

Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com

Vol. 5, No. 11. November, 2003

Bluejacking: Bluetooth Graffiti

If a sudden uptick in hacks is a sign that a technology has gone mainstream, then the overnight phenomenon of “bluejacking” shows that **Bluetooth** is finally here.

Bluejacking exploits a Bluetooth device’s **ability to discover** other nearby Bluetooth devices. The basic concept is similar to **WiFi wardriving**, but instead of siphoning off bandwidth, the main goal of bluejacking is to amuse, irritate or surprise the recipient with an unsolicited message that pops up seemingly out of nowhere. A **new Web site** devoted to bluejacking suggests messages such as:

“*Make of victim's phone*” suck, buy “*make of your phone*”!

Will bluejacking evolve from an annoyance into a security threat on par with wardriving? It is a question that Bluetooth’s backers pondered as far back as 2001 in a **paper that acknowledges some risk**: “The Bluetooth SIG encourages the reuse of existing transport, session and application layer security.”

Bluejacking could pose a risk if hackers use it to cause devices to malfunction, release information (such as a file or an electronic business card) or capture keystrokes from a Bluetooth keyboard.

Further information about Bluetooth security, including a security checklist, is available in Chapter 4 of **NIST Special Publication 800-48. An Analysis of Bluetooth Security Vulnerabilities** by **Creighton C. Hager** and **Scott F. Midkiff** – copyrighted by IEEE in 2003 – presents an overview of the Bluetooth specification, with an emphasis on security features and a security analysis using a general taxonomy and methodology called **VERDICT**.

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:

cnp-sales@cnp-wireless.com

Next Issue Due...

December 22th, 2003.

Future Topics

Wireless Flash Memory Security •
Personal Area Network Security • Radius
for Wireless • 3G Security • Public Keys &
Wireless • 1XEV Security

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:** cnp-sales@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.

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.

IEEE Globecom 2003

1st- 5th December 2003
San Francisco Marriott
San Francisco, CA
www.globecom2003.com

STOS (Security: From Theory to Practice) Symposium 2003

1st- 5th December 2003
George Washington University
Campus
Washington, DC
www.stosdarwin.org

eGov Homeland Security Conference

2nd- 3rd December 2003
Ronald Reagan Building
Washington, DC
www.e-gov.com

The Forum on Information Warfare

2nd- 5th December 2003
Georgetown University
Conference Center
Washington, DC
www.misti.com

Wi-Fi Planet Conference & Exhibition Fall 2003

2nd- 5th December 2003
San Jose McEnery
Convention Center
San Jose, CA
www.jupiterevents.com/80211/fall03/index.html

RTSS 2003

(24th IEEE International
Real-time Systems Symposium)
3rd- 5th December 2003
CasaMagna Marriott
Resort Hotel
Cancun, Mexico
rtss2003.ece.cmu.edu

Angelbeat Regional Technology Forums on Mobility and Wireless

4th December 2003
Sheraton Moana Surfrider
Honolulu, HI
www.angelbeat.com

Mobile Military Communications

8th- 9th December 2003
Holiday Inn on the Bay
San Diego, CA
www.ttcus.com/mcom/index.html

The Emerging Technology Showcase (Sponsored by Forrester Research)

8th-10th December 2003
The Phoenician
Scottsdale, AZ
www.forrester.com/Events

CDMA Americas Congress

8th-10th December 2003
Miami Beach Convention Center
Miami, FL
www.cdma-americas.com

Infosecurity 2003

8th- 11th December 2003
Jacob K. Javits
Convention Center
New York, NY
www.securityfocus.com/calendar/596

SANS CDI East 2003

8th- 13th December 2003
Grand Hyatt Washington
Washington, DC
www.sans.org/cdieast03

Bluetooth Americas

9th- 11th December 2003
San Jose Convention Center
San Jose, CA
www.ibctelecoms.com/bluetoothamericas

802.11 LAN Security Workshop

10th December 2003
Chicago, IL
www.itvshop.com

[Note: this event is being repeated in other locations during December]

CNIS 2003

(Communication, Network and Information Security)

10th- 12th December 2003
Long Island Marriott and
Convention Center
New York, NY

www.iasted.com/conferences/2003/NewYork/cnis.htm

WiFi Warriors ... U-R – Linked!

Discover the extent of WiFi's spread throughout the world using JIWIRE (www.jiwire.com/index.htm). For the sake of convenience, their directory also is available to mobile devices from outside the range of any hotspot. A cell phone enabled with WAP (Wireless Application Protocol) or a PDA equipped with appropriate software can access this website to find:

- News about WiFi, hotspots and cellular,
- Step-by-step instructions for WiFi network setups and,
- Tips for using 802.11 technology (gateways and access points) with other technologies (Bluetooth, Ethernet and Wireless Distribution Systems).

Securing WLANs

Karl Toompuu, Bridgewater Systems

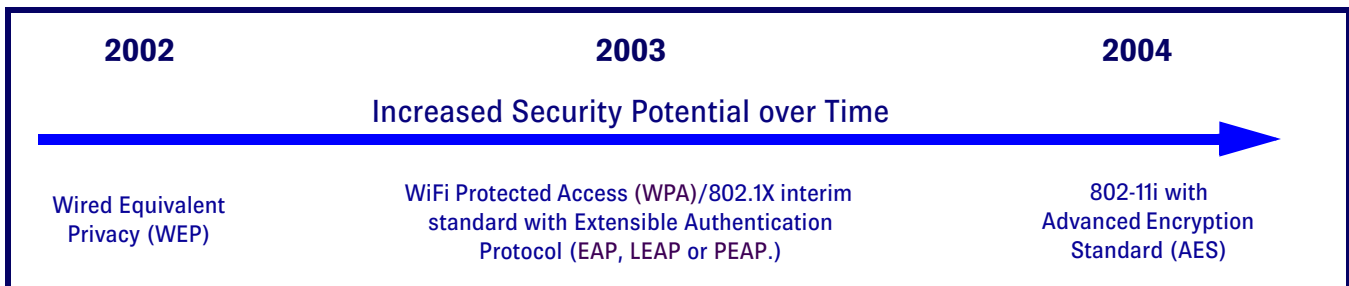
Wireless LAN (WLAN) security currently has interim standards and proprietary solutions vying to address security needs. Stronger standards to meet both current and future requirements are in development, but the current in-between state has created a confusing array of options for organizations seeking robust data protection and network access control solutions for their WLAN and WiFi roaming users.

Figure 1 shows the current standards and the upcoming 802.11i standard, which will deliver the comprehensive security required for enterprise WLANs.

Wired Equivalent Privacy (WEP)

All new WLAN devices are shipped with Wired Equivalent Privacy (WEP). This security mechanism encrypts data as it flows between an access point and a WiFi device, such as a laptop. Unfortunately, access point manufacturers often ship their products with WEP disabled because setting up a network is easier without security features. Often, WEP encryption is *never* turned on, as explained in previous issues of *Wireless Security Perspectives* (principally, the **November 2002 issue**, but also the April 2003 issue). WEP is also easy to defeat, because all devices typically share a single key.

Figure 1: The 802.11 Encryption Transition



WiFi Protected Access (WPA) and 802.1X

WPA is an interim standard comprising two primary elements:

- A more robust encryption mechanism and,
- 802.1X port-based access control and authentication framework.

By creating a re-keying mechanism that rotates security keys with every 10 Kbytes of data, Temporal Key Integrity Protocol (TKIP) encryption helps make WPA more secure against attacks than the previous standards. TKIP fixes a number of the vulnerabilities in WEP and can run on current 802.11 hardware.

The Mathematics Corner

For last month's Mensan question, the series goes like this: ... 661 673 677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977 983 991 997 ...

These are all prime numbers ... so, for our series (929, 941, 953), it follows that the next number would be 971.

Congratulations to Greg Rose and Dave Ott (both from Qualcomm), who submitted the correct answer last month. They were both awarded CNP paraphenalia.

The question for this month: What is next in the series 121393, 75025, 46368, 28657, 17711, 10946?

Submit your answer to wsp@cnp-wireless.com

The second component of WPA is 802.1X security, which addresses user authentication. It provides a framework for mutual authentication between a client and an authentication server. It also provides dynamic WEP keys on a per-session, per-user basis, removing the administrative burden and security issues surrounding single static WEP keys.

The authentication protocol used in 802.1X is called Extensible Authentication Protocol (EAP). See **Table 1** for a list of variants, some of which are proprietary.

Table 1: Current types of Extensible Authentication Protocol (EAP)

Type	Description and usage
EAP-MD-5 (Message Digest)	Typically not recommended since the user password can be derived. It provides for only one-way authentication, and no means to derive dynamic, per-session WEP keys.
EAP-TLS (Transport Layer Security)	The most common, and widely supported by vendors, this implementation is bundled with Windows XP, making it fairly attractive. It is highly secure because it requires asymmetric public and private keys on the client and server side. However, it presents a heavy administrative burden, as it requires distribution of keys to all devices that will access your network.
EAP-TTLS (Tunneled Transport Layer Security)	An extension of EAP -TLS. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel (or “tunnel”), as well as a means to derive dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
LEAP (Lightweight EAP)	Cisco’s proprietary version, used in their access point products. It uses a combination of challenge-based authentication and dynamically allocated, per-session key WEP generation to provide enhanced security. Cisco has recently licensed LEAP to a variety of other manufacturers.
PEAP (Protected EAP)	Co-developed by Cisco and Microsoft. This is a more secure version of LEAP that is now being widely adopted by 802.11 equipment manufacturers. PEAP makes use of certificates to authenticate the network and non-certificate-based authentication methods (user name and password) to authenticate the WiFi device.

More 802.1X Variations

The principle of 802.1X security is to use sign-on authentication as a way to both know and accept the user as valid. In each session, it also delivers a cryptographic key for that session. This rotating, per-session security key is extremely difficult to predict and therefore very difficult to hack.

However, not all 802.1X authentication mechanisms are created equal. There are trade-offs between security and convenience. The most secure methods use both client- and server-side certificates for mutual authentication (EAP-TLS). Other secure methods rely only on server-side certificates, together with simple user IDs and passwords, to authenticate users.

However, the credentials are passed over an encrypted connection, which keeps them secure. Some examples of this approach are EAP-TTLS with PAP (Password Authentication Protocol) and all flavors of PEAP.

It is impractical in all cases to use client certificates, given the administrative burden involved in distributing private keys to the clients. In fact, a server certificate scheme is equivalent in strength to the security used on the Web and for virtually all e-commerce transactions on the Internet.

A good balance is provided by the methods that rely on server-side certificates together with client-side challenge-based password authentication such as **PEAP MS-CHAP v2**. Strong authentication and encryption techniques will come together in the 802.11i standard being developed by the Institute of Electrical and Electronic Engineers (IEEE).

Regardless of the approach, authentication requests are passed from the access point through to some type of security server that authenticates the user’s credentials. This server also defines any policies that dictate the type of access to which the user is entitled.

802.11i Standard

The IEEE is currently working on the 802.11i standard, which will provide stronger authentication and a robust cryptographic algorithm that will meet the security requirements of enterprise-level WLANs. Through the Advanced Encryption Standard (AES), 802.11i enhances the **TKIP** technology of **WPA**. AES is expected to become the *de facto* standard for private, commercial security applications. However, because it is computationally intensive, it will require new hardware.

Work on 802.11i is not expected to be complete until late 2003 or early 2004. However, many components of this standard are already being implemented in the interim standards and proprietary protocols of major equipment vendors discussed in **Table 1**, above.

Creating Secure Enterprise WLAN Environments

When implementing WLANs in an enterprise, it is important to view them as an extension of the existing network. Existing security policies should be updated to include WLANs. Mechanisms should be established to detect breaches of both IP and radio networks through the use of firewalls, intrusion-detection systems and definition of network segments. Disaster-recovery measures should also be defined for use when a security breach occurs, so that access points are turned off and visitors disallowed during the event.

Due to the mobile nature of WLANs and the ease of deploying rogue access points, regular security audits and vulnerability testing become critical. User education also is important so that all enterprise employees understand WLAN security measures and use them properly.

WLAN Implementation Options

Although the hype surrounding WLAN security makes it seem confusing, there are actually several relatively clear-cut ways to provide good security for WLANs. Implementations must be planned in light of the emerging standards, and organizations should ensure that their WLAN will be upgradeable to 802.11i standards. Vendor equipment should be evaluated based on its interoperability and ability to migrate to the appropriate standard with minimal additional expense.

There are two critical areas to be considered when implementing WLANs: securing the airlink and sharing the network.

Securing the Airlink

Securing the airlink involves authentication so that only authorized users are given access and encryption to protect data traveling on the WLAN. As described **above**, there are multiple options for both authentication and encryption that let organizations create an infrastructure suited to both current and future needs.

Access Points. Access points may act as gatekeepers, accepting data via radio signals, checking for authentication, authorizing access, then forwarding the information to the wired network — and relaying information back to the wireless user. Some access points can also monitor the acceptability of other access points around them, thereby detecting potential rogue access points.

Access points are available in two main configurations. A *fat access point* has network intelligence in the same box, handling protocols for user authentication, encryption, management and roaming. Enterprises with many small sites or wanting the added security of segregating traffic at the access-point level will find it best to use fat access points because they push routing functionality for public and private WLAN access closer to the edge of the corporate network. Fat access points can reduce the load on central network switches, although they still require management.

A *thin access point* relies on the controlling intelligence required for Virtual Local Area Network (VLAN) tagging, DHCP servers and AP firmware rules residing elsewhere on the network. Thin access points usually are deployed with specialized gateways, wireless switches or in conjunction with VPNs, where intelligence at the access point is not required.

The main difference between the two varieties is convenience and cost. As a rule of thumb, if only a few large locations exist, use thin access points. If there are many, small locations, fat access points are a better fit.

WLAN Switches. Depending on the applications accessed via the WLAN, enterprises may wish to implement a WLAN switch to manage multiple access points, and even hardwire the bandwidth available to specific access points. For example, when performance must be guaranteed, such as an application accessing patient data records in an intensive care unit, network designers may choose to implement a WLAN switch to guarantee bandwidth to its access point.

Specialized Gateways. There are some specialized gateways or “edge connectors” developed to address current security requirements for WLANs. They sit between the corporate network and WLAN access points, adding security, encryption, VPN access, bandwidth management and access control.

The gateway authenticates users and directs legitimate users to the appropriate part of the network, such as a partner zone on the corporate network or on the public Internet. To do this, gateways interface with corporate user directories — such as LDAP or Remote Authentication Dial-In User Service (RADIUS) servers — to authenticate users and enforce network-security policies, either by associating users with virtual LANs or by implementing traffic partitioning via a firewall.

Gateways are centralized — aggregating traffic from widely distributed access points and enforcing access rules. They work independently of access points, so the customer can use any vendor’s access point and expand the network without concerns about compatibility. They also support multiple types of encryption and authentication methods, but even with only one type, a client-side software such as a VPN is required.

VPN in the Enterprise. Some organizations have chosen to use VPNs to control security in their enterprise WLANs. VPNs are typically used in order to provide secure access to enterprise computing resources by remote offices or individuals, using the Internet or private facilities as the communication medium.

Using special protocols, a VPN creates a secure tunnel through a shared public infrastructure. In this tunnel, all data transmitted between the client and enterprise is encrypted. Each remote computer has client software requiring users to perform an extra login procedure to authenticate themselves and set up the secure VPN connection.

VPNs are commonly used by businesses to give employees remote access when connecting through public facilities, such as a WiFi hotspot. Typically, the roaming user will log onto the hotspot's Internet portal, arrange payment for the hot spot charges (e.g. via credit card), and then connect to their enterprise over the Internet using their VPN client. VPN-based security is necessary today because hot spots typically do not provide any security, due to the lack of a single, ubiquitous standard used by all wireless devices.

Sharing the Network

When implementing enterprise WLANs, one of the major concerns is in network sharing. Examples include:

- Enterprises wish to provide Internet access to visiting customers, suppliers and partners while protecting corporate network assets. They may even wish to limit the bandwidth available to visitors so that they do not overload the network or restrict visitor access to core business hours.
- Hospitals may wish to offer e-mail and Internet access to patients, while providing a secure, high-performance environment for staff and hospital operations. They also may wish to guarantee bandwidth for delivering critical information, such as test result services to emergency room staff.
- Financial institutions may wish to provide an information portal to customers, while totally securing private information.

What all these examples, and many other possibilities, have in common is the need for WLAN public access through corporate wireless and wired networks. This public/private service must be delivered while ensuring:

- A. Security for sensitive information coming from the public side,
- B. Robust security for the organization's information assets and,
- C. Prioritized bandwidth availability to meet quality-of-service (QoS) guarantees.

Creating Virtual LANs. One of the most attractive security implementations for user differentiation in WLANs involves creating virtual LANs (VLANs), using the 802.1X PEAP protocol with a RADIUS server for strong authentication and authorization.

A major benefit of the 802.1X protocol is that it can use RADIUS servers for user authentication, taking advantage of a technology that is widely deployed in enterprise networks to authenticate remote users. Some RADIUS servers are very sophisticated, giving enterprises the ability to create extremely granular security policies to control access to the network, to grant specific quality of service and bandwidth, and to allow access to resources within the network.

When using a RADIUS server, the user's request for access is taken by the access point and passed to the RADIUS server for authentication, which then authorizes the AP to allow the user access and defines user privileges.

VLAN segmentation is often used in physical LANs to segregate different groups of employees with different capabilities, using gateways or firewalls to enforce the set of security policies that apply to each user group.

This same concept can be used with WLANs, and it can be extended to allow a WLAN to be segmented to serve both visitors and employees. A visitor is given a specific wireless identity that provides access to a VLAN segment isolated from the rest of the network. Based on this identity, the user will be granted specific privileges and may also be allocated specific bandwidth and QoS when applications such as voice are deployed over WiFi.

In pay-per-use scenarios, a user is first directed to a VLAN segment that is set up as a visitor's portal. This connects the user to a credit card authorization portal before granting specific privileges. The policies maintained in the RADIUS server can define levels of service, bandwidth allocation and billing information that could be gathered by the RADIUS server to be forwarded with usage data to a specific billing system.

Best Practices

- Implement 802.1X security today, making certain that all vendor equipment provides an upgrade path to 802.11i security standards, and create a migration plan to those standards.
- Although vulnerable to some attacks, employ the existing WEP security measures on all devices. They provide basic protection and will complement other security measures.
- Upgrade WEP-enabled devices to WPA by simple firmware update when vendors make this available.
- Guard against naïve security risks. Ensure that all default mode settings are appropriately changed on equipment, including SSIDs and passwords on access points and wireless interface cards. Educate employees about enterprise WLAN risks, and do all that is possible to stop them from unwittingly

implementing rogue APs. Ensure that employees do not use WLAN cards in ad hoc mode when in public, but instead use the corporate VPN for secure access back to the enterprise.

- Deploy personal firewalls on all mobile machines, and use corporate network security policy to enforce their use.
- Regularly scan for rogue APs in the corporate network.
- Use VPN access for remote users accessing the WLAN through hotspots, and use it internally for wireless security, if necessary.
- Segment the WLAN into VLANs for better control of access and security for employees and visitors.

Conclusion

With security no longer a barrier, organizations can confidently implement WLANs. They can be more complex and time-consuming to implement, secure and manage than LANs, but many organizations can easily accommodate the increased administrative requirements. For those that cannot justify the added capital expense or administrative load, managed WLAN service providers may be the answer.

About the Author. Karl Toompuu Karl.toompuu@bridgewater.com is product line manager for WiFi at Bridgewater Systems. He has over 15 years experience in telecom. Before joining Bridgewater Systems, Karl was product manager at Ceyba, where he concentrated on Opex quantification and reduction. He joined Ceyba from Syndesis, where he focused on transitioning the company into IP and optical provisioning. Karl is a frequent speaker at industry events and conferences.

About Bridgewater Systems. Bridgewater Systems (www.bridgewater.com) is a provider of dynamic IP and data service fulfillment and assurance solutions, enabling service providers to generate profits from their networks while enhancing customer loyalty.

Fraud and Security Patent News

US Patent: 6,651,105

Method for seamless networking support for mobile devices using serial communications

A method, apparatus and computer product for a mobile device to roam securely and seamlessly from one access point to another access point without disrupting an active PPP connection. The method includes establishing, maintaining, and terminating a PPP connection between a mobile device and a PPP server via an access point, wherein the mobile device is equipped with a serial asynchronous communication interface. The PPP server is attached to a packet switched data network, and the access point is acting as a bridge between the serial communication interface and the packet switched communication interface. Also provided is a method to emulate a direct RS-232 cable connection between a mobile device and another computer located several hops away from the mobile device. It provides a method of keeping the RS-232 cable emulation between the mobile device and another computer system intact, despite changes in mobile device's location in the network. It also provides a method of exchanging cookies between peers at the PPP connection establishment time and using them for fast re-authentication. This is a secure method of switching from one PPP proxy to another PPP proxy without disrupting the end-to-end PPP connection.

Issued: November 18, 2003

Inventor: Pravin Bhagwat, *et al*

Assignee: International Business Machines Corporation (Armonk, NY)

US Patent: 6,650,894

Method, system and program for conditionally controlling electronic devices

An electronic device is enabled to detect the proximity of other electronic devices. Multiple proximity-based conditions for usage of the electronic device may be provided by a manufacturer, user and other authorities at the electronic device. The proximity of other electronic devices is compared with the proximity-based conditions and a level of usage of the electronic device is determined, such that the level of usage of the electronic device is conditionally adjusted according to the proximity of other electronic devices.

Issued: November 18, 2003

Inventor: Viktors Berstis, *et al*

Assignee: International Business Machines Corporation (Armonk, NY)

Notable References:

- [1] Sami Levijoki. *Privacy vs Location Awareness*. Helsinki University of Technology, Seminar on Network Security, Dec. 2000, see pages 1, 2, 6, 7 and 8; www.hut.fi/~slevijok/privacy_vs_locationawareness.htm
- [2] Brent Miller. IBM, Pervasive Computing, Bluetooth Applications in Pervasive Computing, Feb. 2000.

US Patent: 6,650,888

Validating a transaction with user voice authentication using wireless communications

A security system comprising a wireless interface coupled to a transaction manager. The wireless interface receives user information, including a user speech sample and a user account code, from a wireless communication device over a wireless communication link. The transaction manager transfers the user speech sample and the user account code to a validation system. The transaction manager receives and displays validation information from the validation system. The validation information indicates if the user is authentic and if the account code is valid. It may also include a picture of the user, and this is displayed by the transaction manager.

Issued: November 18, 2003

Inventor: Fred Cook

Assignee: Sprint Communications Company, L.P.
(Overland Park, KS)

Notable Reference:

- [1] Neuman, et al. *Kerberos: An Authentication Service for Computer Networks*. Sep. 1994, IEEE Communications Magazine, p. 33-38.

US Patent: 6,650,887

Mobile phone system with host processor coordination and internal mobile phone accounting capabilities

A mobile phone system with a mobile phone having internal accounting capabilities for real-time call debiting. It accounts for the billing parameters of a mobile phone unit that is operated in a multi-zone communication network with a complex rate structure. The mobile phone unit has an internal processor with accessible internal memory for storing the accounting program and call data for each call. It also includes a clock and circuit means for activating and deactivating the phone. The accounting program includes an updatable rate table and a complex billing algorithm for calculating the account status on the fly, including multiple rate structure factors such as long distance calls, international calls with country independent local charges, charges for roaming per day and/or roaming per minute, and call surcharges, where the account status of the mobile phone is calculated in real time for decrementing a debit account or calculating an account charge on demand. The mobile debit phone has a signal for alerting the user of account status, which is preferably a display of real-time account status. The mobile phone system includes a communication system for activating and programming a new phone unit over the airways and upgrading the account status in rate table in the phone unit over the airways.

Issued: November 18, 2003

Inventors: Donald McGregor and Gregory McGregor

Assignee: Telemac Corporation (Los Angeles, CA)

About WSP Patent Listings

The US Patent and Trademark Office (USPTO) frequently grants fraud and security patents that will be of interest to some of our wireless security practitioners. Each patent includes the invention title – linked to the corresponding USPTO web page. We briefly describe it and provide, at minimum, its inventor(s) and assignee (owner).

With the listing of patents provided each month, one can see *who* is doing *what* in the world of wireless 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: 6,650,616

Transmission security for wireless communications

A method of transmission-level security, and a corresponding transmission security system. The method consists of the steps of:

- Forming a plurality of digital signals representing a symbol to be transmitted over a communication medium, wherein respective ones of the plurality of digital signals are modulated onto respective ones of a plurality of subcarriers according to a multiple carrier modulation scheme and,
- Introducing a predetermined group delay distortion in one or more of the plurality of subcarriers, such that portions of the one or more of the plurality of subcarriers will be received outside of a time window corresponding to the symbol at a receiver.

In one implementation, an equipped receiver substantially removes the predetermined group delay distortion such that the portions of the one or more of the plurality of subcarriers fit within the time window.

Issued: November 18, 2003

Inventor: James Crawford

Assignee: Magis Networks, Inc. (San Diego, CA)

Notable References:

- [1] Holmes, Jack K., *Coherent Spread Spectrum Systems*. Wiley-Interscience Publication, John Wiley & Sons, pp. 350-356.
- [2] Sollenberger, N.R., et al. *Receiver Structures for Multiple Access OFDM*. Vehicular Technology Conference, 1999 IEEE 49th, vol. 1, 1999, pp. 468-472.
- [3] Stantchev, B., et al. *Time-Variant Distortions in OFDM*. IEEE Communications Letters, vol.: 4, Issue: 10, Oct. 2000, pp. 312-314.

US Patent: 6,650,227

Reader for radio frequency identification system having automatic tuning capability

A reader for an RFID system that has an exciter circuit for generating an excitation signal and a feedback circuit coupled to the exciter circuit for automatically tuning the exciter circuit. The exciter circuit has at least one re-tunable component providing the exciter circuit with adjustable component values and a plurality of signal generating states. The exciter circuit is initially tuned to a first signal generating state, but is re-tunable to additional signal generating states by adjusting the component value of the re-tunable component. The feedback circuit includes a circuit evaluator coupled to the exciter circuit for determining a value of an operational parameter of the exciter circuit. A decision-making circuit is coupled to the circuit evaluator for formulating a decision in response to the value of the operational parameter. An adjustment circuit is coupled to the decision-making circuit and exciter circuit for receiving the decision and conveying an adjustment instruction to the exciter circuit in response to the decision.

Issued: November 18, 2003

Inventor: John Bradin

Assignee: HID Corporation (Irvine, CA)

US Patent: 6,647,260

Method and system facilitating web-based provisioning of two-way mobile communications devices

A system and method for provisioning a two-way mobile communications device having a display screen and user interface that is initiated from the device to be provisioned. The device to be provisioned establishes a secure communications session with a provisioning server device. The subject communications path may utilize an intermediate server device. The user of the device is then presented with several input and choice screens, which may be used in conjunction with the user interface to provide user information and select device features and services. The user information and selected feature and service requests are then forwarded to the provisioning server device. The provisioning server device processes the received information and generates provisioning packages, registration requests, and notifications for the subject mobile

device and for any associated server device providing services. The provisioning packages may comprise software modules, parameters and any required security information.

Issued: November 11, 2003

Inventor: Steve Dusse, *et al*

Assignee: Openwave Systems Inc. (Redwood City, CA)

www.openwave.com

Openwave Systems Inc. provides wireless and wireline carriers, Internet Service Providers, and broadband providers with the software and services needed to build multi-network services for their subscribers. Openwave teams with HP, Siemens, and IBM, to foster innovation and ensure the success and growth of the mobile Internet.

Openwave Systems Inc.
1400 Seaport Boulevard
Redwood City, CA 94063 USA

Phone: +1.650.480.8000

Fax: +1.650.480.8100

US Patent: 6,647,149

Method and apparatus for securely transmitting and processing digital image data

Methods and an apparatus for securely transmitting and processing digital image data for display. The invention provides for decomposing, compressing, and scrambling digital image data and forwarding the decomposed, compressed and scrambled image data to a destination where the image data is decompressed, re-composed, and descrambled prior to display. In particular, digital image data is scrambled before or after being compressed and is subsequently descrambled after being decompressed and prior to display such that unauthorized use of the image content is prevented. The invention can be used in conjunction with most standard block-based image compression algorithms, such as JPEG as well as some types of wavelet transform-based systems.

Issued: November 11, 2003

Inventors: Richard Keeney and Thor Olson

Assignee: Electronics for Imaging, Inc. (Foster City, CA)

www.efi.com

Electronics For Imaging, Inc. (EFI) delivers high-quality, short-run color and black and white digital printing solutions. EFI's emphasis is now on developing software solutions for the professional workflow solutions, controller solutions and enterprise markets.

EFI
Foster City, CA

Phone: +1.888.334.8650

US Patent: 6,643,774

Authentication method to enable servers using public key authentication to obtain user-delegated tickets

A method, system, and computer-readable code for delegating authority in a public key authentication environment from a client to a server machine or process, in order that the server machine or process can then securely access resources and securely perform tasks on behalf of the client. The authority is delegated by obtaining tickets (or other equivalent representation of user credentials) from a private key system, such as the Kerberos system, where the tickets identify a user's access rights or privileges. The invention provides several alternative techniques with which this delegation model can be implemented. In these techniques, the client does not directly access the private key system.

Issued: November 4, 2003

Inventor: John McGarvey

Assignee: International Business Machines Corporation
(Armonk, NY)

Notable Reference:

- [1] Sirbu, et al. *Distributed Authentication in Kerberos Using Public Key Cryptography*. Symposium on Network and Distributed System Security, Feb. 10-11, 1997.

US Patent: 6,643,773

Apparatus and method for authenticating messages in a multicast

An apparatus and method used by a receiving node in a multicast for authenticating a message received from a transmitting node, using tags. More particularly, a first tag received with the message is located and utilized to determine if the transmitting node is in the multicast. The first tag includes data associated with at least one of the receiving node and the transmitting node. A second tag is then generated if the transmitting node is determined to be in the multicast. Once generated, the second tag is transmitted with the message to a third node in the multicast. Among other things, the second tag includes data indicating that the receiving node is in the multicast.

Issued: November 4, 2003

Inventor: Thomas Hardjono

Assignee: Nortel Networks Limited (St. Laurent, CA)

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
800-786-9199 or 703-308-4357