IEEE PSCC S1 SG: IEEE 1686 Standard for Intelligent Electronic Devices Cyber Security Capabilities

Chair: Marc Lacroix
Vice Chair: Éric Thibodeau
Output: Revision of the standard
Established: Dec 2017

Summary Minutes for Subcommittee Report

The S1 WG meeting was held on Monday, May 7, 2018 with 12 members and 14 guests.
The goal of this meeting was to present an overview of the work to do and look at different use cases for IED access.

Thanks to Éric Thibodeau and James Formea for taking notes during the meeting.

Purpose of S1 SG:
The task force will revise the existing IEEE 1686 standard to integrate the latest cybersecurity technologies in order to defines the functions and features to be provided in IEDs to support cybersecurity programs.

Request for Sep 2018 S1 plans to meet as a Working Group in a single session for 40 people and a computer projector.

Patent slides presented

Marc presents the existing TOC of the standard.

Information is on iMeet Central but Marc will continue to try and send emails.

Discussions about elements to be included:

- Capability (or not) to reset audit trail in the standard
- What is required for physical security, are we talking simply of tamper detection?
  - Some brought about a requirement for a TPM.
  - Point of view from utility → Bottom line: "Is someone touching the device". Beyond this is just utility policy.
  - If someone's in, log and alarm about presence.
  - tamper detection/prevention.
  - no exposed JTAG headers, etc
  - perhaps tamper detection instead of physical security?
  - could be about physical security to the communications ports?
  - TPMs be present for key protection. JTAG fuses.
  - 62351-7 addresses physical security of the control cabinet. Ability to report physical access occurrences - plug-in keyboard, open the cabinet, pushing buttons on the front panel
  - monitoring and logging when something is disconnected, etc
  - may need to declare devices as untrusted if they power off and back on unexpectedly until some verification can be done. Availability and reliability still trump security.
  - 2048 events is a small audit trail
- Erasing the log is not allowed now, but it may be possible to erase it by generating more than 2000 events
  - Maybe security events should be differentiated from parameter changes?
- Provisions about time synch / time set manipulation. For example, employee walking in the substation and setting back the clock 5 years before.
  - Multiple sync and cross time-check?

- Bill Dickerson to provide liaison to Industrial Cybersecurity WG (ATIS)
    - Spoofing time is an actual problem that should be addressed in 1686
-

Discussions about use cases:

- Use case 1: Front panel access
    -
- Use case 2: Front panel with token
    -
- Use case 3: Access with terminal emulator
- Use case 4: Remote-access with terminal emulator
- Use case 5: Access with configuration tool
    - Even with a vendor tool, we want the IED to perform actual authentication, not authenticating from a device in the middle
    - Side discussion: Suggestion that role is validated by the front-end server. IED would perform only validation on the role. According to Didier, this does not address defense in depth. Validation should also be done at the IED level. Goes beyond this use case.
    - Also consider area of responsibility and time of responsibility that can also be associated to a given role. Ex: give operator rights on a particular device in a particular time frame, not on every device at once.
    - If network connected, devices should be able to validate authentication to a centralized server. The concept of a number of users inside an IED is outdated. Backup emergency access should still be available.
    - Attributes certificates conveying role of a user could remove requirement for permanent connection to centralized server. This certificate has to be signed by a centralized server, but in the end can be validated by the end device without contact to centralized server. Could be time and area constrained. Like a “work permit”. Appears the right way to do it.
    - Another idea is to require an option to make devices configurable only upon physical access.
    - Physical backdoor to retrieve access locally if access is lost.
    - 62351 moving toward attribute certificates. Short-lived attribute certificates.
    - think of certificates as work orders for the device operator.
    - want to take advantage of devices that have physical control, such as require a user to take a system offline before making configuration changes. Require the user to be present to make configuration changes. "Physical state change to allow any write access."
    - need a device reset capability when all logical access is lost.
    - would like to see communications functions extracted from protection functions so that one can be patched while the other continues to run

<u>Actions items of the previous meeting</u>

1) Marc Lacroix to contact Eyrin to get the latest version of 1686 Word document as published. Done
2) Marc Lacroix to ask Eyrin to get a copy of IEC 62351-7 for the working group. Done
3) Marc Lacroix to set an imeet central profile for S1. To do
4) Marc Lacroix to prepare initial use cases and send to working group members. Done