Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 4, No. 3. March, 2002

Editor at Wireless Security Conference

Les Owens, editor of *Wireless Security Perspectives*, will be speaking at a "Wireless Security Conference" on May 8th and 9th, 2002 in New York City. The conference is being put on by Strategic Research Institute. Topics to be covered include:

- Wireless LAN security
- Hacker methods and motives
- Fixing vulnerabilities in 802.11
- Update on WEP flaws
- Progress in 802.11 standards
- Mobile network security: Vulnerabilities in networks and on the device level; operational security
- Authentication
- Security solutions including analysis of solutions developed by and for finance, healthcare, highway departments, utilities, and campus environments – with comparisons and lessons for wireless security

For more information:

www.srinstitute.com/ck114

or email:

jbach@srinstitute.com

Enterprise Mobile Security – Is It Possible?

By Janet Hendrickson
(Pointsec Mobile Technologies, Inc)

Mobile, portable computing devices, such as laptops and Personal Digital Assistants (PDAs), are now standard equipment within the enterprise. Figures published by IDC predict that global handheld sales will grow to over 63 million units by 2004. The Gartner Group predicts more than one billion handheld computers and mobile phones with wireless network connectivity will be in use around the world by 2003.

Mobile devices move in and out of a company's security perimeter on a daily basis, carrying strategic information out and possibly bringing in hidden viruses, Trojan horses and other malicious code. Worse still, these devices frequently store user passwords, login scripts and other necessary to access the organization's network from the outside.

Security concerns are not limited to mobile devices supplied by the company. Employee-owned devices, such as PDAs are also used to store company data and to access company networks. The ability for the user to synchronize data from their workstation to their PDA is now a standard business practice. It is much more convenient to travel with a lightweight, content-rich PDA than with a five-pound laptop.

About Wireless Security Perspectives

Price

The basic subscription price for *Wireless Security Perspectives* is $300 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$350 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 15th, 2002.

Future Topics

Radius for Wireless • IP Security • Public Keys & Wireless • Security Issues in Ad hoc Wireless Networks • Latest in Watermarking • 3G Security • Blackberry • Security for PDAs • SMS 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**: cnpsales@cnp-wireless.com **Web**: www.cnp-wireless.com/wsp.html **Subscriptions**: $300 for delivery in the USA or Canada, US$350 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: Betsy Harter.
Production: Doug Scofield.
Distribution: Debbie Brandelli.
Marketing: Muneerah Vasanji.
Accounts: Evelyn Goreham.
Publisher: David Crowe.

Upcoming Fraud and Security Events

The following are some upcoming wireless and security conferences and security events that may be of interest to the wireless and network security practitioners.

SANS2002 Annual Conference
1st- 7th April 2002
Orlando World Center Marriott
Orlando, FL
www.sans.org/SANS2002

Next Generation Telecoms Fraud 2002
8th- 12th April 2002
Omni Parker House
London
www.iir-conferences.com

InBuilding Wireless 2002
15th- 17th April 2002
JW Marriott
Las Vegas, NV
www.iir-inbuilding.com

The Information Security Conference
16th- 18th April 2002
McCormick Place
Chicago, IL
www.dci.com/brochure/secchi

Defense and Security – Procurement & Partnership Opportunities
22nd- 26th April 2002
Wyndham City Center Hotel
Washington, DC
www.srinstitute.com

12th Annual CTST Conference and Exhibition
22nd- 25th April 2002
Morial Convention Center
New Orleans, LA
www.ct-ctst.com

Internet World Spring 2002
22nd- 26th April 2002
Convention Center
Los Angeles, CA
www.internetworld.com/events/spring2002

For Security Matters portion of Internet World conference, visit also:
www.internetworld.com/events/spring2002/security

If these synchronized devices are not properly secured, and then fall into the wrong hands – such as a competitor or a criminal – exploitation of valuable corporate data, including trade secrets and financial information could result.

... More Upcoming Events

The Practitioner's Forum on Mobile & Wireless Security
29th- 30th April 2002
American Management Association
Washington, DC
www.frallc.com

Enterprise Wireless Forum Conference & Expo
29th April - 1st May 2002
Convention Center
Santa Clara, CA
www.intmediaevents.com/ewf/spring02

The ISI Forum on Information Security in Government
29th April - 2nd May 2002
Georgetown University
Conference Center
Washington, DC
www.misti.com

Wireless Venture Private Equity Conference - The Wireless Internet
30th April - 1st May 2002
Burlingame, CA.
www.wireless-ventures.com

DallasCon 2002 - Cyberterrorism Summit
4th May 2002
Dallas, TX
www.dallascon.com

PDAs have become recognized as critical business tools and are gaining enhanced communications capabilities, including wireless wide area networking through cellular, WiFi (IEEE 802.11) and wireless data network radio transceivers, allowing quicker and easier access to corporate data. Mobile devices exist to enhance employee productivity, but this improvement is not without risk. A 2002 survey conducted by Pointsec Mobile Technologies revealed a significant risk of device loss – the lost-and-found records of the three largest cab companies in San Francisco during a 6-month period showed, on average, 54 laptops and 72 PDAs were left in cabs.

Some organizations affected or displaced by the September 11, 2001 incident are using mobile communication devices to replace traditional face-to-face meetings that require significant travel. Many have been forced to go almost entirely mobile to sustain their business. Some, whose employees once worked within the Twin World Trade Center Towers, are now working from multiple, distributed locations. Additionally, various agencies within the Pentagon now require that all staff members use mobile devices, so that their data can leave the building with them in the event of an evacuation. A systems analyst with the US Department of Defense (DoD) stated that for every such mobile device, the appropriate level of security must be available, or it will be discarded.

The appropriate level of security means complete disk encryption. Hence, it is believed better to throw away a few thousand dollars in hardware than to let priceless classified information get into the wrong hands.

Free Email Standards Alerts!

Sign up for our new, **FREE** email alert service. Occasional emails with analysis regarding emerging standards or other technical wireless issues. Our first email alert described the various levels of implementation of the US government's security initiative – Wireless Priority Service; the second summarized the many revisions of the ANSI-41 standard used to support inter-system roaming and mobility in CDMA, TDMA and analog systems.

Subscribe or (perish the thought) unsubscribe at:

www.cnp-wireless.com/cnpalerts.html.

We believe enterprise security solutions should meet the following security criteria:

- Enforceable mandatory access control;
- Automatic and transparent data encryption;
- Centralized management;
- Software integration, such as single sign-on for ease of use; and
- Automatic encryption key management.

Mandatory Access Control

Access control can be accomplished in several ways. The most common is by requiring a user name and password before access is permitted. This is standard practice to log into desktop computers, laptops, corporate servers and workstations. However, with some operating systems, such as Microsoft Windows™ 95 and 98, one can easily bypass the password and gain unauthorized access. Even operating systems supporting stronger authentication can be hacked via password cracking products like @stake's LophtCrack, or they can be bypassed using a utility such as NTFS DOS.

An Enforceable Mandatory Access Control (EMAC) requires user authentication before the operating system loads. This prevents brute force attacks because the operating system will only load after successful user validation.

Another technique supports a dynamic password via a security token or a 'smart card'. Tokens add an additional layer of security because the password is dynamic – it is constantly changing, and hence it cannot be lost or stolen – nor can it be predicted. Smart Card integration usually uses the *defacto* standard, PKCS #11 (Public Key Cryptography Standard).

Even though this same technology could be used for authenticating access to a PDA, most people do not want to carry tokens and cards in addition to a device that is chosen, at least partly, because of its small size. Signature authentication to the PDA is not always convenient if the stylus is missing or if you are racing through an airport.

Fixed, alphanumeric or numeric non-dynamic passwords for the PDA pose several security flaws. They are easy to hack, can be memorized by "shoulder surfers," and can become etched in the PDA's face plate and easily copied.

To combat the weaknesses of traditional fixed passwords, Pointsec created a dynamic picture-based alternative called the PicturePIN™ (see Figure 1). Users of this system use a sequence of symbols as the password, making up a mnemonic story to help them remember it much more easily than a sequence of random characters.

Figure 1: PicturePIN™ System

This technology provides EMAC that complies with the new tough security legislation stipulated in both the US Graham-Leach Bliley Act (GLB Act) and the Health Information Portability and Accountability Act (HIPAA). This method of authentication is easy to use, easy to remember and difficult to hack. It is designed to be operable with one hand, as one can use a finger to enter in the authentication sequence.

For the organization whose security policy mandates high-security passwords – typically eight or more characters long – it is easier to make up a mnemonic story using simple symbols than it is to make up a random sequence of letters and digits. The login PIN is entered from a set of images, or numbers, that appear in random order each time the user powers up the PDA, including during Hot Sync and InfraRed data transmission. This reduces concern about shoulder surfers and concern about lifting a password that has been etched on the PDA's face.

If the administrator limits the number of password attempts to three, then, upon the third incorrect entry, the device would lock up, making it inaccessible to illicit entry.

The authorized user can regain access to their device via a challenge / response mechanism further explained within the Centralized Management section. If this fails too many times, the device can only be accessed by the administrator via the Recovery Key that was generated when the security software was originally installed onto the PDA. If an unauthorized user continues attempts break into the device, the PDA remains locked, and a reset is required.

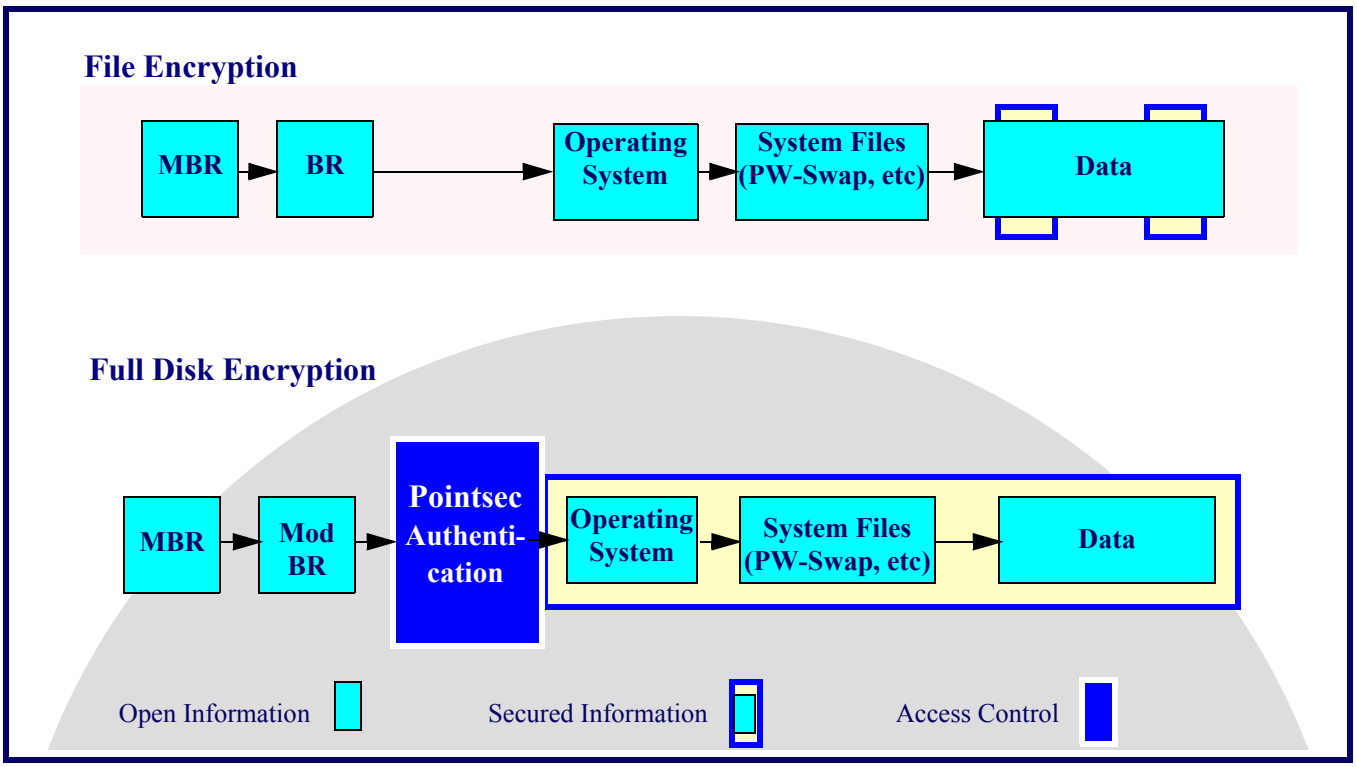
If reset, the illicit user will now be in possession of a data-less PDA and a fully encrypted storage card that will ask to be reformatted when placed into a rogue PDA.

Automatic and User-transparent Encryption

Automatic, complete hard drive encryption that is transparent to the user is another important security feature for the enterprise. Pointsec PC, for example, encrypts everything on the hard drive, including system files, deleted files, and even temporary files. It ensures that all logical partitions are boot protected and encrypted. The Pointsec disk encryption technique, and the typical file encryption method, is illustrated in Figure 2. As shown, the Pointsec encryption approach yields a more secure environment because even the operating system and file system are shielded from access.

The careful integration of boot protection, and automatic and transparent encryption, provides a high degree of security without user involvement or impeding of the laptop's performance. Boot protection prevents subversion of the operating system or the introduction of rogue programs, while sector-by-sector encryption prevents copying individual files for brute force attacks. Full hard drive encryption also secures the data even if the hard

Figure 2: Laptop Encryption Techniques



drive is removed and loaded into an insecure device. This empowers the enterprise to control and enforce security on selected laptops, instead of leaving the responsibility of encryption to the end user.

Transparent encryption means the user is unaware that encryption / decryption is taking place. It is important that initial encryption not render computers unusable, because this would significantly reduce the user's productivity. Some disk encryption products can leave users locked out of their systems for over 10 hours during product installation. It should be possible to initialize the encryption software automatically in the background. Thereafter, encryption and decryption of data should run transparently in the background, with no perceptible degradation in the machine's operating performance.

Security should not be compromised in an attempt to make software more user-friendly. 128 or 256 bit encryption should still be used, even on PDAs. Obviously, encryption should be performed using cryptographically robust algorithms such as the new Advanced Encryption Standard. Typical and proper PDA encryption techniques are shown in Figure 3.

Centralized Security Management

Central administration is essential to making security manageable. When initially deploying a software security product to thousands of mobile devices, it is unthinkable to retrieve every single device in order to install the security software or to upgrade already secured devices.

Security software should be centrally deployed from a designated server controlled by the system administrator. It is essential to centralize the storage of encryption keys to provide remote help and system recovery, but these are only two of the components of central management.

The system administrator should also be able to create an installation profile containing such information as the security policy settings, authorized users, and the products being deployed. Using this installation profile, administrators should be able to perform a silent (automatic) or interactive installation.

Reducing desktop visits via centralized security management saves an enterprise significant time and money. History has shown that for every five dollars spent towards the purchase of a software package, one dollar is spent towards the maintenance of that same package.

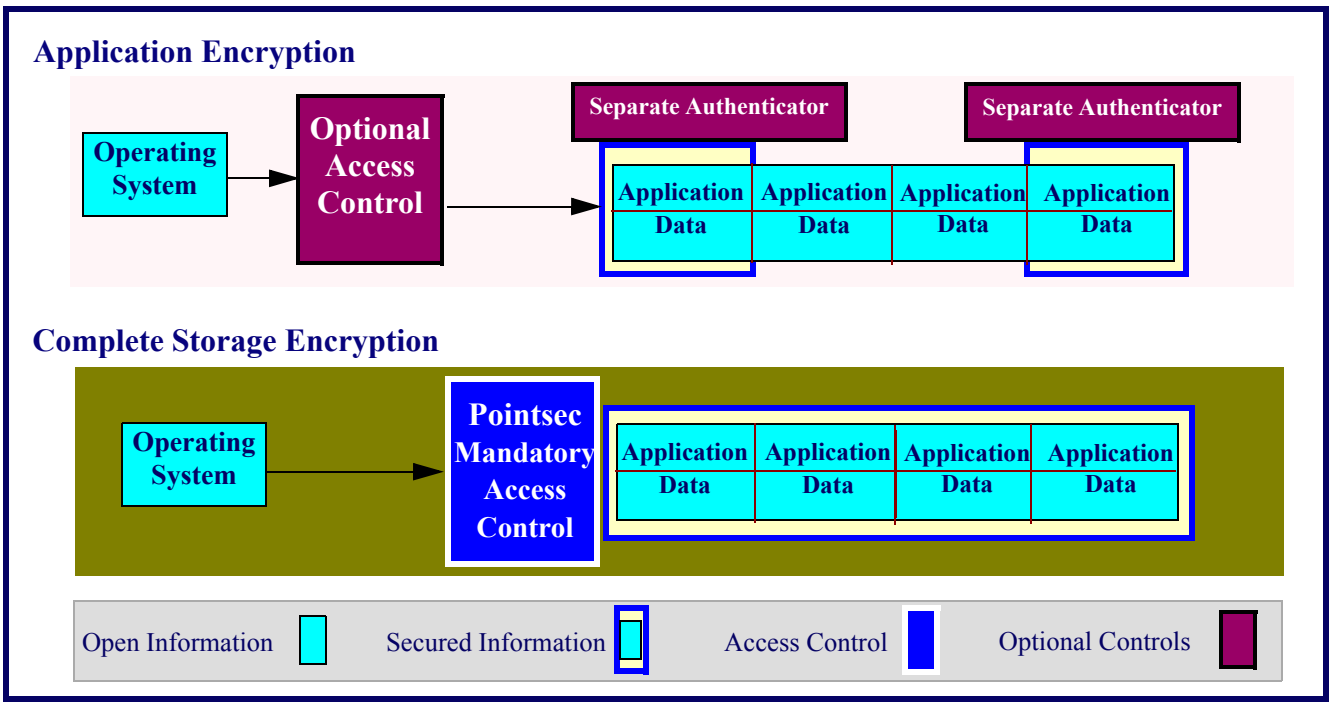
Password Resets

Password resets are costly. Many large organizations spend an average of $200 per employee per year on this security activity. An organization comprising 200,000 employees may employ 180 help desk people whose sole responsibility is resetting passwords.

It is important to provide a remote help function allowing authorized help desk people to provide mobile device access to users when they forget their password. The user contacts the help desk and provides proper identity verification, as well as their username and the challenge shown on their device's screen. The help desk person enters the information into the management system, which calculates the response, which is then provided to the user.

Normally, this will enable the user to regain access to their device and consequently be permitted to reset their password. This should be possible without either individual being connected to the network.

Figure 3: PDA Encryption Techniques



Software Integration

With today's technology, each member of the enterprise work force has many passwords and PINs to remember, both personal and work related.

The use of multiple passwords increases the probability of forgetting one, and it increases security risks, as users are more likely to write their passwords down. Using a system with only one login and password (either fixed or dynamic), the user is able to login to the organization's operating system, PKI product, and network.

Key Management

Enterprise mobile device security needs to be recoverable. To accomplish this, each device's unique encryption key must be centrally accessible. Systems are not acceptable if they utilize a single key to access all devices across the enterprise. This would be like having one key that unlocks all the doors for all the houses in a neighborhood. Nor is it acceptable if they force the administrator to un-install and re-install new keys on every device, should the initial key change due to a security breach or change in personnel.

Though one key does make the recovery process easier, it also means that if multiple laptops are stolen from one organization, all are subject to exploitation. Our recommended method of control is to have each mobile device's encryption key automatically generated and stored when the security software is initially installed. Further, the initial encryption phase will not occur unless the keys are generated and stored within the specified network folder. The keys are saved to a centralized location; typically it is a safely maintained server within the organization's network security infrastructure, not a floppy diskette that is given to the mobile device user.

Machines and humans are fallible; therefore, it is necessary for the enterprise, not the end-user, to have complete control over the recovery keys. Additionally, it is recommended that instead of storing the keys on one central server, recovery keys should be stored on multiple servers.

Keys must be stored centrally so that data and / or systems can be recovered if passwords are forgotten, if the authentication tools are lost, or if the employee has been terminated and is unavailable or unwilling to return their mobile devices. It is crucial that the data recovery process be quick and easy for the administrator.

By having recovery keys stored centrally, an administrator can quickly and easily locate the necessary file and create the recovery disk.

Enterprise Security Is Possible

Some key questions to consider when purchasing a security system are:

- Can the product be integrated across existing multiple networks and operating systems?
- Is there Single Sign-On to these multiple systems?
- Can the product be scaled to tens-of-thousands of users?
- Will end-users have true remote help and access to their devices and data at all times?
- Is the recovery key secure and manageable?

About the Author

Janet Hendrickson is a Technical Marketing Manager at Pointsec Mobile Technologies, Inc. Prior to joining Pointsec Mobile Technologies in late 2000, Janet was the e-commerce security evangelist with CFI Proservices, Inc.,

a financial software vendor, where she developed and led security training and education workshops for banking and financial services executives. Janet has presented at numerous conferences on topics such as PKI, digital certificates, authorization, and other e-commerce solutions for securing on-line banking transactions.

About PointSec

Pointsec™ provides a number of security products and services, including:

- Full login integration (including single sign-on) with Novell™, Microsoft™ and Entrust™ products.
- Enforceable Mandatory Access Control (EMAC) through Pointsec® PC 4.0.
- PicturePIN™ dynamic authentication

To probe further, visit:

www.pointsec.com

IETF Insights

The Internet Engineering Task Force (IETF) has recently published three security-related RFCs (Requests for Comment) that may be of interest to network and wireless security practitioners and theorists.

The first RFC is regarding digital signatures (for authentication, integrity and non-repudiation) for XML – the universal format for structured documents and data on the web. Visit:

www.w3.org/XML

The second RFC is concerned with changing and setting user passwords for Kerberos-based Microsoft Windows 2000. Kerberos, originally developed at MIT, is the strong network authentication protocol based on secret key cryptography. Visit:

web.mit.edu/kerberos/www

The last RFC defines proper procedures for gathering evidence after a "cyber" security incident. This RFC was co-authored by an employee of In-Q-Tel – the DC-based venture catalyst arm of the CIA. Visit:

www.in-q-tel.com

These RFCs are descibed briefly below. For more information, visit the Internet Engineering Task Force website at:

www.ietf.org

or contact the editors of WSP.

RFC 3275: (Extensible Markup Language) XML-Signature Syntax and Processing

Authors: D. Eastlake (Motorola), D. Solo (Citigroup), and J. Reagle (W3C)

Abstract: This document specifies XML (Extensible Markup Language) digital signature processing rules and syntax. XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML including the signature or elsewhere.

RFC 3244: Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols

Published: February 2002

Authors: M. Swift (University of Washington), J. Trostle (Cisco Systems), and J.Brezak (Microsoft)

Abstract: This RFC specifies Microsoft's Windows 2000 Kerberos change password and set password protocols. The Windows 2000 Kerberos change password protocol interoperates with the original Kerberos change password protocol. Change password is a simple "request-reply" protocol that includes a message with the new password for the user.

RFC 3227: Guidelines for Evidence Collection and Archiving

Published: February 2002

Authors: D. Brezinski (In-Q-Tel), and T. Kilalea (neart.org)

Abstract: A "security incident" as defined in the "Internet Security Glossary", RFC 2828, is a security-relevant system event in which the system's security policy is violated. This RFC provides System Administrators (SysAdmins) with guidelines on the collection and archiving of evidence relevant to such a security incident. If evidence gathering is done correctly, apprehending the adversary is more likely, as is successful prosecution.

Fraud And Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following fraud and security patents. These may be of interest to some of our wireless security practitioners. Each patent includes the patent number, the invention title, a brief description, the inventor(s), and the assignee (owner). For select patents, we provide the assignee's URL and contact information. All of these patents were granted in March 2002.

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. These and other references accompanying patents are sometimes useful for broadening one's perspective of wireless communications and security. Access this information using the patent number in the Search field at the USPTO website:

www.uspto.gov

US Patent: 6,360,257

Managing group IP addresses in mobile end stations

Management of group IP addresses, through which various services are provided to groups of mobile end stations in a wireless network, includes accessing the group IP addresses without manually accessing the mobile end stations. This permits efficient management of the membership of the groups that receive the various services.

Issued: March 19, 2002

Inventor: Rydberg, *et al*

Assignee: L.M. Ericsson (Stockholm, SE)

US Patent: 6,360,095

Home location register for a mobile telecommunications network

A HLR (Home location register) has a bus which interconnects a NAP layer, a DBS layer and an OMP layer. All accesses to a memory database are through a single channel – the associated DBS with associated

databases. Each NAP has a directory service identifying the active DB for each item of subscriber data. Each DBS has a shadow DBS to which it automatically writes for real time synchronization.

Issued: March 19, 2002

Inventor: Joseph Cunningham, *et al*

Assignee: Markport Limited (Dublin, IE)

US Patent: 6,360,873

Wireless LAN system and a transmitter-received in a wireless LAN system

In a wireless LAN system, chiefly using a millimeter wave, a satellite station is provided with an active phased planar-array antenna, the radiating directivity characteristic of which can be freely changed. When a master station receives a control frame transmitted from the satellite station prior to the commencement of normal communication, the master station transmits a carrier wave. The satellite station determines such a directivity characteristic of an antenna as to receive this carrier wave with the strongest intensity, and it fixes the characteristic. Thus, an optimal communication environment can be secured. When the number of errors in a received data frame or the receiving electric field intensity received by the satellite station in normal communication is inferior to a respective predetermined threshold, the deterioration of the communication environment can be coped with by determining again. The power consumption of the master station can be reduced by making the transmitting power of a carrier wave for determining less than the transmitting power at the time of normal communication.

Issued: March 19, 2002

Inventor: Naofumi Kobayashi

Assignee: Fujitsu Limited (Kawasaki, JP)

US Patent: 6,359,866

Base station having transceivers for transmitting voice and packet data signals

Support for voice communications and data communications at a base station which has a plurality of transceivers, each having a voice mode of operation and a data mode of operation. A first voice call is assigned to a first transceiver, wherein the mode of the transceiver is set to the voice mode of operation. A data transmission is assigned to a second available transceiver, wherein the mode of the transceiver is set to the data mode of operation. The data transmission is halted when a second voice call needs to be handled by the second transceiver. The mode of operation of the second transceiver is changed from the data mode to the voice mode, and the second call is initiated. The data transmission is then assigned to the next available transceiver, as long as a voice call does not need to be carried, wherein the mode of the transceiver is set to the data mode of operation.

Issued: March 19, 2002

Inventor: H.ang.kan Svensson, *et al*

Assignee: L.M. Ericsson (Stockholm, SE)

US Patent: 6,356,935

Apparatus and method for an authenticated electronic user identification (userid)

A method and apparatus for an authenticated electronic userid is provided. According to one embodiment, an adapted digital signature is generated for an outbound message from a local user that authorizes a remote user to reply to the message. The adapted digital signature becomes part of an authenticated electronic userid and, when a reply from the remote user is made, the reply message includes the authenticated electronic userid. A one-way hash function is employed to generate the adapted digital signature. According to one embodiment, if an inbound message to a local user from a remote user does not have an authenticated electronic userid – in particular the adapted digital signature – then the inbound message is rejected. An advantage of the method and apparatus described herein is that unsolicited bulk electronic messages and other non-authorized communications to a local user of an electronic message system are reduced

Issued: March 12, 2002

Inventor: Benjamin K. Gibbs

Assignee: Xircom Wireless, Inc.

xircom.com

Intel® Corporation acquired Xircom® in March 2001. All corporate information, including press releases, employment opportunities, investor relations, and other information, may be found at:

www.intel.com

US Patent: 6,356,766

Compressed data service in DECT/GSM networking

A DECT fixed part for providing a communications link between a DECT portable part and a GSM mobile switch center, the fixed part comprising a compression negotiation means for: Receiving, from one of the portable part and the mobile switch center, a first message specifying a form of compression for a data service; and using that first message, determining a second message to be sent to the other of the portable part and the mobile switch center, to request it to adopt a corresponding form of compression for the data service; so as to allow the provision of a compressed data service between the portable part and the mobile switch center.

Issued: March 12, 2002

Inventor: Tuomo Sipila

Assignee: Nokia Mobile Phones Ltd (Espoo, FI)

US Patent: 6,356,753

Management of authentication and encryption user information in digital user terminals

Methods and devices for controlling the authentication and ciphering procedures in digital communication devices. In the invention, a means for transmitting and receiving radio signals, is connected with a processing unit. A. SIM is provided, which contains authentication and ciphering information, and this is also connected with the processing unit. The invention provides a memory module, with a first memory location reserved for a authentication flag and a second memory location reserved for a ciphering flag. During operation, an authentication indicator is activated only when the communication device is authenticated during a system access. In addition, a ciphering indicator is activated when the communication device is encrypting data being sent and received from the digital wireless network.

Issued: March 12, 2002

Inventor: Javor Kolev, *et al*

Assignee: Same

US Patent: 6,356,752

Wireless telephone as a transaction device

Utilizing a wireless telephone functioning as a transaction device, the wireless telephone places a call to a site computer controlling a transaction unit. For example, the transaction unit may be a cash register at a supermarket. The wireless telephone then transfers to the transaction unit account information specifying the type of account against which the transaction is to be billed, and it relays identification of that transaction. The site computer controlling the transaction unit responds with a transaction number, which is transmitted to the transaction unit and to the wireless telephone. The user of the wireless telephone then confirms the transaction when the correct transaction number is displayed on the transaction unit. After the transaction is completed, the site computer controlling the transaction unit transmits the data defining the transaction to the wireless telephone, which stores this information in a database associated with the account against which the transaction was charged. In a second embodiment, the transaction number is not visually displayed, but rather, it is transmitted over a second transmission media to the wireless telephone confirming that the correct transaction is taking place.

Issued: March 12, 2002

Inventor: Gary L. Griffith

Assignee: Avaya Technology Corp.

avaya.com

Avaya provides unified messaging, messaging systems, call centers and structured cabling systems; they are also a producer of voice communications systems and services. Avaya's broad customer base includes nearly one million customers worldwide. In fiscal 2001, Avaya had revenue of approximately $6.8 billion and net income of approximately $214 million.

US Patent: 6,356,638

Radio wireline interface and method for secure communication

An interface between a digital communication system and a PSTN establishes a user-configurable, secure, encrypted link to a digital subscriber unit through the digital communication system, and it provides clear (unencrypted) voice to telephone sets through the PSTN. The interface includes a security module for encrypting and decrypting information with user specific algorithms and keys, a transcoder for converting modulated voice to digital voice and a modem for modulating and demodulating data and encrypted voice. Accordingly, the wireline interface allows for user specified security over a digital wireless portion of an end-to-end communication channel. The interface also provides for the communication of unencrypted voice followed by secure voice or secure data.

Issued: March 12, 2002

Inventor: Douglas Allan Hardy, *et al*

Assignee: General Dynamics Decision Systems, Inc.

www.generaldynamics.com

General Dynamics has leading market positions in business aviation, mission-critical information systems and technologies, shipbuilding and marine systems, and land and amphibious combat systems. The company is a leading supplier of sophisticated defense systems to the United States and its allies, setting the world standard in business jets. It is headquartered in Falls Church, Virginia, and it employs approximately 52,000 people worldwide. General Dynamics has four main business segments: Aerospace, Combat System Information Systems and Technology, and Marine Systems.

US Patent: 6,356,529

System and method for rapid wireless application protocol translation

A method and a system for translating between data transmitted according to the WAP network protocols and data transmitted according to IP protocols. The system and method enable the translation process to be performed as soon as a minimal portion of data has been received by the gateway translator. This minimal portion is determined according to rules, such as the type of received data and flags within the received data. Therefore, the translation process is performed according to an atomic, state machine mechanism only on the received data, rather than by forcing the gateway translator to open two complete sessions and then attempting to mediate between these sessions. Thus, the method and system of the present invention are much faster and more efficient than those which are known in the background art.

Issued: March 12, 2002

Inventor: Rony Zarom

Assignee: Converse Ltd. (Tel Aviv, IL)

US Patent: 6,356,192

Bi-directional wireless detection system

A system for detecting at least one event of interest. The system comprises a detector, a programmable controller, and a network. Upon detection of an event of interest, the detector communicates that information to the programmable controller through the network. The programmable controller allows a user, who may be in diverse geographic locations, to control the detector.

Issued: March 12, 2002

Inventor: Raymond Menard

Assignee: Royal Thoughts LLC

US Patent: 6,353,599

Wireless enumeration

A system which includes a plurality of wireless interface devices, adapted to be interfaced with a server, connected in either a wireless or wired LAN. Prior to an interface being established, the wireless interface device broadcasts for available servers which, upon acknowledgment are displayed in a dialog box on the display of the wireless interface device. The user selects an available server from the dialog box for connection to the wireless interface device.

Issued: March 12, 2002

Inventor: Depeng Bi, *et al*

Assignee: NEC Corporation

US Patent: 6,353,472

Device for authenticating a person on the basis of his fingerprints

The device includes a housing having a track for sliding the finger, and a sensor having a dimension less than that of the finger. The sensor is disposed within the track.

Issued: March 5, 2002

Inventor: Richard Bault

Assignee: Same.

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