13 Dec 19

MINISTRY OF DEFENCE
CYBER CELL

CYBER SECURITY ADVISORY 15/2019
SECURITY PRECAUTIONS DURING USAGE FO VOICE ASSISTANT

1. **Background.** Home Digital Voice Assistants (HDVAs) are getting popular in recent years. One can control smart devices and get assistance like turning on lights, fans etc. through HDVAs such as *Amazon Alexa, Google Home, Apple Siri, Cortana* etc. using voice. These assistants sit in the corner of a room and are able to hear your voice from across the room. While this may seem harmless, it poses serious security threats.

2. **Aim**. The aim of this advisory is to create awareness about these HDVAs and provide guidelines to help safeguard personnel.

3. **Guidelines.** Following are the guidelines for effective and safe use of HDAVAs:-

(a) A HDVA must only be connected to a trusted network ***and never on a public network or hotspots.*** The trusted network (usually home Wi-Fi) should be well protected.

(b) ***Complicated passwords must be used*** and Two/ Multi factor authentication must be enabled for protecting all accounts associated with the HDVAs.

(c) One should be careful about which accounts they connect. If there is no requirement for calendar reminders, official addresses etc, one should not use the business account for authorization. Unused features like these should be turned off.

(d) HDVAs can get triggered by commands from other sources. Hence, in order to prevent it/ reduce its probability, a manufacture issued voice recognition feature must be used if the option is there/ available. Voice recognition is not completely fool proof but it's usage is advised.

(e) ***Unintentional triggering*** does happened sometimes in HDVAs. Hence, these should ***either be muted or turned off when not in use*** to prevent accidental commands pick up.

(f) ***Voice purchased option***, which is enabled by default in ***Amazon Alexa***, should be turned off immediately to prevent unwanted purchases.

(g) ***Voice assistant's respond to ultrasonic sounds which is inaudible to the human ear***. Hence, it is advised ***to never connect voice assistants to critical IoT devices like door locks to prevent an attacker from exploiting this feature*** (Dolphin attack).

(h) Keep updating your HDVAs to the latest firmware available. Older versions of

Amazon Echo devices allowed anyone to replace the firmware and add their own code to the device, thereby truing them into a listening device.

(j) Avoid connecting security functions such as door locks to the HDVAs. Also, these devices should not be used to remember passwords or credit card data.

4. Personnel be sensitized to not use their voice assistants for critical works and follow the guidelines. These guidelines may be disseminated to all concerned agencies within the MoD.

Appendix
(Refers to sub sub par
4(a)(x) of Advisory 15/19)

COMPARSION OF SECURITY / PRIVACY FEATURES OF INSTANT MESSAGING APPS

Comparisons Item	**Apple i Message**	**Facebook Message**	**Signal**	**Skype**	**Telegram**	**Viber**	**Whats App**	**Wire**
Company Jurisdiction	USA	USA	USA	USA	UK/Berlin/Germany	Luxembourg/ Japan	USA	Switzerland
Implicated in giving customers' data to intelligence agencies	Yes	Yes	**No**	Yes	**No**	**No**	Yes	**No**
Provides a transparency report	Yes	Yes	Yes	Yes	**No**	**No**	Yes	Yes
General stance on customers' privacy	Poor	Poor	**Good**	Poor	Poor	Poor	Poor	**Good**
App collects customers'' data	Yes	Yes	**Minimal**	Yes	Yes	Yes	Yes	**Minimal**
Encryption turned on by default	Yes	**No**	Yes	Yes	No	Yes(if device supports it)	Yes(if device supports it)	Yes
Cryptographic primitives	RSA-1280(encryption), ECDSA 256(signing)/ AES 128/ SHA-1	Curve 25519/ AES-256/ HMAC-SHA256	Curve 25519/AES-256/HMAC-SHA256	RSA-1536 & 2048/ AES 256/ SHA-1	RSA 2048/ AES 256/SHA-256	Curve 25519 256/ Salsa 20128 HMAC-SHA 256	Curve 25519/ AES-256/HMAC-SHA 256	Curve 25519/ Cha Cha20/ HMAC-SHA 256
App and server are completely open source	No	No	**Yes**	No	No(Clients and API only)	No	No	**Yes**
Anonymous sign up to get App possible	No	No	No	No	No	No	No	No
Manual verify contacts' fingerprints for using apps?	No	**Yes**	**Yes**	No	No(session only, does not provide users' fingerprint information)	**Yes**	**Yes**	**Yes**
Do you get notified if a contact's fingerprint changes?	No	No	**Yes**	No	No(session only, does not provide users' fingerprint information)	**Yes**	No(Setting turn off by default)	**If contact was previously verified**

Comparison Item	Apple i Message	Facebook Message	Signal	Skype	Telegram	Viber	Whats App	Wire
Is personal information (Mobile Number, contact list, etc.) Protected?	No	No	Yes	No	No	No	No	**Yes**
Can messages be read by the company?	**No**	**Yes**	**No**	**Yes**	**Yes**	**No**	**No**	**No**
Does the app enforce perfect forward secrecy?	No	Yes	**Yes**	Could n't find any information	No(session keys do change after being used 100 times)	Yes	Yes	**Yes**
Does the app encrypt metadata?	No	No	**Yes**	Information N/A	No	Information N/A	No	**Yes**
Does the app use TLS/ Noise to encrypt network traffic?	Yes	Yes	**Yes**	Yes	No	Yes	Yes	**Yes**
Does the App allow a Two factor of authentication?	No	No	No	No	**Yes**	No	**Yes**	**Yes**
Are messages encrypted when backed up to the cloud?	No	Information N/A	N/A, Signal is excluded from iCloud/ iTunes &Android backups	Information N/A	Information N/A	Information N/A	iOS: Yes Android: No	Information N/A
Does the app have self-destructing messages?	No	Yes	**Yes**	No	Yes	No	No	**Yes**

(Souce https://www.securemessagingapps.com)