a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M6
Security of Wi-Fi Infrastructure

1. Introduction

1.1 UBC has a large and complex Wi-Fi network that plays an integral role in the operations of the University. Consequently, intruders and hackers may consider the Wi-Fi network an attractive target to breach the security of UBC Electronic Information and Systems.

1.2 This standard defines requirements to ensure that Wi-Fi devices, such as Wireless Access Points (WAPs), which allow Wi-Fi devices to connect to a wired network, are deployed in a secure, controlled and centrally managed way to reduce the likelihood of a security breach. Unless otherwise indicated, the UBC IT NETwork and Infrastructure Team is responsible for ensuring compliance with this standard. This policy applies to areas where WAPs installed by UBC IT provide Wi-Fi coverage.

1.3 In addition to this standard, UBC IT Wi-Fi networks provisioned by UBC IT are governed by Policy SC11, Management of the Wireless Network.

1.4 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Deployment of WAPs

2.1 All deployment of WAPs must be authorized by UBC IT.

2.2 WAP hardware must be protected to ensure physical security mechanisms (e.g. locked cabinet, high ceiling mount, etc.) are in place to prevent theft, alteration, or misuse.

3. Secure Configuration

3.1 All WAPs should be secured using a minimum of Wi-Fi Protected Access (WPA2) with a minimum of AES 128-bit encryption.

3.2 Wired Equivalent Privacy (WEP) is prohibited for Wi-Fi network security, as it is insecure.

3.3 It is recommended that Users connecting to WAPs, providing access to the UBC LAN, be configured to use the "AutoConnect" ubcsecure automated client configuration tool. This will help prevent connecting to rogue WAPs, which have been setup with the same name (spoofing) to steal credentials.

3.4 Console access must be password protected in compliance with the Passphrase and Password Protection standard.

3.5 WAP and wireless controller management must be handled as follows:

3.5.1 utilize secure protocols such as HTTPS, SSH, and CAPWAP;

3.5.2 management must only be over the LAN interface;

3.5.3 if SNMP is used in the management environment, all default SNMP community strings must be changed, otherwise it must be disabled;

3.5.4 vendor defaults such as encryption keys, and administrative passwords must be changed.

3.6 The use of Telnet or other insecure protocols is prohibited.

4. Security Updates

4.1 The operating system or software code on WAP and wireless controllers should be patched and kept current to ensure proper protection from the latest security vulnerabilities.

4.2 WAPs and wireless controllers must be replaced if they have reached end of life for software support.

5. Additional Requirements for Merchant Systems

5.1 Users responsible for Merchant Systems must:

5.1.1 ensure that a perimeter firewall is in place between any Wi-Fi network and Merchant Systems processing Payment Card Industry (PCI) Information. These firewalls must be configured to deny or control any traffic from the Wi-Fi environment to Merchant Systems;

5.1.2 test for the presence of unauthorized WAPs on a quarterly basis. Note: Methods that may be used in the process include, but are not limited to, Wi-Fi network scans, physical/logical inspections of system components and infrastructure, network access control NAC), or Wi-Fi IDS/IPS; and

5.1.3 report any unauthorized WAPs as a security incident, in compliance with the Reporting Information Security Incidents standard.

Related Documents

Policy SC11, Management of the Wireless Network

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

UBC IT AutoConnect Secure Wireless Setup

Passphrase and Password Protection standard

Reporting Information Security Incidents standard