INTERNATIONAL STANDARD

ISO/IEC 27033-6

First edition
2016-06-01

Information technology — Security techniques — Network security —

Part 6: Securing wireless IP network access

Technologies de l'information — Techniques de sécurité — Sécurité de réseau —

Partie 6: Sécurisation de l'accès réseau IP sans fil

Reference number
ISO/IEC 27033-6:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

ISO/IEC 27033 consists of the following parts, under the general title *Information technology — Security techniques — Network security*:

— *Part 1: Overview and concepts*

— *Part 2: Guidelines for the design and implementation of network security*

— *Part 3: Reference networking scenarios — Threats, design techniques and control issues*

— *Part 4: Securing communications between networks using security gateways*

— *Part 5: Securing communications across networks using virtual private networks (VPNs)*

— *Part 6: Securing wireless IP network access*

Introduction

In today's world, the majority of both commercial and government organizations have their information systems connected by networks with the network connections being one or more of the following:

— within the organization;

— between different organizations;

— between the organization and the general public.

Further, with the rapid developments in publicly available network technology (in particular with the Internet) offering significant business opportunities, organizations are increasingly conducting electronic business on a global scale and providing online public services. The opportunities include the provision of lower cost data communications, using the Internet simply as a global connection medium, through to more sophisticated services provided by Internet service providers (ISPs). This can mean the use of relatively low cost local attachment points at each end of a circuit to full scale online electronic trading and service delivery systems, using web-based applications and services. Additionally, the new technology (including the integration of data, voice and video) increases the opportunities for remote working (also known as "teleworking" or "telecommuting") that enable personnel to operate away from their homework base for significant periods of time. They are able to keep in contact through the use of remote facilities to access organization and community networks and related business support information and services.

However, while this environment does facilitate significant business benefits, there are new security risks to be managed. With organizations relying heavily on the use of information and associated networks to conduct their business, the loss of confidentiality, integrity, and availability of information and services could have significant adverse impacts on business operations. Thus, there is a major requirement to properly protect networks and their related information systems and information. In other words, *implementing and maintaining adequate network security is absolutely critical to the success of any organization's business operations.*

In this context, the telecommunications and information technology industries are seeking cost-effective comprehensive security solutions, aimed at protecting networks against malicious attacks and inadvertent incorrect actions, and meeting the business requirements for confidentiality, integrity, and availability of information and services. Securing a network is also essential for maintaining the accuracy of billing or usage information, as appropriate. Security capabilities in products are crucial to overall network security (including applications and services). However, as more products are combined to provide total solutions, the interoperability, or the lack thereof, will define the success of the solution. Security should not only be a thread of concern for each product or service, but should be developed in a manner that promotes the interweaving of security capabilities in the overall security solution.

The purpose of ISO/IEC 27033 is to provide detailed guidance on the security aspects of the management, operation and use of information system networks, and their inter-connections. Those individuals within an organization that are responsible for information security in general, and network security in particular, should be able to adapt the material in this document to meet their specific requirements. Its main objectives are as follows.

— ISO/IEC 27033-1 aims to define and describe the concepts associated with, and provide management guidance on, network security. This includes the provision of an overview of network security and related definitions, and guidance on how to identify and analyze network security risks and then define network security requirements. It also introduces how to achieve good quality technical security architectures, and the risk, design and control aspects associated with typical network scenarios and network — technology areas (which are dealt with in detail in subsequent parts of ISO/IEC 27033).

— ISO/IEC 27033-2 aims to define how organizations should achieve quality network technical security architectures, designs and implementations that will ensure network security appropriate to their

business environments, using a consistent approach to the planning, design and implementation of network security, as relevant, aided by the use of models/frameworks (in this context, a model/framework is used to outline a representation or description showing the structure and high level workings of a type of technical security architecture/design), and is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example, network architects and designers, network managers, and network security officers).

— ISO/IEC 27033-3 aims to define the specific risks, design techniques and control issues associated with typical network scenarios. It is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example, network architects and designers, network managers, and network security officers).

— ISO/IEC 27033-4 aims to define the specific risks, design techniques and control issues for securing information flows between networks using security gateways. It is relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example, network architects and designers, network managers, and network security officers).

— ISO/IEC 27033-5 aims to define the specific risks, design techniques and control issues for securing connections that are established using virtual private networks (VPNs). It is relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example, network architects and designers, network managers, and network security officers).

— ISO/IEC 27033-6 aims to define the specific risks, design techniques and control issues for securing IP wireless networks. It is relevant to all personnel who are involved in the detailed planning, design and implementation of security for wireless networks (for example, network architects and designers, network managers, and network security officers).

It is emphasized that ISO/IEC 27033 provides further detailed implementation guidance on the network security controls that are described at a basic standardized level in ISO/IEC 27002.

It should be noted that this part of ISO/IEC 27033 is not a reference or normative document for regulatory and legislative security requirements. Although it emphasizes the importance of these influences, it cannot state them specifically, since they are dependent on the country, the type of business, etc.

Unless otherwise stated, throughout this part of ISO/IEC 27033, the guidance referenced is applicable to current and/or planned networks, but will only be referenced as “networks” or “the network”.

Information technology — Security techniques — Network security —

Part 6:
Securing wireless IP network access

1 Scope

This part of ISO/IEC 27033 describes the threats, security requirements, security control and design techniques associated with wireless networks. It provides guidelines for the selection, implementation and monitoring of the technical controls necessary to provide secure communications using wireless networks. The information in this part of ISO/IEC 27033 is intended to be used when reviewing or selecting technical security architecture/design options that involve the use of wireless network in accordance with ISO/IEC 27033-2.

Overall, ISO/IEC 27033-6 will aid considerably the comprehensive definition and implementation of security for any organization's wireless network environment. It is aimed at users and implementers who are responsible for the implementation and maintenance of the technical controls necessary to provide secure wireless networks.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27033-1 and the following apply.

3.1
access point
wireless access point
device or piece of equipment that allows wireless devices to connect to a wired network

Note 1 to entry: The connection uses a wireless local area network (WLAN) or related standard.

3.2
base station
wireless base station
equipment that provides the connection between mobile or cellular phones and the core communication network

3.3
Bluetooth
wireless technology standard for exchanging data over short distances

Note 1 to entry: "Bluetooth" is a trademark owned by the Bluetooth SIG.

3.4
core network
part of a mobile telecommunication network that connects the access network to the wider communication network

EXAMPLE The Internet and other public networks are examples of wider communication networks.

3.5
femto cell
home cell
small cell
small, low-power cellular *base station* (3.2)

Note 1 to entry: A femto cell is typically designed for use in a home or small businesses.

3.6
hardening
process of securing a system by reducing its surface of vulnerability

Note 1 to entry: Hardening typically includes the removal of unnecessary software, unnecessary usernames or logins and the disabling or removal of unnecessary services.

3.7
machine to machine
technologies that allow both wireless and wired systems to communicate with other devices of the same type

3.8
power ratio
signal-to-noise ratio
measure that compares the level of a desired signal to the level of background noise

Note 1 to entry: It is defined as the ratio of signal power to the noise power.

3.9
radio access network
part of a mobile telecommunication system that implements a radio access technology such as WCDMA or LTE to provide access for end-user devices to the *core network* (3.4)

Note 1 to entry: The radio access network resides between the end-user device and the core network.

Note 2 to entry: A mobile phone is an example of an end-user device.

3.10
radio network controller
network element in a 3G mobile network which controls the base stations, interface to the *core network* (3.4) and carries out the radio resource management and mobility management functions of the network

3.11
Wi-Fi
wireless local area networking technology that allows electronic devices to network, mainly using the 2,5 GHz and 5 GHz radio bands

Note 1 to entry: "Wi-Fi" is a trademark of the Wi-Fi Alliance.

Note 2 to entry: "Wi-Fi" is generally used as a synonym for "WLAN" since most modern WLANs are based on these standards.

3.12
Wi-Fi Ad-Hoc network
wireless ad-hoc network
decentralized wireless network which does not rely on a pre-existing infrastructure

Note 1 to entry: Examples of pre-existing infrastructure are routers in wired networks or *access points* (3.1) in managed (infrastructure) wireless networks.

4 Abbreviated terms

3G	Third Generation of mobile telecommunications technology
3GPP	Third Generation Partnership Program
4G	Fourth Generation of mobile telecommunications technology
AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
AP	Access Point
ASE	Authentication Service Entity
BYOD	Bring Your Own Device
CCM	CTR with CBC Message authentication code
CCMP	Cipher Block Chaining Message Authentication Code Protocol
CISO	Chief Information Security Officer
DMZ	De-Militarized Zone
DoS	Denial of Service
EAP	Extensible Authentication Protocol
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
GHz	gigahertz
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet message access protocol
IMEI	International Mobile Equipment Identity
IMS	Internet Protocol (IP) Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISM	Industrial, Scientific and Medical
ISP	Internet Service Provider
IT	Information Technology
LTE	Long Term Evolution
MAC	Media Access Control
MIC	Message Interface Code
NIC	Network Interface Card
OBEX	Object exchange
PDA	Personal Digital Assistant
PEAP-GTC	Protected EAP - Generic Token Card
PIN	Personal Identification Number
PKI	Public Key Infrastructure

PLMN	Public Land Mobile Network
POP	Post Office Protocol
RAN	Radio Access Network
RBAC	Role Based Access Control
RF	Radio Frequency
RFCOMM	RF Communication
SAC	Standardization Administration of China
SAE	System Architecture Evolution
SIG	Special Interest Group
SLA	Service Level Agreement
SIM	Subscriber Identity Module
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSID	Service Set Identifier
STA	STAtion
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTLS	Tunnelled Transport Layer Security
UE	User Equipment
UEA1	UMTS Encryption Algorithm #1
UHF	Ultra High Frequency
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
UWB	Ultra-Wide Band
VLAN	Virtual Local Area Network (LAN)
VPN	Virtual Private Network
WAI	WLAN Authentication Infrastructure
WAPI	WLAN Authentication and Privacy Infrastructure
WEP	Wireless Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WNIC	Wireless Network Interface Controller
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPAN	Wireless Personal Area Network
WPA-PSK	Wi-Fi Protected Access Pre-Shared Key
WPI	WLAN Privacy Infrastructure
WRAN	Wireless Regional Area Networks
WWAN	Wireless Wide Area Networks

5 Structure

The structure of this part of ISO/IEC 27033 comprises of the following:

— an overview of wireless networks and its security requirements (see Clause 6);

— security threats associated with wireless networks (see Clause 7);

— security requirements for wireless networks (see Clause 8);

— security controls for wireless network architectures (see Clause 9);

— security design techniques for wireless networks (see Clause 10).

6 Overview

More and more users of communication and processing devices are opting to use wireless interfaces to connect to their network of choice. With ubiquitous wireless networks, users see the benefit of lower costs, always-on connectivity and automatic connection setup as a driver for choosing a wireless connection over a wire line connection. Particularly for wireless networks, availability of unlicensed frequency bands, the high cost of installing a cabling infrastructure into an established or old premise, business or residential zone and the flexibility to allow additional users to connect to the network can make the choice attractive.

For example, in most countries, for Wi-Fi connectivity, one just needs to apply to a service provider for an Internet connection. It is then connected to a wireless access point or router which broadcasts the signal. Network Interface Cards (NIC) in the communications devices or computing device generally come as standard and users need only enable the interface to start the communication process with the wireless network.

For mobile/cellular networks, the challenges when deploying a network are much greater. In some countries, there may be limited spectrum available for a particular wireless technology and national spectrum regulators can take several years to plan, free-up and allocate spectrum to potential service providers. Depending on the technology (3G, 4G), the amount of spectrum required may vary. The cost of obtaining licenses can be substantial for service providers.

The following list describes the major wireless IP network categories and provides examples of selected key technologies.

— Wireless personal area networks (WPANs): small-scale wireless networks that require little or no infrastructure. These WPANs address wireless networking of portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cell phones, pagers, and consumer electronics; allowing these devices to communicate and interoperate with one another. Examples of WPAN technologies include the following.

  — Bluetooth. A wireless technology for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2,4 GHz to 2,485 GHz) from fixed and mobile devices, and building WPANs for wireless networking between small portable devices. The original Bluetooth has a maximum data rate of approximately 720 kilobits per second (kbps) and Bluetooth 2.0 can reach 3 Mbps. Bluetooth 3.0 provides theoretical data transfer speeds of up to 24 Mbps. Bluetooth implements confidentiality, authentication and key derivation based on the block cipher. Bluetooth key generation is generally based on a Bluetooth personal identification number (PIN), which should be entered into both devices.

  — Ultra-Wide Band (UWB). A radio technology used at a very low energy level for short-range, high-bandwidth communications using a large portion of the radio spectrum. It can achieve data rates of up to 480 Mbps over short ranges and can support the full range of WPAN applications such as sensor data collection, precision locating and tracking. Two UWB devices use a shared master key for authentication to establish a secure relationship. The confidentiality is protected

by encrypting the secure payload, while integrity is protected by including a message integrity code (MIC).

  - ZigBee. A technology for lightweight WPANs and designed to address the needs of low-cost, low-power wireless sensor and control networks such as climate control systems and building lighting. ZigBee provides facilities for carrying out secure communications, protecting establishment and transport of cryptographic keys, ciphering frames and controlling devices.

- Wireless local area networks (WLANs). A group of wireless networking nodes within a limited geographic area that is capable of radio communications. WLANs are typically used by devices within a fairly limited range, such as an office building or building campus, and are usually implemented as extensions to existing wired local area networks to provide enhanced user mobility. Examples of WLAN technologies include the following.

  - Wi-Fi. A trademark name and defined as any WLAN products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards. Wi-Fi relies on three security methods known as Wired Equivalent Privacy (WEP), WPA (Wi-Fi Protected Access) and WPA2. WEP and WPA have several well-documented security problems. WPA2 supports the use of pre-shared keys (PSKs) and IEEE 802.1X + EAP for authentication. The data confidentiality and integrity protocol (such as CCMP) used by WPA2 protects communications between stations (STAs) and APs. Deploying WPA2 should ensure that communications between each AP and its corresponding Authentication Services are protected sufficiently through cryptography.

  - HiperLAN. A European alternative for the IEEE 802.11 standards. HiperLAN is a technology on digital high speed wireless communication in the 5,15 GHz to 5,3 GHz and the 17,1 GHz to 17,3 GHz spectrum developed by European Telecommunications Standards Institute (ETSI) and in itself does not support any features directly related to end-to-end security. Secure data transport is obtained in layers above the MAC layer, and is in the case of HiperLAN the responsibility of the HiperLAN service requester.

  - WAPI. WLAN authentication and privacy infrastructure (WAPI) is an alternative for the IEEE 802.11 standards security mechanism developed by Standardization Administration of China (SAC). WAPI mechanism contains two parts: WLAN authentication infrastructure (WAI) protocol and WLAN privacy infrastructure (WPI) scheme. STA, AP and authentication service entity (ASE) utilize the digital certificate and five messages exchange for mutual entity authentication.

- Wireless metropolitan area networks (WMAN). Networks that can provide connectivity to users located in multiple facilities that are generally within a few miles of each other. Many WMAN implementations provide wireless broadband access to customers in metropolitan areas. Examples of WMAN technologies include the following.

  - WiMAX. A wireless communications technology designed to provide 30 megabit per second to 40 megabit per second data rates, with the 2011 update providing up to 1 Gbit/s for fixed stations and provides at-home or mobile Internet access across whole cities or countries. WiMAX supports the use of IEEE 802.1X + EAP for authentication. The data confidentiality and integrity protocol (such as CCM and AES-128) used by WiMAX protects communications between Clients and Base stations.

  - 3G. The third generation of mobile telecommunications technology. 3G telecommunication networks support services that provide an information transfer rate of at least 200 kbit/s. Later, 3G releases also provide mobile broadband access of several Mbit/s to smartphones and mobile modems in laptop computers. 3G finds application in wireless voice telephony, mobile Internet access, fixed wireless Internet access, video calls and mobile TV. 3G networks use the KASUMI block cipher instead of the older A5/1 stream cipher. However, a number of serious weaknesses in the KASUMI cipher have been identified. In addition to the 3G network infrastructure security, end-to-end security is offered when application frameworks such as IMS are accessed, although this is not strictly a 3G property.

— 4G. The fourth generation of mobile telecommunications technology succeeding 3G. A 4G system, in addition to usual voice and other services of 3G system, provides mobile ultra-broadband Internet access, for example to laptops with USB wireless modems, to smartphones, and to other mobile devices. Even though 4G is a successor technology of 3G, there can be signification issues on 3G network to upgrade to 4G as many of them were not built on forward compatibility. Conceivable applications include amended mobile web access, IP telephony, gaming services, high-definition mobile TV, video conferencing, 3D television, and cloud computing.

However, regardless of the type of technology being used there are common security challenges to be considered and addressed.

With any wireless network, the wireless transmissions may be detected by any device capable of receiving and processing these transmissions. So unlike a wired network where the signals are transmitted along the physical medium, with wireless networks, the transmitter of the signal may not be sure who is 'listening' to their broadcasts. In addition, technology is readily available to interfere with the transmitted signal and to disrupt the wireless network thus impacting the "service" of the network.

Hence, it is vital to secure the network to provide the following:

— confidentiality: that the information transmitted is not divulged in any way;

— integrity: that the information transacted is not altered along the way;

— availability: that the network service is available;

— authentication: that the identity of those users or entities seeking access to the network is confirmed;

— access control: that access to networks and network access points is controlled;

— accountability: that any violation of policy will be traceable to a specific user or entity.

With all networks, the above information security principles apply. For wireless networks, there are additional considerations as a result of the different transmission environment. For example, it is much easier to obtain and use a radio frequency (RF) jamming device than an electronic device that can interfere with cabling in a building. Most equipment types that are deployed with a wireless interface will also have an Internet interface or will carry Internet traffic which means that cyber security threats need to be considered and addressed for these elements.

To ensure compliance with these principles for wireless networks, one first has to understand the types of threats that networks are potentially exposed to. Clause 7 deals with security threats and includes some of the typical technical threats that wireless networks are potentially exposed to and which may ultimately be realised as a business threat to the security principles of confidentiality, integrity, availability, authentication, access control and accountability.

Clause 8 defines generic security requirements for the wireless networks and devices that connect to and use the network. Clause 9 establishes generic security controls to meet the needs of the security requirements in order to prevent a threat being realised.

Many different types of wireless devices are being used to conduct business in the home, outdoors, in business/organizations/enterprise environments, in public areas, in service provider deployments and in industrial deployments.

When considering the threats, requirements and controls, it is important that user behaviour, types of user devices, the amount and type of information assets that are being used and the changed threat landscape are taken into consideration. Indeed for organizations and/or enterprises and service providers, this changed user behaviour and new wireless capabilities of devices requires that the information security officer, responsible for establishing, monitoring and enforcing an unambiguous Internet Usage Policy, now has to evaluate wireless threats.

This part of ISO/IEC 27033 will focus on the threats, requirements, controls and design techniques specific to wireless networks.

7 Security threats

7.1 General

Clause 7 provides a list of typical security threats that are particular to wireless networks. However, as new wireless standards are developed, new threats will emerge and existing threats may evolve. It is recommended that service providers and wireless network administrators familiarize themselves with developments in wireless technologies in order to be in a position to adopt new security controls and techniques to counteract potential new threats.

Unauthorized access can result in the disclosure of sensitive information, data modification, denial of service and illicit use of resources. Once an unauthorized user has gained access to the network, monitoring of the now unprotected data can lead to user names and passwords being intercepted, which can then be used for further attacks. Wireless networks are susceptible to all the security threats normally faced with conventional wire line networks but additionally, they are exposed to threats directly associated with the use of wireless access technologies. The nature of most wireless medium makes it practically impossible to confine the radio signals to a controlled area. These radiated signals are subject to clandestine interception and exploitation. In a traditional wire line infrastructure, the physical security of the workplace or service provider's premises provided some protection for the network as users were obliged to physically connect to the network to access its resources. In a wireless environment, this layer of defence is no longer applicable and indeed the whole threat landscape needs to be re-evaluated and this Clause describes some of the main threats that are pertinent to wireless networks.

7.2 Unauthorized access

Wireless networks face similar unauthorized access threats as wired networks. Wireless network access may cause security threats, if available information reveals something, which will enable further investigations. For example, SSID names and settings may give hints for further use of the wireless network. Access to a wireless network is a channel to other resources in that connected network.

Preventing access to these resources is beyond the scope of this part of ISO/IEC 27033.

7.3 Packet sniffing

For Wi-Fi wireless networks that do not have encryption enabled, it is generally not difficult to eavesdrop on connections. Eavesdropping on such a Wi-Fi wireless network requires an antenna, along with the normal wireless networking tools and a network packet sniffer. A network packet sniffer is a program that places the network card in "promiscuous mode". This means that the interface will receive and process all traffic it sees and not only the traffic meant for it. A network sniffer will show the user all network packets and decode them for easy reading. All plaintext traffic is easily read and filters can be defined to look for certain keywords or values. There are several plaintext protocols and services in popular use. Some examples of these are HTTP, POP, IMAP, SMTP, FTP and ICQ. Usernames, passwords and private details in mails and messages are easily retrieved.

There are tools that are designed specifically for detecting packet sniffing attacks. These tools typically monitor network traffic or scan for network cards in promiscuous mode to detect wireless network sniffers. Examples of wireless packet sniffer tools (or packet analysers) are Wireshark and Snoop.

With Wi-Fi communications and indeed with other wireless technologies such as Bluetooth, the more sophisticated the antenna, the higher the power ratio, the easier it is to eavesdrop. While eavesdropping is a passive activity, the attack can progress to other forms such as session hijacking or man-in-the-middle attacks where messages between the user and the wireless access point are intercepted and modified with the objective of gaining unauthorized access to information or to a device, for example.

With cellular or mobile networks, early versions of these networks were susceptible to eavesdropping. However, as the network capabilities evolved and the increased use of these networks to carry confidential and sensitive, information encryption specifications have been defined for the user to access point interfaces.

For example, data encryption in the third generation Universal Mobile Telecommunications System (UMTS) systems support an encryption algorithm called f8, which uses a block cipher called KASUMI (otherwise referred as UEA1 in the 3GPP standards). However, researchers have provided evidence that the Kasumi cipher can be broken. Indeed, an attacker need not resort to cracking sophisticated encryption codes. In some cases where legacy networks exists, a multimode mobile phone may hand-off to an unsecure legacy radio access network thus making the job of eavesdropping of traffic much easier; in the 3GPP standards, this threat is defined as forced handover to legacy radio access technology.

7.4 Rogue wireless access point

Even if all Wi-Fi wireless access points are secure, it is easy for anyone to deploy a Wi-Fi access point of their own. An overly eager employee might install a wireless access point in his office with no regard to security. This will effectively circumvent many of the security measures and perhaps even cause radio interference with the official organization and/or enterprise installation. A rogue wireless access point may also be deliberately installed covertly in order to grant easy access for the perpetrator to the network either locally or remotely. A perpetrator (also known as an evil twin) could also replace an existing wireless access point with one on which he has full configuration and monitoring access or even configure a rogue wireless access point with similar setting but have a higher power ratio to overcome the legitimate wireless access point's signal. Once a legitimate user is deceived into connecting to a rogue wireless access point, confidential connection information can be gathered.

With Public Land Mobile Networks (PLMN), it is much more difficult to deploy a "rogue" radio access point or base station as generally there are physical barriers or defences in place to thwart such attempts. Most mobile network equipment is deployed in specific equipment rooms or locations where it is difficult to access and install rogue equipment.

Nevertheless, with small cell site/home/Femto cell deployments, the equipment may be deployed in business or customer premises and in such scenarios it is possible for an attacker to deploy a base station that has been compromised. The difficulty for an attacker though is that the rogue base station will need to successfully authenticate with the network. Base stations are controlled centrally by the PLMN operator and any security events, degradation in performance of the network around the rogue cell will likely be flagged to the operator. So while it may be possible to launch localized denial of service (DoS) attacks or to avail of some free mobile usage the scope of an attack via a rogue wireless access point may be limited.

7.5 Denial of service attack

The nature of a denial of service (DoS) attack is to exhaust its target's memory and/or computing capacity to significantly slow down or ideally stop the services provided. The target machine is kept so busy responding to the traffic it is receiving from its attacker that it has insufficient resources to respond to legitimate traffic on the network.

DoS is the degradation or prevention of legitimate use of network resources. The wireless network is particularly vulnerable to DoS attacks due to its features of open medium, dynamic changing topology, cooperative algorithms, decentralisation of the protocols, and the lack of a clear line of defence is a growing problem in networks today. Many of the defence techniques developed for fixed wired network are not applicable to this mobile environment.

One crude method for causing a DoS is via RF jamming where a device emits electronic signals or energy in the frequency range of the wireless networks that are in the vicinity of the attacking device. Where the attackers RF signal is sent for short bursts and/or infrequently, this is known as scrambling and can be harder for the network operator to detect.

Another form of this type of attack is mentioned in the previous threat where a rogue access point may cause a denial of service to users trying to access the network.

A more sophisticated scenario may entail an attacker sending legitimate repeated messages to a mobile device with limited power source (such as a remotely located machine to machine device) causing it to deplete it's power supply source such that its loses service earlier than intended.

Other variants of this type of attack can include fuzzing attacks which consists of sending malformed or otherwise non-standard messages or data to a device and observing how the device reacts. If a device's response is slowed or stopped by these attacks, then this could form the basis of a future DoS attack.

7.6 Bluejacking

Bluejacking is an attack conducted on Bluetooth-enabled mobile devices, such as cell phones. An attacker initiates bluejacking by sending unsolicited messages to the user of a Bluetooth-enabled device. The actual messages do not cause harm to the user's device, but they may entice the user to respond in some fashion or add the new contact to the device's address book. This message-sending attack resembles spam and phishing attacks conducted against e-mail users. Bluejacking can cause harm when a user initiates a response to a bluejacking message sent with a harmful intent.

7.7 Bluesnarfing

Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. A successful attack may result in unauthorized access to private and confidential information of these devices.

7.8 Adhoc networks

Generally, a Wi-Fi Network is created by connecting wireless devices to wireless access points/wireless routers but Wi-Fi Ad-hoc networks are created directly between two or more Wi-Fi enabled devices. Even if the devices are not directly connected, they can still communicate with each other through the common computer/other computers.

With some operating systems, ad hoc networks are enabled by default and someone in the immediate range of the transmitting computer may attempt to connect to the device and access shared documents. This is especially true when users do not encrypt the communication over an ad hoc network.

7.9 Other threats

The following are examples of other threats:

— misrouting/rerouting of messages/packets;

— IMSI catching attack;

— UE tracking;

— forced handover;

— threats of unprotected bootstrap and multicast signalling in lte;

— IPsec tunnels that provide confidentiality, but not integrity, may be put out of sync.

Others include threats to user devices and the information stored on them such as encryption keys, etc.

8 Security requirements

8.1 General

Security requirements and controls are equally applicable to both wireless and wire line networks. However, wireless networks require additional security requirements/functions to deal with specific wireless threats (detailed in Clause 7) and Clause 8 will include these additional requirements. When

evaluating how the core security requirements (as listed in 8.2 through 8.7) can be met, the threats and the threat landscape need to be taken into consideration.

8.2 Confidentiality

To mitigate the security concerns to confidentiality of data transmitted through wireless networks, encryption of user data and in some cases signalling, control and management plane data is required to ensure that data cannot be compromised in transit or eavesdropped. Depending on the wireless access technology, different encryption schemes and encryption strengths may be available. To ensure confidentiality of data, the network administrator should look to using the strongest encryption possible while at the same time considering the trade-off on performance of the network, network capacity, key management and usability.

8.3 Integrity

Integrity of data transmitted through wireless networks should be maintained by using appropriate integrity protection schemes which provides assurances that user data or indeed signalling, control or management data has not been altered or tampered with. Each wireless access technology may use different integrity protection schemes with specific encryption strengths available. The network administrator should look to using the strongest encryption possible while at the same time considering the trade-off on performance of the network, network capacity, key management, usability.

8.4 Availability

The availability of the wireless network will depend on a number of factors most of which are common to all wireless technologies. They include the following:

— the RF characteristics of the chosen technology (channel bandwidth, signal strength, frequency band, modulation, encoding, etc.);

— the environment that the network is deployed in (physical terrain, atmospheric);

— the performance of the network under load and under overload conditions;

— how the network is planned (capacity, re-use of spectrum);

— the level of redundancy designed into the network and into the constituent elements;

— the resilience of the network and its constituent elements to DoS attacks.

Network providers, service providers, organizations and/or enterprises may be bound by regulations to provide levels of service to customers. Some customers may negotiate Service Level Agreements (SLAs) with service providers which will influence some of the factors listed above.

8.5 Authentication

Authentication of the origin of the data or of identities of the communicating parties and of administrators and maintenance personnel of the networks is fundamental to the security of wireless networks. Unlike wire line networks, wireless networks transmit over a medium without physical bounds.

Each wireless access technology may use different authentication schemes for user devices attempting to connect to or access the network each with its own specific mandatory authentication protocol. In many cases, the network administrator will have no control over this protocol.

The network administrator should look to use the strongest authentication option possible while taking into account the trade-off on performance of the network, key or password management, usability, the deployment model, etc.

For example, for 3G UMTS mobile networks, the standard defines a number of encryption and integrity protection algorithms which are used between the user mobile device and the Radio Network Controller. The selection of one or other algorithm for use in the network is decided by the network operator.

The algorithms used for encryption and integrity protection are based around KASUMI and SNOW 3G.

In the context of mobile networks, it is the operator that makes the decision on how user devices authenticate to the network and indeed the network access point to the user device. So for PLMN's, the Chief Information Security Office (CISO) or IT person needs to understand the implications of this.

8.6 Authorization

Access control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications.

Each wireless access technology defines access control for end-devices and radio access points and is generally in the form of specifications for user, control and signalling data including device and element management data.

In addition, equipment vendors will also define and implement specific access control schemes for radio access points.

For Wi-Fi networks, the CISO/IT administrator controls which users can access the network. For PLMN's, it is the operator that controls which user devices, as determined by their IMEI's, are allowed access the network so an organization and/or enterprise IT administrator does not directly control this.

NOTE As 3G and 4G femto cell technology is deployed more widely, organizations and/or enterprise administrators will have more direct control over which user devices can access the radio access networks.

8.7 Accountability (Non-repudiation)

Wireless network users accountability needs to be enforced so as to ensure that any violation of policy will be traceable to a specific user.

It provides for the capability for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use). It ensures the availability of evidence that can be presented to a third party and used to prove that some kind of event or action has taken place.

For Wi-Fi networks, Access Points can be configured to log client access information and this data can be used for troubleshooting issues, monitoring the performance of the network and for trending purposes. Client access failure events, authentication failure events, client association history allows the network administrator to monitor for potential security breaches and to trace and help identify the client responsible for a particular activity.

9 Security controls

9.1 General

In a risk assessment of a network, Clause 7 wireless specific threats will augment those threats that are generic to all networks such as unauthorized access, compromise of data in storage or malware. Clause 8 listed security requirements which are defined for wireless networks but could easily be considered fundamental to all networks. So in many cases, security controls listed in Clause 9 are applicable to all types of access networks, e.g. hardening on the access point. One of the purposes of Clause 9 is to highlight the difference between applying a control to a wireless network as opposed to any access network.

For a given security risk, each security asset should be reviewed to establish whether it is relevant and impacts the asset or network and depending on the priority what are the available controls to mitigate that risk. Invariably, most risks can be mitigated by more than one control. For example, access control and authentication are applicable for protecting against malicious code. It is during the risk assessment/management phase of a project that decisions on security control selection or layers of defence are decided.

As with any communication network, the key security strategy for wireless networks is to adopt a multi-level defence.

Some of the key common controls continue to be the following:

— hardening of equipment;

— software patching of equipment;

— information management system based on the asset's risk assessment;

— operator training;

— end user awareness.

Security controls which relate the wireless networks are described below. Note that not all of the controls will be applicable to every wireless technology.

9.2 Encryption control and implementation

In Clause 8, two of the key security requirements enumerated were confidentiality and integrity of data and the primary security control for these requirements is to encrypt the data. For wireless networks, encryption of data on air-interfaces is recommended for nearly all deployments. Generally, the wireless standards define, in detail, the types of encryption for user-data, for signalling/control data and in some cases for device or equipment management data.

In Clause 10, the relevant security standards for a number of the more "commonly" deployed wireless technologies are referenced. The following are parameters the information security officer has to consider for encryption.

— What are the data encryption algorithms available? What data encryption algorithms are implemented in the equipment/network and end user devices?

— Does the end user need to be able select the type of encryption or can it be configured solely by the network administrator?

— Use of the strongest encryption is desirable but may need to be weighed up against the performance of the network interface, the performance of the end user devices and the available bandwidth of the interface.

— How the end user is informed on the level of encryption that their data is subjected, i.e. how secure is their data.

— Management of encryption keys will need to be understood. Is a public key infrastructure (PKI) being deployed? Will the wireless solution deploy a local certificate authority or interface to a public/root certificate authority? The more automated the key management process is the more user-friendly it will be.

— In some jurisdictions, local laws dictate the type of encryption that can or cannot be deployed.

— SLA's may also dictate the type of encryption that should be deployed.

— Interoperability with other (wireless) networks, e.g. if end user devices hand-off to another network does the second network support the same level of encryption as the original network?

— Backwards compatibility with different device/equipment versions. In some cases, earlier versions of a user device may not support the same level of encryption.

Wireless security standards may only define the data encryption mechanism on a per-hop basis or on an interface, e.g. the air-interface. When considering the encryption of data, the information security officer should review the end-to-end flows of data. In some cases, it may be more prudent to consider an end-to-end secure tunnel or VPN connection.

In addition to the end-to-end flow of data, the encryption of data stored in the wireless access points and end devices needs to be considered and this generally would follow best practises for storage of confidential data.

In terms of encryption, the information security officer needs to be aware of any breaches in encryption algorithms that become public. Generally, such breaches become public knowledge certainly within the ICT industry. However, it is important that vulnerability disclosure agreements with all system vendors are in place to ensure that the CISO is informed of such breaches. This is particularly relevant when the vulnerability is related to the implementation of the algorithm (as opposed to its theoretical characteristics) as it's more unlikely that these vulnerabilities will become public knowledge.

9.3 Integrity evaluation

To protect networks against session hijacking, man-in-the-middle attacks, message replay attacks wireless interfaces will use integrity checking mechanisms as a primary layer of defence against such attacks. Wireless standards generally define the integrity checking method and some may have a number of options which the information security person would need to select.

9.2 lists the considerations for data encryption and these can equally be applied to evaluate integrity.

When the information security officer is considering data integrity mechanisms, he/she will need to take into account user data and control data in transit and also for management-related data, such as software downloads or upgrades or configuration downloads.

As attacks become more sophisticated, weaknesses in the data integrity mechanisms and their implementation by a particular vendor can become exposed. The information security officer should maintain his/her vigilance and ensure that he/she is up to date with developments in the wireless security standards or with any breaches that have become public.

9.4 Authentication

To protect against the threat of unauthorized access to the network or to an access point or to data, insertion of rogue access points and man-in-the-middle attacks, wireless technology standards have defined authentication mechanisms which range from password authentication, shared or public/private key authentication to more complex combinations of schemes. The information security officer should consider not only how an end user is authenticated to the access network but also how the end user device is authenticated, how the access point or any interim gateway authenticates itself to the end user device, and how access points authenticate themselves to each other or to the core network. Generally speaking, most wireless technologies have all of these aspects defined in the relevant security standards.

The following considerations are relevant for the information officer.

— What authentication mechanisms are defined by the relevant wireless security standard for the wireless technology being used? Which interfaces are specifically identified in the standard? E.g. is it only the air-interface? What about the interface for management and control of devices and/or access points? Does the standard define mutual authentication for all interfaces?

— What authentication mechanisms are implemented in the equipment/network and end user devices? Some devices and/or access point equipment may not support the latest standard or all security options.

— What options are available to the network administrator in terms of selecting and configuring the authentication mechanism?

— Use of the strongest authentication mechanisms is desirable but it may need to be weighed up against user friendliness, manageability from a network administrator point of view, and cost of deploying the scheme.

— Management of authentication credentials will need to be understood.

— Other credential management aspects that need to be understood include: How failed authentication attempts are dealt with; how credentials are revoked and/or re-instated; how credentials expire. These aspects apply to not only to the user plane but also to control and management plane.

— Wireless technologies like 2G/3G/4G utilise SIM/UICC devices in the end user device which are provided and provisioned by the PLMN operator or can be permanently installed by the device manufacturers. The information security officer needs to understand the relationships between all of these parties. The CISO should also understand the physical security mechanisms that are employed to protect credentials on end user devices or in controllers such as tamper-proof integrated circuits, trusted environments etc.

— In some jurisdictions, local laws dictate the type of authentication mechanisms that can or cannot be deployed.

— SLA's may also dictate the type of authentication that should be deployed.

— Interoperability with other (wireless) networks, e.g. if end user devices hand-off to another network does the second network support the same type of authentication as the original network? The information security officer will generally not be able to configure or control interoperability aspects but should be aware of the capabilities of the different wireless security technologies.

— Backwards compatibility with different device/equipment versions.

9.5 Access control

9.5.1 General

The common access control mechanisms such as RBAC control, file system access controls, firewalls, intrusion detection are considered to be best practise in the designs of a network solution whether they have been integrated into an individual product or positioned as external layer of defence. This is no different for wireless systems but in addition, some specific mechanisms defined in wireless security standards are seen to augment traditional access controls.

The following considerations are relevant for the information officer.

— What access control mechanisms are defined by the relevant wireless security standard for the chosen wireless technology?

— Which access control mechanisms are implemented in the equipment/network and end user devices? Some devices and/or access point equipment may not support the latest standard or all security options.

— What options are available to the network administrator in terms of selecting and configuring the access control mechanism?

— In some jurisdictions, local laws dictate the type of access control mechanisms that can or cannot be deployed.

— Interoperability with other (wireless) networks.

— In general, the information security officer will not be able to configure or control interoperability aspects but should be aware of the capabilities of the different wireless security technologies.

— Backwards compatibility with different device/equipment versions.

— In order to detect and/or prevent unauthorized access to a wireless network, as well as the subsequent impact of such security breach, a wireless intrusion detection/prevention system should be considered.

9.5.2 Permission control

For example, in 802.11 systems, MAC Address filtering is implemented to ensure that only permitted wireless network clients are allowed to connect to the wireless network. Note that this security feature on its own may not be an effective control as an attacker may spoof a legitimate wireless network client. However, it is an example of a layer of defence that a system can employ.

In mobile network standards, the user equipment identifier is seen being used as a mechanism to allow or disallow access to a network. So if user's IMEI (International Mobile Equipment Identity) is blacklisted by the operator, they cannot access the network.

9.5.3 Network-based control

With many wireless technologies, an examination of the standards shows that user data and control protocols are defined and in many cases implemented separately. In defining and implementing the standard in such a manner, logical separation is achieved which in itself provides a level of access control.

With 4G LTE standards, it is recommended that control plane traffic is secured using IPsec-based protocols when traversing a network boundary from one security domain to another (i.e. over an insecure network). This network configuration is also an option for user data if operators wish to do so.

9.6 Denial of service attack resilience

Typical mechanisms for the prevention or ability to handle Denial Of Service attacks range from using secure source coding techniques, source code analysis testing, vulnerability testing to using an network or host-based IDS/IPS systems to detect abnormal behaviour in IP or application traffic. These techniques apply to all ICT networks.

RF jamming is unique to wireless networks whether the RF jamming signal emanates from an attacker or from an accidental source. The CISO needs to ensure that the network has deployed monitoring equipment to ensure that the event is detected and information related to it is logged.

Specific wireless protocol DoS attacks can be detected by anomaly detection systems. The CISO needs to be aware of what is deployed in their network, what the capabilities of the monitoring equipment is and as usual be aware of new or evolved threats in this domain.

9.7 DMZ segregation via firewall protection

As wireless networks can be attacked over an air-interface, it is recommended that any wireless network connected to a secure internal network should be connected via a de-militarized zone (DMZ) network.

This wireless DMZ network should be segregated from the secured network via a firewall which will proactively limit certain traffic from the wireless network to access the secured network.

An example of where this control may be applied is for a wireless guest network as part of an overall organization and/or enterprise network

9.8 Vulnerability management though secure configurations and hardening of devices

A vulnerability management program is recommended to be established. Periodic assessments of applications and infrastructure for vulnerabilities can be performed by wireless vulnerability scanning

tools. The detected vulnerabilities can be fixed by patching applications, OS and devices or by using secure configurations and hardening devices.

9.9 Continuous monitoring of wireless networks

The wireless network should be integrated with the enterprise security monitoring system. Security incident and event management tools and enterprise threat detection tools can be used to provide frequent or continuous monitoring to detect attacks and data leaks.

10 Security design techniques and considerations

10.1 General

Clause 10 provides high level guidance when designing and deploying wireless networks. It deliberately does not define or describe in detail wireless security protocols or interfaces as these are well defined in the appropriate wireless technologies standards. One of the most common wireless standards is the IEEE 802.11 family of standards. 10.2 will provide some details on aspects of 802.11. In 10.2 other standards will be addressed. The list of wireless technologies covered in this part of ISO/IEC 27033 is not exhaustive as no sooner than the document is published that new standards or variants of standards would quickly surpass and potentially replace the standards relevant to the technologies listed here.

During planning, some basic checks can be used to ensure that the CISO, IT system or network architect can review and securely deploy new technologies.

— Performing a risk assessment on the use of new wireless technologies.

— As part of the development of wireless standard and in particular the security section, the standards development organization generally completes a threat analysis describing the threats applicable to the technology and countermeasures to mitigate any exposures. Mitigations or countermeasures will either be listed as recommended or will be integrated into the standard specification itself.

  For example, 3GPP TR 33.821 (Rationale and track of security decisions in Long Term Evolution (LTE) RAN/3GPP System Architecture Evolution (SAE)[5] includes a threat analysis with specific wireless threats and countermeasures, whose output serves as input to other 3GPP Security technical requirements documents.

— The CISO or IT security specialist should be aware of the specific threats relevant to the proposed wireless technology.

— Ensure that the organization has a wireless security policy which specifically addresses the following:

  — the wireless network user authentication;

  — access control for both employees and guest or non-employees to the wireless network;

  — employees accessing other wireless networks outside of the control of the employees organization;

  — who has the authority to allow access points connect to the organizations network.

A wireless security policy may also address the security aspects around BYOD even though security domains for BYOD are not exclusive to wireless technology. A wireless security policy should encompass all wireless technologies that are deployed in the enterprise or organization network.

10.2 Wi-Fi

10.2.1 General

Wi-Fi is defined as any wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards.

This subclause provides guidance on techniques and considerations around Wi-Fi networks and equipment.

A Wi-Fi network is a group of two or more wireless networking devices within a limited geographic area that exchange data through radio communications. The fundamental components of IEEE 802.11 Wi-Fi network are client devices such as laptops, tablets and smart-phones, and access points (AP's), which logically connect the client devices with a distribution system, typically an organization's wired network infrastructure. Some Wi-Fi also use wireless switches, which act as relays between the APs and the distribution system.

The IEEE 802.11 family of standards consists of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. The original standard IEEE 802.11-1997 (legacy) has been superseded by nearly a dozen different amendments, which introduce service amendments and extensions or corrections to the previous specifications, supports different transmission frequency and indeed different security mechanisms.

The security of a Wi-Fi network is heavily dependent on how well each Wi-Fi component (including client devices, APs, and wireless switches) is secured from initial Wi-Fi network design and deployment through ongoing maintenance and monitoring. Unfortunately, Wi-Fi networks are typically less secure than their wired counterparts for several reasons, including the ease of access to the wireless network and the weak security configurations often used for Wi-Fi networks, which tend to favour convenience over security.

Security mechanisms for Wi-Fi are defined in the IEEE 802.11 standards and includes functions covering authentication of client devices to the AP, the AP to the device, user data encryption and user data integrity protection. Note that not all security functions are available in each of the IEEE 802.11 standards.

For enterprises, the organization IT security department is responsible for controlling how security is configured on its infrastructure.

For employees operating in other networks, public hotspots, etc., these users should be advised to use alternative secure mechanisms, e.g. use VPNs when communicating sensitive or confidential information.

10.2.2 User authentication

All users attempting to gain access to a wireless network under the control and management of an organization should authenticate before access is granted to the network or to guest Wi-Fi access points.

Employee access to the network should be accomplished using two-factor authentication (e.g. SecurID or Safeword Token and PIN).

The following should be taken into account in order to authorize guest access to the Internet.

— All wireless network guest registrations should be sponsored by a responsible person within the organization.

— Guest IDs should be unique to maintain accountability. However, IDs and passwords may be shared when it is impractical to assign individual IDs and passwords (e.g. a large customer meeting).

— Password expiration should reflect the business need (up to a week).

— The guest should be provided a “notification of terms” which describes the terms and conditions for access.

10.2.3 Confidentiality and integrity

Data should be encrypted during transmission to/from the organization network. To encrypt data transmissions, the following mechanism should be used:

— Wi-Fi Protected Access 2 (WPA2™) with Advanced Encryption Standard (AES) encryption (128 bit key strength or higher);

— VPN tunnelling with 3DES or AES encryption.

WPA2 also implements a message integrity code, MIC. The message integrity check prevents forged packets from being accepted.

10.2.4 Wireless Wi-Fi technologies

All wireless access equipment connected to an organization network should use IT Security equipment and security configurations that have been approved by the organization’s IT security department.

Approved technologies include the following.

— Access Points - Any 802.11a/b/g/n compliant Access Point that supports WPA2 using Extensible Authentication Protocol (EAP).

— Protected EAP-Generic Token Card (PEAP-GTC) authentication and the AES algorithm, or EAP - Tunnelled Transport Layer Security (TTLS) authentication and the AES algorithm.

— Wireless Access Points should use the IEEE 802.1x/PEAP-GTC or EAP-TTLS authentication frameworks to validate these users via back-end RADIUS/AAA servers.

— Client Devices - any 802.11a/b/g/n compliant wireless Network Interface Card which supports a minimum of WPA2 (AES) encryption.

Wired Equivalent Privacy (WEP) nor WPA should be used as an encryption algorithm due to publicly identified security weaknesses.

10.2.5 Other Wi-Fi Configurations

There may be applications which rely upon wireless configurations that cannot meet the security requirements in this subclause (e.g. warehouse inventory scanners which use AAA authentication).

Therefore, a security risk assessment should be performed to identify complementary controls, such as

— WPA-PSK, with regularly-changed maximum length/security passwords,

— dedicated SSIDs,

— limited radio transmission range,

— limited access to the network, either through TCP firewalls or isolated VLANs, or

— availability of monitoring logs.

10.2.6 Access control — User equipment

In general, access control mechanisms for wireless networks should be the same as for wired/wire line networks.

The wireless security policy may specifically state that guest users should not have access to the organizations intranet via the wireless network.

Some wireless security policies may specify that employees of the organization should not use Wi-Fi to bridge the organization network perimeter (e.g. use Wi-Fi to establish a simultaneous connection to the organizations LAN and an external network not under the control of the organization.) Therefore, employees should not enable IP Forwarding, establish Wireless Peer-to-Peer connections, use ad hoc mode, or establish other forms of routing.

Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS) can provide an effective layer of defense to combat threats such as rogue access points and denial of service attacks.

WIDS/WIPS include sensors that scan the RF spectrum and relays findings back to a management server which can then take action based on analysis of information captured by sensors. Typically, WIDS/WIPS will also include a database server that acts as an information repository.

10.2.7 Access control — Infrastructure access point

Access points should adhere to the following configuration guidelines.

— Change default management passwords for Access Point administration using strong passwords (a non-dictionary word, no less than fifteen (15) alpha-numeric characters long, with at least one numeric or special character).

— Use an AAA network device infrastructure to authenticate Access Point administrators.

— Disable remote Wireless LAN administration and allow only administration over the Ethernet, USB, or Serial interfaces.

— Use transmission encryption for all remote administration (e.g. use https/SSH and disable http/telnet).

— Change all default Simple Network Management Protocol (SNMP) community strings too hard to guess passwords.

— If possible, use SNMPv3 for network management functions on all Access Points.

— When installing Access Points, complete a site survey to measure and establish the Access Point coverage to ensure the broadcast footprint is under appropriate physical control (for example, avoid broadcasting to unintended areas such as parking lots). Limit the router's signal range to a specified area to restrict access for unauthorized users.

— Physically secure all Access Points in an adequate manner to deter theft or tampering.

— Change the SSID (service set identifier) from the default to a consistent network name and allow the Access Points to broadcast their SSIDs.

— According to the nature of the AP, it is easy to establish a wireless network with the same SSID and use highly sensitive directional antennas to cover the wireless signal from the original AP. Each AP specified in a wireless network, under the control and management of an organization, should authenticate the wireless devices when they want to access the network.

— Segregate the wireless network from the organizations intranet and from the Internet.

— Update routers and access points with the latest firmware version in order to increase reliability and security

— Restrict guest access ideally by providing a separate guest network.

In deploying access points, there may be multiple privileged administrative accounts which are used to manage the Access points (there may be one or more privileged accounts per access point) and this presents the problem of how to manage these privileged administrative accounts.

Organizations or enterprises should ensure there is a mechanism to manage these multiple privileged accounts.

Organizations should consider conducting independent third party security audits. A third party that specializes in wireless security audits may be more up-to-date on security vulnerabilities and better equipped to assess the security of a wireless network system.

10.2.8 Availability

In general, availability techniques for wireless networks (such as redundant routers, power supplies, etc.) should be the same as for wired/wire line networks. In case of Wi-Fi, the availability of access points and their cryptographic algorithms are indicated to client computers.

Some additional measures or checks that can be taken for Wi-Fi networks include the following:

— regular auditing of the security configurations of the Wi-Fi network components such as the client device and the access points to ensure that they comply with a minimum level of security or with the organizations standard security configuration;

— monitoring of the Wi-Fi network using wireless intrusion detection and protection systems placed at various points in the organizations facility which can detect anomalies in traffic patterns on the wireless network.

Both of these measures are designed to detect changes in the characteristics of the Wi-Fi network or of the client devices, which could be a prelude an attack. Such a weakness may be exploited which in turn could reduce the availability of the network.

10.2.9 Accountability

When allowed by law or regulation, centralized logging on the access points should be enabled to record user and event activity, such as

— timestamps,

— MAC address,

— user names,

— success or failure of event,

— type of event, for example login attempt,

— reboots,

— configuration changes,

— associations/de-associations, which might indicate denial of service attempts, and

— identification of rogue access points.

The wireless network should be periodically scanned for unauthorized access points in the organizations managed facilities to understand the wireless network security posture.

10.3 Mobile communication security design

Mobile communications systems (also known as mobile cellular systems) generally comprise of base stations, radio network controllers, and interfaces or gateways into an operators core network. The base stations support one or more cells which mapped together may cover large physical areas. Originally developed primarily for voice calls, they supported large numbers of telephony users, hand-off from cell to cell as user devices moved around, and roaming to/from other operator networks. Mobile communications systems such as LTE can provide mobile high speed Internet access, for example, to laptops, smart phones, and other mobile devices.

Security for mobile communication systems includes standards for user equipment (user device) mutual authentication to the network, integrity protection and confidentiality mechanisms, access control to the network. As integration of Wi-Fi and mobile communication systems evolves, the security threats that are specific to such integration are also being addressed in International Standard.

If employees (of an enterprise or organization) are using cellular mobile communication devices, these are generally controlled and maintained by the service provider and thus the "user" may not have control over the security options such as data encryption and authentication of device/access point.

Transmissions on the Radio Access Network (RAN) can be encrypted but there's no guarantee that the End-to-End link is secure.

Because the RAN is controlled by the operator and encryption of communications may not be guaranteed, end-to-end so end-users should be advised to use alternative secure mechanisms, e.g. use VPNs when communicating sensitive or confidential information.

10.4 Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength microwave transmissions in the RF band from 2 400 MHz to 2 480 MHz) from fixed and mobile devices and building personal area networks (PANs).

Bluetooth is managed by the Bluetooth Special Interest Group (SIG) which oversees the development of the specification and manages the qualification program. All versions of the Bluetooth standards are designed for backwards compatibility. Later versions of the standard provide for enhancements to the Bluetooth capabilities, higher data transfer rates, faster connection, discovery of devices, secure pairing of devices, low energy device support and secure encrypted connections.

The security of a Bluetooth point to point link and indeed a Bluetooth PAN is determined to a large extent by the version of Bluetooth standard supported or being used on the device. Vulnerabilities against each of the standards have been published and details can be found in well-known references. Refer to Bibliography for details.

Due to the inherent security weaknesses in Bluetooth protocols, the capability to transfer confidential or sensitive data on Bluetooth devices (under the control of the organization) should be disabled.

Bluetooth exhibits most of the same vulnerabilities inherent to wireless systems in general. A Bluetooth transmitter sends signals across free space to any receiver, legitimate or not, located within range. Additionally, Bluetooth operates in the 2,4 GHz unlicensed band, and there are no restrictions on the sale of devices that transmit and receive in this band. Consequently, an unauthorized monitoring device that is not in direct contact with a Bluetooth transmitter can intercept its transmissions. Such a monitoring device is easy to conceal, undetectable when in use, and can be deployed much more rapidly than a wiretap.

Many attacks against implementation errors or security deficiencies in Bluetooth are documented in public literature. Some examples are as follows.

a) Bluedumping: the aforementioned attack based on reverse calculating the user PIN based on intercepted pairing exchanges.

b) Bluesnarfing: allows an attacker to access phone directory and appointment database on target devices due to implementation errors in the OBEX Push protocol.

c) Bluebugging: utilizes hidden Bluetooth RFCOMM channels and allows an attacker to remotely control most aspects of a phone device, including making unauthorized calls and turning on microphones to turn a phone into an eavesdropping device (bug).

d) Bluejacking: lack of security on OBEX profile on some devices allows an attacker the ability to add arbitrary entries onto the target device's phone list.

e) Bluestabbing: attacker modifies a Bluetooth device with a badly formatted device name which causes target device to crash when it tries to discover other devices in its vicinity.

f) Bluebumping: social-engineering attack which exploits the fact that a paired bond does not really disappear until both devices in a pair delete the connection; the attacker will use social-engineering to convince the target to pair with a device, after which the target will delete the pairing from his/her device afterwards, but the attacker will not, thereby allowing the attacker a hidden "back door" into the target's device.

g) Bluesmacking: badly formatted inquiry strings result in a "ping of death", crashing any devices that the message is sent to.

Users should follow the following best practice security guidelines.

— Enable Bluetooth functionality only when necessary.

— Use the strongest Bluetooth security mode.

— Keep paired devices as close together as possible when the Bluetooth links are active.

— Make devices discoverable only when absolutely necessary.

— Avoid the use of weak fixed passkeys (the manufacturer default is typically "0000").

— Configure the Bluetooth device and software according to established policies.

— PIN needs to be protected from interception or cracking by an attacker.

— The device identifying data and keys should be protected.

— Employ application layer security and a public key infrastructure to provide additional security measures.

— Establish device configuration guidelines, security policies, enforcement mechanisms for the use of Bluetooth devices in the environment.

10.5 Other wireless technologies

There will always be new wireless technologies introduced or variants of existing technologies. Some will have security mechanisms defined for them. It always recommended that a risk assessment be carried out on the information that maybe be transferred over the technology and how the radio technology interfaces with the rest of the organization's IT infrastructure. It is advantageous if an International Standard exists which includes a description or definition of the security mechanisms supported by the technology, a threat analysis of the technology and recommendations on how the technology can be deployed and incorporated securely into an IT infrastructure. If it's not clear that the technology can offer secure mechanisms, then an organization should make a decision on whether it should be used and if it is what additional security procedures should be put in place to ensure security.

In many organizations, multiple wireless technologies are supported and user devices may be connected to multiple wireless networks simultaneously, such as cell phone, Bluetooth and Wi-Fi networks and in some cases, the user device may be connected to the wired/wireline network also. So if an attacker gains unauthorized wireless access to a multi-connected client device, the attacker could then use it to access or attack resources on the wired network. Organizations should assess the risk posed by the use of combinations of wireless technologies and determine how those risks should be mitigated. If one or more of the networks cannot have its risk mitigated to an acceptable level, then dual connections involving that network may pose too much risk to the organization and may need to be prohibited.

Annex A
(informative)

Technical description of threats and countermeasures

A.1 Man in the middle attacks

With man-in-the-middle attacks, the perpetrator positions himself between the victim and his communications partner without either of them knowing it. All traffic flows through the perpetrator so that he is able to monitor it.

A wireless man-in-the-middle attacker appears as the access point to the client and the client to the real access point. The client sees what appears to be the correct access point and associates to it. This fake access point steals the clients MAC address and associates with the real access point. All traffic will now flow through the man-in-the-middle machine.

Most security professionals are aware of the man-in-the-middle attack. This type of attack has somewhat faded due to physical security and the complexity of the current switched networks that usually reside between the two end points. However, this type of attack is seeing a revival in popularity with new tools that make it easier to exploit this vulnerability becoming available.

A.2 Session hijacking

Session hijacking is when a third party "takes over" one's session. The object of session hijacking is not to hijack the wireless connection but Web application session being carried over the wireless connection. Sniffing a session in order to prepare for hijacking the session of a Web application may be performed by a "man-in-the-middle".

A classic technique to sniff the session ID was using IP source routing. In current wireless environment, sniffing became possible by just monitoring the wireless communications.

There are various ways to accomplish this. Wi-Fi networks can be vulnerable to this because there are no physical connections to alter. This technique can be used to either take over a specific communications session or to gain access to the Wi-Fi network by stealing the identity of the victim. This technique can be used in situations where the network access is protected by a web portal.

Most portals require the user to authenticate by using a username/password or similar scheme and are based on MAC access lists. When authentication is successfully completed, the portal adds the clients MAC address to the access list for a specified duration. A session hijacking of this security setup would be to monitor the victim and wait for him to complete his authentication. Then the attacker (pretending to be the access point) sends the victim an 802.11 MAC disassociate message. The victim is kept disassociated with a DoS attack of such messages while the hijacker assumes the victim's identity by changing his MAC address to match the victim's. This would work until the next time the portal requires authentication.

A much easier approach is to wait for the victim to leave the wireless network and immediately assume his identity before the portal registers the victim as idle and de-authenticates him. A combination of a sniffer, ping and MAC change will accomplish this. On most portals, this time-out is set to several minutes.

Countermeasures to the threats include

— choosing a suitable technology which includes a cryptographic algorithm and key exchange mechanism for the wireless connection protocol such as the ones listed in Clause 10, and

— requiring Web applications to use encrypted communication technology (e.g. TLS), to avoid monitoring of session IDs.

A.3 Wardriving

Wardriving is the act of searching for Wi-Fi wireless networks by somebody using equipment or a device with Wi-Fi detecting capabilities. Historically, the term was associated with hackers, who would cruise around in their cars looking for open wireless networks, identified by their Service Set Identification (SSID). SSID is not a security measure. It is not a "password" the users must know to be able to connect to the wireless network. Any client that configures his SSID to "Any" will discover and connect to the nearest available and open access point, regardless of the SSID used. This is because the access points broadcasts the SSID as part of the answer to clients calling for a "Broadcast Request".

Thus, it is not difficult to map out all open wireless networks within a defined area. In fact, if the owner of these open wireless networks named their wireless network access points after their company (department), a virtual map of all wireless network resources in this defined area can be obtained, as well as who they belong to.

There are many open source, free, and easy-to-use tools which can be downloaded to portable devices that are capable of mapping wireless access points. Using such tools for discovering wireless access points is called "Wardriving" An effect of Wardriving is "Warchalking", marking wireless network discovery with a symbol for others to find. Variations of this threat include Warwalking and Warflying but they all exploit the same basic vulnerability of Wi-Fi wireless networks.

Bibliography

[1] NIST Special Publication 800-153 — Guidelines for securing Wireless Local Area Networks (WLANS), February 2012.

[2] NIST Special Publication 800-121 — Guide to Bluetooth Security, June 2012.

[3] IT Security — Technical Publication — 802.11 Wireless LAN Vulnerability Assessment (ITSPSR-21A), Communications Security Establishment Canada (CSEC), May 2009.

[4] IEEE 802.11, *IEEE Standard for Information technology — Telecommunications and information exchange between systems*

[5] 3GPP TS 33.821 — Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE) (http://www.3gpp.org/DynaReport/33821.htm)

[6] NIST Special Publication 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007.

[7] IEEE 802.15[1)]*Working Group for WPAN*

[8] IEEE 802.11[2)]*WIRELESS LOCAL AREA NETWORKS*

[9] The IEEE 802.16 Working Group on Broadband Wireless Access Standards (http://ieee802.org/16/)

[10] IEEE 802.22[3)]*Working Group on Wireless Regional Area Networks*

[11] ZigBee Alliance. https://www.zigbee.org/

[12] Wi-Fi Alliance. http://www.wi-fi.org/

[13] Alliance W.A.P.I. http://www.wapia.org/

[14] Bluetooth technology (https://www.bluetooth.com/)

[15] WiMAX Forum. http://www.wimaxforum.org/

[16]. NIST Special Publication 800-48 — Guide to Securing Legacy IEEE 802.11. Wirel. Netw. 2008 July

1) http://www.ieee802.org/15/

2) http://ieee802.org/11/

3) http://ieee802.org/22/

ICS 35.040
Price based on 26 pages