Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 5, No. 8. August, 2003

Security for 802.16 Networks

Carl Eklund, Nokia Research Center

The IEEE 802.16 standard, published in April 2002, standardizes an air interface specification for wireless metropolitan area networks (MANs). The standard defines medium access control (MAC) layer and physical layer specifications for point-to-multipoint radio systems operating in bands between 10 GHz and 66 GHz. These systems are also referred to as WirelessMAN-SC systems, with SC referring to the single carrier modulation used in the radio.

The standard's scope was broadened by IEEE 802.16a, published in April 2003, to include systems operating at frequencies from 2 GHz to 11 GHz and using a mesh topology. This standard also includes orthogonal frequency division multiplexing (OFDM), referred to as WirelessMAN-OFDM. To ensure interoperability between WirelessMAN-SC and WirelessMAN-OFDM systems, companies supporting the IEEE 802.16 standards formed the WiMAX Forum. This association works with the IEEE 802.16 working group to create compliance test specifications. Eventually, they will certify systems for interoperability.

This article discusses the link layer security features defined in the IEEE 802.16 standards.

Overview of 802.16 MANs

Today's WirelessMAN systems are second-generation technology for broadband wireless access (BWA), linking homes and businesses to core telecommunications networks world-wide. These systems are used in metropolitan area networks with either a point-to-multi-point (PMP) or a mesh topology. The PMP system consists of a Base Station (BS) and a number of Subscriber Stations (SS). The BS communicates directly over the wireless link with all Subscriber Stations, while each SS only is in direct communication with the BS. The system architecture is illustrated in **Figure 1**.

In the mesh case, the BS only communicates with a subset of the Subscriber Stations. Each of these can, in turn, relay traffic to and from others that might not be directly reachable from the BS. The mesh system might be deployed as depicted in **Figure 2**.

About Wireless Security Perspectives

Price

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

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

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

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

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due…

September 29th, 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**: cnpsales@cnp-wireless.com **Web**: www.cnp-wireless.com/wsp.html **Subscriptions**: $350 for delivery in the USA or Canada, US$400 elsewhere. **Payment**: accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery**: Email or 1st class mail. **Back Issues**: Available individually for $35 in the US and Canada and US$40 elsewhere, or in bulk at reduced rates. **Discounts**: Educational and small business discount: 25% off any order. **Copies**: Each subscriber is licensed to make up to 10 copies of each issue or back issue. Call for rates to allow more copies.

Technical Editor and Illustrator: Les Owens.

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

Figure 1: WirelessMAN System Architecture

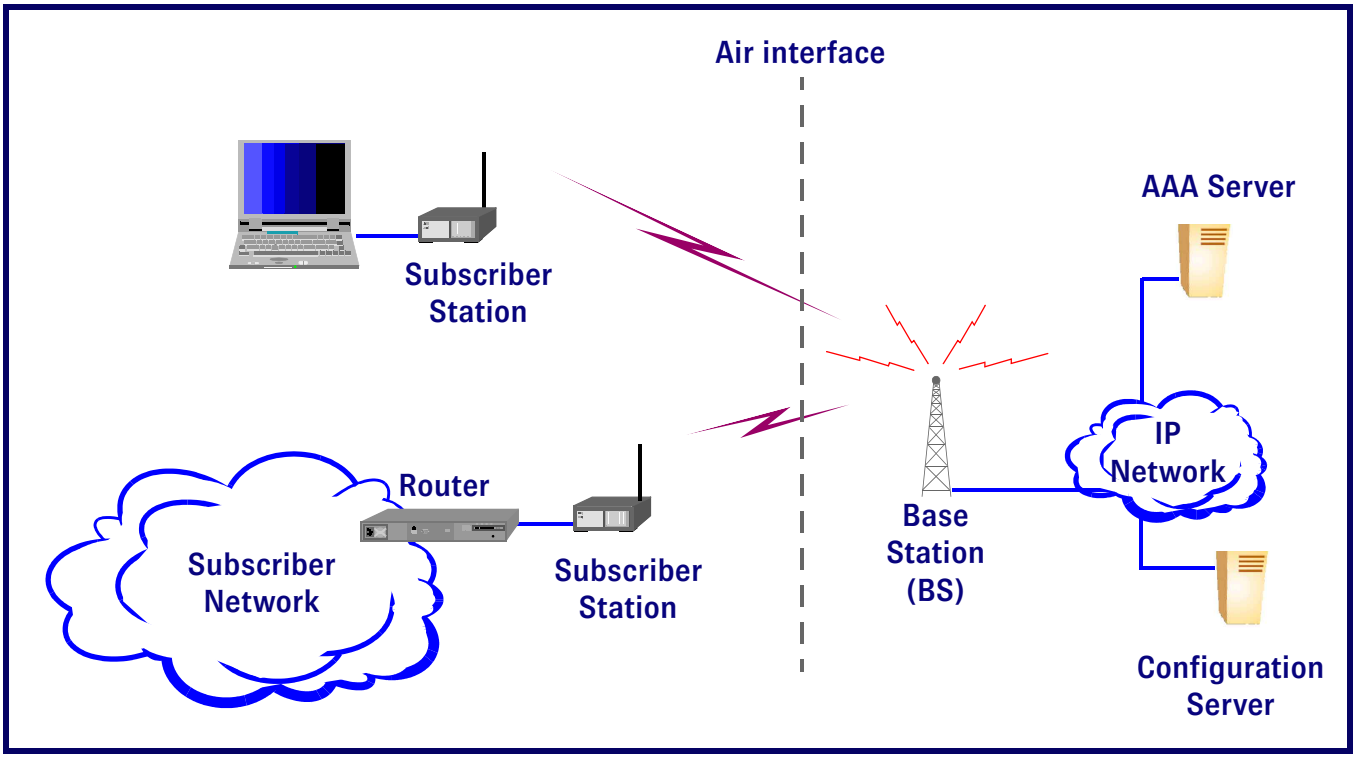
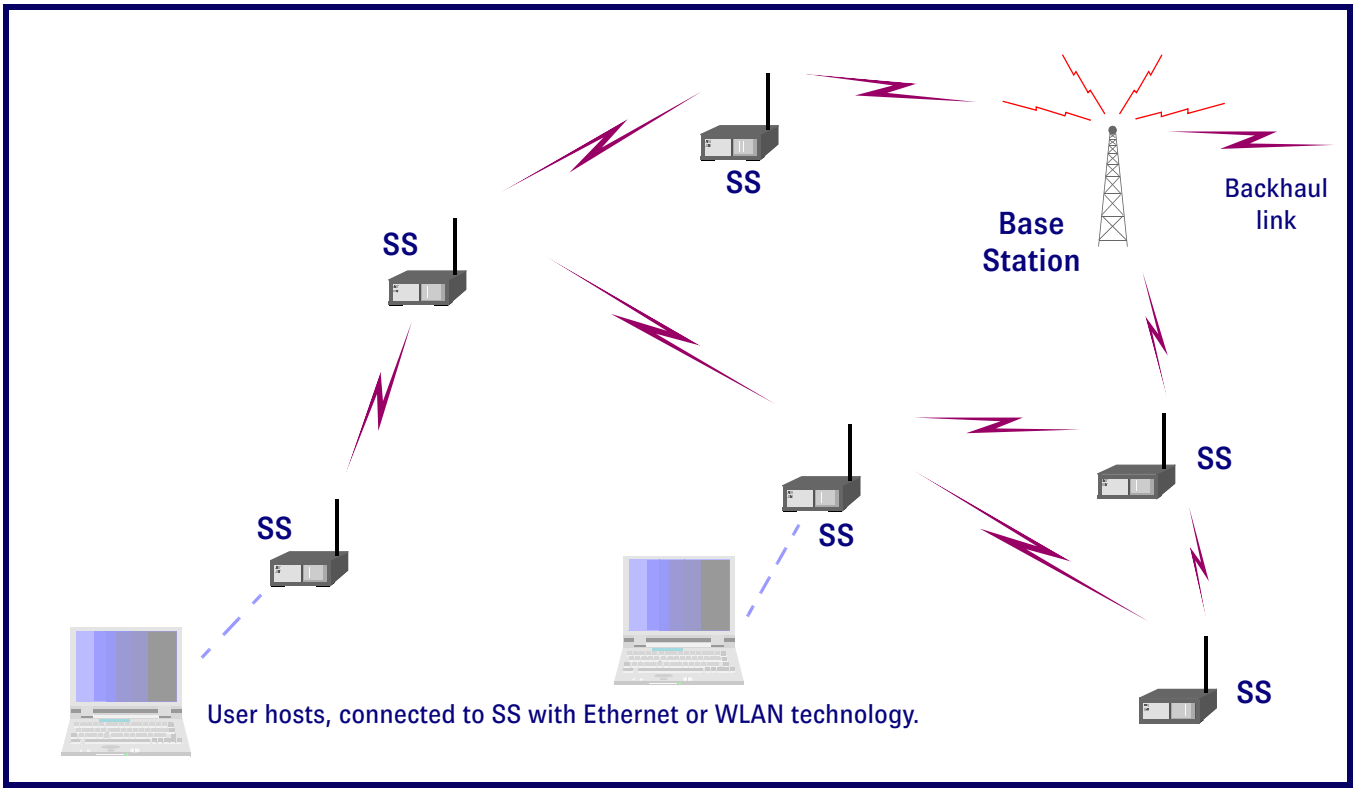


Figure 2: Example of Mesh Deployment (Subscriber Network)



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.

802.11 Planet Conference & Expo Japan 2003

1st- 2nd September 2003
Shibuya Mark City
Tokyo, Japan

www.idg.co.jp/expo/j802.11/eng/index.html

The Third International Conference on Peer-to-Peer Computing

1st- 3rd September 2003
Linkopings University
Linkoping, Sweden

www.ida.liu.se/conferences/p2p/p2p2003

8th Annual Conference and Exhibition – Information Security World Australia 2003

2nd- 4th September 2003
Melbourne Convention Center
Melbourne, Australia

www.isecworldwide.com

Network Security Conference 2003

8th- 10th September 2003
Caesars Palace
Las Vegas, NV

www.isaca.org/nsc2003.htm

802.16 Working Group Session on Broadband Wireless Access Standards

8th- 11th September 2003
Denver Marriott City Center
Denver, CO

ieee802.org/16/meetings/mtg27/agenda.html

Mobile & Wireless RoadShow

10th September 2003
The Ritz Carlton, Pentagon City
Washington, DC

www.winnetmag.com/roadshows/wireless

[Note: This event is held in numerous other locations during September.]

Wireless Opportunities Workshop (WOW) 2003 – Wireless in the New Regime

14th- 15th September 2003
Owens Banquet Hall – Virginia Tech
Blacksburg, VA

www.conted.vt.edu/wow

ACM MobiCom 2003

14th- 19th September 2003
Westin Horton Plaza Hotel
San Diego, CA

www.sigmobile.org/mobicom/2003

Gartner IT Security Summit 2003

15th- 16th September 2003
Royal Lancaster Hotel
London, UK

www.gartner.com/2_events/conferences/2003/sec1i/sec1i.jsp

SANS New England 2003

15th- 20th September 2003
Boston Park Plaza & Towers
Boston, MA

www.sans.org/newengland03

Angelbeat Regional Technology Forums on Mobility and Wireless

17th September 2003
Manchester San Diego Grand Hyatt
San Diego, CA

www.angelbeat.com

[Note: This event is held in numerous other locations during September.]

ACM Workshop on Wireless Security (WiSe 2003)

19th September 2003
Westin Horton Plaza Hotel
San Diego, CA

www.ece.cmu.edu/~adrian/wise2003

PWC 2003 – The 8th International Conference on Personal Wireless Communications

23rd- 25th September 2003
Telecom Italie Future Center
Venice, Italy

www.iit.cnr.it/pwc2003/intro.html

4th Annual Exhibition and Conference – Mobile Commerce World 2003

23rd- 24th September 2003
ExCel
London, UK

www.mobilecommerceworld.com

HealthSec Conference and Expo 2003

23rd- 25th September 2003
The Hilton Chicago & Towers
Chicago, IL

www.misti.com/06/hs03ba16inf.html

The Conference and Expo on Mobile and Wireless Security

23rd- 25th September 2003
The Hilton Chicago & Towers
Chicago, IL

www.misti.com

802.11 Planet Conference & Expo Europe 2003

29th- 30th September 2003
Forum Hotel
Munich, Germany

www.jupiterevents.com/80211/munich03/agenda.html

WiFi's Air Apparent?

Although the 802.16 standard is only 17 months old, the technology is already being groomed for mainstream success. Just as "WiFi" quickly became 802.11's moniker outside of engineering circles, 802.16 is being rebranded as "WiMAX," a name that is also similar enough to WiFi to ride on the coat-tails of its brand awareness.

But despite a catchier name and plenty of coverage in the mainstream and trade press, can WiMAX really kick-start the moribund fixed broadband wireless sector? "It depends," says an ABI Research report that publishes Oct. 3. "What lies beneath the consumer-centric names like WiFi and WiMAX are rigorous standards that promote development of common technologies, interfaces and protocols, bringing component and equipment prices down."

ABI is concerned about the potential for competition among the protocols within the WiMAX family. There is also potential competition from without: 802.16e is a mobile version of WiMAX that is going up against 802.20. Confusion and overlap could stymie the WiMAX market, which ABI says is worth $2 billion over the next five years.

Other analysts argue that testing and certification also are key to WiMAX's success. "Because IEEE does not perform interoperability or conformance testing, the WiMAX Forum must invest in a testing lab, determine product-testing prices, and eventually perform the certification and interoperability procedure," the Yankee Group wrote in a May 23 research note.

The good news is that the WiMAX Forum is in the process of establishing testing and certification guidelines, which will include a "WiMAX Certified" label. Those should be done by April 2004, the WiMAX Forum said in a press release that also highlighted its ambitions: "WiMAX will use the same approach the WiFi Alliance used to help ignite the wireless LAN industry."

Introduction to the Security Features of 802.16

The 802.16 system provides authentication, confidentiality, integrity, quality of service (QoS) and attack protection while maintaining flexibility.

Confidentiality across the fixed broadband wireless network is delivered through what is called the 'Privacy' sublayer of the MAC layer. This provides secure key exchange, and an encrypted connection between an SS and its BS. In addition, it provides operators with strong protection from theft of service (fraud) by providing SS – hence the user – identify verification. The Base Station protects against unauthorized access to data transport services by enforcing encryption of the associated service flows across the network. An authenticated client-server key management protocol controls distribution of keying material to client Subscriber Stations.

The 'Privacy' sublayer has two component protocols:

A. An encapsulation protocol for encrypting packet data across the fixed broadband wireless access network. This protocol defines:
   1. A set of supported cryptographic suites, i.e., pairings of data encryption and authentication algorithms, and;
   2. The rules for applying those algorithms to a MAC PDU payload (Medium Access Control, Protocol Data Unit payload). Encryption (confidentiality protection) is always applied to the MAC PDU. The MAC header remains in the clear.

B. A key management protocol (Privacy Key Management, or PKM) providing the secure distribution of cryptographic keying data from a Base Station to Subscriber Stations. Through this key management protocol, SS and BS synchronize keying data. A Base Station also uses PKM to provide access control to the network.

The PHY layer, targeted for operation in the 10 – 66 GHz frequency band, is designed with a high level of flexibility for optimizing cell planning, cost, radio capabilities, services, and capacity. For example, the framing mechanism in 802.16 provides adaptive burst profiling to adjust to the needs of each SS. This flexibility can also be used for enhancing security.

Confidentiality in the 802.16 standard includes several time-dependent features governing authentication and encryption. For instance, one of its QoS features is accurate uplink time slot synchronization, which is supported through a ranging calibration procedure defined by the MAC sublayer. This feature ensures non-interference of uplink transmissions by multiple users.

Time-dependent features built into WirelessMAN networks, based on a timer at the BS, trigger events that disable authentication or encryption when pre-specified conditions are not met. For example, encryption keys have a limited life and a grace period. During each key's grace period, the system must re-key or re-authorize itself, or else the key expires.

Design assumptions

The WirelessMAN standard assumes that users trust the access network provider. This relationship differs from that of 802.11 WiFi, where users often get service from any publicly available signal. For 802.16, the control point of the system resides in the BS, which is

under direct operator supervision. The Base Station has full control over all decisions made during protocol exchanges, including allocation of resources between the Subscriber Stations in the network. The only aspect it does not fully control is the internal scheduling of packets between the various connections in an SS.

In most cases, it is assumed that authorized personnel install the WirelessMAN equipment. The exception is the optional mesh mode, which supports secure self-installation. The Privacy Key Management (PKM) protocol, a protocol of the DOC-IS BPI+ specification, is designed primarily to prevent theft of service using cloned or stolen equipment or via terminals that have been hacked by malicious users. The PKM protocol also provides reasonable protection against eavesdropping on the air link.

Less emphasis has been put on preventing denial-of-service attacks, because radio systems generally can be jammed using less sophisticated means. Also, because one of the main goals of the WirelessMAN design is to maximize link capacity, there is no default mechanism for hiding usage patterns. However, with proper system configuration, operators can provide a service that hides any internal traffic structure.

The reference model in a broadband wireless access system is similar to that of a cable modem system, so the security issues are almost identical. As a result, the 802.16 working group chose the BPI+ (Baseline Privacy Plus Interface) specification developed for DOCSIS as the basis for the standard's security features.

Subscriber Station (SS) Authorization

Before it can access the network, every SS must go through an authorization procedure – as illustrated in **Figure 3** – which begins as soon as the radio parameters have been negotiated. The authorization procedure relies on X.509 certificates (IEFT RFC 2459) and RSA public key methods – Public Key Cryptography Standard #1 (PKCS #1).

During manufacturing, each SS is assigned two certificates: a self-signed manufacturer certificate and an SS certificate signed by the manufacturer. The manufacturer certificate is the same for all devices made at each manufacturing location, while the SS certificate is unique for every device. The SS certificate binds the SS's 48-bit IEEE MAC address to its public RSA key.

The authorization process begins with the SS sending two messages to the BS: the Authentication Info, which contains the manufacturer certificate, and the Authorization Request, which contains the SS certificate. The Authorization Request also lists SS security capabilities. Currently, the specification assumes the BS (operator) has acquired the contents of the manufacturer certificate via some other trusted channel. It does not have to rely on the content of the Authentication Info message, which is unreliable,

> *"Bluetooth security will become a real issue in the next year or two. There are currently more Bluetooth radios in existence than 802.11 radios, but most corporate security departments don't know the first thing about Bluetooth security."*
>
> *— Bruce Potter, a security expert with US Think Tank, The Shmoo Group*

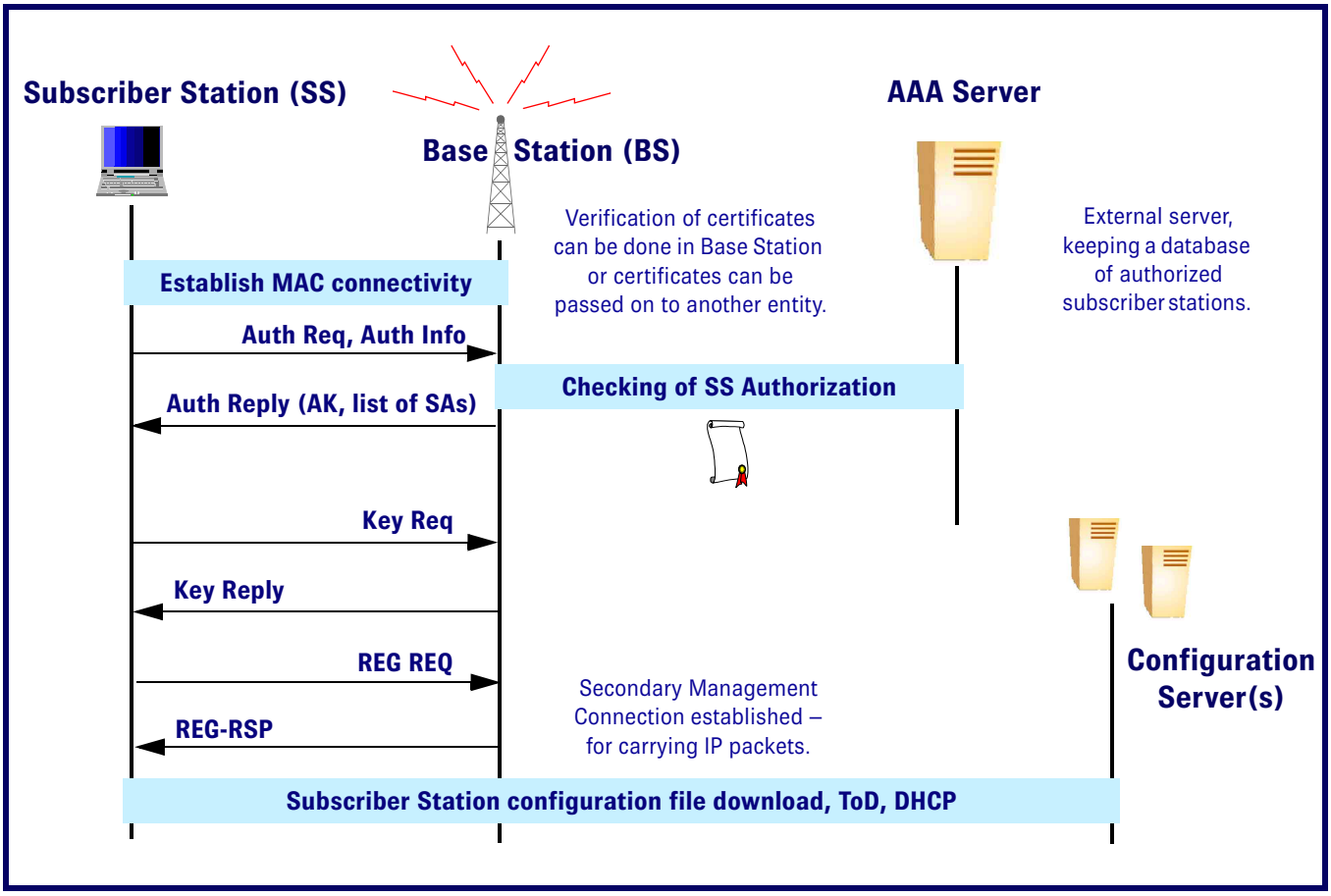
since it is self-signed. The Authentication Info is written into the standard as a way to accommodate a future situation where all interoperable manufacturers would replace their self-signed manufacturer certificates with certificates assigned by a central certification authority. This kind of model is successfully used for DOCSIS cable modems, and Cable Labs is the certifying authority in that case.

After the BS has successfully authenticated the certificate, the BS can check for the authorization of the SS from a database residing, for example, in a central AAA server using a protocol such as RADIUS or DIAMETER. If the SS is authorized, the BS provides the SS with two Authorization Keys (AK), encrypted with the public key of the SS – together with their lifetimes – in the Authorization Reply message. The message also contains the list of Security Associations and their parameters. Reception of the Authorization Reply message is implicitly acknowledged by the SS, since it begins key exchange procedures for each of its Security Associations. The initialization sequence depicted in **Figure 3,** then, leads to the key exchange depicted in **Figure 4**.

The SS is re-authorized at regular intervals, and the AKs' lifetimes overlap each another: When one pair of keys expires, the authorization procedure is invoked. However, because the SS still possesses a valid AK during the re-authorization, there is no service interruption.

For mesh systems, the procedure is slightly more complicated. The authorization messages are forwarded to the BS by a sponsoring node, which is selected by the candidate SS. The sponsoring node uses a key installed by the network operator to do an initial verification of the identity of the candidate SS.

Figure 3: 802.16 Authorization



Security Associations (SA)

The central concept in PKM is the Security Association (SA) – a set of shared information supporting secure connections between a BS and one or more Subscriber Stations. Each SA is a set of cryptographic methods and the associated keying material – including, for example, Traffic Encryption Keys (TEKs) and ciphering vectors used for MAC PDU authentication.

Every SS establishes at least a primary SA at start-up time. The BS may specify additional SAs in the Authorization Response message. Later, it can also dynamically add SAs to an SS, without performing a full re-authorization of the SS. This is done using a special message: the SA-Add message.

For encrypted downlink multi-cast, an SA can be shared between multiple Subscriber Stations. However, the maintenance of these shared SAs is done using the same point-to-point signaling that would be used for private SAs.

Traffic Encryption Key (TEK) Exchange

The SS initiates a TEK exchange for each SA specified in the Authorization Response or in response to a new SA being created via an SA-Add message. For Point-to-Multipoint systems, the default method for exchanging DES TEKs is 3DES, using a key derived from the AK.

The reason for using a stronger symmetric algorithm to exchange the TEKs is because it consumes significantly less computation resources in the SS than would a public key method.

As shown in **Figure 4**, the SS sends a Key Request to the BS to initiate TEK exchange. The BS generates two keys for the SA – with overlapping lifetimes and consecutive sequence numbers. The BS then sends these back in a Key Reply message. As with the AKs, the overlapping keys are to prevent service interruption when a key expires. In mesh deployments, where the two nodes establishing an SA do not share the same AK, the Subscriber Stations instead use the RSA public key method to exchange the TEKs.

Encryption of User Data

All user data transported in an IEEE 802.16 connection is mapped to a specific SA, which defines the method to be used to encrypt the payload of each MAC PDU. When receiving a MAC PDU on a connection, the receiving party is required to check that the correct processing has been performed on the PDU.

Each MAC PDU header contains the two least significant bits of the TEK sequence number used to encrypt the payload. This allows the receiver to determine which one of the two currently valid keys the transmitter used for encryption. To prevent discrepancies in this determination while new keys are being generated, several rules are followed:

- The BS always uses the older of its two active keys to encrypt downlink traffic.
- At the expiration of the older TEK, the BS immediately starts to use the newer key.
- The SS always uses the newer of its two keys to encrypt transmissions.
- Both the SS and BS must be able to decrypt data encrypted with either key.

These rules are illustrated in **Figure 4**.

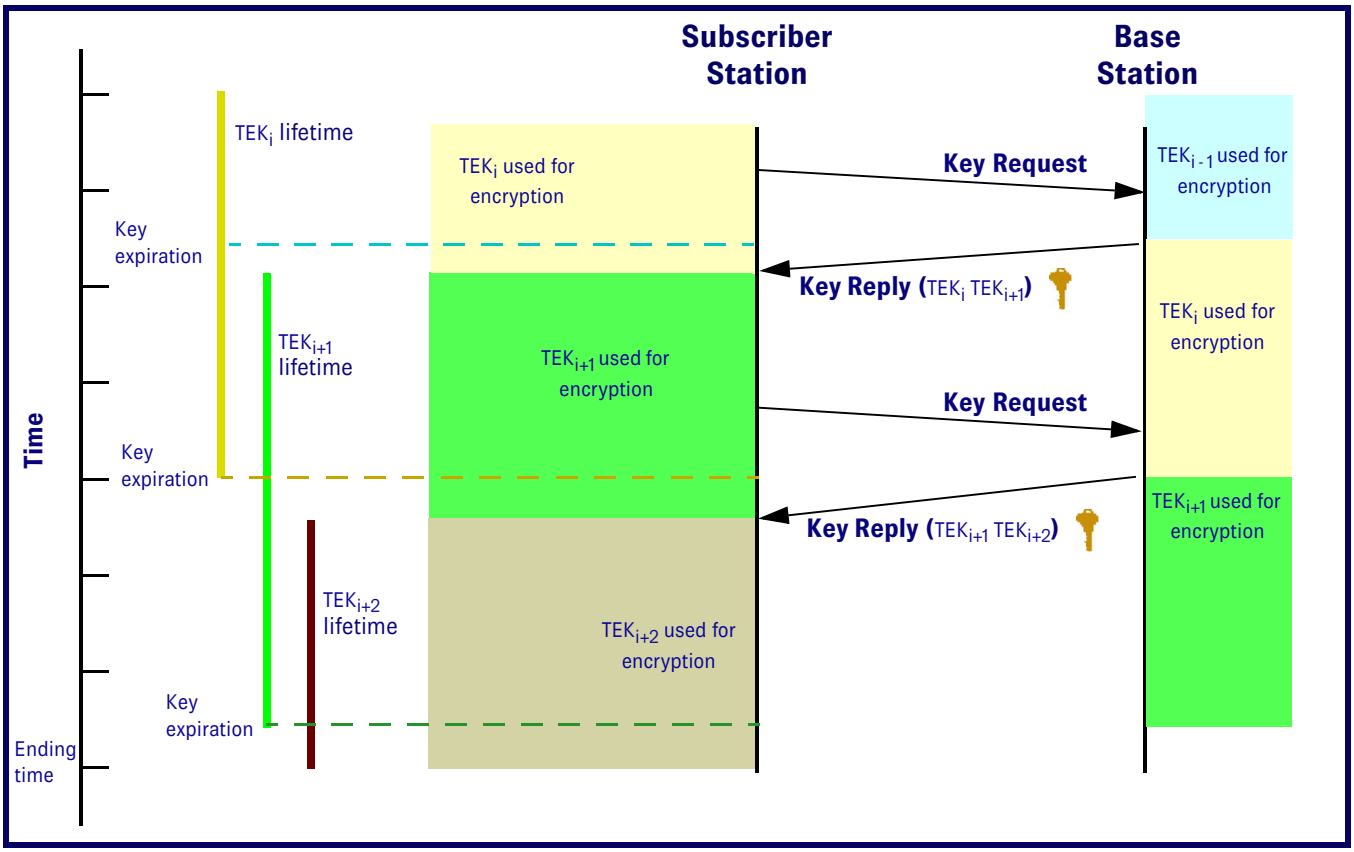
PKM Ciphering

The only currently mandatory method for user data encryption is DES in CBC mode (CBC: cipher block chaining – one of the four modes of the Data Encryption standard). However, in PKM, all the necessary hooks are in place for introducing newer and stronger algorithms.

Editor's note: The 56-bit DES block cipher algorithm has effectively been replaced by the Advanced Encryption Standard (AES) – the newer, NIST-approved block cipher with variable-length key. AES is now approved for the protection of classified data. Because the aging DES, with its relatively small keyspace, is considered weak today, in cryptanalytic terms, the 802.16 should be revised to mandate AES or perhaps triple DES. Also, it should be noted that the WiFi (802.11 wireless LAN) community has progressed substantially with its security, subsequent to the tremendous press about WEP (Wired Equivalent Privacy) flaws. Considerable work has gone into the development of "Robust Security Networks" within the IEEE 802.11 TGi (Task Group i). It would be propitious for the two standards organizations to perform security 'harmonization' – to leverage each other's strengths and security expertise. Last, although the 802.16 standard does indeed capitalize on some of the critical cryptographic primitives for securing communications – and it appears "secure" prima facie – it would be prudent for an independent, third party to perform a rigorous, top-down, security analysis – analyzing all aspects of the standard's protocols, algorithms, and techniques. Any takers?

Read more about DES and AES in our **September** and **December 2001** issues of *Wireless Security Perspectives*.

Figure 4: Traffic Encryption Key (TEK) Exchange



Getting back to encryption of user data, the initialization vector (IV) used to initialize the CBC block chaining for DES is computed as the exclusive-or (XOR) of the IV parameter (included with the keying information) and the content of the PHY synchronization field in the most recent Downlink Map message. The exact content of the PHY synchronization field depends on the actual physical layer specification, but generally, it contains a frame counter, which it increments from frame to frame. Thus, the IV is unique per frame and key, assuming the key is exchanged frequently enough. For the WirelessMAN-SC with 1 ms frames, the frame counter rolls over every 4.66 hours, so the key should be changed six times a day, which is a tolerable overhead cost. For the WirelessMAN-OFDM system, the longer frame duration allows for longer key lifetimes.

Message Integrity Protection

Protecting the integrity of certain MAC Management messages is crucial for preventing theft of service. The protection is achieved using standard HMAC-SHA1 message digests calculated over the messages. In 802.16, a message can be fragmented for transport in several MAC PDUs. Currently, PKM does not define a method for authentication of each MAC PDU. Again, the 802.16 standard is designed to support such a feature, should the need arise in the future.

Protected messages include all Dynamic Service messages used for setting up the connections and their traffic parameters over the air. These are messages related to authorization and key exchange, and protection is also used for control messages with the potential to severely disrupt the service. Real-time control messages are generally not protected, to avoid excessively long response times.

Conclusions

The PKM protocol in IEEE 802.16 defines strong mechanisms based on well-known cryptographic methods to prevent theft of service and protect against eavesdropping on the air interface. The protocol is built to be future-proof, and stronger algorithms can easily be incorporated later on, if needed.

About the Author

Carl Eklund (carl.eklund@nokia.com) is a Senior R&D Engineer at Nokia Research Center in Helsinki. He served as chair of the MAC Task Group during the development of the IEEE 802.16 standard, and subsequently as vice chair of the working group. He has an MSc in Engineering Physics from Helsinki University of Technology.

Biometrics Cellphone

The new F505i cellphone from Fujitsu is the first phone ever sold in Japan with a built-in finger-print reader. This phone, designed for NTT's PDC (Pacific Digital Cellular) 2G system (not their 3G FOMA system) uses biometrics to protect the user's data within the phone. This replaces the numeric PIN that has previously been used by many phone models.

The security problem solved by this phone is relatively limited, although it is important, as the amount and importance of data stored within phones increases. A much more challenging problem would be to use biometrics to authenticate access to the cellular network, or to services such as online banking or shopping, accessed via that network. These problems would require that the network have knowledge of the biometric data, and would require methods for secure transmission of it across the radio interface.

WiFi (in)Security in the News

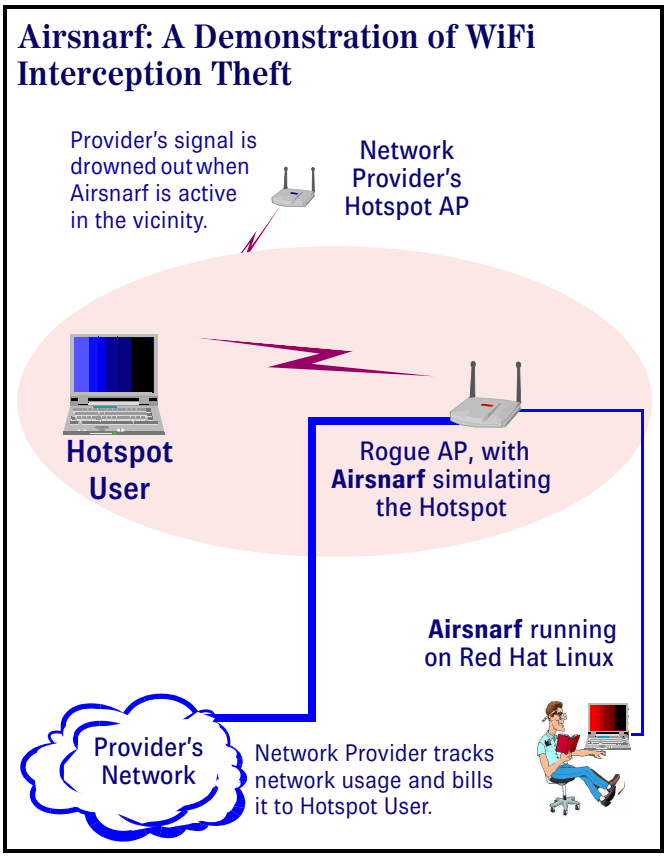
At a DefCon event in early August, 2003, a couple of wireless security practitioners demonstrated a 40-pound, mobile robot equipped with two 802.11b network interface cards: one for sniffing wireless networks and the other for reporting information to – or receiving commands from – the human acting as "master." With a wheel-base close to 24 inches (61 cm) wide and a height of less than 18 inches (45 cm), the wireless computing device is a War-driving robot that can motor along at the rate of a fast walk. Its snooping system is capable of intercepting Telnet and POP passwords transmitted within its range, and as with any sniffer, it gains network access whenever possible, making it useful as either a defensive tool (WiFi network testing and monitoring) or as an offensive device (hacking and espionage).

This news from Defcon illustrates the obvious in WiFi networks: vulnerabilities are still a problem. With the continued explosive growth of WiFi – and robust security still lagging – other specialized "hacker" gadgets will likely continue to appear. The end of newly invented ways to exploit these wireless networks is not yet in sight – a flashback to the CopyCat boxes and ESN Readers of cellular.

Rogue AP Gadget

Airsnarf, a device designed by the Shmoo group, impersonates an Access Point (AP). It exploits authentication weaknesses in most public WiFi hotspots. By overpowering the signal of its target, it sets up a fraudulent hotspot and prompts each user for the username and password for the hotspot provider's network.

Most users supply this information, unwittingly believing this is the accepted way to access the provider's hotspot. After this mock authentication,



the user gains access to the provider's network through the portal of the rogue access point, and the captured userid and password are mailed to root@localhost. This rerouted connection through the rogue AP is almost totally transparent. The user only sees the Airsnarf splash screen requesting userid and password on the first attempt to access any website. Without knowing this is the problem, the user is easily persuaded to let their guard down during their entire use of the system.

Although Airsnarf can obviously be used for malicious purposes, Shmoo has developed it for the legitimate purpose of demonstrating security weaknesses.

Fraud and Security Patent News

US Patent: 6,606,708

Secure server architecture for Web-based data management

A double firewalled system for protecting remote enterprise servers that provide communication services to telecommunication network customers from unauthorized third parties. A first router directs all connection requests to one or more secure web servers, which may utilize a load balancer to efficiently distribute the session connection load among a high number of authorized client users. On the network side of the web servers, a second router directs all connection requests to a dispatcher server, which routes application server calls to a proxy server for the application requested. A plurality of data security protocols are also employed. The protocols provide for an identification of the user, and an authentication of the user to ensure the user is who he/she claims to be and a determination of entitlements that the user may avail themselves of within the enterprise system. Session security is described, particularly as to the differences between a remote user's copper wire connection to a legacy system and a user's remote connection to the enterprise system over a "stateless" public Internet, where each session is a single transmission, rather than an interval of time between logon and logoff, as is customary in legacy systems.

Issued: August 12, 2003

Inventor: Carol Devine, *et al*
Assignee: WorldCom, Inc. (Clinton, MS)

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 webpage – a brief description, the inventor(s), and the assignee (owner). All of these patents were granted in August of 2003.

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: 6,606,706

Hierarchical multicast traffic security system in an internetwork

Multicast networks are partitioned into hierarchical security domains. Each security domain may comprise one or more lower security domains. Each security domain includes a security broker that distributes a group key and translates multicast data destined to the security domain, if necessary. A primary security broker at the second level of the hierarchical multicast system distributes the top security key to all peer members, including all peer security domain brokers to establish trust relationships. For each security domain boundary with security domain border routers, a multicast virtual link is configured that connects the security domain border routers and the security broker for the security domain to reduce the latency in forwarding multicast data. It can also make the backbone of the security domain contiguous so that multicast data can travel unchanged across the backbone. The multicast data is forwarded to the security domain through the security broker with security translation. A group key is distributed at each hierarchy level by exchange of Group Key Request and Group Key Reply messages. The re-key process is accomplished by multicasting Rekey Announcement messages, either regionally by a security broker, or globally by the group controller through the primary top regional security broker.

Issued: August 12, 2003
Inventor: Yunzhou Li
Assignee: Nortel Networks Limited (St. Laurent, CA)

Reference:

[1] Mittra, Suvo. *Iolus: A Framework for Scalable Secure Multicasting*. SIGCOMM '97 Cannes, France, pp. 277-288.

US Patent: 6,606,663

Method and apparatus for caching credentials in proxy servers for wireless user agents

A credential caching proxy server handling credential caching for a set of wireless client devices. The credential caching proxy server handles most credential transactions for wireless client devices attempting to access resources within a protected realm where the protected realm requires credentials. In one embodiment, the credential caching proxy server intercepts and caches a wireless client's credentials when a credential is first sent from the wireless user agent to a protected server. The cached credential will then be used for all requests to resources within the same protected realm. Thus, after first sending a first credential for accessing the resource in a particular realm, the wireless user agent does not need to attach the credential for all the subsequent requests for any other resources belong to the same realm. In an alternate embodiment, the proxy server sends a special request to the wireless client device requesting a credential for a particular resource. The special request may take the form of a simple preformatted display page such that a "dumb terminal" wireless client device can be used to communicate with protected Internet resources even though the "dumb" wireless client device has no concept of authentication and authorization.

Issued: August 12, 2003
Inventor: Hanqing Liao, *et al*
Assignee: Openwave Systems Inc. (Redwood City, CA)

References:

[1] Patiyoot, *et al. Techniques for Authentication Protocols and Key Distribution on Wireless ATM Networks.* Oct. 1998, ACM SIGOPS Operating Systems Review, vol. 32, Iss. 4, pp. 25-32.

[2] Geng, *et al. Defending Wireless Infrastructure Against the Challenge of DDoS Attacks.* Jan. 2002, Mobile Networks and Applications, vol. 7, Iss. 3, pp. 213-223.

[3] Molva, *et al. An authentication protocol for mobile users.* 1994, IEE, pp. 4/1-4/7.

[4] Lin, *et al. A Wireless-based Authentication and Annymous Channels for Large Scale Area.* 2001, IEEE, pp. 36-41.

US Patent: 6,606,491

Subscriber validation method in cellular communication system

A dual-mode communication system made up of an AMPS network and a GSM network provides for communication to and from dual-mode terminals equipped with corresponding SIM cards. The mobile terminals store a terminal-based ESN, and the SIM cards store a SIM-based ESN and MIN. The dual-mode system uses the terminal-based ESN and MIN for registration in the AMPS network. For authentication purposes, however, the dual-mode system uses the SIM-based ESN for key-based authentication in the AMPS network.

Issued: August 12, 2003

Inventor: Richard Peck
Assignee: Telefonaktiebolaget LM Ericsson (publ) (Stockholm, SE)

US Patent: 6,606,393

Message authentication code using image histograms

A system for generating a message authentication code for a conventional digital video stream. The system operates on the rows and columns of block data for a video stream, and more specifically on histograms of DC coefficients from each row and column, to produce a compact code that is nonetheless descriptive of the underlying images in the video stream. The message authentication code can be reproduced from the images of a received video stream, and if desired, compared with a digital watermark embedded in the video stream in order to confirm the accuracy of the video content or identify the source of the video stream.

Issued: August 12, 2003

Inventor: Liehua Xie
Assignee: Verizon Laboratories Inc. (Waltham, MA)

References:

[1] Graveman, *et al. Approximate Message Authentication Codes.* 1999 Proceedings: Third Annual Federated Laboratory Symposium on Advanced Telecommunications/Information Distribution Research Program (ATIRP), pp. 411-415.

[2] Liehua Xie, *et al. Secure MPEG Video Communication by Watermarking.* Abstract; Department of Electrical and Computer Engineering, University of Delaware, pp. 459-463.

US Patent: 6,606, 387

Secure establishment of cryptographic keys

A system and method for securely establishing a cryptographic key between a first cryptographic device, for example a host cryptographic security module, and a second cryptographic device, for example a bank Automated Teller Machine (ATM). A plurality of key components is generated from a pool of random numbers and a unique reference number indexes each of the key components. The key components are encrypted, stored and indexed in the host security module by the corresponding reference numbers. The key components are arbitrarily distributed to field personnel in tamper-evident envelopes to be entered into the ATM. Each of the tamper-evident envelopes is marked with the reference number corresponding to the key component contained in the envelope. At least two field personnel each enter a different key component into the ATM to form the cryptographic key. Each then communicates, to the host security module, the reference number corresponding to the key component and the identification number of the ATM. The host security module retrieves the encrypted key components corresponding to the reference numbers provided by the field personnel, decrypts them, and combines the two decrypted key components to recreate the cryptographic key created in the ATM. The encrypted cryptographic key may be transmitted to a third cryptographic device by means of a previously established cryptographic key.

Issued: August 12, 2003

Inventor: Dennis Abraham
Assignee: Trusted Security Solutions, Inc. (Matthews, NC)

US Patent: 6,606,386

Cryptographic key split combiner

A cryptographic key split combiner, which includes a number of key split generators for generating cryptographic key splits and a key split randomizer for randomizing the cryptographic key splits to produce a cryptographic key, and a process for forming cryptographic keys. Each of the key split generators generates key splits from seed data. The key split generators may include a random split generator for generating a random key split based on reference data. Other key split generators may include a token split generator for generating a token key split based on label data, a console split generator for generating a console key split based on maintenance data, and a biometric split generator for generating a biometric key split based on biometric data. All splits may further be based on static data, which may be updated, for example, by modifying a prime number divisor of the static data. The label data may be read from a storage medium, and may include user authorization data. The resulting cryptographic key may be, for example, a stream of symbols, at least one symbol block, or a key matrix.

Issued: August 12, 2003

Inventors: Edward Scheidt and Jay Wack
Assignee: TecSec INC (Vienna, VA)

US Patent: 6,606,385

Data encrypting/decrypting conversion methods and apparatuses and data communication system adopting the same

Encrypting/decrypting conversion method and apparatus capable of controlling dynamically cyclic shift independent of data to undergo encrypting/decrypting conversion, which includes two or more different fixed circulating shift processing means for shifting cyclically the data by a fixed bit number leftward or rightward, a cyclic shift processing selecting means for selecting fixed cyclic shift processing means. The selecting sequence determined by the cyclic shift processing means is determined on the basis of data for determining the shift number selecting sequence.

Issued: August 12, 2003

Inventor: Makoto Aikawa
Assignee: Hitachi, Ltd. (Tokyo, JP)

References:

[1] *The RC5 Encryption Algorithm*, MIT Laboratory for Computer Science, Ronald Rivest, pp. 86-96.

[2] *Improved Differential Attacks on RC5*, Lars R. Knudsen, pp. 216-228.

US Patent: 6,603,857

Method and apparatus for controlling release of time-sensitive information

A method and apparatus for controlling release of time-sensitive information is accomplished by a server that establishes access information for a specific future time, which only becomes active once the specific future time has passed. When the specific future time has passed, the server releases the access information such that an end-user or end-users may utilize the access information to obtain time-sensitive information. The access information may be a random number which can be used to calculate a decryption key and an encryption key. The encryption key can be released by the server at any time such that an end-user may encrypt time sensitive information for release at the specific future time, but the random number is not released until the specific future time has passed. When the random number is released, end-users may generate the decryption key and subsequently decrypt the time-sensitive information.

Issued: August 5, 2003

Inventors: Mark Batten-Carew and Michael Wiener
Assignee: Entrust Technologies Limited (Ottawa, CA)

US Patent: 6,603,761

Using internet and internet protocols to bypass PSTN, GSM map, and ANSI-41 networks for wireless telephone call delivery

A method and system to provide GSM subscribers roaming into CDMA or TDMA networks, and CDMA or TDMA subscribers roaming into GSM networks, with basic call delivery wireless services, as long as the roamers can pay the bill with their valid credit card, and to do so independently of and as a bypass of GSM Memorandum of Understandings for cellular/PCS services. This is achieved by integrating the proper pieces of wireless and wireline networks and secure communications, using IP networks and protocols as an alternative to the existing telephony-based approach.

Issued: August 5, 2003

Inventors: Jin Wang and Patuardhana Gorrepati
Assignee: Lucent Technologies Inc. (Murray Hill, NJ)

References:

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

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

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

Further Patent Information

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

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

800-786-9199 or 703-308-4357

Comments

We welcome comments on the format or contents of *Wireless Security Perspectives*. We can be reached via email at:

cnpsales@cnp-wireless.com