

Inside

COVER STORY

Wireless Communication: Safeguarding Data in a Mobile World

How safe is the wireless transmission of data?

Fast Facts2

Grill Your Security Officer3

Looking for answers to security issues? Then check out these Q & A's — or send us your own.

Securing Wireless Data Access – What You Can Do3

Security controls to help safeguard sensitive data during wireless transmission.

Securing Wireless Data Access at Home3

Security controls to help safeguard sensitive data during wireless transmission from home.

Resources4



onGuard

is published monthly by Native Intelligence, Inc.

www.nativeintelligence.com

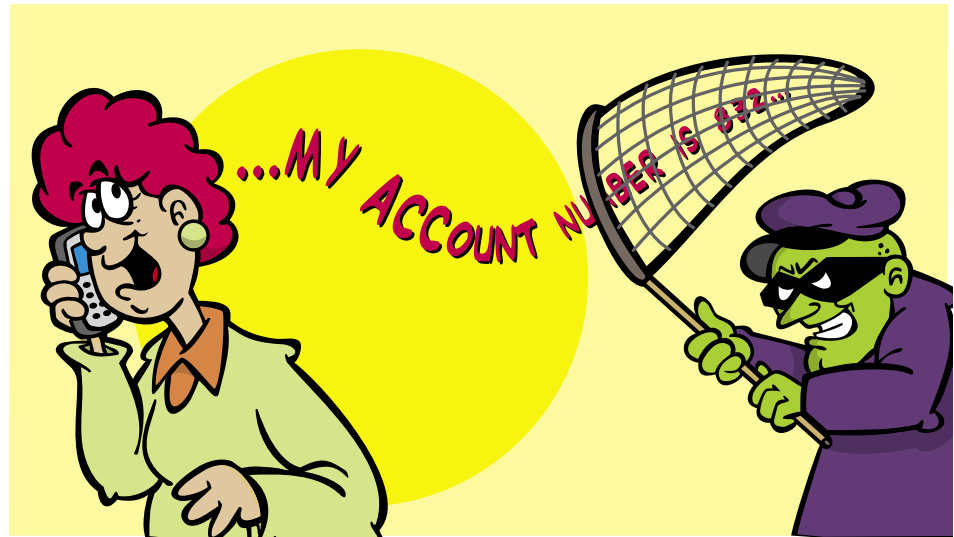
Direct inquiries and correspondence to:

onguard@nativeintelligence.com

© 2006 Native Intelligence, Inc.

onGuard

Focused on Security Awareness, Training, and Motivation



© 2006 NativeIntelligence.com

Wireless Communication: Safeguarding Data in a Mobile World

Wireless communication technology has made it possible for us to access information “on the go” at work or at play – but how secure is the data we transmit and receive?

Wireless laptops, Personal Digital Assistants (PDAs), and Internet-enabled cell phones use radio waves to transmit data. Wireless access points connect wired networks to wireless signals. Access points broadcast and receive radio waves that are picked up by wireless devices (e.g., Blackberries, laptops). Most current laptops have built-in wireless adapters. To add wireless to older laptops and most desktops requires an add-on wireless adapter or wireless laptop card (e.g., an aircard).

Bluetooth

Bluetooth is a wireless technology largely used in the cell phone and

wireless headset markets. Bluetooth is also available in automobiles and wireless computer keyboards, mice, and printers. Bluetooth is designed to connect devices within a short range, for example, from your ear to a cell phone in your pocket. The range can be extended to over a mile with special antennas.

Software programs can allow intruders to identify nearby Bluetooth-enabled devices. If those devices are unprotected, information can be easily stolen over the air. Theft of information over a Bluetooth link is called “Bluesnarfing.” Sending an unsolicited message to a Bluetooth device is called “Bluejacking.”

Bluetooth security is often the responsibility of the user. Users may not be aware that on many wireless devices the security features are not enabled by default.

(see Wireless Communication, page 2)

from page 1

Wireless Communication

NOTE: The courts have held that there is no expectation of privacy with a cordless phone. Do not discuss Confidential Information on a cordless phone.

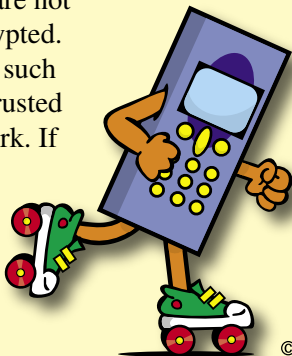
BlackBerry

BlackBerry Personal Digital Assistants (PDAs) use cell phone technology to transmit wireless data. BlackBerries have strong encryption between the handset and the enterprise server. This can protect text messaging and e-mail within our organization.

Wireless Vulnerabilities

Wireless connections are not as secure as wired ones because they do not have the protection of the physical building perimeter. Buildings protect against attack for wired networks because wires have to be physically accessed to make a connection. Wireless networks can be attacked without physical access.

Wi-Fi Hotspots (open access or open networks) — public wireless access, such as at airports, coffee shops, Internet cafés, libraries, and hotels are not Wi-Fi encrypted. There is no such thing as a trusted open network. If you or network personnel did not configure



© 2006 NativeIntelligence.com

the network, and you can't identify everyone connected to it, it's an open network. Whenever you use an open network, others could be reading and using the information you see and send.

Range — many people are unaware of how far their wireless devices and networks can transmit. Wireless adaptors are low-power devices



© 2006 NativeIntelligence.com

designed to have a short range. Radio waves, however, do not care about manufacturer specifications. They just keep going, becoming fainter with distance. Cheap antennas can extend wireless signals to several miles. Remember the words of General John Sedgwick right before he was killed in 1864: "They couldn't hit an elephant at this distance."

Wireless Users — may open backdoors to the private networks. An employee's laptop with a wireless network connection could be plugged into the wired company network while the wireless connection is active. If this happens, the laptop will act as a bridge from the wireless network to the company network. This can allow attackers to bypass the network firewall.

FAST FACTS!

■ Research by Gartner indicates that 64% of businesses expect to increase their wireless network deployments over the next year. Security was one of their top 5 concerns, with 60% of the businesses reporting that they have inadequate security for their wireless environment.

■ Travelers left 85,000 cell phones and 21,000 handheld devices in Chicago taxis during a six month period in 2005.

■ Fewer than 5% of mobile device users voluntarily set password protection, unless they are required to do so by company mandated enforcement.

NOTE: Always disable your wireless adapter before connecting a laptop to the wired network. Contact IT security for support or assistance.

Threats to Wireless

Wi-Fi Jacking — if you do not turn on the security features of your wireless Internet devices, you may be the victim of "Wi-Fi Jacking." This is where criminals walk or drive through business areas (and neighborhoods) and identify unprotected wireless LANs from the street using laptop or handheld computers. When they find an unprotected network, they can hijack that wireless connection to download illegal materials, send spam, etc. This also puts the criminals closer to being able to

(see *Wireless Communication*, page 4)

GRILL YOUR SECURITY OFFICER

I'm concerned about talking on my cell phone because someone might be listening in. Can people tap calls I make from my cell phone?

Older analog cell phones could be heard using a mail order police radio scanner. Today's digital cell phone transmissions are much harder to tap in to. There is a greater risk of someone overhearing your conversation. Many cordless phones are not secure. Especially the ones that use the frequencies 46 MHz or 900 MHz. Their transmissions can be picked up with a radio receiver or even a baby monitor. There is less chance of your call being eavesdropped on if you use a spread-spectrum 2.4 GHz or 5.8 MHz digital phone. Always use a wired landline phone for making confidential calls.

(see Grill Your Security Officer, page 4)

Want to grill us on security issues?...

Send questions to:
grillus@nativeintelligence.com

Securing Wireless Data Access – What You Can Do

Implementation of any wireless network is strictly prohibited without proper authorization. Wireless networks must address specific business needs not currently met by the wired network.

- Do not enable wireless or aircards while connected to internal network.
- Only use wireless access within authorized areas to connect to the public Internet.
- Always disable your wireless adapter before connecting a laptop to the wired network.
- Do not allow visitors to roam around facilities using Wireless LANS. Many Access Points can



© 2006 NativeIntelligence.com

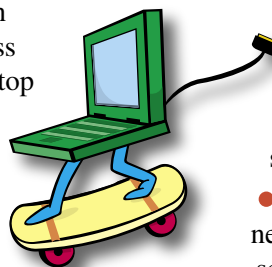
be physically reset to insecure factory default settings by pressing a reset switch on the box.

- If possible, use an encrypted connection or a Virtual Private Network (VPN). Contact IT Security for information on VPNs.
- Avoid connecting to public networks. When you connect to an open wireless network, you should have no expectation of privacy or security.
- If you have to use an open wireless connection, do not visit Web sites that require user names, passwords, or account numbers, such as online banking. Use an encrypted connection or a VPN.
- Turn off your wireless network when you're not using it.

Securing Wireless Data Access at Home

Home wireless LANs are less likely than work LANs to be configured securely. The range of wireless LANs is large enough to expose home networks, even in homes on large suburban lots. Wireless signals do not necessarily stop at the walls of a building. Thus, unauthorized users outside may be able to receive the signal and use your Internet connection. To protect your home wireless connection:

- Place your wireless base station in the center of your home, away from outside walls.



© 2006 NativeIntelligence.com

- Make sure that you have wireless security enabled on your laptops and routers — preferably Wi-Fi Protected Access (WPA). Consult your manual for specific details on these tips.
- Change the default password on your router to a strong password.
- Name your wireless network. In your access point's setup dialog, change the Service Set Identifier (SSID), which is the name of the network typically broadcast by the access point. The default setting is often the brand

(see Securing Wireless Data, page 4)

from page 3

Grill Your Security Officer

What should I do if my BlackBerry is stolen?

Immediately report lost or stolen devices such as BlackBerry Personal Digital Assistants (PDAs), laptops, and cell phones to your supervisor and IT Security. Upon notification of equipment loss, IT Security along with your department must assess the potential exposure of customer or sensitive data. Remember the theft or loss of any equipment containing Confidential Information must be reported immediately.

Remember: REPORT LOST OR STOLEN MOBILE DEVICES IMMEDIATELY!

from page 3

Securing Wireless Data

name of the router. Don't use your address as your SSID.

- Set the access point so that it does not broadcast the SSID. Often, this can be done by selecting a checkbox on the same setup page where the SSID name is changed.
- Turn off your wireless network when you are not using it.
- To be most secure, enable Media Access Control (MAC) filtering on your wireless access point. Add the MAC address (a unique 12-digit number) of each device, e.g., your laptop or home computer, that you want to access your Wi-Fi connection.

from page 2

Wireless Communication

hack into the victim's computer and steal information and identities.

Evil Twin Hotspots — an evil twin is a free, wireless hotspot created by a criminal. The evil twin mimics an Internet access hot spot such as the ones found at airports, coffee shops, and bookstores. Evil twin hotspots look legitimate. People connect to the twin and do online banking and send e-mail, unaware that the criminal is recording their user names, passwords, account numbers, and more.

Mobile Device Viruses — are malicious software that exploit vulnerabilities in Bluetooth, wireless encryption protocols, and other wireless technologies. Mobile viruses target handheld devices, cell phones, and wireless networks. Mobile viruses spread in the same way as traditional computer

viruses: through downloading of infected programs and files such as photos, video clips, ring tones, and cell phone themes. Bluetooth-enabled mobile devices can become compromised when brought in range of an infected Bluetooth device.

Other Threats — include jamming to cause Denial of Service (DoS) and sniffing. Jamming can be on purpose

or by accident. The presence of other devices, such as cordless phones, that operate in the same frequency as the wireless network can cause jamming. Sniffing is a passive attack that occurs when someone listens to or eavesdrops on network traffic. Use encryption to defend against sniffing on a wireless network.

Protecting Data Through Wireless Encryption — WEP and WPA

One of the most common ways to encrypt wireless communications is Wired Equivalent Privacy (WEP).

WEP is an older specification that is fairly easy to break with programs available on the Web. Wi-Fi Protected Access (WPA or WPA2) is much more secure, but not all Wi-Fi equipment supports WPA.

NOTE: Encrypted data can be susceptible to decryption. There is no guarantee that your transmission has not

been recorded and decrypted later. Because of this, some data is too sensitive to send over wireless connections. Check with IT Security if you are unsure whether your data can be safely sent over wireless.

VPNs and SSL also provide encryption. Ask IT Security for help with encryption. 🔒



© 2006 NativeIntelligence.com

October 2006:

Newsletter will focus on –
Business Continuity

Security Awareness Resources

For more information on workplace security awareness, visit:

<http://nativeintelligence.com>