

INSIDE:

CBI Web Site
Spotlight:
www.mcgreal.com

Web Sites You
Can Use

The CBI System
Review:
A Management Tool

CBI Becomes
eSoft VAR

CBI Payment
Options
Expanded

CBI Now A
WORLDOX
Systems
Integrator

Windows 2003
Server Ships

Bits You Can Use...

FALL | 2003

Kicking Down Your Wireless Doors

BY SCOTT ELLIS, CONSULTANT
PART 1 OF 2

The number of wireless users is expected to number 4.2 million this year, and will increase to more than 31 million by 2007, a recent Gartner study says. There are several factors behind the surprisingly steep increase. This article will shed some light on each reason.

The Truth

Many IT purchasers, planners, and managers are being confronted with an array of networking solutions embracing wireless technologies. cursory research on the web yields mind-boggling results and only increases indecision. This article has gone beyond the cursory, both in research and experience, to bring in-depth analysis of wireless technologies and explanations of terms, implementations, limitations, and solutions. When making any potential investment in wireless technology, consider this:

- The seemingly best available product today will not be the choice of tomorrow.
- Current information about industry developments is unusually obfuscated and conflicted.
- The landscape of wireless is undergoing upheaval now, in the latter part of 2003.
- Wireless investments today may very well be completely worthless within a year.

Considering these points, and in a knowledge vacuum, how do IT managers make these decisions? In most cases, the two factors that the decision are likely to be based on are cost and compatibility. Wireless can allow for quick, and inexpensive, expansion, especially in a marketplace where in terms of ROI, expansion can be costly.

However, is wireless really the golden cure-all it is cracked up to be, or is it a symptomatic, palliative treatment that is ineffective as a long-term solution?

Darkness Falls

To answer that, first we must understand that never has there been such a free-for-all in the subculture of the hacking and cracking community as is provided by wireless networks. Rarely has there been such rampant corporate blasé towards flawed products. However, their foot shuffling movement (or "Market

Glossary of Terms:

AP/WAP: Access Point/Wireless Access Point

WEP: Wired Equivalent Privacy

SSID: Service Set Identifier – this is the encrypted password attached to wireless network packets.

IEEE 802.11b: Wireless communication standard

IEEE 802.11i: Wireless Standard (still in review) to host WPA technology

Wi-Fi: Soft name of IEEE 802.11x - undoubtedly invented by marketing agencies in late 2002 as a response to the cute "Bluetooth" standard

WPA: Wi-Fi protected area - boasts high security

Bluetooth: Competing wireless RF standard that has some overlap with Wi-Fi market share

IPSEC: Encryption protocol used with VPN "tunnels"

MAC: Media Access Control

Chimera: Mythological creature made up of pieces of real creatures - doesn't really exist

Repositioning") has been remarkable.

What, you ask, then, is being SO neglected and fascinates the elements of darkness? You've probably already guessed it - security. Wireless networks, when hastily or unprofessionally installed, are a computer hacker's playground.

A wireless network in a bank branch office or the office of a financial institution where large amounts of money are transferred, balances change frequently, and account numbers are flowing freely is a bad idea. In a sales office where salespeople are in and out with their laptops, meet remotely, need to form ad hoc networks, and aren't passing overly sensitive information is not such a bad idea, provided that the proper system security protocols are in place.

War Driving, Walking, and Chalking, Under Cover of Darkness

There exists, already and profusely, and probably in your community, a practice called *war driving* in which youngsters (and probably overgrownsters as well) assemble a device comprised of a laptop, a PCMCIA wireless Ethernet card (about \$70), and a homemade (Pringles can) or purchased antenna. They then get in their car, and drive or walk about

continued on page 2

Kicking Down Your Wireless Doors

continued from front page

town to tally, map and chalk special symbols on your sidewalk or alley wall regarding your network.

One *war driver*, whose name shall remain anonymous, posted the following on his website:

“The equipment [sic] for this project (laptop excluded) cost under \$200 US.

Tools to sniff wireless networks and reconfigure a wireless card’s mac address are freely available [sic]. Using AirSnort I could have broken half of the remaining 35 networks encryption keys. Security on wireless networks can be done correctly using 128 bit WEP encryption, MAC filtering and an IpSEC implementation. However, unless all three elements are in place, breaking into wireless networks is far easier than taking candy from a baby. Park, crack in, drive away.”

Unfortunately, he’s 100% correct. A network built to IEEE 802.11b wireless, without all three measures in place, is at varying degrees of risk and can be rather easily accessed by anyone with

the right tools, the right software, and the wrong motivations.

Amelioration

802.11b comes with its own set of so-called security tools, none of which are activated by default when the network is installed. These tools are WEP and MAC filtering which, when used in conjunction, will stop most war drivers but won’t stop a deliberate attempt at intrusion. Most war drivers are curiosity/thrill seekers curious to learn how many people leave WEP turned off. They consider themselves a public service/nuisance, operating without mandate.

Largely, in part due to this, many clients and their consultants are currently operating under the false notion that, if WEP is enabled, their wireless networks are secure. Most war drivers won’t waste their time cracking into a WEP enabled network. WEP security is based on a static key that is passed between the host and the client and, because of the way that key information is passed between computers,

security cannot be assured unless there are multiple layers of security in place. Much like the lock on your house, it only serves to keep the amateur burglar out. One or two swift kicks will open most doors.

For those who don’t at least have WEP or MAC filtering in place, your network is exceedingly at risk of penetration. All you have to do to gain access is be in range with a laptop that has a wireless card and it will practically attach itself to the network for you. The receiver will search for a wireless network, and tell you the SSID. You then only need to double click your choice, and you are connected.

The Downfall of WEP

Administrators and networkers who have ostensible familiarity with 802.11b wireless networking may be wondering, “What’s wrong with WEP? What makes it so weak?”

First, this is what WEP is: when WEP is used, authentication can take place using either open system or shared key (WEP) methods. To be associated with an AP implies that the client is fully connected to the AP and is now allowed to pass traffic through the AP. In short, the computer, or “client,” now has complete access to the rest of the network, both wireless and wired.

Second, this is why it is weak: In 2001, Scott Fluhrer, Itsik Mantin and Adi Shamir published a paper titled “Weakness in the Key Scheduling Algorithm of RC4.” This paper outlined a method for pulling up the master WEP key that would allow a hacker to pose as a legitimate user of the network. Summarized, it boils down to this: by capturing challenge frames and successful response frames, a listener can derive a keystream that will successfully decrypt future challenges. There is a countermeasure, a type of check built in to prevent this sort of attack, but it is based on the Cyclic Redundancy Check (CRC) mechanism that many data-link protocols use, and CRC doesn’t depend on a cryptographic key, so it’s easy to get around this obstacle.

It didn’t take long after that before a piece of software called “AirSnort” appeared on the Internet. This software can detect the WEP master key within seconds after listening to enough network traffic. Maybe now you’re thinking, “I can’t even get my wireless to reach into the next room with the

continued on page 5

Bluetooth Wireless

No discussion of wireless technologies would be complete without also addressing the concerns of those who have wireless networks built upon the Bluetooth standard. Just like Wi-Fi built upon 802.11b, Bluetooth can cause network administrators serious headaches due to inherent security flaws. But unlike 802.11b, the standard is not the source of the flaw. Rather, it is a result of the improper setup and use of existing security configurations. Inherently, Bluetooth can operate in several security modes:

- Security Mode 1- This is the most promiscuous mode. When operated in this mode, a device is passive, and allows other devices to establish control. Slaved to initiating devices, it will not initiate any security measures.
- Security Mode 2- This mode enforces security after establishment of the link between the devices. It allows for the creation of flexible security policies.
- Security Mode 3- This mode enforces security controls such as authentication and encryption at a level called the “baseband” level. 802.11b offers little or no encryption at its comparable level.


As with any wireless technology, Bluetooth operates at 2.4 GHz—this is the only frequency range that the FCC will approve. Bluetooth devices range 32 feet (10 meters) but this may vary depending on manufacturer and equipment and with a transfer rate of 1 Mbps. This is faster than parallel and serial ports, but is 10-100 times slower than twisted pair network cable.

Due to its low speed (higher encryption means slower speeds!), Bluetooth is generally more useful in environments where mobility is the greatest concern. Bluetooth products include USB wireless devices, jacket slots for PDAs, USB scanners, wireless car kits (for cell phones), and pocket PCs. 3Com, Nokia, Toshiba, Palm, Compaq, and Intel are all members of the Bluetooth consortium SIG.

CBI Web Site Spotlight:

www.mcgreal.com

In this edition of *Bits You Can Use*, our CBI Web Site Spotlight focuses on the web site of one of our clients, McGreal Johnson & McGrane (MJM). MJM is a progressive CPA and business consulting firm located in the southwest suburb of Oak Lawn, IL. They have been a CBI client for almost eight years, and they are also CBI's accounting firm.

Although they have had a web site up and running for some time now, MJM recently decided that they would like their site upgraded so that it contains increased functionality and additional valuable information for visitors. After receiving that directive, CBI web consultants dug in, and the finished product can now be seen at www.mcgreal.com. Note the plethora of technical information available on the site, including a newsletter archive loaded with usable information, a federal and state tax refund tracking utility, multiple finance calculators for assistance with various analyses, and more. 

McGreal Johnson & McGrane is located at 5740 W. 95th Street in Oak Lawn. They can be reached by phone at (708) 422-8600.

Web Sites You Can Use

Technical

www.f-secure.com/virus-info/hoax - A comprehensive list of virus hoaxes

www.edu.com - Vastly discounted software for students

www.pestpatrol.com - Contains an anti-hacking utility that detects and removes hacker tools, spyware, and trojan horses

www.consumerreports.org - Independent reviews on products across many industries

www.networksolutions.com - After accessing this site, click on "Whois" (at the top of the page) and enter a URL address for site registration information.

Bandwidth Meters

www.testmyspeed.com/speedtests/illinois.htm - Test your internet speed by state

<http://webservices.cnet.com/Bandwidth/> - Test your internet speed

www.2wire.com - Test your internet speed, and find faster ways to connect.

Study Help

www.sparknotes.com - Literature reviews and study guides

www.emule.com/poetry/ - Poetry archives to help students

home.planet.nl/~napel/roman.htm - Roman numeral translator

www.onelook.com - Online "umbrella" dictionary that searches multiple sites for results

www.webopedia.com - Technology dictionary

Fun/Misc.

www.ojbmusic.com - Home site for a popular local jazz band

www.truthorfiction.com/search.htm - Get information about eRumors, warnings, offers, requests for help, myths, hoaxes, virus warnings, and humorous or inspirational stories that are circulated by email

www.snopes.com - Find out the truth behind that urban legend

www.census.gov/statab/www/ - Statistical data on the U.S.

www.chicagoplays.com - Information on plays that are currently being produced in Chicago

www.anywho.com/ri.html - Reverse lookup for phone numbers in the Chicagoland area

www.metromix.com - A roundup covering the Chicagoland entertainment/nightlife scene

www.bls.gov/oco - Occupational outlook handbook (useful if you are interested in how much others in your field are making)

www.donotcall.gov - National registry where individuals can submit a request to have their names taken off telemarketing lists

The CBI System Review: A Management Tool

Q:


How do I know if my network technology is current, secure, adequate and ready for future enhancements and updates?

A:

**Sign up for a CBI
System Review!**

The question above, or a variation of it, is one that we here at CBI hear over and over again in our daily work. Many network administrators, office managers, executives or business owners know that they have a network in place, but aren't necessarily sure if their server is up to date, if they have the most appropriate operating systems on their workstations, if their data is being backed up and stored in a proper manner, etc. There are so many components of today's modern network that, at times, it can be difficult to be sure that each one set up in an optimal and effective manner.

If you have wished at times that you could have an expert examine your network and assess its current state, as well as make enhancement suggestions for the future, the CBI System Review may be exactly what you've been looking for. This management tool includes a formal on-site review of your current network, after which a report is generated that provides the following information to the client: Software Inventory and Analysis; Hardware Inventory and Analysis; and Administrative Analysis.


The purpose of the CBI Review is to give your organization a snapshot of where your network stands at the present, as well as to provide a roadmap regarding the future. When you hire CBI to perform a System Review, you will know what needs to be done in the short-term, as well as the long-term, to make sure that your network remains capable, safe and operational. 

If you are interested in a system review for your organization, please contact Mary Beth Sheehan at (312) 399-7505 to make arrangements.

CBI Becomes VAR for eSoft/ InstaGate, Offers Free Seminars

Computer Bits, Inc. was recently named a VAR for eSoft. Founded in 1984 and based in Broomfield, Colorado, eSoft strives to provide small and mid-sized enterprises with the most sophisticated network security solutions available in the simplest possible way.

eSoft's main product offering, the InstaGate line, delivers next-generation Internet security appliances that integrate all the security tools and services that organizations need on one extensible platform, reducing the time and complexity required to mount an effective defense enterprise-wide. With services like intrusion detection and prevention, firewall protection, anti-virus, centralized VPN management, web site and content filtering and more, eSoft solutions ensure a high degree of customization and scalability while reducing the costs and complexity typically associated with maintaining an effective network security system.


As security becomes an ever-expanding challenge in today's workplace, CBI is now better prepared than ever before to assist your organization in that arena. For additional information on the InstaGate product line or to sign up for our free October 1st or November 12th "Introduction to InstaGate" seminar, please contact Mary Beth Sheehan at **(312) 399-7505**, or Rich Larsen, Certified eSoft System Engineer, at **(708) 275-0907**. 

CBI Payment Options Expanded

There is now a new payment option available from CBI. In addition to choosing either to pay our standard hourly billing rate or enroll in one of our Prepaid Professional Services Plan, clients now have the opportunity to choose our “Pay As You Go” option.

Under “Pay As You Go”, a client commits to purchase a minimum number of CBI service hours every month for at least a year, and in return receives a discount on our time. The minimum number of hours a month is 10, which yields a 5% discount to the client. If the client decides that they need more assistance and requires 20 hours a month or more, the discount rises to 10%.

The client is billed at the beginning of each month, with that month’s hours being deposited into an account. Hours used during the course of the month are subtracted from the account balance. If a client’s balance rises to more than twice their monthly purchase commitment, an invoice will be generated in order to bring the balance back down to zero.

Experience has clearly taught us and our clients that the best-maintained networks and equipment are the most effective networks and equipment. Therefore, we strongly encourage any “Pay As You Go” clients to use their monthly allotment to schedule regular maintenance or project visits (e.g., every Monday for four hours, first Wednesday of the month for a full day, etc.). 

** Just a reminder that CBI now accepts Visa, MasterCard and American Express.*

Kicking Down Your Wireless Doors

continued from page 2

door closed, therefore nobody outside will be able to see me.” Wrong. That weak signal travels infinitely into space (just like any electromagnetic wave) and as long as you have the correct antennae (such as a 14dB yagi), you’ll catch it at up to a few hundred yards and, if you go with a parabolic dish antennae, miles.

MAC Addressing - Answer To WEP Insecurity?

Every computer that attaches to a wireless network has a MAC address assigned to it. MAC filtering is the process whereby an access point (AP) is configured with a list of MAC addresses that will be allowed access to network resources. Addresses not on that list are not allowed access.

Gee, sounds like a great idea. Right? The answer to the problems with WEP, right? Sorry. While most war drivers will be stopped by the proper configuration of the WEP, networks without WEP enabled and relying only on MAC are asking for trouble. If MAC is not used, the wireless network “sees” the rogue and the rogue “sees” the network. If MAC filtering is used, the process is much less mutual, the signal will take longer to be sniffed out, and the key won’t be as easy to get. Unfortunately, MAC addresses are transmitted in the clear, so a wireless protocol analyzer can pick them up immediately and attach itself to the network as if it was a legitimate, wired computer.


With AirSnort handling the decryption, any laptop with a PCMCIA wireless Ethernet card can, through a simple registry edit, be reconfigured to any MAC address at all, even with WEP and MAC configured properly. The directions on exactly which key in the registry needs to be altered are easily found on the Internet.

Now, if concern is still lingering (possibly growing), there have been wireless networks setup and run with as much security as one could expect to attain. This is done through the creation of network, encrypted tunnels, or VPN connections, which are known to be secure. VPNs are a firewall technology, and can be complicated to implement and tend to need some maintenance. If your network needs a high level of security, then you should consider VPN technology to protect your wireless data.

Alternatively: Wi-Fi WPA, Coming Soon

Wi-Fi, the name now commonly being used to refer to the 802.11x standard, has undergone a transformation to improve the security and maintain the high rate of data transfer that has made it so popular (despite the security flaws). Starting this Fall and by the Spring of 2004, all Wi-Fi devices will boast functionality that supports the Temporal Key Integrity Protocol (TKIP), also known as WPA (Wi-Fi Protected Areas). By incorporating a mutable key, which provides strengthening corrections, WEP (IEEE 802.11i standard) is strengthened. However, for reasons of backward compatibility, the encryption cannot be stronger than 20bit. This is pretty weak, so it is shored up by some countermeasure utilities. Unfortunately, these countermeasures are like the antitheft devices on cars. As such, wireless networks will be increasingly vulnerable to other types of attacks, such as Denial of Service, that can be launched from a single laptop using relatively innocuous software—software that is commonplace and does not incriminate by virtue of having it. 802.11b, of the WPA flavor, is simply a new hole for hackers to exploit.

The End

Ultimately, regardless of the standard implemented, the security of the network will depend on the proper configuration of things such as WEP, WPA, or security levels in Bluetooth (see sidebar article). Many of the war driving web sites described an overwhelming majority of network locations that had no security enabled at all. Aside from the inherent weaknesses in all the technologies being used to create a communication network, nothing will do more damage than failing to properly configure security settings, install firmware updates (when available), ensure product compatibility, and ensure that neither users nor intruders can alter security settings. The risk with 802.11b is high. Without VPN tunneling, there is no question that you are basically driving your business down the autobahn at 150 mph with no insurance, no seatbelts, no airbag, and the top down. 

Part 2 will be published in our next newsletter.



134 N. LaSalle St.
Suite 408
Chicago, IL 60602

PRSRST STD
U.S. POSTAGE
PAID
Buffalo Grove, IL
Permit No. 518

CBI Now A WORLDOX Systems Integrator

Computer Bits, Inc. was recently named a WORLDOX Systems Integrator by World Software Corporation, headquartered in Secaucus, NJ. WORLDOX is a multi-award-winning document management system that incorporates both document management and e-mail management. WORLDOX's unique SQL-free software is currently installed in over 2,500 companies worldwide, over 2,000 of which are law firms and legal departments.

WORLDOX works on Windows XP, 2000, 98, 95, NT or Novell, and is tightly integrated with Microsoft Office, Corel/WordPerfect Office Suites and other products. WORLDOX is installed directly onto your file server. The only additional hardware requirement is a dedicated PC for indexing.

For more information on WORLDOX, please contact Mary Beth Sheehan, Business Development Manager, at (312) 399-7505 (cell).

Free "Introduction To WORLDOX" Seminars Coming In September and October!

CBI is pleased to announce that we will be hosting two "Introduction To WORLDOX" seminars. The seminar information is as follows:

What: "Introduction To WORLDOX" seminar

When: Wednesday, September 17, or Wednesday, October 15, 2003, 9:00 A.M. – 11:30 A.M.

Where: Computer Bits, Inc., 134 N. LaSalle St., Suite 408, Chicago, IL, (312) 849-3813 (office phone)

RSVP: Mary Beth Sheehan, (312) 399-7505 (cell)

Includes: A brief discussion of document management system capabilities and a live demo of the WORLDOX program, to be followed by a question and answer period.

Presenter: James Harmening, President, CBI

Cost: Free of charge

Seating is limited, so please contact us ASAP if you are interested in joining us!

Windows 2003 Server Ships

Microsoft recently began shipping their new Windows 2003 Server product. CBI consultants will be testing and evaluating this product over the coming months, and we will begin recommending it to our clients once it has been proven in the marketplace.

Please watch this space in future newsletters for more information on Microsoft's latest network operating system offering.