# Wi-Fi, Wi-MAX

## Taking wireless security seriously

**By David Crowe**

The world is going crazy over wireless. Mobile phones, wireless PDAs, Wi-Fi in airports, hotels, homes and coffee shops, and WiMAX to connect those homes into the big bad Internet.

And the Internet is both very big and parts of it are very bad. E-mail systems are flooded with spam. Corporate Web sites dragged down by denial of service attacks. Browsers buried under unwanted pop-up windows. Spyware waiting and ready to send credit card numbers and other personal information back to a gang in a foreign land.

No communications technology can ignore security. While securing wireless links will not make the Internet a playpen again, new holes cannot be opened. Wireless is particularly vulnerable because there is no way to physically protect the communications link.

It was not always this nasty. Back at the beginning of time (wirelessly speaking), around 1984, some people thought that the ESN (Electronic Serial Number) for analog cell phones was overkill. But, they changed their mind when, by the mid 1990s the US cellular industry was losing about half- a-billion dollars a year to 'cloning', a method of stealing service by transmitting the MIN (Mobile Identification Number) and ESN of another phone. How were the MIN and 'unchangeable' ESN obtained? By monitoring the airwaves for cellular transmissions.

GSM, and then TDMA, AMPS and CDMA, developed forms of authentication that are still in use today. They use a Challenge/Response method, which requires that an Authentication Centre (AC or AuC) and the mobile both know a secret number, known as the root key or A-Key. It would obviously be insecure for the phone to transmit the key, because it could be captured by others and used to clone a phone. Therefore, the network must determine whether a phone possesses this number indirectly. It sends a large random number to the mobile as a 'Challenge'. The mobile and the network both execute a one-way algorithm using the root key and the random number to

produce a response, which is another large number. The network then just has to check that the response sent from the mobile matches the response that it also calculated. In some systems, the opposite process is used by a truly paranoid mobile to authenticate the network.

The algorithm is called 'one-way' because it is relatively simple to take the inputs (Random Challenge and Root Key) and produce the output (Response), but extremely difficult to take the output and calculate the inputs. This is important because the output (the authentication response) will be transmitted wirelessly, and therefore publicly.

This is not absolute proof that the mobile is legitimate, but if care is taken, it is the next best thing to it. Network operators should ensure that the root key in both the phone and the AuC are reasonably well protected. It should not be possible, for example, to view the root key on the phone, otherwise people could easily steal service if they had a few minutes alone with a phone (they could also steal the phone, but stealing the root key is an invisible crime, and would take much longer to detect). Systems must be careful not to repeat the random challenges (a temptation especially in GSM) because that opens the system up to a 'replay attack'. Someone monitoring the radio channel could capture the challenge, response and mobile identification, and then initiate a call as soon as the legitimate phone disconnects. If they are lucky and the same challenge is issued, they can respond with the same response.

It is also very important that carriers protect their databases of keys. A secure data centre and stringent controls and auditing of access to the database are necessary.

One critical, but easily overlooked, aspect of this security system is the global interconnection of systems. When a phone is roaming, the current serving system has to be able to communicate with its AuC knowing only the phone's identification (MIN or IMSI). Luckily, for cellular authentication, this was possible because systems were already interworked for other reasons using the GSM or ANSI-41 MAP (Mobile Application Part). Wherever there is roaming, there is a connection at the MAP level.

This type of authentication is more difficult for other wireless systems to implement because global interworking was never part of the plan.

## Wi-Fi

Wi-Fi (802.11), for example, was designed as Ethernet cable replacement. Mobility was not considered in its design. It was believed that devices could be connected together without cabling, but would still always stay in one place. A printer might be shared by several computers in an office, but would not get legs and walk away.

However, humans are natural nomads, and it didn't take long for Wi-Fi to get into laptops and then roaming seemed like a natural thing to do.

The problem was that the security system for Wi-Fi was called Wired Equivalent Privacy (WEP). Many people criticize the algorithm as being weak, and it is, but the major problem is that the key is owned by the Access Point (base station) and not by the Wi-Fi clients. This means that every client in the same area has to use the same key and that clients have to have multiple keys in order to roam, potentially one key per access point.

This seems insane, but it does make sense if you think of Wi-Fi as an Ethernet cable replacement technology. One computer would be on one network and therefore have one key. However, it only makes sense from this perspective, and this perspective is only of historical interest. But we should not be too harsh on the designers. 802.11 was not the first technology group blown away by the success of their own brainchild. Lest cellular proponents get too complacent, they should remember being blind-sided by cloning when a 'hardened' ESN was their only form of security.

WEP is actually a reasonable solution for personal Wi-Fi networks, and those in small offices. It does not work well for large offices, nor for people who use Wi-Fi extensively while traveling.

The single key per access point in WEP creates a management nightmare. To properly secure a WEP system you should change keys on a regular basis so that devices can be prevented from accessing the system. If this is not done, then a fired employee could sit in the parking lot and access the Wi-Fi system and get into your corporate computers. This means that an IT department that relied on WEP for security would have to find a mechanism to ensure that every mobile has the key of every Access Point which it is authorized to access, and that this information is updated whenever keys are changed or added. The difficulty of managing this means that most IT departments do not rely on a WEP system, which results in a Wi-Fi network with no security, or alternatively, they assign all Access Points in the com-

pany with the same, static key, which provides some very limited protection.

However, all is not lost. Placing the Access Points outside the firewall, requiring a VPN (Virtual Private Network) to enter, ensures that important communications are secure, and that unauthorized access to corporate data and networks is not possible. This is not an ideal solution, but it works reasonably well. It does not protect the Wi-Fi connection itself, however, meaning that outsiders can still steal Internet service quite easily, although they cannot get inside the corporate network. This is not a problem for companies with their own buildings, as Wi-Fi signals do not leak far, but will be a problem for companies in small buildings, or in multi-storey office towers.

One of the reasons for this flawed design is the lack of a network to provide standardized access to a home AuC. In fact, there is no concept of a 'home' Wi-Fi system for a device. Devices commonly have legitimate access to many different systems. Consequently, there is no place to go to get the root key that could be used to authenticate the mobile.

The importance of authentication is that once the identity of the mobile is known reliably, a database of authorized users can be consulted, and the appropriate access restrictions can be applied. Furthermore, since the network and the mobile device would both know the same root key, both could apply encryption to their communications without further ado.

WPA (Wi-Fi Protected Access) is a step in the right direction. It involves a login server to validate the credentials of the mobile, and keys are changed frequently. But this does not significantly reduce the management burden, and there still is no concept of a single login server for a device. Users would still need to be registered in one server for their company, one for the hotel chain they frequent, one for each of the hot spot providers they use at airports, and so on.

Further down the road is the RSN (Robust Security Networks) that IEEE 802.11i is developing to be a long-term solution to Wi-Fi's security woes. There is a good chance, however, that this will only apply to new devices and not to the current installed base.

## WiMAX

WiMAX (802.16) is another wireless technology from the IEEE. It standardizes Point-to-Multipoint or mesh microwave transmission, and could be used, for example, to connect homes or businesses to an ISP for high-speed Internet connectivity. In this mode it does not really compete with Wi-Fi, but it is complementary. It provides the long-distance transmission and some of its end points might actually be Wi-Fi networks.

This application of WiMAX makes the security challenges easier than for Wi-Fi. Client devices are often installed by technicians, and can have the security association with the network established through the use of X.509/RFC 2459 certificates that were built-in at the time of manufacture.

Security is a little bit more complicated for mesh networks. These networks use the client devices as mini-base stations, increasing the reach of the network. Special mechanisms are required to establish security without the intermediate client devices being weak links in the security chain.

Rather than the private key security used in cellular, WiMAX has chosen to use public key encryption. Private key encryption is often called 'symmetric', because both ends have the same key (the Root Key or A-Key), while public key encryption is 'asymmetric', with

each device having a private key to decrypt incoming transmissions and a public key to encrypt outgoing transmissions. Because of the extra overhead, WiMAX just uses public key encryption during the initial establishment of security. Private key encryption is used for real-time operations (such as the encryption of transmitted data).

Security information can be stored by the network immediately connected to the WiMAX base station, so there is no need for global networking. This is because only a limited and relatively static list of clients is entitled to connect to that base station. Nobody obtaining WiMAX service as an Internet access alternative is going to expect to take their modem with them when they travel and obtain service.

However, if WiMAX becomes built-in to laptops and other mobile devices, and starts to be used as a higher range, higher capacity replacement for Wi-Fi, then similar security challenges will occur.

## MAC LIMITATIONS

One of the problems with security is that it often relies on the MAC (Media Access Control) address. This is because this 48-bit number is globally unique. No two Internet devices (whether Ethernet, Wi-Fi or other) will have the same address. The problem with this is that the MAC address only identifies the device and the manufacturer. This is similar to the ESN and IMEI (International Mobile Equipment Identity) used in cellular.

ESN and IMEI are not, however, used as mobile identifiers. The MIN or IMSI (International Mobile Subscriber Identifier) are used for this purpose. Both of these number types identify the home system, and thus allow communication with the correct HLR (Home Location Register) or AuC as soon as the mobile transmits it to the network. Some wireless systems use an NAI (Network Access Identifier), which is like an e-mail address (e.g. David.Crowe@wi-fi-erewhon.com). This identifies the user – not the device – and the domain name (after the '@' sign) identifies the home network provider.

## CONCLUSIONS

I predicted in Wireless Telecom in 2003 that cellular carriers would be big players in the Wi-Fi hotspot market. I felt that only they had the experience with wide area networking for authentication, validation and billing, and that this experience would be important to get true roaming working in hotspots. This networking is essential to provide strong security that is not burdensome on the user. Ideally, a mobile device would access a wireless network, providing its identity, which would allow a network query to another Wi-Fi provider to obtain the security information necessary to establish a security association with the device. Wi-Fi has made great strides, but still has a long way to go before public Wi-Fi access is as ubiquitous, secure and easy to access as cellular.

The good news is that everyone is taking wireless security seriously. Systems are not perfect, and there are still many restrictions on where you can obtain wireless data due to limited networking, but it has been proven that security and mobility can co-exist for any wireless technology. ■

*David Crowe is a wireless standards, technology and numbering resource consultant based in Calgary. He can be reached at David.Crowe@cnp-wireless.com or (403) 289-6609.*