Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CYBER JOURNAL

EDITION 3 – SUMMER 2013

IN THIS EDITION

NETWORK SECURITY: PROTECTING OUR INFORMATION ASSETS

The Government of Canada (GC) depends on its networks, both wired and wireless, for communications and day-to-day operations. Unfortunately, threat actors are always discovering new vulnerabilities which can be used to exploit GC networks.

Compromises to GC networks are expensive and threaten the availability, confidentiality, and integrity of our information assets. In order to have a complete and thorough security plan, we must consider that the risks come from not only malicious actors, but also from the inherent complexity of the technology and the inadvertent errors of end users.

Since the IT security knowledge level of GC users can range from novice to adept security specialists, we require both technical protections and a heightened awareness among all employees. Awareness of the dangers is an integral step in the development of a risk managed defence strategy and educational effort.

In this edition of the Cyber Journal, CSEC offers advice and guidance on processes, procedures, and policies to securely plan, implement, manage and support the security and risks associated with GC IT networks.

Toni Moffa
Deputy Chief, IT Security

www.cse-cst.gc.ca

Canada

NETWORK SECURITY ZONES

Using network security zones to protect high value assets is mitigation measure #7 on the CSEC Top 35 Mitigation Measures list. A simple enterprise network with a single security zone means that all information assets are protected by a single perimeter that once breached, exposes the network. An enterprise network that uses multiple security zones is more resilient to cyber-intrusions because each zone must be subverted in succession in order to compromise the entire network.

Problem: If a network that does not employ zoning contains both unclassified and sensitive information, either the unclassified information will be over-protected or the sensitive information will be under-protected:

- Over-protecting unclassified information results in increased IT infrastructure costs and tighter access controls; this impacts valid users by restricting access to the network and by limiting the availability of the unclassified information; and
- Under-protecting sensitive information may result in the loss of its confidentiality, integrity and availability by exposing sensitive information to unauthorized network users.

Mitigation: A network security zone is a construct used to implement security within an interconnected network environment. Each 'security zone' is a discrete area (sub-net) that has a specific security requirement and a defined network boundary. Security zones are used to reduce the threat to network assets by providing security-in-depth through the use of multiple and/or nested security boundaries. Enhanced security is achieved by:

1. Limiting access to each 'zone' to discrete entry points;
2. Limiting access to each 'zone' to authenticated users; and
3. Monitoring and filtering network traffic at the entry points.

Employing network security zones by itself will not meet all security requirements; it should be used in conjunction with platform, application, and administrative security controls as part of your overall Enterprise Security Architecture (ESA).

For more details, please refer to ITSG-22: Baseline Security Requirements for Network Security Zones and ITSG-38: Network Security Zoning.

For more information on mitigation measures, please refer to the Top 35 Mitigation Measures.

NEW RELEASES!

ITSG-41: Security Requirements for Wireless Local Area Networks

ITSB-98: Java Vulnerability Mitigation

ITSB-65: Risk Management for iPads

ITSB-64: Mobile Device Management Solutions

ITSA-64: April Edition of Forbes Magazine Contains a Wi-Fi-Router

SMART COMPUTING TIPS FOR EVERYONE

Keep your software up-to-date

New versions of software are frequently released to address security concerns.

Use anti-virus software

It should be from a reputable company and should be kept up-to-date.

Monitor your social media accounts

Do not put sensitive personal information on the internet, and check your privacy settings on social websites.

Do not open suspicious e-mails

If someone has sent you an e-mail that seems strange, do not open it or click on any embedded links.

Back-up your files

Plan ahead and save your data to an alternate device such as an external hard drive.

Use strong passwords

Passwords should be a combination of upper and lower case letters, numbers and symbols.

Use different passwords

If your password is compromised, an intruder may then be able access your other accounts.

Beware of theft

Lost or stolen devices pose a risk to your personal and business information.

SECURING WLANS

Did you know that the threats to Wireless Local Area Networks (WLANs) that arise most frequently include:

1. Unauthorized association (accidental or malicious);
2. Ad-hoc network creation;
3. Identity cloning;
4. Denial of service;
5. Wireless interception; and
6. Device theft.

While WLANs offer many benefits over their wired LAN counterparts including a reduction in cabling costs, ease of deployment within existing buildings and support for roaming, they also introduce a broader range of security risks. Deployments of WLANs are becoming increasingly popular within the GC. Given this technology paradigm, departments are also subject to additional vulnerabilities which may lead to the compromise of the confidentiality, integrity, or availability of their information systems and IT assets.

The physical boundaries of the WLAN coverage area often extend beyond the physical security perimeter of the department, such that intruders do not need to be located within the physical security boundaries of the organization to launch attacks on the network.

Considering the increase in potential risks, specific security controls must be selected and the associated control elements tailored based on the type of WLAN solution being deployed. ITSG-41: Security Requirements for WLANs addresses the types of WLAN deployments which are currently identified as business needs of the GC:

- Government hot spot;
- Wireless user to wired network connection; and
- Wired network to wired network via wireless bridge.

Departments will benefit from leveraging ITSG-41 during the requirements analysis and high-level design phases of a system to help mitigate against typical WLAN threats.

RISK MANAGEMENT FOR IPADS

The iPad's ease of use, short boot up time and portability makes the device more convenient than traditional laptops. Employees consider the iPad to be a great companion device, and are using it to replace paper, to take notes in meetings, and to read documents while travelling. This trend is leading employees to desire remote access to their department's network via an iPad.

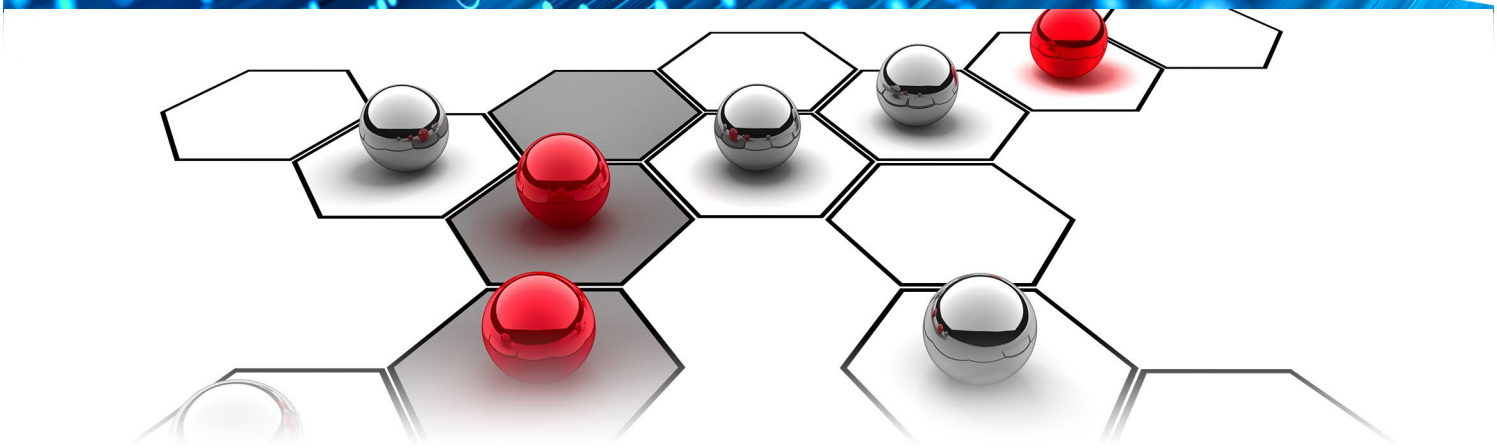
However, iPads will also introduce new risks to an organization's business and the security of its information. The security risks are numerous, and must be considered carefully, clearly understood and security controls and safeguards put in place before iPads are allowed to remotely access a department's network.

Security controls for iPad deployments should be determined according to the department's threat-risk profile. Security controls need to be implemented and verified for the complete information system, from the iPad through to the departmental network services that support the business processes and information assets.

CSEC has recently released ITSB-65: Risk Management for iPads which explains the top 5 vulnerabilities associated with iPads as well as their potential mitigations and safeguards. The Top 5 Vulnerabilities are:

1. Data at Rest;
2. Malware;
3. Jailbreak;
4. Wireless Network Access; and
5. Provisioning and Management.

Please refer to ITSB-65 and CSG-30: Apple iPad Security and Best Practices as a starting point when considering using these devices within your environment.



COMMON CHALLENGES TO ADOPTING A RISK MANAGEMENT STRATEGY

The goal of IT security risk management is to ensure information systems can support the missions and objectives of GC departments in a dependable manner. If IT security risks are not managed correctly, or are unmanaged, information systems may have too little security, too much security, mitigate the wrong threats, or generally be unfit for protecting the confidentiality, integrity, and availability of departmental business activities. The ITSG-33 guidelines provide a modern process to help departments implement risk management activities; however, security practitioners may face some or all of the following challenges:

1. **Governance**
   A strong and effective governance structure helps to ensure that conflicting objectives of multiple stakeholders can be resolved in an adequate manner; an appropriate governance structure should be in place before commencing IT projects;

2. **Organizational Culture**
   Maintaining clear and continuous communication lines with the IT security governance body, taking opportunities to educate stakeholders, and planning ahead will enable the organizational culture to overcome obstacles in facing today's IT security challenges;

3. **Alignment Between Organizational Teams**
   It is important that all the teams supporting the IT security practitioner (such as the business owners, the IT security function, IT projects, and IT operations), be properly aligned through a clear governance structure and have accountable representatives working together during significant IT security initiatives;

4. **IT Security Resources**
   Limited resources allocated to IT security activities can be a major challenge to overcome. The lack of skilled staff, budget, time and training opportunities can force security practitioners to make difficult choices regarding the implementation of IT security in their organization. Practitioners should communicate to the organization's IT security governance body the most significant consequences stemming from the limited resources available; and

5. **Use of Mature Processes**
   Another challenge lies in the current maturity of the processes used during the design, development and operations of information systems. For organizations with mature processes for IT security oversight, project management, system engineering, system security engineering and IT operations, the transition to ITSG-33 will require only a moderate quantity of resources and time. For organizations without established processes, it is recommended that you apply ITSG-33 slowly through various initiatives spanned over time.

To learn more, visit our IT Publications website and download ITSG-33: IT Security Risk Management: A Lifecycle Approach or consult past editions of the Cyber Journal.

MINIMIZING ADMINISTRATIVE PRIVILEGES

Minimizing the number of users with domain or local administrative privileges is mitigation measure #4 on the CSEC Top 35 Mitigation Measures list. The concept of Least Privilege is designed to enhance security by reducing user access privileges to the minimum required to perform job related tasks. Problems arise when privileged users consistently access the system using their privileged access rights, such as:

- While working, a legitimate privileged-user may make a mistake and inadvertently cause damage to the network environment; and/or
- An intruder may gain access to a legitimate privileged-users' credentials which gives them unfettered access to valuable information assets and the opportunity to deliberately modify systems that the privileged-users control.

FACT: In general, policies are not regularly checked and enforced. 59% of organizations do not have or strictly enforce access governance policies, and 61% do not immediately check access requests against security policies before the access is approved.

Ponemon Institute, 2010 Access Governance and Trends Report

The implementation of Least Privilege helps mitigate the problem by minimizing the exposure of privileged sessions to cyber intruders. Users should have two sets of access credentials: one with minimal privileges used for everyday access (i.e.: limited to changes to the local environment only), and another with enhanced privileges used only when necessary to effect changes to the network environment.

For Least Privilege for Administrators to be most effective:

1. Ideally, utilize Domain Group Accounts that have tailored administrative privileges instead of using local administrator accounts. Use domain security groups to control access to network assets;
2. At the very least, do not permit local-administrator accounts with credentials shared amongst more than one host. If administrative functions can be achieved without using the local administrator account it should be disabled; and
3. Trigger a change of administrator passwords based on an established schedule or after a security incident.

Least Privilege for Administrators limits the potential damage from a compromised system by minimizing the use of shared credentials within an enterprise network environment. This provides security in depth by forcing a potential intruder to sequentially compromise more than one network asset to undermine the network's security, and facilitates effective management of privileged-users credentials.

For more details please refer to ITSB-94: Minimizing Administrative Privileges Explained.

MATCH THE THREAT TO THE EFFECT

1. VIRUS	A. Masquerades as a useful program, performs surreptitious functions beyond those of the program, causes data corruption.
2. WORM	B. False e-mail message that can prompt reader to delete valid executable files.
3. TROJAN HORSE	C. Method to bypass normal authentication procedures, allows the attacker to secure remote access to a computer.
4. SPYWARE	D. Makes a copy of itself, does not need a host file to replicate, may damage or compromise the security of a computer.
5. HOAX	E. Attaches to a new host, self-replicates, can damage data or crash computers.
6. BACKDOOR	F. Little snippets of code embedded in files, actively tracks all browsing and reports back to a marketing server.

See page 8 for answers.

CYBERJOURNAL

EDITION 3 – SUMMER 2013

EMBEDDED WI-FI HOTSPOTS

Electronics are continually being offered at a lower cost and in a smaller, more compact format; therefore, it is becoming easier to introduce them into products that are not traditionally considered to be carriers of electronics.

For example, the April edition of Forbes Magazine contained an ad campaign by Microsoft to promote their cloud-based Office 365 software. The cover of the magazine included a large orange graphic that indicated Free Wi-Fi. A cardboard ad insert concealed a fully functional wireless router that could be activated to provide free Wi-Fi service for 15 days for up to 5 simultaneous users.

Note: WiFi hotspots are considered Restricted Items and should not be permitted into secure facilities as they pose a potential technical threat to GC information and systems.

For more information download: ITSA-64: Forbes Magazine Contains WiFi-Router

IT SECURITY TRAINING NEWS

The IT Security Learning Centre (ITSLC) has released its new catalogue and the 2013-2014 Calendar. In this catalogue, you will find opportunities to help maintain a high-level of cyber security knowledge to support your department's or agency's IT security role. In addition, you will find IT security tips and contact information for CSEC.

CHANGES TO COURSES AND PROGRAMS OF STUDY

The environment in which we work rapidly changes as new threats emerge, and as such, IT security requirements and best practices are continually evolving. The ITSLC courses and programs of study are regularly reviewed for relevance, compliance, and efficiency and consequently, there may be changes to the programs of study and courses.

The 102 course has been superseded due to the new approach discussed in ITSG-33. The new ITSG-33 concepts and information are included in a new course titled "Information System Security Implementation Process" (ISSIP) (105). This course highlights integration of IT security risk management within the System Development Lifecycle as described in ITSG-33: IT Security Risk Management: A Lifecycle Approach. Upon completion, participants should be able to apply the Information System Security Implementation Process to a typical IT project where the objective is to implement a new information system or a new capability in an existing information system.

JAVA MITIGATION MEASURES

Java is a programming language and computing platform used by a multitude of authorized system and business processes and has an installation base of nearly one billion. It has become a target of great interest to cyber intruders who have discovered and exploited a large number of Java vulnerabilities. Some of the exploits have proven to be critical 'zero-day' vulnerabilities capable of compromising the security of the department's network and information holdings without warning.

The delay between 'vulnerability discovery' and 'mitigation patch' may render the department's network vulnerable for extended periods of time.

Only 5.5% of Java-enabled browsers have the most up-to-date versions of the software's browser plug-in installed.

Websense, 2013 Threat Report

The GC has thousands of systems installed with the Java platform. In most circumstances, the systems that utilize these Java applications execute on networks with internet access. This is problematic: if Java is plugged into the default browser and the user connects to a malicious website, the computer can be exploited through a vulnerability in the Java plugin exposing the department's network (through the users' connection) to a cyber-intruder with privileged access to the departments' network.

Normal mitigation options (i.e., patch management) are not sufficient to reinforce Java security because of the perceived decline in its security assurance. Each department's ITS Threat and Risk Assessment (TRA) should be revised to include existent Java vulnerabilities. The following are the recommended mitigation options:

- Ensure most recent patches have been installed;
- If possible, uninstall Java, otherwise:
  - disable the Java Browser Plugin;
  - disable Java in all but the Default Browser; and
  - restrict access to Java at the firewall.

READ ONLINE:
Java Vulnerability Mitigation (ITSB-98)

SECURITY PATCHING AND CVES

When security researchers or vendors discover new vulnerabilities in software applications or operating systems, they release security patches. In releasing this information, they are making public previously unknown vulnerabilities or exposures. These vulnerabilities then become known as Common Vulnerabilities and Exposures (CVEs).

Cyber threat actors monitor these releases and immediately begin writing code to take advantage of the advertised flaws before users install the fixes. The longer the gap between the patch release and application of those patches, the greater the likelihood that the CVE will be used to exploit computer networks and systems.

FACT: The U.S. National Vulnerability Database run by National Institute of Standards and Technology (NIST) currently contains more than 55,000 CVEs.

A large proportion of successful compromises rely on a small set of publicly known vulnerabilities for which patches are available. Analysis of the vulnerabilities that were most successfully exploited in the GC last year indicated that the majority of the exploits could have been avoided by patching a few CVEs, for which patches had long been available.

To minimize the risk posed by vulnerabilities, network administrators can:

- Run vulnerability scanning tools;
- Deploy automated patch management tools;
- Subscribe to vulnerability notification services to keep informed of new CVEs;
- Apply patches on all systems, even those that are air-gapped; and
- Remediate known vulnerabilities as quickly as possible, and within 48 hours for critical CVEs.

For more information, please download Assessing Security Vulnerabilities and Patches: ITSB-96.

BEING ACCOUNTABLE FOR COMSEC

GC Departments use COMSEC devices and key material to protect sensitive information. Losing control of COMSEC devices or key material is not only embarrassing, it can also compromise national security and international agreements. Fortunately, the possibility of compromises can be largely mitigated if they are reported promptly to the CSEC National COMSEC Incident Office (NCIO) at 613 991 8175 through the Departmental COMSEC Authority (DCA).

Here are the Top 5 most common types of incidents that the GC reported last year:

1. **Lost or Missing COMSEC material or Controlled Cryptographic Item (CCI)**
   Inability to locate or account for COMSEC material or CCI;
2. **Destruction of COMSEC material or CCI**
   Failure to destroy COMSEC material or CCI within prescribed time limits;
3. **Found COMSEC material or CCI**
   Discovery of COMSEC material not listed on current COMSEC inventory or in possession of (or easily accessible to) an unauthorized person;
4. **Unauthorized Access to COMSEC material or CCI**
   Unauthorized maintenance on COMSEC material or failure to maintain required Two-Person Integrity (TPI) or No-Lone Zone (NLZ) controls for TOP SECRET key; and
5. **Unauthorized Extension of Crypto Period**
   Continued use of superseded key without approval or failure to keep appropriate destruction records.

Answers from page 5: 1-E, 2-D, 3-A, 4-F, 5-B, 6-C

ABOUT THIS NEWSLETTER

Cyber Journal has been prepared for GC IT practitioners and stakeholders and is published on a periodic basis. This publication reflects the CSEC IT Security commitment to share information, advice and guidance with the broader GC community to help Departments and agencies better protect themselves from cyber threats. The aim is to highlight key security issues and stimulate discussion about security within your Department. In addition, the newsletter profiles key products and services offered by CSEC with information on how you can leverage them to help your GC organization. Security awareness throughout an organization is an essential element to improving the GC's security posture. As such, we encourage you to share this information within your organization.

SUBSCRIBE

To be notified of future releases, contact: itsclientservices@cse-cst.gc.ca.

CONTACT US

For general advice and security guidance support, contact:

✉ **itsclientservices@cse-cst.gc.ca**

✆ **General Inquiries: (613) 991-7654**

To report a cyber-incident contact the Cyber Threat Evaluation Centre:

✉ **ctec@cse-cst.gc.ca**

For planning, support or any issues regarding COMSEC devices, contact COMSEC Client Services:

✉ **comsecclientservices@cse-cst.gc.ca**

✆ **General Inquiries: (613) 991-8495**

COMSEC custodians can contact the Crypto Material Assistance Centre (CMAC):

✉ **cmac-camc@cse-cst.gc.ca**

✆ **General Inquiries: (613) 991-8600**

For education and training services, contact the IT Security Learning Centre:

✉ **its-education@cse-cst.gc.ca**