Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 5, No. 1. January, 2003

In the News: GPS Impacts from a Kit-built Jammer

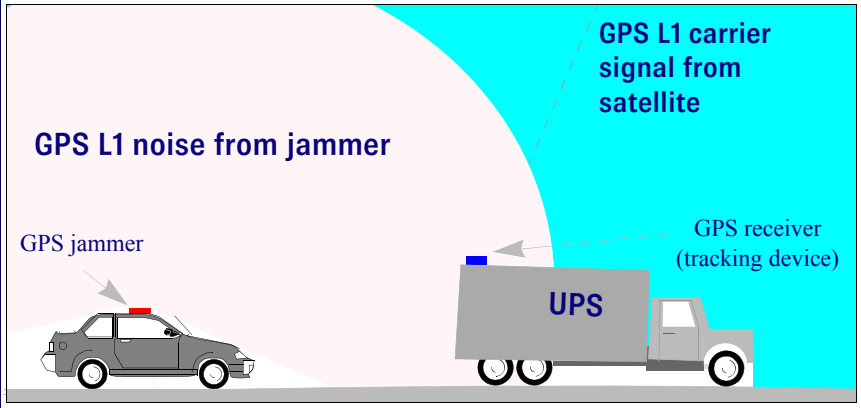
Recently, an Internet group released instructions for building a GPS (Global Positioning System) jamming device. Although it is not an easy device to build, it seems to pose a significant threat to commerce and defense, since even the U.S. Department of Defense (DoD) is concerned about it.The jamming device disrupts the C/A code (coarse acquisition) in civilian-use GPS microwave signals that are received on the frequency of 1575.42 MHz (GPS L1). After having travelled 12,000 miles or so between the satellite and the earth, these signals are left with a low strength, which makes them an easy target for jamming. The effect of the device is to stop GPS receivers from locking onto the carrier signal.

This jammer does not compete with military jammers. Its normal jamming radius (for GPS receivers which are not in the high-quality category) is expected to be only a few hundred feet. Higher quality GPS L1 systems would only become jammed within an even smaller radius.

Figure 1 illustrates one example of the many ways this device could disrupt commerce. The device has potential for disturbing trucking companies and law enforcement agencies, who frequently mount GPS tracking devices on their vehicles to augment the organization's supervisory tasks.

Figure 1: Sample Jamming Scenario

A car equipped for disturbing businesses could park or travel close to its target. Unintended targets with communication already established would, while passing by the car, lose their lock on the carrier GPS signal.



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…

February 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.

How does it work?

The jammer transmits a narrow-band gaussian noise signal on the L1 GPS frequency. It includes a phase locking system and a noise generator.

The phase locking is accomplished through use of a 10 MHz quartz crystal coupled with various integrated circuits, modules, capacitors and a passive loop filter – components available from electronic parts retailers. A diode and transistor in the noise generator configuration produce a raw signal of less than 100 MHz, which is amplified and low pass filtered using a typical audio amplifier integrated circuit. The resultant low-frequency noise signal is then mixed with the signal produced from the phase locking system – using a 100 Ohm potentiometer – to produce the final jamming signal: 1575.42 MHz with a deviation of +/- 1.023 MHz – GPS L1 noise.

The device, requiring only 300 mA, can be powered by a car battery or a string of small batteries or a solar panel, making it extremely portable. Depending upon the type of antenna used, it would be capable of producing GPS L1 noise in a radial spread or in a directed beam aimed at a target.

Other Versions and The Counter-attack

In addition to jamming GPS L1 devices, the source supplying the kit instructions also stated their device could become a stepping stone for designing a 1.9 GHz CDMA jammer and could possibly be adapted to jam the new civilian C/A-code signal to be transmitted on the GPS L2 (1227.6 MHz) frequency.

Internet instructions for building jamming devices or for employing jamming techniques have been available for over a year and a half. However, news of this jammer's threat to GPS signal security – and possibly to other signals – could lead the U.S. Department of Defense to transfer anti-jamming technology to civilian and commercial applications. Currently, GPS anti-jamming configurations are kept secret by the military. Unlike other threats in the recent past, this time the DoD seems motivated to protect civilian GPS signals and users. This posed threat could impact military GPS devices – even though this

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.

ATIS Security Summit: Security of Service Provider Infrastructure in the Era of Convergence
4th – 5th February 2003
Intelsat Headquarters
Washington, DC
www.atis.org

SANS Orlando
4th – 9th February 2003
Walt Disney World Swan Hotel
Orlando, FL
www.sans.org/orlando

The 10th Annual Network and Distributed System Security Symposium
6th– 7th February 2003
Catamaran Resort Hotel
San Diego, CA
www.isoc.org/isoc/conferences/ndss/03/cfp.shtml

Cybercrime 2003 Conference & Exhibition
9th– 11th February 2003
Foxwoods Resort Casino
Mashantucket, CT
www.cybercrime2003.com

allNetDevices Conference & Expo
10th– 11th February 2003
DoubleTree Hotel San Jose
San Jose, CA
www.jupiterevents.com/allnet/spring03/glance.html

The Conference on Mobile & Wireless Security
11th– 13th February 2003
Marriott Mountain Shadows Resort
Scottsdale, AZ
www.misti.com

Smart Card Alliance Mid-Winter Meeting and Educational Institute
12th– 13th February 2003
Salt Lake City Center Hilton
Salt Lake City, Utah
www.smartcardalliance.org

3GSM World Congress 2003
17th– 21st February 2003
Congress Centre Cannes
Cannes, France
www.3gsmworldcongress.com/congress

Asia Pacific Regional Internet Conference on Operational Technologies 2003
19th– 28th February 2003
Taipei International Convention Center
Taipei, Taiwan
www.apricot2003.net

Wireless System Design Conference and Expo 2003
24th– 27th February 2003
San Jose Convention Center
San Jose, Ca
www.wsdexpo.com

Black Hat Windows Security 2003
25th– 28th February 2003
Sheraton Hotel
Seattle, WA
www.blackhat.com

Third Annual Privacy Summit
26th– 28th February 2003
Hilton Washington
Washington, DC
www.privacyassociation.org

EyeforWireless West 2003 – WLAN / WWAN Seamless Roaming Hotspot Footprint Expansion
27th– 28th February 2003
Sheraton Gateway San Francisco Airport
San Francisco, CA
www.eyeforwireless.com/mixwireless

GPS Wireless 2003
27th– 28th February 2003
Marriott San Francisco Airport
San Francisco, CA
www.gps-wireless.com

kit-built jammer does not jam the P(Y) code used in the military GPS signal. It could affect almost all military GPS equipment, since they use the C/A code to acquire the P(Y) code (during initialization).

Obviously, the military is bound to release only enough of it's secret anti-jamming technology to provide protection for all civilian GPS and CDMA devices, while at the same time retaining many more secrets for its self-preservation.

Wireless Security Technology Panel at IEEE Conference

The 2003 IEEE Wireless Communication and Networking Conference (WCNC)

www.research.panasonic.com/ieee/adg/wcnc03/WCNC03_BAS-12.html

will be held in conjunction with the CTIA Wireless conference in New Orleans, Louisiana. The IEEE WCNC '03 event will include a wireless security panel organized and moderated by Les Owens. This 90-minute panel, one of two scheduled for WCNC this year, will be held on March 17th at 1:30 PM. It will allow panelists to discuss some of the critical operations, management, scalability and other business issues surrounding security for several wireless local and wide area network technologies. Panelists will include senior technologists from Ecutel, Newbury Networks and SafeNet.

Security Requirements for the Management Plane

ATIS (the Alliance for Telecommunications Industry Solutions – atis.org) is balloting a new standard entitled "Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane."

The purpose of the standard is to incorporate the requirements of the U.S. President's National Security Telecommunications Advisory Committee (NSTAC) to protect access to telecommunications network management systems.

Traditional telecom network management systems transmitted control data 'out of band', using a separate network than the one that carried user traffic (e.g. voice calls). Many carriers are implementing, or at least considering, systems where all traffic – voice, data and signaling – is merged. This results in lower capital and operating costs, but it could make management systems more vulnerable to attack.

The new standard is not revolutionary; it merely brings 'state of the art' security technologies to the management of telecom networks.

Threats considered by this standard were:

- Unauthorized access.
- Masquerading as an authorized user.
- Integrity threats (unauthorized manipulations to signaling messages or data stored in management systems).
- Confidentiality threats (e.g., eaves-dropping on management sessions).
- Denial of service (flooding the network with useless data to prevent normal operations).

Some of the recommendations include:

- For symmetric (private key) encryption, to prefer the use of AES rather than TDES (triple key DES) or, worse yet, plain DES.
- For asymmetric (public key) encryption, the use of RSA with at least 2,048 bit keys, Diffie-Hellman (prime group of at least 2,048 bits) or Elliptic Curve Cryptography with at least a 160-bit key.
- For data integrity, symmetric key systems should use HMAC-MD5 with 128-bit keys or HMAC-SHA-1 with 160-bit keys. Asymmetric key systems should use an algorithm as strong as RSA or DSS.
- Secure key management should be implemented, protecting the generation, distribution, storage, replacement and recovery of keys.
- Authentication of management systems should be X.509 certificate-based.
- User authentication should require, at a minimum, a user id, a static password and a dynamic password (e.g,. SecurID card).
- Static passwords must meet a minimum standard of complexity (e.g., mixture of upper case and lower case letters, digits and special characters).
- Auditing should provide a detailed log of at least the most important system events, such as each login by privileged users.
- Management traffic should be strongly secured (e.g., using authentication and encryption).

The standard also defines five different types of user roles that must be supported by management systems:

1. System security administrator (the highest level, the 'super user')
2. Application security administrator.
3. System administrator
4. Application administrator
5. Application user/operator (the lowest level)

This standard will make a useful guide for people designing or implementing telecommunications management systems, and it could be used when sourcing new hardware and software, or for identifying weaknesses in existing systems.

The ballot version of the standards is available at:

ftp://ftp.t1.org/T1M1/NEW-T1M1.5/2m151252.zip

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

NIST-sponsored WiFi Workshop

A summary of a December 4th – 5th, 2002 NIST (National Institute of Standards and Technology) workshop on 802.11 Wireless LAN ('WiFi') security is available at:

www.csrc.nist.gov/wireless

This summary gives a good overview of the workshop objectives, and its conclusions. It also provides an agenda of the workshop, along with links to many of the presentations.

CALEA: What a Long, Strange Trip It Has Been

William J. Sill and Elizabeth Braman

In response to the need of Law Enforcement Agencies (LEAs) to conduct electronic surveillance in a digital environment, Congress passed the Communications Assistance for Law Enforcement Act of 1994 (CALEA)[1]. The act established a federal triumvirate comprised of the Department of Justice, the Federal Communications Commission (FCC) and the courts. Jointly, these organizations are responsible for developing, implementing, clarifying and enforcing a plan by which wireless carriers, wireline carriers and equipment manufacturers will modify the public switched telephone network (PSTN) so that the LEAs' ability to conduct effective surveillance will not be undermined.

Prior to CALEA's enactment, LEAs were concerned that their wiretapping methods, developed in an analog environment, would be rendered ineffective by the digitalization of the PSTN. LEAs believed that as cell phones became ubiquitous, it was only a matter of time before organized crime, drug dealers and other criminals embraced wireless telephony. Ironically, it might turn out that the actions of our country's enemies — particularly September 11th — have galvanized the regulators and the regulated into action.

CALEA jointly entrusts the U.S. Attorney General and the FCC to enact regulations prescribing the surveillance capabilities carriers will have to supply and the deadlines by which they must be met. Equally important, under CALEA, the courts play the essential role of providing parties who disagree with agency decisions with a forum for appeal.

Congress recognized that equipment manufacturers and carriers would be hard pressed to design and operate CALEA-compliant equipment and networks without guidance as to which surveillance functions must be supported. CALEA gave the FCC and the Attorney General the responsibility to establish the capability and capacity standards that wireless and wireline networks must meet.

One example is assistance capability requirements, which carriers must meet so that they can respond to a court order obtained by an LEA and:

- Intercept a wire communication;
- isolate call-identifying information;
- deliver intercepted communications and call-identifying information in a format the government can receive; and
- minimize interference to a subscriber's service caused by the surveillance.

The capacity requirements prescribe the actual and maximum number of LEA surveillance interceptions that a carrier must be able to support. Recognizing that CALEA implementation would be capital-intensive, the act includes a mechanism for government reimbursement of certain CALEA capability and capacity upgrades.

Dissension and Deadlines

For assistance in carrying out CALEA's mandates, the Attorney General designated the Federal Bureau of Investigation (collectively the FBI/DoJ) to assist in the implementation of CALEA on behalf of all federal, state, and local law enforcement agencies. The FBI/DoJ, in turn, created the CALEA Implementation Section (CIS), which established capacity requirements for each carrier, developed the CALEA flexible deployment schedule, reviewed each carrier's schedule, and was tasked with reviewing carriers' requests for cost recovery.

Figure 2 is an overview showing legislative, administrative and judiciary events related to the CALEA roll-out.

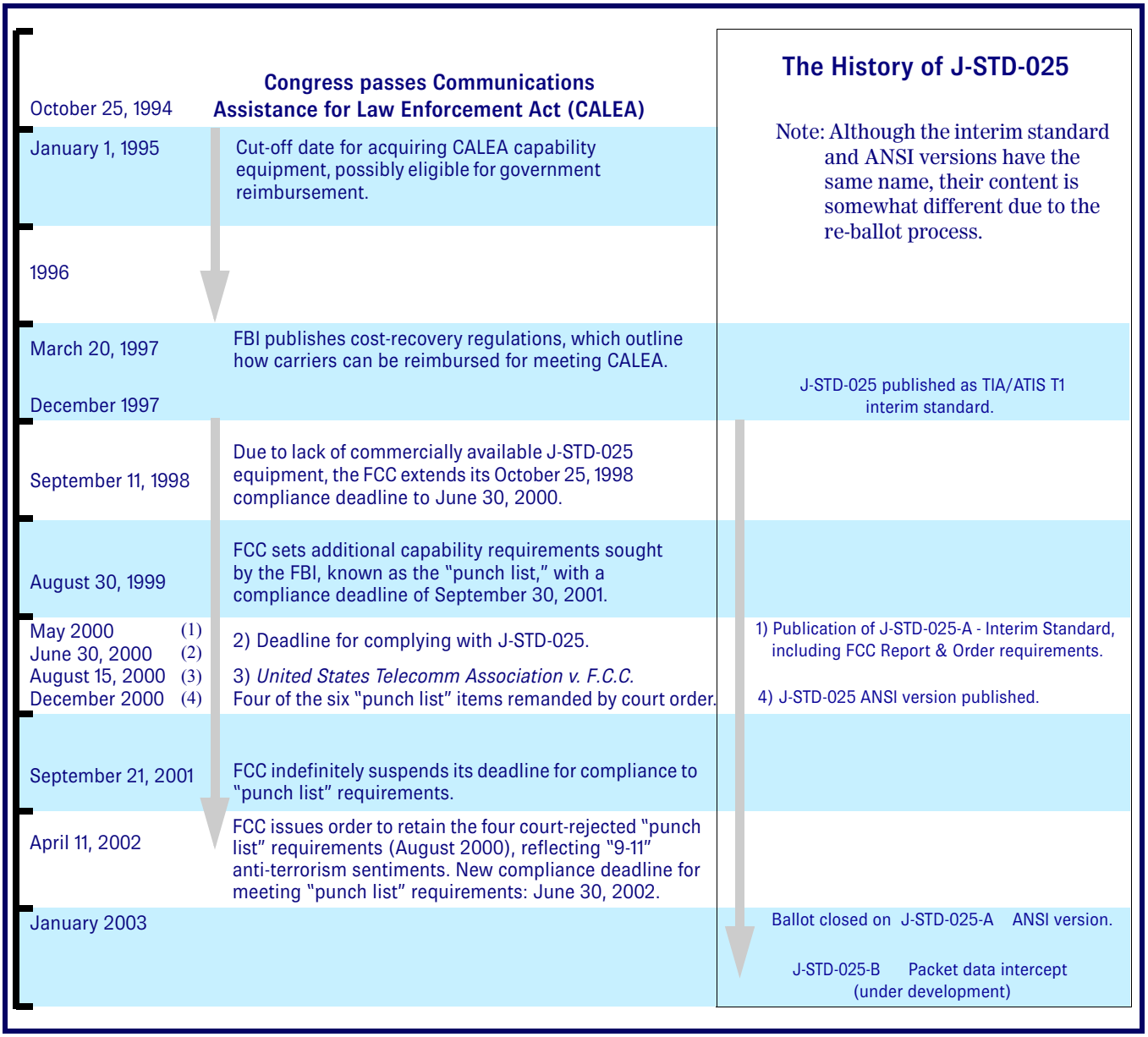
The FCC's involvement grew as it became clear that its assistance was required if CALEA was to be rolled out expeditiously. Any optimistic view that CALEA capabilities would be quickly agreed upon was soon dashed. In December 1997, the Telecommunications Industry Association (TIA) unanimously approved the draft release of the interim J-STD-025, commonly known as the *J-standard*, which was developed by TIA TR-45.2 and Committee T1 of the Alliance for Telecommunications Industry Solutions (ATIS). The vote sparked controversy because the LEAs were not TIA members, and thus, they could submit comments, but could not actually vote on the disposition of the standard.

After the adoption of the J-standard, the Cellular Telecommunications & Internet Association (CTIA), the Center for Democracy and Technology, TIA and the FBI/DoJ filed petitions at the FCC to enlist the commission's further involvement. In August 1999, the FCC issued its decision: The interim J-standard alone was inadequate for law enforcement's needs.[2]

To fill this perceived void, the FCC ruled that the industry must adopt additional technical requirements known as the "punch-list" capabilities. The FBI/DoJ proffered nine punch-list capabilities, which the FCC winnowed down to six.[3] The FCC's decision also created the first of many CALEA deadlines: June 30, 2000 was the J-standard compliance deadline, and September 30, 2001 was the punch-list deadline.

By August 2000, disagreement over the punch list and its related privacy issues spilled over into the federal courts. In *United States Telecomm Association v. F.C.C.* (*USTA v. FCC*), the U.S. District Court of Appeals for the District of

Figure 2: Key Dates in the CALEA Saga



Columbia Circuit was asked to determine which capabilities should be included in the punch list and how privacy issues should be resolved. The FBI/DoJ, the USTA, the Electronic Privacy Information Center and the FCC all weighed in. In the end, the court concluded that the FCC had not provided sufficient justification for four (as listed in [4]) of the six punch-list items, and it sent the decision back to the FCC for further consideration.With the September 30, 2001 deadline for punch-list compliance looming, and with the uncertainty over the breadth of the punch-list capability requirements, equipment manufacturers and carriers came down with a case of regulatory angst. Under the gun of the FCC's deadlines, equipment manufacturers – who under Section 106 of CALEA [5] have a statutory obligation to cooperate in CALEA efforts – have had to scurry to develop new CALEA products and design them to be compatible with existing network equipment.

Carriers' main concerns were not just the cost and availability of CALEA-compliant equipment. They also knew that if the September 30 deadline was not extended, and if the requisite equipment was not available, each of them faced the possibility of daily fines – $10,000 for each day of non-compliance.

Nine days before the September 30 deadline, the FCC suspended the deadline until it released an order in response to the court's remand of the USTA v. FCC decision.[6] On April 11, 2002, the FCC issued its decision reiterating the necessity of the additional four punch-list items — the same four items that the court had rejected.[7] Although nearly identical to its earlier decision, the April 2002 decision clearly reflects a post-September 11 mindset and

emphasizes the importance of preserving LEAs' ability to effectively execute surveillance techniques.

Recognizing that carriers and equipment manufacturers could not immediately comply with its decision, the FCC extended the punch-list deadline until June 30, 2002. It is worth noting that the FBI/DoJ, carriers, equipment manufacturers and public advocates did not contest the FCC's findings.[8] We believe that this response might reflect a new consensus, forged by the events of September 11, that CALEA now has a new, important role as a weapon in the war on terrorism.

As the June 30, 2002, deadline approached, it became clear that none of the six major equipment vendors were capable of supporting every punch-list capability. Not surprisingly, hundreds of carriers, from large to small, petitioned the FCC for an extension.[9] The FCC has not yet acted on those petitions.

Two Unresolved Issues

Although CALEA's high-pitched battles may be behind us, two sources of uncertainty remain: The regulatory treatment of packet-mode communications [10] and CALEA cost reimbursement. Both represent hurdles to the effective implementation of the act.

Packet-Mode Remains A Question Mark

The unique technological characteristics of packet communications raise significant concerns for carriers. In pleadings submitted to the D.C. Circuit Court in USTA v. FCC, carriers argued that packet headers (call-identifying information) cannot be separated from packet bodies or payloads (call content). As a result, the carriers urged the court not to include packet-mode capabilities as a CALEA capability. The court disagreed and found that the FCC had justified including packet-mode capabilities.

On September 21, 2001, the FCC rejected CTIA's request for a blanket indefinite extension of the packet-mode communications requirements, but it agreed to extend the deadline for compliance with packet-mode obligations to November 19th, 2001. Although numerous carriers have filed petitions with the FCC to extend the packet-mode deadline, the FCC has yet to act on their requests.

Even though the November 19th compliance deadline has long since passed, fundamental packet-mode issues remain unresolved. The FCC has received petitions requesting both clarification of requirements and extensions of time to meet the deadline. Although the FBI/DoJ contends that CALEA applies to capabilities, regardless of the method of transmission (i.e., circuit-switched or packet), some of the petitioners have questioned whether certain packet-mode capabilities are information services, and thus should be exempt from CALEA. FCC staff characterize these petitions as individual carrier extension requests rather than petitions raising industry-wide concerns. Thus, the FCC has left these issues largely unresolved, stating only that it has already clarified the distinction between information services and telecommunications services in its August 31, 1999, order.[11]

Some carriers and public interest groups view the possible inability to separate call-identifying information from call-content information as creating thorny privacy issues. Until such separation is technologically and economically feasible, carriers might be faced with a 'Catch 22' dilemma whenever an LEA requests call-identification information.

For example, by delivering the packet to an LEA with both call-identifying and call-content information intact, the carrier opens itself up to liability for revealing the call-content information, which was not requested. Conversely, if the carrier declines to honor the LEA request, it could be held liable for up to $10,000 per day in fines. Worse, the FBI/DoJ has not provided carriers with any guidance about how it expects carriers to fulfill their packet-mode obligations.

CALEA Reimbursement Remains an Unfulfilled Promise

Despite CALEA's enormous price tag, reimbursement remains more of a promise than a reality. By making CALEA compliance more affordable, the theory went, equipment manufacturers would be encouraged to quickly develop compliant products, and carriers would be encouraged to quickly integrate them into their systems. For example, Congress established a $500 million CALEA-reimbursement fund and the FBI/DoJ said it would enter into software-licensing agreements with equipment manufacturers so that carriers' CALEA expenses could be reduced. Both efforts have gone awry.

CALEA sets requirements that carriers must meet in order to receive reimbursement for upgrades to capacity or capabilities. To receive reimbursement for capacity upgrades, carriers were required to have filed statements in September 1998, detailing the necessary modifications.[12]

An entirely different set of considerations governs capability reimbursement, which is permitted only for reasonable costs directly associated with modifications necessary to bring into compliance any equipment deployed on or before January 1, 1995.[13] However, the carrier is not eligible for reimbursement if the equipment, facility or service "has been replaced or significantly upgraded or otherwise undergoes major modification."[14]

To further clarify the terms under which capability reimbursement will be made, the FBI/DoJ released a Supplemental Notice Of Proposed Rulemaking (SNPRM) in October 2001. In the SNPRM, the FBI/DoJ tentatively chose very narrow definitions of two terms in the act: "replaced" and "significantly upgraded." Their choice raised concern that if those definitions were implemented, even minor equipment modifications could prevent reimbursement.

In response to the SNPRM, CTIA submitted comments questioning whether the proposed definitions indicated that there will be no

reimbursements to carriers for equipment or hardware associated with CALEA capability upgrades. Although it has been over a year since comments were received, the FBI/DoJ has yet to issue a decision.

Even if the FBI/DoJ were to issue favorable reimbursement guidelines, it may well be a pyrrhic victory because the $500 million reimbursement chest appears to be inadequate. About four-fifths of the chest has been depleted by the FBI/DoJ's decision to use the fund so that carriers could receive – at no cost – CALEA software under nationwide RTU licensing agreements. Based on CTIA [**15**] and the FBI/DoJ [**16**] early cost estimates, it appears they would both agree that the amount in the chest is inadequate. But the prospect for a quick infusion of additional capital does not appear in sight. The FBI staff has informed carriers that its request for approximately $200 million in additional funding was denied.

Currently, reimbursement efforts appear to be stalled. The DoJ Office of Inspector General's (OIG's) last bi-annual CALEA audit report to Congress noted that, as of March 2002, no carrier had received reimbursement for deployment of their technical solutions.[**17**] The report indicates that the agency recently entered into its first carrier agreement: Qwest, for $6.2 million for modifications to equipment that was installed or deployed after January 1, 1995.

However, this agreement appears to be the exception rather than the rule, because Qwest required CALEA upgrades in preparation for the 2002 Winter Olympics in Salt Lake City, Utah. FBI staff recently confirmed that no other carriers, wireless or wireline, have received direct CALEA reimbursement.

Although it appears doubtful that carriers will have their CALEA capability and capacity costs completely reimbursed, the failure to come to grips with this issue endangers a ubiquitous CALEA roll-out, because certain carriers will not be obligated to become CALEA-compliant if they are not reimbursed. Congress established "safe harbors" for eligible carriers that did not receive reimbursement.[**18**] A carrier is deemed to be capacity- or capability-compliant if it is eligible for reimbursement but the FBI/DoJ fails to do so.[**19**] One would expect carriers to lawfully avail themselves of the CALEA safe harbors, especially when confronted with a downturn in the economy and increased wireless competition.

Uncertainty Undermines CALEA

The FCC's April 2002 order has been followed by a lull in both regulatory decision-making and litigation. Carriers have either met their CALEA obligations or, more likely, have petitions on file with the FCC and are relying on CALEA's safe harbors. Despite the brief reprieve, carriers and equipment manufacturers are left in a quandary, scrambling to become CALEA compliant, while technical standards and the ability to receive reimbursement remains unclear.

As a practical matter, it has been difficult for carriers to make effective long-range economic plans as deadlines shift and as CALEA capabilities requirements mandate purchases of new switches and other equipment, which either would not have been purchased or would have been purchased later when customer demand required it. Ironically, some carriers may be uncertain about how to meet the compliance benchmarks set in their flexible deployment plans without jeopardizing their reimbursement potential. Without the prospect of meaningful reimbursement in the foreseeable future, an expeditious and ubiquitous roll-out of CALEA might be impossible.

Small carriers feel disproportionately affected by CALEA obligations because they would not need to make many of the required upgrades to their switches if it were not for CALEA. These carriers may be compelled to make the unusual decision of purchasing equipment to respond to demands from regulators rather than customers. Unlike larger carriers that have significant subscriber bases, small, rural carriers have far fewer subscribers to help defray CALEA's costs. To make up for the shortfall caused by CALEA expenditures, smaller carriers are more likely to have to siphon capital from their internal budgets, including monies that would have otherwise gone towards expanding their systems' coverage and improving service quality.

Equipment manufacturers have had to scramble under difficult deadlines to develop innovative CALEA solutions that can retrofit existing networks. At various times during the design stage, manufacturers were unsure of exactly which capabilities had to be incorporated to meet regulatory obligations, so their ability to deliver a product at a set price in a timely manner is compromised.

Only through collective action can CALEA's roll-out be expedited. The triumvirate of the courts, the DoJ and the FCC can play a pivotal role by removing, or at the very least minimizing, the uncertainties confronting carriers and equipment manufacturers.

Several positive signs indicate this is beginning to occur. Over the past two years, the FBI/DoJ and the FCC have shown an increasing willingness to work together by, for example, establishing procedures to ensure that a carrier does not request a deadline extension until it first submits an FBI flexible-deployment schedule that is consistent with the extension request.

Meanwhile, many of the major issues surrounding CALEA have been hashed out. For example, the J-standard and the punch-list capabilities are set, and equipment manufacturers have made great strides towards meeting those technical capabilities.

However, much work remains. For example, the FCC could remove uncertainty by deciding the issues raised by the outstanding packet-mode petitions. Without a decision, the carriers, manufacturers and public interest groups cannot gain closure at either the FCC or in the courts.

It is also unclear whether or not a packet-mode standard, when it is finally set, will resolve, or even address, all of the issues surrounding packet-mode. Perhaps the FCC, in conjunction with the FBI/DoJ,

also could explore innovative methods to help carriers recover CALEA expenses, such as permitting carriers to pass on their CALEA expenses to customers as a cost of service. By proactively deciding the issues, the FCC would take an important step toward freeing the parties from limbo, allowing them to begin implementing agreed upon functions in a lawful manner.

The FBI/DoJ could do its part by removing the uncertainties surrounding reimbursement, by issuing a decision in its capability rulemaking proceeding. In addition, it would seem prudent for the FBI/DoJ to estimate additional funds required for reimbursement, and Congress should be asked to increase the CALEA chest in accordance to such estimate. The issues surrounding CALEA reimbursement still hang over carriers, manufacturers and the law enforcement community. Until this cloud is removed, CALEA's roll-out will be hindered.

LEAs face the daunting challenge of thwarting criminal elements that, along with the general public, can utilize wireless digital systems. The current challenge is for regulators, carriers and manufacturers to amicably resolve the remaining CALEA issues so that CALEA can be rolled out in the most expeditious and cost-effective manner possible. The sooner these issues are resolved, the sooner the LEAs will have a far more ubiquitous and potent tool with which to catch the "bad guys."

*The **February** issue of Wireless Networking Perspectives will address the technical aspects of CALEA.*

About the Authors

*Mr. Sill (*wsill@wbklaw.com*) is a partner, and*
*Ms. Braman (*ebraman@wbklaw.com*) is an associate at*
Wilkinson Barker Knauer LLP.

End-notes and References

[1]. *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Third Report and Order, 14 FCC Rcd. 16794 (rel. August 31, 1999).

[2]. *Communications Assistance for Law Enforcement Act,* Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in various sections of 18 U.S.C. and 47 U.S.C. §§ 229, 1001-1010, 1021.)

[3]. The six adopted punch-list capabilities include:
- Content of subject-initiated conference calls;
- party hold, join, drop on conference calls;
- subject-initiated dialing and signaling information;
- in-band and out-of-band signaling;
- timing information, and;
- dialed digit extraction.

[4]. The four punch-list items rejected by the court were:
- Party hold/join/drop messages;
- subject-initiated dialing and signaling information;
- in-band and out-of-band signaling information, and;
- dialed digit extraction.

[5]. 47 U.S.C. § 1005; CALEA § 106.

[6]. *Communications Assistance for Law Enforcement Act,* CC Docket No. 97-213, *Order*, 16 FCC Rcd. 17397 (rel. September 21, 2001).

[7]. *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, *Order on Remand*, 17 FCC Rcd. 6896 (rel. April 11, 2002).

[8]. The sole petition for reconsideration, filed by the Rural Cellular Association (RCA), limited itself to requesting further time for compliance of the punch-list efforts. The extension period requested passed without the FCC acting on the Petition.

[9]. Under CALEA, carriers are permitted to file for an extension giving a maximum of two years, but they may file a subsequent extension when the first is expired.

[10]. The interim J-standard describes packet-mode as a "communication where individual packets or virtual circuits of a communication within a physical circuit are switched or routed by the accessing telecommunication system. Each packet may take a different route through the intervening network(s)." *Order on Remand*, 17 FCC Rcd. at 6898, n. 12.

[11]. *America At War: Inside the FBI: CALEA*, Washington Post Live Online Chat, Dec. 31, 2001:

discuss.Washingtonpost.com/wp-srv/zforum/01/bi1220.htm

[12]. Last year, in *United States Telecom Association v. Federal Bureau of Investigation*, 276 F.3d 620 (D.C. Cir. 2002), the D.C. Circuit Court affirmed the FBI/DoJ's definitions of modifications eligible for reimbursement, agreeing that the statute could be read to limit reimbursement for capacity modifications to those specified by a carrier in its Carrier Statement. USTA filed a Petition for Rehearing of the case with the D.C. Circuit, however the petition was denied in June of 2002.

[13]. 47 U.S.C. § 1008(d); CALEA § 109(d).

[14]. In addition, a carrier may request reimbursement for such upgrades if the FCC approves the carrier's petition which asks the FCC to find that CALEA compliance is not "reasonably achievable" for equipment deployed after January 1, 1995. 47 U.S.C. § 1008(b); CALEA § 109(b).

[15]. At one point, CTIA estimated nearly $1 billion in CALEA expenses, but with approximately half of that amount representing wireless carrier's CALEA expenses. Edward Warner, *CALEA: Real Cooperation*, Wireless Week (May 24, 1999).

[16]. The FBI/DoJ has estimated that the costs could exceed the amount currently available in the 'chest' by approximately $200 million dollars. Michael P. Clifford, *Communications Assistance for Law Enforcement Act (Focus on Technology)*, The FBI Law Enforcement Bulletin 71, p. 11 (August 1, 2002).

[17]. *Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation*, Report No. 02-04, Office of the Inspector General (March 2002).

[18]. Colloquially, these exemptions from compliance have been referred to as the safe harbors, although they are not within the CALEA section 107 "safe harbor" provision. 47 U.S.C. § 1006; CALEA § 107.

[19]. 47 U.S.C. §§ 1003, 1008; CALEA §§ 104; 109.

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: 6,507,908

Secure communication with mobile hosts

A method for secure data communication with a mobile machine in which a data packet is received from the mobile machine having a particular network address. A pool of secure addresses is established, and a data structure is created to hold address translation associations. Each association is between a particular network address and a particular one of the secure addresses. If the received data packet is a secure data packet, an association between the received data packet's network address and a secure address in the data structure is identified, and the data packet's network address is translated to the associated secure address before forwarding the data packet on to higher network protocol layers. When the received data packet is not secure, it is passed on without address translation to the higher network protocol layers. For outgoing packets addressed to a secure address, the secure address is translated to a real network address (e.g., IPv4 or IPv6 addresses) and the packet payload is encrypted. Outgoing packets that are addressed directly to real network addresses pass through in a conventional manner.

Issued: January 14, 2003

Inventor: Germano Caronni

Assignee: Sun Microsystems, Inc. (Palo Alto, CA)

US Patent: 6,507,904

Executing isolated mode instructions in a secure system running in privilege rings

A method for executing isolated instructions in isolated execution mode. An execution unit executes an isolated instruction in a processor operating in a platform. The processor is configured in one of a normal execution mode and an isolated execution mode. A parameter storage contains at least one parameter to support execution of the isolated instruction when the processor is configured in the isolated execution mode.

Issued: January 14, 2003

Inventor: Carl Ellison, *et al*

Assignee: Intel Corporation (Santa Clara, CA)

Interesting references:

[1] Berg C: *How Do I Create a Signed Applet?*, Dr. Dobb's Journal, M&T Publ.; Redwood City, CA, US, vol. 22, No. 8, 8 '97; p. 109-111, 122.

[2] Gong L, *et al*: *Going Beyond the Sandbox: An Overview of the New Security Architecture in the Java Development Kit 1.2*; Proceedings of the Usenix Symposium on Internet Technologies and Systems; Monterey, CA, 13 '97; pp. 103-112.

US Patent: 6,507,762

Method and system for remotely controlling an appliance using a personal digital assistant

A method and system for remotely controlling an appliance including a first wireless communication port.

In one aspect, the method and system provide a portable digital device for remotely controlling an appliance. The portable digital device includes a processor, a second wireless communication port coupled with the processor, and a control program for use by the processor. Upon a query provided from the second wireless communication port to the first wireless communication port, an interface residing on the appliance is provided from the appliance to the portable digital device. This allows the control program to control the appliance using the interface.

In another aspect, the method and system includes providing the interface residing on the appliance.

The interface is capable of being uploaded to a portable digital device including a processor, a control program, and a second wireless communication port.

In a another aspect, the method and system includes provision of a command from the second wireless communication port of the portable digital device to the first wireless communication port of the appliance, executing the command using the appliance, and providing a response from the first wireless communication port of the appliance to the second wireless communication port of the portable digital device.

Issued: January 14, 2003

Inventor: Yousef Amro, *et al*

Assignee: International Business Machines Corporation (Armonk, NY)

US Patent: 6,507,734

Method and system which uses sound-wave-based communication to generate a secure wireless link between a handset and base station

Methods and apparatus for establishing secure wireless links between a handset and a base station in cordless telephone systems. A method of generating a secure wireless link between a handset and a base station includes initiating a linking procedure, generating a security code, transmitting the security code from a sound transmitter, receiving the security code at a sound receiver and then establishing a radio frequency link between the handset and the base station utilizing the security code. A cordless telephone system capable of generating a secure wireless link includes both a handset and a base station. The handset includes a control circuit, an RF transmitter and an RF receiver coupled to the control circuit, along with a sound receiver also coupled to the control circuit. The base station includes a control circuit, a code generation circuit coupled to the control circuit, a sound transmitter coupled to the control circuit for transmitting a code generated by the code generation circuit, and an RF transmitter and an RF receiver coupled to the control circuit.

Issued: .January 14, 2003

Inventor: Doug Berger, *et al*

Assignee: Skyworks Solutions, Inc. (Newport Beach, CA)

skyworksinc.com

Skyworks Solutions, headquartered in Woburn, Massachusetts, is focused exclusively on wireless semiconductor solutions. The company offers front-end modules, RF subsystems and cellular systems to wireless handset and infrastructure OEMs, ODMs and contract manufacturers. Skyworks' portfolio includes switches and power amplifier modules, and it offers integrated direct conversion transceivers. Skyworks has also launched products for next generation cellular handsets.

Skyworks
20 Sylvan Rd.
Woburn, MA 01801

Ph. (781) 376-3000

US Patent: 6,507,727

Purchase and delivery of digital content using multiple devices and data networks

A system facilitating the purchase and delivery of audio and video content (e.g., entertainment media) over the Internet. In a preferred embodiment of the invention, the system allows a user who hears or sees an audio or video broadcast to use a cell phone or other wireless device to order the broadcast material, and have it remotely delivered to an independent device (e.g., the user's personal computer) without further user intervention. Thus, the system allows the user to order the desired content using a wireless device that the user will often have in his or her possession when he or she hears or sees the desired content, but the user will have the content delivered to a second remote device.

Issued: January 14, 2003

Inventor: Robert Henrick

Assignee: Same

US Patent: 6,507,610

Cordless modem system having multiple base and remote stations which are interusable and secure

A cordless modem system, which includes a mobile station unit (MSU) located in the computer and a base station unit (BSU) connected to the telephone line. A radio frequency (RF) link is developed between the two units to allow a cordless connection. A series of commands are used between the two units to allow the MSU to request a channel, the BSU to grant a channel, the BSU to notify of a ring, and the MSU to request the BSU to go off hook. In addition, there is preferably a command sequence to allow authorization of a particular MSU or BSU. There are two full duplex channels in each MSU and BSU. This allows multiple BSUs and MSUs to be utilized in a small area. Communications between the two units are secure, based on address values – for each unit – contained in the various commands. The communications software utilized in the computer is not even aware of the presence of the cordless connection. Two embodiments of the MSU are provided: One configured as an external data access arrangement (DAA) to be connected with laptop modems configured to utilize external DAAs; and in a second embodiment, the MSU is incorporated with the modem hardware to provide a single, fully integrated unit. The BSU is a single, preferably relatively small, box which simply plugs into the telephone line.

Issued: January 14, 2003

Inventors: Said Saadeh and Paul Fulton

Assignee: Compaq Computer Corporation (Houston, TX)

US Patent: 6,505,238

Method and system for implementing universal login via web browser

A method for allowing remote login to a user's personal workstation. The workstation is a client terminal connected to a server within a network. The method comprises the steps of searching, from a remote location, for a login web page of the network via a web browser, and then entering a series of login credential information into a particular login request area on the web page. In response to correctly entering the login credential information into the login request area, the user is provided with a graphical user interface (GUI) of the particular user's network terminal, and the user has full access to the personal network information such as software applications stored in the memory of the client terminal. (i.e., simulating the user's client terminal GUI and providing full access to locally stored software and functional elements of the user's client terminal). In a preferred embodiment, the login credential information includes the server site,

the user identification, and the user's security password. The search for the particular web page and user's workstation using the login credential information is managed by a directory access protocol.

Issued: January 7, 2003

Inventor: Trung Tran

Assignee: International Business Machines Corporation (Armonk, NY)

US Patent: 6,505,193

System and method of fast biometric database searching using digital certificates

A system and method for conducting fast biometric database searches using iris recognition and digital certificates. Authentication of a computing platform is provided, based on digital certificates attached thereto. Fast database searching and identification of a person at the computing platform are provided, based on the digital certificate, which is used to point to a database partition having stored biometric images and an obtained biometric image, such as an iris template, which is compared to the stored biometric images in order to identify the person. Access to the database containing stored biometric images may be granted, based on the results of the digital certificate authentication process. The use of digital certificates narrows the database search to only those individuals who have authorized access to a particular computing platform by using the digital certificates. The inclusion of the iris template allows for the reliable identification of an individual at the computing platform using digital certificates both as the secure transport method and as the means to ensure the privacy of the individual and their iris template. A level of access and other entitlements to use the computing platform may also be granted to the person, based on the results of the identification process.

Issued: January 7, 2003

Inventors: Clyde Musgrave and James Cambier

Assignee: Iridian Technologies, Inc. (Moorestown, NJ)

Interesting reference:

[1] John Daugman Webpage; Cambridge University, Computer Laboratory, Cambridge, UK; printed from the Internet on Sep. 27, 28, and 29, 1999; 34 pages.

US Patent: 6,505,046

Method and apparatus for distributing location-based messages in a wireless communication network

The process and network processes a mobility origination message, derives the subscriber's location and constructs a set of coupons or advertisements based on that location, for that subscriber, and at that particular time. The coupons or advertisements are then transmitted to the subscriber's handset. A retailer enters the various advertisements or coupons into the network for transmission to subscribers who call a predefined telephone number.

Issued: January 7, 2003

Inventor: Steven Baker

Assignee: Nortel Networks Limited (St. Laurent, CA)

US Patent: 6,504,907

Call detail reporting for lawful surveillance

A lawfully authorized electronic surveillance operation requires reporting of detailed call data for a variety of calls associated with the subject of the surveillance. For at least some specified calls to or from the subject, the invention provides profile data in a switching office serving the subject that causes the office to generate accounting messages for each call, essentially in the same manner as for billing, regardless of whether the calls are billable. Accounting records formed from the messages are uploaded to a server system, for processing and formatting as necessary, for delivery to the law enforcement agency. The surveillance could entirely rely on these accounting records for the data reporting. In the preferred embodiments, however, the surveillance also involves monitoring of common channel signaling messages to accumulate call detail records for surveillance purposes with respect to many calls associated with the subject. The preferred embodiment utilizes a special CLASS code, set against the subject's profile in the serving end office. The CLASS code in the profile causes that office to produce the accounting messages for each of the subject's calls processed through the office that does not involve a monitored form of interoffice signaling.

Issued: January 15, 2003

Inventor: Robert Farris, *et al*

Assignee: Verizon Services Corp. (Arlington, VA)

Interesting references:

[1] Lucent Technologies. *Local Number Portability.* May 28, 1998. p. 1-2.

[2] Siemens Telecom Networks. *Topic 5: Siemens Telecom Networks: Local Number Portability: Tomorrow's Network – the Location Routing-Number Architecture.* Apr. 2, 1998. p. 1-4.

[3] USTA. *Local Number Portability (LNP): Overview of LNP.* Apr. 2, 1998. p. 1.

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