Protection profile of an industrial wireless basestation

Version 1.0 short-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 mid-term version of the protection profile.

1 Product description

1.1 General description

The ToE considered in this protection profile is a wireless base station. This kind of device allows connecting a wired industrial control system to a subset of wireless industrial devices. A wireless base station can support technologies such as IEEE 802.15.4, IEEE 802.11, etc. In many cases, such devices make the communication possible between a static system and mobile elements.

The wireless base station must run properly in an hostile environment. In particular, it must operate correctly in case of humidity, dust or extreme temperatures.

The security of wireless links does not only rely on the base station security mechanisms. In particular, the security of cryptographic mechanisms depends on the wireless devices connected to the base station. In some architectures, the authentication is ensured by an external server. In other architectures, there is a controller which manages partially or totally the security. Depending on the situation, this devices must be included in the perimeter of the security target or they must be subject to an independent security evaluation.

In most cases, the wireless base station includes the folowing elements:

Wireless interfaces These interfaces allow to connect wireless elements. The can also serve as relay to another base station.

Wired interfaces In many cases, the wired base station connect wireless devices to a wired network.

Administration interfaces These interfaces allow the configuration of the device and, in particular, the security of wireless channels.

1.2 Features

The ToE includes the following features:

- **Wireless communication:** Radio devices can connect to the ToE thanks to its wireless interface.
- **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.).
- **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

The ToE is mainly used in two different configurations. In the first use case, it is directly connected to the wired network and it used as a access point for wireless devices. For each connection, only the last hop is wireless. This use case is depicted on figure 1.

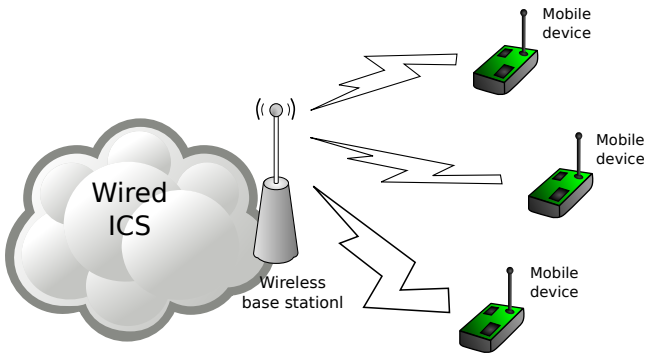

Figure 1: Wireless base station with mobile devices

In the second use case, some devices are out of the radio range of the access point. In this case, the wireless base station can be used as a relay and some connections require two wireless hops. This second use case is depicted on figure 2.

In the third use case, two wired industrial networks must communicate but the usage of a wired connection is not possible as it is the case for the communication between the platform and an embedded system on board for a vehicle. This use case is depicted on figure 3.

Finally, in some cases, especially when the physical protection of the wireless base station is difficult to ensure, we can use a light-weight acess point with an associated controller, that is stored in safer premices. This situation is given in figure 4.

In all described use cases, a network interface must be dedicated to administration in order to be connected to an administration network, isolated from the production network. Ideally, this network interface should be physically different from the production interface. At least, a virtual segregation with a VPN or VLANs must be used. For the relay base station represented on figure 2, a dedicated wireless link on a distinct bandwidth can be used. If this is not possible, a segregation with VPN or at least VLANs on the same channel can be used.

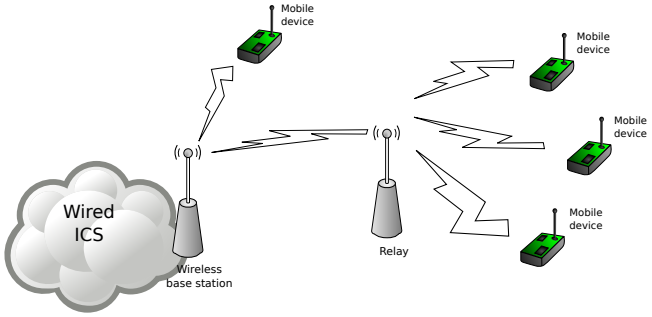

Figure 2: Network with a relay

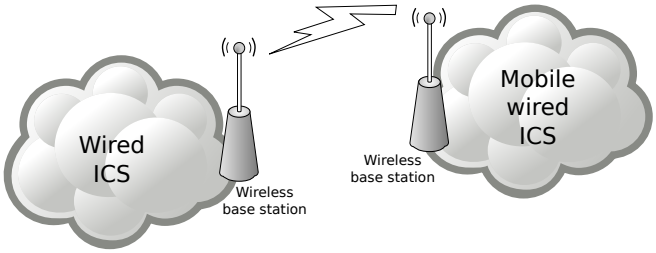

Figure 3: Wireless communication between to wired networks

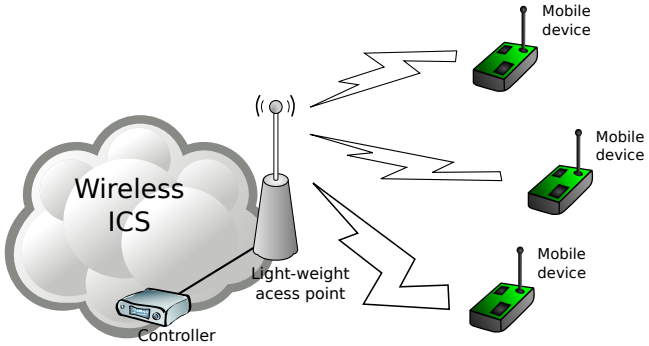

Figure 4: Light-weight base station with a controller

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.
- **Administrators:** ToE administrators are competent, trained and trustworthy.
- **Premises:** The ToE is located in secure premises with a restricted access limited to trustworthy people. In particular, the attacker does not have access to the physical ports of the ToE.

  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.
- **Wireless authentication policy:** We assume that the authentication 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.
- **Active logging:** We assume that local and remote logging are operational and that local logs are not corrupted.
- **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.
- **Roaming:** The ToE must ensure the communication handover when the device is moving inside the network.
- **Logical segregation:** The ToE ensures the network logical segregation between sub-networks.
- **Wireless devices authentication:** The ToE authenticates the end devices on the wireless channel.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Frames	X	X	X	X
Roaming	X			
Logical segregation	X		X	
Wireless 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.

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	
X: mandatory (X): optional				

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 wireless device within range:** The attacker manages a device in the radio range of the ToE but it does not have valid credentials on the ToE.
- **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.

3.2 Threats

The following threats are considered:

- **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.

[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.

- **Network segregation violation:** The attacker manages to violate the logicial network segregation.
- **Wireless communication alteration:** The attacker manages to corrupt data sent on the wireless channel between the ToE and legitimate radio devices.
- **Wireless communication compromise:** The attacker manages to compromise data sent on the wireless channel between the ToE and legitimate radio devices.
- **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.

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).
- **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 wireless communication:** The ToE supports secure communication mechanisms on the wireless channel.
- **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, integrity and authenticity of the new firmware are checked before updating.

- **Configuration confidentiality and integrity:** The access control prevents any unauthorized person to read or modify the configuration of the ToE.

A Critical assets vs threats

	Frames	Roaming	Logical segregation	Wireless devices authentication	Firmware	Configuration	User authentication mechanism	User secrets	Access control policy
Denial of service	Av	Av	Av I	Av					
Network segregation violation			I						
Wireless communication alteration	I Au								
Wireless communication compromise	C C								
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

B Threats vs security objectives

	Denial of service	Network segregation violation	Wireless communication alteration	Wireless communication compromise	Firmware alteration	Configuation alteration	Configuration compromise	Credentials theft	Authentication violation	Access control violation
Malformed input management	X									
Network segregation policy		X								
Secure connection with the authentication server									X	
Secure wireless communication			X	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			

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