Dear Ms Chia,

I would like to thank IMDA for the opportunity to provide my input on the new proposed Technical Specification for Residential Gateways. In general, I support the creation of a minimum security requirements for Residential Gateways. However, I feel that some points of the Technical Specification should be revised.

Question 1: IMDA invites comments relating to the requirements on preloaded credentials and password strength for RGs as set out in paragraph 4.1.

On Para 4.1.2, IMDA proposes a password strength/complexity requirement. I feel that these requirements should be refined.

I refer to the Microsoft Password Guidance (Hicock, 2016), which states that requiring long passwords and use of complexity rules actually serve to weaken the strength of the password. This advice is mirrored by NIST in their guidelines. (National Institute of Standards and Technology, 2017) Both Microsoft and NIST recommend a minimum password length of 8 characters and no complexity rules.
In addition, I am of the opinion that the requirement in 4.1.2(b) should be removed. To not allow consecutive identical characters is too strict, especially if the character is only repeated twice. This will have a significant detrimental effect on the user experience, while not improving security by much, if any. In general, the addition of password policies makes it easier to guess the password as it reduces the amount of possible password combinations. If the idea is to prevent the user from utilising an overly simplistic password, such as '11111', the rule is still unhelpful as it is highly unlikely that a user who would have chosen such a simple password in the first place would go on to pick a significantly more complex password, but would in all likelihood simply pick another password such as '121212'.
To prevent users from utilising weak passwords, a list of blacklisted passwords should be maintained. This list should include common passwords and passwords that are simple to guess, such as repeated or sequential characters. This form of password control is also recommended in both the Microsoft and NIST guideline.

Question 3: IMDA seeks feedback on the requirements on RG administration as set out in paragraph 4.2, in particular the applicability of maintaining secure communication protocols such as SSH or HTTPS for device management interfaces to the RG as indicated in paragraph 4.2.5.

With regards to 4.2.3, specifically subsection b, passwords should be hashed but not encrypted. Encryption would allow anyone with a valid key to expose the plaintext password, which is not a desirable property.
Secondly, it would be ideal for IMDA to specify the methods passwords should be stored. An example they could take guidance from would be the NIST Special Publication 800-63B section 5.1.1.2, which specifies that a key derivation function, rather then simply a simple hash and salt should be used. (National Institute of Standards and Technology, 2020) They also specify acceptable

hash algorithms that can be used for the key derivation function.
Finally, by enforcing the use of a hash or key derivation function over encryption, it would be impossible for the device to reverse and obtain the plaintext password. This would meet the requirements in 4.2.4, specifically subsection a and b as it would be impossible for the device to display something it does not have.

With regards to paragraph 4.2.5, I support the use of SSH but not HTTPS.
The paragraph states specifically for HTTPS, a certificate from a trusted CA or a self-signed certificate can be used. These are not practical solutions.
Shipping a router with a certificate issued from a trusted CA would mean that the router would have to be loaded with the private key of the certificate, and this private key would inevitably be leaked, providing no security benefit whatsoever. This is precisely what happened to Netgear a few months back. (Starke, 2020) Worse still, the current CA/Browser Forum Baseline Requirements require that CA revoke any certificate whose private key has been compromised. (CA/Browser Forum., 2020) Currently, all major browsers such as Google Chrome, Microsoft Edge and Mozilla Firefox do not allow the user to bypass a revoked cert error, essentially locking users out of their routers the moment the certificate is revoked.
However, utilising a self-signed certificate is also not a good idea. A self-signed certificate will naturally throw up an invalid certificate authority error when users visit the site. The product vendor will then have to provide instructions to the user on how to bypass this warning. This is a bad idea, as it desensitises the user to TLS warnings, and increases the chances they will simply bypass the warnings even when not accessing their router.
Finally, as per paragraph 4.2.5, the purpose of implementing HTTPS is to prevent the connection from being sniffed by unauthorised actors. However, a person wishing to sniff the connection can simply perform a TLS interception, and supply his own self-signed certificate to the user. The only way to detect this attack would be to compare the public key or hash of the certificate, something a majority of users are unlikely to do.

As SSH utilises the trust on first use authentication scheme, it does not suffer from the problems listed.

I would like to thank IMDA again for taking into consideration my viewpoints on portions of the proposed Technical Specifications.

Yours sincerely,
Nathaniel Chan

References

CA/Browser Forum. (2020, May 4). *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.* Retrieved from CA/Browser Forum: https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.7.0.pdf

Hicock, R. (2016, May). *Microsoft Password Guidance.* Retrieved from Password Guidance: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf

National Institute of Standards and Technology. (2017, June). *Digital Identity Guidelines.* Retrieved from NIST Special Publication 800-63B.

National Institute of Standards and Technology. (2020, March 02). *NIST Special Publication 800-63B.* Retrieved from Digital Identity Guidelines Authentication and Lifecycle Management: https://doi.org/10.6028/NIST.SP.800-63b

Starke, N. (2020, January 20). *Netgear Signed TLS Cert Private Key Disclosure*. Retrieved from https://gist.github.com/nstarke/a611a19aab433555e91c656fe1f030a9