Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: wsp@cnp-wireless.com Vol. 3, No. 11. December, 2001

Cryptography in the News

U.S. Government Approves AES

On December 4, the United States Secretary of Commerce announced approval of the Advanced Encryption Standard, or AES – the new information technology encryption standard for the federal government. U.S. Government organizations may use AES to protect sensitive, unclassified information. The National Institute of Standards and Technology (NIST) also anticipates AES will be used by other individuals, organizations, and institutions both inside and outside of the U.S. The new cryptography standard is published as Federal Information Processing Standard 197. To obtain FIPS197, visit:

csrc.nist.gov/publications/fips/fips197/fips-197.pdf

The NIST announcement brings to an end the 4-year long effort by the Commerce Department to select a highly-secure algorithm for the AES. In August 1998, NIST began the review process with 15 candidate cryptographic algorithms that were "attacked" for vulnerabilities and scrutinized by the worldwide cryptographic community. The list of candidate algorithms was then narrowed to five in April 1999. Finally, just slightly more than one year ago, in October 2000, NIST chose the Rijndael cryptographic algorithm for the AES. Rijndael, pronounced "Rhine-doll," was developed by Belgian cryptographers Joan Daemen and Vincent Rijmen – two highly respected international cryptography experts.

Rijndael is a symmetric block encryption algorithm. The algorithm supports key sizes of 128, 192 and 256 bits. For a 128-bit key, the "key space" is approximately 3.4×10^{38}. Perhaps it helps to think of such a huge number this way: The number of possible keys for a 128-bit key is approaching the number of atoms in the planet. For a 256-bit key, there are a staggering 1.1×10^{77} possibilities! In contrast, the 56-bit Data Encryption Standard, or DES – the algorithm that is being replaced for government use – has a mere key space of only 7.2×10^{16} keys. NIST believes that, given the unlikeliness of exhaustive 'brute force' key search attacks being feasible, AES will remain secure for more than 20 years, even after factoring in advances in technology.

The Rijndael algorithm was chosen because a number of factors, including: Cryptographic security, efficiency, performance, flexibility, and ease of implementation. In particular, NIST notes that Rijndael:

- Performs well in both hardware and software across a wide range of computing environments;
- Has very low memory requirements, which makes it well suited for space-constrained environments (such as wireless devices); and
- Has mathematical operations that efficiently defend against power and timing attacks.

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…

January 15th, 2002.

Future Topics

Wireless Packet Data Security • IP Security • Public Keys & Wireless • IP Mobility Security • Security Issues in Ad hoc Wireless Networks • Electronic Signatures in Wireless • Latest in Watermarking • Security for PDAs •

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.

Upcoming Fraud and Security Events

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

Cybercrime on Wall$treet
10-11 January 2002
New York, NY
www.iirusa.com/cybercrimeonwall$t/Index.cfm/Link=1

SANS Peachtree 2002
18-24 January 2002
Atlanta, GA
www.sans.org/Peachtree02.htm

COMNET Conference & Expo
28-31 January 2002
Washington Convention Center
Washington, DC
www.comnetexpo.com

Prepaid Wireless Services 2002
29 January - 2 February 2002
JW Marriot Hotel
Miami, FL
www.iirusa.com/prepaid/Index.cfm/Link=11

2nd Annual CyberSABOTAGE! – Combating Online Credit Card Fraud and Cybercrime
30 January - 1 February 2002
JW Marriot Hotel
Miami, FL
www.marcusevansconferences.com

Second Annual Privacy and Data Security Summit
30 January - 2 February 2002
Hyatt Regency on Capital Hill
Washington, DC
www.privacyassociation.org/html/conferences.html

The Conference on Mobile and Wireless Security
12-13 February 2002
Caesars Palace
Las Vegas, NV
www.misti.com

Information on Rijndael is available at:

csrc.nist.gov/encryption/aes/rijndael

This site includes reference code, test values, intellectual property (IP) statements, and specifications. NIST notes that the Rijndael will be made available royalty-free.

For more information on the official AES announcement, contact Jim Dyke or Trevor Francis at (202) 482-4883, or visit:

www.nist.gov/public_affairs/releases/g01-111.htm

New cdma2000 Security Group

Frank Quick
V.P. Engineering
Qualcomm

In July, 2001, the 3GPP2 Steering Committee approved new Terms of Reference for TSG-S, adding security as a new responsibility. Specifically, a bullet item in the Terms of Reference which read

> "- System Reference Model Development and Maintenance"

was replaced by:

> "- Management, technical coordination, as well as architectural and requirements development associated with all end-to-end features, services, and system capabilities including, but not limited to, security and QoS (Quality of Service)."

This change was made in response to proposals from Qualcomm and other companies. The proposals were intended to move the development of CDMA2000 security requirements and architecture to 3GPP2 from the TIA TR-45 AHAG, where most such work took place in the past. The AHAG, as a TR-45 entity, serves both the CDMA and TDMA communities within TR-45. Moving CDMA security development to 3GPP2 allows 3GPP2 to develop CDMA security requirements within the cdma2000 community.

In response to this change in the Terms of Reference, TSG-S Working Group 4 (WG4) was formed in August, 2001 to perform security requirement and architecture development for TSG-S. Frank Quick (Qualcomm) was appointed to the position of Chair. Michael Marcovici (Lucent Technologies) and Masayoshi Ohashi (KDDI Laboratories) were appointed joint Vice-Chairs.

Working Group 4 held its second meeting in Shenzhen, China on October 30, 2001. It is presently working on security requirements for IP multi-media services, and it is coordinating the transfer of other work items from the TR-45 AHAG to WG4. WG4 expects to meet in the same location as the TSG-S plenary throughout 2002.

TIA TR-45 AHAG will retain responsibility for cryptographic algorithm specifications for the immediate future. 3GPP2 is not likely to attempt to develop algorithm specifications until the relevant export and import laws in the 3GPP2 partner countries are fully under-

. . . More Upcoming Events

RSA Conference 2002
18-22 February 2002
McEnery Convention Center
San Jose, CA
www.rsasecurity.com

Internet World Wireless East 2002
20-22 February 2002
Jacob Javits Center
New York, NY
www.internetworld.com/events/weast2002

Network Infrastructure Security Conference
25-27 February 2002
Park Hyatt
Washington, DC
www.iirusa.com/networksecurity/Index.cfm/Link=1

Mobile Business for the Enterprise
13-15 February 2002
McCormick Place
Chicago, IL
www.dci.com/brochure/mbchi

stood, and until suitable working procedures are determined. If proposed procedures are not satisfactory for all partner countries, algorithm specification work will need to remain in the regional standards development organizations, in which case the AHAG (representing the United States) may be expected to play a major role.

###

Editor's note: At first glance, it seems apparent that TIA AHAG should dissolve and be totally replaced by 3GPP2 TSG-S. TDMA standards, however, still have a significant presence in the TIA, and they rely on AHAG specifications. While TDMA (TIA/EIA-136) has a limited life span in North America (most major TDMA carriers have declared allegiance to GSM and Wideband CDMA), this is still measured in years, and maintenance of the security standards for TDMA will still be required. Consequently, one can anticipate that the AHAG will slowly decline in productive work as the TIA/EIA-136 work also diminishes.

Fraud And Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following fraud and security patents on December 11, 2001. The patent number, invention title, inventor, assignee (owner), and an invention description are provided.

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, contact information, and some information about the assignee.

For a complete analysis of the applicability, efficacy and merit of the patents below, contact the editors of *Wireless Security Perspectives*.

US Patent: 6,330,678

Block cipher method

Issued: December 11

Inventor: Frank C. Luyster

Assignee: Same

Invention: A multi-round data encryption system is presented. It encrypts an n-bit block of input, where n is preferably 128 bits or more.

US Patent: 6,330,677

Object-based security system

Issued: December 11

Inventor: Ashraf Madoukh

Assignee: Sprint Communications Company, L. P. (Kansas City, MO)

Invention: The invention is for authentication of processes and inter-process messaging.

US Patent: 6,330,675

System and method for secure transfer of digital data to a local recordable storage medium

Issued: December 11

Inventor: Philip Wiser et. al.

Assignee: Liquid Audio, Inc. (Redwood City, CA)

Invention: A device securely decrypts and writes an encrypted digital file to a local recordable storage medium using two decryption engines.

www.liquidaudio.com

Contact:

Liquid Audio, Inc.
800 Chesapeake Dr.
Redwood City, CA 94063

Telephone: (650) 549-2000

Liquid Audio provides software and services for Internet music delivery. This patent enables musicians, record labels, Web sites, music retailers and other businesses to publish, distribute and sell music online with copy protection and copyright management.

US Patent: 6,330,674

Use of biometrics as a methodology for defining components for ECC encryption

Issued: December 11

Inventor: Michael Angelo et. al.

Assignee: Compaq Computer Corporation (Houston, TX)

Invention: A method for defining the elliptic curve for purposes of elliptic curve encryption using biometrics such as a fingerprint to define the elliptic curve equation's coefficients.

US Patent: 6,330,671

Method and system for secure distribution of cryptographic keys on multicast networks

Issued: December 11

Inventor: Ashar Aziz

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

Invention: A method and apparatus providing secure and scalable key management in a multicast network environment.

US Patent: 6,330,670

Digital rights management operating system

Issued: December 11

Inventor: Paul England et. al.

Assignee: Microsoft Corporation (Redmond, WA)

Invention: A digital rights management operating system protects rights-managed data, such as downloaded content, from access by untrusted programs while the data is loaded into memory or on a page file as a result of the execution of a trusted application that accesses the memory.

US Patent: 6,330,668

Integrated circuit having hardware circuitry to prevent electrical or thermal stressing of silicon circuitry

Issued: December 11

Inventor: Andreas Curiger et. al.

Assignee: Dallas Semiconductor Corporation (Dallas, TX)

Invention: An integrated circuit, such as a microprocessor, which incorporates hardware mechanisms to prevent the circuitry from operating outside the proper bounds of design (clock speeds, temperatures and voltages).

US Patent: 6,330,660

Method and apparatus for saturated multiplication and accumulation in an application-specific signal processor

Issued: December 11

Inventor: Kumar Ganapathy

Assignee: VxTel, Inc. (Fremont, CA)

Invention: An application-specific signal processor (ASSP) performing vectorized and nonvectorized operations. This ASSP is also suited to handling voice and data compression/decompression in telecommunication systems where a packetized network is used to transceive packetized data and voice.

US Patent: 6,330,608

Method and system of a computer system for establishing communication between a service provider and a central service factory and registry in a computer system

Issued: December 11

Inventor: Ian Stiles

Assignee: Stiles Inventions L.L.C. (Salem, UT)

Invention: A system and method for registering computer software modules to allow or reject it for opportunities of interacting with a computer system – hardware and software – and receiving service requests.

US Patent: 6,330,586

Reconfigurable service provision via a communication network

Issued: December 11

Inventor: Martin Yates et. al.

Assignee: British Telecommunications Public Limited Company (London, GB)

Invention: A services provision system providing information services over one or more communications networks. It includes a software infrastructure divided into domains providing access control to functionality at different levels with security against fraudulent use.

US Patent: 6,330,562

System and method for managing security objects

Issued: December 11

Inventor: Edward Boden et. al.

Assignee: International Business Machines Corporation (Armonk, NY)

Invention: A data model for abstracting customer-defined VPN security policy information. The model can dynamically manage secure connections at the IP level with other VPN's. Its tasks include negotiation, creation, deletion and maintenance of the connection.

US Patent: 6,330,347

Method and device for identifying fingerprints using an analog flash memory

Issued: December 11

Inventor: Zsolt Vajna

Assignee: STMicroelectronics S.r.l. (Agrate Brianza, IT)

Invention: A method for identifying fingerprints, which includes: The steps of acquiring a primary image and a secondary image; determining notable points in the primary image; comparing with one another the primary image and the secondary image (from a flash cell array) in order to identify the correspondences between the primary image and the secondary image; and validating the possible correspondences.

Contact:

STMicroelectronics
1000 East Bell Road
Phoenix, Az 85022
Telephone: (602) 485-6100

eu.st.com

STMicroelectronics is a global independent semiconductor company that designs, develops, manufactures and markets a broad range of semiconductor integrated circuits (ICs) and discrete devices used in a wide variety of microelectronic applications, including telecommunications systems, computer systems, consumer products, automotive products and industrial automation and control systems.

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 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

Try a little fun @ ...

www.cnp-wireless.com/quiz.html

Try some of the old ciphers to see how much about the wireless heritage. Les' quiz question from September remains unsolved.

Winners have a prize coming to them. Cheaters . . . well, check it out to see what you get.

Enjoy the light-hearted spirit of the wireless world, and if you have a quiz question you would like to share, send it to:

wsp@cnp-wireless.com

New Wireless Security Solution for 802.11's WEP

It has been reported widely now for nearly a year, that the standard which specifies the methods for encrypting data on the 802.11 wireless LANs – WEP (Wired Equivalent Privacy) – is insecure. The insecurities of the WEP protocol make wireless LANs highly vulnerable to attack, presenting potentially significant risks for businesses that have deployed this wireless technology. Financial transactions of many types and any of an organization's proprietary information broadcast on the wireless links could be compromised by determined adversaries. RSA Security Inc. recently announced that it helped create a more secure solution for the encryption standard in WEP. The solution, called "Fast Packet Keying," is designed to generate a unique RC4® cryptographic (see **note** on this page) key for each data packet sent over the wireless LAN. Customers who have deployed WLAN technology can quickly update the existing vulnerable equipment with the solution. Wireless LAN vendors will simply provide the solution to customers as a software (or firmware) patch.

The weaknesses in WEP are not flaws in the actual RC4 cryptographic algorithm. Instead, the weaknesses stem from how the keys for different data packets are derived from the secret root key shared between wireless terminals and access points (AP). "Fast Packet Keying" is designed to rapidly and efficiently generate keys which are adequately dissimilar.

This solution was developed by RSA Security, Hifn and other members of the IEEE 802.11 committee. Co-developer, Hifn, believes organizations can now "safely turn to wireless networks for operational flexibility and efficiency without sacrificing the integrity of their systems." The IEEE 802.11 committee has already accepted the scheme.

For more technical information on the "Fast Packet Keying" solution, visit:

www.rsasecurity.com/rsalabs/index.html

For more information on Hifn, phone: +1-408-399-3500 or visit:

www.hifn.com

For more information on RSA Security, visit:

www.rsasecurity.com

Note: RC4® is the "Rivest Cipher #4," a variable-key-length symmetric stream cipher. It was invented by Ron Rivest for RSA Security in 1987 as an alternative to DES for fast bulk encryption. It is at least ten times as fast as DES in software and very compact in terms of code size, while being immune to many crypanalytic attacks. It has been widely used by developers who want to export their products. For more information, visit:

www.achtung.com/crypto/rc4.html

Figure 1 below depicts RC4 in the WEP protocol of 802.11 wireless LAN technology.

Figure 1: Simplified View of RC4® in WEP