Technical Specification

Security Requirements for Residential Gateways

IMDA TS RG-SEC
Issue 1, October 2020

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

Content

Security Requirements for Residential Gateways

1 Scope

In light of the vast and increasing deployment of Internet of Things ("IoT") devices in Singapore and globally, this Specification defines the minimum technical security requirements for design and management of Residential Gateways that are the gateways to home IoT devices, examples of which are as shown in Figure 1.

This IMDA Technical Specification sets out to minimise the vulnerability of the individual Residential Gateway, ensuring that these devices are better protected when purchased and deployed by consumers, thus safeguarding both the Communication Networks and the home IoT devices from security threats from the Internet.

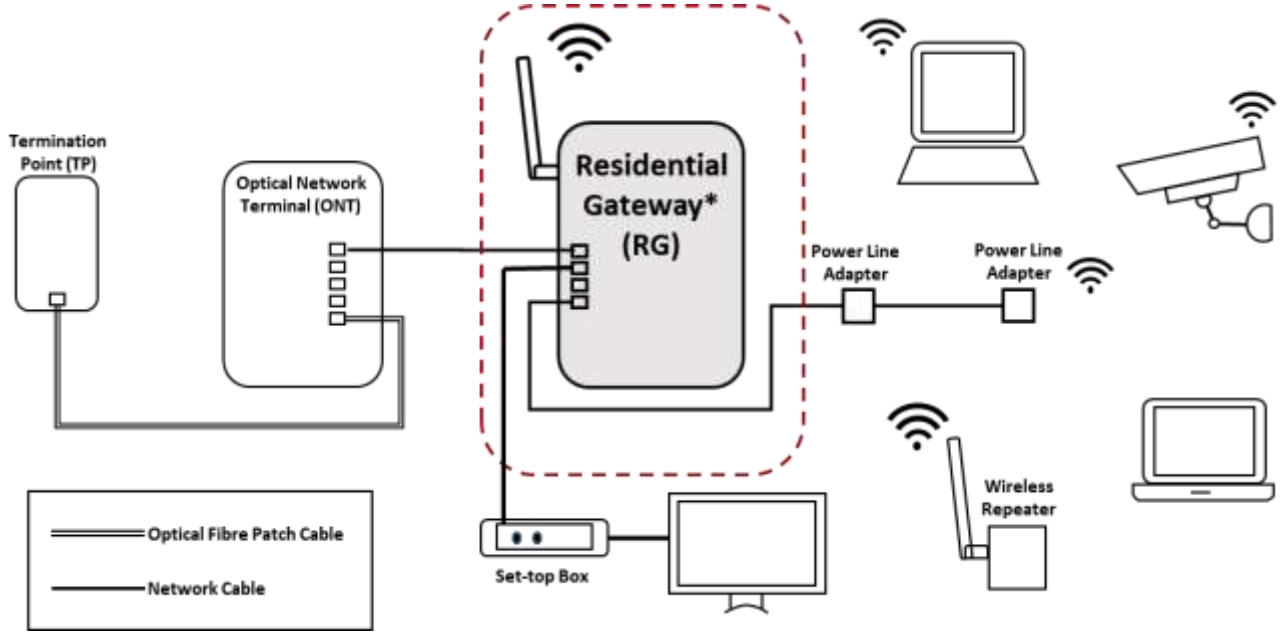

Figure 1: Typical Home Network Connection with Residential Gateway

2 References

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

a. ENISA, Nov 2017: Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures

b. GSMA CLP.13: IoT Security Guidelines Endpoint Ecosystem Version 2.0 31 October 2017

3 Definitions and Abbreviations

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

3.1 Definitions

Residential Gateway	A powered home networking device, typically used as a gateway to connect devices in the home to the Internet Access Service Provider's ("IASP") network as shown in Figure 1.
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
CPE	Customer Premises Equipment
DDoS	Distributed Denial of Service
HNAP	Home Network Administration Protocol
HTTPS	HyperText Transfer Protocol Secure
ID	Identifier
IoT	Internet of Things
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
LAN	Local Area Network
NAT	Network Address Translation
NAT-PMP	NAT Port Mapping Protocol
PCP	Port Control Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
UPnP	Universal Plug and Play
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPS	Wi-Fi Protected Setup
XSS	Cross-Site Scripting

4 Security Requirements

4.1 Login Credentials Management

The Residential Gateway 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 such as participation in botnets to perform DDoS attacks, Man-in-the-Middle attacks and/or through it to infiltrate other connected home IoT devices. 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

Factory pre-loaded login credentials such as passwords shall be randomised and unique for each Residential Gateway. If pre-loaded login credentials are used and they are not randomised and unique, the Residential Gateways shall be in a disabled state (non-functioning) until the user successfully set new login credentials upon first attempt to access the device's administration login page and the device's configuration settings.

4.1.2 Minimum Password Strength

Access to Residential Gateway's administrative login page 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 Residential Gateway needs to manage and control the access to device's administration page; ensuring only authorised personnel are able to edit the configuration settings. While it is important to restrict intruder access, the Residential Gateway also needs to protect the device from being unintentionally or maliciously locked out.

4.2.1 Device Pre-loaded Settings

a. The Residential Gateway shall disable the following system services (on both LAN and WAN interfaces) by default:
    i. WPS
    ii. HNAP
    iii. SSH
b. The Residential Gateway shall disable the following Residential Gateway WAN interfaces by default:
    i. NAT-PMP
    ii. PCP
    iii. Remote Administration
    iv. SNMP
    v. Telnet
    vi. UPnP
c. The Residential Gateway shall disable feature(s) that collects and sends the device's network statistics data back to manufacturer by default.
d. The Residential Gateway shall enable its firewall by default and support NAT to prevent its internal systems from being accessed directly from the Internet.
e. The Residential Gateway shall disable IPv6 tunnelling mechanisms by default. Most modern operating systems use IPv6 by default and thus, some operating systems will attempt to pass IPv6 traffic in an IPv4 wrapper using tunnelling capabilities, such as Teredo, 6to4, or ISATAP.

These tunnels could be used to create a hidden channel of communication to and from the Residential Gateway.

4.2.2 Initial Setup Handling

First attempt to access to the Residential Gateway's administration page/settings 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 Residential Gateway shall ensure strong authentication, and protect against brute force and/or other abusive login attempts to the administration page/settings [ENISA GP-TM-25]:

a. Unprotected access to the Residential Gateway's management webpage shall be prohibited. Access to the Residential Gateway's management webpage shall only via authenticated credentials.
b. Authentication credentials shall be salted and hashed.
c. Periods of login delay shall be employed after each subsequent failed attempt.
d. The login account shall be blocked after a fixed number of unsuccessful login attempts.
e. Secure alternative authentication mechanism or physical factory reset shall be provided to fall-back on, when a login account is blocked.

4.2.4 Credentials Handling

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

a. Password fields shall prevent its contents from being copied.
b. Password shall not be displayed by default on a user's screen and shall be masked with the asterisk character, or another benign glyph. Residential Gateway may have an option to unmask passwords at user's own discretion.
c. Password recovery or reset mechanism shall be protected and does not supply an attacker with any form of information indicating a valid account [ENISA GP-TM-26]
d. Network management credentials, e.g., remote login credentials specified in Broadband Forum's Technical Report 069 ("TR-069")[1], shall not be displayed on the Residential Gateway's management web page.

4.2.5 Device Management Interface

The Device management interface to the Residential Gateway 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 Residential Gateway shall automatically download the latest security patches.
b. The Residential Gateway shall be updated with the latest security patches automatically. Patching could be carried out through different means and mechanisms, e.g., when Residential Gateway is powered off and on.
c. The Residential Gateway should also provide means for users to manually run and install the downloaded security patches.
d. The Residential Gateway shall verify the patches are digitally signed before installing them.
e. Minimum period of the firmware support received by the Residential Gateway shall be provided upfront to the user.
f. The device manufacturer should ensure the patches:
    i. do not contain sensitive data such as hardcoded credentials; and
    ii. are transmitted via secured connection.

[1] TR-069 is a technical specification of the Broadband Forum that defines an application layer protocol for remote management of customer-premises equipment (CPE) connected to an Internet Protocol (IP) network.

g. Security updates for the Residential Gateway 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 Wireless Access Protection

a. The Residential Gateway should employ strong passwords as described in Section 4.1.2 for Wi-Fi connection.
b. The Residential Gateway shall use encryption such as AES, with at least WPA2 protection by default. If weaker security protection such as WPA is chosen by users, warning(s) of the higher security risk to use these encryption algorithms shall be displayed.
c. The Residential Gateway should have the feature to allow user to setup guest networks. If a guest network is setup, separate credentials shall be provided for authorised guest users & guest IoT devices of the home network, isolating these accounts from the main home network.

4.5 Data Protection

a. The data elements used by the Residential Gateway shall be salted and hashed.
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.

4.6 Validation of Data Inputs

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

4.7 Vulnerabilities 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 Residential Gateway.

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 Residential Gateways ("IMDA TS RG-SEC")

Please note:

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

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

"**C**" means that compliance with the technical requirement set out in the IMDA TS RG-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 RG-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 Residential Gateway
	4.2.1.b	C		If the features are available in the Residential Gateway
	4.2.1.c	C		If the features are available in the Residential Gateway
	4.2.1.d	C		If the features are available in the Residential Gateway
	4.2.1.e	C		If the features are available in the Residential Gateway
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		
	4.2.3.e	M		
4.2.4	Credentials Handling	-	-	
	4.2.4.a	M		
	4.2.4.b	M		
	4.2.4.c	M		
	4.2.4.d	M		
4.2.5	Device Management Interface	M		
4.3	Firmware Updates	-	-	
	4.3.a	M		
	4.3.b	M		
	4.3.c	V		

	4.3.d	M		
	4.3.e	M		
	4.3.f	V		
	4.3.g	V		
4.4	Wireless Access Protection	-	-	
	4.4.a	V		
	4.4.b	M		
	4.4.c	C		If the features are available in the Residential Gateway
4.5	Data Protection	-	-	
	4.5.a	M		
	4.5.b	C		If the features are available in the Residential Gateway
	4.5.c	V		
4.6	Validation of Data Inputs	M		
4.7	Vulnerabilities Reporting	M		