Wireless Security Perspectives

Cellular Networking Perspectives

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

Crypto in the News

FIPS198 Published

Keyed-Hash Message Authentication Code (HMAC)

On April 8, the National Institute of Standards and Technologies released an updated version of FIPS 198. This Federal Information Processing Standards Publication (FIPS PUB) describes a keyed-hash message authentication code (HMAC), a mechanism for message authentication using cryptographic hash functions.

The primary purpose of the HMAC is to authenticate the source and the integrity of a message. It may also be used as the cryptographic algorithm in "challenge-response" systems such as that used in North American ANSI-41 cellular systems. The HMAC can be used in combination with any iterated cryptographic hash function such as MD5 and SHA-1. The HMAC has two functionally distinct parameters: An input message and a cryptographic key. The cryptographic key is one that is shared between the sender and the recipient of a message.

As illustrated in **Figure 1**, the HMAC is typically used as follows for two communicants: The sender and recipient:

1. The sender computes a value by applying a cryptographic key and the input message to the HMAC algorithm. The resulting value is called the MAC (message authentication code).
2. The sender transmits the MAC and the original input message to the recipient.
3. The recipient computes a value by applying the received message and a cryptographic key (one shared with the sender) to the HMAC algorithm.
4. The recipient compares the received MAC with the MAC computed on the received message. If the two MACs are equal, the recipient can be confident that the message has not been modified in transit and that the message came from the sender with whom the recipient shares a key.

The primary objectives of the HMAC are the following:

- To use available cryptographic hash functions without modifications. In particular, hash functions that perform well in software (and for which code is freely and widely available);
- To use without significant degradation in hash function performance;
- To manipulate cryptographic keys in a simple way;
- To have a well-understood crypto-graphic strength of the authentication mechanism; and
- To allow the hash function to be replaced easily – specifically, if a faster or more secure hash function is required for the underlying hash function.

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…

May 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.

FIPS198 is based on the IETF RFC 2104 (Request for Comment)

www.ietf.org/rfc/rfc2104.txt?number=2104

For a copy of the FIPS198, click on:

csrc.nist.gov/publications/fips/fips198/fips-198a.pdf

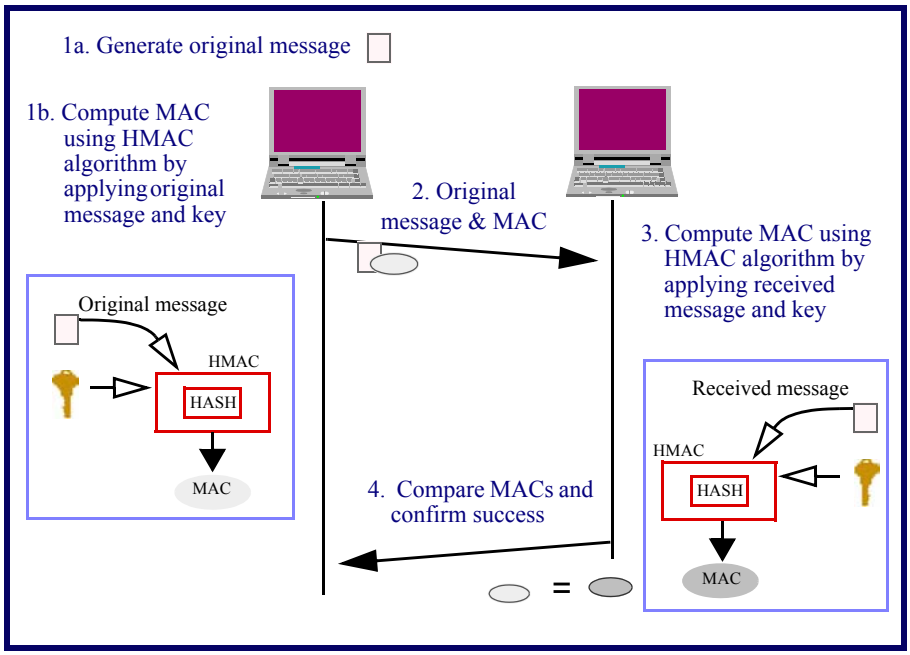
If you have any questions or need more information regarding this or any FIPS, contact Liz Lennon at:

Elizabeth.Lennon@nist.gov

or call 301-975-2832.

For information on applications for or how to embed the HMAC, contact the editors of WSP.

Figure 1: Typical Use of HMAC to Verify Message Integrity and Source Authentication



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.

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

Internet Untethered
6th May, 2002
Ritz Carlton Tyson's Corner
McLean, VA
www.angelbeat.com/DC56.shtml

Wireless Internet 2002 – Data and Enterprise Applications
6th- 7th May 2002
Sunset Village, UCLA
Los Angeles, CA
www.wireless.ucla.edu/2002

Telecoms Contingency Planning to Enable Business Continuity 2002
13th- 16th May, 2002
The Mayfair Conference Center
London
www.iir-conferences.com

CTIA Wireless Agenda 2001
14th- 18th May, 2002
The Adams Mark Hotel
Dallas, TX
www.wow-com.com/events

Information Security Conference 2002
15th- 16th May, 2002
New York, NY
www.nymissa.org

SANS Washington DC
6th- 12th May, 2002
Omni Shoreham Hotel
Washington, DC
www.sans.org/CapitolHill

Information Security: Combating Enterprise Espionage and Protecting Corporate Assets
15th- 17th May, 2002
Sheraton Chicago Hotel & Towers
Chicago, IL
www3.gartner.com

3G 2002 – 6th Annual Conference (Third Generation Mobile Systems)
20th- 23rd May, 2002
Amsterdam Hilton
Amsterdam
www.iir-3g.com

CTIA Critical Issues Forum
22nd- 23rd May 2002
Washington, DC
www.wow-com.com

Anti-Money Laundering 2002 (Combating and Overcoming the Increased Complexity of Money Laundering)
30th- 31st May, 2002
Marriott East Side
New York, NY
www.marcusevansconferences.com

eSecurity Conference & Expo
29th- 30th May, 2002
Sheraton Premiere at Tyson's Corner
Vienna, VA
www.intmediaevents.com/esec/spring02/index.html

802.11 Planet Conference & Expo – Spring 2002
10th- 12th June, 2002
Pennsylvania Convention Center
Philadelphia, PA
www.80211-planet.com

Fraud 2002
24th- 25th June, 2002
Marble Arch Marriott
London
www.iir-conferences.com

Wireless Security in a Mobile World

by Ann McCown

Wireless LAN (WLAN) technology based on the 802.11 family of standards has emerged as one of the few areas of growth in the infrastructure market. Wireless LANs are beginning to be perceived as an inexpensive substitute for wired LANs in organizations valuing the convenience and ease of deployment of wireless technology. Enterprises, organizations in vertical markets, and educational institutions are all adopting 802.11 technology.

Despite the growing popularity of wireless LANs, however, significant problems remain. These include:

- Security holes
- Missing management capabilities
- Lack of support for mobility or applications

These problems represent a major obstacle to the widespread deployment of 802.11-based WLANs. Because no organization can afford to have its communications tampered with and mismanaged and its resources violated, all organizations deploying 802.11 technology need solutions to these problems.

Security in WLANs

It is useful to think about network security as protecting two valuable resources:

- The network itself; and
- the traffic that is traveling through the network.

Protecting the network prevents potentially hostile traffic getting into the enterprise's network. Protecting traffic provides users with the assurance that they will not face a hostile network environment where their data can be delayed, deleted or modified.

Protecting the Network

Enterprise networks must be protected from both destruction and theft of valuable data. Typically, this has been handled through host access control systems, but this is not necessarily adequate, particularly with WLANs. For this reason, network managers must evaluate and implement protection schemes that are integrated into the network itself.

Potential network users fall into two camps - the untrusted (and unwelcome) user, and the trusted (and welcome) user. Both must be dealt with, albeit with different techniques and concerns.

Untrusted Users

One of the main goals of network security is to keep untrusted (i.e. unauthorized) users out. In the wired network world, strong physical security techniques are often sufficient. However, in a wireless network, physical security does not work – because radio waves can go through walls, leaking the edge of the network beyond locked doors. In addition, access points may be installed throughout the network, inside the firewall, often without the knowledge of the network manager. This gives untrusted users many more points at which to attack. Authorization enforcement is needed to verify that only allowed users are putting traffic onto the network.

Trusted Users

A more subtle security concern is the use of the network by trusted users. The continuing threat of viruses and worms has taught us that just keeping the bad guys off the network is not enough. However, restricting the user's ability to see certain subnets or components, based on location, is not effective in the wireless world, since it is much more difficult to control the physical access points, as was possible when access meant plugging into a jack in the wall. User-aware access controls – based on individual user and device identity, and factors such as location or time of day – are needed to ensure authorized users see a controlled view of the network with respect to what resources they can access.

Network security systems supporting WLANs should be designed to allow the network manager to enforce user-based authentication policies that are effective even with a highly distributed access edge. Centralized control logic is needed to allow simple growth of the network without complicated configuration of every component at the edge. This necessitates interfaces with existing authentication services, including RADIUS, LDAP, Kerberos, NT Domain, and 801.1x. If a site chooses RADIUS as the authentication mechanism, for example, a one-time configuration at a central server should be all that is required, and with this, the mechanism is enforced automatically whenever a new access point is turned on. Users should experience access control through an interface they are comfortable with, such as a Web-based login, or seamless integration with existing login services.

In addition, firewall semantics should be based on the specific user, not merely the traffic type. This allows 802.11 access to be controlled by the business policies that are relevant to each user, a characteristic that was never in the design goals of the typical firewall.

The network manager requires absolute control of the user's view of the network and *all* its resources at all times. Rights management software should allow different rights to be assigned to different groups of users, including guests and contractors. When installed in the forwarding path between access points and network backbones, it should enforce rules, which will ALLOW, DENY or REDIRECT each packet. Enforcement of rights and policies must be based on parameters such as user ID, time-of-day, session length and access location. It should not matter where, when, or how the user accessed the network. Components or whole sections of the network may need to be hidden from view, based on the identity of user or the time of day.

Protecting Traffic

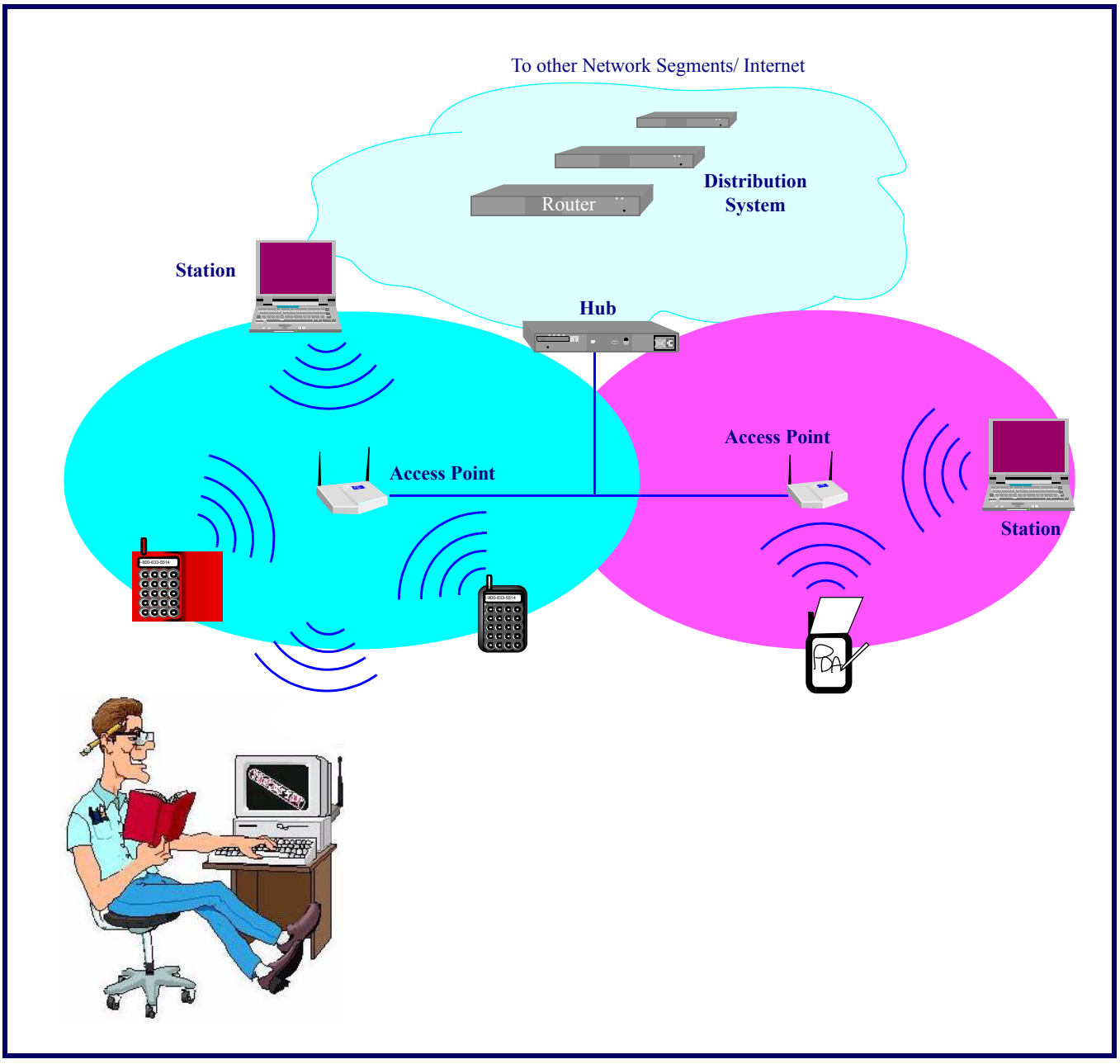
It is important to protect traffic as it travels through potentially hostile network domains. In a wired network, this is generally accomplished through "tunneling" – encapsulating the actual application session within an encrypted connection between the client device and some termination point within the home network. The highest level of this type of connection are VPNs, which provide true end-to-end secure connections across whatever path the user may happen to use. In wireless networks, traffic flows

through the air, through walls, beyond traditional IT boundaries and into public spaces such as lobbies and parking lots. Such networks are only as secure as their transmissions through the airwaves. **Figure 2** depicts a possible predicament.

One solution to this security threat is to encrypt 802.11 traffic. The 802.11b standard specified an encryption protocol, WEP (Wired Equivalent Privacy), for encrypting traffic between 802.11b devices and the network. Unfortunately, WEP has proven to be easily hacked; its design is now regarded as inherently insecure. 802.11b vendors and customers are looking to other standards – such as 801.1X, or proprietary technology – for a solution to secure the airwaves.

The Vernier solution: A preferred solution to this problem is to create encrypted tunnels for data traffic between WLAN network access managers and devices using industry standard security mechanisms such as PPTP, IPsec and L2TP/Ipsec. This offers a flexible, scalable solution that fits well within an enterprise's existing VPN strategy, and it allows a network manager to support end-users with the minimum amount of client re-configuration. In addition, this approach ensures that new wireless users will not impose an unexpectedly large increase in capacity demand on the existing VPN concentrator, which, in turn, provides an incrementally deployed solution scaled appropriately by access point deployment.

Figure 2: 802.11 WLAN Hacking



Management

Because the network has become a core asset for many enterprises, the network manager must balance the needs of many users and applications, committing to and delivering sufficient capacity and service for all the expected demands. Furthermore, network outages or service reductions often represent enormous financial losses. It is no longer sufficient for the network manager to guess where a particular problem is occurring, or who is causing it. The network manager must have the overall capacity necessary, along with the tools to control the allocation of this capacity. Appropriate levels of reporting and accounting are necessary to react quickly to changing demands and to accurately predict the demands of the future.

Capacity Management

In the wired world, the simple answer to capacity demands has usually been over-provisioning. This has been practical to implement because technology providers have regularly delivered huge capacity increases in all parts of the infrastructure. The wireless world, unfortunately, represents a giant step backward for network capacity. 802.11b products represent at best a 6 Mbps shared media world (the actual aggregate bandwidth of a typical 802.11b access point). We expect that the bandwidth limitations of radio technology will be with us for a long time. This is driving a demand for the network manager to bring fine-grained control to the traffic entering through the wireless edge.

WLAN security systems should support network policies to ration shared network resources, such as access to servers and network bandwidth. Traffic management capabilities should control access by each packet, based on user, time, application and location, with the possibility of denial based on capacity shortages and on the packet's calculated priority. Critical users and applications will receive the most reliable service, because network managers can manage traffic to meet their needs. A system should: Limit the number of users that can log on through a particular access point; limit the bandwidth available to individual users or particular types of traffic, set queuing priorities for network traffic; and control which users can access a specific application or server.

Logging and accounting information should be maintained to enable the network manager to monitor the actual use of the network by user, time, or location. Because all traffic on the network is authenticated and associated to a user, the logging capabilities increase the chance that the network manager can immediately identify the source of a problem, saving hours, days or even weeks of extensive manual debugging.

Client Device Management

Finally, management of the network must also include the management of the client devices using the network. Historically, the model for managing client-network configuration has been client focused. However, because client configuration is very labor intensive and inherently error prone, this is not a scalable or manageable model for the long term. As the wireless world migrates from primarily Windows laptops to a world of many different devices, operating systems, network interfaces, and applications, the model must revert to one of an intelligent network supporting true plug and play for IP clients.

Client configuration systems should automatically detect the configuration of each device and determine the best way to connect the device to the network. Reconfiguration should be performed automatically so that users always experience prompt, hassle-free access to the network, regardless of the network settings of their devices. Clients having TCP/IP protocol stacks – including PCs, laptops, PDAs, pocket PCs, printers and scanners – should not require additional client-side software.

Mobility

Today, garden-variety handheld computing and communication devices contain more raw processing power than mainframes of the not too distant past. They are increasingly expected to participate in high bandwidth data communications, as users assume that the long-held vision of "always connected" is finally coming true. To fully meet these expectations, the IP networks of tomorrow must include two basic enhancements:

- Persistent connections while roaming, and
- location-aware services.

Persistent Connections

Persistent connections are a challenge to the original designs of the IP network. TCP assumes stable network addresses at the end points, to maintain a connection. As IP clients roam around the WLAN, the client IP address must change to reflect the new edge location, thus breaking existing TCP sessions and eliminating the ability to deliver a persistent connection.

To provide full Layer 3 support for roaming, it is necessary to track user identities and locations through a centralized control server. With this, the system can detect the movement of users between coverage zones. Upon verifying that the user has access rights for the new coverage zone, the system can perform an automatic "hand-off" across access points (managed by a single Access Manager) or across Access Managers managing multiple access points. Although it is theoretically possible to route all traffic directly to the new access point, this is not compatible with all existing software. To be most compatible, the system should automatically tunnel active TCP sessions, so that activities begun in the first coverage zone can continue in the second. New TCP sessions should be initiated within the new coverage zone, and should not require tunneling through the old access point or coverage zone. At any time, a user should be able to run a combination of tunneled and non-tunneled sessions. With this approach, users (and the applications they are running) experience uninterrupted service, and cannot distinguish tunneled sessions from non-tunneled ones.

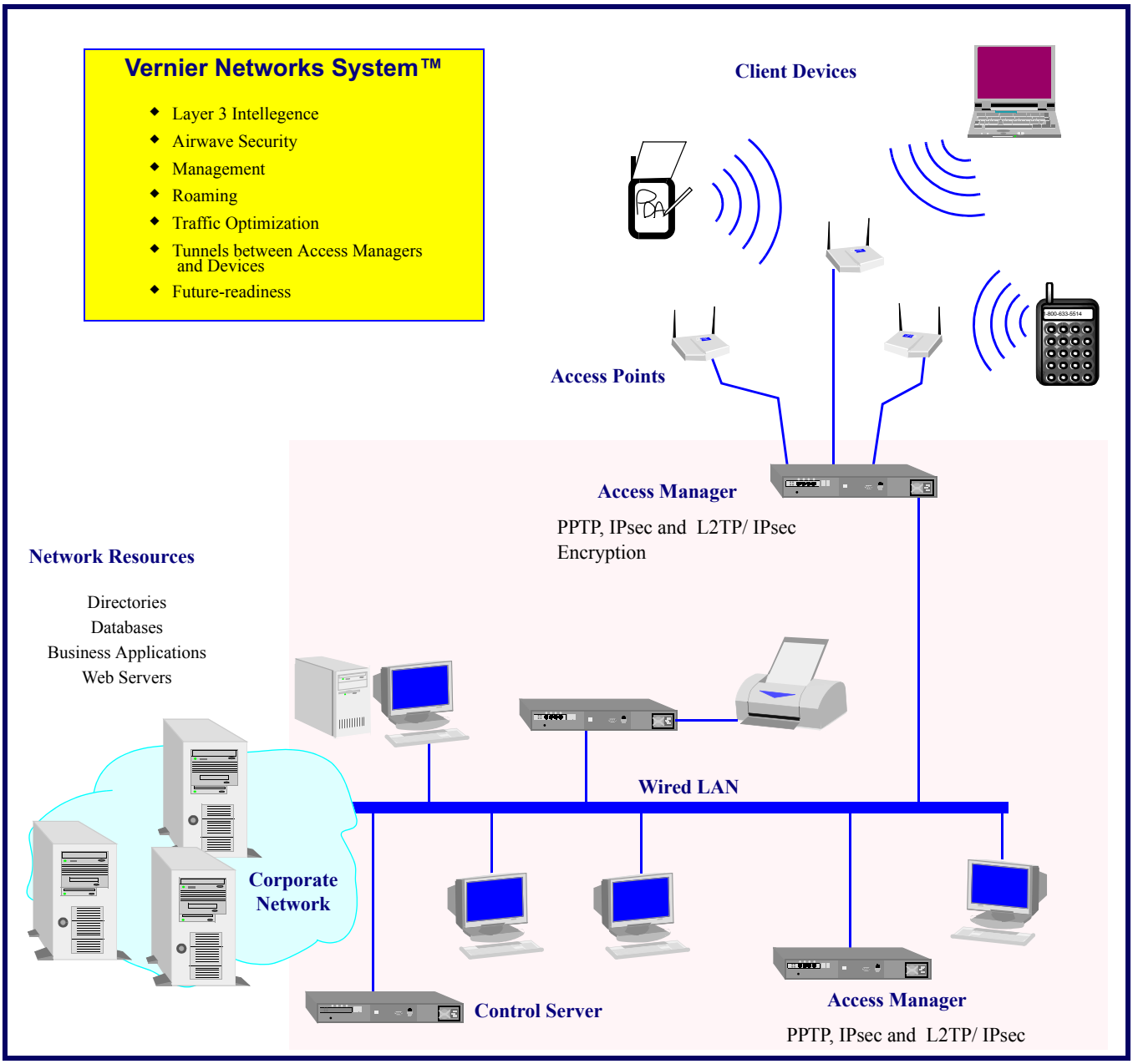
Location-Aware Services

As users come to expect IP connectivity everywhere and anywhere, they will demand new capabilities from their applications. A significant new opportunity will be the addition of location sensitive services. This type of capability is the subject of many discussions, but before it

can become a reality, the network must be supplemented with the basic infrastructure to provide a logical platform upon which to build.

Most network services today still assume that users are stationary and that devices have fixed positions, determined by their wiring. In contrast, WLAN solutions must be designed with mobility in mind. Such solutions provide user- and location-specific data, and controls needed to provide users with location-aware services, such as access to the printer closest to their current location, or special access rights at specific locations.

Figure 3: Basic Topology of Vernier Networks Solution



The Vernier System

Vernier Networks believes it is possible to take the best practices of the security world and to map them into the new demands placed on security by a widely-distributed "external access edge" along with numerous mobile users. The Vernier Networks system (illustrated in **Figure 3**) combines intelligent packet inspection with the ability to interface with site-specific authentication, applications, and business rules. Their system enables fine-grained network access control, network traffic control, and robust, persistent and consistent mobility support for a broad variety of wireless clients.

The Vernier System consists of two primary components: One or more *Access Managers* installed at the access

edge of the network; and a *Control Server,* installed anywhere within logical reach of the Access Managers. Used together, these components allow the network manager to:

- Block any network access until the user has been authenticated
- Control exactly what traffic is allowed on the network and what network resources can be seen by the individual user
- Offer network access to any IP-capable client, with no required changes in the client configuration requiring no additional software for any client
- Support mobility requirements, such as roaming (persistent TCP connections) and location aware services.

The Access Manager is a device that is typically installed in a wiring closet just behind the 802.11b access points. It supports up to 4 access points, and it provides the intelligent packet inspection engine necessary to enforce a set of traffic rules defined by the network manager. These rules can include denial, re-direction, or pass through. In addition, the Access Managers, working through the coordination of the Control Server, support tunneling of TCP sessions to offer true Layer 3 roaming.

The Control Server provides management and configuration control for the site Access Managers, giving the network manager simple and centralized control of the distributed edge devices. It also provides the coordination service necessary for session handoff when a user roams from one Access Manager to another. Central to its role in the overall system, the Control Server includes a sophisticated set of rights management tools and authentication interfaces.

The Vernier Networks rights management system gives the network manager an intuitive GUI to control a fine-grained set of access rules for network traffic. These rules are then mapped against individual users or groups, time of day, or a specific location at the access edge. It is this ability to implement arbitrary business policy to network usage, with complete precision for each user, time, and location – independent of the physical or logical topology of the network – which makes the Vernier System unique in the network infrastructure market.

About Vernier Networks

Founded in March 2001, Vernier Networks develops innovative systems and software to protect, manage, and enhance wireless networks. Vernier's user-aware, intelligent networking technology allows network managers to centralize wireless LAN usage policies, secure wireless network access at the edge, and deploy scalable wireless mobility across the enterprise. The Vernier Networks System won the Best of Show award at Net-World+Interop Atlanta in October 2001, and the COMNET New Product Achievement Award for Wireless/Mobile in January 2002. A privately held company, Vernier has received funding from Packet Design, a technology development company founded by Judy Estrin and Bill Carrico; Foundation Capital, Doll Capital Management, Masthead Venture Partners, and Weber Capital Management.

For more information, visit the Vernier Networks web site at

www.verniernetworks.com

CONTACT:

Vernier Networks
Arlene Dickson, (650) 237-2216

arlene@verniernetworks.com

or

Gallagher Public Relations
Tynesha Correa,
(510) 749-6800 ext. 234

tcorrea@gpr.com

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 – linked to the corresponding USPTO webpage, a brief description, the inventor(s), and the assignee (owner). All of these patents were granted in April 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. Patents often include other references, and these are sometimes useful to broaden one's perspective of wireless communications and security.

US Patent: 6,374,355

Method for securing over-the-air communication in a wireless system

In the method for securing over-the-air communication in a wireless system, a mobile sends a system access request and dummy data associated with the system access request to a network. The network sends a first data stream including a first data portion to the mobile in response to the system access request and the dummy data. The mobile extracts the first data portion from the first bit stream, and it sends a second bit stream to the network. The second bit stream includes a second data portion. The mobile and the network both generate a key based on the first data portion and the second data portion, establishing a first encrypted and authenticated communication channel in cooperation using the key. The mobile then transfers authorizing information to the network over the first encrypted and authenticated communication channel. If accepted, a second encrypted and authenticated communication channel is established. The network then sends sensitive information such as the root or A-key to the mobile over the second encrypted and authenticated communication channel.

Issued: April 16, 2002

Inventor: Sarvar Patel

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

US Patent: 6,374,278

Method and apparatus for the generation of statistically random numbers

A digital platform comprises a peripheral and a processing unit. The peripheral produces noise source data that is used by the processing unit to produce a statistically random data stream. In particular, a run-length coding scheme is performed on digitally sampled noise source data to produce a of runs, each run having a count and a pattern value. Then, an intermediary data stream based on the count of each run of the plurality of runs is formed. An anti-biasing scheme is performed on the intermediary data stream to remove bias and to produce a statistically random data stream.

Issued: April 16, 2002

Inventors: Rodney Korn and Vu Nguyen

Assignee: Intel Corporation (Santa Clara, CA)

US Patent: 6,374,122

Method and apparatus for supporting expanded electronic serial number (EESN) format

A 32-bit digital "amended electronic serial number" (AESN) is generated from a 56-bit "extended electronic serial number" (EESN). The AESN distinguishes each subscriber unit within a wireless system from each other subscriber unit. Two distinct methods are disclosed. In the first method, a manufacturers code field ("MFR") is tested to determine whether the subscriber unit has been assigned an EESN. If so, then the least significant 8 bits of the manufacturer's code field ("EMFR") are appended to the "serial number" field ("SN"). In the second method, each manufacturer generates serial numbers by applying a pseudo-random sequence. The "seed" for the pseudo-random sequence is based on the manufacturer's EMFR. This serial number is then combined with the 8-bit MFR.

Issued: April 16, 2002

Inventor: Nikolai Leung

Assignee: QUALCOMM Inc. (San Diego, CA)

US Patent: 6,373,948

Cryptographic method and apparatus for restricting access to transmitted programming content using program identifiers

A system for restricting access by transmitting a program identifier with the encrypted programming content. A set-top terminal, or similar mechanism, restricts access to the transmitted multi-media information using stored decryption keys. The set-top terminal preferably receives entitlement information periodically from the head-end, corresponding to one or more packages of programs that the customer is entitled to for a given period. Each program is preferably encrypted by the head-end server prior to transmission, using a program key, (K), which may be unique to the program. The set-top terminal uses the received program identifier, (p), together with the stored entitlement information, to derive the decryption key necessary to decrypt the program. Each of the k-bit program keys, (K).sub.(p), used to encrypt transmitted programs, is a linear combination of a defined set of k-bit master keys. The head-end server preferably generates a new set of master keys for the matrix, (M), once per billing period. Since each program key is a linear combination of the set of master keys, (M), a customer desiring (r) programs, obtains access to the smallest linear subspace of programs, (U), that contains those (r) programs. In addition, a package consists of program identifiers for some (i) less than or equal to (n), which need not all be assigned to programs. An optional check matrix, (C), allows the set-top terminal to determine, in advance, whether a received program is in the entitled subspace, (U).

Issued: April 16, 2002

Inventor: Avishai Wool

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

US Patent: 6,373,946

Communications Security

A satellite mobile telecommunications system includes mobile terminals 2a and 2b, which can communicate with one another using end-to-end encryption and decryption techniques. When secure end-to-end communication is required, each terminal uses a common encryption code (RAND) to encode data and decode data transmitted between the terminals. The encryption code is transmitted in a secure manner from a remote database station to the terminals. Each terminal stores a terminal key on its SIM card and the keys are also held in the remote station. Partial keys comprising the pseudo random number (RAND) and the keys stored at the station are produced at the station by an exclusive OR process, in order to mask the keys and the random number. The partial key is sent to terminal 2a. At the terminal 2a, the partial key is exclusive OR-ed with the locally stored terminal key on the SIM card, so as to recover (RAND). The common code (RAND) is determined by the same process at terminal 2b, from K.sub.pb = K.sub.b +(RAND) and the locally stored key K.sub.b. The terminals then both run a GSM encryption algorithm (A5) to encrypt and decrypt transmitted data, on the basis of the common code (RAND).

Issued: April 16, 2002

Inventor: Thomas Johnston

Assignee: ICO Services Ltd. (London, GB)

US Patent: 6,370,402

Portable radio terminal

A portable radio terminal comprising: 1) An off-memory in which a power-off time is stored; 2) an on-memory in which a power-on time is stored; 3) a difference memory in which a difference between the power-off time and the power-on is stored; 4) a user data registration memory; 5) and a portable terminal control unit 3, wherein, when a value stored in the difference memory reaches a predetermined time, the portable terminal control unit 3 waits for a password to be entered, and in response to the password entered, it erases contents of the user data registration memory.

Issued: April 9, 2002

Inventor: Tomoko Hakomori

Assignee: NEC Corporation (Tokyo, JP)

US Patent: 6,370,400

Method for avoiding fraudulent use of a mobile radiotelephone by blocking an interface after a certain inactive period of time and mobile radiotelephone performing the same

A telephone including circuits that enable a user of the telephone to receive incoming calls and to set up outgoing calls. A controller puts the telephone interface in a blocking state to prevent normal use of the telephone when the interface receives a block signal, and it puts the interface in a service state to make the telephone accessible with use of an unblocking code. The telephone has a timing circuit that supplies the block signal to the controller after a given period of inactivity of the telephone. An erroneous unblocking code, used a predetermined number of times, puts the telephone in a state of total block, which includes a power shutdown of the telephone. After turning ON the telephone, the total block state remains effective.

Issued: April 9, 2002

Inventors: Philippe Decotignie and Sabine Giorgi

Assignee: U.S. Philips Corporation (New York, NY)

US Patent: 6,370,380

Method for secure handover

In a mobile, wireless telecommunications network, communications relating to a mobile terminal can be protected during a handover of the mobile terminal from a first access point to a second access point. This may be accomplished by transmitting a security token from the first access point to the mobile terminal, and then from the mobile terminal to the second access point, over the radio interface. Thereafter, the security token is transmitted from the first access point to the second access point through the fixed network to which both the first and the second access points are connected. The communications link between the mobile terminal and the second access point needed to achieve secure handover is then established only if the second access point determines that the security token received from the mobile terminal matches the security token received from the first access point.

Issued: April 9, 2002

Inventor: Arne Norefors et. al.

Assignee: Telefonaktiebolaget LM Ericsson (publ) (Stockholm, SE)

US Patent: 6,370,374

Personal chip card for a mobile radio terminal

A mobile radio telephone terminal for communication (voice and data transmission) via a mobile radio telephone network, in which at least one access number to a telecommunication network service (e.g., calling card service) and a corresponding personal identification number are stored in a personal chip card. The mobile radio telephone terminal provides and transmits the access number and the personal identification number after an already-effected authentication to the mobile radio telephone network for communication establishment.

Issued: April 9, 2002

Inventor: Siegfried Eichinger et. al.

Assignee: Orga Kartensysteme GmbH (Paderborn, DE)

US Patent: 6,370,373

System and method for detecting cloning fraud in cellular/PCS cmmunications

A system and method for proactive detection of cloning fraud in a cellular mobile telephone environment. Information is collected, which corresponds to registration notifications of the cellular telephones as they operate within the cellular mobile telephone environment. The registration information is used to detect time-space peculiarities. Specifically, the system identifies registrations having the same mobile identification number and occurring in different mobile switching centers within a predetermined time interval. This time interval – based on a reasonable travel time between the cells covered by the different mobile switching centers from which the registrations originated – is used as a threshold for detection of cloning fraud.

Issued: April 9, 2002

Inventor: Donald Gerth et. al.

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

US Patent: 6,370,233

Security system with call management functionality

A security system with call management functionality is coupled to a telephone network for providing a telephone service and at least one telephone line. This system also includes a call management controller for enabling, disabling or changing telephone service, based on user presence and identity. User presence and identity is determined by a security controller coupled to a plurality of sensors for providing at least one home security function.

Issued: April 9, 2002

Inventors: Raymond Bennett and John Beardsley

Assignee: Ameritech Corporation (Hoffman Estates, IL)

US Patent: 6,369,719

Apparatus and method for collecting and transmitting utility meter data and other information via a wireless network

A system for remotely monitoring and transmitting data and other information received from utility and other devices. The universal meter reader of the present invention includes a device for sensing and collecting data at a first location. The sensed data, which is in analog form, is converted to a digital signal, and a processing unit processes the data. The data is subsequently stored in a memory device for subsequent transmission to an interested party. In one embodiment, the data can be digitally transmitted over a GSM or TDMA technology digital network via a control channel. In addition, the universal meter reader includes a connective interface for connecting to a telecommunications system at a first location to establish a wireless telecommunications connection. An improved infrared reader of the present invention includes an infrared transmitter and receiver. A reflective member is displaced between the transmitter and the receiver, which creates an optical communication with the utility usage indicator indicator located within a conventional utility meter. The improved meter is capable of measuring the number of disk, dial or mechanical indicator rotations, and it is also capable of calculating and storing utility usage data from the number of disk rotations. Usage data can then be transmitted via a wired or wireless connection to the universal meter reader or a display unit.

Issued: April 9, 2002

Inventors: Michael Tracy and Robert Hinze

Assignee: Tracy Corporation II (Scottsbluff, NE)

US Patent: 6,369,710

Wireless security system

A system provides a mobile transmitter and a plurality of boundary tags for receiving communication from the mobile transmitter. Preferably, the mobile transmitter is coupled to a mobile unit, which can be an inanimate object capable of moving or being moved, or it can be a living being. The boundary tags mark the boundaries of an area within which the mobile unit is allowed to move. The mobile transmitter transmits a signal to a boundary tag. The system determines if the mobile transmitter has come into proximity of a boundary tag by receiving a reflected modulated signal from the boundary tag. If the mobile transmitter has come into proximity of a boundary tag, a response is generated. The response can be a stimulus or an alert, or both. The response can be generated at a central control station, or at a mobile transceiver that includes the mobile transmitter and a mobile receiver. In one embodiment, the boundary tag modulates a reflection of the signal transmitted by the mobile transmitter. This reflected modulated signal can be received by either the mobile transmitter or by the central control station. In an alternative embodiment invention, the boundary tag records the receipt of the signal from the mobile transmitter. The central control station transmits a second signal to the boundary tag. The boundary tag modulates a reflection of the second signal to produce the reflected modulated signal, which is then received at the central control station. Optionally, the boundary tags may have unique identifiers. The system could then include a processor programmed to determine if the mobile transmitter is in proximity of a boundary tag whose unique identifier matches one of the predetermined unique identifiers. The processor can be located in the central control station, or in the transceiver, or in another location in the system.

Issued: April 9, 2002

Inventors: David Poticny and Anthony Shober

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

US Patent: 6,368,273

Networked system for interactive communication and remote monitoring of individuals

The invention presents a networked system for communicating information to an individual and for remotely monitoring the individual. The system includes a server and a remote interface for entering, in the server, a set of queries to be answered by the individual. The server is preferably a web server, and the remote interface is preferably a personal computer or remote terminal connected to the server via the Internet. The system also includes a remotely programmable apparatus connected to the server via a communication network, preferably the Internet. The apparatus interacts with the individual in accordance with a script program received from the server. The server includes a script generator for generating the script program from the set of queries entered through the remote interface. The script program is received and executed by the apparatus to communicate the queries to the individual, to receive responses to the queries, and to transmit the responses from the apparatus to the server.

Issued: April 9, 2002

Inventor: Stephen Brown

Assignee: Health Hero Network, Inc. (Mountain View, CA)

US Patent: 6,367,014

Enhanced short message and method for synchronizing and ensuring security of enhanced short messages exchanged in a cellular radio communication system

The invention concerns a particular structure of enhanced short message, and a method for synchronizing and ensuring the security of exchanged enhanced short messages having this structure. Conventionally, an enhanced message is transmitted by a message service center to a subscriber identification module (or SIM module) of a mobile station. The body of this enhanced message contains, in particular, a first field for remote commands pertaining to a remote application. This body also contains a second field for storing the current value of a synchronizing counter, to be compared to a previous value of the synchronizing counter, stored in the SIM module. The body can contain another field for storing a certificate, the body signature – for proving the authenticity of the enhanced message, and the identity of its transmitter. The enhanced message is accepted or refused by the SIM module, depending on the coherence of these values with the internal status of the SIM module.

Issued: April 2, 2002

Inventor: Philippe Proust et. al.

Assignee: Gemplus S.C.A (Gemenos, FR)

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

www.uspto.gov