SECURITY GUIDELINES FOR WI-FI DEPLOYMENT
## CONTENTS

1. Executive Summary ................................................................. 2
2. PURPOSE AND SCOPE .................................................................. 2
3. INTRODUCTION ............................................................................ 2
4. WLAN SECURITY ........................................................................... 3
5. Wi-Fi DEPLOYMENT LIFECYCLE .................................................. 4
6. ABBREVIATIONS ........................................................................... 13
7. REFERENCES ................................................................................ 14
1. EXECUTIVE SUMMARY

Wireless networks are an important component of modern network architecture. They are required to support mobile devices and provide connectivity to various devices where wired connections are not practical or cost prohibitive. But the missing physical control of the medium does require additional precautions to control access to wireless networks.

The 802.11 standard for wireless networks does offer encryption and authentication methods like WPA and WPA2. But in an enterprise environment, these controls have to be implemented in a scalable and manageable way. This paper presents a hands-on guide to implementing a secure Wi-Fi network in an enterprise environment.

2. PURPOSE AND SCOPE

The purpose of this guideline is to provide organizations with recommendations for improving the security configuration and monitoring of their IEEE 802.11 wireless local area networks (WLANs) and their devices connecting to those networks. The scope of this guideline is limited to Wi-Fi services provided under Unlicensed frequency bands. This document also intends the various steps and different security considerations which can be adopted during the Wi-Fi installation at every subsequent stages.

This guideline supplements and hence does not supersede the recommendations in other guidelines issued from time to time by DoT, such as those issued vide letter no. 842-725/2005-VAS dated 23.02.2009.

3. INTRODUCTION

WLANs created using Wi-Fi technology can be used to connect personal computers, mobile phones, tablets and other appliances to a local network, which in turn provides connectivity to the Internet. These WLANs can be operated for private use, such as in the home, or to create short-range, public networks, known as “hotspots”, which can be found in public places like airport lounges, coffee shops or neighborhoods.

WLANs are usually implemented as extensions to existing wired local area networks (LANs) to provide enhanced user mobility and network access. WLAN technologies are based on the IEEE 802.11 standard and its amendments. Throughout the rest of this document, the generic term “WLAN” refers to an IEEE 802.11 WLAN.
The two fundamental types of WLAN components are client devices (such as laptops and smartphones) and access points (APs), which logically connect client devices with a distribution system (DS), typically the organization’s wired network infrastructure. The DS is the means by which client devices can communicate with the organization’s wired LANs and external networks such as the Internet. Some WLANs also use wireless switches, which act as intermediaries between APs and the DS. The purpose of the switch is to assist administrators in managing the WLAN infrastructure. Figure 1 shows a simplified view of WLAN components that includes a wireless switch. WLANs without wireless switches have a similar architecture, except that the APs connect directly to the DS.

![Figure 1: Basic WLAN Architecture (Ref:NIST 800-153)](image)

### 4. WLAN SECURITY

Security has remained a major concern in WLANs around the globe. While wireless networks provide convenience and flexibility, they also increase network vulnerability. Security threats such as unauthorized access, denial of service attacks, IP and MAC spoofing, session hijacking and eavesdropping can all be problems for WLANs. To address these issues various authentication, encryption and administrative control techniques are used in WLANs, but even then poor planning and insecure configurations have allowed attackers to break into banks, businesses, and government agencies.

Organizations should have standardized security configurations for their common WLAN components, such as client devices and APs. A standardized configuration provides a base level of security, minimizes vulnerabilities and reduces the impact of successful attacks.
Organizations need to identify the risks, the businesses assets, and the steps necessary for mitigation and protection.

Although it is impossible to eliminate the risks completely, but by implementing certain security best practices the risk can be minimized. To ensure comprehensive Security, the security provisions should be considered at each phase of Wi-Fi deployment.

5. **WI-FI DEPLOYMENT LIFECYCLE**

Security best practices needs to be followed throughout the various phases of the entire lifecycle model of Wi-Fi deployment like design phase, implementation phase and operation and maintenance phase. This section explains the five phases of lifecycle model for Wi-Fi deployment and best practices which should be adopted for ensuring security. The phases of life cycle are as follows:

5.1. **Initialization Phase:**

This phase includes the tasks that an organization should perform before it starts to design its WLAN solution. These include providing an overall vision for how the WLAN would support the mission of the organization, creating a high-level strategy for the WLAN’s implementation, developing a WLAN use policy, and specifying business and functional requirements for the solution as requirements may effect decision on type of security measures should be deployed to protect the network. For example, if guest access is required, security best practices for guest access should be considered in the design stage.

5.2. **Planning:**

During this phase, details of WLAN solution and its whole architecture is to be specified including the features and filtering rules of traffic to the framing of security policies. A site survey is also be planned to determine the number and placement of access points, as well as how they integrate into the existing network.

5.3. **Configuration Design:**

While planning WLAN security, configuration designers should consider the security not only of the WLAN itself, but also how it may affect other networks that are accessible through it, such as internal wired networks reachable from the WLAN. An important principle of WLAN security is to separate WLANs with different security profiles. For example, there should be separate WLANs for external (guest, etc.) and internal use. Devices on an organization’s external WLAN should not be able to connect through that WLAN to devices on the organization’s other WLANs. This helps to protect the organization’s other networks and devices from external devices and users. Organizations often set up external WLANs
primarily to provide Internet access to visitors; such WLANs should be architected so that their traffic does not traverse the organization’s internal networks. For external WLANs that do need internal network access, WLAN client devices should be allowed access only to the necessary hosts or subnets using only the required protocols.

i. **Comprehensive Site Surveys:**

Site survey is an important part while considering the security scenario of organization. It provides definitive set of information for developing a wireless deployment and security plan. The survey is a defined set of tasks performed in the facility that documents the wireless characteristics of the physical facilities, coverage areas, and interference sources. This information is essential to understanding the optimal number and placement of WAPs and WIDS/WIPS devices to provide desired coverage and functionality in a facility. Excessive coverage by the wireless signal could pose significant threat to the organization.

ii. **Security Standards:**

Organizations should keep track of latest Wi-Fi Security standards and should use latest security standards. Presently WPA2/AES is recommended standards. Although a vulnerability has been discovered recently in this protocol but it can only be exploited from within the physical proximity of the target Wi-Fi network and not remotely through the Internet. WPA2 is still a more secure solution compared to WEP -the previous Wi-Fi protocol. Hence, switching to an older -trivially exploitable- protocol, is highly discouraged. It is better to continue using WPA2 along with its latest patches released by the respective vendors.

WPA3 protocol specifications are under development and expected to be released in later 2018 and by the time the actual products implementing WPA3 hit the market, WPA2 is the recommended solution.

Securing the access points is one of main step in protecting a wireless network. Equipment shall conform to WPA2 based on IEEE 802.11i standard and access control authentication based on 802.1X / EAP Standard.

iii. **Secure management of Dual connected clients:**

The term “dual connected” generally refers to a device that is capable of being connected to two different types of networks like wired network and WLAN, cellular network and WLAN, Bluetooth and WLAN etc. The primary concern with dual connected configurations is that an attacker may be able to gain unauthorized wireless access to the client device and then use it to attack resources on the organization’s internal network. Organizations should have policies that clearly state which forms of dual connections are permitted or prohibited for their WLAN client devices under various circumstances.
a. For all their WLAN client devices: disable all network interfaces that are not authorized for any use and configure the device so that the user cannot enable them or otherwise circumvent the restrictions.

b. For all their WLAN client devices not authorized for dual connections:
   • Implement the appropriate technical security controls so that all dual connected configurations are prohibited.
   • If feasible, configure the devices to disable bridging (passing traffic between the networks). This is precautionary in case an unauthorized dual connection occurs.

c. For all their WLAN client devices authorized for dual connections:
   • Implement the appropriate technical security controls so that the authorized dual connected configurations are only active when necessary and that all other dual connected configurations are prohibited.
   • Configure the devices to disable bridging (passing traffic between the networks) unless absolutely necessary.

d. Configure the device’s BIOS so that WLAN connections are automatically terminated when a wired connection is detected. The BIOS setting for this is often called LAN/WLAN switching.

e. Enable specialized software-based controls that permit either WLAN or wired network access, but not both simultaneously. These controls could be built into the operating system (OS), provided as part of the WLAN driver or management software, provided by the device manufacturer (e.g., laptop vendor), or acquired from third parties. These controls typically favour wired connections over WLAN because of their relative reliability, performance, and security.

f. Configure host-based network security tools (e.g., host-based firewalls, host-based intrusion detection and prevention systems) to prevent multiple network interfaces from being used at one time.

g. Specify and enforce authorized network profiles and/or unauthorized profiles through OS/domain controls, third party policy-based software, etc.

iv. Controlled wireless coverage

As per information collected from site surveys appropriate location of access points can be designed to avoid excessive coverage by the wireless network and hence limit the possibility of intrusion. In addition to proper placement of the access points, adjusting the radio frequency (RF) power transmission or using directional antennas can also control the propagation of the RF signal and hence control coverage of a wireless network.

Due to the limited transmission capacity of a wireless network, a malicious attacker can easily launch a Denial-of-Service (DoS) attack to bring down the network. Segmenting access
point coverage areas can balance the loads on a wireless network and minimize any impact from DoS attacks.

v. Separate Wireless Networks from Wired Networks

It is always recommended that Inside an organization wireless network and wired network should not be directly connected to each other. Firewalls can be deployed to separate and control the traffic between different networks.

5.4. Define Wireless Security policy

The organization should develop a strong wireless security policy to address all the usage options of wireless networks and the types of information that can be transmitted. The policy should outline a framework for the development of installation, protection, management and usage procedures. Security and operation guidelines, standards and personnel roles should also be clearly defined.

5.5. Procurement Stage:

After planning and designing the system, procurement should be done as per required configuration and supported standards. WPA2-Enterprise certified STA and AP products only should be procured. Organizations that plan to deploy authentication servers as part of an IEEE 802.1X and EAP implementation should procure products with the Enterprise level certification as WPA2 have both enterprise and personal modes of operation.

5.6. Implementation Stage:

During this phase, procured equipment is first configured to meet operational and security requirements, and then installed and activated on a production network. At this stage, initial emphasis is to be done on whether all implementation is done as per recommended planning procedures. i.e Configuration is designed as per adequate security standards. In addition to this following procedures should be adopted:

i. Strong Physical controls should be implemented:
Any network equipment such as access points should be mounted in less accessible locations with strong physical security controls as it will minimize risk of theft.

ii. Wireless Networks coverage:

Excessive coverage of wireless networks should be avoided. As per information collected from site surveys proper placement of access points can be designed to avoid excessive coverage by the wireless network and hence limit the possibility of intrusion. In addition to proper placement of the access points, adjusting the radio frequency (RF) power
transmission or using directional antennas can also control the propagation of the RF signal and hence control coverage of a wireless network.

iii. Security of Access points and Wireless Access Controller:

Securing the access points is one of main step in protecting a wireless network. Equipment shall conform to WPA2 based on IEEE 802.11i standard and access control authentication based on 802.1X / EAP Standard. Wireless Controllers and Access points should set up with Remote Authentication Dial-In User Service (RADIUS) Authentication for Securing Management access as per IETF RFC 2865 to maintain authentication and authorization.

The following general measures should be adopted while securing access points:

a. Change the default configuration settings;
b. Change encryption keys regularly;
c. Ensure that all access points have strong, unique administrative passwords and change the passwords regularly;
d. Disable all insecure and unused management protocols on access points and configure the remaining management protocols for least privilege;
e. Activate logging features and direct all log entries to a remote logging server;
f. Enable wireless threshold parameters, such as inactivity timeouts and maximum supported associations.

iv. Internal Networks should be properly separated:
Isolate the network using proper network segmentation logically. The LAN segments that connect to wireless APs should connect to a corporate Virtual Private Network (VPN) gateway, but not directly to the internal network. Eliminating APs from the internal network minimizes the risk of attack techniques.

v. Usage of non-suggestive SSID conventions:
SSID is generally broadcasted in wireless network area. By using suggestive names of SSID it may be chance that attacker may get internal information of organization by collecting reconnaissance information of wireless network.

vi. Disable “Ad-Hoc Mode” Transmissions:
In ad-hoc mode, it is possible that attacker can gain access to client easily if station is not properly configured. Hence it is ad-hoc mode should be disabled in device while using enterprise network.

vii. Up to date security patches should be used.
Security patches should be updated and installed in device addressing the newly discovered security vulnerabilities.
viii. MAC address filtering on access points:
   In enterprise wireless implementation MAC address filtering may be used and by using this the device with pre-approved MAC address can be granted access to network. But this solution is not very feasible in Public Wi-Fi hotspots.

ix. Usage of Wireless Intrusion Detection/Intrusion Prevention Systems:
   Deployment of Wireless Intrusion Detection Systems can help detect and prevent malicious activities along with detection of rogue access points. It also monitors any unauthorized access to network and take necessary steps for its prevention. Processes and policies should be properly defined for reviewing and acting on data provided by IDS/IPS Systems.

5.7. **Operation and Maintenance Phase:**

This phase includes security related tasks that organizations should regularly perform after entire network become operational.

5.7.1. **Continuous Security monitoring of WLAN**

Organizations with WLANs should implement continuous monitoring solutions for their WLANs that provide all of the following detection capabilities:

i. Unauthorized WLAN devices, including rogue APs and unauthorized client devices

ii. WLAN devices that are misconfigured or using weak WLAN protocols and protocol implementations.

iii. Unusual WLAN usage patterns, such as extremely high numbers of client devices using a particular AP, abnormally high volumes of WLAN traffic involving a particular client device, or many failed attempts to join the WLAN in a short period of time

iv. The use of active WLAN scanners (e.g., war driving tools) that generate WLAN traffic. The use of passive sensors cannot be detected through monitoring controls.

v. DoS attacks and conditions (e.g., network interference). Many denial of service attacks are detected by counting events during periods of time and alerting when threshold values are exceeded. For example, a large number of events involving the termination of WLAN sessions can indicate a DoS attack.

vi. Impersonation and man-in-the-middle attacks. For example, some WIDPS (Wireless Intrusion Detection and sensors can detect when a device is attempting to spoof the identity of another device.

Organizations with WLANs should also have the capability to identify the physical location of a detected WLAN threat by using triangulation i.e. estimating the threat’s approximate distance from multiple sensors by the strength of the threat’s signal received by each sensor, then calculating the physical location at which the threat would
be the estimated distance from each sensor. This allows an organization to send appropriate personnel, such as physical security staff, to the location to address the threat.

5.7.2. User Security and authentication:
Ensure that wireless traffic leverages at least Advance Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection. Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.

There are primarily two methods which could be adopted for authentication and access to users:

i. EAP-SIM/AKA Based Authentication
   2 factor authentication may be adopted for all type of network/service access. Subscribers or employees within an enterprise network may get authenticated directly using SIM/AKA Credentials for access of services. MAC filtering should be adopted at access points as a second factor of authentication.

ii. Captive Portal based Authentication
   A captive portal is a Web page that the user of a public-access network is obligated to view and interact with before access is granted. Captive Portals allow for the separation and segregation of guest traffic. As guest users will have different ACLs based on a company’s security policies, they will have limited access inside the corporate network. This will give the right users the right amount of access within any network.
   Guest users using an enterprise Wi-Fi network should be granted access only after authentication through captive portal.

5.7.3. Periodic Security assessment of WLAN
Organizations with WLANs should conduct regular periodic technical WLAN security assessments. These assessments should be performed at least annually to evaluate the overall security of the WLAN. In addition, organizations should perform periodic assessments at least quarterly unless continuous monitoring of WLAN security is already collecting all of the information about WLAN attacks and vulnerabilities needed for assessment purposes. For example, an organization that does not have comprehensive WIDPS coverage of its facilities should use mobile WIDPS sensors, WLAN scanners, or other tools with similar capabilities to search for rogue WLANs in areas outside the WIDPS’s range.
5.7.4. Detection of rogue access points:
Network vulnerability scanning tools should be configured to detect wireless access points connected to the wired network. Devices thus detected should be reconciled against a list of authorized wireless access points. Unauthorized (i.e. rouge) access points should be deactivated.
Wireless intrusion detection and prevention systems (WIDPS) should also be used to identify rouge wireless devices and detect attack attempts and successful compromises. In addition to this, all wireless traffic should be monitored by WIDPS as traffic passes into the wired network.

5.7.5. Other miscellaneous best practices
i. Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).
ii. Disable peer-to-peer wireless network capabilities on wireless clients.
iii. Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.
iv. Create separate virtual local area network (VLANs) for BYOD system or other untrusted devices. Internet access from this VLAN should go through the same border as corporate traffic. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly.
v. Security patches addressing the newly discovered security vulnerabilities should be installed and updated in all the devices connected to the WLAN.
vi. In enterprise wireless implementation MAC address filtering may be used so that only the devices having pre-approved MAC address can be granted access to WLAN. But this solution may not be feasible for Public Wi-Fi hotspots.
vii. VPN access is recommended for accessing highly confidential services through WLAN. After authentication, authorized users communicate using an encrypted tunnel between the connecting device and the WLAN, reducing the risk.

5.7.6. Maintenance, monitoring and Analysis of Audit logs:
An audit process should be developed to ensure that any unauthorized behaviour and security breach can be detected mainly to capture security relevant events. Audit logs should be regularly checked and any abnormalities if observed should be analyzed and addressed.
5.7.7. **Incident response procedures:**

Incident response procedures should be developed to address any security attacks and should be updated regularly.

5.8. **Security guidelines for Users:**

User should be educated as awareness of user is always a critical step in maintaining security. Following are the guidelines which user needs to adopt for ensuring maximum security:

i. Device should be protected by proper password implementation. It should also be updated regularly.

ii. Wireless connections should be disabled when not in use.

iii. Wireless Network Interface Card drivers should be updated regularly as and when updates are received.

iv. Antivirus software with updated virus definitions should be used.

v. Encrypt the sensitive and personal data on device.

vi. Wired and wireless interface cards should not be enabled at the same time.

vii. Authenticity of captive portal should be checked before accessing Wi-Fi by verifying the server certificate.

viii. While disposing old wireless components, all sensitive configuration such as SSIDs or encryption keys should be erased.
6. ABBREVIATIONS

i. AES  Advanced Encryption Standard
ii. AP  Access Point
iii. BIOS  Basic Input/output System
iv. BYOD  Bring Your Own Device
v. DDoS  Distributed Denial of Service
vi. DoT  Department of Telecommunication
vii. DS  Distribution Systems
viii. EAP-TLS  Extensible Authentication Protocol-Transport Layer Security
ix. IDS  Intrusion Detection Systems
x. IPS  Intrusion Prevention Systems
xi. MAC  Media Access Control
xii. OS  Operating System
xiii. RF  Radio Frequency
xiv. SSID  Service Set Identification
xv. TLS  Transport Layer Security
xvi. WAP  Wireless Application Protocol
xvii. WIDPS  Wireless Intrusion Detection and Prevention System
xviii. WLAN  Wireless Local Area Network
xix. WPA  Wireless Protected Access
7. REFERENCES

i. A Guide to Securing Networks for Wi-Fi (IEEE 802.11 Family) by Department of homeland Security
ii. NIST 800-153- Guidelines for Securing Wireless Local Networks (WLANs)
iii. NIST 800-97- Guidelines for Securing Wireless Local Networks (WLANs)
iv. WIRELESS NETWORKING SECURITY by The Government of the Hong Kong Special Administrative Region
v. A Secure Approach to Deploying Wireless Networks by SANS institute