Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 6, No. 1. January, 2004

RFID Alternative in an 802.11 Network

In December 2003, National Scientific Corporation demonstrated an alternative tracking system: the WiFi Tracker. Using triangulation, this system provides location information with an accuracy of a few feet when within range of any standard WiFi 802.11x network.

With its broader signal range, this device may help launch a new set of applications that are difficult or impossible with RFID technologies. For example, a WiFi tag could be programmed to report its position when certain conditions are met (e.g, a minimum time and distance from the last report has been exceeded) and it is within range of a WiFi access point. In an 802.11 system provisioned with access points, network cards and a map image of the premises (formatted as BMP, JPG or PNG), the WiFi tag responds to queries originating from the Ekahau positioning tool , which then produces an up-to-the-minute image of all tagged devices.

A WiFi tag could also be coupled with sensors to report air temperature, humidity, the presence of toxic gases, or even images taken by a remote camera. For example, these could be installed on remotely controlled vehicles at a huge mining operation, thus avoiding the use of human operators in areas of questionable safety. A system like this is beyond the capability of an RFID system.

Unfortunately at this time, the prototype WiFi Tracker unit has a few disadvantages: 1) it cannot be hidden within small items, since it is about the size of a deck of cards; 2) battery life is limited; and 3) it uses the security-risk-proneWiFi technology.

Due to these disadvantages, it is not likely to compete well with RFID for retail or wholesale inventory tracking. By January 2005, the 100 largest suppliers to Wal-Mart must add radio frequency identification (RFID) tracking technology to crates and pallets. That requirement translates into roughly 1 billion tags and should drive down the cost of an RFID tag, currently between 30¢ and 50¢, to about 5¢, a point where more retailers can make a business case for adopting the technology.

WiFi tags will have benefits for tracking expensive assets, where the cost of the tracking device is minimal. They will be most applicable in campus environments where WiFi connectivity will be available a good amount of the time. A big advantage with these tags is that they can report remotely, using WiFi for communications, unlike RFID, where the reader has to be very close to the tagged device.

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:

cnpsales@cnp-wireless.com

Next Issue Due…

February 26th, 2004.

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.

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.

Wireless LAN and 802.11 Security Workshop

3rd February 2004
Courtyard Houston
Houston, TX

www.itvshop.com

The 11th Annual Network and Distributed System Security Symposium

4th- 6th February 2004
Catamaran Hotel
San Diego, CA

www.isoc.org/isoc/conferences/ndss/04/index.shtml

Financial Cryptography '04

9th- 10th February 2004
Holiday Inn Beachside
Key West, FL

fc04.ifca.ai/index.htm

Wireless Security Technical Conference

10th February 2004
ISA Headquarters
Research Triangle Park, NC

www.isa.org/wiresec

CDMA200 1xEV-DO and 1xEV-DV

11th- 12th February 2004
Qualcomm
San Diego, CA

www.pcca.org/news/Agendas/ag04-02.htm

Servicing Today's Mobile and Global Enterprise

18th February 2004
Korn Hall, UCLA
Los Angelos, CA

www.cio-conference.ucla.edu/index.asp

Wireless Networking and the Evolving Telecommunications Infrastructure

23rd- 25th February 2004
UC Berkeley
Berkeley, CA

www.unex.berkeley.edu/cat/303586.html

RSA Conference 2004

23rd - 27th February 2004
Moscone Center
San Francisco, CA

www.rsasecurity.com

Broadband Wireless World 2004

24th- 25th February 2004
San Diego Convention Center
San Diego, CA

www.shorecliffcommunications.com/bww04

Janet Wireless Event

26th February 2004
Coventry Techno Center
Coventry, UK

www.ja.net/conferences/wireless/feb-04/prog.html

URL of the Month

Information Security Magazine – library category: Wireless Security

library.infosecuritymag.com/data/rlist?t=1016747982_81244038

This URL links to a number of white papers that will be of interest to the wireless community:

Understanding the Layers of Wireless LAN Security & Management – **AirDefense**

Practical Solutions for Securing Your Wireless Network – **Aventail**

Developing Custom Solutions to Extend Your Data Wirelessly – **Blackberry**

Wireless LAN Security - What Hackers Know That You Don't – **AirDefense**

802.11g - The Need for Speed – **Arirmagnet**

Wireless LAN (WLAN) End to End Guidelines for Enterprises and Public Hotspot Service Providers – **Intel**

Are You The Arcanist of Them All?

For the series in last month's Arcanist question, each number, when read out a digit at a time, describes the previous number. So, 312211, the last number in the series, can be described as One Three, One One, Two Twos, Two Ones, or 13112221.

Congratulations to Duncan Ho of Qualcomm for submitting the correct answer last month (he declined the prize).

The question for this month: What is next in the series: 212, 312, 213, 214 ... ? And why?

Submit your answer to wsp@cnp-wireless.com

Securely Enabling Intermediary-based Services

Sneha Kasera, Semyon Mizikovsky,
Ganapathy S. Sundaram and Thomas Woo
Lucent

Erratum. In last month's *Wireless Security Perspectives* article about China WiFi, the acronym "CCM" was said to represent Counter Code-book Mode. CCM is actually, "Counter with CBC-MAC" ... a generic authenticated encryption block cipher mode.

Wireless carriers are evolving from providing basic Internet connectivity (a "dumb-pipe") to offering intermediary-based services and performance optimization to enhance users' experiences, including TCP performance improvements, multimedia packet filtering, header compression and prevention of denial-of-service (DoS) attacks. These services need the assistance of intermediate nodes placed in the carrier's network between communicating end-points.

An intermediate node could be a router, a switch, an application gateway, a middle box [1], a performance-enhancing proxy [2] or a node of an overlay network. It uses the knowledge of aggregated and per-flow traffic behavior at its location, as well as its processing, caching and filtering capabilities. To enable intermediary-based services users may need to communicate with network intermediaries for configuration and solicitation of service. They must also make information available to the intermediary that might be necessary for the requested services.

The second problem is very challenging, especially when an end-to-end security solution such as IPsec is used. This currently enforces the encryption and authentication of the entire payload that is received from the upper layers. This ensures the security of the entire payload, including the transport headers and even network layer headers in some cases, between two end-points that have established a security association [3]. Unfortunately, the current IPsec architecture prevents even trusted intermediaries from examining the payload and therefore prohibits the provision of value-added services and performance optimization.

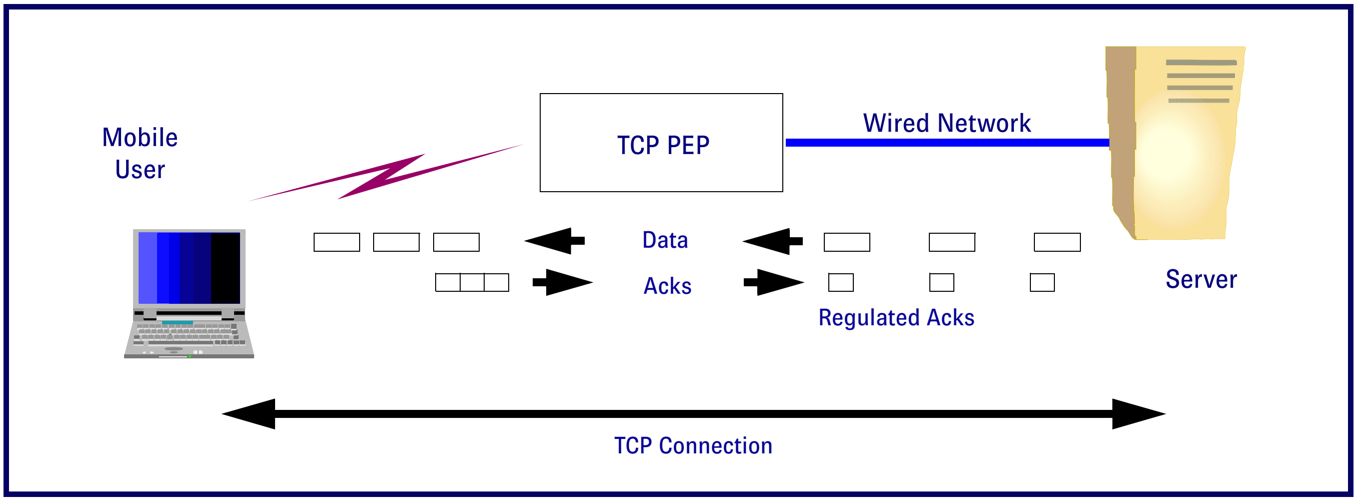
It is possible to use two separate IPsec security associations, one between the end-user and the intermediary and another between the intermediary and the remote end-point. Such a split-IPsec solution is unacceptable to many users because it forces them to expose all of their data to the intermediary.

Intermediary-Based Services and Performance Enhancements

TCP Enhancements

Variance in delay greatly influences TCP performance [4]. Large delay variance decreases the effective client throughput of all TCP-based applications. An accepted mechanism for enhancing TCP (Transmission Control Protocol) performance in such situations is the implementation of a TCP-PEP (IETF RFC 3135) at an intermediate node. The TCP-PEP (TCP with Performance Enhancing Proxies) can examine, modify or generate TCP packets to match the characteristics of the wireline and wireless interfaces, improving end-to-end TCP performance. **Figure 1** shows an example of TCP throughput enhancement for a wireless user communicating with a server using TCP. An intermediate TCP-PEP regulates the acknowledgments (Acks)[4] from the mobile host to adapt to the large variations in wireless delay experienced by data flowing towards the mobile, thereby enhancing overall TCP throughput by smoothing out the burst of TCP data that would follow the receipt of a burst of Acks.

Figure 1: TCP Ack Regulator

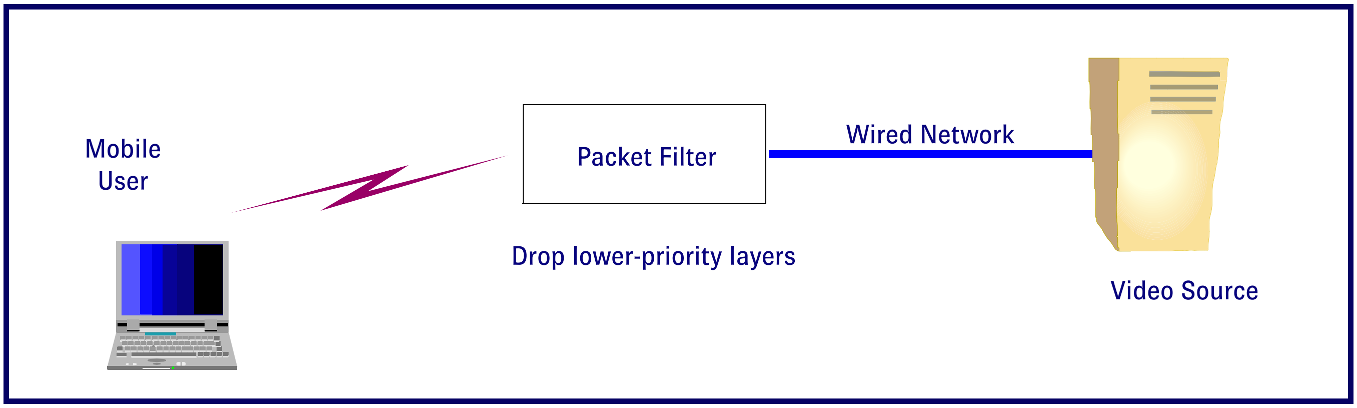


Packet Classification and Policy Implementation

An intermediate node can identify flows based on source and destination IP addresses, TCP or UDP source and destination port numbers, and next protocol identity, to offer QoS guarantees and priority treatment to more important packets. For example, the intermediate node could assign lower priority to nonconforming UDP traffic and a higher priority to TCP traffic during link congestion.

The specific classification method and policy implementation depend on the application. Figure 2 shows an example of filtering packets based on multimedia header information to dramatically improve video quality [5]. Multi-layer video is transmitted from the source to a wireless receiver. Based on changing air link conditions, the intermediate node, in the path from the source to receiver, selectively drops packets of lower priority layers. The priority of the layers is found in the multimedia transport header. The intermediate node performing the selective dropping must understand the multimedia header format.

Figure 2: Multimedia Packet Filtering



Header Compression

Compressing protocol headers saves wireless bandwidth by eliminating redundant or repetitive information [6, 7]. Although, it is possible to achieve header compression between two end points of an IP tunnel or two adjacent IP hops, most of the header compression schemes are sensitive to delays and loss between the end-points [8, 9]. Achieving header compression and decompression close to a congested link with the help of an intermediary will improve the performance of header compression schemes.

One might argue that if the last hop wireless link is the only congested link that contributes most of the loss and delay, then an intermediary-based header compression will not necessarily improve performance over end-to-end header compression. This is not the case when both the end points are wireless users. Future multi-hop wireless networks will contain multiple wireless links. For each of these, bandwidth will be limited and transmission potentially lossy. Implementing end-to-end header compression will only result in partial gains. Intermediary-based header compression, performed independently for every wireless link, will improve the performance of header compression due to lower loss and delay [8, 9].

Prevention of Denial-of-Service

Intermediate nodes could filter out packets from unwanted sources to enterprise VPN clients, which typically establish secure sessions with their enterprise gateways for accessing their company resources (i.e, computers and servers). These clients – especially bandwidth-limited wireless users – have the potential for being flooded with unwanted IPsec packets from spoofed enterprise IP addresses.

These unwanted packets could be “ingress-filtered” at an intermediate node (e.g, a Packet Data Serving Node) on the path from the enterprise client to the enterprise gateway by setting up an additional authentication tunnel between the enterprise gateway and the intermediate node. On receiving packets with source addresses set to valid enterprise IP addresses, the intermediate node will pass through only those packets that it can authenticate. (Figure 3).

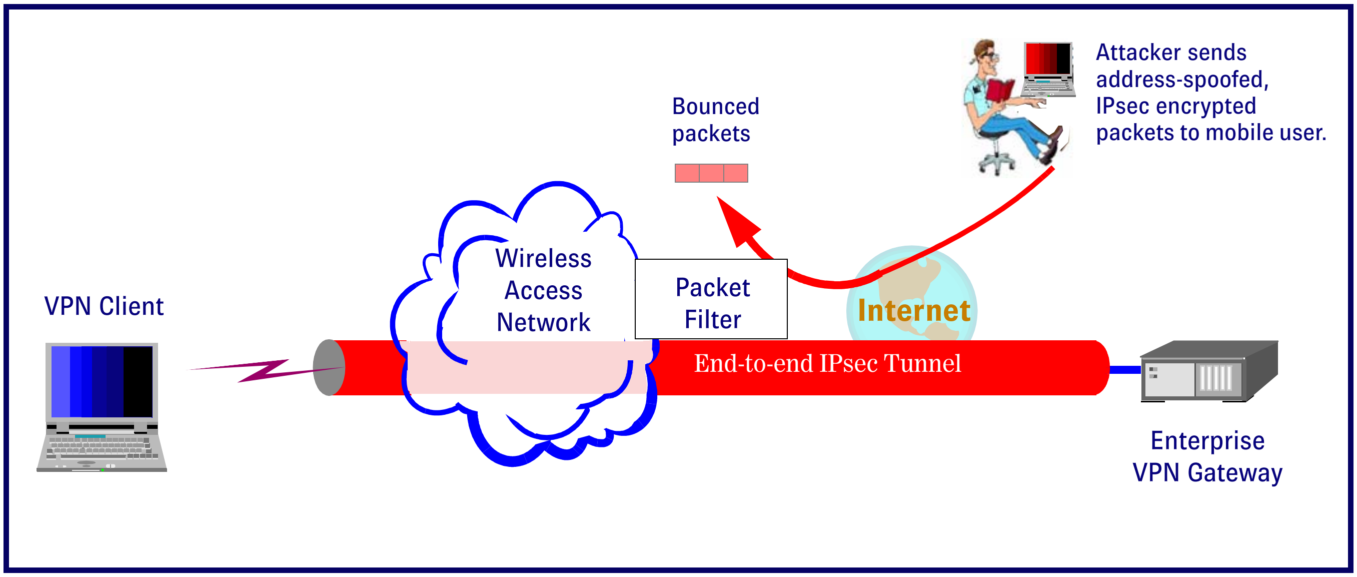
Architecture

Our architecture for securely enabling intermediary-based services has four components.

Communication between End-points and Intermediary

Communication between end-points and the intermediary may be necessary in order to advertise, configure, provision, register, solicit, consent and negotiate services. For example, a network intermediary must be configured to set up additional authentication tunnels for enabling DoS protection. Even in cases where an intermediary can transparently perform its services without actively interacting with the end-points, explicit communication between end-points and the intermediary may be required when end-to-end security solutions (e.g, IPsec) are used to set up trust relationships and security associations.

Figure 3: Prevention of Denial-of-Service



Our architecture includes a protocol that is built on top of a reliable communication channel (using TCP) between the end-points and the intermediary. This protocol is used for all the communication between the end-points and the aforementioned intermediary. In fact, this protocol is necessary to securely set up intermediary-based services even when there is no end-to-end security mechanism in place.

The communication protocol includes:

- **Advertisement** lets intermediaries advertise the services and performance enhancements that are offered.
- **Registration** includes the processes of the client choosing the services, as well as mutual authentication between the intermediary and the end points.
- **Provisioning** includes the exchange of all necessary parameters for the relevant services, as well any session key that the end points might need to exchange individually with the intermediary. Our protocol requires the intermediary to be addressable at the IP layer1.

Exposing Information

Another key aspect of enabling intermediary-based services is selective exposure of information to an intermediary by the end points that might be required for offering services. Typically, in order to provide service, an intermediary may need access to the protocol headers of the data packets. For example, an intermediary providing a TCP PEP service [10] will need access to the TCP headers. Currently, there is no standard way of exposing and accessing protocol headers when an end-to-end security protocol such as IPsec Encapsulating Security Payload (ESP) [3] is used.

In our architecture, we propose a new IPsec option called Encapsulating Security Variable Payload (ESVP) for selectively exposing information.

The information that is exposed to an intermediary is secured from the rest of the network by using additional security layers between the end points and the intermediary. Our architecture allows the flexibility of using additional IPsec layers between the end points and the intermediary, and any link layer security mechanisms between a wireless user and the intermediary if the intermediary is its link layer peer. In many cases, the wireless link layer security is mandatory, so our architecture allows this to be used without incurring additional overheads at the IP layer.

It should be noted that the service for preventing DoS attacks does not require exposing any information. It only requires communication between the end-points and the intermediary to set up additional authentication tunnels.

Policy Engine

There are several critical dimensions of the problem of selectively exposing information. Who decides what to expose and whom to expose to? And who has access rights to the exposed information? What information should be exposed to the intermediary will depend upon the services offered by the intermediary and the security requirements of the end user applications. The question of who has the authority – an end-point or an intermediary – to decide what to expose is extremely important and has serious security implications.

Another important issue is whether an intermediary should be allowed to only inspect the exposed information but not modify it, or whether an intermediary should be allowed to both inspect and modify the exposed information. The answers to these questions will once again be service or application-specific (or both). Our architecture provides a policy engine that generates the rules for addressing these questions. Although our policy engine is flexible, we believe only the end points should decide what information should be exposed, to which intermediary it should go, and what access rights to the information are allowed. Once the rules are made for a particular session or sessions requiring a certain kind of service, a rule engine at the end points generates the appropriate ESVP packets for a session.

Detecting Inappropriate Behavior of the Intermediary

Preserving acceptable security and allowing an intermediary to perform its services while selectively exposing information to an intermediary is a challenging task. Once again, this aspect of the problem is also multi-dimensional.

First, how much trust could be placed on an intermediary? The answer depends on the end user applications and services. Second, how can one ensure that the intermediary does not play "end-to-end" games? For example, an intermediary with access to TCP headers could change the ordering of TCP packets even when the TCP payload is encrypted. We are considering adding additional fields in the encrypted portion of the ESVP packet to detect any attempts by the intermediary to play end-to-end games. The details of the overheads – in terms of bytes, how often the additional fields are added (with every packet or statistically with only a small random subset of packets), enhanced rule engines to add these bytes and detect inappropriate behavior at end-points – these points are still being worked out.

To be continued...

In our **February, 2004 issue** we will continue with a discussion of the 'Encapsulating Security Variable Payload' (ESVP) protocol, including a description of potential applications and a comparison of ESVP with related work.

References

[1] P. Srisuresh, et al. *Middlebox Communication Architecture and Framework*. RFC 3303, Aug. 2002.

[2] J. Border, et al. *Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations*. RFC 3135, June 2001.

[3] S. Kent and R. Atkinson. *Security Architecture for the Internet Protoco*l. RFC 2401, Nov. 1998.

[4] M. Chan and R. Ramjee. *TCP/IP Performance over 3g Wireless Links with Rate and Delay Variations*. In Proc. of ACM Mobicom, Sep. 2002.

[5] R. Keller, et al. *An Active Router Architecture for Multicast Video Distribution*. In Proc. of IEEE Infocom, Mar. 2000.

[6] V. Jacobson. *Compressing TCP/IP Headers for Low-speed Serial Links*. RFC 1144, Feb. 1990.

[7] C. Bormann, et al. *Robust Header Compression (ROHC): Framework and Four Profiles: RTP, UDP, ESP, and Uncompressed*. RFC 3095, July 2001.

[8] M. Degermark, H. Hannu, L. Jonsson, and K. Svanbro. *Evaluation of CRTP Performance over Cellular Radio Links*. IEEE Personal Communications, pages 20–25, August 2000.

[9] S. Dorward and S. Quinlan. *Robust Data Compression of Network Packets, 2000.*

www.cs.belllabs.com/cm/cs/who/seanq/networkcomp.pdf

[10] H. Balakrishnan, S. Seshan, and R. Katz. *Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks*. ACM Wireless Networks, Dec. 1995.

About Bell Laboratories and Lucent Technologies.

Lucent Technologies' Bell Labs is a leading source of new communications technologies. It has generated more than 30,000 patents since 1925 and has played a pivotal role in inventing or perfecting key communications technologies, including transistors, digital networking and signal processing, lasers and fiber-optic communications systems, communications satellites, cellular telephony, electronic switching of calls, touch-tone dialing, and modems. Bell Labs scientists have received six Nobel Prizes in Physics, nine U.S. National Medals of Science and eight U.S. National Medals of Technology. For more information about Bell Labs, visit its web site:

www.bell-labs.com

For a Good Chuckle...

www.cnp-wireless.com/acronyms.html

… has a collection of humorous definitions for common telecom and computer acronyms.

Some of these might be construed to belittle your favorite technology, but you may send us your favorite acronym barb. You'll help us spread the light-hearted spirit of the wireless world.

Fraud and Security Patent News

US Patent: 6,681,304

Method and device for providing hidden storage in non-volatile memory

A method and device for providing hidden storage in non-volatile memory. A memory device is disclosed comprising a main flash array. A hidden storage area is connected to the main flash array. The hidden storage area can not be accessed without a valid password according to the present memory device.

Issued: January 20, 2004

Inventor: James Vogt, et al
Assignee: Intel Corporation (Santa Clara, CA)

US Patent: 6,681,243

Network environment supporting mobile agents with permissioned access to resources

A method and system for providing an environment allowing agents to function on a set of devices having resources – the environment providing services allowing agents access to those resources. Each agent has an associated permission list indicating which services the agent may access. Each agent may move from an environment on one device on a network to an environment on another device.

Issued: January 20, 2004

Inventor: David Putzolu
Assignee: Intel Corporation (Santa Clara, CA)

Notable References:

[1] Hansoty, et al. *JAVA: Secure Delegation of Mobile Applets.* IEEE Workshops, pp. 242-247, Jun. 18-20, 1997.

[2] Liotta A, et al. *Modelling Network and System Monitoring Over the Internet with Mobile Agents,* IEEE Network Operations and Management Symposium, US, New York, NY: IEEE, vol. Conf. 10, Feb. 15, 1998, pp. 303-312.

[3] Grimm, et al. *Security policies in OSI-management experiences from the DeTeBerkom project BMSec.* Computer Networks and ISDN Systems, NL, North Holland Publishing, Amsterdam. vol. 28, No. 4, Feb. 1, 1996, ISSN: 0169-7552, whole document.

US Patent: 6,681,118

Method of providing cellular and landline cordless service using a dual mode mobile telephone

A mobile station that can communicate with both a cellular network – by which it is assigned a mobile identification number – and to a cordless cellular base station utilizing the same cellular frequency range and communications protocol. The cordless cellular base station is preferably connected to a public switched telephone network and is assigned a landline number. The cordless cellular base station acts as a conduit between the mobile station and the public switched telephone network. When the mobile station comes within range of a cordless cellular base station, it deregisters automatically from the cellular network and registers with the cordless cellular base station. Once the mobile station is communicating with the cordless cellular base station, the cordless cellular base station communicates with the cellular network to instruct the cellular network to route all calls for mobile identification number to the cordless cellular base station's landline number. In addition, all calls placed on the mobile station are sent through the cordless cellular base station to the public switched telephone network. When the mobile station severs contact with the cordless cellular base station, the mobile station registers with the regional cellular base station of the regional cellular network. The cordless cellular base station then sends a network forwarding cancellation message to the cellular network to cancel the forwarding of calls for the mobile station's identification number. Once the mobile station is registered with the regional cell, calls to the mobile station's identification number are directly routed by the cellular network to the mobile station.

Issued: January 20, 2004

Inventor: Michael Raffel, et al
Assignee: AT&T Wireless Services, Inc. (Redmond, WA)

Notable References:

[1] TIA/EIA Interim Standard, *800MHz TDMA Cellular--Radio Interface--Mobile Station--Base Station Compatibility--Digital Control Channel.* Telecommunications Industry Association, TIA/EIA/IS-136.1, Dec. 1994.

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 web page. We briefly describe it and provide, at minimum, its inventor(s) and assignee (owner).

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.

[2] TIA/EIA Interim Standard, *TDMA Cellular/PCS--Radio Interface--Minimum Performance Standards for Base Stations.* Telecommunications Industry Association TIA/EIA/IS-138-A (Revision), Jul. 1996.

US Patent: 6,681,029

Decoding steganographic messages embedded in media signals

Relating to steganographic decoding. A decoder process reads a message steganographically encoded in a composite signal. One decoding process operates on a potentially modified version of the composite signal. The message is comprised of one or more symbols, each being associated with predetermined signal characteristics. The decoding process correlates these predetermined signal characteristics with the potentially modified composite signal to decode message symbols. Another decoding process analyzes a potentially modified version of the composite signal to gather evidence of signal characteristic associated with a message symbol. Based on the evidence, it determines whether the message symbol is present in the potentially modified version of the composite signal. Yet another decoding process analyzes the composite signal to gather evidence of characteristics associated with the message symbols in the message. Based on the evidence, it estimates message symbols. It compares the estimated message symbols with one or more message symbols known to be included in the message to assess whether the composite signal has a valid message.

January 20, 2004

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

Notable References:

[1] Bender, *Techniques for Data Hiding.* Massachusetts Institute of Technology, Media Laboratory, SPIE vol. 2420, 1995.

[2] Boland, et al. *Watermarking Digital Images for Copyright Protection.* Fifth International Conference on Image Processing and Its Applications, Conference Date: Jul. 4-6, 1995, Conf. Publ. No. 410, pp. 326-330.

[3] Komatsu, et al. *Authentication System Using Concealed Image in Telematics.* Memoirs of the School of Science & Engineering, Waseda Univ., No. 52, 1988, pp. 45-60.

[4] Frequently Asked Questions About Digimarc Signature Technology, Aug. 1, 1995, 9 pages,

www.digimarc.com

US Patent: 6,680,922

Method for the recognition and operation of virtual private networks (VPNs) over a wireless point to multi-point (PtMP) transmission system

Relating to a packet-centric wireless point to multi-point telecommunications system. The system includes: a wireless base station coupled to a first data network; one or more host workstations coupled to the first data network; one or more subscriber customer premise equipment (CPE) stations in wireless communication with the wireless base station over a shared wireless bandwidth using a packet-centric protocol; one or more subscriber workstations coupled to each of the subscriber CPE stations over a second network; resource allocator optimizing end-user quality of service (QoS) and allocating shared bandwidth among the subscriber CPE stations; and a scheduler to schedule an internet protocol (IP) flow over the shared wireless bandwidth. The scheduler includes a prioritizer for prioritizing the IP flow based on priorities of a virtual private network (VPN). The system can include an analyzer for analyzing the virtual private network (VPN) priorities for the IP flow, or for prioritizing all VPN IP flows. The system can include a prioritizer to prioritize the IP flow based on one or more subscriber-defined parameters. In the system, the VPN can include a directory enabled networking (DEN) table management scheme.
The VPN can be implemented using a point-to-point tunneling protocol (PPTP). Also included is a method for accomplishing the above.

Issued: January 20, 2004

Inventor: Jacob Jorgensen
Assignee: Malibu Networks, Inc. (El Dorado Hills, CA)

Notable References:

[1] Broadcom Corporation, BCM3300 Product Brief,. *BCM3300: QAMLink Single-Chip DOCSIS Cable Modem Universal Set-top Box Transmission Solution.* Dec. 2, 1999.

www.broadcom.com

[2] Kim, et al. *The AT&T Labs Broadband Fixed Wireless Field Experiment.* IEEE Communications Magazine, Oct. 1999, pp 56-62.

[3] Iera, et al. *Wireless Broadband Applications: The Teleservice Model and Adaptive QoS Provisioning.* IEEE Communications Magazine, Oct. 1999, pp. 71-75.

[4] Balakrishnan, et al. *Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks.* Computer Science Div., Dept. of Electrical Engineering and Computer Science, Univ. of California at Berkeley, Nov. 1995, pp 1-18.

portal.acm.org/
citation.cfm?id=276437&dl=ACM&coll=portal

US Patent: 6,678,822

Method and apparatus for securely transporting an information container from a trusted environment to an unrestricted environment

A method for operating a data processing system of a type that includes a first data processing entity located within a trusted environment and a second data processing entity located within an untrusted environment. The method includes a first step, executed at the first data processing entity, of operating a first software agent for detecting a presence of an information container of interest and for producing a modified information container by automatically identifying and at least one of removing, masking, or replacing at least one predetermined type of restricted or private information in the information container. A second step of the method transports the modified information container from the first data processing entity to the second data processing entity for further processing. The further processing may entail an analysis of the modified information container to locate and/or identify an undesirable software entity, such as a computer virus.

January 13, 2004

Inventor: John Morar, et al

Assignee: International Business Machines Corporation (Armonk, NY)

US Patent: 6,678,733

Method and system for authorizing and authenticating users

Authentication to a walled garden. The walled garden contains links to one or more servers providing network-based services. A walled garden proxy server (WGPS) controls access to the walled garden. When a user of a client wishes to access a service in the walled garden, the client sends a request to the WGPS including a plot number identifying the service and a ticket granting the client access to the service. The WGPS denies access to clients lacking a ticket or presenting invalid tickets. In response, the client contacts a gateway server (GS) having a database of users and associated access rights. The user presents authentication information to the GS. If the user positively authenticates, the GS generates a ticket containing a Box ID from the client, an expiration date, and a set of bits representing the access rights of the user. The GS encrypts the ticket and gives it to the client. When the WGPS receives a request to access a service in the walled garden, it decrypts the ticket and uses the plot number as an index into the set of bits representing the user access rights. The indexed value indicates whether the WGPS allows the client to access the service. Accordingly, services provided by the walled garden can be sold individually or in tiers.

Issued: January 13, 2004

Inventor: Ralph Brown, et al

Assignee: At Home Corporation (Redwood City, CA)

US Patent: 6,678,707

Generation of cryptographically strong random numbers using MISRs

Random number generation by periodically issuing an operating system call to retrieve values from a number of multiple input shift registers (MISRs) which are coupled to a number of microprocessor buses. The number of MISR readings are then stored in a temporary location, or a number of values based on the MISR readings are stored in a temporary location. A random number is then generated from the stored MISR readings or stored values.

Issued: January 13, 2004

Inventor: Richard Butler

Assignee: Hewlett-Packard Development Company, L.P. (Houston, TX)

US Patent: 6,677,852

System and method for automatically controlling or configuring a device, such as an RFID reader

A system and method for automatically controlling or configuring, a device, such as an RFID Reader. The reader reads a master control tag to upload sets of instructions from the tag to memory resident in the reader. Thereafter, the reader may read a control tag to select one or more sets of instructions stored in memory. The reader may thus be readily programmed without the need for physically connecting the reader to a computer, and without employing expensive key pads and display screens.

January 13, 2004

Inventor: Jeremy Landt

Assignee: Intermec IP Corp. (Beverly Hills, CA)

US Patent: 6,671,804

Method and apparatus for supporting authorities in a public key infrastructure

A system and method for supporting authentication services in a cryptographic device storing a number of templates. The cryptographic device receives inputs representing a request for authentication services. The cryptographic device then compares the syntax of the input to the syntactic constraints defined in one of the templates, where each template includes syntactic constraints associated with at least one authority. When the cryptographic device determines that the syntax of the input is consistent with the template, the cryptographic device validates the input.

December 30, 2003

Inventor: Stephen Kent

Assignee: BBNT Solutions LLC (Cambridge, MA)

Notable References:

[1] *ITU-T Recommendation X.509*, International Telecommunications Union, Aug. 1997.

[2] *S/MIME Version 3 Certificate Handling*. Network Working Group, RFC 2632, The Internet Society, Jun. 1999, pp. 1-10.

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