Add value.
Inspire trust.

RESPONSE TO CONSULTATION ON SECURITY REQUIREMENTS FOR RESIDENTIAL GATEWAYS

Submitted by:

Chien Koh Wei
Assistant Vice President
Product Service/ Electrical Electronic Centre
Phone: +65 6885 1356/ +65 9173 2058
E-mail: Koh-Wei.CHIEN@tuv-sud-psb.sg

TÜV SÜD PSB Pte Ltd
No. 1 Science Park Drive
Singapore 118221

Submission Date: 13th May 2020
Version 1.0

Table of Contents

1. Summary of major points 3
2. Statement of Interest 3
3. Comments 4
    Question 1 4
    Question 2 6
    Question 3 7
    Question 4 7
    Question 5 8
    Question 6 9
    Question 7 9
    Question 8 9
    Question 9 10
    Question 10 11
    Question 11 11
4. Conclusion 12

1. Summary of major points

The questions stated by IMDA in the consultation paper for Residential Gateways are responded here by TÜV SÜD. The comments are reflected in the table of section 3 in the form of clarifications, suggestions and proposed changes.

2. Statement of Interest

TÜV SÜD welcomes new regulations that IMDA is setting up for Residential Gateways. We would like to participate more actively in offering our technical expertise and test services to the industry in creating a more secured cyber environment.

TÜV SÜD has a rich history of more than 150 years of participating in the creation of standards across various industries and is currently a **seating member of standards organizations like IEC, EN, ETSI, IEC, ENISA, European Union Safety and Security group**. At the present moment, we are also active in the discussion of the new IoT regulations such as NIST 8259 and ETSI EN 303 645, where we have written up detailed test procedures to answer the needs of manufacturers.

We have read through the IMDA TS RG-SEC and have consolidated our views and comments into this document. We hope these comments would be helpful to provide the public with a better understanding of requirements of IMDA TS RG-SEC.

Furthermore, if there is such a process for a laboratory to apply for recognition by IMDA, we are open to discussion on how TÜV SÜD can become recognized in order to perform security tests for manufacturers/suppliers of Residential Gateways.

3. Comments

No.	IMDA Question No.	Clause	Type of comment	Comments	Proposed changes
1	1	4.1	Suggestion	The error message of failed logins shall not divulge any information about the existence of username. This is to prevent the malicious intend to obtain more information of the valid user account, but wrong password.	To add a new subclause: “ 4.1.3 Error Message of Failed Logins The error message shall not divulge any information about the existence of username. For example: “Wrong username or password” is preferred over “Wrong username” or “Wrong password” ”
2	1	4.1.1	Clarification & Suggestion	More clarification is required on the definitions of factory preloaded credential and default login credentials. There might not be referring to the same thing. Unique passwords might not be the same as default passwords. Universal default password might not be the same as default password.	To modify the text to: “ Factory pre-loaded login credentials such as passwords shall be randomised and unique for each Residential Gateway. If factory pre-loaded login credentials are not unique, the Residential Gateways shall be in a disabled state (non-functioning) until the user successfully sets new login credentials upon first attempt to access the device’s administration login page and the device’s configuration settings. ”
3	1	4.1.1	Suggestion	In addition to the manufacturers’ declaration of conformity, the manufacturers’ documentation on how they produce unique usernames or passwords is also required to be able to evaluate whether these credentials are indeed randomly generated.	n/a

No.	IMDA Question No.	Clause	Type of comment	Comments	Proposed changes
4	1	4.1.2	Clarification & suggestion	a. Why is the required minimum password length 10 characters? Suggest to refer to NIST 800-63B Section 5.1.1.1 for minimum of 8 characters as requirement. Refer to (https://pages.nist.gov/800-63-3/sp800-63b.html#sec5). b. For (a-iv), to allow any printable special character to increase the key space, instead of punctuation only. And to exclude white space because leading, trailing or consecutive white spaces are hard to identify. Refer to (https://owasp.org/www-community/password-special-characters).	To modify the text to: “ a. The minimum length of a password shall be 8 characters, and shall meet … iv. Minimally 1 special character (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~) b. (unchanged) c. The password shall not have a string of more than two consecutive characters of increasing or decreasing orders. E.g. ‘123’ or ‘cba’ d. Values used in the login ID and password shall not be the same regardless upper or lower case E.g. login ID: ‘TVSUD’, password: ‘tvSUD#01’ ”

No.	IMDA Question No.	Clause	Type of comment	Comments	Proposed changes
5	2	4.2.1	Suggestion	Only requiring that the explicitly listed services and interfaces to be turned off by default (similar to blacklisting) means that any other insecure service or interface can be turned on by default. It is, therefore, recommended to use a whitelisting approach instead and only allow for a minimal set of secure services and interfaces by default. a) and b) could be combined and rephrased as follows to require more hardening.	To combine text of a) and b): “ a) The Residential Gateway shall only offer a minimal set of secure ways to access its management interface by default. System services and interfaces that are not required for the Residential Gateway’s core functionality shall be turned off by default. These include, but are not limited to: i. WPS ii. HNAP iii. Remote Administration iv. SNMP v. NAT-PMP vi. Telnet vii. UPnP viii. FTP ”
6	2	4.2.1	Suggestion	Additional voluntary requirement to firewall settings in Residential Gateway.	To add a new text: “ x) The Residential Gateway shall provide documentation stating a minimal set of firewall configuration. In addition to the manufacturers’ declaration of conformity, the documentation on the minimal firewall configuration is also required. ”

No.	IMDA Question No.	Clause	Type of comment	Comments	Proposed changes
7	3	4.2.4	Suggestion	Displaying password in cleartext can be very useful, particularly for entry of a long random password.	To modify the text to: “ b) “Passwords shall be masked with the asterisk character, or another benign glyph by default. Residential Gateway should have an option to unmask passwords at user’s own discretion.” ”
8	3	4.2.5	Clarification	There is no information of minimum requirement for a secure communication protocol provided. Some manufacturers are known to use HTTP in combination with own proprietary encryption to access the Residential Gateway. Can this be acceptable?	n/a
9	3	4.2	Suggestion	A factory reset mechanism would be helpful for password recovery.	To add a new subclause: “ 4.2.6 Factory Reset The Residential Gateway shall offer a factory reset mechanism that can only be triggered by authorized users to revert to default configuration. ”
10	4	4.3	Clarification	e) What does ‘upfront’ mean? Shall the minimum period of firmware support be printed on the purchased RG box or otherwise known to the user before the purchase of the RG?	n/a

No.	IMDA Question No.	Clause	Type of comment	Comments	Proposed changes
11	4	4.3	Suggestion	Add an additional requirement (voluntary) with respect to a) and b).	To add a new subclause: “ h) The Residential Gateway should inform the user when a patching process starts and report the status upon completion. E.g. ‘Patch 1.2.3 installed successfully. ”
12	5	4.3	Clarification & Suggestion	For g), to change this requirement from voluntary to mandatory as it is important that the Residential Gateway can provide critical security update on time. Upper limit for a security update shall be within 90 days. A patch for a critical vulnerability shall be rolled out within 30 days. However, we also understand that it may be challenging for manufacturers to meet this requirement. Manufacturers could publish a table that shows how soon they intend to fix vulnerabilities based on their criticality. A verification mechanism would be required to confirm compliance of this requirement as it will be a post-market implementation.	n/a
13	5	4.3	Suggestion	An additional mandatory requirement for manufacturers to inform users about new vulnerabilities within a timeline.	To add a new subclause: “ h) The device manufacturer shall inform users about new vulnerabilities in a timely manner. ”

No.	IMDA Question No.	Clause	Type of comment	Comments	Proposed changes
14	6	4.4 & 4.5	Suggestion	For b), there is no strong justification to enforce AES encryption because there are other secure algorithms available. Therefore, rephrase as follows.	To modify the text to: “ b) The Residential Gateway shall use state-of-the-art encryption, such as AES, with at least WPA2 protection by default. If weaker security protection such as WEP or WPA is chosen by users, warning(s) of security risk to use these encryption algorithms shall be displayed. ”
15	7	4.6	Suggestion	Third-party test laboratories can verify the proper implementation of input validation based on testing guides such as OWASP. The chapter on input validation testing from OWASP’s web security testing guide can be used as a reference: (https://github.com/OWASP/wstg/tree/master/document/4-Web_Application_Security_Testing/07-Input_Validation_Testing).	To add new text: “ Manufacturers shall specify in their declaration of conformity how they test input validation, for example simple input validation or fuzzing. ”
16	8	4.7	Suggestion	In addition to their declaration of conformity, manufacturers should provide a document with the process including the person who is responsible for checking the information on the contact point. Manufacturers should clearly state where they will publish information about known vulnerabilities in their products.	n/a

No.	IMDA Question No.	Clause	Type of comment	Comments	Proposed changes
17	8	4.7	Suggestion	As seen in ETSI EN 303 645 draft standard, Section 5.2 says the following: “Coordinated Vulnerability Disclosure (CVD) is a set of processes for dealing with disclosures about potential security vulnerabilities and to support the remediation of these vulnerabilities. CVD is standardized by the International Organization for Standardization (ISO) in the ISO/IEC 29147 [i.4] on vulnerability disclosure and has been proven to be successful in some large software companies around the world.” We recommend IMDA security specifications to take the same approach and reference to the same CVD process.	To modify the text to: “ An easily accessible public 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. The vulnerability disclosure policy of the Residential Gateway shall also be made public. ”
18	9		Suggestion	Logging mechanism: Security events such as logins on the management interface with admin rights, failed logins, changes of passwords, changes of firewall settings, etc. shall be logged. Manufacturers shall log critical functions only and turn off logging that has user data by default. Manufacturers should inform users of logging services and specify how to turn the function off for non-critical logging.	n/a

No.	IMDA Question No.	Clause	Type of comment	Comments	Proposed changes
19	9		Suggestion	Backup mechanism: Manufacturers shall implement a backup and restoration mechanism so that important files such as configuration files, certificates, etc. can be backed up on a regular basis and restored if necessary, for example after a factory reset. Note: Allowing users to upload backup files to the RG might increase the attack surface if protection mechanisms such as integrity, signature checks and input validation are missing or not properly implemented.	n/a
20	9		Suggestion	Security related user documentation: Manufacturers shall describe the RG's security functions in the user manual. In addition, they shall inform users on security best practices such as: 1) Use unique and secure passwords. 2) Do not share passwords. 3) Do not change secure default settings	n/a
21	10			No comment	
22	11			No comment	

4. Conclusion

The manufacturers should be clear on the guidelines given in the Technical Specification and consumers shall be informed by the manufacturers on details regarding the security of the Residential Gateway. This would greatly benefit users by making the Residential Gateways more secure.