Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 5, No. 2. February, 2003

Don't Miss IETF Meeting #56

The 56th meeting of the Internet Engineering Task Force (IETF) is planned for March 16 – 21, 2003 in San Francisco, CA. For those who wish to be a part of networking standardization, this is a meeting you should plan to attend; it is loaded with an agenda of wide-ranging topics, as shown at:

www.ietf.org/meetings/agenda_56.html

In the News: National Cybersecurity

In our **September issue** of *Wireless Security Perspectives*, one of our topics was *The Draft Strategy to Secure Cyberspace*. On February 14th, 2003, President Bush released the final draft, *The National Strategy to Secure Cyberspace*. The document is available at the Department of Homeland Security (DHS) website:

www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf

The content of this document provides a comprehensive overview of methods to improving cybersecurity. It is consistent with the Canadian government's approach to cybersecurity.

In its 68 pages, the document makes a wide variety of recommendations. All of them seem to lead toward the idea of a partnership between government and private industry. The partnership idea, woven throughout the entire Strategy, includes various approaches for reaching out to all types of entities – except, of course, the criminal types. It mentions a "culture of security," which involves cooperative strategies used in public and private IT systems for development, training, implementation and review.

Sample Cybersecurity Recommendations

Some actions related to the Strategy's recommendations listed below will bring changes to wireless networks:

- *Vigilant Network*. The Strategy supports a "watch and warn network" and an out-of-band early-warning communications network that spans the public and private sectors. National and international connectivity in these networks would enable wide-spread capabilities for discussing Internet threats and attacks, for distributing analysis and warning information, and for managing crises. Inclusion of United States allies would, of course, require cross-compatibility with systems among these foreign allies.
- *Privacy*. The Strategy upholds the idea of maintaining personal privacy while at the same time improving security by using better policies and practices in cyber-attack detection and management (Guiding Principle #2 and in the Priority I section).
- *Market driven*. The Strategy calls for market impetus, rather than government regulation, as the best driving force for improving national cybersecurity. This point is intended to minimize the frustrating effects of low-cost, bare-minimum solutions, which are a common occurrence in regulated industries.

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…

March 18th, 2003.

Future Topics

Wireless Security for the Enterprise • Wireless Flash Memory Security • Radius for Wireless • 3G Security • Public Keys & Wireless • Security for Mesh Networks • 802.11 Wireless LAN "Hotspot" Roaming Security • Security Issues in Ad hoc Wireless 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.

- *Prosecution of crime*. The document clearly recommends prosecution of cyber criminals. It does not, however, introduce proposals for adding new criminal code.
- *Internet changes*. To the extent legally possible, back-bone Internet providers would be given power to obtain information needed to analyze the health of the network.

  The Strategy also recommends adoption of IPv6, since its improved security includes native IPsec. This is no surprise, seeing it is being given serious consideration in many other regions (e.g., Europe, Japan, and China).

  Further, it recommends greater Internet security through more robust BGP and DNS protocols, and that Internet Routers should filter out forged source addresses to help reduce DoS attacks.
- *Certification*. The Strategy calls for a broadly accepted certification program for maintaining a pool of well-trained cybersecurity professionals.
- *Security standards*. Stronger security standards are favored in the Strategy, including development and adoption of internationally shared standards. The DHS plans to promote voluntary standards efforts in the private sector.
- *WLAN Security*. Federal agencies would procure leading-technology WLAN products to stimulate market demand.
- *Review of Developing Technologies*. The Strategy recommends the National Science and Technology Council would review developing technologies (wireless being one of them) in the context of possible homeland and cyberspace security implications.

In its conclusion, the Strategy states: "The federal government will employ performance measures – and encourage the same for state and local governments – to evaluate the effectiveness of the cybersecurity programs outlined in this Strategy."

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.

IACON 2003 – The 12th Congress
5th – 6th March 2003
Hilton London Paddington
London, UK
www.iir-conferences.com

SANS National Information Assurance Conference (NIAL) 2003
5th – 12th March 2003
Sheraton San Diego Hotel and Marina
San Diego, CA
www.sans.org/SANS2003/nial.php

802.11 Planet Conference & Expo – Japan 2003
14th March 2003
Shibuya Markcity
Tokyo, Japan
www.jupiterevents.com/80211/tokyo03/index.html

56th IETF Meeting
16th – 21st March 2003
Hilton San Fransisco
San Fransisco, CA
http://www.ietf.org

IEEE Wireless Communications and Networking Conference (WCNC)
16th – 20th March 2003
Ernest N. Morial Convention Center
New Orleans, LA
www.wcnc.org

[Note: This conference is co-located with CTIA Wireless 2003]

CTIA Wireless 2003
17th – 19th March 2003
Ernest N. Morial Convention Center
New Orleans, LA
www.wireless2003.com

[Note: This conference is co-located with IEEE WCNC]

2003 IEEE International Workshop on Information Assurance
24th March 2003
Fraunhofer - IGD
Darmstadt, Germany
www.ieee-tfia.org/iwia2003

Workshop on Privacy Enhancing Technologies
26th – 28th March 2003
Hotel Elbflorenz
Dresden, Germany
petworkshop.org

8th International Conference on Intelligence in next generation Networks (ICIN)
31st March – 3rd April 2003
Cite Mondiale
Bordeaux, France
www.adera.fr/icin2003/montage/programme/page-1.htm

First International Conference on Security in Pervasive Computing
12th – 14th March 2003
Boppard, Germany
www.dfki.de/SPC2003

Enterprise Architectures Conference
18th – 20th March 2003
Crowe Plaza
New York, NY
www.dci.com/brochure/eacny

InternetWorld Essentials
14th – 17th April 2003
San Jose Convention Center)
San Jose, CA
www.internetworld.com/events/spring2003

New yard-sticks may appear in the coming months or years, if the DHS determines, in its ever-deepening quest for more effective cyberdefense, that the current set of performance measures is lacking.

The Strategy is a starting point. Its lack of detail provides little, if any, useful information to potential cyber-attackers. Further details, then, would require individuals or organizations to inquire at a lead agency (as listed in the Strategy) or at a team organized under one of these agencies. It is not clear whether the US government has the capacity to provide this information, nor how it will verify that those asking for the information are trying to strengthen cyberdefenses and are not covertly looking for cracks.

CALEA Packet Data Intercept for CDMA Packet Data Networks

Mike Borella

The Communications Assistance for Law Enforcement Act (CALEA) of 1994 mandates that telecommunications systems provide legally authorized intercept capabilities to law-enforcement agencies (LEAs). Compliance with CALEA – and with other laws requiring intercept of packet-data traffic – poses a challenge to service providers and equipment manufacturers.

Third generation (3G) wireless networks offer high-speed network access to cell phones, Personal Digital Assistants (PDA) and laptops. Currently, there are two main variations of 3G: CDMA2000 and UMTS. These systems differ mainly in their access technologies and in their relationships with legacy 2G and 2.5G systems. Although UMTS can be deployed throughout most of the world, and the first system deployed was in Japan, Europe currently is the geographic area with the most UMTS networks deployed or under construction. CDMA2000 is currently deployed in Canada, China, India, Japan, Korea, South America and the United States, as well as several Eastern European countries.

Since CALEA applies only to the United States, the focus of this article will be CDMA2000, the principal 3G technology used in this country.

Current CDMA2000 deployments mostly use the 1xRTT variant, which allows up to 144 Kbps both upstream and downstream, although most CDMA2000 service providers plan to eventually upgrade their systems to 1xEVDO (up to 2.4 Mbps downstream, 144 Kbps upstream) or 1xEVDV (several Mbps upstream and downstream).

The Communications Assistance for Law Enforcement Act (CALEA) of 1994 mandates that telecommunications service providers must be able to respond to a court order for electronic surveillance on a particular user. The court order typically is obtained and delivered by a law enforcement agency, such as the FBI or a local police department. Once the order is served, the service provider determines the appropriate subject, as well as the start time and stop time for the surveillance. The order will indicate whether just Call Identifying Information (CII) or both CII and Communications Content (CC) must be provided to law enforcement.

- CII includes start and stop times for calls and each session's called and calling party information.
- CC includes the actual content of the communications session, such as the voice.

The service provider also must either be able to undo any transforms – such as encryption or stateful compression – that it applies to the user's data – or give the LEA sufficient information with which the LEA can undo them. However, the service provider is not responsible for undoing any user-performed transforms, such as Virtual Private Networks (VPNs).

Surveillance tasks must be accomplished in a way that is unobtrusive to the subject and to other customers using the same facilities. For example, the setup latency of a call under surveillance should not be noticeably different from that of a normal call, and it should not noticeably impact calls that are already in progress for other people.

CALEA law and technical specifications were initially written for circuit mode communications, and in particular, voice communications. Given the ubiquity of the Internet, packet-mode CALEA capabilities are now required.

Currently, the method for applying CALEA to packet data is unclear, due to technology limitations and concerns over costs to the parties involved.

The CDMA2000 Network Architecture

The CDMA2000 network architecture for packet data communications is shown in **Figure 1**. Mobile devices connect through a carrier's Radio Access Network (RAN) to a Packet Data Serving Node (PDSN) in the Visited Network. The mobile user session is encapsulated in the Point-to-Point Protocol (PPP) and then tunneled over the A10/A11 interface, which uses Generic Routing Encapsulation (GRE).

There are two types of data calls: Simple IP and Mobile IP.

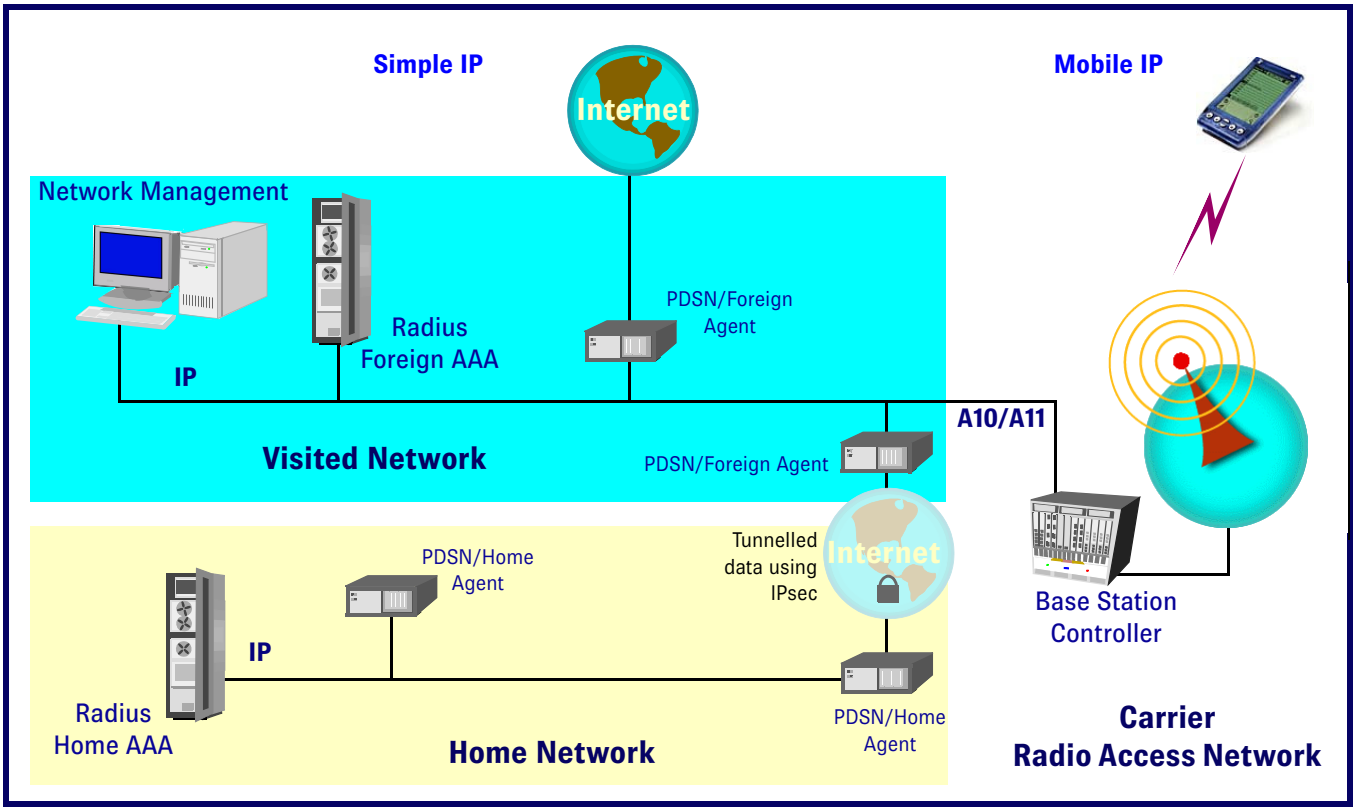
Simple IP calls provide basic IP network access, with the Visited Network assigning an IP address to the mobile. If a mobile using Simple IP roams to a new RAN, it is likely to be assigned to a different PDSN, and therefore it will receive a new IP address. This will interrupt any data transfer in progress.

Under Mobile IP, the Home Network assigns an IP address, which the mobile keeps as it roams across PDSNs. A Mobile IP call will maintain application state and data transfer between hand-offs, enhancing the overall user experience. Mobile IP calls are tunneled between the PDSN and the Home Agent using IP-in-IP, GRE or IPsec.

Both types of calls are authenticated by the Authentication, Authorization And Accounting (AAA) infrastructure, which consists of a Foreign AAA (FAAA) server and a Home AAA (HAAA) server. The user's profile and associated information resides in the HAAA, so the FAAA acts as a proxy for requests and responses between the PDSN and HAAA. The Home Agent (HA) may also communicate with the HAAA directly, for a further round of authentication, if necessary, or to acquire an IP address for the mobile.

Although **Figure 1** shows the general architecture of CDMA2000, every service provider has their own unique architecture based on their technical and business requirements. Some networks are Simple IP only, while others support both Simple IP and Mobile IP. Some network architectures are centralized, with PDSNs and HAs co-located in one or more points of presence, while others employ a distributed architecture.

Figure 1: The CDMA2000 Network Architecture



CALEA Support in CDMA2000

The features and functionality of CALEA, as it applies to CDMA2000, have not been fully specified at the time of this writing. The joint TIA/ATIS standard J-STD-025 currently supports circuit-switched intercepts, and it is being upgraded to support packet-data intercepts.

However, the first step in adapting a network architecture to support CALEA is to identify the Intercept Access Points (IAPs). These are the components in a network where CALEA intercept occurs. In a CDMA2000 network, the IAPs may include:

- *The Packet Data Serving Node (PDSN).* Both Simple IP and Mobile IP calls traverse the PDSN. User data may be compressed over the PPP link from the PDSN to the mobile and over a Mobile IP tunnel to the HA, so the PDSN may be the only component in the network with the ability to read a user's information unobstructed (i.e., in the clear). If the court order encompasses the Visited Network, the PDSN must be equipped with the ability to intercept user data.
- *The Home Agent (HA).* For Mobile IP calls, the HA will have access to user data in the clear. While the intercept function could, in principle, be implemented by a passive data monitor, or sniffer, on the Internet side of the HA, this solution may not be practical for two reasons:
  a. Service providers may not want the overhead of provisioning, operating and managing an additional component in their network.
  b. The service provider may be supplying an additional VPN from the HA to another network, such as an enterprise network. In the latter case, the sniffer would be unable to read user data encrypted by the VPNs in to and out of the HA.
- *The Home Authentication, Authorization and Accounting server (HAAA).* For Simple IP calls where the intercept subject is roaming in another service provider's network, but there is a court order in the Home Network, the HAAA will be the only component of the Home Network that has knowledge of the user's calls and call attempts. As in the case of the HA, a passive sniffer solution may not be sufficient because RADIUS packets may be encrypted between the Visited Network and HAAA server.

In addition to these IAPs, there may be a requirement in some networks for intercepting AAA traffic on the FAAA server as well.

IAPs establish signaling and, in some cases, management relationships with a Delivery Function (DF). The DF receives and converts and reformats raw intercept data.to an acceptable standard set by the receiving LEA.

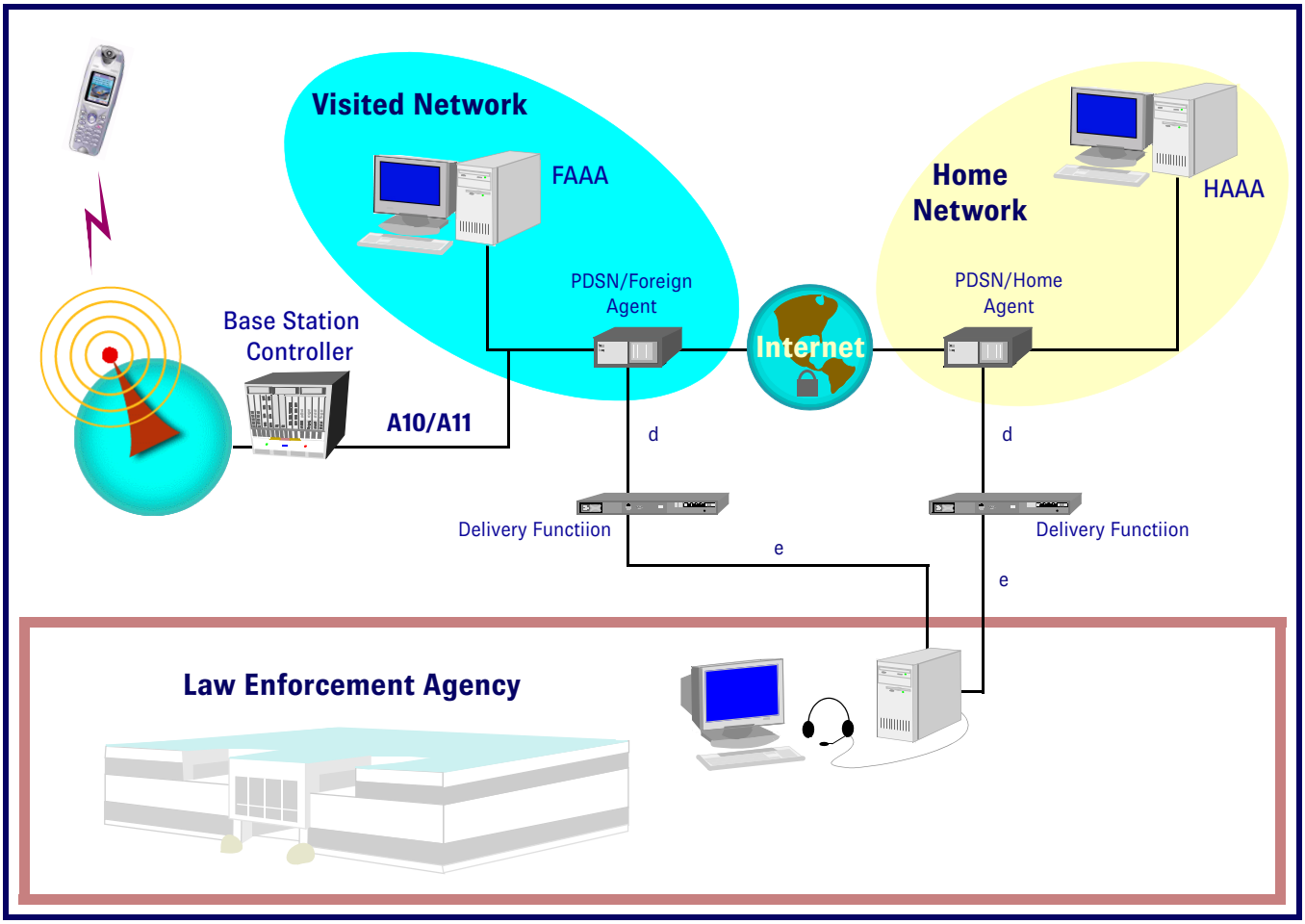
The interface between the IAP and DF is the J-STD-025 "d" interface, and the interface between the DF and the LEA is the "e" interface. The "d" interface is optional because the equipment manufacturer may integrate DF

Huh?

If there are any acronyms or terms you are unfamiliar with, check our website glossary. You will probably find them there.

www.cnp-wireless.com/glossary.html

Figure 2: CALEA Architecture for CDMA2000 (Mobile IP)



"e" interface must conform to J-STD-025 Revision B, which is still being developed.

Figure 2 shows a generic CDMA2000 architecture modified to include components for packet-mode CALEA.

Packet Mode CALEA

Defining CALEA capabilities for packet-mode data is inherently difficult. The act only applies to "telecommunications services" and not "information services." However, the distinction between the two is not clear in the context of packet data. For example, Web browsing may be considered an information service, while voice over IP (VoIP) is likely to be considered a telecommunications service. Likewise, half-duplex voice services such as push-to-talk (a CDMA service similar to that of Nextel's Direct Connect) are likely to be considered telecommunications while their text-based analogue services – instant messaging – could go either way. More advanced services are likely to integrate voice and data, making the distinction even more difficult.

Deceiving the IAP

Distinguishing telecommunications traffic from non-telecommunications traffic creates a significant problem, regardless of how the traffic is defined. A clever opponent will be able to develop or use existing software to hide communications sessions from CALEA intercepts. For example, if CALEA is interpreted to only apply to a telecommunications service, such as VoIP, then the IAPs must be able to determine, in real time, which packets to intercept. However, most VoIP systems use establishment and control protocols such as Session Initiation Protocol (SIP) and H.323 and a separate bearer plane protocol, such as Routing Table Protocol (RTP). While the IAP can monitor the SIP or H.323 flow for the information necessary to identify the RTP flow, the opponent may be able to establish the RTP flow via some other signaling mechanism, or they may "juggle" the identifying information such that the IAP will not be able to reliably identify the flow of packets in the voice session. Thus, the multi-application nature of IP networks makes it difficult to identify instances of a particular application, because the endpoints can conspire to deceive a passive listener.

The industry consensus seems to be that all packet-mode communications may be subject to CALEA, pending further clarification by the courts. Furthermore, recent laws passed in the United States, such as the Patriot Act, broaden the government's wiretapping powers, and these may not distinguish between telecommunications and information services.

Definition Problems

Regardless of how this debate plays out, another significant hurdle needs to be overcome – there is no accepted definition of Call Identifying Information (CII) for packet data. CII has been interpreted to refer to packet headers,

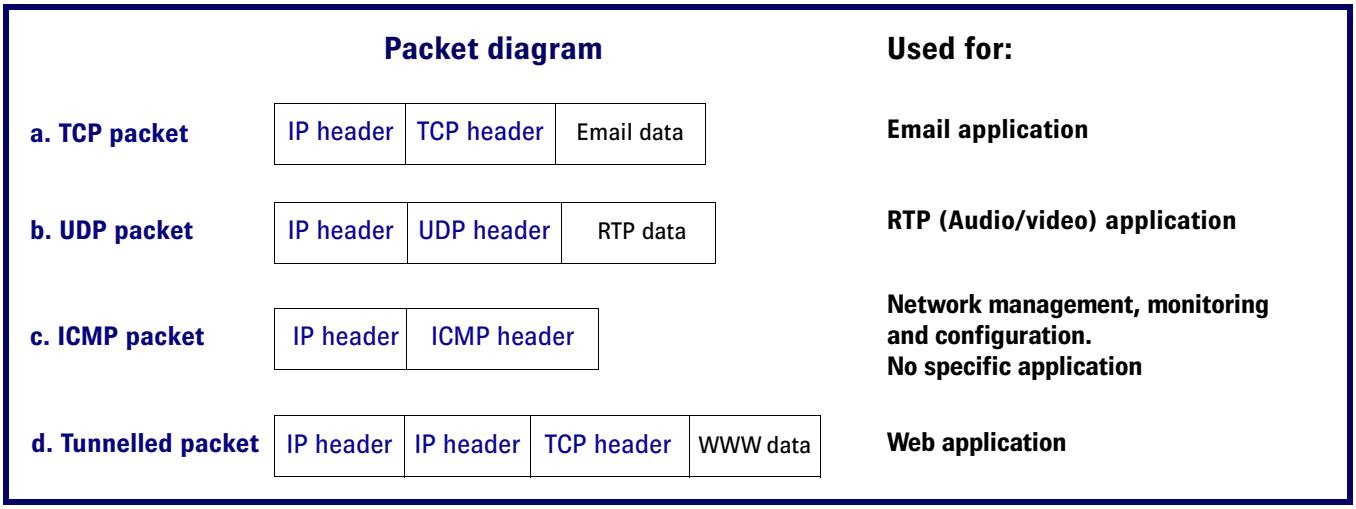
but IP protocols can tunnel communications sessions within other communications sessions. Because of this, the exact number and type of headers present in IP packets can vary.

Not all IAPs may be capable of doing extra processing for each packet of a call under surveillance, without breaking the rule that surveillance must be unobtrusive. However, not doing some processing beyond the basic IP/UDP or IP/TCP headers may result in the loss of important information, such as the IP addresses of the sender and recipient of the data.

Figure 3 illustrates this point with four example packets, representing:

a. IP/TCP encapsulation,
b. IP/UDP encapsulation,
c. IP/ICMP encapsulation and,
d. IP/IP/TCP encapsulation.

Figure 3: Example Packet Headers and Encapsulations



If a CALEA-compliant IAP is required to parse these packets for CII, then the implementation must first analyze the IP header and determine, from the next protocol field, what the next header is. If the next header is TCP or UDP, that header can be processed and its port numbers read. It is possible to determine the application by reading the port numbers, since many applications use well-known ports. However, this is subject to deception. If the packet is IP encapsulated in IP, then the processing of the inner IP header must occur before the processing of the TCP or UDP header.

Each additional layer requires additional processing on the part of the IAP, although the overhead is limited because, in practice, it is rare to see encapsulations more than three IP headers deep.

A simplistic approach that may satisfy LEAs in the short term can be called "IP+8." In this scheme for reporting CII, the entire outer IP header and the first 8 bytes of the next header, are intercepted and sent to the LEA. Because the TCP and UDP ports reside in the first 8 bytes after the IP header, this method would work unless there is another IP header or an Internet Control Message Protocol (ICMP), IPsec or GRE header after the outermost IP header.

High performance hardware platforms, such as those enabled with network processors or hardware-based classification engines, will be able to perform this extra processing at gigabit or higher speeds. However, today's networks consist of many legacy network components built on relatively cheap, low-end, and – in many cases – obsolete general-purpose processors. These devices may struggle to perform CII on a number of calls while still maintaining their normal workload of non-intercepted calls.

No Parsing Keeps it Simple

Although providing CII continues to be a challenge – mainly because the definition of CII is quite vague – providing CII and CC together is simple. In this case, the IAP copies the entire packet to the LEA. The operation is fast on many of today's platforms. It should not be obtrusive unless the ratio of CALEA calls to total call capacity is quite high. Unfortunately, this does not help a great deal, as the majority of intercepts only ask for CII.

Non-Technical Roadblocks

In addition to these technical questions needing answers before CALEA can be deployed unambiguously, there are significant non-technical issues currently holding up the specification and deployment of packet-data legal intercept.

One issue is purely financial. Service providers do not have faith that the LEAs will reimburse them to cover their legal-intercept-related costs. Service providers need to upgrade existing equipment, purchase new components, backhaul intercepted traffic and train employees to perform CALEA requests. Congress allocated funds to cover the initial upgrade of circuit equipment to support CALEA, but these are long gone. The current heightened level of legal intercept activity is eating into the already low margins of struggling telecommunications providers.

Although part of the cost stays with the service provider, some of the cost is passed on to the packet-data-equipment provider, which now has to develop and test a CALEA solution. Due to the lack of standards, the equipment provider may have to develop several variations of

their CALEA solutions, each fine-tuned to the needs of and interfaces employed by their customers.

Finally, but perhaps most importantly, service providers are concerned that the end users of telecommunications services may have privacy concerns with respect to legal intercept. With wireless voice and data providers already fighting each other for shares of a mature market, none of them want to be the first to implement CALEA, because by doing so, they run the risk of alienating their customers.

Conclusion

Given the current political landscape, it seems inevitable that CALEA, and perhaps other forms of legal interception, will be mandated for CDMA2000 3G packet-data services. It is currently unclear when this functionality will be available in commercial networks. Unless there is a carrot, such as sufficient funds to cover the costs of deployment, or unless the FCC produces a stick, such as a mandate setting a firm implementation date, the rollout of CALEA will continue to move at a snail's pace.

*This article complements a previous article – published in our **January issue** of Wireless Security Perspectives – about CALEA's legal aspects.*

About the Author

Michael Borella works in the Wireless Solutions Business Unit of CommWorks. He is the manager of the Advanced Technologies group and lead system architect of the product line. His responsibilities include product and feature definition, standards, new technologies, and intellectual property. He has published numerous technical articles, and he holds over 20 patents in telecommunications and Internet-related fields. He received the Ph.D. degree from the University of California, Davis, in 1995.

mike_borella@commworks.com

CommWorks (commworks.com) provides a number of products for IP telephony, including protocol interworking, AAA, VoIP and Mobile IP. They are a 3Com company.

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). All of these patents were granted in January of 2003.

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: 6,523,116

Secure personal information card database system

A database system for personal information, used for storing personal information in a database remote from the person using the public key of a person as a record identifier. The person's public key is published on a card, which may be a physical card or a virtual card, published on an Internet site in unencrypted form, together with unencrypted demographic information of the user. The person's public key is a unique identifier which becomes the person's record identifier, as well as possibly a social security number, medical record number, tax identification number, insurance file number, etc. The card contains the person's public key in eye-readable format and in machine-readable format, such as bar-coded format. It can be used to gain access to personal information in the database. In an alternate embodiment, the personal information may additionally be encrypted with the public key of a target agency, such as an insurance company or a bank. The target agency for the personal information obtains the card and gains access to the information by scanning the bar code and by using the acquired public key of the person, plus its own private key, to decrypt the information.

Issued: February 18, 2003

Inventor: Phillip Berman
Assignee: **Eastman Kodak Company** (Rochester, NY)

US Patent: 6,523,013

Method and apparatus for performing automated fraud reporting

A meter and/or base (or computer), coupled to one or more modems, performs automated fraud reporting to a service center, upon detection of particular ones of detectable faults. Diagnostic software and/or tamper detection devices test the meter to ensure the meter operates in an expected manner. A detected fault can be classified into one or more categories or levels. For faults within certain levels, an alarm message is sent to the service center. Corrective action can be performed in accordance with a response from the service center. For major faults, the meter can be disabled until service is performed and the alarm message can be sent to the postal inspectors.

Issued: .February 18, 2003

Inventors: Chandrakant Shah and David Coolidge
Assignee: **Neopost, Inc.** (Hayward, CA)

US Patent: 6,522,874

User key validation to prevent fraud during system handoffs

A user key validation during a hand-off verifies the subscriber using the wireless communication system and prevents fraudulent use of the system. A wireless communication system has a number of satellites with which a subscriber unit establishes a communication link. However, as the quality of the transmitted signal between an active satellite and the subscriber unit degrades, a handoff of the communication link with the subscriber unit will occur if the

subscriber meets the authentication requirements of the system. The active satellite generates user keys and transmits the user keys to the active subscriber units. A request of a handoff is made from the individual subscriber unit (ISU) to the losing SV. The losing SV communicates with the gaining SV to establish a handoff. The losing SV sends the user key of the ISU to the gaining SV. The gaining SV authenticates the ISU by comparing the ISU user key to a user key stored in the losing SV. The gaining SV becomes the active satellite, and it generates and transmits the user key to the ISU. Notification of the authentication is sent to an earth terminal controller. The earth terminal controller provides the losing SV with notification that the handoff is complete. The authentication prevents further fraud if the subscriber fraudulently obtained access to the system during the original call set up.

Issued: February 18, 2003

Inventor: Thomas Chu and Darryl Sale
Assignee: **Motorola, Inc.** (Schaumburg, IL)

US Patent: 6,522,769

Reconfiguring a watermark detector

Methods, devices and systems for reconfiguring a watermark detector. In many applications, it is useful to be able to change the operation of a watermark detector. Such changes may include changing how the watermark detector decodes or interprets a watermark embedded in a signal of a given media type, such as audio, video or still images.

Issued: February 18, 2003

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

US Patent: 6,519,331

Telecommunications system, service control point and method for pre-screening telephone calls to help prevent telephone toll fraud

The telecommunications system includes a service control point capable of receiving information about a telephone call originated by a calling party, and further, it is capable of determining whether the telephone call has a fraudulent attribute. If the telephone call has a fraudulent attribute, then the calling party is informed that there is a possibility of telephone toll fraud occurring if the telephone call is connected to a called party. And, if the telephone call does not have a fraudulent attribute, then the telephone call is automatically connected to the called party.

Issued: February 14, 2003

Inventors: Gilman Stevens and Babu Mani
Assignee: **Alcatel** (Paris, FR)

US Patent: 6,516,414

Secure communication over a link

A method and apparatus of protecting communications in a receiver having a first and a second module, which includes issuing a request to a transmitter. The identities of the first and second modules are verified based on information in the request. The transmitter transmits a predetermined message to the receiver after verification. The first and second devices are authenticated based on the predetermined message.

Issued: February 4, 2003

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

Interesting references:

[1] Digital Video Broadcasting, *DVB Shows Conditional Access Common Sense*, pp. 1, printed from web site:
www.dvb.org/dvb_news/dvb_pr025.htm
dated at least as early as Dec. 30, 1998.

[2] Electronic Privacy Information Center, *Digital Signatures*, pp. 1-2, printed from web site:
www.epic.org/crypto/dss
dated as early as Jan. 14, 1999.

[3] Electronic Privacy Information Center, *CSL Bulletin*, pp. 1-6, printed from web site (Jan. 1993):
www.epic.org/crypto/dss/nist_dss_bulletin.html

US Patent: 6,510,515

Broadcast service access control.

Techniques and systems for controlling access to information broadcast over point-to-multipoint resources in radiocommunication systems. These techniques can be used to provide controllable access to broadcast information services, e.g., security quote services, sports information services, etc., which broadcast services can be provided in conjunction with more conventional cellular radiocommunication services, e.g., voice calls. Exemplary embodiments of the present invention enable subscribing users' equipment to output broadcast information using, for example, either a status variable within the remote equipment or encryption for which subscribing devices have a corresponding decryption key.

Issued: January 21, 2003

Inventor: Alex Krister Raith
Assignee: **Telefonaktlebolaget LM Ericsson** (Stockholm, SE)

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