MUNICIPAL WIRELESS NETWORK

May 2009

Disclaimer: Whilst the Government endeavours to ensure the accuracy of the information in this paper, no express or implied warranty is given by the Government as to the accuracy of the information. The Government of HKSAR accepts no liability for any error or omission arising from or related to the use of the information.

TABLE OF CONTENTS

SUMMARY

Citywide wireless broadband initiatives are receiving increased attention today. More and more major cities across Asia, such as Taipei and Singapore, have already deployed citywide wireless networks. These large open networks have almost certainly experienced a number of challenges in the course of their deployment. Business models and infrastructure technology for municipal wireless networks are evolving at a rapid pace, converging on a managed-service or public/private partnership model. This article focuses on the security issues that are most likely to be encountered during implementation of any municipal wireless network. It also discusses measures that should be considered to tackle important security issues. In addition, as citywide wireless broadband initiatives evolve, they may bring new security challenges to organisations and the general public. In this article, we discuss the challenges facing both organisations and individuals, and make recommendations on how these challenges can be met.

I. MUNICIPAL WIRELESS NETWORKS IN CITIES

FACTORS DRIVING THE MUNICIPAL WIRELESS EVOLUTION

Wireless broadband initiatives for cities are gaining more attention today. Many major cities have already announced the deployment of citywide wireless networks. There are a number of key driving forces that have led to the current wave of municipal wireless network services:

Low-cost Deployment

The cost of citywide wireless network deployment is relatively inexpensive when compared to the older wired alternative. Firstly, the unit cost for wireless network equipment has dropped significantly as a result of the large-scale demand and production of Wi-Fi chipsets. Secondly, municipal governments can make use of existing urban assets, such as lampposts and government buildings, that serve as excellent antenna sites for wireless nodes.

Interoperability

Industry-led standardisation of wireless technology through the IEEE and Wi-Fi Alliance has ensured broad interoperability. This has fuelled the technology’s integration as standard equipment into mobile devices, such as notebook computers and personal digital assistants (PDAs), and has stimulated the widespread propagation of wireless technology.

Digital Inclusion

As wireless technologies become more widespread, municipal wireless networks can be considered a catalyst of digital inclusion. A wireless infrastructure may be able to provide low-cost or free Internet access to those less well-off, and could be part of a programme to make computers — and Internet access — available to disadvantaged families.

Because of this, local governments have been active in rolling-out or announcing plans to build citywide wireless networks capable of providing high-speed Internet access to residents and businesses. According to MuniWireless[1], as of 1st August 2007, there were over 400 cities and counties in the United States with live municipal wireless networks, or with networks in the deployment / planning phase.

[1] http://www.muniwireless.com/article/articleview/6279/1/23

II. BUILDING A SECURE MUNICIPAL WIRELESS NETWORK

PLANNING MUNICIPAL WIRELESS NETWORKS

A municipal wireless network is generally operated by a local government authority, or under a public/private partnership agreement. As a result, there is often a public perception that this type of wireless network provides a safe computing environment for a wide spectrum of users, including children. It is therefore important to analyse all possible security issues in the planning phase of a large-scale wireless network project. The following are areas that may need to be considered.

Types of Attacks

When planning a municipal wireless network project, a number of defensive layers should be considered. Threats related to a municipal wireless network can be categorised into three areas:

1. Attacks against endpoints
2. Attacks against the wireless network itself
3. Attacks launched from within the wireless network

Attacks against endpoints

Once a user connects his mobile device to a municipal wireless network, the device is vulnerable to attacks over the network, such as attempts at unauthorised access or virus propagation. Although the user should be responsible for the security of his or her own mobile device, there is still a general expectation that the network provider (i.e. the local government) should have adequate protection in place to safeguard from malicious attacks. As such, a certain level of basic protection should be deployed on the network as a first line of defence to protect client devices from malicious attacks.

Attacks against the wireless network itself

A municipal wireless network can be an appealing target for criminals and those bent on causing disruption. One possible assault is a denial-of-service attack, which can bring down a wireless network. An attacker may leverage certain vulnerabilities in access points by sending out vast quantities of malicious requests to targeted access points across the network, forcing them to not respond to legitimate requests, hence bringing the network down. There is therefore a need to implement certain basic security measures such as firewalls and intrusion prevention systems (IPSs) to fortify the edge of the network against this type of intrusion.

Attacks launched from within the wireless network

A municipal wireless network may provide low-cost or even free Internet access, making computers and the Internet available to a wider portion of the population. But those with malicious intent can also be beneficiaries of the network if measures to protect the system are not adequate. Attackers could leverage the free availability of a wireless service as a vehicle for launching all kinds of attacks against the Internet users right across the Internet, not just users of the wireless service, who may not have adequate protection on their devices.

Inappropriate Use of the Wireless Network

Inappropriate use of the wireless network, in particular access to obscene material or infringement of copyrighted works through Bit-Torrent (BT) type services (or similar utilities) is a major concern, and needs to be addressed.

Confidentiality of Communications

Eavesdropping is a security concern in any public wireless network that does not have adequate encryption systems in place. Without them, data generally gets transmitted as plain text, and with easily available packet sniffing tools, a malicious user can quickly capture information being transmitted across the network without any problem. Encryption systems may be considered to address these concerns. Yet the complexity of enabling an encryption feature on a client computer or mobile device may reduce people's interest in using the wireless network, so it is necessary to strike a balance between security and convenience.

User Anonymity

Anonymous access may be permitted by the service provider in order to maximise usage of their public wireless hotspots. In some municipal wireless implementations, the configuration details of the wireless network are made public and no user authentication is required. However, this may make it much easier for malicious users to use the wireless network for improper purposes. Without authenticating the identity of users, the audit logging ability of the network is severely limited.

SECURING MUNICIPAL WIRELESS NETWORKS

To properly secure a municipal wireless network, both administrative and technical controls are essential. The following are some of the most important administrative and technical security measures needed for the protection of any municipal wireless network:

Define an Acceptable Use Policy for the Network Service

An acceptable use policy is a set of rules that define acceptable practices for use of the wireless network service. The statement outlines the consequences of violating the policy. Common actions taken would be withdrawing the service from the violator and, if the activities appear to be illegal, informing the appropriate authorities such as the police. This policy should be tied in with any information security policies. The following are common elements in an acceptable use policy:

1. Prohibited Uses
2. Responsibilities of users
3. Conditions for suspension or termination of the service
4. Privacy

Central Security and Detection Measures

Network security measures such as firewalls, anti-virus solutions, intrusion detection systems (IDS) / intrusion prevention systems (IPS), rogue access point detection, and wireless IPS should be deployed to protect users from network intrusion. Another consideration may be the need for a content filtering mechanism. Instead of allowing free and uncontrolled access to the Internet, providers may feel the need to control or filter out access to indecent websites, pornographic or obscene material, and sites offering illegal downloads.

Captive Portal

As a deterrent mechanism, the service provider could also consider setting up a captive portal, so that a landing page is shown whenever the user starts a new browser session on the wireless network from their client device. The acceptable use policy can be displayed on this landing page to remind people about proper use of the service.

User Authentication Service

When designing the wireless network service, the provider needs to put in place a system for enabling and disabling authentication of individual SSIDs for people who use the service.

Mechanisms should be put in place to track the location of possible intrusions within the municipal wireless network. In Wireless@SG (in Signapore), all users need to register and input their name, address and mobile phone numbers before the service can be activated.

Wireless Encryption

To provide basic over-the-air interface protection to users, a native wireless encryption feature, such as Wi-Fi Protected Access (WPA) with Advanced Encryption Standard (AES) or Wi-Fi Protected Access 2 (WPA2) with AES, should be made available as an option. However, because some legacy network equipment may not support AES encryption, service providers should take this into consideration in the service design phase and may provide both encrypted and unencrypted services to suit different users' security needs.

Wireless Network Access Control

Access control to the wireless service should be considered as the first layer of defence for the network, so that the service provider has the ability to remotely grant or block access to any wireless client device. This can help contain any adverse impact should a security incident occur.

Client Isolation

Most installed wireless networks today operate in an "infrastructure" mode that requires the use of one or more access points. With this configuration, all traffic on the network traverses these access points. By controlling the communication between client stations at these access points, providers can prevent malicious attempts to gain access to vulnerable client stations.

Physical Security

The loss of network equipment might pose a significant threat to the wireless network if configuration information can be retrieved from a missing access point or wireless interface card. Securely mounting network equipment, such as access points, at inaccessible locations along with strong physical security controls, can minimise the risk of theft.

Logging and Auditing Functions

Service providers should consider implementing logging and auditing functions to record all network connections, especially any attempts at unauthorised access. Authorised personnel should review the log regularly.

Security Risk Assessments and Audits

Security risk assessments and audits are an essential means for checking the security level of a wireless network, and identifying any corrective measures necessary to maintain an acceptable level of security. They help in identifying loopholes in the wireless network, such as poorly configured access points using default or easily guessed passwords and SNMP community strings, and the presence or absence of encryption. However, a security risk assessment can only provide a snapshot of the risks to the information system at a particular time, so it is important to perform risk assessments and audits regularly once the wireless network is up and running.

In addition, a number of best practices for security management, including the establishment of clear incident response procedures, should be drawn up. As the individual Internet user is often the weakest link in the security chain, education awareness and tips for safe Internet surfing should be promoted regularly to the general public.

III. ESTABLISHING A POLICY ON USING A MUNICIPAL WIRELESS SERVICE AND WIRELESS HOTSPOTS TO ACCESS A CORPORATE NETWORK

Due to the popularity of Wi-Fi hotspots, and the proliferation of municipal wireless services around the world, travellers may leverage these services to access their corporate network while they are on the road. This may pose a number of security risks to the corporate network if security measures for protecting this kind of remote access connection are inadequate. A malicious attacker could possibly capture sensitive information and even break into the corporate network through the account of an unsuspecting employee.

A clear security policy on using municipal wireless services or public wireless hotpots to access corporate networks should be defined. Employees who travel should be made aware of the potential risks of using these services when accessing the corporate network.

IV. END-USERS: BEST PRACTICES WHEN USING MUNICIPAL WIRELESS NETWORKS

Although municipal wireless services provide convenient and sometimes free Internet connectivity, users of these services should take certain steps to protect themselves from potentially damaging attacks. The following are general tips for individual end-users:

1. Always treat a municipal wireless service as an untrusted network and do not login to sensitive websites that do not use encryption channels such as SSL. It is also not a good idea to access company servers from a municipal wireless service without the protection of a Virtual Private Network (VPN) or other similar encryption mechanisms to ensure the confidentiality of communications. Split tunnelling, which allows a person to connect to the Internet while at the same time maintaining a VPN connection to a private network, should also be disabled when using VPN.

2. When connecting to a public hotspot, the user may be redirected to a captive portal page. Attackers could also setup fake captive portal pages to obtain sensitive information. Therefore, it is important to check the authenticity of a captive portal by verifying the certificate of the website in question.

3. Some operating systems offer a feature for the user to create a list of preferred wireless networks. Once this list is defined, the system will keep searching for preferred networks and try to automatically connect to them when within range. By capturing information sent out from a person’s system in this way, an attacker could setup a fake wireless access point that corresponds to the settings of a wireless network on the victim’s Preferred Network List. In doing so, the user is automatically connected to the attacker's wireless network. To prevent this kind of attack, the Preferred Network List feature should be disabled or removed.

4. Computer-to-computer wireless networking should be avoided. "Ad Hoc" mode networking enables a person’s wireless device to communicate with other computers directly through a wireless connection, but it offers minimal security against unauthorised incoming connections. This feature should be disabled to prevent attackers gaining access to information resources on the individual’s device. Network shared resources should also be turned off.

5. Individual users should always protect their computer when connecting to a municipal wireless service by running anti-virus / anti-spyware software with the latest signature files, applying the latest patches to system components, and turning on their personal firewall. Sensitive and confidential information stored in any wireless device should also be encrypted using strong encryption algorithms. Common security safeguards such as power-on login to a device or system login authentication, and password-protected screen savers should also be used when accessing the Internet in public places.