Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: wsp@cnp-wireless.com Vol. 3, No. 10. November, 2001

Wireless LAN Security in 802.11b Enterprise Networks

Christopher W. Klaus
(Internet Security Systems, Inc.)

Editor's Foreword

Last month's issue of *Wireless Security Perspectives* was an article, written by RSA Security, about one of several industry proposals for enhancing the security of IEEE 802.11b WLAN technology. Many of the proposals were developed to address the problems of WEP, including weak authentication, poor confidentiality protection and key management that does not scale. This issue of *Wireless Security Perspectives* is a practical view of some of the risks in the 802.11b environment.

This issue's article, written by Internet Security Systems, identifies some of the security problems organizations are having today. Its intent is to raise awareness and understanding, and to provide some straight-forward guidelines for minimizing the security risks in an 802.11b environment, which can be used both in the short-term and over the long haul.

Introduction

Although a variety of wireless network technologies have reached or will soon reach the general business market, wireless LANs based on the 802.11 standard have already become quite popular in corporate environments, and soon they are likely to become widely prevalent. Current 802.11b products operate at 2.4GHz,delivering up to 11Mbps of bandwidth. This is comparable to the performance of a standard Ethernet wired LAN. An upcoming version called 802.11a moves to a higher frequency range and promises significantly faster speeds. However, it is expected to have security concerns similar those of 802.11b.

The low cost of 802.11b, combined with its strong performance and ease of deployment, have provided impetus for many organizations – and even individual consumers – to use 802.11b at home or at work. This increased usage often occurs without permission or knowledge of the IT staff and security management administrator. This article addresses the security concerns raised by both current and upcoming 802.11 network technologies.

Known Security Risks of 802.11b

802.11b wireless LAN technology's low cost of entry is one very attractive characteristic for deployment. However, inexpensive equipment also often creates the opportunity for adversaries to mount security attacks against it. Attacks against 802.11b and other wireless technologies will undoubtedly increase in number and sophistication over time.

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…

December 17th, 2001.

Future Topics

Wireless Packet Data Security • IP Security • Public Keys & Wireless • IP Mobility Security • Security Issues in Ad hoc Wireless Networks • Electronic Signatures in Wireless • Latest in Watermarking • Security for PDAs • Blackberry • 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: Les Owens.
Article Sourcing: Betsy Harter.
Production: Doug Scofield.
Distribution: Debbie Brandelli.
Marketing: Muneerah Vasanji.
Accounts: Evelyn Goreham.
Publisher: David Crowe.

However, most current 802.11b risks fall into seven fundamental categories.

- Insertion attacks
- Interception and unauthorized monitoring of wireless traffic
- Jamming
- Client-to-Client attacks
- Brute force attacks against access point passwords
- Encryption attacks
- Misconfigurations

Fully understanding these risks and using this to proactively thwart their success is a wise security strategy. Anyone deploying 802.11b (or any wireless technology, for that matter) should follow this strategy to mitigate these risks and avoid potential security breaches. It is also important to note that this risk classification applies not only to 802.11b, but to any wireless technology.

Insertion Attacks

Insertion attacks are based on simple unauthorized access by wireless devices. The unauthorized access can occur on a "known" wireless network or on one created, perhaps surreptitiously, without going through a methodical security process and review. These two methods are discussed briefly below.

Unauthorized Clients – An attacker connects a wireless client, typically a laptop or PDA, to an access point without authorization. Access points (AP's) can be configured to require a network name to be programmed for client access. This network name, the SSID (Service Set ID), is sometimes considered a password, but it is really simply an identifier. If no identifier is programmed, an intruder can connect to the internal network by simply powering on the wireless client and having it actively scan for the access point, to which it will automatically attach. Note also, however, that some access points use the same identifier for all client access. As a result, this requires all users to adopt a new identifier every time the identifier is changed. This presents some challenging scalability problems.

Unauthorized or Renegade Access Points – An organization may not be aware that an internal employee has deployed wireless capabilities on the enterprise network. For example, the IT team may not be aware that a member of product development has deployed an AP to facilitate in-building mobility and productivity enhancement. This lack of awareness could lead to the attack described previously – unauthorized clients gain access to corporate resources through this 'rogue' access point. Organizations need to implement an IT security policy to ensure that:

a. Whoever is responsible for network security is aware of plans for installation of access points, and

b. AP's are installed with a secure configuration.

Additionally, the organization should consider instituting a process whereby the network is scanned for the presence of unauthorized devices.

Interception and Monitoring of Wireless Traffic

As in wired networks, it is possible to intercept and monitor network traffic across a wireless LAN. The attacker needs to be close for this attack to work, whereas a wired attacker can be anywhere, provided there is a functioning network connection. The advantage for a wireless interception, however, is that, whereas a wired attack requires the placement of a monitoring agent on a compromised system, a wireless intruder needs only a "sniffer" and access to the network data stream as it is broadcast.

There are two important considerations to keep in mind with the range of 802.11b access points. First, although legitimate 802.11b clients must be within about 100 meters (300 feet) of an access point, directional antennas can significantly extend the transmission or reception range, increasing the risk of interception. Second, access points transmit signals in a manner that almost always extends beyond the physical boundaries of the work area it is intended to cover. This signal can be intercepted outside buildings or even through floors in multi-story buildings. Careful antenna placement can significantly affect the ability of the 802.11b signal to reach beyond physical corporate boundaries.

Below are three examples of interception attacks that further clarify this risk:

Wireless Packet Analysis – A skilled attacker captures wireless traffic using techniques similar to those employed on wired networks. Many of these tools capture the first part of the connection session, in which the data typically includes the user name and password. An intruder can then masquerade as a legitimate user by using this captured information to hijack the user session, subsequently issuing unauthorized commands, in the usual cases.

Broadcast Monitoring – If an access point is connected to a hub rather than a switch, any network traffic across that hub can be potentially broadcast over the wireless network. Because the Ethernet hub broadcasts all data packets to all connected devices, including the wireless access point, an attacker can monitor sensitive data that is not intended for any wireless clients as it goes over wireless.

Access Point Clone (Evil Twin) Traffic Interception - An attacker fools legitimate wireless clients into connecting to the attacker's own network by placing an unauthorized access point with a stronger signal in close proximity to wireless clients. Users attempt to log into the substitute servers and unknowingly give away passwords and similar sensitive data.

Jamming

Denial-of-service attacks are also easily applied to wireless networks, where legitimate traffic cannot reach clients or the access point because illegitimate traffic overwhelms the ISM-band (Industrial, Scientific, and Medical) frequencies. An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency, corrupting the signal until the wireless network ceases to function. In addition, cordless phones, baby monitors and other devices that operate on the 2.4 GHz band can potentially disrupt a wireless network using this frequency. These denials of service can originate from outside the

Upcoming Fraud and Security Events

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

802.11 Planet Conference and Expo – Fall 2001
27-28 November, 2001
Convention Center
Santa Clara, CA
seminars.internet.com/80211/fall01

Wireless LANs
28-30 November, 2001
Radisson Miyako
San Francisco, CA
www.iirusa.com/wirelesslans/index.cfm

International Cryptography Institute 2001: Global Challenges, Trends, and Best Practices in Cryptography
29-30 November, 2001
Four Seasons Hotel
Washington, DC
www.nipli.org

Information Integrity World Summit
2-5 December, 2001
Omni Rosen Centre Hotel
Orlando, FL
www.411integrity.com

The Business of eBusiness Conference and Expo
2-5 December 2001
Phoenix, AZ
www.misti.com

Privacy By Design 2001
3-5 December, 2001
Fairmont The Queen Elizabeth Hotel
Montreal
privacy.zeroknowledge.com/privacybydesign2001

Infosecurity Conference and Exhibition
4-6 December, 2001
Jacob Javits Center
New York, NY
www.infosecurityevent.com

work area serviced by the access point, or they can inadvertently arrive from other 802.11b devices installed in other work areas that degrade the overall signal.

Client-to-Client Attacks

Two wireless clients can communicate directly to each other in an *ad hoc* fashion, bypassing the access point. Users, therefore, need to defend clients against each other, in addition to external threats. Below are two attacks associated with client-to-client communication.

. . . More Upcoming Events

Asiacrypt 2001
9-13 December, 2001
Gold Coast – Australia
www.isrc.qut.edu.au/asiacrypt

Internet World Fall 2001
10-14 December, 2001
Jacob Javits Center
New York, NY
www.internetworld.com/events/fall2001

Annual Computer Security Applications Conference
10-14 December, 2001
Sheraton New Orleans
New Orleans, LA
www.acsac.org

Mobile Business for the Enterprise Conference and Exhibition
12-14 December, 2001
Convention Center
Los Angeles, CA
www.dci.com/ffa

SANS Institute
Cyber Defense Initiative – West
16 - 21 December, 2001
San Francisco, CA
www.sans.org/CDIwest/glance.htm

Chaos Communication Congress
27-29 December, 2001
Berlin, Germany
www.ccc.de/congress

File Sharing and Other TCP/IP Service Attacks – Wireless clients running TCP/IP services such as a Web server or file sharing are open to the same exploits and misconfigurations as any user on a wired network.

Denial of Service – A wireless device floods other wireless clients with bogus packets, creating a denial of service attack. In addition, duplicate IP (Internet Protocol) or MAC (Media Access Control) addresses, both intentional and accidental, can disrupt the network.

Brute Force Attacks Against Access Point Passwords

Many access points use a single cryptographic key that is shared with all connecting wireless clients. Brute force attacks attempt to compromise this key by methodically testing every possibility. The intruder gains access to the access point once the key is guessed.

Additionally, keys can be compromised through less aggressive means. A compromised client can then expose the access point. Not changing the keys on a frequent basis or when employees (e.g., terminated) leave the organization also subjects the access point to attack. Managing a large number of access points and clients only complicates this issue, often resulting in lax security practices.

Attacks against Encryption

The 802.11b standard uses an encryption system called the Wired Equivalent Privacy (WEP) protocol. WEP has several known and well-publicized weaknesses. Refer to:

www.isaac.cs.berkeley.edu/isaac/wep-faq.html

for more information. Moreover, these issues are not scheduled to be addressed by the IEEE until 2002. Some tools are readily available for exploiting WEP and a sophisticated attacker can certainly build his own.

Misconfiguration

Many access points are shipped in an unsecured configuration in order to facilitate ease of use and rapid deploy-

ment. Unless administrators understand wireless security risks and unless they properly configure each unit prior to deployment, these access points will remain at a high risk for attack or misuse. Below we present several examples of misconfigurations.

Service Set Identifier (SSID) – The SSID (Service Set ID) is a configurable identification parameter allowing clients to communicate with an appropriate access point. With proper configuration, only clients with the correct SSID can attach to access points. In effect, the SSID acts as a single shared "password" between access points and clients. Access points come with default SSIDs. If these are not changed, the result can be easy compromise. Four common manufacturer default SSIDs are the following: *tsunami, 101, WLAN, and Default SSID*. The SSID is transmitted wirelessly *in-the-clear*, allowing it to be captured by anyone monitoring the network's traffic. Additionally, clients of some manufacturers connect to the access point using the configured SSID, or an SSID configured as "any" or even if null (empty).

Wired Equivalent Privacy (WEP) – WEP can be typically configured with no encryption, with 40-bit encryption or with 128-bit encryption. However, most access points ship with WEP disabled as the default. Although 128-bit encryption is, in general, more effective than 40-bit encryption, both key strengths are subject to WEP's known flaws.

SNMP Community Passwords – Many wireless access points run SNMP (Simple Network Management Protocol) agents. If the SNMP community string is not properly configured, an intruder can read and potentially write sensitive data on the access point. If SNMP agents are enabled on the wireless clients, the same risk applies to them as well. By default, many access points are read accessible by using the community string "public".

Configuration Interfaces – Access points typically have several interfaces for viewing and modifying configuration data. These include SNMP, a serial interface, a Web interface, and a telnet interface. An attacker who locates an access point with a Web interface can easily get the SSID from the "system properties" menu display. Some access points do require a password on the Web interface for write privileges. However, this password is frequently a default that is never changed.

Client Side Security Risk – Clients store sensitive information for authenticating and communicating to an access point. This information can be compromised if the client is not properly configured. Some manufacturers' client software stores the SSID in the Windows registry. Storage in this way allows easy access. Also, the WEP keys are available for access. These keys are sometimes stored in the firmware or stored encrypted or in plaintext form in the Windows registry. As a result, these can be viewed and potentially compromised.

Managing Wireless Information Security

Process and technology are always easily confused, and this seems never more so than with wireless information security management. In fact, the same business processes establishing strong risk management practices for physical assets and wired networks also work to protect wireless resources.

The following cost-effective guidelines help organizations establish proper security protections as part of an overall wireless strategy. These methods will continue to work in spite of the rapid evolution of wireless networking. The following items are an introduction to this approach.

Wireless Security Policy and Architecture Design – Security policy, procedures and best practices should include wireless networking as part of an overall security management architecture to determine what is and is not allowed with wireless technology.

Treat Access Points As Untrusted – Access points need to be identified and evaluated on a regular basis to determine if they need to be quarantined as untrusted devices before wireless clients can gain access to internal networks. This determination means appropriate placement of firewalls, virtual private networks (VPNs), intrusion detection systems (IDSs), and authentication between access point and intranets or the Internet.

Figure 1 depicts a properly configured intranet or internal network for handling wireless traffic, with two firewalls in place, plus intrusion detection and response sensors to monitor traffic on the wireless segment. One firewall controls access to and from the Internet. The other controls access to and from the wireless access point. The access point itself is the bridge connecting mobile clients to the internal network. Note the inclusion of an intrusion detection system for detecting anomalous or illegal network activity.

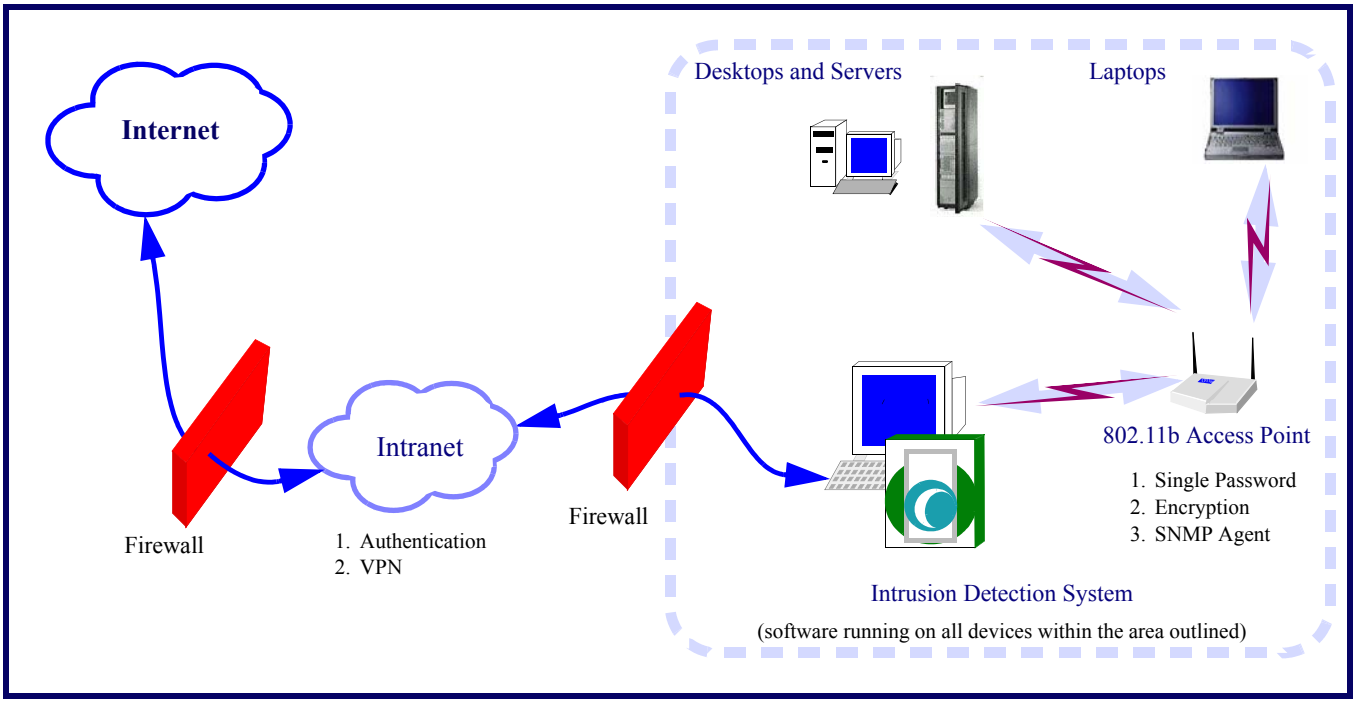
Access Point Configuration Policy – Administrators need to define standard security settings for any 802.11b access point before it can be deployed. These guidelines should cover SSID, WEP keys and encryption, and SNMP community strings.

Access Point Discovery – Administrators should regularly search outwards from a wired network to identify unknown access points. Several methods of identifying 802.11b devices exist, including detection via banner strings on access points with either Web or telnet interfaces.

Wireless network searches can identify unauthorized access points by setting up a 2.4 GHz monitoring agent – a sniffer – that searches for 802.11b packets in the air. These packets may contain IP addresses that identify which network they are on, and this information could indicate rogue access points operating in the area. It is important to note that this process may also detect access points from other organizations in densely populated areas.

Access Point Security Assessments – Regular security audits and penetration assessments quickly identify poorly configured access

Figure 1: Typical Enterprise with 802.11b Wireless LAN Enablement



points, default or easily guessed identifiers, passwords and community strings, plus these should reveal the presence or absence of encryption. Router ACLs (Access Control Lists) and firewall rules also help minimize access to the SNMP agents and other interfaces on the access point.

Wireless Client Protection – Wireless clients need to be regularly examined for good security practices. These procedures should include the presence of some or all of the following:

- Distributed personal firewalls to lock down access to the client
- VPNs to supplement encryption and authentication beyond what 802.11b can provide
- Intrusion detection and response to identify and minimize attacks from intruders, viruses, Trojans and back-doors (as shown above)
- Desktop assessments to identify and repair security issues on the client device

Managed Security Services for Wireless – Managed Security Services (MSS) help organizations establish effective security practices without the overhead of an extensive in-house solution. MSS providers handle assessment, design, deployment, management and support across a broad range of information security disciplines. These providers offer 24/7/365 solutions. Working with the customer, they help to set policy and architecture, plus they provide emergency response, if needed. These services may help an organization operating wireless networks to:

- Deploy firewalls that separate wireless networks from internal networks or the Internet
- Establish and monitor VPN gateways and VPN wireless clients
- Maintain an intrusion detection system on the wireless network to identify and respond to attacks and misuse before critical digital resources are placed at risk.

Following the guidelines presented here will help enable organizations to establish proper security protections as part of an overall wireless strategy.

About Internet Security Systems (ISS)

Internet Security Systems (ISS) is a world leader in software and services that protect critical online resources from attack and misuse. Their services include policy design, security assessments and penetration testing for networks, including 802.11. They also provide training, vulnerability scanning and intrusion detection specifically oriented to networks with 802.11 components. In addition, their website maintains a list of security advisories. RealSecure® is their intrusion dectecion system specifically designed for use in 802.11 corporate intranets.

ISS is headquartered in Atlanta, GA, with additional operations throughout the United States and in Asia, Australia, Europe, Latin America and the Middle East. For more information on ISS, visit their web-site at:

www.iss.net

For more information on wireless information security, on 802.11 security guidelines or for assistance with a wireless security strategy or implementation, please contact the author at:

author@iss.net.

About the Author

Christopher W. Klaus is the Founder and Chief Technology Officer of Internet Security Systems, Inc. (ISS), a leading global provider of information protection solutions that secure the IT infrastructure and key online information assets. Klaus founded Internet Security Systems in 1994 to help corporations and organizations around the world safeguard their critical data from the ever-growing number of network security vulnerabilities and threats. By offering industry leading security management software, managed security services, strategic consulting and education – offering solutions for enterprise, mid-tier, SOHO and consumer markets – ISS is the trusted security provider for its customers, protecting online resources and ensuring/enabling safe, uninterrupted business operations.

Crypto in the News

The National Institute of Standards and Technology (NIST) approved the Secure Hash Standard more than 5 years ago. The standard specifies a Secure Hash Algorithm (SHA-1) for computing a "condensed representation of a message or a data file" – basically, creating a digital "fingerprint" of the data. When a message of arbitrary length is applied to the SHA-1 algorithm, it produces a 160-bit output called a message digest (or hash). The 160-bit hash value, because of some critical cryptographic properties of SHA-1, represents the data that was provided to the algorithm.

The SHA-1 hash algorithm can be used in various applications to provide a data integrity security service – that is, to detect if data has been modified in transit or in storage. SHA-1 is also intended for computationally intensive digital signature applications. For digital signatures, it is much quicker and more efficient to sign a digital "fingerprint" than to sign an actual message. With the use of the hash, performance is improved immensely and robust security is not compromised. Incidentally, SHA-1 is also specified for Third Generation (3G) cellular radiolink integrity protection.

Dallas Semiconductor has recently announced a few additions to its family of secure memory products. Capitalizing on the security capabilities of SHA-1, their one-wire EEPROM (Electrically Erasable Programmable Read-Only Memory) products can be used in secure memory storage applications. The SHA-1 algorithm can be used to prevent the cloning of devices such as circuit cards, memory modules and battery packs. The small footprint, low-power devices can cheaply increase the security of embedded designs. Some of the memory components also come with handy on-board real-time clocks.

For information on Dallas Semiconductor secure memory products and other secure integrated circuits, visit:

www.dallassemiconductor.com

For more information on SHA-1, visit the NIST site at:

www.itl.nist.gov/fipspubs/fip180-1.htm

Contact the editors of WSP for more information on how to use Dallas Semiconductor security components or use SHA-1 to improve the security of a design or network.

Fraud And Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following 15 fraud and security patents. The patent number, invention title, inventor, and assignee (owner) are provided. All of these patents were granted in October or November 2001.

These may be of interest to some of our wireless security practitioners. 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, the references cited or other references included in the patent. For select patents provided below, we provide the URL, contact information, and some information about the assignee.

For a complete analysis of the applicability, efficacy and merit of the patents below, contact the editors of *Wireless Security Perspectives.*

US Patent: 6,314,521

Secure configuration of a digital certificate for a printer or other network device

Issued: November 6, 2001

Inventor: Roger K. Debry

Assignee: International Business Machines Corporation (Armonk, NY)

US Patent: 6,314,519

Secure messaging system overlay for a selective call signaling system

Issued: November 6, 2001

Inventors: Walter Lee David and Jeff LaVell

Assignee: Motorola, Inc. (Schaumburg, IL)

US Patent: 6,314,468

System and method for managing transmission of electronic data between trading partners

Issued: November 6, 2001

Inventors: John Murphy and Lee Anderson

Assignee: MCI WorldCom, Inc. (Washington, DC)

US Patent: 6,314,440

Pseudo random number generator

Issued: November 6, 2001

Inventor: James O'Toole et. al.

Assignee: Micron Technology, Inc. (Boise, ID)

US Patent: 6,314,425

Apparatus and methods for use of access tokens in an internet document management system

Issued: November 6, 2001

Inventors: Michael Serbinis and Evan Chrapko

Assignee: Critical Path, Inc. (San Francisco, CA)

www.cp.net

Contact:

Critical Path Inc.
532 Folsom Street
San Francisco, CA 94105

Telephone: (415) 808-8777 or toll-free at (877) 441-PATH

Critical Path provides communication technology and messaging solutions to service providers, wireless and wireline carriers, enterprise corporations and postal authorities around the globe. From headquarters in San Francisco, Critical Path is focused on providing solutions that move companies from basic messaging to intelligent messaging.

US Patent: 6,314,409

System for controlling access and distribution of digital property

Issued: November 6, 2001

Inventors: Paul Schneck and Marshall Abrams

Assignee: Veridian Information Solutions

www.veridian.com

Contact:

Veridian
1200 South Hayes Street, Suite 1100
Arlington, VA 22202

Telephone: (703) 575-3100

Veridian is a knowledge applications company providing full service, integrated solutions to customers in national defense, critical infrastructure and essential business systems. Veridian is also involved in cyber security controls to ensure delivery of secure infrastructure.

US Patent: 6,314,408

Method and apparatus for controlling access to a product

Issued: November 6, 2001

Inventor: Pito Salas et. al.

Assignee: eRoom Technology, Inc. (Cambridge, MA)

US Patent: 6,314,401

Mobile voice verification system

Issued: November 6, 2001

Inventor: Stephen Abbe et. al.

Assignee: New York State Technology Enterprise Corporation (Rome, NY)

US Patent: 6,314,190

Cryptographic system with methods for user-controlled message recovery

Issued: November 6, 2001

Inventor: Philip Zimmermann

Assignee: Networks Associates Technology, Inc. (Santa Clara, CA)

US Patent: 6,311,272

Biometric system and techniques suitable therefor

Issued: October 30, 2001

Inventor: Carmi David Gressel

Assignee: M-Systems Flash Disk Pioneers Ltd. (Kfar Saba, IL)

US Patent: 6,311,171

Symmetrically-secured electronic communication system

Issued: October 30, 2001

Inventor: Paul Dent

Assignee: Ericsson Inc. (Research Triangle Park, NC)

US Patent: 6,311,170

Method and apparatus for making payments and delivering payment information

Issued: October 30, 2001

Inventor: Mark Embrey

US Patent: 6,311,167

Portable 2-way wireless financial messaging unit

Issued: October 30, 2001

Inventor: Walter Davis et. al.

Assignee: Motorola, Inc. (Schaumburg, IL)

US Patent: 6,311,160

Method and system for registering the location of a mobile cellular communications device

Issued: October 30, 2001

Inventor: Thomas Evans et. al.

Assignee: Cellemetry LLC (Atlanta, GA)

www.cellemetry.com

Contact:

Numerex Technologies
1600 Parkwood Circle, Suite 200
Atlanta, GA 30339

Attn: Cellemetry Data Services

Telephone: (770) 635-0730 or toll-free at (800) 665-5686

Cellemetry provides two-way, wireless data connectivity for a variety of machine-to-machine communications that remotely monitor, measure or track fixed and mobile assets.

US Patent: 6,310,549

Wireless security system

Issued: October 30, 2001

Inventor: Jon Loftin et. al.

Assignee: Digitech International (Asheville, NC)

To review the specification and claims of these patents, visit the US Patent and Trademark Office web-site at

www.uspto.gov

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