GC Security Zones and Dongle Effectiveness

APRIL 2017 | AWARENESS SERIES | ITSAP.00.002

Mobile devices are important business tools that help government employees communicate and perform their duties in an effective and timely manner. Mobile devices use a microphone for voice communication, recording and voice commands.

When the microphone is on, the information being discussed could be at risk. Threat actors can install malicious software (malware) which enables them to turn on the microphone remotely. Once the microphone is on, a threat actor could capture conversations from up to 20 meters away and transmit the information obtained to their counterparts without your knowledge.

To counter this threat, a headset simulator plug (HSP), also known as a **dongle**, was designed to imitate a headset. In older versions of mobile devices, inserting the dongle into the headset plug physically disconnected the internal speaker and microphone.

Today's Threat Environment

Modern mobile devices now use the device's software to turn on and turn off the microphone. A threat actor can compromise the device's software to remotely turn on the microphone making the dongle ineffective at preventing this type of threat.

Likewise, using mobile devices close to IT systems that handle sensitive or classified information poses an additional risk to GC information and assets. CSE's *ITSB-104 Security Considerations for Exposure of Classified IT Systems to Mobile Devices and Wireless Signals* provides additional considerations for protecting GC information and assets.

IT Security Actions

Based on today's threat environment, CSE recommends users leave their mobile devices outside of areas where sensitive discussions are occurring. For more information consult the TBS *Operational Security Standard on Physical Security* and RCMP's *Guide to the Application of Physical Security Zones*.

For more information including mitigation strategies for mobile device security and dongles, contact CSE's ITS Client Services.

Efficacité des fiches bloque-son et zones de sécurité du GC

AVRIL 2017 | SÉRIE SENSIBILISATION | ITSAP.00.002

Les dispositifs mobiles sont des outils opérationnels importants qui facilitent les communications du gouvernement et permettent aux employés d'exécuter leurs tâches de manière efficace et opportune. Les dispositifs mobiles utilisent un microphone pour les communications vocales cellulaires, l'enregistrement et les commandes vocales.

Lorsque le microphone est activé, la communication pourrait être à risque. Les auteurs de menaces peuvent installer des logiciels malveillants (maliciels) qui leur permettent d'activer le microphone des dispositifs à distance. Lorsque le microphone est activé, un auteur de menaces peut enregistrer des conversations ayant lieu jusqu'à 20 mètres de loin et transmettre l'information obtenue à leurs homologues sans que vous en ayez connaissance.

Pour contrer cette menace, une fiche bloque-son, également appelée **bouchon**, a été conçue pour imiter un casque d'écoute externe. Dans les anciennes versions des dispositifs mobiles, l'insertion du bouchon dans la prise de casque d'écoute désactivait le haut-parleur et le microphone internes.

Environnement de menace actuel

Les dispositifs mobiles modernes utilisent maintenant le logiciel du dispositif afin d'activer et de désactiver le microphone. Un auteur de menaces peut compromettre le logiciel du dispositif à distance afin d'activer le microphone, ce qui annule l'efficacité du bouchon dans l'atténuation de ce type de menaces.

Par ailleurs, l'utilisation de dispositifs mobiles à proximité de systèmes TI qui traitent de l'information sensible ou classifiée met à risque les renseignements et les actifs du GC. La publication ITSB-104 *Répercussions sur la sécurité de l'exposition de systèmes TI classifiés à des dispositifs mobiles et à des signaux sans fil* du CST fournit de plus amples détails sur la protection de l'information du GC contre l'exfiltration de données.

Mesures de sécurité des TI

Étant donné l'environnement de menace actuel, le CST recommande aux utilisateurs de laisser leurs dispositifs mobiles à l'extérieur des zones où l'on discute d'informations sensibles. Pour obtenir plus d'information, prière de consulter la *Norme opérationnelle sur la sécurité matérielle* du Secrétariat du Conseil du Trésor ainsi que le *Guide pour l'établissement des zones de sécurité matérielle* de la Gendarmerie royale du Canada (GRC).

Pour plus de détails sur les fiches bloque-son et la sécurité des dispositifs mobiles, veuillez communiquer avec les Services à la clientèle de la STI.