Protection profile of an industrial switch

Version 1.0 mid-term

GTCSI

July 13, 2015

Preface

In the whole document, the acronym ToE (Target of Evaluation) designates the component being evaluated.

Text in red differs from the short-term version of the protection profile.

1 Product description

1.1 General description

The considered ToE is an industrial switch, designed for harsh environment where IT switches can not properly operate due to heat, humidity or dust for instance.

From a feature perspective, the industrial switch interconnects different devices or network segments using Ethernet. It supports logical network segregation with VLAN.

1.2 Features

The ToE includes the following features:

- **Network segregation:** The device includes network segregation (thanks to VLANs for instance) and the associated configuration interfaces.
- **Network interfaces management:** The ToE offers the possibility to disable unused ports.
- **MAC address filtering:** The ToE offers the possibility to define a white list of MAC addresses for each Ethernet interface.
- **End-devices authentication:** The ToE supports end devices authentication using a protocol such as IEEE 802.1x.
- **Administration functions:** The ToE includes administration functions in order to configure, or program the other functionalities of the ToE. Several administration interfaces are possible:
  - thick-clients (sometimes also called, depending on the context, administration console, programming workstation. . .);
  - web-clients;
  - removable devices (USB drives, SD memory cards, etc.).
- **Redundancy functions:** The ToE includes redundancy functions in order to ensure high avaibility for one or several functions.
- **Local logging:** The ToE supports the configuration of a local logging policy. It is possible, in particular, to log security and administration events.

- **Remote logging:** The ToE supports the definition of a remote logging policy. In particular, it is possible to log security and administration events.

1.3 Product usage

Industrial switches can be used in many different contexts. Nevertheless, we can distinguish two great categories with field networks connecting remote I/O with PLCs and supervision networks connecting PLCs with the SCADA system.

In low criticality systems, it is possible to use VLAN for segregating administration functions. Such an example of a topology is given on figure 1. On this figure, the segregation ensures that each PLC can only communicate with a given remote sensor and a given actuator (VLAN 2 and 3) It also prevents the communication between PLCs (VLAN 2 and 3 for the field network and 4 and 5 for supervision network). Finally, a VLAN is dedicated to the administration of the switches and the SCADA workstation.

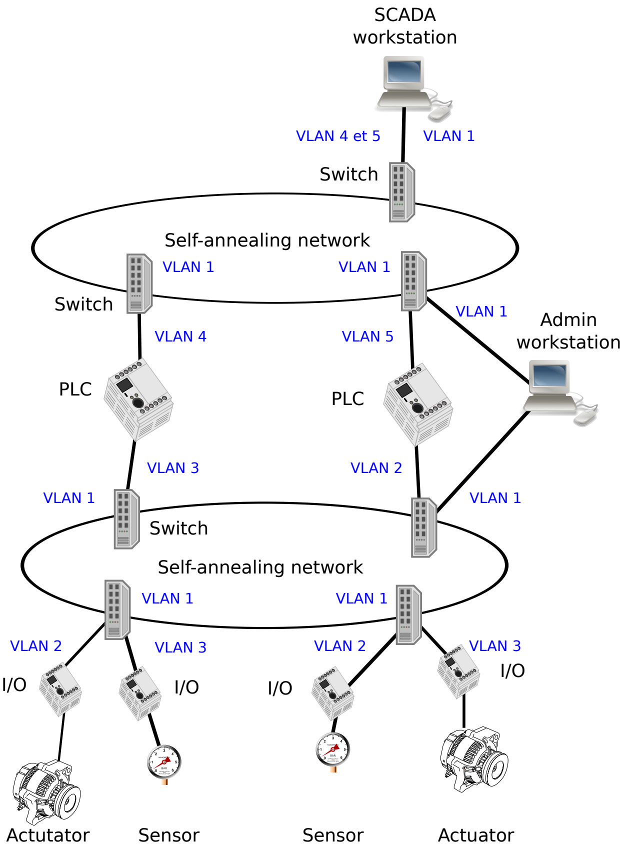

Figure 1: Networks with VLAN segregation

1.4 Users

The users that may interact with the ToE are the following:

- **Administrator:** user having the permission to modify the configuration of the ToE.
- **Auditor:** User having the permission to consult logs of the ToE.

- **Super-administrator:** User having all the privileges on the ToE. He can, in particular, create, modify or delete user accounts.
- **End-device:** End device directly or indirectly connected to the ToE.

Remark: A user is not necessary a human being, it may be a device or a third-party software. Moreover, the same person may own several user accounts corresponding to different profiles.

1.5 Assumptions

Assumptions on the environment and the use case of the ToE are the following:

- **Logs checking:** We assume that administrators check regularly the local and remote logs produced by the ToE.
- **Super-administrators:** Super-administrators are trained for performing the tasks they are responsible for. They follow instructions and administration manuals of the ToE and they are not hostile.
- **Premises:** The ToE is not necessarily in secured premises and the attacker can have access to all physical interfaces of the ToE. Similarly, the attacker can plug a trapped device (for instance, a USB drive or a SD card) on any physical port of the ToE. Conversely, the attacker cannot disassemble the ToE or perform physical attacks on it.

  Since identical products to the ToE may be purchased freely, the attacker may purchase one in order to research vulnerabilities by any possible mean.
- **Segregation policy:** We assume that the network segregation policy set up on the ToE is adapted to the use case.
- **Dimensioning:** We assume the ToE is properly dimensionned for its tasks.
- **Authentication servers:** When appropriate, the authentication servers used for authenticating users are assumed uncompromised and properly configured.
- **Unevaluated services disabled by default:** Services of the ToE which are not covered by the security target are disabled in the default configuration (also named factory default configuration).
- **Security documentation:** The ToE is provided with a complete documentation for a secure usage. In particular, all secrets are listed in order to allow their customization.

  All recommendations included in this documentation are applied prior to the evaluation.

2 Critical assets

2.1 Critical assets of the environment

The critical assets of the environment are the following:

- **Frames:** The ToE ensures the filtering and the switching of frames between end devices.
- **Logical segregation:** The ToE ensures the network logical segregation between subnetworks.
- **End devices filtering:** The ToE offers the capability of defining whitelists of MAC addresses for each Ethernet interface.
- **End devices authentication:** The ToE authenticates directly connected end-devices.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Frames	X			
Logical segregation	X		X	
End devices filtering	X		X	
End devices authentication	X		X	X
X: mandatory (X): optional				

2.2 ToE critical assets

The critical assets of the ToE are the following:

- **Firmware:** In order to work properly, the firmware must be protected both in integrity and authenticity.
- **Configuration:** The configuration of the ToE must be protected in confidentiality and integrity. The attacker must not be able to discover the configuration of the ToE by other means than the ToE activity.
- **User authentication mechanism:** This mechanism can be based on a local database or on a remote authentication server. In both cases, the ToE must ensure the integrity and authenticity of the mechanism[1].
- **User secrets:** The user secrets can be passwords, certificates. . . They can be stored in the ToE or stored in a remote authentication server. In all cases, the ToE must ensure the integrity and confidentiality of these credentials.
- **Access control policy:** The policy can be stored locally or remotely on a authentication server. In both cases, the ToE must ensure the integrity of the access control policy.
- **Local logging:** Once configured, the local logging must remain operational.
- **Remote logging:** The ToE is capable of remote logging. Once configured, the logging must remain operational.
- **Local logs:** The integrity of the local logs must be ensured by the ToE.
- **Remote logs:** The remote logs generated by the ToE must be protected in integrity and authenticity. A mechanism must be present to detect the absence of a message in a sequence of properly received messages.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Firmware			X	X
Configuration		X	X	
User authentication mechanism			X	X
User secrets		X	X	
Access control policy			X	
Local logging	X			
Remote logging	X			
Local logs			X	X
Remote logs			X	X
X: mandatory (X): optional				

[1] All authentication mechanisms offered by the ToE may not necessarily be part of the security target. However, those which are not included in the security target must be disabled by default.

3 Threat Model

3.1 Attackers

The following attackers are considered:

- **Evil end-device:** A device connected to the ToE is controlled by the attacker.
- **Evil administration device:** A device plugged on the administration network is controlled by the attacker but the attacker may not have valid credentials on the ToE.
- **Compromised administration account:** The attacker managed to compromise the credentials of a given account. This account can correspond to any role except the super-administrator.

3.2 Threats

The following threats are considered:

- **Denial of service on redundancy:** By exploiting a bug or a vulnerability of the ToE, the attacker manages to prevent, even temporarly, a topology change due to another device failure.
- **Denial of service:** The attacker manages to generate a denial of service on the ToE by performing an unexpected action or by exploiting a vulnerability (sending a malformed request, using a corrupted configuration file. . .). This denial of service can affect the whole ToE or only some of its functions.
- **Network segregation violation:** The attacker manages to violate the logicial network segregation.
- **Device filtering policy violation:** The attacker manages to connect an end device to the ToE and makes the ToE to transmit some of its traffic despites the filtering policy.
- **Firmware alteration:** The attacker manages to inject and run a corrupted firmware on the ToE. The code injection may be temporary or permanent and this does include any unexpected or unauthorized code execution.

  A user may attempt to install that update on the ToE by legitimate means.

  Finally, the attacker manages to modify the version of the firmware installed on the ToE without having the privilege to do so.
- **Configuation alteration:** The attacker manages to modify, temporary or permanently, the ToE configuration.
- **Configuration compromise:** The attacker manages to illegally obtain some parts of the ToE configuration.
- **Credentials theft:** The attacker manages to steal user credentials.
- **Authentication violation:** The attacker succeeds in authenticating himself without credentials.
- **Access control violation:** The attacker manages to obtain permissions that he does not normally have.
- **Local logs alteration:** The attacker manages to delete or modify a local log entry without being authorized by the access control policy of the ToE.
- **Remote logs alteration:** The attacker manages to modify a remote log entry without the receiver being able to notice it. The attacker manages to delete a remote log message without the receiver being able to notice it.

4 Security objectives

The following security objectives are considered:

- **Malformed input management:** The ToE has been developped in order to handle correctly malformed input, in particular malformed network traffic.
- **Network segregation policy:** The ToE support logical network segregation (with VLANs or PVLANs).
- **End-device filtering enforcement:** The ToE supports MAC address filtering.
- **Secure connection with the authentication server:** The ToE supports secure connection with the authentication server. The secure connection allows authenticating both peers and protecting the integrity and the authenticity of exchanges. It guarantees also non replay of exchanges.
- **Secure storage of secrets:** User secrets are securely stored in the ToE. In particular, the compromise of a file is not sufficient for retrieving them.
- **Secure authentication on administration interface:** Session tokens are protected against hijack and replay. They have a short lifespan. The identity and the permissions of the user account are systematically checked before any privileged action.
- **Access control policy:** The access control policy is strictly applied. In particular, the implementation guarantees the authenticity of privileged operations, i.e. operations that can alter identified critical assets.
- **Firmware signature:** At each update of the firmware, the integrity and authenticity of the new firmware are checked before updating. The integrity and authenticity of the firmware are also checked at boot time.
- **Configuration confidentiality and integrity:** The access control prevents any unauthorized person to read or modify the configuration of the ToE.
- **Logs integrity:** The integrity of the generated local logs is ensured and only the super-administrator is permitted to modify them.
- **Alarms integrity:** The ToE supports secure remote logging where authenticity and integrity are ensured. The transmission is also protected against replay and a mechanism is implemented for detecting missing logs.

A Critical assets vs threats

	Frames	Logical segregation	End devices filtering	End devices authentication	Firmware	Configuration	User authentication mechanism	User secrets	Access control policy	Local logging	Remote logging	Local logs	Remote logs
Denial of service on redundancy	Av												
Denial of service	Av	Av I	Av	Av						Av	Av		
Network segregation violation		I											
Device filtering policy violation			I										
Firmware alteration					I Au								
Configuation alteration						I							
Configuration compromise						C C							
Credentials theft								C I C					
Authentication violation				I Au			I Au						
Access control violation									I				
Av: Availability, I: Integrity, C: Confidentiality, Au: Authenticity													

	Frames	Logical segregation	End devices filtering	End devices authentication	Firmware	Configuration	User authentication mechanism	User secrets	Access control policy	Local logging	Remote logging	Local logs	Remote logs
Local logs alteration												I Au	
Remote logs alteration													I Au
Av: Availability, I: Integrity, C: Confidentiality, Au: Authenticity													

B Threats vs security objectives

	Denial of service on redundancy	Denial of service	Network segregation violation	Device filtering policy violation	Firmware alteration	Configuation alteration	Configuration compromise	Credentials theft	Authentication violation	Access control violation	Local logs alteration	Remote logs alteration
Malformed input management	X	X										
Network segregation policy			X									
End-device filtering enforcement				X								
Secure connection with the authentication server									X			
Secure storage of secrets								X				
Secure authentication on administration interface						X	X	X	X			
Access control policy										X		
Firmware signature					X							
Configuration confidentiality and integrity						X	X					
Logs integrity											X	

	Denial of service on redundancy	Denial of service	Network segregation violation	Device filtering policy violation	Firmware alteration	Configuation alteration	Configuration compromise	Credentials theft	Authentication violation	Access control violation	Local logs alteration	Remote logs alteration
Alarms integrity												X

C Contributors

This protection profile has been produced by the working group on cybersecurity for industrial systems, supervised by the French Network and Information Security Agency (ANSSI).

The following compagnies and organisms contributed to this document:

- Amossys
- ARC Informatique
- Belden
- DGA/MI
- Gimelec
- Oppida
- Phoenix Contact
- RATP
- Schneider Electric
- Siemens
- Sogeti
- Stormshield
- Thales