INFOCOMM MEDIA DEVELOPMENT AUTHORITY

Technical Specification

Security Requirements for Private Automatic Branch Exchanges (PABX)

Draft IMDA TS PABX-SEC
Issue 1, May 2024

Info-communications Media Development Authority of Singapore
Infocomm Resource & Technology
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Content

ADVISED TO OBTAIN THEIR OWN LEGAL AND/OR TECHNICAL ADVICE IN RELATION TO THE IMPLEMENTATION OF THE STANDARD IF REQUIRED.

Security Requirements for Private Automatic Branch Exchanges (PABX)

1 Scope

This Specification defines the minimum technical security requirements for design and management of Private Automatic Branch Exchanges (PABX) that can connect to the Telecommunication Provider Networks, examples of which are as shown in Figure 1.

This IMDA Technical Specification sets out to minimise the vulnerability of the individual Private Automatic Branch Exchanges (PABX), ensuring that these systems are better protected when purchased and deployed by enterprises, thus safeguarding both the Telecommunication Provider Networks and enterprise PABX from security threats from the Internet.

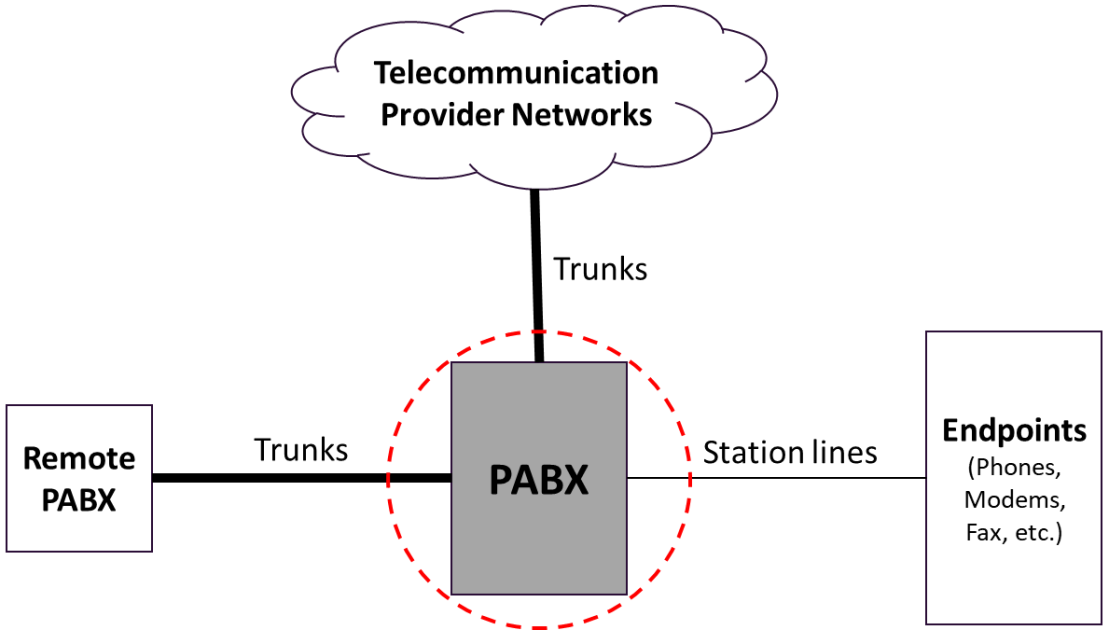

Figure 1: Typical connectivity of Private Automatic Branch Exchange (PABX)

2 References

For the technical requirements captured in this specification, references have been made to the following best practices and recommendations.

a. ITSA, Nov 2016: Recommendations for secure deployment of an IP-PBX

3 Definitions and Abbreviations

For the purpose of this specification, the following terms and definitions apply.

3.1 Definitions

Private Automatic Branch Exchange	A private telephone network used by enterprises to connect its staff to telecommunication provider networks and other PABXs. It provides multiple telecommunication lines for its clients to reach its staff and for its staff to outreach its clients.
Access Control	Functions that include identification, authentication, authorisation and accountability.
Login Credential	A set of identity data such as username and password, used to obtain access to system or network resources.
Default Login Credential	A set of predesignated common identity data that is usually provided for initial setup or after factory reset.
Management Interface	A network interface used specifically for configuration and management operations.
Data Elements	Information with unique meaning and distinct values such as account number, name and address.

3.2 Abbreviations

AES	Advanced Encryption Standard
HTTPS	HyperText Transfer Protocol Secure
ID	Identifier
LAN	Local Area Network
SSH	Secure Shell
WAN	Wide Area Network
WPA2	Wi-Fi Protected Access 2

4 Security Requirements

4.1 Login Credentials Management

The PABX system with pre-loaded login credentials, such as usernames and passwords, can be easily compromised, thereby allowing an attacker to gain access and use the device for malicious activities. The following measures are typical of industry practices to ensure that login credentials used for access controls are adequately protected.

4.1.1 Factory Pre-loaded Login Credentials

The PABX system shall be in a disabled state (non-functioning) until the user successfully set new login credentials upon first attempt to access the device's administrator interface and the device's configuration settings

4.1.2 Minimum Password Strength

Access to PABX system's user/administrator interfaces (e.g., administrator page, extension registration page, voicemail) and device's configuration settings shall only accept unique passwords that meet the following requirements:

a. The minimum length of a password shall be 10, and shall meet at least 2 out of the following 4 complexity rules:
    i. Minimally 1 uppercase character (A-Z)
    ii. Minimally 1 lowercase character (a-z)
    iii. Minimally 1 digit (0-9)
    iv. Minimally 1 special character (punctuation and/or space)
b. The password shall not have consecutive identical characters.
c. Values used in the login ID and password shall not be the same.

4.2 Device Setup & Administration

The PABX system needs to manage and control the access to device's user/administrator interfaces; ensuring only authorised personnel are able to edit the configuration settings. While it is important to restrict intruder access, it also needs to protect the device from being unintentionally or maliciously locked out.

4.2.1 Device Pre-loaded Settings

a. The PABX system shall disable the following system services (on both LAN and WAN interfaces) by default:
    i. SSH
    ii. FTP
    iii. TFTP
    iv. Any services or ports that are not in use
b. The PABX system shall disable feature(s) that collects and sends the device's network statistics data back to manufacturer by default.
c. The PABX system shall enable its firewall by default to prevent its internal systems from being accessed directly from the Internet.
d. The PABX system shall allow changes to its default ports for all its services when needed.

4.2.2 Initial Setup Handling

First attempt to access to the PABX system administrator interface should be conducted through a wired connection. If a wireless connection is used, the wireless communication should leverage on at least AES encryption, with at least WPA2 protection.

4.2.3 Authentication Handling

The PABX system shall ensure strong authentication, and protect against brute force and/or other abusive login attempts to the user/administrator interfaces:

a. Unprotected access to the PABX system's user/administrator interfaces shall be prohibited. Access to the PABX system's user/administrator interfaces shall only via authenticated credentials.
b. Authentication credentials shall be salted and hashed.
c. The login account shall be blocked after a fixed number of unsuccessful login attempts. A lockout period shall be enforced after account has been blocked.
d. Secure alternative authentication mechanism or physical factory reset shall be provided to fall-back on, when a login account is blocked.

4.2.4 Password Handling

The PABX system shall ensure that the credentials are properly managed to avoid them being compromised when they are used:

a. Password shall not be displayed by default on a user's screen and shall be masked with the asterisk character, or another benign glyph. Private Branch Exchange System may have an option to unmask passwords at user's own discretion.
b. Password recovery or reset mechanism shall be protected and does not supply an attacker with any form of information indicating a valid account.

4.2.5 Device Management Interface

The PABX system's user/administrator interfaces shall be protected via international standardised secure communication protocol such as HTTPS to prevent the communication channel from being sniffed by unauthorised actors with malicious intent. Signed certificates from a Certification Authority ("CA") and self-signed certificates can be considered for this purpose.

4.3 Firmware Updates

a. The PABX system shall automatically download the latest security patches.
b. The PABX system shall be updated with the latest security patches automatically. Patching could be carried out through different means and mechanisms, e.g., when Private Branch Exchange System is powered off and on.
c. The PABX system should also provide means for users to manually run and install the downloaded security patches.
d. Minimum period of the firmware support received by the PABX system shall be provided upfront to the user.
e. The device manufacturer should ensure the patches:
    i. do not contain sensitive data such as hardcoded credentials; and
    ii. are transmitted via secured connection.
f. Security updates for the PABX system should be provided in a timely manner. "Timely" in this context varies with the criticality of the identified vulnerability, the availability of a fix and the complexity of fix. The complexity of the fix is dependent on factors, such as constrained devices, involvement of multiple stakeholders, hardware versus software fix, etc.

4.4 Data Protection

4.4.1 Data Confidentiality

The PABX system shall ensure that data used within its scope of functionality are secured and confidential.

a. The PABX system should provide the option to encrypt media and data using protocol such as Secure Real-Time Transport Protocol (SRTP).
b. If the data elements are encrypted, the encrypted key shall be securely stored.
c. Encryption algorithms used should be replaceable so that improved encryption algorithms can be adopted without significant change to existing device.

4.4.2 Event Notification

If the PABX system has an Event Notification features, there should be a notification created to sent alerts on important events occurred (e.g., functions failure).

4.4.3 Data Backup

The PABX system should have an option to schedule backup for purpose of restoring configuration and data.

4.5 Securing the Trunk

Usage of PABX system's functions for outbound or international calls should be restricted for each user to prevent misuse. The following measures can help to increase security:

a. Setting different outbound routes for different trunks:
    i. Internal
    ii. Local
    iii. International

    Assign outbound route permission only to users that require the use of it.
b. Disallow anonymous incoming calls to prevent attacker from dialing into PABX system to generate an outbound call, and incur call charges. If Interactive Voice Response (IVR) is used, limit the extension dialling to only necessary extension.
c. The Private Branch Exchange System shall have the feature to allow user to configure restrictions on outbound calls. Restrictions shall include user authentication with unique account code and/or limiting the number of outgoing calls within a user defined period.

4.6 Validation of Data Inputs

Data input to the device via all interfaces shall be validated, to minimally protect the PABX system from actions such as information leakage, remote code execution and cross-site scripting.

4.7 Reporting

4.7.1 Report on Calls

The PABX system shall have an option to schedule report(s) to review on call logs daily.

4.7.2 Vulnerability Reporting

A point of contact, e.g., email address and contact number shall be provided to allow the reporting of security vulnerabilities relating to the PABX.

Annex A

Conformance Testing / Verification Checklist

This Checklist is intended for facilitating Supplier's Declaration of Conformity to the technical requirements defined in the IMDA Technical Requirements for Security Requirements for Private Automatic Branch Exchange ("IMDA TS PABX-SEC")

Please note:

"**CR**" indicates that the technical requirement set out in a particular section or sub-section ("§") of the IMDA TS PABX-SEC is a **Compliance Requirement**.

"**M**" means that it shall be **Mandatory** for the PABX to comply with the technical requirement set out in the IMDA TS PABX-SEC § cited in this Checklist (Table given below).

"**C**" means that compliance with the technical requirement set out in the IMDA TS PABX-SEC § cited in this Checklist is **Conditional**. In this case, the need to comply is contingent on the conditions as indicated in the remarks column.

"**V**" means that compliance with the requirement is **Voluntary**.

IMDA TS PABX-SEC §	Parameter	CR	Yes/No/NA	Remarks
4.1	Login Credentials Management	-	-	
4.1.1	Factory pre-loaded Login Credentials	M		
4.1.2	Minimum Password Strength	-	-	
	4.1.2.a	M		
	4.1.2.b	M		
	4.1.2.c	M		
4.2	Device Setup & Administration	-	-	
4.2.1	Device Pre-loaded Settings	-	-	
	4.2.1.a	C		If the features are available in the PABX system
	4.2.1.b	C		If the features are available in the PABX system
	4.2.1.c	M		
	4.2.1.d	C		If the features are available in the PABX system
4.2.2	Initial Setup Handling	V		
4.2.3	Authentication Handling	-	-	
	4.2.3.a	M		
	4.2.3.b	M		
	4.2.3.c	M		
	4.2.3.d	M		
4.2.4	Password Handling	-	-	
	4.2.4.a	M		
	4.2.4.b	M		
4.2.5	Device Management Interface	M		
4.3	Firmware Updates	-	-	
	4.3.a	C		If the system has i) internet connection or ii) an intermediary solution that allow Private Branch Exchange System to received security patches.
	4.3.b	M		
	4.3.c	V		
	4.3.d	M		

	4.3.e	M		
	4.3.f	V		
4.4	Data Protection	-	-	
4.4.1	Data Confidentiality	-	-	
	4.4.1.a	M		
	4.4.1.b	C		If the features are available in the PABX system
	4.4.1.c	C		If the features are available in the PABX system
4.4.2	Event Notification	V		If the features are available in the PABX system
4.4.3	Data Backup	M		
4.5	Securing the Trunk	-	-	
	4.5.a	M		
	4.5.b	C		If the features are available in the PABX system
	4.5.c	M		
4.6	Validation of Data Inputs	M		
4.7	Reporting	-	-	
4.7.1	Report on Calls	M		
4.7.2	Vulnerability Reporting	C		If vendor/product has a feature that allow security vulnerability related to PABX to be reported