DECISION ISSUED BY THE

INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY

SECURITY REQUIREMENTS FOR RESIDENTIAL GATEWAYS

12 October 2020

Background

1. On 13 March 2020, the Info-communications Media Development Authority ("**IMDA**") issued a proposed new Technical Specification for Residential Gateways ("**RGs**"), namely "IMDA TS RG-SEC" for public consultation. The IMDA TS RG-SEC aims to minimise the risk of unauthorised access of the RGs (commonly known as Home Routers) and thus, mitigate associated cybersecurity threats, such as unauthorised access by actors and perpetrators for malicious activities, for example, in the use for Distributed Denial of Service ("**DDoS**") attacks. Hence, the IMDA TS RG-SEC sets out the minimum security requirements and stronger credential settings for RGs sold and used in Singapore, with the objective of strengthening the resilience of Singapore's telecommunications networks.

2. At the close of the public consultation on 15 May 2020, IMDA received comments from 12 respondents (individually referred to as a "**Respondent**" and collectively, the "**Respondents**")

3. IMDA thanks all Respondents for their responses to the consultation.

4. This document sets out the key issues raised in the public consultation and IMDA's responses and decisions on these issues.

Proposed Security Requirements for Residential Gateways

Login Credentials (Ref: IMDA TS RG-SEC Paragraph 4.1)

IMDA's Proposal

5. To protect against actors and perpetrators gaining and taking control of RGs for malicious cyber activities, the proposed IMDA TS RG-SEC had required stronger login credentials for RGs such as randomised and unique pre-loaded credentials and minimum password strength.

Comments Received

6. All the Respondents agreed on the importance of having strong login credentials. However, there were various views on the strong password structure requirements. While some Respondents agreed with the password requirements proposed by IMDA, other Respondents expressed concerns with the proposed password structure, including a minimum password strength of 10 characters and the need to use special characters, as it might be difficult for users to remember. These Respondents suggested to make reference to the guidelines set out in the US National Institute of Standards and Technology's ("**NIST**") digital authentication guidelines, NIST SP 800-63B-3, for the password requirements.

7. A few Respondents proposed additional requirements, including using Multi-Factor Authentication ("**MFA**"), self-generating unique password / picture code, and/or maintaining a blacklist of passwords.

8. One Respondent sought clarification on whether it was mandatory for a user to set his/her credentials before an RG could be connected. Another Respondent suggested for the requirement text to be modified by removing the use of the term 'default' to avoid any misinterpretation.

IMDA's Decision

9. IMDA notes that while all Respondents agreed on the need to have strong passwords, there are diverse views on the password strength/structure requirements. Some Respondents suggested to adoption of US' NIST SP 800-63B-3, which requires only a minimum of 8 characters for the password without any added complexity, such as using of upper and lower case, and special characters. While IMDA notes the citing of NIST SP 800-63B-3, other literatures had recommended the adding of complexity to passwords, such as those published by the European Union Agency for Cybersecurity ("**ENISA**"). After much consideration, IMDA will reduce the minimum required complexity rules stated in paragraph 4.1.2a of the proposed IMDA TS RG-SEC from 3 to 2. Notwithstanding, while the required complexity rules are reduced, IMDA encourages the industry to adopt more complexity rules for password strength.

10. With regard to the suggested additional functions/features, such as using MFA and maintaining a blacklist of passwords, IMDA agrees that while they will help

further secure the RGs, IMDA notes that such implementation can be costly. As the IMDA TS RG-SEC is intended to specify baseline security requirements for RGs, IMDA is of the view that these additional functions/features can be left to manufacturers who wish to adopt a stronger security posture for their RGs.

11. IMDA would like to also clarify that it is not necessary for users to set their own credentials in order for them to use the RGs. The login credentials can be pre-set by the manufacturers and need not be changed as long as they are unique to each device, and complies with the security requirements specified, e.g., password requirements. As to the suggestion on the use of the term 'default', IMDA agrees that it could be misread and has thus revised the text accordingly for better clarity.

Device Setup & Administration (Ref: IMDA TS RG-SEC Paragraph 4.2)

IMDA's Proposal

12. To prevent the RG's features and functions from being used for cybersecurity attacks, the proposed IMDA TS RG-SEC had required that its interfaces be turned off by default and some of the pre-loaded settings of RGs be disabled, such as Home Network Administration Protocol ("**HNAP**") and Internet Protocol Version 6 ("**IPv6**") tunnelling. In addition, the IMDA TS RG-SEC specified the handling of authentication and passwords to ensure that only authorised personnel could configure them. The proposed IMDA TS RG-SEC had also required the device management interface to be secure, thereby preventing communication channels from being sniffed by unauthorised actors.

Comments Received

13. Several Respondents supported IMDA's recommendations on the pre-loaded settings, i.e., for those system services and interfaces that could pose security risks and are not used by the majority to be switched off by default. One Respondent further suggested for IMDA to rephrase the requirements to allow only a minimal set of secure services and interfaces to be opened by default. Other Respondents had however viewed that some of the specified features such as Wi-Fi Protected Setup ("**WPS**") and Universal Plug and Play ("**UPnP**") should be allowed to be switched on by default, citing that these features were used to support common applications on home network. One Respondent had enquired on the treatment of Port Control Protocol ("**PCP**"), which was similar to Network Address Translation - Port Mapping Protocol ("**NAT-PMP**").

14. One of the Respondents commented that while Wi-Fi Protected Access 2 ("**WPA2**") should be used for default wireless connection, other protocol of connection such as WiFi Protected Access ("**WPA**") should also be allowed as there may be older devices that do not support WPA2. Another Respondent suggested auto/auto setting rather than defining WAP2 and Advanced Encryption Standard ("**AES**") as the default setup requirement for device compatibility.

15. A number of the Respondents commented that the authentication requirements in paragraph 4.2.3 seemed to suggest that after a certain number of failed login attempts, access to the RG would be permanently blocked if the manufacturer has no alternative authentication mechanism, which might be challenging to implement. Instead, the manufacturer should provide for either a delay in access for specified amount of time before allowing login attempts again, or factory reset. One Respondent commented that if a user logs in with authenticated credentials, it should be considered as protected. In addition, a Respondent commented that passwords should just be salted and hashed but not encrypted as encryption would allow anyone with a valid key to expose the password. Finally, Respondents commented that it might be useful to allow an option to unmask passwords at user's discretion.

16. Several Respondents had noted that the use of a signed certificate from a Certification Authority ("**CA**") would increase the cost of RGs while a self-signed certificate would produce a browser warning, which might cause confusion to users. In addition, a few Respondents commented that Secure Shell ("**SSH**") and HyperText Transfer Protocol Secure ("**HTTPS**") should be disabled. One Respondent enquired if the use of HyperText Transfer Protocol ("**HTTP**") in combination with their own proprietary encryption is allowed. Another Respondent suggested to allow remote administration of RGs via a secure channel from a trusted authorised device or application. Further, a Respondent commented that this clause was not necessary as the other protection requirements would be sufficient.

IMDA's Decision

17. IMDA notes the comments on the possible uses of some of the system services and interfaces such as WPS and UPnP. IMDA would like to clarify that only those system services stated in paragraph 4.2.1a of the proposed IMDA TS RG-SEC document[1] are to be switched off on both Local Area Network ("**LAN**") and Wide Area Network ("**WAN**") sides by default. Those interfaces stated in paragraph 4.2.1b of the proposed document are required to be switched off by default only on the WAN side[2]. IMDA understands that while some RG users may need these system services and interfaces, majority of the RG users do not need them. In addition, IMDA would like to highlight that while these system services and interfaces are required to be switched off by default, IMDA does not require them to be removed from the RGs. Hence, users could always enable them during RG set-up if needed. In view of the above, IMDA will retain the requirements, minimising the potential risk exposed to majority of the RG users. IMDA will also include the switch off of PCP by default on the WAN side and will update paragraph 4.2.1b accordingly.

18. IMDA notes that some older home devices may not support WPA2. IMDA would like to clarify that the IMDA TS RG-SEC does not mandate the minimum use of

[1] Services to be turned off on both LAN and WAN interfaces are WPS, HNAP and SSH.
[2] Services to be turned off on WAN interface are NAT-PMP, PCP, Remote Administration, Simple Network Management Protocol ("**SNMP**"), Telnet and UPnP.

WPA2 with AES encryption. Nonetheless, IMDA encourages for the wireless connection to at least leverage AES encryption with WPA2 protection.

19. IMDA would like to clarify that to provide factory reset after certain number of failed login attempts is one possible approach. IMDA has amended paragraph 4.2.3 of the proposed document to make clear that this option is acceptable. IMDA agrees not to require credentials to be encrypted and has removed the same. IMDA has also amended paragraph 4.2.3 of the proposed document to clarify that access to the RG's management webpage shall only be via authenticated credentials. IMDA has amended Paragraph 4.2.4 of the proposed document to allow an option to unmask passwords at user's own discretion. Given that this addition may not be in line with what was set out in the GSMA CLP.13, the reference to GSMA CLP.13 has been removed to avoid any misinterpretation of the requirement.

20. It is IMDA's position that paragraph 4.2.5 of the proposed document is necessary as secure communications are important to the security of RGs and should not be removed. Notwithstanding, IMDA noted Respondents' concern with regard to SSH protocols and agrees for it to be disabled by default. However, IMDA is of the view that HTTPS is still a secure means to access the RG and hence will retain the requirement. IMDA notes the concern of the pop-up browser warning as a result of the use of a self-signed certificate. Manufacturers can nonetheless mitigate that by informing or educating users via advice in the banner or by explaining how to deal with such situations in the RG's manual. Finally, IMDA will clarify that IMDA will only accept internationally standardised protocols and has amended paragraph 4.2.5 of the proposed document accordingly. IMDA would like to clarify that while the IMDA TS RG-SEC sets out the baseline or minimum specifications for RG devices, we will leave it to manufacturers who wish to take a stronger security posture and decide to go above the minimum requirement, e.g. remote administration via a secure channel.

Firmware Updates (Ref: IMDA TS RG-SEC Paragraph 4.3)

IMDA's Proposal

21. The proposed IMDA TS RG-SEC had required the RGs to download and update the latest available firmware versions automatically. However, the proposed IMDA TS RG-SEC did not specify the minimum period for RGs to be updated with the latest firmware because if the updating of firmware is disrupted or not done properly, it could affect the RGs' proper functioning.

Comments Received

22. Respondents generally agreed that firmware updates were important to patch security loopholes and managing software vulnerabilities. However, they deferred in how such updates should be implemented. A number of Respondents commented that it was not practical to specify the timeline by which patches would be rolled out as the time needed to develop the patches would depend on the complexity and severity of the vulnerabilities found. Some

commented that RGs should have a feature to allow the user to disable/enable auto-updates and inform the user when the update had started and completed. One Respondent commented that it was not ideal to have frequent updates as there were instances where the router failed after an update. Other Respondents recommended that should an update fail to complete or is interrupted; the RGs should fall back on the previous version of the firmware and could attempt to update again at the next opportunity.

23. A number of Respondents sought clarifications on what paragraph 4.3(e)[3] of the proposed document entailed while one commented that paragraph 4.3(f)[4] seemed unnecessary if the patches are signed. Finally, one Respondent recommended that the requirement in paragraph 4.3(g)[5] should be made mandatory as it would be important for critical updates to be provided on time. It suggested that manufacturers could provide guidance on how soon they would fix vulnerabilities based on their criticality.

IMDA's Decision

24. IMDA is of the view that it is not practical to fix a time to address all vulnerabilities due to the complexities and severities that may be associated with them. IMDA would thus like to clarify that the requirement to update the RG's firmware in paragraph 4.3 of the proposed document does not specify the time needed to fix identified vulnerabilities. Rather, the requirement is for such patches to be done in a timely manner. IMDA notes the Respondent's concerns regarding the possible failure of an RG in the event that an update fails or is interrupted. In such an event, IMDA understands that typically, the patch will be downloaded again when the connection is re-established, and installation will begin after the completion of the download and the patches are verified accordingly. Manufacturers/developers will have the flexibility to decide how to roll out the security patches that will minimise the impact on the functionality of the RG.

25. With regard to the proposed features to allow users to disable/enable auto-updates, informing users of available updates or when the updates start/end, IMDA has no objections to such features on condition that the RGs shall by default enable auto-updates.

26. With reference to the queries on paragraph 4.3(e) of the proposed document, IMDA would clarify that it is requiring manufacturers to state clearly to a user the minimum time period by which they will provide security patches to that RG. This should be done upfront before a user makes the purchase, e.g., on the RG package box or via the manufacturer's website and could be linked to the warranty period. With regard to the comment on paragraph 4.3(f) of the proposed document, IMDA clarifies that the requirement is not mandatory and will leave it to the manufacturers to decide whether to implement. Nonetheless,

[3] Requires the minimum period of the firmware support received by the RG to be provided upfront to the user.
[4] Recommends device manufacturer to not include sensitive data in patches and to also transmit the patches via secured connection.
[5] Recommends security updates for the RG to be provided in a timely manner.

IMDA encourages the adoption of the recommendation. The proposal to change the requirement in paragraph 4.3(g) to mandatory may not be practical as it is not meaningful to specify a fixed time period. As pointed out, the availability of the fix depends on the complexity and impact of the vulnerability, which manufacturers will have to assess and determine the time needed to develop the fix.

Wireless Access & Data Protection (Ref: IMDA TS RG-SEC Paragraphs 4.4 & 4.5)

IMDA's Proposal

27. The proposed IMDA TS RG-SEC had specified the default encryption algorithms for an RG's communication with connected devices in the home and the storage of data that they used in order to ensure that such communications were secure. The RG should also allow a user to set up guest networks with separate login credentials for authorised guest users of the home network.

Comments Received

28. A number of Respondents agreed that the requirement to warn a user of the higher security risk when selecting weaker encryption algorithms was useful. A couple of Respondents commented that WEP was not supported or might no longer be supported in the future. One Respondent noted that there were other secure algorithms available besides AES encryption. Another Respondent proposed that the requirement in paragraph 4.4(c) of the proposed document to set up guest networks should only apply if an RG has such features. Finally, one Respondent commented that requiring to encrypt the information used and stored by an RG as set out in paragraph 4.5 will cause delays, which end users might not be able to accept.

IMDA's Decision

29. IMDA agrees with the comments on the use of AES and will edit paragraph 4.4(b) of the proposed document to state that an RG can use other secure encryption algorithms including AES. In addition, IMDA notes the concerns with WEP and will amend paragraph 4.4(b) by removing the reference to WEP. With regard to the requirement to allow users to setup guest networks, IMDA agrees that while this feature helps to further protect the RG, it may not be widely used currently by users despite many RGs having this feature. Hence, IMDA agrees not to mandate for RGs to have this feature and will update the specification to reflect this change. Nonetheless, IMDA would still recommend RG manufacturers to include this feature in their products for more robust protection.

30. With regard to the concerns with paragraph 4.5 of the proposed document, IMDA has reviewed the requirement and assesses that data elements used by RGs need not be encrypted as long as they are salted and hashed. IMDA will thus update the requirement accordingly and will leave it to manufacturers to

decide whether to encrypt the data elements. If the manufacturer decides to do so, the encryption key shall be securely stored.

Validation of Data Inputs (Ref: IMDA TS RG-SEC Paragraphs 4.6)

IMDA's Proposal

31. IMDA had proposed for data inputs to be validated to protect the RGs from known security vulnerabilities, such as information leakage, remote code execution and cross-site scripting. Hence the proposed IMDA TS RG-SEC had required the RGs to validate data inputs via all interfaces.

Comments Received

32. Most of the Respondents who have commented on this paragraph 4.6 not only agreed with the requirements but also recommended that more prescriptive tests should be done. However, one Respondent noted that extensive testing would cause noticeable delay or degradation in the performance of the RGs which might not be acceptable to users.

IMDA's Decision

33. IMDA notes the possible advantages with more prescriptive tests but is of the view that the RGs should ensure that validation is done to protect the three listed vulnerabilities at a minimum, namely information leakage, remote code execution and cross-site scripting. IMDA has amended paragraph 4.6 of the proposed document accordingly. With regard to the comment on the impact to the performance of RGs, IMDA would like to clarify that testing(s) are expected to be performed during the design and manufacturing phases and is of the view that the requirements will not impact or degrade the performance of RGs.

Vulnerabilities Reporting (Ref: IMDA TS RG-SEC Paragraphs 4.7)

IMDA's Proposal

34. The proposed IMDA TS RG-SEC had required that a point of contact be provided for the public to report discovered vulnerabilities, thereby allowing the manufacturers to develop security patches to address these vulnerabilities.

Comments Received

35. Most of the Respondents agreed with the requirement. However, one Respondent noted that the approaches to public disclosure of vulnerabilities would need to be carefully considered and not be allowed to provide malicious parties to exploit such information.

IMDA's Decision

36. IMDA notes the importance for manufacturers to provide an avenue to report vulnerabilities and proper management/handling of these reported vulnerabilities to avoid them from being exploited. IMDA will allow manufacturers to set up the public reporting channels or mechanisms and the safeguards to put in place to minimise such risks to allow the public to report vulnerabilities securely and in confidence.

Other Recommendations

Comments Received

37. A few Respondents provided additional suggestions, including the offering of secure Domain Name System ("**DNS**"), demonstration of 'trustworthiness' in supply chain, design practices, and setting an RG's upgrading plans to switch out the older RGs.

38. One Respondent suggested for an application to be installed in an RG to detect new connections and potential rogue transmissions from connected devices.

39. One Respondent commented that some requirements set up in the specifications could not be fulfilled by RGs managed by an Internet Service Provider ("**ISP**"). An example of these requirements was the disabling of remote administration interface by default. Hence, the Respondent suggested for managed RGs to be excluded from the need to comply with these requirements.

IMDA's Decision

40. IMDA agrees that the additional suggestions such as offering secure DNS may further help to secure the use of RGs and the home IoT networks. Nonetheless, IMDA would like to highlight that the IMDA TS RG-SEC focuses on the security requirements for RGs only and may consider the need to do so for other home IoT networks in the future.

41. IMDA notes the possible use of applications to further enhance the security of the RGs. However, as explained in previous sections, the IMDA TS RG-SEC aims to provide baseline security requirements and thus, IMDA will not mandate the installation of such applications and will leave it to the manufacturers to do so as a differentiator for their products.

42. IMDA notes that it may be challenging for ISP network-specific and managed RGs to fulfil all the requirements set up in the specifications. However, IMDA is also concerned that excluding these network-specific and managed RGs from these requirements will defeat the policy intent of setting baseline security requirements for RGs sold in Singapore. Notwithstanding, IMDA may consider on a case-by-case basis if ISPs need exemptions to be provided. For the avoidance of doubt, regardless of any approval of exemptions granted by IMDA, if obtained, the dealer/vendor is still required to register these RGs with IMDA via the existing equipment registration scheme.

Implementation Plan and Timelines/Proposed Registration Scheme and Process for RGs

43. Respondents who have commented on the proposed implementation plan and the registration scheme for RGs have expressed no objection to the proposed timelines. Hence IMDA will proceed with the proposed timelines as set out below and via the Enhanced Simplified Equipment Registration ("**ESER**") scheme: