Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 5, No. 4. April, 2003

In the News: WiLDing The Hotspot

WiFi (IEEE 802.11) hotspots are popping up everywhere – in homes, offices and in public areas, where their services may be offered for sale to increase revenues or as a freebie to attract customers and build customer loyalty. Many using these hotspots do not understand how vulnerable their data is. They might be particularly shocked to find out that some people make a hobby of detecting these systems, mapping them, and perhaps tapping into them without authorization.

Hot Spot Operators (HSOs) do not offer inherently secure connections. Data is free and clear to any device running a compatible wireless card (e.g, for 802.11b). Even the minimal security of WEP is not often used, because of the need to configure devices for each hotspot and because of the inability to control access except by frequently changing keys. Security could be provided using IPsec or SSL (Secure Sockets Layer), but this is even more complex to configure for casual usage. These types of secure links are feasible for private or commercial hotspots, where the list of users is relatively static, but they do not address the difficulties faced at the public access hotspots.

The abundance of commercial hotspots connected to a high-speed Internet connection – often in convenient locales – makes an attractive target. Public users, both ethical and unethical, are well-equipped to find them.

'Scaring Up' Connections

The components typically needed to gain hotspot access are easy to obtain and install – a WiFi card, special software and GPS converts a laptop into a wireless sniffer.

An increasingly popular activity known as WiLDing (WiFi Location Discovery) or "War driving" revolves around the sniffer's ability to find hotspots. These devices are likely being used by some shady characters, although today it seems that most people operating sniffers are just curious.

WiLDing can occur while driving around town, walking or even while vacationing or riding elevators. For some, the exercise is simply to map the abundance of Access Points (APs) available, while for others it is for poking around at open networks to see where they can freeload on an Internet connection – or worse. The sniffer software makes it easy to record the findings on a laptop for later exploitation. Table 1 lists information a sniffer might record. Some WiLDers publish the hotspot locations they discover – including related information – on the Internet.

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…

May 22nd, 2003.

Future Topics

Wireless Flash Memory Security • Radius for Wireless • 3G Security • Public Keys & Wireless • Software-defined Radio Security • Security for Mesh Networks • Security in Wireless ad hoc Networks

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.

Table 1: "Sniffer" Feedback

Type of data recorded	Explanation
MAC Address	Unique identity of a computer or AP
AP Identity	The access point's designated name and the AP manufacturer.
Associated with ...	Service Set Identifier (SSID) and (optional) the identity of their client (e.g, restaurant name) derived from the MAC address.
Signal location	Wireless channel
Signal strength	Dynamically monitored while within range.
Signal encryption	Showing if WEP is enabled.
Broadcast speed	bits per second
Geo-location	Latitude and longitude of the access point giving the strongest signal at the time of record.

Recognizing the existence of WiLDers looking for purported loyalty incentives, such as wireless customer service via secure-link hotspots, the WiFi Zone program (www.wi-fizone.org) is designed to make their search easy.

All users of hotspots should beware of the unethical WiLDer. Their sniffer can detect another wireless user's laptop running a network card. While a hotspot user is connected with a non-secured link, the sniffer can be capturing userids and passwords.

Reach

WiFi hotspot signals typically reach 100 yards to a quarter of a mile, and some sniffers pick them up from a distance of almost a mile. Without too much difficulty, a serious unlicensed

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.

Networld+Interop
27th April – 2nd May 2003
Las Vegas Convention Center
Las Vegas, NV
www.interop.com/lasvegas2003

2003 Economic Crimes Summit
4th – 7th May 2003
Hyatt Regency Crystal City
Crystal City, VA
www.summit.nw3c.org

In-building Wireless 2003
5th – 7th May 2003
Sheraton National
Arlington, VA
www.iirusa.com/InBuildingWireless

SANS North Pacific 2003
5th – 10th May 2003
Doubletree Hotel
Portland-Jantzen Beach
Portland, OR
www.sans.org/northpacific03

Convergence 2003 – IT Conference and Technology Exposition
6th – 7th May 2003
Calgary Roundup Center
Calgary, Alberta
www.converge2003.com

Mobile and Wireless World
6th – 9th May 2003
JW Marriott Desert Springs Resort
Palm Desert, CA
www.mwwusa.com

2003 IEEE Symposium on Security and Privacy
11th – 14th May 2003
The Claremont Resort
Oakland, CA
www.ieee-security.org/TC/SP-Index.html

IEEE 2003 International Conference on Communications
11th – 15th May 2003
The William A. Egan Civic & Convention Center
Anchorage, AK
www.icc2003.com

The 15th Annual Canadian Information Technology Security Symposium
12th – 15th May 2003
Ottawa Congress Center
Ottawa, Canada
www.cse-cst.gc.ca/en/symposium/symposium.html

Wireless Profitability and Migration Summit
19th – 21st May 2003
Trump International Sonesta Beach Resort
Miami, FL
www.iirusa.com/mobileamericas

ICDCS 3003 – The 23rd International Conference on Distributed Computing Systems
19th – 22nd May 2003
Brown University
Providence, RI
www.cse.msu.edu/icdcs

DallasCon Wireless Security Conference
24th – 25th May 2003
The Plano Center
Plano, TX
www.dallascon.com

World Wireless Congress
27th – 30th May 2003
Renaissance Parc 55 Hotel
San Francisco, CA
www.wirelesscongress.com

Wireless Connections 2003
29th – 30th May 2003
Rozsa Centre,
University of Calgary
Calgary, Canada
www.wirelessconnections2003.com/may.html

wireless operator with an extensive home system (including a home-made antenna) could broadcast a signal that a sensitive sniffer could pick up from 8 miles away. To date, the world record distance (according to the Swedish Space Corporation) for picking up a WiFi signal is 192 miles (310 Km), achieved only by using highly specialized equipment. With this capability, and with rapid expansion of WiLDing private, public and commercial hotspots, the WiFi network practitioner should expect every signal escaping from its intended domain will be intercepted by someone.

Concluding Remarks

WiLDing, a reaction to the proliferation of unprotected hotspots, is a simple, cheap and "fun" drive-by past-time. It can be experienced vicariously in a mini-documentary streaming video presentation (titled "War Driving Demonstration").

The latest developments in technology are offering multi-band support to hotspots. This add-on allows the user to connect to 802.11a and 802.11b, and even the not-yet-ratified 802.11g, using one device.

Quick and easy High-speed Internet access to mobile phone users could become widespread. Already available in limited regions of Canada, this is made possible by a combining of technologies offered by mobile phone carriers and an HSO (FatPort, in this case). To gain hotspot access anywhere in the world, users provisioned by a participating carrier need no new or upgraded hardware or software, and no reconfiguration. Businesses enabling hotspots have a new audience where they can drag their advertising hooks. To expand the hotspot market even more, Boingo (another HSO) plans to roll out GPRS, CDMA 1XRTT and iDEN '2.5G' support. Judging by these business plans, the opportunities for WiLDing are only beginning.

Comments

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

wsp@cnp-wireless.com

Enterprise Mobility and Security: Can You Have Both?

By Dzung Tran, Ecutel

A sign of the popularity of WiFi is that the IEEE continues to work on 802.11 security upgrades, such as WiFi Protected Access (WPA) and 802.11i (also known as Robust Security Network (RSN)) and other higher speed standards, such as 802.11g, 802.11a, 802.16a and 802.20. We have not seen this much effort by the IEEE organization since the creation of the IEEE 802.3 (Ethernet) standard.

At the same time, IP-based virtual private networks (VPNs) have become the preferred method for securing communication between enterprise resources and a remote location or user. Some of these VPN products started out simply as firewalls and later became hybrids that combine VPN and firewall functions. VPNs have become a ubiquitous part of our technical lexicon.

Corporate Chief Information Officers (CIOs) are realizing that augmenting their wired network with wireless technologies not only empowers their mobile workforce and enhances worker productivity, but that it also gives them a competitive edge by having their workers more connected. In addition to WiFi, there are a number of wide-area wireless networks (including cdma2000, GPRS, EDGE, PHS and UMTS) that can help with that mobility and productivity. WiFi does not have widespread coverage, but where it is made available, it provides high bandwidth, easy setup and low price (because of its use of unlicensed spectrum). With all these available technologies, one can envision, or hope for, an easy way to connect to the enterprise network using the best available bandwidth or the cheapest available network.

There is no cookie-cutter approach when it comes to enterprise wireless security for heterogeneous networking. However, there are several industry standards and practices that have been proven over the years and that can also be leveraged for these new technologies. This article focuses on enterprise network architecture and the protocols that can provide these networks with secure mobile access in a heterogeneous network environment.

Manageable Network Architecture

Within the last 18 months, the WiFi Wired Equivalent Privacy (WEP) protocol has been proven insecure. As a result, most IT security professionals have not wanted to risk deploying WiFi access points inside the corporate firewall. Rather, they have relocated these access points to the public side or de-militarized zone (DMZ) – frequently forcing employees to use VPN technology to secure traffic and to gain access to inside resources. Connectivity of 802.11 APs outside the enterprise firewall is depicted in **Figure 1**.

At first glance, this architecture appears to solve the access problem by applying the same security regimen to all methods of accessing inside resources. However, some IT professionals quickly learned that if users want to roam freely in WiFi, these access points had to be configured with the same SSID and had to be placed in the same subnet or the same VLAN. This configuration is necessary because network applications and VPN sessions are sensitive to changes in the IP address. If a user's IP address changes due to subnet connection changes during roaming, then application connections can drop, forcing the user to re-establish his VPN session.

It is obvious that a more comprehensive solution must be used to solve the inter-WiFi roaming problem, which includes roaming between existing LAN networks (inside the firewall), between new WiFi networks (outside the firewall), between hot spots and with wireless wide-area networks.

Figure 2 depicts, conceptually, seamless and secure roaming from one access technology to another while maintaining the VPN tunnel.

One way to provide seamless and secure roaming between heterogeneous networks is by implementing protocols such as IETF Mobile IP and IPSec to provide mobility and security, respectively. This approach can also leverage additional security measures such as RADIUS and PKI, as back-end authentication protocols – to authenticate user devices to corporate servers.

Figure 1: WiFi Access Points are placed Outside the Corporate Firewall

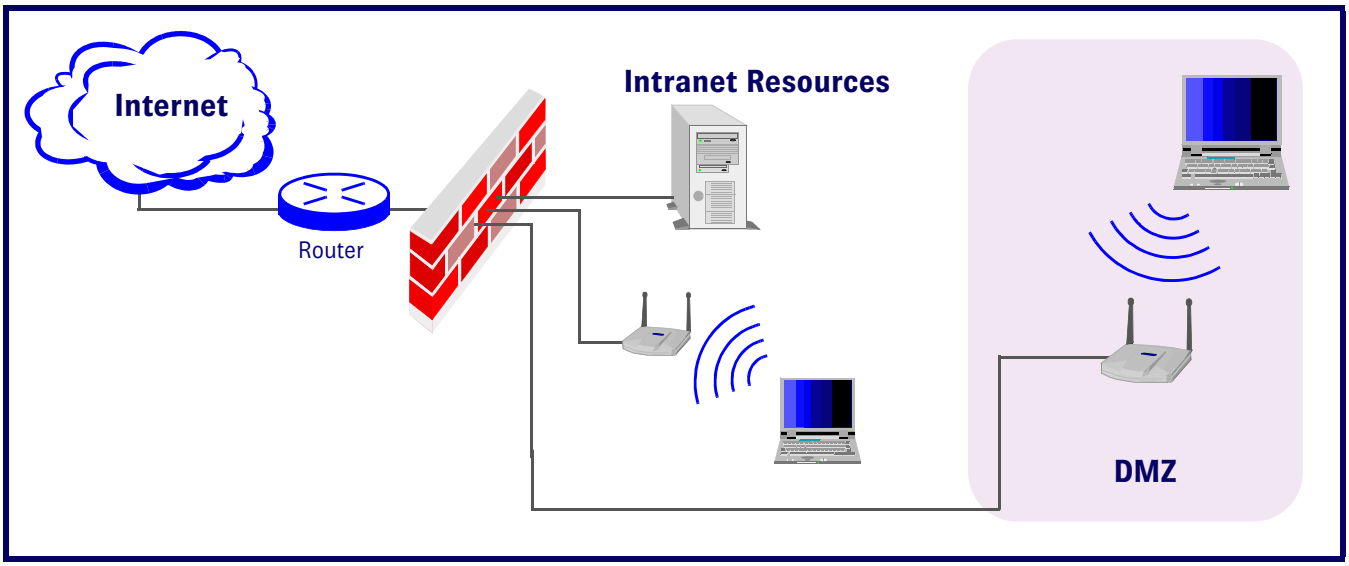
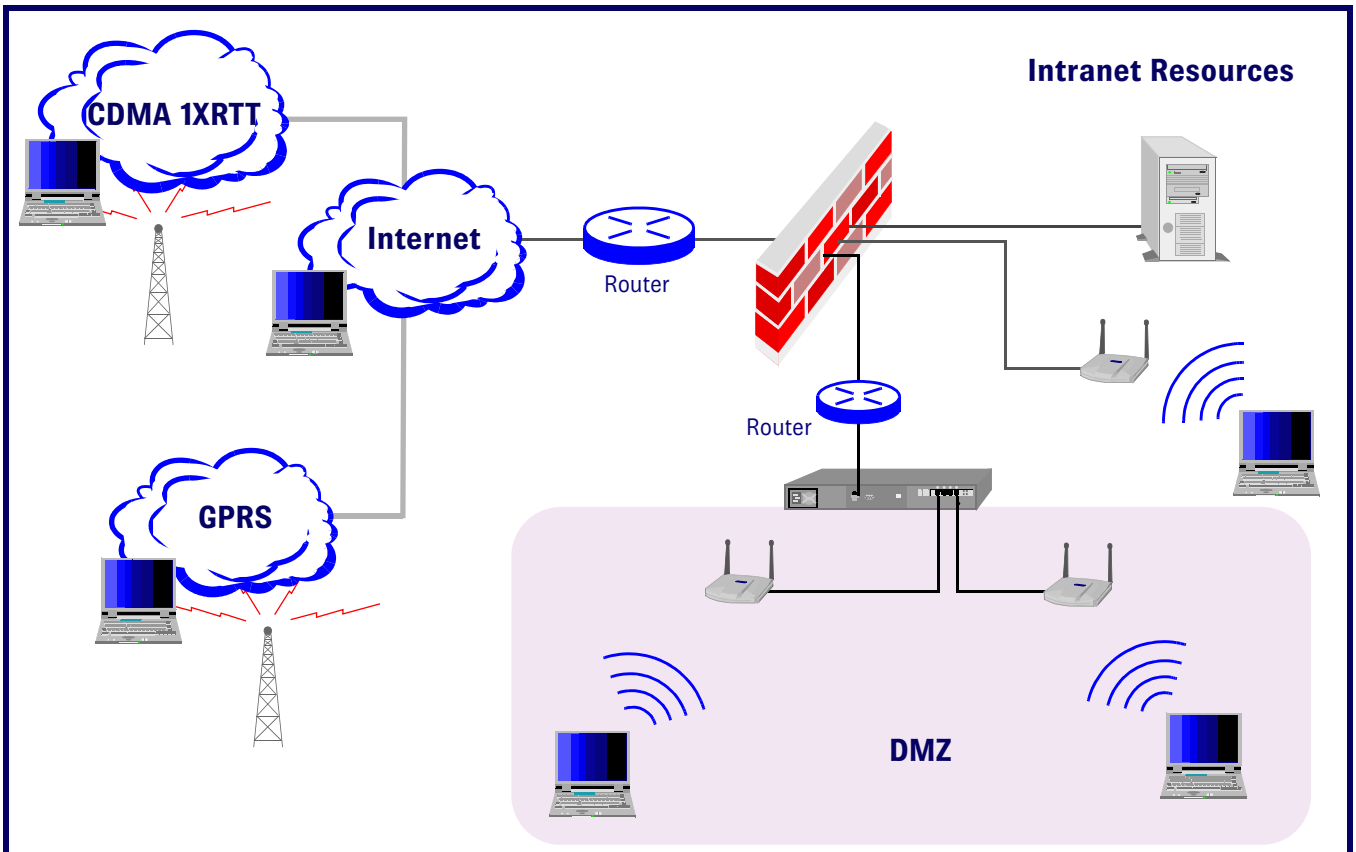


Figure 2: Heterogeneous Roaming with Security



Heterogenous Secure Roaming – The device is able to connect at all locations where the illustration shows the laptop.

To implement this solution in an enterprise, three issues must be addressed: Network-agnostic mobility, mobile network security and device provisioning. These issues will be addressed in the following paragraphs.

Network-Agnostic Mobility

Traditional layer-2 mobility, which provides mobility within the same network type, such as between two GSM networks or between two WiFi hotspots, is too limited for today's wireless world.

Network-level mobility requires a network-layer protocol implementation on mobile devices and within the network infrastructure. By using layer-3 mobility, a mobile device can take on a new IP network connection and still be able to maintain the same layer-3 "persistent" IP address, regardless of the type of network to which it is connected. The mobile device can then roam anywhere, using the same identity parameter (IP address), just like cellular roaming keeps people reachable by their same phone number. This ability to maintain the same IP address regardless of where the device connects enables a seamless connection to the enterprise network as the user moves from one network to another.

The Internet Engineering Task Force (IETF) Mobile IP, or MIP, is a protocol providing such mobility capability. For details, refer to:

www.ietf.org/rfc/rfc2002.txt?number=2002

and

www.ietf.org/rfc/rfc3344.txt?number=3344

Mobile IP consists of the following components:

- **Mobile Node.** The Mobile Node (MN) is the mobile host device that is "roaming" from one network or subnetwork to another.

- **Home Agent.** The Home Agent (HA) resides within the enterprise network infrastructure in a particular subnet called the home subnet, which is the base subnet for registered mobile users. The HA is a specialized router on the mobile node's home network which tunnels data for delivery to the mobile host and which maintains current location information for the mobile node.

- **Foreign Agent.** The Foreign Agent (FA) resides in a subnet other than the home subnet, and it relays traffic to the HA. The FA is also a specialized router providing services to the mobile node.

Each time an MN-enabled device roams from one network to another, it immediately acquires a new IP "care-of address" via DHCP, PPP, or the FA. The MN informs its assigned HA of its new address through a process called MIP registration, which is the exchange of UDP packets containing registration information. For integrity protection of this data, a message digest (or hash), using MD-5, is computed, based on a pre-shared secret, known only by the MN and the HA.

If an MN connects to a subnet with an FA, the MN would then ask the FA to forward its registration to the assigned HA, and it later will use the FA's IP as its care-of address. After successful registration, all IP packets sent to the MN via the home subnet will be intercepted by the HA and immediately tunneled to the roaming MN via its care-of address. The reverse traffic originating from an MN may either be 'reverse tunneled' through the HA using the care-of address or sent directly to the destination IP address, as illustrated in **Figure 3**.

Mobile Network Security

IPSec is an IETF standard (RFC 2400 series) designed for the network layer or layer-3 security is IPSec. Although complex, it is the only industry-standardized protocol for network security. IPSec provides strong mutual peer-to-peer authentication, IP traffic anti-forgery protection, anti-replay protection, source header authentication and data confidentiality. It also provides key agreement and IP packet processing.

In simple terms, IPSec works as follows:

1. Two peers exchange security policies with each other so that they can agree on a set of cryptographic parameters to protect IKE (Internet Key Exchange) traffic.
2. Both sides exchange a random number and a self-generated public value of the Diffie-Hellman algorithm.
3. Both sides generate internal shared secrets based on a Diffie-Hellman computation, to protect subsequent traffic.
4. Using a pre-shared secret or an X.509 digital certificate to compute a digital signature, this traffic is used to allow the peers to present their identities and signature proofs to each other.

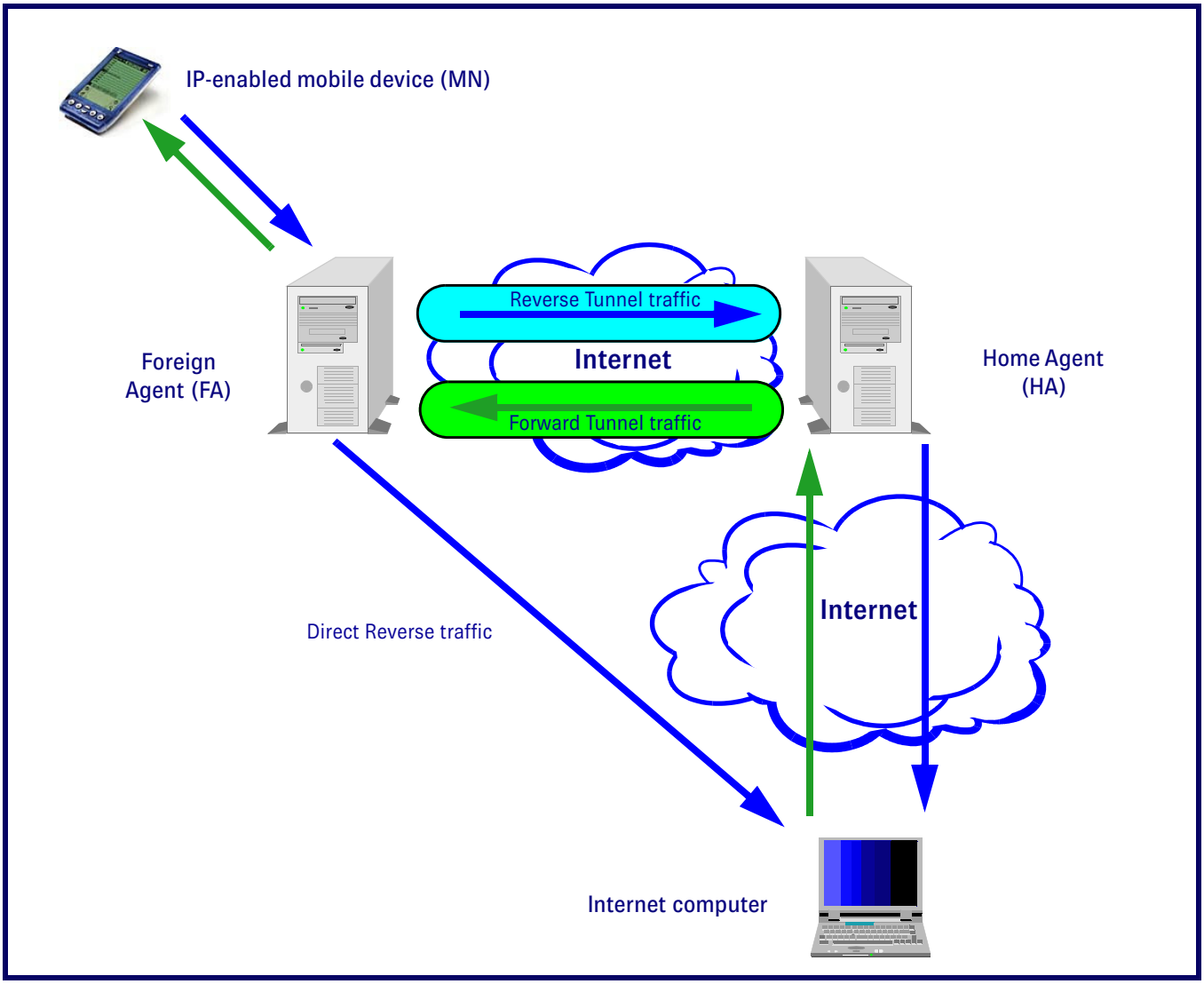
These four steps are part of IKE Phase 1 Main Mode. The IPSec protocol also allows IKE Phase 1 Aggressive Mode key exchange, which cuts in half the total number of Phase 1 steps, but each peer's identity is not protected with encryption while being transmitted. During the last steps of IKE Phase 1, IKE payloads are protected with algorithms such as 3-DES and HMAC-SHA-1.

IKE Phase 2 (also known as Quick Mode), starts after IKE Phase 1 is completed, to allow both peers to establish symmetric keys, which are used for packet encryption and packet integrity computation. All IKE Phase 2 exchanges are protected with algorithms such as 3-DES and HMAC-SHA-1.

IPSec also supports Perfect Forward Secrecy (PFS), where one additional Diffie-Hellman key exchange can take place immediately before the start of IKE Phase 2, under protection of encryption and integrity algorithms, to derive a shared secret to protect later symmetric key material exchanges. This is done to ensure that, in the unlikely event a key is compromised, the key cannot be used to derive subsequent keys to decrypt subsequent traffic.

It is feasible to integrate device mobility registration, mutual IPSec security authentication, data confidentiality and packet integrity control based on Mobile IP and IPSec. Specifically, MIP can be used first to establish an MN-HA tunnel, in which persistent IP-based applications traffic between the MN and the HA is further protected by the IPSec protocol. These two standards, in addition to other relevant cryptographic standards (on which these standards are based), have been thoroughly scrutinized by the Internet standards bodies and industry to ensure that they provide the best techniques to implement network mobility and security.

Figure 3: Mobile IP Tunnelling



Device Provisioning

Remote access using an IP VPN is still a viable and popular method in many enterprise environments. Remote access can be accomplished from a wired or a wireless connection to a fixed VPN gateway. This model is built on the static IPSec framework to provide data security to remote but stationary users. This static framework, however, places constraints on users, and it does not leverage technologies that best fit the user's working environment and habits, such as LAN and WiFi at the office, and CDMA 1XRTT while on the road.

To enhance mobile node mobility, the IT department needs to establish a network-based policy-provisioning system to give mobile devices secure roaming access capability. Provision should ensure that the Mobile IP protocol is used as an extension to the network stack. This enables a mobile device to roam seamlessly across heterogeneous network boundaries – using wired or wireless technologies – while maintaining a persistent network IP address. Persistent IP addresses allow application sessions to continue while the mobile device roams between networks, and even between access technologies (e.g, WiFi, 1XRTT and GPRS). The complexity of network IP address changes for each interface is hidden from the applications.

The provisioning system should also automatically enforce security policy so that limited user intervention is required and security is handled as transparently as possible.

The degree of success of a secure heterogeneous network access provisioning system should be measured in terms of return on investment (ROI) and users' ability to focus on their work. A highly successful network does not fritter away users' time by forcing them to set up security parameters.

Assessment

The IEEE 802.11i protocol will soon be ratified, and products are expected to be available by the end of 2003 or early in 2004. However, IT security managers are not expected to rush out and buy new WiFi access points in anticipation of better security than WEP. After the WEP debacle, IT managers are likely to

remain cautious about deploying WiFi access points inside the firewall, continuing to treat them as hostile.

Until WiFi networks are again embraced within the firewall, IT departments are challenged with finding ways to support their mobile users. The challenge suggests a focus on providing comprehensive security and seamless mobility across disparate networks in order to increase productivity and to reduce the support cost associated with the mobile users. The combination of Mobile IP and IPSec, as we have seen, is a near-term, viable solution.

About the Author

Dzung Tran is co-founder and CTO of Ecutel. Since the early 1980s, he has worked in areas such as decision aids, network control, network mobility, data security, wireless communications, and project management. Before Ecutel, he held positions with MITRE Corporation, Delfin Systems, E-systems Raytheon, and PRC (Northop Grumman). He has an M.S. in computer science from George Washington University and a B.S. in computer science, *magna cum laude*, from the University of Maryland.

The author can be contacted at:

dtran@ecutel.com

About Ecutel

Ecutel specializes in mobile VPN software for maintaining security regardless of whether users are inside or outside their offices. It works with wired and wireless networks, including wireless LANs and WANs. Ecutel's technology is based on security and mobility standards such as IPSec and Mobile IP.

Ecutel was founded in 1996 by two former Department of Defense (DoD) software information network experts. The company refined its technology as consultants to the DoD on its security and mobility problems. Today, Ecutel's products solve the same problems in other organizations, public and private. Viatores™, the company's flagship product, was released in August 2001. Ecutel is based in Alexandria, VA.

Fraud and Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following fraud and security patents. These will 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).

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.

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: 6,553,129

Computer System linked by using information in data objects

Various improvements to steganographic systems, and a listing of applications for which these improvements are intended.

The improvements include:

- Facilitating scale and rotation registration for steganographic decoding by use of rotationally symmetric, steganographically embedded patterns and subliminal digital graticules;
- improved techniques for decoding without access to un-encoded originals;
- improving robustness of steganographic coding in motion pictures and/or in the presence of lossy compression/decompression, and;
- representing data by patterned bit cells whose energy in the spatial domain facilitates decoding registration.

Applications include enhanced-security financial transactions, counterfeit-resistant identification cards, fraud deterrent systems for cellular telephony, covert modem channels in video transmissions, photo duplication kiosks with automatic copyright detection, and hotlinked image objects (e.g, with embedded URLs) for use on the Internet.

Issued: April 22, 2003

Inventor: Geoffrey Rhoads
Assignee: Digimarc Corporation (Tualatin, OR)

US Patent: 6,550,008

Protection of Information Transmitted over Communication Channels

A method and apparatus for protecting information communicated between a first and a second device includes generating a request to a third device, the request including information identifying the first and second devices. The third device verifies the first and second devices based on the information in the request. Predetermined information is sent to at least one of the first and second devices, and the first and second devices authenticate each other based on the predetermined information.

Issued: April 15, 2003

Inventors: Minda Zhang and Richard Takahashi
Assignee: Intel Corporation (Santa Clara, CA)

Interesting references:

[1] Menezes. *Handbook of Applied Cryptography.* 1996. sec. 1.9, sec. 9.4.

[2] Digital Video Broadcasting. *DVB Shows Conditional Access Common Sense.* pp. 1, printed from web site:

www.dvb.org/dvb.sub.-news/dvb.sup.-pr025.htm

dated at least as early as December 30, 1998.

[3] Electronic Privacy Information Center, Digital Signatures, pp. 1-2, printed from web site:

www.epic.org/crypto/dss

dated as early as January 14, 1999.

US Patent: 6,549,625

Method and System for Connecting Mobile Terminal to a Database

A communication system and a method of communication.
The communication system includes:

- An information source;
- a position transceiver disposed at a broadcast location and coupled to the information source, the position transceiver broadcasting information from the information source within a broadcast area where the position transceiver is located, the information including identification information relating to the information source;
- a mobile terminal within the broadcast area comprising first and second transceivers, the first transceiver communicating with the position transceiver;
- a network communicating with the second transceiver, and;
- a database, communicating with the network, storing information which is transmitted to the second transceiver associated with the identification information in response to the database receiving at least the identification information by transmission of the network from the mobile terminal to the database.

Issued: April 15, 2003

Inventor: Heikki Rautila, *et al*
Assignee: Nokia Corporation (Espoo, FI)

US Patent: 6,549,623

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: April 15, 2003

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

US Patent: 6,546,492

System for Secure Controlled Electronic Memory Updates via Networks

A system and method for updating software for a remote unit over a network. The system and method includes the remote unit, an authentication server and an update server. The remote unit may have a flasher host for communicating over the network and for transmitting commands to the remote unit.
The system and method allows for the verification of a request message from the remote unit, and a response from the authentication server.
The response message to the remote unit from the authentication server will contain a decryption key to decrypt the update file that will be sent by the update server. Such an authentication process prevents rogue programs from being sent to the remote unit, which is a means for decreasing the potential for cellular fraud.

Issued: April 8, 2003

Inventors: Anthony Walker and John Petty
Assignee: Ericsson Inc. (Research Triangle Park, NC)

US Patent: 6,543,536

Spread Spectrum Communications with Selectable Data Transfer Rate

A spread spectrum communications system that is operable to provide user-selectable data transfer rates, comprising a user station for generating an access request and a gateway server for receiving the access request. The gateway server includes:

- A rate unit for comparing a requested rate to assigned rates, a selector for selecting an available user channel and an available signaling alphabet and,
- an allocation unit for assigning the carrier, user channel, and alphabet to the access request.

One of several offered transfer rates is assigned to the available user channel. Each offered rate corresponds to a set of signaling alphabets with low cross-correlation for data transfer.

Issued: April 1, 2003

Inventor: John Hershey, *et al*
Assignee: General Electric Company (Niskayuna, NY)

US Patent: 6,540,138

Voting Method and System

A voting system providing a voter identification card to a voter, the card having an optical code including voter identification information. The optical code on the card is read at a polling station prior to permitting the voter to vote, and a digital signature is received from the voter. A handheld wireless data acquisition device is provided to the voter for making voting selections, and a receipt with the voting selections made by the voter is printed. The voting selections are wirelessly transmitted from the handheld wireless data acquisition device to a host computer, where the voting selections are tallied from a plurality of voters.

Issued: April 1, 2003

Inventors: James Hall and Jerome Swartz
Assignee: Symbol Technologies, Inc. (Holtsville, NY)

US Patent: 6,539,092

Leak-resistant Cryptographic Indexed Key Update

Methods and apparatuses for increasing the leak-resistance of cryptographic systems using an indexed key update technique. For example, a cryptographic client device could maintain a secret key value as part of its state. The client can update its secret value at any time – for example, before each transaction, using an update process that makes partial information about the secret – that might have previously leaked to attackers – no longer useful. By repeatedly applying the update process, information leaking during cryptographic operations – and collected by attackers – rapidly becomes obsolete. Thus, such a system can remain secure (and in some embodiments, it is provably secure) against attacks involving analysis of measurements of the device's power consumption, electromagnetic characteristics, or other information leaked during transactions.

This invention can be used in connection with a client and server using such a protocol (as described above). To perform a transaction with the client, the server obtains the client's current transaction counter. The server then performs a series of operations to determine the sequence of transformations needed to re-derive the correct session key from the client's initial secret value. These transformations are performed, and the result is used as a transaction session key.

This invention includes a sequence of client-side updating processes that allow for significant improvements in the performance of the corresponding server operations.

Issued: March 25, 2003

Inventor: Paul Kocher
Assignee: Cryptography Research, Inc. (San Francisco, CA)

Interesting references:

[1] Hachez, *et al. Timing Attack: What Can Be Achieved by a Powerful Adversary?* 1999.

[2] Paul Kocher. *Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attacks.* Report 7, December, 1995.

[3] J. Ryan. *Blinds for Thermodynamic Cipher Attacks.* Unpublished material on the world wide web at:

www.cybertrace.com/papers/thrmatak.html

March, 1996.

[4] E. Biham, *et al. Differential Fault Analysis of Secret Key Cryptosystems* in: Kaliski, B., Advances in Cryptology – CRYPTO 97, (Berlin, Springer, 1997) 17th Annual International Cryptology Conference, August 17-21, 1997. pp. 513-525.

[5] Friedrich L. Bauer. *Cryptology – Methods and Maxims.* Technical University Munich, 1998. pp. 31-48.

US Patent: RE38,070

Cryptography System and Method

A cryptography system architecture providing cryptographic functionality to support an application requiring encryption, decryption, signing and verification of electronic messages. The cryptography system has a cryptographic application program interface (CAPI) which interfaces with the application to receive requests for cryptographic functions. The cryptographic system further includes at least one cryptography service provider (CSP) that is independent from, but dynamically accessible by, the CAPI. The CSP provides the cryptographic functionality and manages the secret cryptographic keys. In particular, the CSP prevents exposure of the encryption keys in a non-encrypted form to the CAPI or application. The cryptographic system also has a private application program interface (PAPI) to provide direct access between the CSP and the user. The PAPI enables the user to confirm or reject certain requested cryptographic functions, such as digitally signing the messages or exportation of keys.

Issued: April 8, 2003

Inventor: Terrence Spies, *et al*
Assignee: Microsoft Corporation (Redmond, WA)

Interesting references:

[1] Description of Internet payment system from CyberCash Inc. (February, 1995).

[2] Description of Internet market system from Virtual Holdings, Inc. Copyright 1994-1995.

[3] Bellare, *et al. IKP-A Family of Secure Electronic Protocols.* April 16, 1995.

[4] Gifford, *et al.* Payment Switches for Open Networks. (1995).

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