Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 5, No. 3. March, 2003

In the News: Cellphone Denial of Service Attack

A Denial of Service (DoS) vulnerability has been exposed in a European GSM (900/1800 MHz) phone, the Nokia 6210. Its vCard (an electronic business card in the IETF RFC 2426 format) can cause the phone to lockup or reboot. This occurs when a vCard contains format strings which are not correctly processed by the SMS software.

DoS attacks such as this one are annoying, but not serious. No user data is compromised, and no permanent damage occurs to the phone. The phone may stop receiving SMS messages, may automatically restart or, at worst, may need to have the battery removed before restarting. According to @stake, Nokia has no plans to issue a software fix for the problem. Although this attack is not very serious, it does illustrate the new avenues for security attacks with the increasing sophistication of wireless devices.

A Bugtraq report on this is at:

www.securityfocus.com/bid/6952

Huh?

If there are any acronyms or terms you are unfamiliar with, check our website glossary. You will probably find them there.

www.cnp-wireless.com/glossary.html

Securing WLANs with Location-Enabled Networks

Chuck Conley, Newbury Networks

Growth in the wireless LAN (WLAN) market continues to be driven by the corporate and educational sectors, where increased productivity is one of the main selling points. In fact, a recent study commissioned by Cisco Systems found that in companies implementing WLANs, employee productivity rose as much as 22%.

However, those benefits and the enterprise market's potential are both at the mercy of Wi-Fi's Achilles' heel: Security. To address this, the IEEE 802.1x protocol was developed to provide a framework for a more reliable security solution for 802.11-based WLANs. Although 802.1x offers a centralized, server-based authentication approach for end users, it does not solve all of the security issues an organization will face with a WLAN. The promise of ubiquitous access and freedom to perform tasks traditionally confined to an office can still become a logistical and security nightmare for any IT organization deploying a WLAN.

The drive for increased productivity remains, despite the shaky security aspects of WiFi. Apparently, the industry is confident these problems will be solved. Intel's introduction of the new Centrino chipset, which will soon embed 802.11b in laptops from Dell, Fujitsu, Gateway, IBM, Toshiba and others, seems to demonstrate this

About Wireless Security Perspectives

Price

The basic subscription price for *Wireless Security Perspectives* is $350 for one year (12 issues) for delivery by emailed PDF file or by first class mail within the US or Canada. International subscriptions are US$400 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees to allow more readers.

We provide discounts to educational institutions and small businesses (less than 10 employees).

Back issues are available individually, or in bulk at reduced prices.

Delivery is by first class mail or by email (Acrobat PDF file).

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due…

April 24th, 2003.

Future Topics

Wireless Flash Memory Security • Radius for Wireless • 3G Security • Public Keys & Wireless • Security for Mesh Networks • 802.11 Wireless LAN "Hotspot" Roaming Security • Security Issues in Ad hoc Wireless Networks

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary, Alberta T2N 3W1, Canada. **Phone**: 1-800-633-5514 (+1-403-274-4749) **Fax**: +1-403-289-6658 **Email**: cnpsales@cnp-wireless.com **Web**: www.cnp-wireless.com/wsp.html **Subscriptions**: $350 for delivery in the USA or Canada, US$400 elsewhere. **Payment**: accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery**: Email or 1st class mail. **Back Issues**: Available individually for $35 in the US and Canada and US$40 elsewhere, or in bulk at reduced rates. **Discounts**: Educational and small business discount: 25% off any order. **Copies**: Each subscriber is licensed to make up to 10 copies of each issue or back issue. Call for rates to allow more copies.

Technical Editor and Illustrator: Les Owens.

Article Sourcing:	Tim Kridel.
Production:	Doug Scofield.
Distribution:	Debbie Brandelli.
Accounts:	Evelyn Goreham.
Publisher:	David Crowe.

confidence. A further indication of the industry's perspective is shown by the fact that the number of WLAN deployments in the United States doubled between August 2001 and August 2002, according to the Yankee Group. That report also found more than 1 million wireless access points are in use by more than 700,000 enterprises.

Meanwhile, Windows XP – when it is used with a device having an embedded NIC (Network Interface Card) – includes the ability to detect 802.11 networks automatically. That ability makes it more convenient to log onto the corporate network, but it is also easier for careless users to pick another network by mistake, and these users are unlikely to consider the associated security risks involved.

The combination of WLAN proliferation and log-on ease yields increased potential for unauthorized users gaining access to networks, along with greater potential for exposure to security breaches. Basic security measures — such as requiring passwords to access files and other sensitive data — can limit damage from unauthorized users, and usually their impact would be nothing more than a monopolizing of the bandwidth and reduced performance. Yet, a sophisticated hacker still has the potential to gain full access to everything the network supports.

WLAN Vulnerabilities

Although the 802.11 standard supports some basic security processes and protocols such as WEP (Wired Equivalent Privacy) and MAC (Media Access Control) address filtering, WLAN vulnerabilities are compounded by the fact that the IT organization has very limited detection capabilities.

In a traditional wired network, every laptop accesses the network through a designated port. Locations are known, and testing or troubleshooting such a system is relatively simple. In a typical WLAN, however, it is impossible to determine the precise location of the user (e.g, wireless client) or network equipment (e.g, access point or router).

Upcoming Wireless Security and Fraud Conferences & Events

The following are upcoming wireless, wireless security and general security conferences and events that may be of interest to our wireless security and network security practitioners.

2003 SecurE-Biz Summit
1st – 2nd April 2003
Hilton Crystal City
Arlington, VA
www.secure-biz.net/index.html

13th Annual Conference on Computers, Freedom & Privacy
2nd – 4th April 2003
New Yorker
New York, NY
www.cfp2003.org

Workshop on Issues in the Theory of Security (WITS '03)
5th – 6th April 2003
Marriott Hotel Lisbon
Warsaw, Poland
www.dsi.unive.it/IFIPWG1_7/wits2003.html

In-building 2003
7th – 10th April 2003
Marriott Hotel Lisbon
Lisbon, Portugal
www.iir-conferences.com

SANS Inner Harbor 2003
7th – 12th April 2003
Sheraton Inner Harbor Hotel
Baltimore, MD
www.sans.org/innerharbor03

Broadband Wireless World
9th – 10th April 2003
McEnery Convention Center
San Jose, CA
www.shorecliffcommunications.com

RSA Conference 2003
13th – 17th April 2003
Moscone Center
San Francisco, CA
www.rsaconference.com/conf2003_portal.html

InternetWorld Essentials
14th – 17th April 2003
San Jose Convention Center
San Jose, CA
www.internetworld.com/events/spring2003

ISPCON 2003
23rd – 25th April 2003
Baltimore Waterfront Marriott
Baltimore, MD
www.ispcon.com/spring2003

CDMA 2000, Wireless VPNs, Wireless Security
24th April 2003
Westin Hotel San Francisco Airport
San Francisco, CA
www.pcca.org/news/Agendas/ag02-04.htm

2nd Annual PKI Research Workshop
28th – 29th April 2003
National Institute of Standards and Technology
Gaithersburg, MD
www.nist.gov/public_affairs/confpage/new030428.htm

The Fifth Annual International Techno-security Conference
27th – 30th April 2003
Wyndham Myrtle Beach Resort
Myrtle Beach, SC
www.techsec.com/html/Techno2003.html

2003 Workshop on Mobile and Wireless Networks
19th – 22nd May 2003
Brown University
Providence, RI
cs.ua.edu/mwn

Wireless Connections 2003
29th – 30th May 2003
Rozsa Centre
University of Calgary
Calgary, Canada
www.wirelessconnections2003.com

An unauthorized client or device can access the WLAN via any compliant 802.11 network interface card (NIC) associated with the network. Without the system administrator knowing when it occurs, the network identifier – coming from any of the network's access points – can be broadcast to anyone within range. If, for instance, unauthorized access is gained via an intercepted network identifier, and if the connection is then used for downloading large audio or video files, the network bandwidth and performance can be reduced or saturated, which could limit or exclude authorized users (employees, for example) from using their company's network. Given the bandwidth constraints of the WLAN, an IT department is handicapped if it attempts to resolve such problems, as they cannot determine *what* and *where* the problem is and *which* equipment is the cause.

Four Common Security Breaches

A campus or an office environment commonly experiences the following four security breaches:

- **Rogue Access Points.** An employee or hacker can connect an off-the-shelf access point – a rogue access point – to an open port in a wired network. This broadcasts corporate network access – possibly including mission-critical data or sensitive information – to anyone with an 802.11 client device, authorized or unauthorized. In most cases, the employee does not understand the security implications of this set-up. They are merely looking to enjoy the benefits of mobility while remaining connected to the network.
- **Ad Hoc Mode.** Ad hoc mode can be handy for spontaneously creating a WLAN. But, although establishing an ad hoc network is great for smaller, peer-to-peer groups, it can also pose a security problem. When an employee's laptop network card is put into ad hoc mode, it also opens a gateway to data on the laptop, as well as to the network to which it is connected. Worse yet, the user could easily be unaware the network card being used is in ad hoc mode. Regardless of whether ad hoc mode is chosen deliberately or accidentally, a casual network snooper or hacker may be able to connect, via this laptop, to the corporate network.
- **Connection Hijacking.** Similar to the rogue access point scenario, a hijacker can connect an access point to their laptop, with DHCP (Dynamic Host Control Protocol) bridging, but with no WEP capabilities turned on. This can cause havoc on an internal network. Employees connected to a wired network might connect wirelessly to this rogue access point for some time before determining that it is rogue (as it will not give them access to their corporate network). For the duration of this connection, the hijacker is given access both to their systems (through Network Neighborhood) and to their wired network (over the bridged connection).
- **Neighborhood Nuisance.** When an employee's laptop is connected to a wired network, and when its wireless connection connects with an access point at a business across the street, network security at the employee's work site is also at risk. An intruder can bridge this connection between the laptop and the neighboring corporate network using basic system utilities in Linux or Windows XP. Having this type of bridge established, the neighboring business can easily log on to the employee's laptop, and it could possibly connect to the employee's corporate network.

In each of these cases, IT personnel and corporate security analysts should implement processes and company-wide education to minimize the security risks. However, those actions do not help if simple log-on errors occur and if hackers work against conventional security practices.

Enter the Location-Enabled Network

Location-enabled networks (LENs) are a new breed of network technologies and services designed to meet these network security challenges. They are a breakthrough approach to help organizations manage their WLAN deployments by managing the locations within the wireless network. This brings numerous business and operational efficiencies to corporate campuses.

Figure 1 illustrates a comparison between a typical WLAN and a network including deployment of a LEN.

The core component to a LEN is the *locale*, which is a contextually-defined location or space within the wireless network, such as conference rooms, offices, cubicle areas, lobby or even an area outside the building, such as a parking lot. One helpful analogy is to think of LENs as creating virtual sub-nets for specific physical areas. Each sub-net is a locale.

Locale resolution is between 2 to 3 meters (6 to 10 feet). In other words, the *actual* location of a network device, for example, is frequently 2 to 3 meters from the LEN-reported location of it.

Being defined by its context within the structure of the organization where a LEN is deployed, any given locale may be set up to offer or push – to authenticated users – a variety of applications, depending on the user's location. Applications can include web or intranet access, streaming video presentations, interactive applications, and dynamic content (e.g., Instant Messaging). Provisioning can also offer location querying to allow users the ability to find other users within the scope of the LEN's coverage, or to find fixed or moveable items, such as a printer or the nearest rest room.

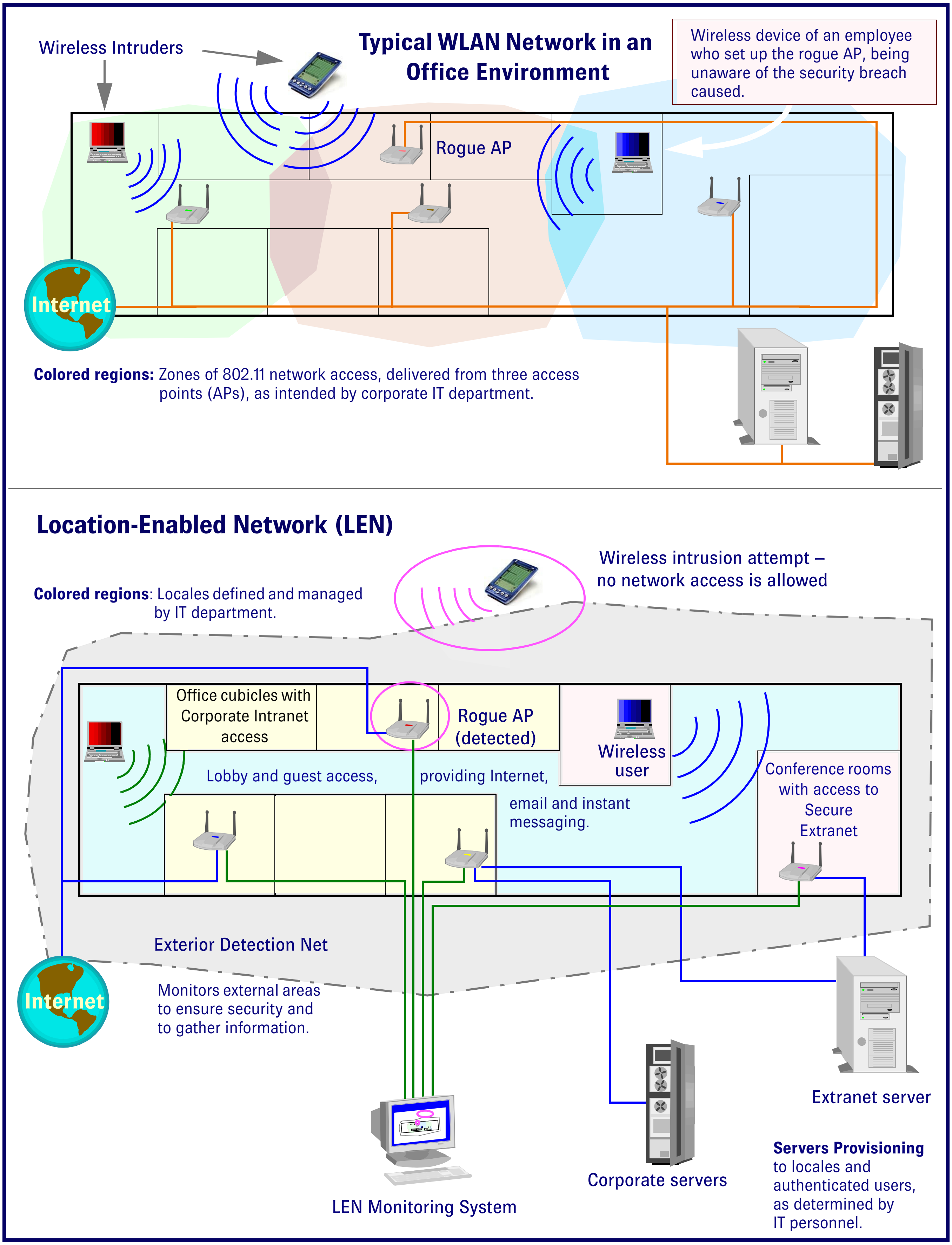
A LEN's value is in securing the information or content available within its locales. This is achieved through avenues of user authentication, detection, and reporting. For example, placing a (virtual) exterior detection net around the office to secure the wireless signal broadcast from the network is one way to detect unauthorized users before they penetrate the corporate network.

The position of each device is based on the signal strength of one client as received at multiple access points, processed by a specialized triangulation algorithm. GPS is not currently applicable, as few client devices have this capability and the relatively small footprint of access points makes triangulation more competitive than in wide-area wireless, where cells can be several kilometers across.

Closing the Gaps

The core features in a LEN provide a means for addressing the challenging issues in a typical WLAN security breach. In general, good security would provide a sensing system, a warning system and a data storage and reporting

Figure 1: The Security Challenge of WiFi: WLAN versus LEN


Typical WLAN Network in an Office Environment
Wireless Intruders
Wireless device of an employee who set up the rogue AP, being unaware of the security breach caused.
Rogue AP
Internet
Colored regions: Zones of 802.11 network access, delivered from three access points (APs), as intended by corporate IT department.
Location-Enabled Network (LEN)
Colored regions: Locales defined and managed by IT department.
Wireless intrusion attempt – no network access is allowed
Office cubicles with Corporate Intranet access
Rogue AP (detected)
Wireless user
Lobby and guest access,
providing Internet,
email and instant messaging.
Conference rooms with access to Secure Extranet
Exterior Detection Net
Internet
Monitors external areas to ensure security and to gather information.
LEN Monitoring System
Corporate servers
Extranet server
Servers Provisioning to locales and authenticated users, as determined by IT personnel.

system. An IT department can analyze the issues within a network with a deployed LEN, because they have access to information such as:

- **Monitoring 802.11 Traffic.** Security administrators can know the precise location of authorized and unauthorized user traffic on a WLAN. This can provide unprecedented security capabilities to an organization.
- **Intrusion Detection.** Whenever an unauthorized device or user is identified in a WLAN environment, the system or network administrator can be immediately alerted. Immediate action is important, since the best protection occurs when the intruder is quickly shut down.
- **Rogue Access Point Detection.** Merely detecting a rogue access point (AP) on the network will not always solve the problem, because one would still have to find where it is located. LEN's location-based rogue access point detection capability can go a long way toward solving the problems, regardless of whether they were set up by an employee or a hacker.

  One company cited Rogue APs as the major reason they decided to deploy LEN technology.
- **Usage Traffic Patterns.** Security at a corporate campus can greatly improve, since the IT administrator can highlight patterns in public-access areas, including the location and movement of strangers or undesirable guests.

LENs provide data analysis capabilities to support the reporting necessary for a better understanding of office or campus trouble spots. Yet, there is even more reason for confidence while using a WLAN with LEN technology.

LENs' Additional Layer of Security

LENs provide an additional layer of security by complementing existing (802.11-based) and emerging standards such as WEP (Wired Equivalent Privacy), WPA (WiFi Protected Access) and RSN (Robust Security Network). In many cases, LENs provide the most important layer of security because often, standard features such as WEP are not turned on.

A WLAN secured with current or emerging standards would not achieve the enhanced security LEN components can provide, which are:

- **Network Provisioning by Location.** LENs can deliver network access based on location and user privileges. Through integration with a corporate RADIUS or 802.1x server, network administrators can facilitate the granting or denying of access based on *where* the employee is located, in addition to information supplied about the user's identity. The lower portion of Figure 1 illustrates two denied intrusion attempts (one staged from a PDA and the other from a red-screened laptop).

  With this level of network security, administrators can also provide the convenience of access to the closest network services and devices, such as printers or fax machines available in secured locations of the office.
- **Wireless Location Tracking and Monitoring.** Using location as another input to authentication, as provided in LENs, can be a powerful security component. For example, network administrators can create authentication policies based on a user's location trail (e.g., parking lot or outside lobby). If it is clear that the user spends large amounts of time in unauthorized public areas, that user's device can be shut off from the wireless network immediately.
- **Location-Based Logging and Analysis.** Delivering critical information on space usage, employee traffic patterns and 802.11 device movement are just some of the valuable benefits LENs offer IT personnel. Whether it is for securing valuable equipment for asset management purposes (e.g., tracking critical medical equipment in a hospital) or for using traffic analyses to determine more secure access point placement, LENs can deliver added security when enhanced with data mining capabilities.

Newbury Networks' Experience with LENs

Although LENs are a new concept in the WLAN security arena, corporate IT departments usually recognize their role and value almost immediately. For example, Newbury Networks is in the midst of installing a LEN at a large enterprise with many WLAN users on many floors of multiple buildings in a large campus. They described the current situation as "out of control," with the most worrisome problems including rogue APs and WLAN signals leaking outside the buildings.

This enterprise will use LENs to monitor traffic, to detect rogue APs and to maintain perimeter security. The latter is particularly helpful for suburban office campuses, where ample parking lots provide a convenient place for hackers to sit and sniff out unsecured WLAN signals leaking out of nearby buildings. The risk of "drive-bys" will be drastically limited, since users can only log on from within the building.

In October of 2002, another company announced it would install a LEN at its customer demonstration center in Houston, Texas. Their installation highlights another selling point for LENs: They apply the technology for providing a "digital concierge" service, pushing relevant information to customers' handheld devices as they visit each location during the demonstration tour. This installation is an opportunity to showcase the ability of a LEN to provision content to the public, while at the same time enhancing security.

Conclusions

WLANs are gaining widespread popularity in many vertical markets, but concerns about their inherent network security risks are often a barrier for its delivery to mainstream markets such as healthcare, federal agencies and traditional corporate campuses. LEN technology addresses the risks head-on, with a unique detection solution. While an attacker is just beginning to exploit a WLAN vulnerability, IT staff can be alerted and given the opportunity to quickly and efficiently react against the breach.

Giving enterprises more control over network security helps WLANs live up to their potential in the corporate market. By providing a layer of security that complements standard features such as WEP and WPA, LENs strike a balance between productivity and security.

About the Author

Chuck Conley is vice president of marketing at Newbury Networks. His 18 years of experience in software marketing includes senior management positions at CenterLine Software (Compuware), Idiom Technologies, NetMorf, Segue Software and Softbridge (Teradyne). He has a B.A. in Business Administration from the University of Massachusetts, Amherst.

The author can be contacted at:

chuck@newburynetworks.com

About Newbury Networks

Newbury Networks specializes in location-based management tools for 802.11 networks. The company's Location-Enabled Network™ technology enables content and network provisioning, tracking, monitoring, logging and analysis. Newbury Networks was founded in 2001 and is headquartered in Boston.

Visit the Newsroom page or the Products page (try the two product features demos) at the Newbury Networks website:

www.newburynetworks.com

Fraud And Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following fraud and security patents. These will be of interest to some of our wireless security practitioners. Each patent includes the patent number, the invention title – linked to the corresponding USPTO webpage – a brief description, the inventor(s), and the assignee (owner). These patents were granted in February and March of 2003.

With the listing below, one can see *who* is doing *what* in the world of inventions. Moreover, it is often instructive to read issued patents, since they include patent claims, specifications, illustrations, detailed descriptions and cited references. Patents often include other references, and these are sometimes useful to broaden one's perspective of wireless communications and security.

If the wording in these is difficult to understand, recognize that the patent abstracts are generally provided in their raw legal-jargon form, straight from an attorney's word-processor. Sometimes we edit the abstracts for readability when the legalese is too impenetrable.

US Patent: 6,535,979

Method of ciphering data transmission, and cellular radio system

A cellular radio system and a method of ciphering data transmission in this system, comprising at least one transceiver communicating with other transceivers on a radio connection including one or more parallel radio bearers or logical channels. Ciphering is performed on the bearers using selected ciphering method parameters. To ensure diverse and efficient ciphering, different ciphering method parameters can be used on each parallel radio bearer.

Issued: March 18, 2003

Inventors: Jukka Vialen and Juhana Britschgi

Assignee: Nokia Mobile Phones Limited (Espoo, FI)

US Patent: 6,535,728

Event manager for use in fraud detection

A fraud detection system that receives data relating to telecommunications activity and generates events from the received data, with each having a weight corresponding to an increased or decreased likelihood of fraud. The aggregated events for a subject (a subscriber or an account) determine a score for the subject, which is used to prioritize the subject in an investigation queue. Human analysts are assigned to open investigations on the investigation queue, according to the priority of subjects. In this manner, investigation resources can be applied more effectively to high-risk subscribers and events.

Issued: March 18, 2003

Inventor: Michael Perfit, *et al*

Assignee: Lightbridge, Inc. (Burlington, MA)

www.lightbridge.com

Lightbridge, Inc
67 South Bedford Street
Burlington, MA 01803

Phone: 781-359-4000

Lightbridge helps communications providers manage their customer transactions quickly and cost-effectively. They help communications providers, e businesses and other enterprises empower their customers and mobilize their business.

US Patent: 6,535,726

Cellular telephone-based transaction processing

A retail transaction system providing enhanced customer convenience and increased transaction security by sending transaction information to a cellular network provider via a customer's digital cellular phone. For example, a fuel dispenser is equipped with a communications link allowing direct communications to a customer's cellular phone. When a customer desires to conduct a transaction using the fuel dispenser, the fuel dispenser transmits select information to the customer's cellular telephone using this communications link. A telephone number is included in the select information. When the customer presses send, or otherwise causes their telephone to dial the number transferred from the fuel dispenser, the select information along with any additional customer information is sent to the cellular network. This information is used by the network to authorize a purchase transaction for the customer – with authorization information returned to the fueling station at which the fuel dispenser is located – via a cellular link. For enhanced security, the customer may be required to input their PIN in order to complete the transaction. The PIN and the remainder of the transaction information sent from the customer phone to the cellular network is intrinsically secure due to the digital cellular encryption. Optionally, the system may be configured to cause the customer's cellular phone to automatically dial the number transferred by the fuel dispenser.

This capability may be enabled at the customer's option. The system may be extended to other retail systems including in-store point-of-sale systems (POS).

Issued: March 18, 2003

Inventor: William Johnson
Assignee: Gilbarco Inc. (Greensboro, NC)

www.gilbarco.com

7300 West Friendly Avenue
Greensboro, NC 27420
Phone: Tel 226-547-5000

Gilbarco Veeder-Root™ represents the leading brands of solutions and technologies that provide convenience, control, and environmental integrity for retail fueling and adjacent markets. A leading manufacturer of Process/Environmental Controls and Tools and Components, Gilbarco, Veeder-Root and Gasboy are wholly owned by the Danaher Corporation (NYSE: DHR), headquartered in Washington DC.

US Patent: 6,529,881

System and method for identifying an unidentified customer at the point of sale

A system for identifying an unidentified customer, including a database that contains utterance data (speech samples) corresponding to a known customer. A processing system coupled to the database receives this information at the point of sale, and compares it with the utterance data in the database to identify the unidentified customer. In response, the processing system may automatically retrieve stored information corresponding to the known customer.

Issued: March 4, 2003

Inventors: Sanford Morganstein and Sergey Zaks

Assignee: Distributed Software Development, Inc. (Chicago, IL) and Sanford Morganstein (West Dundee, IL)

US Patent: 6,529,885

Methods and systems for carrying out directory-authenticated electronic transactions including contingency-dependent payments via secure electronic bank drafts

Computer-implemented methods and systems for secure electronic transactions including electronic drafts, wherein payment on at least one of the drafts is contingent upon the removal of an associated contingency. The method may include steps of establishing a secure computer site accessible only by authenticated parties to the transaction and by any authenticated contingency approver. The site includes a representation of the transaction that includes a representation of each of the drafts and an option to remove any associated contingencies.

Parties and contingency approvers requesting access to the computer site are authenticated by:

- encrypting identification information over a secure channel and
- matching the encrypted identification information with a unique encrypted identifier stored by a bank.

Payment on the drafts of the transaction is released by the bank only when the option to remove each contingency associated with the draft is exercised, within a given time, by an authenticated party or authenticated and authorized contingency remover. Complex transactions may thereby be carried out securely, remotely and without compromising personal or financial information.

Use of the computer-implemented system and method removes the need to disseminate identification surrogates such as credit card numbers over public networks as well as the need to rely upon in-person signatures on paper documents for authentication purposes.

Issued: March 4, 2003

Inventor: Richard Johnson

Assignee: Oracle Corporation (Redwood Shores, CA)

US Patent: 6,526,509

Method for interchange of cryptographic codes between a first computer unit and a second computer unit

The method provides that a session code can be agreed between computers, without it being possible for any unauthorized third party to gain access to useful information relating to the codes or the identity of the first computer unit. This is achieved by embedding the principle of the El-Gamal code interchange in the method, with additional formation of a digital signature via a hash value of the session code which is formed by the first computer unit.

Issued: February 18, 2003

Inventor: Gunther Horn, *et al*
Assignee: Siemens Aktiengesellschaft (Munich, DE)

Interesting references:

[1] *L. Harn. Public-Key Cryptosystem Design Based on Factoring and Discrete Logarithms.* IEE Proceedings – Computers and Digital Techniques, May 1994, vol. 141, No. 3, pp. 193 – 195.

[2] H. Tsubakiyama. *Security for Information Data Broadcasting system with Conditional-Access Control.* IEEE Global Telecommunications Conference (1993), vol. 1, pp. 164 – 170.

US Patent: 6,526,390

Independent billing settlement for call origination by wireless subscribers roaming to foreign wireless networks

A method and system to bypass GSM Memorandum of Understandings for cellular/PCS services so that GSM subscribers roaming into CDMA or TDMA networks, and CDMA or TDMA subscribers roaming into GSM networks, can be provided with basic call origination services as long as the roamers can pay the bill with their valid credit card. This is achieved by integrating the proper pieces of wireless and wireline networks and secure communications.

Issued: February 25, 2003

Inventors: Jin Wang and Patuardhana Babu Gorrepati

Assignee: Lucent Technologies Inc. (Murray Hill, NJ)

Interesting references:

[1] S.J. Shepherd, *et al.* *An efficient key exchange protocol for cryptographically secure CDMA systems.* Telecommunications Research Group, University of Bradford, Bradford, BD7 1DP, UK.

[2] *UMTS Universal Mobile Telecommunications System.* Sept. 1998. IEEE. 0-7803-4984.

[3] *Simple authenticated key agreement algorithm.* Electronics Letters, June 24, 1999, vol. 35, No. 13.

US Patent: 6,526,389

Telecommunications system for generating a three-level customer behavior profile and for detecting deviation from the profile to identify fraud

A telecommunications system for detecting any unusual activity in customer behavior. A comprehensive behavior profile of a customer is generated on the basis of customer transactions. The profile includes a short-term customer behavior obtained from all of the customer's transactions, and it further includes a long-term customer behavior obtained on the basis of the generated short-term behavior. Any behavior deviation from the profile is detected and identified as fraudulent or unusual.

Issued: February 23, 2003

Inventors: Uzi Murad and Gadi Pinkas

Assignee: Amdocs Software Systems Limited (Dublin, IE)

www.amdocs.com

Amdocs provides information solutions to the leaders of the communications and the IP industry worldwide, offering CRM, billing and order management systems for communications providers, and business support systems for directory publishing companies. Amdocs offers a range of flexible delivery options: Stand-alone application modules, pre-integrated products, product-based customized solutions and a wide range of outsourcing of CRM, billing and data center operations. Amdocs products and solutions support convergent multi-service operations, emerging markets and next generation services across all lines of business – wireline, wireless, broadband, electronic and mobile commerce and IP services. Amdocs offers full voice and IP capabilities with a comprehensive single customer view and convergent product catalog.

US Patent: 6,526,126

Identifying an unidentified person using an ambiguity-resolution criterion

A system for identifying a person, including a database containing utterance data (speech samples) and an ambiguity-resolution criterion corresponding to a known person. A processing system is coupled to the database and receives utterance information and an ambiguity-resolution identifier corresponding to the unidentified person The processing system compares the stored utterance information with the captured utterance data to provide a list of possible matches. If the processing system does not uniquely identify the person, the processing system compares the ambiguity-resolution identifier with the ambiguity-resolution criterion to identify the unidentified person. After identifying the person, the processing system may automatically retrieve stored information corresponding to the identified customer.

Issued: February 25, 2003

Inventors: Sanford Morganstein and Sergey Zaks

Assignee: Distributed Software Development, Inc. (Chicago, IL) and Sanford Morganstein (West Dundee, IL)

Interesting references:

[1] Atal, Bishnu S., *Automatic Recognition of Speakers from Their Voices.* Reprinted from Proc. IEEE, vol. 64, Apr. 1976. pp. 460 – 475.

[2] Furui, Sadaoki. *Speaker-dependent-feature extraction, recognition and processing techniques.* Speech Communication 10, 1991. pp. 505 – 520.

[3] Birnbaum, Martha; Larry A. Cohen; Frank X. Welsh. *Report: A Voice Password System for Access Security.* AT&T Technical Journal, Jul. 17, 1986. pp. 68 – 74.

US Patent: 6,526,033

Delivering calls to GSM subscribers roaming to CDMA networks via IP tunnels

A system for integrating wireless/wireline and circuit/packet networks (to bypass GSM Memorandum of Understandings) for cellular/PCS services so that GSM subscribers roaming into CDMA networks can be provided with basic call delivery cellular services as long as the roamers can pay the bill with a valid credit card. This is achieved by integrating wireless and wireline networks as well as circuit and packet networks, using IP networks and protocols as an alternative to the existing telephony-based approach.

Issued: February 25, 2003

Inventor: Jin Wang and Patuardhana Babu Gorrepati

Assignee: Lucent Technologies Inc. (Murray Hill, NJ)

Interesting references:

[1] Perkins. *IP Mobility Support.* Network Working Group, RFC 2002, Oct. 1996.

[2] Droms. *Dynamic Host configuration Protocol.* Network Working Group, RFC 2131, Mar. 1997.

[3] *A Primer of the H.323 Series Standard.* DataBeam Corporation, May 15, 1998

Further Patent Information

To obtain a complete copy of these patents, contact the US Patent and Trademark Office at the address or telephone numbers below:

General Information Services Division
U.S. Patent and Trademark Office
Crystal Plaza 3, Room 2C02
Washington, DC 20231