Wireless Security
Mike McMurry
January 22, 2001

Wireless Synergy:

The idea of constant access to information has spawned numerous wireless devices and almost as many methods to transfer that information to the user. The worldwide market for wireless Internet transactions will grow to $38 billion by 2003, in that same timeframe use of Internet devices will increase from 240 million users in 1999 to 602 million users in 2003. Most of those 602 million users will want a wireless option for their Internet utilization. As with most IT based initiatives the security aspects have either been overlooked or are playing catch-up after the fact.

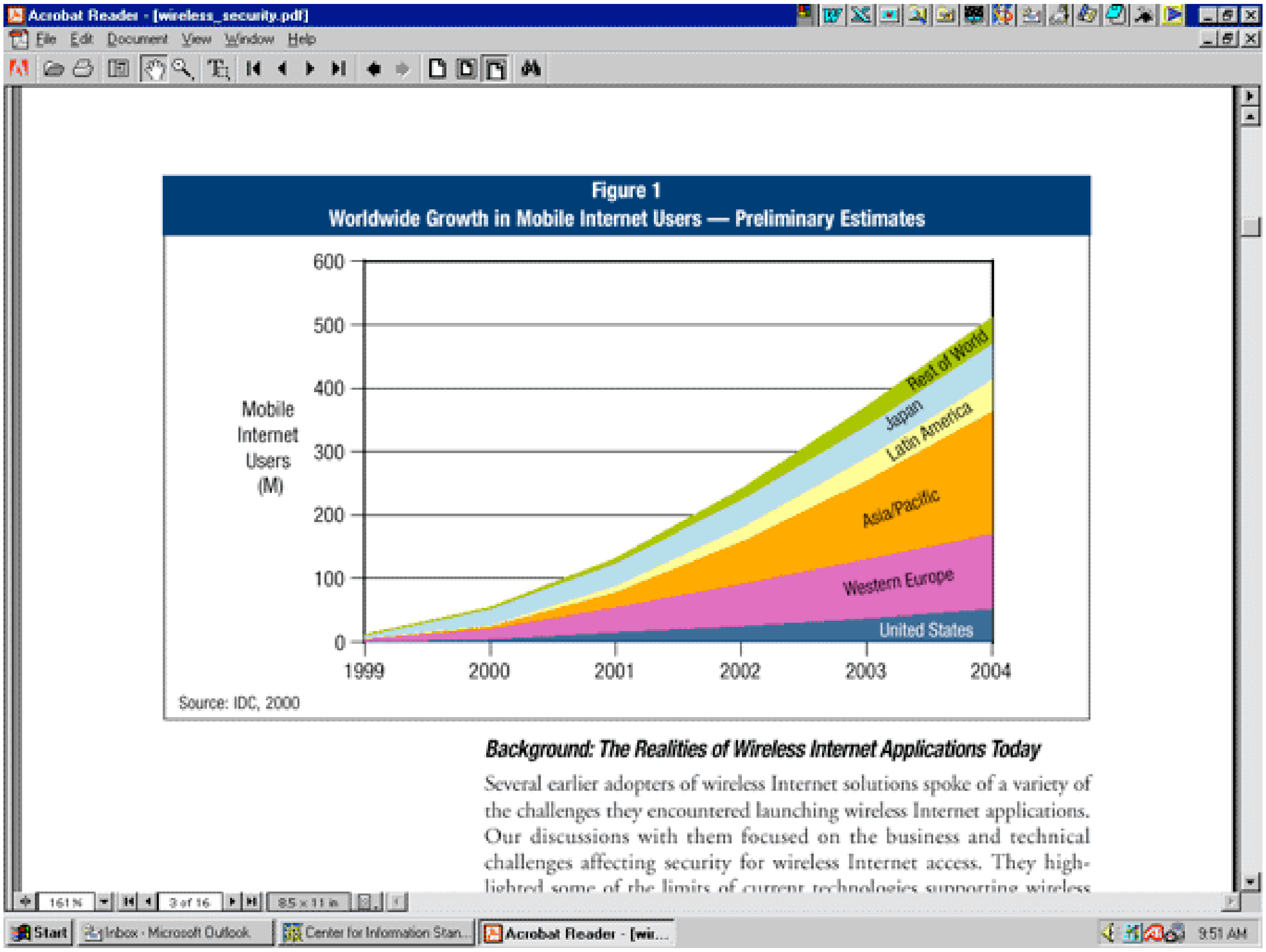

Figure 1
Worldwide Growth in Mobile Internet Users — Preliminary Estimates

Source: IDC, 2000

Background: The Realities of Wireless Internet Applications Today

Several earlier adopters of wireless Internet solutions spoke of a variety of the challenges they encountered launching wireless Internet applications. Our discussions with them focused on the business and technical challenges affecting security for wireless Internet access. They highlighted some of the limits of current technologies supporting wireless

Wireless devices are unique though for several reasons. First of all they are by their nature, mobile. A Personal Data Assistant (PDA) can fit in your front pocket so it has a few more security considerations than say a desktop computer, because of this these two items cannot be treated the same from a security standpoint. PDA's must be protected at several levels. First, the obvious physical security of something that small must be looked at, then the transmission of wireless data must be analyzed, because these devices use relays the integrity of the data must be ensured while at a gateway, then finally the data must be protected when it hits your various servers.

Physical Security:

Policy is the only real player when it comes to physical security of a mobile device. Management must ensure strong policy guidance and perform random audits to maximize its effectiveness. Use of mobile devices will certainly increase productivity of an organization but employees must respect their purpose and limit their use to official purposes. Because wireless devices are highly mobile they are also easily stolen or lost. User authentication becomes critical since they can easily fall in to the wrong hands. Unfortunately user authentication is the exception, not the rule with companies like Bluetooth, that authenticate the device and not the user. Third party software that incorporates

PIN numbers, smart-card technology and even time-outs for repeated password input are necessary to ensure a secure network. Some companies like BarPoint.com have altered their business practices so that during this time of limited wireless security they can feel a bit safer. Barpoint has separated their workgroups in to 3 separate areas, each with their own layer of encryption. No one is allowed to share keys with anyone outside of their group so that if a wireless device falls into the wrong hands the damage would be limited to only one area of the company.

Transmission Security:

Transmission of data is another key area for protection. For every method of transmission there are several methods of stealing or auditing that transmission. Relatively inexpensive scanners can pick up radio transmissions and even Cellular Digital Packet Data transmissions. Brute force methods of wireless security include simply limiting the amount of stray radiation, point-to-point laser or microwave links can accomplish this but are expensive. Spread spectrum transmissions are one method that telephone makers have incorporated. "Frequency hopping" assures that even if an evesdropper has the ability to listen in on your transmissions they cant do it very long because you are "off" to the next frequency within seconds or even milliseconds. This method is expensive though, for both the user investing in the handheld and the company transmitting the data. For its cost and relative simplicity the method that seems to be gaining the most acceptance is data encryption. Currently the only limit with wireless devices is the fact that they have somewhat limited processing capability. Currently IEEE 802.11 allows for 40-bit and 128-bit level encryption using RC4 PRNG (Pseudo Random Number Generator), when adding encryption the throughput dropped about 1M bps for 40-bit encryption and between 1M bps and 2M bps for 128-bit encryption, overall a small price to pay for wireless transmission protection.

Gateway Security:

The only problem encountered with the current state of the Wireless Application Protocol (WAP) is that the encryption in essence "goes away" when the packet gets to its gateway. Since the data must be routed around any number of areas it must have and address, this address can only be read if it is unencrypted and as soon as that happens it becomes vulnerable to eavesdroppers. Some providers have worked around this problem by moving their wireless gateways behind their trusted network, or at the very least launched only less-sensitive applications for wireless use until a more robust fix can be implemented (kind of a do what you can, not what you want to approach). The next version of WAP apparently addresses this shortfall and is due out sometime in 2001.

Server Security:

For the most part server security can mirror your in-place security policies for traditional wired portholes. Good security practices are universal, although the scale of the wireless enterprise needs to be examined. Wireless Internet initiatives are integrating literally tens of thousands of devices into your existing enterprise Internet framework (Bluetooth PAN, LAN, phones, PDA’s etc). Companies must deal with the security implications of this *before* implementation, not after. Since there is a need, and since this is a world safe for capitalism, third-party software companies have products available for implementing security practices and policy for the endless scalability and manageability tribulations they are sure to encounter. IBM has its "Tivoli Secure Way Policy Director" which manages both wireless and traditional security architectures with the key security components for any secure applications portal; strong authentication and comprehensive access control. Companies should also limit which applications you can access via a wireless device. Banks have adopted access control policies for their users, for example they may allow you to check your balance, but only transfer funds to another one of your accounts, thus deterring any would-be criminal with limited capability.

Conclusion:

The Strategis Group estimates that the number of wireless users will break the *one billion* user mark by 2004. As mentioned earlier the transactions of these users will top $38 billion dollars, with that many users and that much money crisscrossing the wireless community it only makes sense that there will be some very motivated criminals waiting to intercept those transmissions. IT departments must not simply keep up with those who would do them harm but rather remain a step ahead of them. Good planning before implementation, selective application development and continued concentration on security at the development level will help ensure that all wireless users and providers are protected.

Sources:

"IDC Outlines Ideal Security Infrastructure for Wireless eBusiness"
http://www.tivoli.com

"WAP: Wireless Internet Today", The WAP Forum
http://www.wapforum.org/

"Crossing the Wireless Security Gap", Computerworld
http://computerworld.com/cwi/story/0,1199,NAV65-663_STO55583,00.html

"M-Commerce Security, A Moving Target", eWeek Jan 15, 2001

"The LAN, PAN, WAN Plan", eWeek Jan 15, 2001

"Widening Your Secure eBusiness to Wireless" IDC White Paper, December 2000