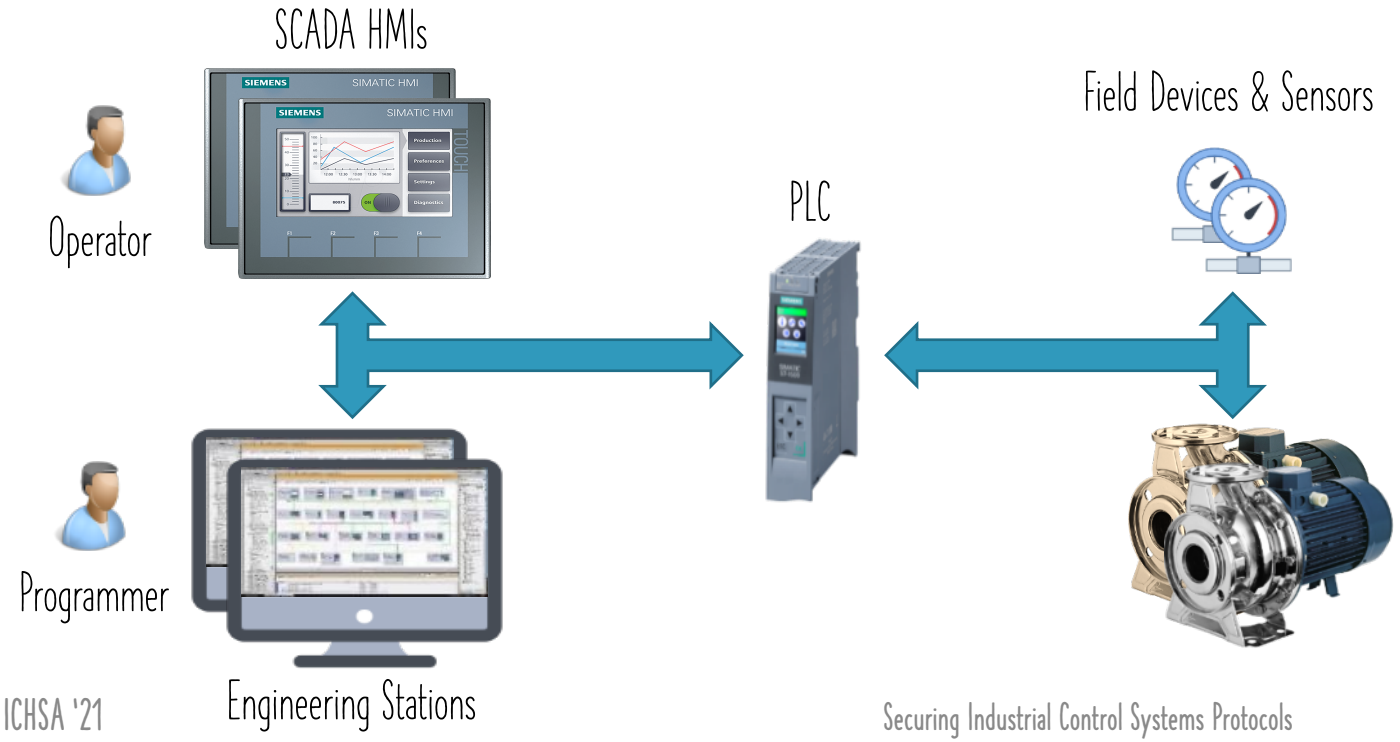
SECURING INDUSTRIAL CONTROL SYSTEMS PROTOCOLS

Eli Biham, Sara Bitan and Alon Dankner
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.

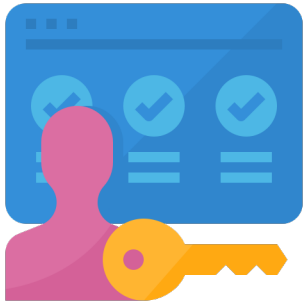
Rogue Engineering Station

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

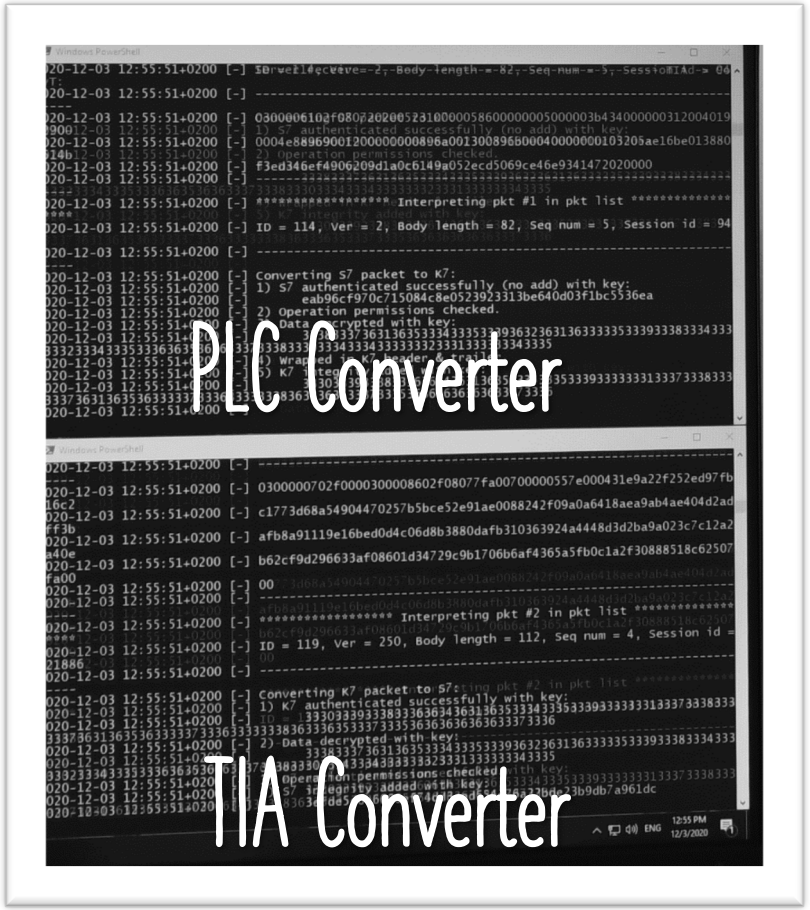
- There is no support for ICS permissions, e.g., program download or upload.
- No policy mechanism.
  - Who can perform which operation on which device.



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



SUMMARY

- 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 ☺