


CITY OF BREMERTON		WIRELESS SECURITY	
INDEX Information Management 2-20-18	EFFECTIVE DATE: February 1, 2008	 APPROVED <hr/> CARY BOZEMAN, Mayor	

1.0 INTRODUCTION

The purpose of this policy is to provide guidance for the secure operation and implementation of wireless local area networks (WLANs) and Internet-enabled handheld devices throughout the City of Bremerton (City) environment. Ensuring sufficient security is a vital concern when designing, deploying, and managing wireless networks and devices. When introducing wireless technologies into the City environment, special care and consideration must be exercised since they introduce both comparable vulnerabilities as in the wired world as well as unique vulnerabilities due to their electromagnetic and portable characteristics.

This policy provides consistent and up-to-date guidance for implementing secure WLANs and Internet-enabled handheld devices in the City environment, and establishes a comprehensive wireless network security policy that sets the foundation and direction for sound implementation and usage of WLANs and their devices. Since wireless technologies are continuously evolving, it is essential to remain abreast of the current and emerging trends in the technologies and in the security or vulnerabilities of these technologies. This policy is intended to achieve the confidentiality, integrity, availability, and accountability requirements of the City Enterprise data network (wired network) and addresses the minimum requirements for mitigating the risks associated with wireless network device deployment.

1.1 Scope

The purpose of this document is to provide the City with guidance for implementing secure wireless networks and the use of Internet-enabled handheld devices, whether standalone or connected as an extension of the City Enterprise data network. All offices that connect to the City Enterprise data network must follow this policy guidance since the improper introduction of WLANs in one office can create a backdoor and make not only their data and resources vulnerable, but potentially put the entire City Enterprise data network at risk. This policy provides direction to secure transmissions between the wireless station and an access point (AP). A wireless station, or client, is typically a laptop, notebook personal computer (PC), or personal digital assistant with a wireless network interface card [NIC]. The wireless NIC uses radio waves to connect to the WLAN. The access point, which acts as a bridge between the wireless and wired networks, is typically a wired network interface and bridging software. The access point

functions as a base station for the wireless network, aggregating multiple wireless stations onto the wired network. This policy serves as the foundation for a comprehensive risk mitigation strategy that is enhanced by published security standards, best practices, policies, and technologies of the wired local area network (LAN).

2.0 SECURITY THREATS IN WIRELESS NETWORKING

In order to deploy an effective City wide security policy it is important to first initiate and execute a proper threat analysis. Not only is it important to define the potential security threats but also to define what services and assets that need to be protected, as well as the value of those assets, the cost of having them compromised, and what security services are required to protect them.

2.1 *Eavesdropping*

The anonymous attacker can passively intercept radio signals and decode data being transmitted. The equipment used to perform eavesdropping on the network can be as simple as the equipment used to gain access to the network itself. With little or no modification, the devices can be configured to capture all traffic on a particular network channel or frequency. The attacker must be in proximity to the transmitter in order to receive the transmission. These types of attacks are nearly impossible to detect and even harder to prevent.

Eavesdropping is used to gather information on the network under attack.

The primary goals of the attacker are:

- to understand who uses the network
- what is accessible
- what the capabilities of the equipment on the network are
- when it is used least and most
- what the coverage area is.

This information is needed to launch an attack on the target network. Active eavesdropping is possible when an attacker can connect to a wireless network. Active eavesdropping on a wireless local area network (LAN) normally involves Address Resolution Protocol (ARP) spoofing. Essentially this is a man-in-the-middle attack (MITM) at the data link layer. The attacker sends out unsolicited ARP replies to target stations on the LAN. The target stations will send all traffic to the attacker instead of the intended destination and the attacker will then forward the packet to the originally intended destination. Therefore, it is possible for a wireless station to sniff the traffic of another wireless client that is out of signal range or a wired client on the local network.

2.2 *Communications Jamming*

Jamming occurs when an intentional or unintentional interference overpowers the sender or receiver of a communications link, thereby effectively rendering the communications

link useless. An attacker can apply jamming in several ways.

2.3 Denial of Service (DoS) Jamming

Jamming the entire network can cause a denial of service (DoS) attack. DoS attacks on wireless networks may be difficult to prevent and stop. Most wireless networking technologies use unlicensed frequencies and are subject to interference from a variety of different electronic devices.

Client Jamming - Jamming a client station provides an opportunity for a rogue client to take over or impersonate the jammed client. Jamming can also be used to DoS the client so that it loses connectivity and cannot access the application.

Base Station Jamming - Jamming a base station provides an opportunity for a rogue base station to stand in for the legitimate base station. The jamming can also deprive clients of service or a telecom company from revenue.

2.4 Injection and Modification of Data

Injection attacks occur when an attacker adds data to an existing connection in order to hijack the connection or maliciously send data or commands. An attacker can manipulate control messages and data streams by inserting packets or commands to a base station and vice versa. Inserting control messages on a valid control channel can result in the disassociation or disconnection of users from the network. Injection attacks can be used for DoS. Bait-and-switch attacks or midstream insertion attacks are also possible if the upper-layer protocols do not provide real-time integrity checks in the data stream.

2.5 Replay Attacks

A replay attack is a breach of security in which an attacker stores and retransmits information to trick the receiver into unauthorized operations, such as false identification or duplicate transactions. Without proper replay protection, it is possible for an attacker to record messages sent during the authentication of a legitimate user and later use these messages to get access to the system.

2.6 Man-in-the-Middle (MITM) Attacks

Similar to injection attacks are MITM attacks. MITM attacks can take many forms and are designed to subvert the confidentiality and integrity of the session. MITM attacks are more sophisticated than most attacks and require significant information about the network. An attacker will normally impersonate a network resource. When a victim initiates a connection, the attacker will intercept the connection, and then complete the connection to the intended resource and proxy all communications to the resource as shown in the image below. The attacker is now in a position to inject data, modify communications, or eavesdrop on a session that would normally be difficult to decode, such as encrypted sessions.

2.7 *Rogue Client*

After studying a client in the field, an attacker may choose to mimic or clone the client's identity and attempt to gain access to the network and advertised services. A common wireless security mechanism was supposed to use layer 2 (Data Link Layer) access controls to limit access to resources. This failure was shown in the 802.11 wireless LAN standard with Media Access Controls (MACs) that can be easily circumvented by a skilled attacker.

2.8 *Rogue Network Access Points*

An adept attacker can set up a rouge access point to impersonate a network resource. Clients may unknowingly connect to this false access point and divulge sensitive credentials such as authentication credentials. This type of attack can be used in conjunction with directive jamming to block the ears of the legitimate network access point.

Note: Users with access to the wired network may also install rogue access points, unknowingly opening up the network to attacks. Users may install a wireless access point seeking the convenience of wireless without knowing the security concerns. These access points can serve as backdoors to the wired network because they are normally installed with the default configuration so they are wide open to attack. Attackers can easily connect to these access points and have the same access that a wired user would have. Most networks rely on firewalls for perimeter security and are not prepared for an attack from an attacker on the inside.

2.9 *War Driving*

War driving is the process of searching for open wireless LANs by driving around a particular area.

Note: War driving software is freely available on the Internet.. Many attackers are searching out networks not to attack internal resources, but to gain free anonymous Internet access. One important thing to note here is that the access can be used for a malicious attack against other networks, thus making you liable for damage inflicted against other networks.

2.10 *Client-to-Client Attacks*

Once on a network, other network clients can be attacked directly. If successful, the attacker may gain the credentials required to gain further access into the corporate or telecom network. Successful attacks on wireless-connected clients may reveal sensitive information such as the username and password that can be used to access other network resources. All Internet or wireless-connected stations need to be adequately hardened.

2.11 Infrastructure Equipment Attacks

Incorrectly configured infrastructure equipment is a prime target for attackers and usually provides a means for attaining further penetration into the network. These are sometimes referred to as stepping stones and can be used to bypass access controls. Network devices such as routers, switches, backup servers, and log servers are prime targets. Many network administrators rely on layer 2 security mechanisms such as virtual LAN's (VLANs) to keep wireless networks separate from wired networks. There are many documented attacks that can be used to bypass VLAN security. There are many attacks depending on the switch, but they break down into three main categories: switch attacks, MAC attacks, and routing attacks.

Switch attacks take many different forms. Some involve flooding the MAC or ARP table in the switch to cause it to fail open. This attack is often caused inadvertently by administrators choosing a low-quality switch. Other attacks against the switch involve manipulating the protocol that switches use to communicate such as spanning tree. MAC attacks include ARP spoofing and other physical layer attacks that can be used to fool network devices into sending the data to unintended recipients. Routing attacks are very difficult and normally involve participating in the routing protocol, such as Open Shortest Path First (OSPF) or Enhanced Interior Gateway Routing Protocol (EIGRP), to change the flow of traffic for DoS or sniffing.

2.12 Covert Wireless Channels

Wireless implementers must consider when evaluating or designing a wireless network that, due to the low cost of wireless access points and the ease of creating software-based access points consisting of a standard desktop or laptop computer and a wireless NIC, one must be vigilant in detecting incorrectly configured or unintentionally deployed wireless equipment on the wired network. This equipment can poke very damaging holes in the fabric of the wired infrastructure, which will be exposed to attackers within several miles of a target network.

2.13 Cryptographic Threats

CDMA and GSM cellular networks and wireless Ethernet networks have employed cryptographic mechanisms in order to deter eavesdropping and stymie unauthorized network usage. However, in both networks, oversights resulted in the compromise of communications and fraudulent use.

Wired Equivalent Privacy (WEP) is a cryptographic mechanism designed to provide security for 802.11 networks. Implementation flaws and key management issues have proved WEP almost useless. WEP was designed with a single static key that was to be used by all users. Controlling access to these keys, changing the keys frequently, and detecting compromises is nearly impossible. An examination of the implementation of the RC4 algorithm in WEP has revealed weaknesses that enable an attacker to completely recover the key after capturing minimal network traffic. Tools are available on the Internet that allow an attacker to recover the key in a number of hours. Therefore, WEP

cannot be relied on, by itself, to provide authentication and confidentiality on a wireless network.

2.14 Dictionary Attacks

Also known as brute force attacks. Passwords and encryption keys created by a human being often include a name or a word that has some form of meaning. A dictionary attack exploits this fact and uses a dictionary to try to find the right password. A computer with a reasonable amount of computing resources could easily, within minutes or hours, guess a password. It is therefore important to define a strict password policy, requiring the passwords to be of a certain length and complexity. Also, the security system should be able to detect a dictionary attack and take proper actions, for example locking out the user account that is being attacked.

3.0 POLICY REQUIREMENTS

It is essential that the following policy requirements for wireless connectivity to the City data network be observed to ensure the security and integrity of the City-wide systems. All wireless network devices and technologies that provide a bridge between the City Enterprise data network and the wireless network, or any device that is designed to communicate with such a device via the wireless network that do not comply with this policy shall not be permitted to operate. All requests and accompanying justifications for wireless connectivity shall be thoroughly reviewed and approved by the City Information Systems Office (IS) before deployment. Only wireless devices and City-owned access points that have been authorized by the IS will be permitted to operate and connect to the City Enterprise data network. As part of the overall defense-in-depth strategy of the City IS, both the wired and wireless networks will be monitored for unauthorized use or devices. WLANs and wireless devices existing throughout the City environment, or connected to the City Enterprise data network, before the establishment of this policy will be audited by the City IS and required to meet the standards set forth in this policy to continue operating.

3.1 Authentication

This security service verifies the identity of communicating client stations and provides access control to the network by denying access to client stations that cannot authenticate properly.

All wireless devices must positively authenticate the network.

Digital PKI Certificates will be installed on all wireless device clients. These certificates will be used by the network to authenticate the device.

All wireless devices must be positively authenticated by the network.

Digital PKI Certificates will be installed on all authentication servers. These certificates will be used by the wireless device to authenticate the network.

All wireless device users must be authenticated to the network using personal user id's and passwords.

If a central authentication server or VPN gateway is used in the WLAN architecture, each wireless user must uniquely and successfully authenticate to the WLAN.

Wireless device users must use strong passwords (alphanumeric and special character string at least eight characters in length).

All wireless users must logon to the City Enterprise data network services as a separate step from the WLAN authentication.

3.2 Encryption

All WLAN traffic must be encrypted to limit eavesdropping and ensure confidentiality.

All Wireless Access devices connected to the City Network will conform to the WiFi Protected Access 2 standard and shall employ 802.11x/EAP authentication and AES-CCMP encryption (WPA2-Enterprise mode).

All wireless handheld devices must encrypt information leaving the device for an adequate level of protection.

Wireless device default settings must not be set to “no encryption.”

Sensitive data and application data files stored on handheld devices must be protected with robust encryption and password protection utilities. It is required that sensitive data files be deleted from the handheld device once they are no longer needed and archived on a desktop PC.

Data residing on external storage modules should be encrypted and stored in a secure manner.

3.3 Access Control

All access to the WLAN system, including its data and resources, shall be restricted unless authorized by the City IS. Data traversing wireless networks and data accessible via wireless entry must be protected from unauthorized access, use, modification, or deletion using access control methods.

To mitigate data leakage, Infrared (IR) ports must be disabled during periods of inactivity.

File sharing on wireless client devices shall be disabled.

Wireless client devices shall only operate in infrastructure mode. (Ad Hoc mode disabled)

Non-City employees, excluding approved vendors and contractors, must not have access to WLANs that connect to the City Enterprise data network.

Service Set IDs (SSIDs) must be changed from the factory default to something that is meaningless to outsiders. SSID character strings must not reflect names,

locations, or products being used.

Broadcast mode of SSIDs must be disabled in products that permit it so that the client SSID must match that of the access point. Where possible, the wireless network should be configured with the longest beacon interval.

The authentication server, firewall, and/or VPN gateway must enforce access control mechanisms.

3.4 Antivirus Software

All WLANs and handheld devices must utilize antivirus software as directed in the City Security Policy.

Antivirus software for handheld devices shall scan all entry ports (i.e., beaming, synchronizing, email, and Internet downloading) as data is imported into the device, provide online signature update capabilities, and prompt the user before it deletes any suspicious files.

3.5 Personal Firewalls

Personal firewall software helps mitigate threats of confidentiality, integrity, and authenticity of information being transferred over the Internet.

It is highly recommended that WLAN client and handheld devices utilize personal firewall software.

Users that access public wireless networks (e.g., in airports, conference centers, coffee shops) should install personal firewall software on all WLAN client and handheld devices. A personal firewall protects against wireless network attacks and rogue access points (e.g., Ad hoc networks, accidental or malicious association, soft access points) that can be easily installed in public areas.

3.6 Physical Security

The physical security of all wireless access points and handheld devices is the first line of defense in WLAN security. It is essential that proper physical countermeasures be in place to mitigate risks such as theft of equipment, insertion of rogue access points, and wireless network monitoring devices.

Access points must be physically secured upon proper configuration to prevent tampering and reprogramming (i.e., to prevent unauthorized physical access).

Access points must be placed in secure areas, such as high on a wall, in a wiring closet, or in a locked enclosure to prevent unauthorized physical access and user manipulation. Devices must not be placed in easily accessible public locations. To mitigate eavesdropping, access points shall be placed strategically within the building so that the range does not exceed the physical perimeter of City-controlled facilities and allow unauthorized users to eavesdrop near the perimeter. Access points shall be placed to minimize or prevent the distance that the signal can travel outside the area that is under the control of the organization, including

buildings, court yards, adjacent parking areas, etc.

In areas where utilization is not required on a 24 hours per day, 7 days per week basis, access points shall be turned off during all hours during which they are not used (e.g., after hours and on weekends) to minimize potential exposure to malicious activity.

The transmission power of WLAN access points must be restricted to the lowest power required for coverage.

In the event that the reset function of an access point is used, the device must be restored to the latest security settings.

Wireless handheld devices and Network Interface Cards (NICs) must be physically protected from loss and theft.

Wireless handheld devices, backup modules, and NICs (e.g., laptop computers) must be stored in a secure area, such as a desk with drawers that lock, or a file cabinet that locks when they are not being used.

3.7 Logical Security

All wireless LAN access points and handheld devices must be authorized. All access points shall be logically separated and isolated from the City Enterprise Data network, such as on a different segment, in a demilitarized zone (DMZ), or in a virtual LAN (VLAN).

WLANs must be treated as insecure counterparts to their wired associates. Access to resources on the wired network must be restricted.

All access points must be firewall protected outside the wired network. Placement of access points and channel assignments shall be such that coverage/throughput is maximized while interference (denial of service) is kept to a minimum between different access points or WLANs.

Access points shall be physically situated so that authorized users can connect, yet away from sources of interference such as microwave ovens and Bluetooth devices.

To keep interference to a minimum, access point channels shall be at least five channels different from all other nearby access points on different WLANs. Some coordination may be required if multiple WLANs are to be used within close proximity.

All insecure and nonessential management protocols shall be disabled.

If SNMP is turned on for management purposes, the SNMP Community Strings must be changed from their manufacturer default to unique and difficult to guess strings. SNMP settings must be set to least privilege (read only).

Web-based management of access points shall be from pre-defined management stations controlled by access lists on the access point. SNMP requests shall only be accepted from specified management devices.

SNMPv3 products or equivalent cryptographically protected protocol shall be used since they include mechanisms to provide strong security.

3.8 Inventory, Monitoring and Audit

All wireless access points must meet the current security configurations established by the City IS.

All wireless LANs and handheld devices must be routinely monitored and security audits performed to verify that security configurations comply with this policy, access points and wireless devices are authorized, and to identify unauthorized activity.

The City IS will conduct yearly audits of access points to ensure that security configurations conform to this policy and to maintain a current inventory of the devices.

If DHCP is used in the environment, logs shall be reviewed for static addresses to determine if rogue access points have been installed.

Access logs and system audit trails shall be routinely monitored.

The City IS will conduct routine controlled penetration tests or packet sniffing/wireless traffic analysis on WLANs and within the coverage area.

All access points must have Intrusion Detection Systems (IDS) at designated areas on House property to detect unauthorized access or attack.

Procedures must be established and followed for the inventory and control of wireless devices and equipment.

3.9 System Administration/Vendor Responsibilities

It is the System Administrator's / Vendor's responsibility to ensure that Wireless LANs and devices meet the technical standards outlined in this policy at all times. System Administrators / Vendors are required to operate Wireless LANs and devices in a secure manner.

This includes, but is not limited to, proper authorization and termination of access, proper configuration and placement of wireless components and associated security technologies, routine, random, and event-driven maintenance, support monitoring and audit functions, etc.

System Administrators / Vendors are required to change factory default settings and use strong administrative passwords on all wireless devices to ensure a higher level of security. (On some wireless devices, the factory default password is blank.)

All insecure and nonessential management protocols must be disabled.

To the extent possible, System Administrators / Vendors shall ensure that their wireless implementation and associated security technologies are up-to-date with evolving standards and best practices. Client NICs, access points, and handheld devices must support firmware upgrade so that security patches and upgrades may be fully tested and deployed as they become available.

System Administrators / Vendors are required to maintain a list of authorized wireless device users to enable them to perform periodic inventory checks and security audits.

3.10 User Responsibilities

It is the wireless user's responsibility to comply with this policy. Wireless users must only access information systems using approved wireless device hardware, software, solutions, and connections.

Wireless device hardware, software, solutions, and connections that do not meet the standards of this Policy will not be authorized for deployment.

Wireless users must act appropriately to protect information, network access, passwords, cryptographic keys, and wireless equipment. Wireless users are required to report any misuse, loss, or theft of wireless devices or systems immediately to the City Information Systems Help Desk at (360) 473-5475.