INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA (IIUM)

Document No :
IIUM/ITD/ICTPOL/4.3

Effective Date :
13/11/2008

Standard For IIUM Wireless Networking

Chapter : Network

Status : APPROVED

Version No : 01
Revision No : 00

1.0 OBJECTIVE

The objective of this document is to define the standards for IIUM wireless networking.

2.0 GOVERNING POLICY

2.1 (IIUM/ITD/ICTPOL/4.1) Policy for Network Services
2.2 (IIUM/ITD/ICTPOL/4.2) Policy for Wireless Networking
2.3 (IIUM/ITD/ICTPOL/9.1) Policy for Service desk and Incident Management

3.0 STANDARD

The standards are as follows:

3.1 Approved equipment

3.1.1 All wireless network devices shall use University-approved vendor products and security configurations.

3.2 Monitoring of uncontrolled wireless devices

3.2.1 All locations where permanent data networks are installed shall be equipped with sensors and systems to automatically detect, classify, and disrupt communication with unapproved wireless access points.

3.2.2 All locations where permanent data networks are installed shall be equipped with sensors and systems to automatically detect the presence of wireless devices forming a connection between the network and any wireless network. This would include laptops that are serving as a bridge between wired and wireless networks.

3.2.3 In locations where wireless LAN access has been deployed, wireless intrusion detection systems and network access control shall be deployed to monitor attacks and backdoor intrusion against the wireless network. The wireless intrusion detection system shall be integrated with the wireless LAN access system whenever possible.

3.2.4 All installed access point shall use the world wide non-overlapping channel to avoid radio interference.

3.2.5 All wireless Local Area Network shall be configured to drop all unauthenticated and unencrypted traffic. Wireless implementations shall maintain point to point hardware encryption compliant to current standards. All implementations shall support a hardware address that can be registered and tracked. All implementations shall support and employ strong user authentication which checks against an external database.

3.2.6 The SSID shall not broadcast the name to reduce possible unauthorized connections.

3.3 Authentication of wireless clients

3.3.1 All access to wireless networks shall be authenticated.

3.3.2 The University's existing strong password policy shall be followed for access to wireless networks.

3.3.3 Authentication method shall consist of three combinations which are username, password and MAC address

3.3.4 The strongest form of wireless authentication permitted by the client device shall be used. For the majority of devices and operating systems, WPA or WPA2 with 802.1x/EAP-PEAP shall be used. WPA2 is preferred wherever possible.

3.3.5 Where 802.1 x authentications are used, mutual authentication shall be performed. Client devices shall validate that digital certificates presented by the authentication server are trusted and valid. Under no circumstances, clients shall disable validation of server certificates and blindly trust any certificate presented. EAP methods that do not support certificate-based mutual authentication shall not be used.

3.3.6 EAP methods that exchange authentication credentials outside of encrypted tunnels shall not be used. These methods include EAP-MD5 and LEAP.

3.3.7 Legacy devices that do not support WPA or WPA2 are used on a wireless network, they shall be isolated from all other wireless devices and shall be restricted to the minimum required network access. Violations of the configured rules, indicating that an intrusion has taken place, shall cause the device to be immediately disconnected and blocked from the network.

3.3.8 Any user with an account in a user database shall be able to authenticate at any University location where wireless access is present.

3.4 Encryption

3.4.1 All wireless communication between devices and networks shall be encrypted. Wireless networks providing only Internet access for guest users are exempted from this requirement.

3.4.2 The strongest form of wireless encryption permitted by the client device shall be used. For the majority of devices and operating systems, WPA using TKIP encryption or WPA2 using AES-CCM encryption shall be used. WPA2 with AES-CCM is preferred wherever possible.

3.4.3 Client devices that do not support WPA or WPA2 shall be secured using VPN technology such as IPSEC where allowed by the client device.

3.4.4 The use of WEP requires a waiver from Information Security. Client devices that require the use of WEP shall be isolated from all other wireless devices and shall be restricted to the minimum required network access. Violations of the configured rules, indicating that an intrusion has taken place, shall cause the device to be immediately disconnected and blocked from the network.

3.5 Access Control Policies

3.5.1 Access to corporate network resources through wireless networks shall be restricted based on the business role of the user. Unnecessary protocols shall be blocked, as shall access to portions of the network with which the user has no need to communicate.

3.5.2 Access control enforcement shall be based on the user's authenticated identity, rather than a generic IP address block. This is also known as "identity-based security."

3.5.3 The access control system shall be implemented in such a way that a malicious inside user is unable to bypass or circumvent access control rules.

3.5.4 Access control rules shall use stateful packet inspection as the underlying technology.

3.6 Remote Wireless Access

3.6.1 Employees working from remote locations shall be provided with the same wireless standards supported in branch campus.

3.6.2 Employees shall be discouraged from connecting University computers though consumer type wireless equipment while at home in lieu of University-provided equipment.

3.7 Client Radio Standards

3.7.1 The highest bandwidth of wireless radio transmitted by the client device shall be used. Wireless radio standard of 801.11a and 802.11g is preferred wherever possible.

3.7.2 The use of 802.11b standard downgraded the radio communication to all users connected to a particular access point. Employee shall be discouraged to use 802.11b as a radio standard.

*note: 802.11b with 11Mbps shall be restricted. It will interrupt the whole performance of 802.11g (54 Mbps). When AP communicates with the users, AP will open its communication level equivalent to users. For example: 5 users currently communicate with AP via 802.11g with 54 Mbps. Then, a user connects with a 802.11b client. AP can not communicate via 2 communications simultaneously. The AP will turn down the access in order to serve the 802.11b. The AP will then open its 802.11b. Other users will communicate to the AP via 802.11b. When the 802.11b client turns off its computer, they will communicate again via 802.11g.

3.8 Client Security Standards

3.8.1 Where supported by the client operating system, the wireless network shall perform checks for minimum client security standards (client integrity checking) before granting access to the University network. Specifically:

3.8.2 All wireless clients shall run on University approved anti-virus software that has been updated and maintained in accordance with the University's anti-virus software policy.

3.8.3 All wireless clients shall run host-based firewall software in accordance with the University's host security policy.

3.8.4 All wireless clients shall have security-related operating system patches applied that have been deemed "critical" in accordance with the University's host security policy.

3.8.5 Clients not conforming to minimum security standards shall be placed into quarantine condition and automatically remediate.

3.8.6 Client operating systems that do not support client integrity checking shall be given restricted access to the network according to business requirements.

3.9 Wireless Guest Access

3.9.1 Wireless guest access shall be available at all facilities where wireless access has been deployed.

3.9.2 All wireless guest access shall be authenticated through a web-based authentication system.

3.9.3 A single username/password combination shall be assigned for all guest access. The password for guest access shall be changed monthly and distributed to local facility managers.

3.9.4 Wireless guest access is available from the hours of 7:00 until 20:00 local time.

3.9.5 Wireless guest access bandwidth is limited to 2Mbps per user.

3.9.6 Guest access shall be restricted to the following network protocols:

a. HTTP (TCP port 80)
b. HTTPS (TCP port 443)
c. POP3 (TCP port 110)
d. IKE (UDP port 500)
e. IPSEC ESP (IP protocol 50)
f. PPTP (TCP port 1723)
g. GRE (IP protocol 47)
h. DHCP (UDP ports 67-68)
i. DNS (UDP port 53)
j. ICMP (IP protocol 1)

4.0 RESPONSIBLITY FOR IMPLEMENTATION

The responsibility for the implementation of this policy lies with the Network Engineer and Head of Department (Network and Telecommunication Department), ITD.

5.0 ENTITIES AFFECTED BY THIS POLICY

Staff members and students of the University are affected by this policy.

6.0 DEFINITION

Term	Definition
802.11	A set of Wireless LAN/WLAN standards developed by the IEEE LAN/MAN standards committee (IEEE 802). Also commonly referred to as "Wi-Fi."
802.11i	An amendment to the IEEE 802.11 standard specifying security mechanisms for wireless networks.
802.1x	A framework for link-layer authentication specified by the IEEE.
AES-CCM	Advanced Encryption Standard-Counter with CBC-MAC. A wireless encryption protocol specified by IEEE 802.11i. Currently regarded as the strongest form of wireless encryption.
EAP	Extensible Authentication Protocol. A series of authentication methods used inside 802.1x to achieve wireless authentication.
IETF	Internet Engineering Task Force. Develops and promotes Internet standards, in particular those of the TCP/IP protocol suite.
IPSEC	IP Security. An IETF standard for protecting IP communication by encrypting or authenticating all packets.
LEAP	Lightweight Extensible Authentication Protocol. A proprietary protocol supported by Cisco Systems that acts as an EAP method within 802.1x. LEAP was proven insecure in 2003 and does not comply with current security standards.
PEAP	Protected Extensible Authentication Protocol. A tunnelled EAP method that uses a server-side digital certificate for server authentication and a username/password for client authentication.
Stateful Packet Inpection	A filtering or firewall technology that keeps track of the state of network connections, such as TCP streams, travelling across it. Only packets which match a known connection state shall be allowed, while others are rejected.
VPN	Virtual Private Network. A method of building private networks on top of public networks such that the private network is protected and separate.
WEP	Wired Equivalent Privacy. This is the encryption protocol specified in the original version of IEEE 802.11. It is now deprecated and does not meet current security standards.
Wi-Fi	A set of product compatibility standards for wireless LANs based on IEEE 802.11. The Wi-Fi term is managed by the Wi-Fi Alliance. Products carrying Wi-Fi certification have passed a series of compatibility tests.
WLAN	A type of wireless system based on the IEEE 802.11 series of protocols.
WPA	Wi-Fi Protected Access. WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work

	with all wireless network interface cards. Products displaying the WPA logo have passed a certification program run by the Wi-Fi Alliance.
WPA2	Wi-Fi Protected Access version 2. WPA2 implements the full IEEE 802.11i standard, but shall not work with some older network cards. Products displaying the WPA2 logo have passed a certification program run by the Wi-Fi Alliance.

7.0 REVISION HISTORY

Requestor	Description	Submission Date	Approval Date
Shukri Abd Rahman, ITD	Initial Draft	26/09/2008	_
Shukri Abd Rahman, ITD	Reviewed by ICT Policy Review Committee No. 3/2008	13/11/2008	_
Shukri Abd Rahman, ITD	Approved by ICT Policy Review Committee No. 3/2008	_	13/11/2008