Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 6, No. 5. May, 2004

When Keyboards Talk

What does your keyboard say about you? A lot, it turns out. Two IBM researchers have figured out a way to re-create text based on the sounds that a keyboard makes during typing.

Collecting information based on spurious emissions is nothing new. One of the most straightforward and best-known approaches is recording the sounds made when numbers are entered on a phone or lock keypad, and then entering them later. Other approaches are more sophisticated. For example, one new type of side-channel' attack (described in report #577 by Marcus G. Kuhn) consists of tracking the high-frequency variations in light emitted from computer displays in order to reconstruct the on-screen text. Another type – described by RSA co-inventor Adi Shamir – listens to sounds produced by a computer's CPU to extract secret keys.

The latest twist exploits sounds produced by keyboards and keypads, including those on laptop and desktop PCs, ATMs and phones. IBM researchers Rakesh Agrawal and Dmitri Asonov documented (in their report: *Acoustic Keyboard Emulations)* that, although key clicks sound alike to the human ear, there is enough subtle variation for a computer to distinguish one from another. Their system has two primary parts: a basic PC microphone or, for long-range eavesdropping, a parabolic mike; and a neural network simulator, which was trained to differentiate sounds.

The system centers around sound variations based on a key's location on the keyboard. "Different parts of the keyboard plate produce different sounds when the nearby key is pushed," Agrawal and Asonov concluded in their paper, presented at the IEEE Symposium of Security and Privacy in early May. "By analogy with a drum, striking a key at different locations on the plastic plate provides different timbres."

In its current form, the system is not perfect, but it is close enough, with an average of only one incorrect recognition for every 40 keystrokes on a PC keyboard. The technique is robust enough to accommodate variations in typing styles – even one-finger hunting and pecking – and background noise. In one experiment, the system worked even when a parabolic mike was aimed at a user 15 meters away, typing in a noisy cubicle.

In the case of telephone keypads, the system was slightly less robust, but still effective. For example, recognition varied among phone models, but it was still possible to train the system with one phone and then use it to

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…

June 24th, 2004.

Future Topics

Light-weight Security Protocols • Security for UWB • MANET Security • Radius for Wireless • Handheld Device Security • 4G Security • Zigbee Security • PKE-enabled Wireless

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published **11** times a year 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.

eavesdrop on a different model. One way to avoid this problem would be to use a virtual keyboard, such as the one produced by Canesta.

The virtual keyboard projects an image onto a surface (e.g., a tabletop). Another counter-measure, useful for a PC keyboard, is a rubber protector such as the type used to catch spilled coffee. The catch is that both are an added expense and less comfortable for extended use.

US Law Enforcement Petitions for More Eavesdropping

On March 10th the US Department of Justice (DoJ), FBI and Drug Enforcement Agency (DEA), on behalf of US law enforcement, petitioned the FCC for an "expedited rule-making" to clarify (i.e. expand) the jurisdiction of CALEA lawfully authorized electronic surveillance (LAES) over packet data (especially wireless packet data) and broadband access and telephony, including Voice over IP (VoIP) and Push-to-Talk (PTT/PoC).

Background on Surveillance

Law enforcement and judicial approaches to surveillance of communications date back to when the postal system was the most important form of communication and letters the major target of interception.

Information was divided into *Identifying Information* and Content. Everything on the envelope – the destination, the return address (if present) and the cancellation stamp, containing the name of the post office and the time of processing – was *Identifying Information* and everything within the envelope was Content. There was (and still is) a higher level of justification required before a judge authorizes access to *Content* than to *Identifying Information.*

Phone calls follow the model established by surveillance of mail. Call Identifying Information includes the dialed digits (destination), the calling party number (return address) and the time and duration of the call. *Call Content* is the voice or other user traffic. Access to content requires a *Title III* court order based on the strict requirements of Title III of the 1968 "Omnibus Safe Streets and Crime Control Act".

CALEA (Communications Assistance for Law Enforcement Agencies) is a law established by the US Congress in October, 1994 "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for Law Enforcement purposes." This was in response to the increasing difficulty of law enforcement performing surveillance on digital facilities and wireless systems.

CALEA specifically exempted *Information Services* such as email and instant messaging from the scope of the law. However, this does not mean that these services are untappable; this just needs to be done with different legal means, and without CALEA technology.

Are You the Arcanist?

The series given last month was: 58, 108, 145, 228, 778, 1426, ...?

The distances of the planets from the sun (in millions of kilometers, rounded off to the nearest million) are: Mercury – 58; Venus – 108; Earth – 145; Mars – 228; Jupiter – 778; Saturn – 1426; Uranus – 2867; Neptune – 4490; and Pluto – 5910 km.

The interesting thing about this is that the distances almost appear to be a mathematical series of doublings, and there has been a great deal of speculation over whether this is just a coincidence, particularly whether the asteroids in the big gap between Mars and Jupiter represent a planet that either exploded or never quite formed properly. Imagine if the Earth was at about 200 million km and Mars at about 400. Then the series would be nearly perfect (with the exception of Pluto, which many people do not consider to be a fully fledged member of the planetary club).

The question for this month:
Given: [616, 150, 634]; [600, 250, X]. What is "X"?

Submit your answer to wsp@cnp-wireless.com

Instead of having intercepted data transmitted to a central law enforcement monitoring point, special equipment (such as the FBI's *Carnivore*) might need to be located on the information service provider's premises, making the interception more time consuming and expensive…but still possible.

Even with traditional phone calls there are a number of grey areas and a greater number with wireless. More sophisticated telephony systems have more signaling, and it is not as tightly coupled with the facility carrying the call.

One example that occurred during the development of CALEA standards was the debate over whether DTMF tones dialed during a call were identifying information or content. Law Enforcement said that they were only call identifying information even though they are often transparent to the carrier and are clearly not always call identifying information. They can be used to set up calls (e.g. via a long distance carrier) but also to do many other things, such as access an answering machine or banking services.

Similarly, Short Message Service (SMS) may be carried over the SS7 signaling channel that mostly conveys information that clearly is used to identify calls, yet SMS is usually treated as an information service.

The Internet Revolution

The revolutionary aspect of the Internet is that it is a new form of global communications. Probably only the development of postal services and telephone networks have had a similar impact.

Like any new technology, the Internet can be analogized to older technologies, albeit imperfectly. The separation of Identifying Information from *Content* which was blurred by telephone systems has become almost invisible with the packet-oriented Internet.

It is true that every packet on the Internet has some identifying information and some content, but this is not a very useful distinction for a number of reasons:

- Protocol layering has been taken to new levels. The content portion of one layer may contain packets of a higher layer which are divisible into identifying information and content, or it may contain a higher layer which has information and content distributed over many packets at the lower layer.
- Identifying information that is easiest to obtain may be of the least value. The IP addresses at the IP layer may be dynamic, making it difficult to identify the parties communicating at any point in time.
- Identifying information that is most useful, such as SIP addresses, is difficult to extract except at network nodes that terminate the protocol (e.g. SIP proxies).
- Protocols may be used in parallel by one user. An Internet session may include a mixture of voice services (including VoIP) and data services. Even data services such as email and web access could include voice components.
- Wireless complicates matters even further by mixing traditional circuit-switched voice with data and even allowing simultaneous operation of circuit-switched voice calls and packet data services.

One solution provided by J-STD-025-B is for telecommunications carriers to provide all data that could possibly be related to a subject to them, and have them responsible for 'minimizing' the stream (i.e. removing all data that they do not have the legal authority to monitor). Law enforcement would prefer that this information be analyzed by service (e.g. Email, VoIP or web access). Carriers, however, see an endless task trying to incorporate and maintain software to interpret all available Internet protocols.

This illustrates one of the critical issues – How *Identifying Information* should be defined for the portions of packet data systems, like the Internet, that are covered by CALEA. Carriers generally argue that it should be just what is reasonably available, often just an IP address, though their network may be transparently passing through higher protocol layers containing more meaningful address information (such as email and website addresses).

Telecommunications carriers, for their part, are anxious to balance several competing interests: the right of law enforcement to perform surveillance; the right of their customers to privacy; and keeping the costs of support for surveillance to a manageable level.

Standards Development

The major standard to support CALEA is TIA/ATIS J-STD-025 created by a joint *ad hoc* group formed in 1995. The reference model for this standard is shown in **Figure 1**.

The first version of J-STD-025 was published without a list of eleven items (the "punch list") that law enforcement wanted but that carriers felt were beyond the scope of CALEA. Due to disputes over its status as an ANSI standard, this standard was published as a TIA interim/ATIS trial use standard in 1997, but not as an ANSI standard until much later.

The question of which of the punch list items should be included in J-STD-025 was argued within the TIA TR-45 ad hoc, during the FCC's initial rulemaking and during the appeal of that ruling to the US Court of Appeals. After the FCC's initial ruling was overturned, the FCC provided the justification requested by the court and in its second decision ruled that 6 of the 9 punch list items (2 were withdrawn voluntarily) should be supported, and these were included in J-STD-025-A, published in April 2003.

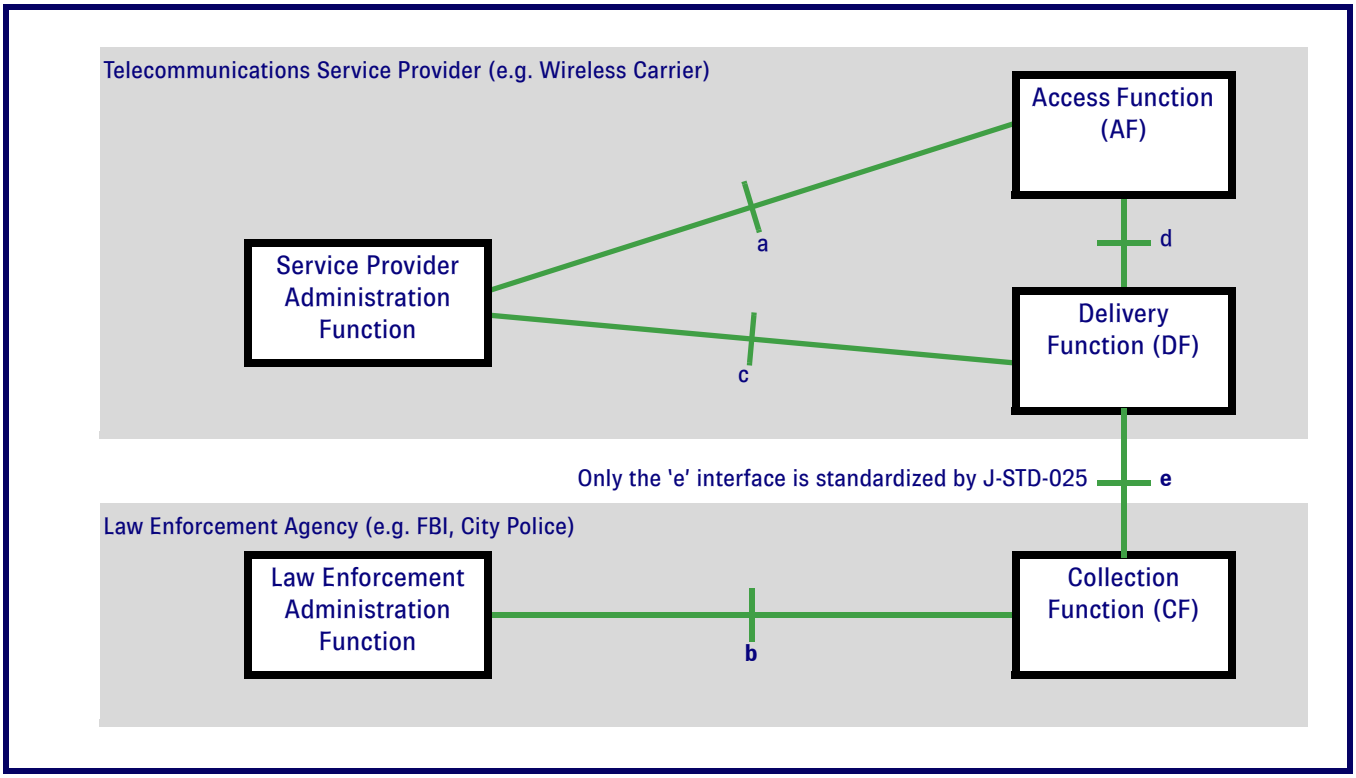
Just before J-STD-025-A was published the FBI announced that they would no longer participate in the *ad hoc*. Among other things, they objected to the consideration of regulatory and legal issues by an engineering committee. Their petition states, for example, that "the packet-mode standards that have been published [e.g. J-STD-025-B] are deficient". The TIA, in their response to the petition, imply that law enforcement would like to gain control over the standards process, rather than being a consultative voice in a forum dominated by telecommunications companies.

The FCC ruling also required that carriers support surveillance of packet data communications. They were given more time for this, and this was included in J-STD-025-B, which was published in February 2004.

Although this standard has always allowed the entire packet stream to be forwarded to law enforcement, Revision B added the ability to send some signaling information instead, assuming that the carrier is able to interpret the signaling at the appropriate protocol level and assuming law enforcement does not have a Title III, entitling them to the entire packet stream. It provides general guidelines for all wireless systems, but only provides specifics for cdma2000 packet data.

The next version of the standard, J-STD-025-C, will provide CALEA support for IP Multimedia Systems ('All IP'), including VoIP.

Figure 1: J-STD-025 Network Reference Model



Other standards for lawfully authorized electronic surveillance support include:

- ATIS T1.678 for wireline VoIP.
- ATIS T1.724 for GPRS and UMTS support, including IMS and VoIP.
- 3GPP TS 33.108, an international version of T1.724.
- ETSI ES 201 671 entitled *Telecommunications Security; Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic*.
- PKT-SP-ESP-I03-040113 (CableLabs) entitled *Packet Cable Electronic Surveillance Specification*, with ongoing development since 1999.
- Digital Dispatch Surveillance Standard #1 from AMTA, with ongoing development since 1999.
- Three paging standards from PCIA, with ongoing development since 1998.

A very useful, and much more detailed, history of the development of standards to support CALEA, written by Terri Brooks, chair of the joint TR-45/ATIA *ad hoc*. It is a 54-page PDF (with attachments following the 19 pages written by Terri Brooks) available at:

gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6516182017

"Please, sir, I want some more."

The petition from law enforcement is a clear statement that they are dissatisfied with the development of standards for CALEA, the implementation of CALEA and the interpretation of CALEA by the telecommunications industry.

Judging by past experience, the FCC will probably give law enforcement most of what they are asking for, but probably not all. It is quite certain that nobody will be completely happy with whichever compromise they produce.

The major requests of law enforcement are to:

- include surveillance of broadband access services in the scope of CALEA.
- include Push-to-Talk (PTT/PoC) services.
- include "broadband telephony" (e.g. VoIP).
- clearly define "packet-mode services".
- make carriers responsible for implementation costs.
- make law enforcement responsible only for costs directly associated with a requested wiretap.

Broadband access service is defined in the petition as including "the platforms currently used to achieve broadband connectivity (e.g., wireline, cable modem, wireless, fixed wireless, satellite, and power line)."

The law enforcement petition can be found at:

www.askcalea.com/jper.html

This petition has generated a large number of comments – comments that will likely be repeated during the formal rule-making process.

Some say "No Way!"

Internet privacy and openness advocates are, not surprisingly, strongly opposed to the law enforcement petition.

The Center for Democracy and Technology (cdt.org) claims that extending CALEA to broadband access is unjustified as the legislation was written to exclude the Internet (the term used was 'information services'). They point out that surveillance of the Internet is already possible, just not under CALEA.

On somewhat shakier ground, advocates such as the Electronic Frontier Foundation and the American Civil Liberties Union claim that VoIP and other voice-over-packet technologies are information services and thus exempt from CALEA. They do note that there are no large VoIP carriers in the local voice access marketplace – at least not at present. This argument that these new voice services have too insignificant a customer base to bother with would be invalidated if they do eventually take over a significant portion of local phone service.

Similar concerns were stated by the CTIA (ctia.org). In addition, they claim that the technical challenges "would require carriers to re-engineer the Internet and other private networks within 15 months."

Some commenters have quoted FBI Director Louis Freeh, testifying during the development of CALEA in 1994, stating that the Internet was explicitly excluded from CALEA.

Monetary Issues

Some of the biggest disputes over CALEA have been financial, rather than technical. CALEA initially promised reimbursement of up to $500 million to carriers for upgrading equipment installed before 1995. Yet, even with this large sum, law enforcement claims that only 20% of systems are fully CALEA compliant.

Carriers receive payment for each wiretap they install on behalf of law enforcement. Law enforcement claims that carriers should not include the costs of preparing their systems to support CALEA (e.g. capital, installation and maintenance). They want only to pay the costs exclusively associated with each wiretap event.

Rural carriers are particularly hard hit. They may be forced to implement support for CALEA, but in some cases they have never been asked to perform surveillance. They consequently have no way to recover their costs from law enforcement, and they have a smaller subscriber base to help subsidize them.

Finances and technology are interlinked with CALEA. Different technical approaches can have radically different associated costs, and also radically different trade-offs in the provision of adequate information to law enforcement and protection of the privacy of US citizens.

Understanding the Disputes

The reason for the disputes over CALEA may be because law enforcement wants to increase centralization and eliminate the loss of information. Centralization reduces the number of court orders that are required to intercept communications for a subject.

Using our example from circuit-switched eavesdropping of the interception of DTMF tones, these are normally carried transparently by telecommunications carriers after a call has been established. The carrier is unaware that they are being used to access voice mail, telephone banking and set up long distance calls.

Technically, it makes the most sense for interception to occur at the place where the tones are interpreted but this would mean law enforcement would need one court order for the phone company, one for each bank that the subject might use and one for each long distance company.

Centralization increases the burden on the carrier, because they now have to include DTMF receivers on calls that are being intercepted.

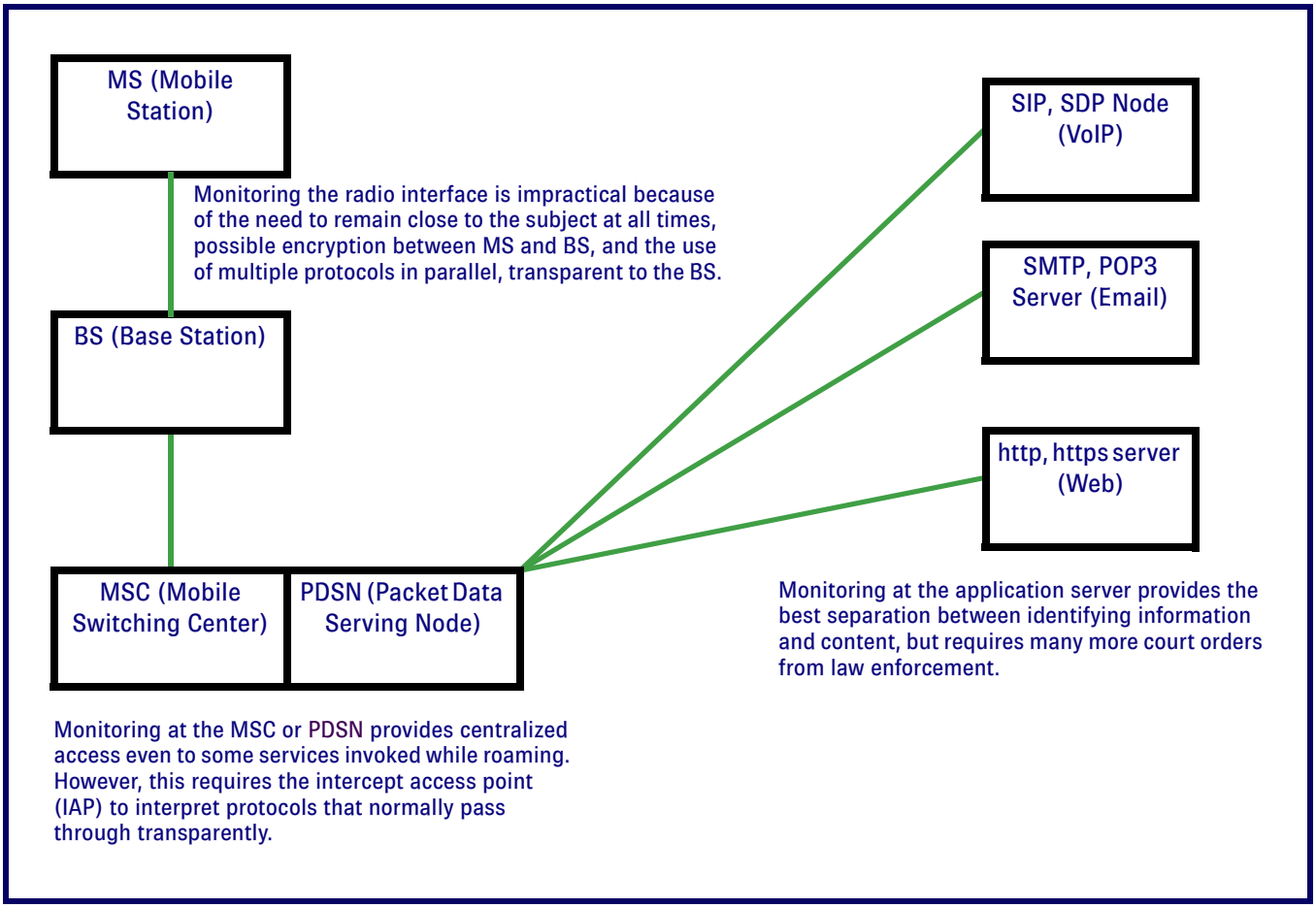
Problems like this are even more severe for Internet-based communications, as there are many more protocols that can be layered (with different terminating points in many cases) and used in parallel. Law enforcement obviously would like to intercept all this information at a single point, but then the problem of interpretation becomes acute.

Law enforcement is worried about the loss of information, but civil liberties organizations are worried about the collection of superfluous information. The *ad hoc* group's approach to packet data (in J-STD-025-B) was to provide the entire packet stream to law enforcement, which often will include much information that law enforcement is not legally entitled to have. However, with Internet-based protocols it is hard to see how a precise division would be possible.

Two other approaches to the problem are to maintain intercepts at a central point but with more intelligent analysis of the data, or to decentralize the intercepts to the places where the application terminates. The former is preferred by law enforcement, while the latter approach is preferred by those concerned about privacy because it allows the most precision in interception.

This conundrum is illustrated in **Figure 2**.

Figure 2: The Intercept Conundrum: "Location, Location, Location"



The TIA noted in their comments that this dispute over where identifying information should be intercepted is not relevant for Title III court orders where law enforcement has legal access to all information, but only to lesser court orders that only cover identifying information.

Likely Outcome

Law enforcement's request for broadband access surveillance appears to be their weakest argument. Their major argument is that the FCC had previously ruled that if facilities were used for both telecommunications and information services, they are still subject to CALEA. If interpreted broadly, that would open up virtually the entire Internet to be within the scope of CALEA.

Their demand for CALEA support for VoIP and PTT makes more sense. These are clearly voice services and can, to a considerable extent, replace traditional circuit-switched telephony services. They do not have significant penetration at present, but may well in the future. Verizon, in particular, has supported the inclusion of VoIP within the scope of CALEA, probably because they do not want to see new entrants freed of a burden that they have to bear.

It would make sense, however, to treat these services as telephony services only in network nodes that can interpret the voice-related protocol. It makes little sense for an IP router to be able to intercept voice traffic when the vast majority of packets passing by will not be voice-related. In fact, such a requirement would probably destroy the ability of the router to process traffic. It makes more sense for a SIP proxy, as an example, to support CALEA, because that network node does understand voice services, and could easily distinguish call content from call identifying information. However, this approach increases the number of court orders that law enforcement will have to obtain for each subject, although the information they would obtain would be far more focussed, and with less need for complex analysis.

Next Steps: FCC

The ball is now in the court of the FCC that is expected to issue an NPRM fairly quickly. This will propose rules to support the parts of the petition that they feel are justified. Law enforcement, carriers and others will be able to respond to this and eventually the FCC will publish the new rules.

The FCC is somewhat going to be a prisoner of their own rhetoric. They have recently declared that VoIP is an "unregulated information service" (www.fcc.gov/voip)

which would imply that it is exempt from CALEA. Yet the FCC has also been strongly supportive of law enforcement demands for CALEA.

The FCC will also have to juggle technical, financial and legal issues. The legal issues, in particular, are often based on analogies with older technologies – analogies that are very much subject to the mindset of the analogizer. Technical and financial solutions will also have to have some parallels in rules set earlier for circuit-switched services.

After the rules are published it is still possible for organizations that feel they are excessive or inadequate to go to court to get a second opinion.

Even with the expedited rule-making that law enforcement has requested, and assuming no legal appeals, this process is likely to take many months.

To Probe Further ...

The subject of CALEA and LAES has been covered extensively in our sister publication *Cellular Networking Perspectives*. Some of the most relevant articles, forming useful background and chronological information include:

- July and August 1997 – An overview of J-STD-038 (SP/PN-3580).
- October 1998 – CALEA deadline extended until June, 2000.
- December 1998 – FCC releases Notice of Proposed Rule-making on CALEA.
- September 1999 – FCC rules on CALEA.
- September 2000 – US Court of Appeals overturns FCC rule-making.
- July 2002 – FCC produces a modified rule-making that gives law enforcement most of what they want.
- February 2003 – An analysis of the impact of packet data surveillance requirements.
- January 2004 – J-STD-025 Revision B is published.

Back issues can be ordered from:

cnpsales@cnp-wireless.com

Back issues are normally $25 each, but if you order the full set of nine issues listed above we will provide them at a discounted price of $150 (value $225). This includes all articles in each of these issues.

FBI CALEA Website

www.askcalea.com

FCC CALEA Website

www.fcc.gov/calea

Comments on this particular rule-making can be located by entering the FCC identity, RM-10865, in the "Proceeding" box at:

gullfoss2.fcc.gov/prod/ecfs/comsrch_v2.cgi

Fraud and Security Patent News

US Patent: 6,742,120

System and method for controlling access to computer code in an IC card

The present invention is a system for controlling access to one or more sets of programming instructions embedded in read-only memory. The system is in a multiple application card system including an IC card comprising a microprocessor, a read-only memory, a random access memory and an electronically erasable programmable read-only memory. The memory comprises means for storing on said IC card for at least one application loaded onto said card at least one access flag having a value indicating whether or not access by the at least one application to the at least one set of programming instructions shall be granted and means dependent on said value for allowing access to one or more sets of programming instructions.

Issued: May 25, 2004

Inventor: Dimitrios Markakis, *et al*
Assignee: Mondex International Limited (London, GB)

US Patent: 6,742,115

Method for negotiating weakened keys in encryption systems

The present invention is for a method and apparatus for permitting encrypted communications between two stations. The two stations are operable with encryption algorithms that accept encryption keys having work factors with different values, by determining the lower one of the values; providing an initial encryption key having a first work factor value; comparing the first work factor value with the lower one of the work factors when the first work factor value is greater than the lower one of the work factor values, performing a first hash function on the initial encryption key to produce a first output, and deriving from the first output a first intermediate key having a work factor value not greater than the lower one of the work factor values; performing the first hash function on the first intermediate key to produce a second output, and deriving from the second output a final encryption key having a work factor value not greater than the lower one of the work factor values; and using the final encryption key to encrypt communications between the two stations; and when the first work factor value is found to not be greater than the lower one of the work factor values, using the initial encryption key to encrypt communications between the two stations.

Issued: May 25, 2004

Inventor: Gregory Rose
Assignee: Qualcomm, Inc. (San Diego, CA)

Upcoming Wireless & Wireless Security Events

The following are upcoming wireless and wireless security events for June that may be of interest. The venue and URL are provided for convenience.

WCA 2004 (Wireless Communications Alliance)
1st- 4th June 2004
Marriott Wardman Park Hotel
Washington, DC
www.wcai.com

Infosecurity Canada
1st- 3rd June 2004
Metro Toronto
Convention Center
Toronto, Ontario
www.infosecuritycanada.com

The Wireless Community & Mobile User Conference
2nd-4th June 2004
Monterey Conference Center
Monterey, CA
wetec.csumb.edu/WeTEC_conference.htm

Sixth Annual Techno Security Conference
6th- 9th June 2004
Marriott Resort at Grande Dunes
Myrtle Beach, SC
www.technosecurity.com/html/Techno2004.html

Sensors Expo & Conference
7th- 10th June 2004
Cobo Conference & Exposition
Detroit, MI
www.sensorsexpo.com/spring04/V40/index.cvn

Wireless Connectivity World
8th- 10th June 2004
Amsterdam RAI
Amsterdam, The Netherlands
www.wiconworld.com/training.asp

Wi-Fi Planet Conference & Expo
8th- 11th June 2004
Baltimore Convention Center
Baltimore, MD
www.jupiterevents.com/wifi/spring04/agenda2.html

Applied Cryptography and Network Security
8th - 12th June 2004
Huangshan International Hotel
Yellow Mountain, China
www.onets.com.cn/zhuceenglish.htm

International Workshop on Theoretical Aspects of Wireless Ad Hoc, Sensor, and Peer-to-Peer Networks
11th- 12th June 2004
Illinois Institute of Technology
Chicago, IL
www.cs.iit.edu/~xli/workshop

NetSec '04
14th- 16th June 2004
Hyatt Regency Embaradero
San Francisco, CA
www.gocsi.com/events/netsec.jhtml

Wireless Optimization Mini-Conference – Meeting of PCCA (Portable Communication and Computer Association)
16th- 17th June 2004
Newark Liberty International
Airport Marriott
Newark, NJ
www.pcca.org/news/Agendas/ag04-06.htm

SUPERCOMM 2004
20th- 24th June 2004
McCormick Place
Chicago, IL
www.supercomm2004.com

ICC 2004 – The 2004 International Conference on Communications
20th- 24th June 2004
Disneyland Resort Paris
Paris, France
www.icc2004.org

ICWN '04 – The 2004 International Conference on Wireless Networks
21st- 24th June 2004
Monte Carlo Resort
Las Vegas, NV
juliet.stfx.ca/~lyang/icwn-04

700MHz Networking & Educational Conference 2004
22nd- 23rd June 2004
Holiday Inn Chicago Mart Plaza
Chicago, IL
www.shorecliffcommunications.com/700users

Wireless LAN & 802.11 Security Workshop
24th June 2004
Marriott – Tysons Corner
Tysons Corner, VA
www.itvshop.com

USENIX '04 Annual Technical Conference
27th June – 2nd July 2004
Boston Marriott Copley Place
Boston, MA
www.usenix.org/events/usenix04

Quote of the Month

"We must plan for freedom, and not only for security, if for no other reason than that only freedom can make security secure."

Sir Karl Popper

US Patent: 6,742,094

System for access control to hidden storage area in a disk drive

The present invention is a disk drive that has a disk assigned with a plurality of hidden storage areas. The disk drive includes an authentication module which performs authentication processing for each hidden storage area in response to an access request from a host system. The authentication module exchanges information with the host system and performs authentication processing to determine access permission for each hidden storage area by using key information and unique information defined for each hidden storage area.

Issued: May 25, 2004

Inventor: Fubito Igari
Assignee: Kabushiki Kaisha Toshiba (Tokyo, Japan)

US Patent: 6,742,038

System and method of linking user identification to a subscriber identification module

This invention is a system and method for providing access to a server by a wireless computing device. A server and a wireless computing device and a communications link between the wireless computing device and the server are provided. The wireless computing device includes a hardware component including a processor and a memory. The server generates instructions and converted data based on data requested by the wireless computing device. The wireless computing device also includes an identification module. The identification module can provide identification data to the server.

Issued: May 25, 2004

Inventor: Joe Freeman Britt, Jr.
Assignee: Danger, Inc. (Palo Alto, CA)

www.danger.com

Danger Inc., of Palo Alto, makes software to run mobile devices for consumers – particularly young, hip ones. Danger develops wireless solutions, like hiptop, that enable wireless operators to provide new services and products to their customers. The Danger solution was designed to address the needs of wireless operators to take advantage of next generation data networks.

Danger, Inc.
3101 Park Blvd.
Palo Alto CA 94306

Tel: 1.650.289.5000
Fax: 1.650.289.5001

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 brief ly 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.

US Patent: 6,741,872

Method of authorizing access to a cellular mobile radio network from a simplified telephone and an associated mobile radio system and simplified telephone

The present invention describes a method of authorizing access to a cellular mobile radio network from a simplified mobile telephone, simplified in particular in that it does not include a reader adapted to receive a subscriber identification module (SIM). According to the invention, access to the network is made possible in particular by a service initialization phase during which a subscriber to the network supplies to the network data representing a serial number specific to the simplified mobile telephone – for example its IMEI number, and data characteristic of each telephone number that can be called from the simplified mobile telephone. All of the data is stored in a data base of a server of the network in a private directory associated with the simplified mobile telephone.

Issued: May 25, 2004

Inventor: Francis Penault
Assignee: Alcatel (Paris, France)

US Patent: 6,741,861

Method and apparatus for rapid assignment of a traffic channel in digital cellular communication systems

This invention is a method and apparatus for rapidly assigning traffic channels to a plurality of mobile stations in a wide area high-speed packet data cellular communication system. Mobile stations transmit access probes on randomly selected access channels to selected base stations to initiate traffic channel assignments. The access probe comprises a pilot preamble, a traffic channel request, and a pilot/data request channel (DRC). The pilot preamble allows the selected base station to easily detect the access probe transmission. The traffic channel request includes data that identifies the mobile station. Immediately after transmitting the traffic channel request, the mobile station begins communicating with the base station on both the forward and reverse communication links. The selected base station immediately supervises the mobile station's transmission power. The mobile station selects from a group of available power control sub-channels. The mobile station selects an available channel and an associated power control sub-channel from the list.

Issued: May 25, 2004

Inventor: Paul Bender, *et al*
Assignee: Qualcomm, Inc. (San Diego, CA)

US Patent: 6,741,857

Access method and apparatus for a wireless local loop telephone network

The present invention is for a fixed wireless terminal that uses a method for accessing a wireless local loop (WLL) telephone network to provide both a diagnostic mode of operation and a digital data delivery mode of operation in a system which utilizes a protocol which provides support for only the digital data delivery mode of operation. The method includes setting up a call to a WLL device which includes a mobile station and a communication interface. The mobile station receives call setup signals followed optionally by a predetermined guard time. The communication interface is responsive to a predetermined guard time for switching to a diagnostic mode, and in the absence of the predetermined guard time being transmitted, the communication interface maintains the digital data delivery mode.

Issued: May 25, 2004

Inventor: James Warden, *et al*
Assignee: Motorola, Inc. (Schaumburg, IL)

US Patent: 6,741,856

Communique system for virtual private narrowcasts in cellular communication networks

The present invention is a communication system for private virtual narrowcasts that operates with existing cellular communication networks to provide private virtual narrowcast communication services, that are initiated by a narrowcast host, to subscribers. The communication can be unidirectional (broadcast) or bi-directional (interactive) in nature, and the extent of the communication is narrowcast, where cells and/or cell sectors are grouped to cover a predetermined geographic area or demographic population or subscriber interest group to transmit information to a private group of subscribers who populate the target audience for the narrowcast transmissions. The grouping of cells to form the communication coverage area for the narrowcast transmissions need not be contiguous and can comprise dynamic combinations of contiguous and non-contiguous cells as well as combinations of in-building wireless coverage areas, standard terrestrial cells, non-terrestrial cells, orchestrated in a hierarchical manner. The private virtual narrowcasts use the code, frequency and time domains to enable multiple users to share the same wireless resource in a manner that, from the user's perspective, has dedicated spectrum or channel capacity to their particular application. The applications can include asymmetric bi-directional communications where private virtual narrowcasts stimulate the generation of point-to-point responses from subscriber terminal devices.

Issued: May 25, 2004

Inventors: Daniel McKenna and James Graziano
Assignee: Vesuvius Inc. (Boulder, CO)

Vesuvius, based in Steamboat Springs, is a technology development and intellectual property company. The company conceives, develops and patents novel wireless services for overlay on existing architectures for the delivery of content in a multicasted / narrowcasted fashion over second-, third- and fourth-generation cellular networks.

US Patent: 6,741,852

Method and device to authenticate subscribers in a mobile radiotelephone systems

This invention is for a method and device to authenticate a subscriber of a digital mobile radiotelephone system vis-a-vis an authentication entity, wherein the subscriber firstly initializes vis-a-vis the authentication entity by executing several times the authentication algorithm containing stored subscriber-specific components and by storing the corresponding response parameters of the subscriber-specific components in a non-volatile memory. Systematic authentication of the subscriber of the mobile radiotelephone system vis-a-vis the authentication entity via a common interface is made possible by the authentication parameters stored in the memory since the authentication entity can always refer back to the response parameters of the individual subscriber module it already knows.

Issued: May 25, 2004

Inventor: Walter Mohrs
Assignee: DeTeMobil Deutsche Telekom MobilNet GmbH (Bonn, Germany)

US Patent: 6,741,851

Method for protecting data stored in lost mobile terminal and recording medium therefor

The present invention describes a method for protecting data stored in a lost mobile terminal and a recording medium for storing the data are provided. In the method, a user who has lost the mobile terminal transmits protection control information to the lost mobile terminal, using a communication apparatus. The lost mobile terminal receives and discriminates the protection control information. User identifying information, which is included in the protection control information, is compared with information which is previously stored in the lost mobile terminal. When the user identifying information is identical to the information previously stored in the lost mobile terminal, the data which is stored in the lost mobile terminal is processed according to the user's data protection request which is included in the protection control information.

Issued: May 25, 2004

Inventors: Tae-seung Lee and Sang-seo Lee
Assignee: Samsung Electronics Co., Ltd. (Kyungki-Do, S. Korea)

US Patent: 6,741,704

Method of setting encryption for a connection in a radio system

In combined systems of different radio systems, for example in a combined system of the radio access network (RAN) of the IMT-2000 system and the core network (MSC) of the GSM system, a problem exists in transferring encryption settings from a system element to the others. The present invention relates to a method of setting encryption for a connection in such a combined system, where the handling of the encryption settings of the switching center (MSC) and the base station (BTS) of the radio network is carried out at different protocol layers than the handling of the encryption settings of the mobile terminals (MT). In the method, encryption is arranged for the connection between the radio access network (RAN) and the mobile terminal (MT), and an encryption setting is transmitted from the switching center (MSC) to the control unit (BSC) of the radio access network (RAN). According to the invention, the method is characterized in that an encryption setting is transferred from the control unit (BSC) to the mobile terminal (MT) transparently from the point of view of the base station.

Issued: May 25, 2004

Inventor: Sami Virtanen
Assignee: Nokia Corporation (Espoo, Finland)

US Patent: 6,738,907

Maintaining a soft-token private key store in a distributed environment

The present invention discloses methods, systems, and devices that provide for securely updating private keys, key pairs, passwords, and other confidential information in a distributed environment. A transaction is created including appropriate encrypted soft-token content, and then transmitted to a new location. Comparisons are made to determine whether the new soft-token content should be recognized as authentic and entered at the new location. Updates are accomplished without ever sending the plain text form of a key or a password across the wire between the distributed locations.

Issued: May 18, 2004

Inventor: Stephen Carter
Assignee: Novell, Inc. (Provo, UT)

US Patent: 6,738, 905

Conditional access via secure logging with simplified key management

The present invention describes a method and apparatus for distributing content data from a content provider to a subscriber. The method includes encrypting content data by the content provider and providing the content data from the content provider to a broadcaster. The content provider also provides a content descriptor, including keys to decrypt the encrypted content, to a conditional access provider. The broadcaster distributes the encrypted content information to a subscriber. A business service provider negotiates with the subscriber to deliver individual content programs or packages of content programs to the subscriber for a fee. The conditional access provider distributes a content descriptor including keys necessary to decrypt the programs the subscriber selected from the business service provider. A CAM retained by the subscriber maintains a log of programs accessed, and uploads the log to the business service provider, which is used to determine the appropriate fee which the subscriber should be charged. Alternatively, the subscriber may purchase a package plan which does not require logging, and thus allows unidirectional communication.

Issued: May 18, 2004

Inventors: David Kravitz and David Goldschlag
Assignee: Digital Video Express, L.P. (Herndon, VA)

US Patent: 6,736,312

Electronic apparatus, electronic apparatus operation system, authentication system, authentication method, and information storage medium

The present invention is for an electronic apparatus with authentication capabilities. A system controller reads first identification information from a semiconductor storage medium. The system controller causes an audio block to operate when a portion of the first identification information coincides with one of a whole and a portion of the second identification information stored in a non-volatile memory. The system controller stores another portion of the first identification information as a portion of the second identification information in the non-volatile memory. Even if a user adds the first identification information to the semiconductor storage medium, an onboard audio apparatus reads and stores an additional portion of the first identification information in the non-volatile memory. The first identification information added by the user is used for a next operation enable/disable determination for the audio block.

Issued: May 18, 2004

Inventors: Tadahisa Komurasaki and Sei Onishi
Assignee: Sony Corporation (Tokyo, Japan)

US Patent: 6,735,624

Method for configuring and authenticating newly delivered portal device

A portal device is described comprising: a processor; and a memory for storing instructions which, when executed by the processor, cause the processor to receive data transmitted from a portal server on which a user of the portal device is registered, the data being identified by the user upon registering a user account with the portal server.

Issued: May 11, 2004

Inventor: Andrew Rubin, *et al*
Assignee: Danger, Inc. (Palo Alto, CA)

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