Communications Security Establishment | Centre de la sécurité des télécommunications

Security Considerations for Exposure of Classified IT Systems to Mobile Devices and Wireless Signals

IT Security Bulletin for the Government of Canada

ITSB-104 **October 2014**

1 Purpose

Many Government of Canada (GC) departments and businesses use wireless technologies to enable collaboration through convenience, flexibility and mobility for employees. Mobile devices and wireless signals are a key component in reaching this goal, but can pose a threat to the GC and its information assets as departments and their networks are frequently targeted by threat actors looking to gather information on GC employees, projects, and systems.

This bulletin aims to describe the risks posed by, and possible mitigations for, the exposure of classified IT systems to wireless signals and mobile devices that are not authorized to connect to those systems. The intended audience for this bulletin includes those responsible for IT security risk management activities as well as information system security practitioners.

2 Impact

Mobile devices contain powerful computing capabilities and have the ability to communicate with Wi-Fi®, cellular networks, or with other devices via protocols such as Bluetooth. Mobile devices are also vulnerable to the same cyber threats as traditional computers, including malware, spyware, or Trojan horses. Allowing wireless capable devices in areas that host sensitive or classified information creates a conduit for exfiltration (leakage) of data or voice via these devices. Exfiltration can be intentional or unintentional, and could be facilitated by a threat actor's implant on the device. Video, photography, voice recording, or connecting the device directly to a wired infrastructure are potential avenues for a threat actor to acquire GC information.

The exfiltration threat is enhanced when a wireless signal from a non-GC wireless network (e.g., free Wi-Fi® from a local coffee shop) is within range of a GC wireless network or GC owned mobile device. A GC device could inadvertently or intentionally become connected to a non-GC network, or act as a bridge between an external wireless network and a GC network, thus providing an exfiltration route.

Locating classified IT systems in close proximity to radio frequency (RF) transmitters may also cause unintentional information leakage.

3 Mitigation Strategies

To mitigate the risks to sensitive or classified information from mobile devices or wireless signals, it is important that GC departments implement sound security practices and ensure employees are aware of the security implications. When implemented together, the following can help reduce the risk of the compromise of information.

3.1 Policies and Procedures

Clear departmental-level policies and procedural rules should be developed on the use of wireless capable devices in, or close to, areas that process sensitive or classified information. Departments must consider the Royal Canadian Mounted Police (RCMP) *G1-026: Guide to the Application of Physical Security Zones* as an element of the overall risk management strategy.

For departments implementing a Mobile Device Management (MDM) solution, security configurations should be clearly articulated in departmental policies and procedures. CSE's publication *ITSB-64: MDM Solutions* can aid in the selection of an MDM solution.

Regular awareness activities on the related vulnerabilities and proper usage behaviours should be made available to all users with access to departmental systems.

3.2 Technology

GC departments and agencies should consider adopting the following security controls on their mobile device resources:

- Using whitelisting to impose enterprise wide application restrictions;
- Controlling camera and wireless transmitter use; and
- Restricting Wi-Fi® connections to GC authorized access points.

4 Implementation

To avoid unintentional information leakage, classified IT systems should be located as far away as possible from RF transmitters such as Wi-Fi® access points, signal repeaters, portable end user devices (e.g., laptops, tablets, or mobile phones), and supporting wireless technologies (e.g., Wi-Fi® or cellular). It should be noted that stationary RF transmitters introduce a greater risk than portable mobile devices. Consult *ITSG-11: COMSEC Installation Planning – Guidance and Criteria* for further guidance related to the installation of classified IT systems in close proximity to RF transmitters.

5 Conclusion

It is essential that GC departments implement protective measures to secure the confidentiality, availability and integrity of their IT information and assets. Allowing the use of mobile devices and wireless signals in close proximity to IT systems that handle sensitive or classified information poses a risk to GC information and assets. Departments can enhance the security features of their networks and provide protection against data exfiltration threats through the use

of strong security policies, training and awareness programs, tailored security controls and a robust risk management process.

6 Contacts and Assistance

For more information, phone, or email our Contact Centre:
Contact Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

© Government of Canada, Communications Security Establishment, 2014