Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: wsp@cnp-wireless.com Vol. 3, No. 6. July, 2001

CryptoNews: New Federal Cryptography Standard Approved

On 27 June, the US Department of Commerce formally approved the Federal Information Processing Standard (FIPS) 140-2. This FIPS – *Security Requirements for Cryptographic Modules* – will replace FIPS 140-1, setting a new benchmark for minimum levels of cryptography in federal security products. FIPS140-1 has served as the *de facto* cryptographic module standard since 1994. Numerous standard-setting bodies and international testing organizations have used FIPS 140-1, which provides federal government employees with guidelines for computer security purchasing decisions.

According to its authors, FIPS 140-2 has been updated to reflect changing technology. It does not differ drastically from the preceding specification. The new security specification outlines the security requirements that must be satisfied by a cryptographic module. It covers more than 10 areas related to the "design and implementation of a cryptomodule," including: Cryptographic key management; identity-based authentication; physical security; operational environment; electromagnetic interference/ electromagnetic compatibility (EMI/EMC); ports and interfaces; and self-tests. For instance, the new security specification, in the physical security requirements area, mandates that products provide tamper-evident coatings or seals, or pick-resistant locks. FIPS140-2 provides four increasing levels of security, intended to cover a wide range of potential operating environments and applications. Level 4, the highest security level, builds upon the other requirements, and it includes a zeroize requirement – the ability to electronically erase information in the certain circumstances.

For information on FIPS140-2, visit the NIST (National Institute of Standards and Technology) web-site. Visitors to the site (csrc.nist.gov/cryptval) can obtain a white paper detailing the differences between FIPS 140-1 and FIPS 140-2. To download the specification, click on:

csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Also, Federal security standards consulting company, Corsec (www.corsec.com), has written a FIPS 140-2 whitepaper, located at:

www.corsec.com/fips_whitepaper.php

FIPS 140-2 will go into effect November 25, 2001

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

About Wireless Security Perspectives

Price

The basic subscription price for *Wireless Security Perspectives* is $300 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$350 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…

August 15th, 2001.

Future Topics

Wireless Packet Data Security • AES (Rijndael) • m-Commerce Security • IP Security • Public Keys & Wireless • IP Mobility Security • Security Issues in Ad hoc Wireless Networks • Electronic Signatures in Wireless • Latest in Watermarking

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**: $300 for delivery in the USA or Canada, US$350 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: Les Owens.
Article Sourcing: Betsy Harter.
Production: Doug Scofield.
Distribution: Debbie Brandelli.
Marketing: Muneerah Vasanji.
Accounts: Evelyn Goreham.
Publisher: David Crowe.

Encryption and Export Controls

Frank Quick

Encryption always has been subject to export controls from the United States government. Over the years, these controls have caused some special problems for the Telecommunications Industry Association (TIA), which oversees the development of standards for TDMA (IS-54 through ANSI-136) and CDMA (IS-95 through IS-2000 and beyond) cellular and PCS telephone systems, as well as analog cellular (IS-3 through EIA/TIA-553 and IS-91) incorporating security algorithms. These complications have also trickled into other standards bodies. Although standards must be developed in a due process environment where the proposed standards text must be freely available for examination and content, export limitations and privacy procedures restrict the free availability of these standardized algorithms.

Before 1996: ITAR

Commerce is the world's oldest industry, and U.S. export regulations go back hundreds of years. Prior to 1996, encryption was controlled by the U.S. Department of State, under the International Traffic in Arms Regulations (ITAR). At the time, encryption equipment, software and algorithms were treated in the same manner as armament and other military equipment. This led to some amusement, such as Matt Blaze's famous *My Life as an International Arms Courier* [1] – a recounting of his misadventure when he attempted to follow the rules by declaring the encryption code in his laptop computer when leaving the United States. These laws also led to some problems for TIA. When TR45.3 began to discuss privacy procedures for the first cellular standard to incorporate authentication and encryption (IS-54-B), representatives of the U.S. government came to the meeting and stated that such topics could not be discussed in the presence of foreign persons. "Foreign" was later defined to mean someone who is not a permanent resident of the United States or Canada.

TIA subcommmittee TR-45.3 accepted the policy to exclude foreigners from the portions of its meetings which included such discussions of sensitive documents, in order to abide by ITAR, but the TIA Engineering Guidelines forbade holding a standards meeting with restricted attendance. This dilemma was solved by implementing a rather convoluted policy:

- Because TIA rules require open attendance only for formulating groups (i.e., groups within TIA that are authorized to create public standards), an ad hoc non-formulating group could be created with special operating rules, allowing it to close meetings to persons not satisfying the residency requirement. In 1991, the Ad Hoc Authentication Group (AHAG) was formed under TR45.3 for this purpose.
- To incorporate encryption methods into standards, the AHAG could create documents withrestricted distribution, but which could be incorporated into standards as normative referenences by the formulating groups. Appendix A of *IS-54-B* was created and managed in this manner.
- Rather than publishing openly, TIA would hold the AHAG documents, with distribution restricted to U.S. and Canadian entities. To satisfy the need for open review of all normative parts of a proposed standard, an export license would be obtained, allowing the documents to be sent outside the United States and Canada to those foreign parties reviewing the proposed standards.

In 1992, a second TIA subcommittee, TR45.5, was formed to create a digital cellular standard based on CDMA. TR45.5 also wanted to support user privacy, and they decided to use the same network procedures and key management algorithms developed by TR45.3. To allow the AHAG to support both subcommittees, AHAG was moved from TR45.3 to the parent committee, TR-45, with the same operating rules.

TIA TR-45 Ad Hoc Authentication Group (AHAG) Chairmen

1991-92	Richard Levine (SMU)
1992-93	Alan Angus (NovAtel)
1993-96	Les Owens (GTE Labs)
1996 -	Chris Carroll (GTE Labs)

Shortly after moving to the committee level, the AHAG produced the export-controlled document, *Common Cryptographic Algorithms*, containing the same algorithms as in Appendix A of *IS-54-B*, but packaged in such a way that the algorithms could be referenced by either TR45.3 or TR45.5. A companion document, *Interfaces to Common Cryptographic Algorithms*, provided enough information for the formulating groups to specify the setting of the inputs and the use of the outputs of the algorithms, without requiring an export license for access to the document.

Under ITAR, there were very strict limits on the strength of encryption algorithms allowed for export in cellular equipment. In 1991, key size was limited to 32 bits for encryption of user data. Today, of course, a 32-bit key would be seen as a joke, since a brute-force attack by guessing the key only takes today's PCs a few minutes. Before the end of ITAR control of cellular encryption, the key size limit was raised to 40 bits. This is still not very impressive by current standards, although you will still find many Web browsers that only offer 40-bit SSL encryption.

Stronger algorithms were permitted for authentication. In fact, authentication itself was not export controlled, but TIA algorithms for authentication fell into another trap: The authentication process created the encryption keys, hence they were controlled anyway. Thus the size of the root authentication key was limited to 64 bits because it set the strength of the derived encryption keys.

When new algorithms were considered, AHAG needed to consult with the U.S. government about the exportability of those algorithms. These consultations were provided by the export control

Upcoming Fraud and Security Events

The following are several upcoming fraud and security conferences that may be of interest to the wireless security practitioners.

The Blackhat Briefings '01
11-12 July, 2001
Caesars Palace
Las Vegas, NV
www.blackhat.com/html/bh-usa-01/bh-usa-01-index.html

SANSFIRE (SANS Forensics, Investigations, Response & Education)
30 July – 4 August, 2001
Omni Shoreham
Washington, DC
www.sans.org/sansfire/sansfire.html

Electronic Signatures
21-22 August 2001
Toronto, Ontario
www.iqpc.com/cgi-bin/templates/9945204041634826660150002/genevent.html?event=1704&topic=82

Crypto 2001
19-23 August 2001
Holiday Inn
Santa Barbara, CA
www.iacr.org/conferences/c2001

Second Modes of Operation Workshop (Modes of Operation for Symmetric Key Block Ciphers)
24 August 2001
Holiday Inn
Santa Barbara, CA
csrc.nist.gov/encryption/modes/workshop2/index.html

Usenix Security Symposium
13-17 August 2001
JW Marriott
Washington, DC
www.usenix.org/events/sec01

The Conference on Mobile & Wireless Security
24-25 September 2001
Atlanta
www.misti.com/conference_show.asp?id=MWS

Plastic Card and Online Fraud Prevention
24-25 September 2001
Hotel Inter-Continental
Zurich, Switzerland
www.iir-conferences.com/site/_prod-grp.cfm?DirName=KJ1823&ConfCode=KJ1823&iv=23

3G Technical Fraud
30-31 October 2001
The Forum Hotel
London
www.iir-conferences.com/site/_prod-grp.cfm?DirName=cg1074&ConfCode=cg1074&iv=23

group at the National Security Agency (NSA), since the Department of State relied on NSA for such decisions. There were many pilgrimages to Fort Meade, MD, to talk to NSA, and NSA often sent representatives to AHAG for direct discussion of the export rules.

After 1996: EAR

On November 15, 1996, Executive Order 13026 (61 FR 58767) transferred control of commercial encryption exports from the ITAR under Department of State to the Export Administration Regulations (EAR [2]) under the Bureau of Export Administration (BXA [3]) of the Department of Commerce (DoC). While this ended the treatment of encryption as "arms," it created other problems because the DoC was unprepared for the wave of new export issues that arrived on its doorstep.

Under ITAR, NSA had placed some of its staff in the Department of State to speed up the license review process. Under the DoC, however, NSA no longer played a pivotal role in license review. Instead, NSA became only one of several government agencies required to approve licenses. Pilgrimages to Fort Meade were no longer sufficient: One needed to consult the Department of Defense, FBI and other agencies to deal with license issues, and it was often difficult to find the individuals who should be contacted.

Furthermore, the transfer from ITAR to EAR made no immediate change in the criteria for export control. AHAG and TIA continued to operate in the same manner as they had under the ITAR.

During this period, however, events were overcoming the export regulators. Appendix A of IS-54-B was leaked and posted on Web sites all over the world. Some of the algorithms were shown to be even weaker than their design. This seems to be an inevitable consequence of designing algorithms so that they have a large key, when in fact, they can be broken in fewer steps than required by brute-force key guessing. Someone usually finds that the intentional weakness creates an unintentional one, making the algorithm weaker than desired.

Meanwhile, experts outside the United States and Canada were creating encryption algorithms that were as strong as any. (For example, the Advanced Encryption Algorithm selected by NIST to replace DES was developed in Belgium.) These algorithms were often published and freely available so that attempts to restrict algorithm exporting from the United States had no effect except to reduce U.S. influence on cryptography. After a few years, the United States and its partners in the Wassenaar agreement relented – to a certain extent.

Current Regulations: License Exception TSU

In many ways, the EAR still looks the same as ever, but there is one very important change which allowed the AHAG to modify its operating procedures a bit. 15 CFR 740.13(e)(1) defines a license exception, "Technology and Software - Unrestricted" (TSU), that applies to publicly available source code. This exception is subject to a long list of

conditions, but it does allow AHAG to post its proposed documents on a publicly accessible web site (ftp.tiaonline.org/tr-45/tr45ahag/public%20documents [4]). With this procedure, it is now possible for AHAG to make its documents available for general review without requiring an export license.

Caveat: Exceptions to the Exception

The EAR gives you a number of things you should consider before rushing to post encryption source code on the Web:

- The source code must be "considered publicly available under §734.3(b)(3) and … not subject to an express agreement for the payment of a licensing fee or royalty for commercial production or sale of any product developed with the source code."
  However: "Intellectual property protection (e.g., copyright, patent or trademark) will not, by itself, be construed as an express agreement for the payment of a licensing fee or royalty for commercial production or sale of any product developed using the source code." This could be interpreted to mean: You have to give away the source code itself, even though there may still be patents on the algorithms. You could, apparently, charge a license fee for your patents, and still claim exemption TSU for export of source code implementing those patents, as long as you don't charge a fee for use of the source code itself. No doubt a clever lawyer would argue the opposite; hence, don't try this at home without legal advice.
- You have to send BXA a copy of the source code – or you must send them the URL where the code will be posted – prior to posting it.
- "You may not knowingly export or re-export source code or products developed with this source code to Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria." Some lawyers claim this includes telling someone from those countries the URL where the code is posted. Thus, this issue of *Wireless Security Perspectives* may be an export-controlled item!

More Caveats

The creation of license exception TSU does not eliminate the controls on encryption. All it does is to reduce (somewhat) the insanity by no longer controlling the export of information already freely available outside the United States. Several things still have to be considered:

- Deemed Export

  Giving controlled items to a foreign national while inside the United States or Canada is still considered an export and is subject to the EAR. You can, of course, give such a foreign person source code under exception TSU, but you have to send a copy to BXA first.
- End-to-End Encryption

  "Cellular" phone equipment containing encryption is exempt from encryption export controls (though not from other export controls), provided the equipment does not support end-to-end encryption. Note that the initiatives in 3GPP to define end-to-end encryption capability for 3G handsets would place export restrictions on those handsets.
- User-Supplied Encryption

  You can't get around the encryption export restrictions by shipping products that have no encryption included if they can easily be adapted by inserting encryption at the destination. Products with this design are explicitly export controlled.
- Technology

  Finally, there is the infamous *technology* category. This is a separate subsection in each part of the export regulations, intended to control the export of things that would enable foreign entities to create their own designs for restricted items. For example, export category 5E002 controls: *Technology* according to the General Technology Note for the *development*, *production* or use of equipment controlled by 5A002 or 5B002 or *software* controlled by 5D002.

  Items in italics are formally defined within the EAR, though the definitions can seem very broad and confusing. For example (15 CFR 772):

  > "*Development*. (General Technology Note) is defined as anything related to all stages prior to serial production, such as: Design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, layouts."

  This definition is very broad. Together with the deemed export rules, this means that, in most cases, a license is needed to permit the export of "technology" to each foreign national working for a telecommunications manufacturer.

The Future of EAR

The Wassenaar partners continue to meet, and changes to the export regulations continue to be discussed. U.S. manufacturers are currently lobbying for relaxed controls on technology for digital cellular and PCS systems, but there seems to be resistance from some other countries to such changes. What can the industry do to influence the process?

The DoC sponsors Technical Advisory Committees (TACs) providing input to Commerce from U.S. industry on export matters. The Information Systems TAC (ISTAC) has responsibility for computers, integrated circuit manufacture and telecommunications. It meets four times per year, usually at the DoC building in Washington, D.C. Typically, the ISTAC provides the DoC with industry updates on emerging technology, assists in the review and interpretation of Wassenaar proposals, and suggests changes to the EAR. Those in other countries may find similar groups in their government's export administration.

The telecommunication industry is under-represented at the ISTAC, whose membership is mainly involved in computers and integrated circuits. Membership on a TAC is by appointment. Interested U.S. parties should visit the

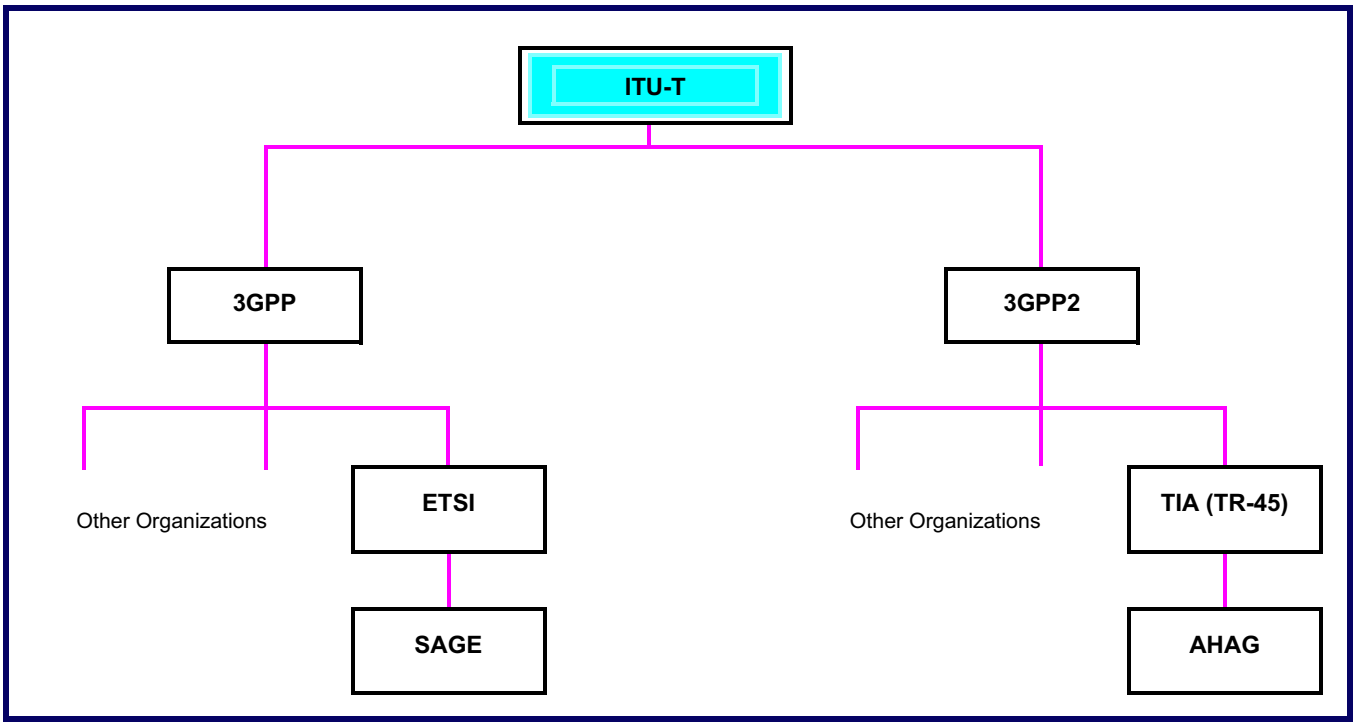
TAC Web site listed below, and consider application for membership.

The Future of AHAG

Export restrictions have eased slightly over the past few years, allowing AHAG to post its controlled documents for public review. While no foreign nationals have attended AHAG in recent months, they could, in principle, do so by downloading encryption-related documents prior to the meeting. It may not be practical to notify BXA in advance when passing out paper copies of documents. Thus, with the proper operating procedures, it should no longer be necessary to close AHAG meetings to foreign persons. Taking this to its logical extreme, there should really be no need for a special ad hoc group, since it would seem that a formulating group could operate under the proper rules for discussion of encryption.

We have, however, only examined the situation with TIA, which operates under U.S. law. Other entities, such as 3GPP, 3GPP2 and ITU, operate internationally. These organizations (especially ITU) can meet anywhere, and they can have representatives from any country in attendance, including countries embargoed by the United States. This is no small problem: As a test, QUALCOMM applied for an export license to present cryptographic algorithms to ITU. The license was denied because of the likely presence of representatives from Syria, Cuba and other embargoed countries. Thus, ITU in particular cannot have an AHAG-like entity within it. This organization must rely on regional standards bodies such as TIA to create encryption standards. 3GPP and 3GPP2 have solved the issue by relying on ETSI (SAGE) and TIA (AHAG), respectively, to perform their algorithm development. Figure 1 depicts the relationships between these organizations.

Figure 1: Cryptographic Standards Development Groups



These factors make it very likely these specialized groups will continue to exist. Such groups within regional standards organizations will continue to oversee the development of encryption algorithms. In principle, every regional standards organization could have its own group, though the proliferation of regional security algorithms would be likely to interfere with compatibility of terminals roaming internationally. This situation must be weighed carefully against the possible desire for security tailored to regional requirements.

It is unlikely TIA will give up its security development capability to rely on a standards body outside the United States. AHAG will probably continue its role in algorithm development for TIA for the foreseeable future.

About the Author

Frank Quick is Senior Vice President, Engineering, in the Corporate Research and Development group at Qualcomm Incorporated, in San Diego, California. He is a graduate of MIT and Carnegie-Mellon University. He has been Vice Chair of the TR-45 AHAG since 1994, and he is the editor of the AHAG's authentication and encryption specifications.

References

[1]. Matt Blaze's *My Life as an International Arms Courier* can be found at www.crypto.com/papers.

[2]. The Export Administration Regulations are available at www.access.gpo.gov/bxa/ear/ear_data.html.

[3]. Information on the BXA Technical Advisory Committees can be found at bxatac.doc.gov.

[4]. *Common Cryptographic Algorithms* and other AHAG public documents can be accessed at ftp.tiaonline.org/tr-45/tr45ahag/public%20documents

Fraud And Security Patent News

The US Patent and Trademark Office (UPTO) recently granted the following 15 fraud and security patents. The patent number, invention title, inventor, and assignee (owner) are provided. All of these patents issued in either June or July 2001.

These may be of interest to some of our wireless security practitioners. 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, the references cited or other references included in the patent. For select patents provided below, we provide the URL for the assignee.

US Patent: 6,256,514

Secure radio personal communications system and method

Inventors: Paul Dent and Jacobus Haartsen

Assignee: Ericsson, Inc.

US Patent: 6,253,193

Systems and methods for the secure transaction management and electronic rights protection.

Inventors: Karl Ginter et. al.

Assignee: InterTrust Technologies Corporation (www.intertrust.com and www.metatrust-certified.net)

US Patent: 6,249,777

System and method for remote postage metering

Inventors: Salim Kara and Martin Pagel

Assignee: E-stamp Corporation (www.e-stamp.com)

US Patent: 6,249,585

Publicly verifiable key recovery

Inventors: David McGrew and David Carman

Assignee: Network Associates, Inc. (www.nai.com)

US Patent: 6,249,575

Telephony security system

Inventors: Craig Heilman and Todd Beebe

Assignee: SecureLogix Corporation (www.securelogix.com)

US Patent: 6,243,815

Method and apparatus for reconfiguring and managing firewalls and security devices

Inventors: Anand Antur et. al.

Assignee: Inventors

US Patent: 6,243,695

Access control system and method therefor

Inventors: Khaled Assaleh and William Campbell

Assignee: Motorola, Inc.

US Patent: 6,240,402

Charge allocation in a multi-user network

Inventor: Nicolas Lynch-Aird

Assignee: British Telecom

US Patent: 6,237,095

Apparatus for transfer of secure information between a data carrying module and an electronic device

Inventors: Stephen Curry, Donald Loomis and Christopher Fox

Assignee: Dallas Semiconductor Corporation (www.dallassemiconductor.com)

US Patent: 6,236,851

Prepaid security cellular telecommunications system

Inventors: Douglas Fougnies and Dan Harned

Assignee: Freedom Wireless, Inc. (www.freedomwireless.com)

US Patent: 6,233,565

Methods and apparatus for internet based financial transaction with evidence of payment

Inventors: Richard Lewis et. al.

Assignee: Saranac Software, Inc. (www.saranacsoftware.com)

US Patent: 6,233,446

Arrangement for improving security in a communication system supporting user mobility

Inventor: Thanh Van Do

Assignee: Telefonaktiebolaget LM Ericsson

US Patent: 6,233,234

Secure LAN/internet telephony

Inventors: James Curry and Robert Farris

Assignee: Bell Atlantic Network Services, Inc.

US Patent: 6,226,511

Method and apparatus for configuration of authentication center operations in a mobile telephone system

Inventors: Pamela Jacobs and James Lamb

Assignee: Compaq Computer Corporation

US Patent: 6,219,793

Method of using fingerprints to authenticate wireless communications

Inventors: Yang Li et. al.

Assignee: Hush, Inc. (www.hush.com – provider of HushMail.com)

To review the specification and claims of these patents visit the US Patent and Trademark Office web-site at www.uspto.gov. To obtain a copy of one of these patent number from 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