Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

## *Information Technology Security Guidance*

# *Security Requirements for Wireless Local Area Networks*

## Overview

## ITSG-41

**March 2013**

# Foreword

The *ITSG-41 Security Requirements for Wireless Local Area Networks* document is an UNCLASSIFIED publication, issued under the authority of the Chief, *Communications Security Establishment Canada* (**CSEC**).

Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSEC.

Requests for additional copies or changes in distribution should be directed to your Client Services Representative at CSEC.

For further information, please contact CSEC’s ITS Client Services area by e-mail at ITSclientservices@cse-cst.gc.ca, or call 613-991-7654.

# Effective Date

This publication takes effect on 2013-03-14.

Originally signed by

*Toni Moffa*

*Deputy Chief, IT Security*

# Executive Summary

The information provided in this document is intended to assist in the mitigation of threats associated with a *Wireless Local Area Network* (**WLAN**) deployment by offering security advice to be used during the high-level design phase. The typical threats arise principally due to the lack of a secure physical boundary and include:

- Unauthorized association (accidental and malicious);
- Ad-hoc network creation;
- Identity theft;
- Denial of service;
- Wireless interception; and
- Device theft.

The types of WLAN deployments addressed in this document are based on the currently identified business needs of *Government of Canada* (**GC**) Departments in the unclassified and classified domains and are as follows:

1) Government hot spot: Guests of the Department connect their wireless enabled workstations to the Internet through WLAN services supported by the departmental network which have no access to departmental applications;

2) Wireless user to wired network connection: Employees within the physical boundaries of the Department connect their wireless enabled workstations to the wired departmental network through WLAN services; and

3) Wired network to wired network via wireless bridge: Employees within the physical boundaries of the Department connect their wired workstations to a wired subnet. The connectivity between the subnet and the departmental network is achieved using a WLAN bridge.

Reference high-level designs are specified for each business use case and security is subsequently addressed through the identification of prospective technology-related control elements (i.e., elements of security controls) and their placement.

This guidance is structured to be used within the framework of IT security risk management activities defined within the publication: *ITSG-33 - IT Security Risk Management: A Lifecycle Approach* (**ITSG-33**) **[1]**[1].

[1] Numbers formatted like "[9]" refer to references listed under the ***References*** heading on the last page of this document.

# Revision History

| Document No. | Title | Release Date |
|---|---|---|
| ITSG-41 Overview | Security Requirements for Wireless Local Area Networks – Overview | 2013-03-14 |
| | | |
| | | |

# Table of Contents

# List of Figures

# List of Annexes

# List of Abbreviations

| | |
|---|---|
| AES | Advanced Encryption Standard |
| Department | GC Department or agency |
| ISSIP | Information System Security Implementation Process |
| IT | Information Technology |
| LAN | Local Area Network |
| SDLC | System Development Life Cycle |
| Technology-related control elements | Elements of Security controls to be addressed through the implementation of information system technologies (i.e. hardware or software) |
| WIDS | Wireless Intrusion Detection System |
| Wi-Fi | Wireless Fidelity (also referred to as “Wireless”) |
| WLAN | Wireless Local Area Network |
| WLAN Services | WLANs deployed within departmental networks |
| WPA | Wi-Fi Protected Access |

# 1 Introduction

## 1.1 Context

WLAN deployments extend the topology of a departmental network in a manner similar to adding a wired *Local Area Network* (**LAN**). As a result, the security requirements necessary to secure an additional wired LAN would be similar to those required to secure a WLAN. However, because the WLAN coverage area cannot be physically secured as well as a wired LAN, there are additional security considerations required to protect the confidentiality, integrity and availability of WLAN communications and to protect the departmental network and its information services against compromises and attacks.

This document describes WLANs in the context of wireless end user devices connecting to network access points via Wi-Fi, based on the IEEE 802.11 [Reference 2] suite of standards (e.g. it does not describe end user devices that connect to a WLAN via Bluetooth).

## 1.2 Purpose

Through the use of defined business use cases, this document will describe the technology based security requirements as they relate to typical departmental WLAN deployments. These requirements are further represented within a zoned reference architecture which can then be leveraged to produce an initial high-level WLAN design.

This guidance is structured to be used within the framework of *Information Technology* (**IT**) security risk management activities defined in ITSG-33**.**

## 1.3 Target Audience

This overview is intended for information system/security practitioners, executive level decision makers and those who are responsible for IT security risk management activities associated with the design and implementation of WLANs.

## 1.4 Publication Taxonomy

This document is part of a series of documents that together form the ITSG-41 publication suite. The other documents in the series are listed below:

- *Annex 1 - Government Hot Spot High-Level Design Guidance;*
- *Annex 2 - Wireless User to Wired Network Connection High-Level Design Guidance;*
- *Annex 3 - Wired Network to Wired Network via Wireless Bridge High-Level Design Guidance; and*
- *Annex 4 - Identification of Control Elements from Security Controls.*

## 2. Common Vulnerabilities Facing WLANs

WLANs have many benefits over their wired LAN counterparts including reduction in cabling costs, ease of deployment within existing buildings (i.e., less invasive) and support for roaming. As a result, deployments of WLANs are becoming increasingly popular within the GC. Given this technology paradigm, Departments are subject to additional vulnerabilities which may lead to 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. Given this, attackers do not need to be located within the physical security boundaries of the Department to launch attacks within the network as illustrated in *Figure 1 - Transmission Patterns*. Through this associated extension of the environment, additional threats need to be considered when selecting security requirements for a solution.

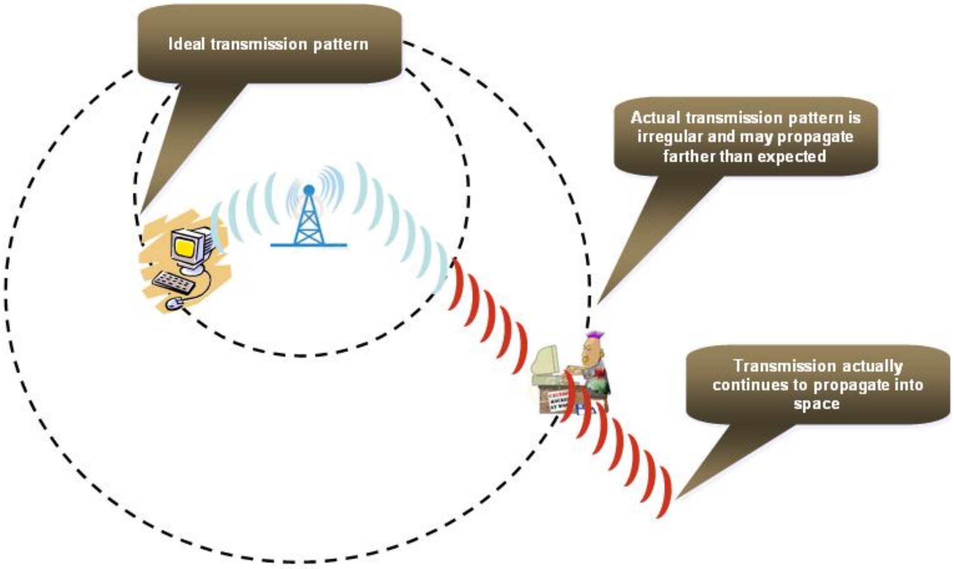
Ideal transmission pattern
Actual transmission pattern is irregular and may propagate farther than expected
Transmission actually continues to propagate into space

**Figure 1 - Transmission Patterns**

Typical vulnerabilities facing WLAN deployments are:

- **Unauthorized Association**
  - Accidental: Departmental devices connecting automatically to an access point within range but not part of the Departments network. Also, staff members inadvertently adding WLAN Access Points without management approval, creating unsecured backdoors to the corporate network.
  - Malicious: Departmental devices connecting to a rogue access point masquerading as a valid access point (e.g., The “Man in the middle” attack routes traffic through a rogue intermediary device, thus allowing the user to access departmental resources while capturing all traffic).
- **Non-traditional:** Secondary devices (e.g., Wi-Fi printers, Bluetooth devices) overlooked by the Department and leveraged by threat agents as entry points into the network.
- **Ad-hoc Networks:** Peer-to-peer connections enabled on departmental devices (e.g., laptops allowing other devices to connect directly to them), thus allowing outside rogue devices to connect to the network through these departmental assets.
- **Identity Cloning:** Attacker gains access by listening to an authentic connection and clones a valid identity.
- **Denial of Service:** Outside systems flooding departmental access points with bogus access requests or useless data, thus denying users from gaining access and potentially bringing down the WLAN network.
- **Wireless Interception:** Traffic over the air not properly encrypted which allows outside users the ability to eavesdrop on wireless information.
- **Device Theft:** Increased likelihood of stolen wireless devices due to their portability, thus facilitating device/network compromise.

Considering the increase in potential risks, specific security controls need to be selected and the associated control elements tailored based on the type of WLAN solution being deployed.

# 3. Technology-Related Control Elements for WLAN Services

As part of a Department's *System Development Life Cycle* (**SDLC**) process, a requirements analysis phase is conducted (as defined in ITSG-33 - Annex 2 [Reference 1]) in order to select an approved set of security controls for a WLAN services deployment. The selection of the security controls address:

a. The WLAN services business needs for security; and

b. Any departmentally mandated security controls applicable to the deployment.

*Figure 2 - Security Controls Categorization* shows the approved set of security controls for the WLAN services deployment that include security controls from the management, technical and operational classes. As per ITSG-33 these are defined as:

a. Management Class - includes security controls that are not implemented within an information system and focus on the management of IT security and IT security risks;

b. Technical Class - includes security controls that are typically implemented within an information system using hardware, software, or firmware components; and

c. Operational Class - includes information system security controls that are typically implemented and executed by people (i.e., adherence to policies or execution of procedures).

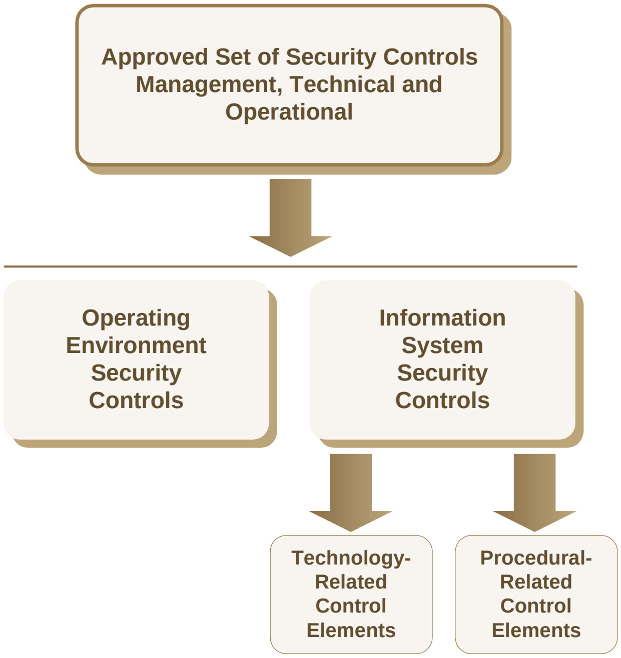
Approved Set of Security Controls
Management, Technical and Operational
Operating Environment Security Controls
Information System Security Controls
Technology-Related Control Elements
Procedural-Related Control Elements

**Figure 2 - Security Controls and Control Elements**

These security controls are then further grouped into two categories:

- Operating Environment security controls; and
- Information System security controls.

Operating environment security controls are not described in detail within this document as they are predominately management or operational in nature and implemented through programs, policies or procedures at the departmental level.

The remaining information system security controls are further subdivided into:

- Technology-related control elements - defined as elements of security controls that are to be implemented using technology (e.g., firewall); and
- Procedural-related control elements - defined as elements of security controls that are implemented using policies or manual procedures (e.g., human review of firewall logs).

Given procedural-related control elements are highly dependent on the implementation of the technology requirements (e.g., the selection of IT products, departmental policy and risk tolerance), this document focuses solely on the technology-related control elements. Departments will therefore need to define the corresponding procedural-related control elements in support of their chosen solution.

# 4. Business Use Cases

The types of WLAN deployments and the associated technology-related control elements addressed in this document are based on the typical business needs of Departments. The different types of WLAN deployments range from a rudimentary hot spot architecture to more complicated implementations such as interconnecting departmental networks through WLAN Services.

## 4.1 Government Hot Spot

The Government Hot Spot Business Use Case describes the deployment of WLAN services to allow guests of the Department (i.e., non employees) to connect their wireless enabled devices to the internet (Figure 3). The role of the departmental network in this business use case is to solely route the guest communications to and from the Internet.  Other departmental services supported by the departmental network would not be accessible by the guests as described in *Annex 1*.

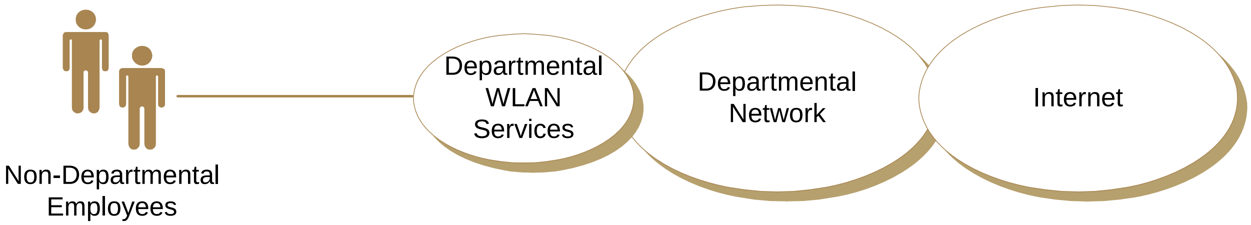

**Figure 3 - Government Hot Spot Business Use Case**

An example of this business use case would be a department providing internet access to visitors within a common area (e.g., waiting area or meeting room).

## 4.2 Wireless User to Wired Network Connection

The Wireless User to Wired Network Connection Business Case describes the deployment of WLAN services to allow employees within the physical boundaries of the Department to connect their wireless enabled workstations (i.e., laptops or desktops) to the departmental network (Figure 4). Employees can connect to the WLAN services while they are at their desk or they can roam (without session interruption) throughout the Department where the WLAN services are available as described in *Annex 2*.

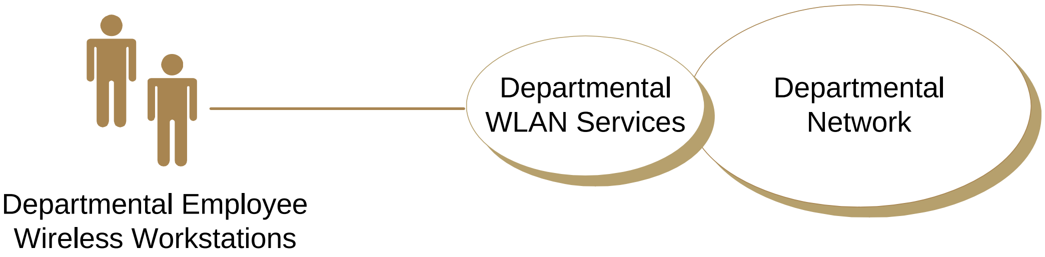
Departmental WLAN Services
Departmental Network
Departmental Employee Wireless Workstations

**Figure 4 - Wireless User to Wired Network Connection Business Case**

An example of this business use case would be an employee on site using a wireless laptop to connect to departmental resources to conduct day to day activities.

## 4.3 Wired Network to Wired Network via Wireless Bridge

Wired Network to Wired Network via Wireless Bridge Business Case describes the deployment of WLAN services to bridge a segregated wired LAN to a departmental network (Figure 5). The segregated wired LAN has no physical connection to the departmental network. The WLAN service extends network access and allows employees within the segregated wired LAN to access departmental network services as described in *Annex 3*.

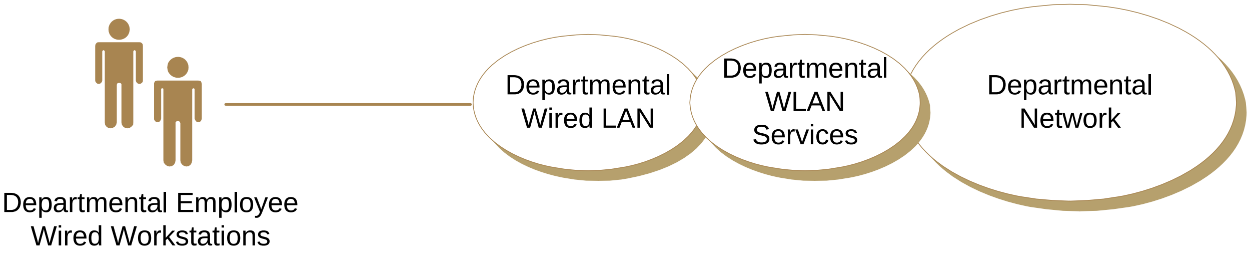
Departmental Wired LAN
Departmental WLAN Services
Departmental Network
Departmental Employee Wired Workstations

**Figure 5 - Wired Network to Wired Network via Wireless Bridge**

An example of this business use case would be a two separate network infrastructures interconnecting through wireless services (e.g., ship to shore).

# 5. Summary

By leveraging the information in this document during the requirements analysis and high-level design phases of a SDLC, appropriate security controls and the subsequent technology-related control elements will be identified to help mitigate against typical WLAN threats. The technology-related control elements presented in the annexes of this document are described within the context of a 'zoned' network architecture for each business use case.  Security practitioners should therefore select the applicable annex based on their use case and apply the associated information to assist in the completion of their high-level zoned design.

# 6. References

[1] *ITSG-33 - IT Security Risk Management: A Lifecycle Approach - Overview;* **CSEC** (Nov 2012)

[2] *The IEEE Standards Association* (standards.iee.org)