Wireless Security Perspectives

Cellular Networking Perspectives

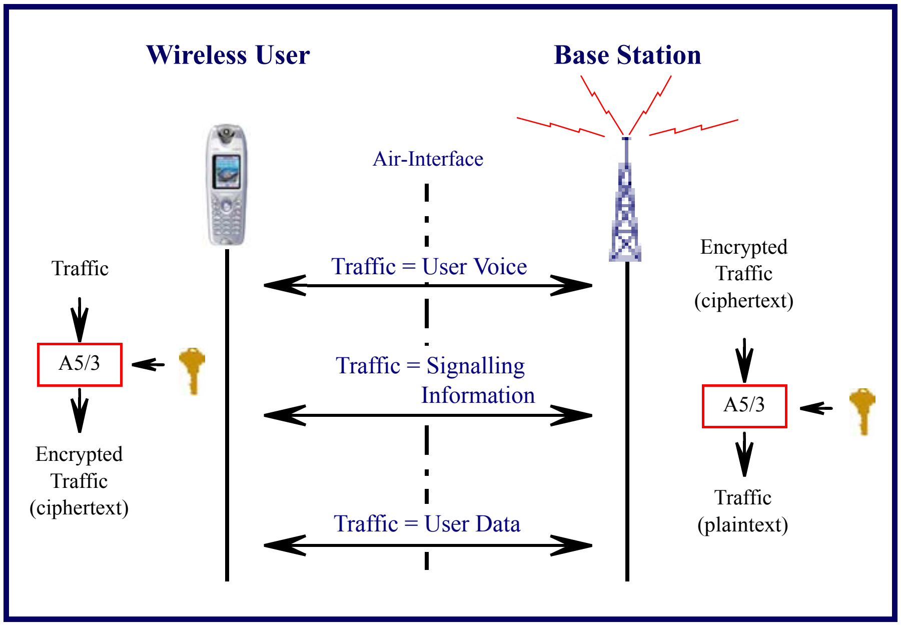
Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 4, No. 6. July, 2002

Cryptography In The News

New Algorithm Developed: A5/3 Cipher

Earlier this month, technologists announced the availability of a new security algorithm to provide a higher level of protection of GSM (Global System for Mobile Communications) wireless traffic. The algorithm, known as A5/3, is a cryptographic cipher for the protection of traffic on the GSM air-interface – the interface between the handset and the wireless network (see **Figure 1**). The algorithm is for use in 2nd generation GSM networks, although it is a derivative of cryptographic algorithms developed for 3rd generation systems. That is, A5/3 is derived from the so-called "Kasumi kernel", which in turn is a derivative of the Mitsubishi-developed MISTY algorithm.

Figure 1: Ciphering of the GSM System Air-Interface



A5/3 will protect the following types of bi-directional, wireless traffic in GSM systems:

- Voice calls,
- Signalling information (e.g., user PIN, dialed digits),
- User data.

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, 2002.

Future Topics

Radius for Wireless • IP Security • Public Keys & Wireless • Security Issues in Ad hoc Wireless Networks • Latest in Watermarking • 3G Security • Blackberry • Security for PDAs • SMS Security

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 and Illustrator:
Les Owens.

Article Sourcing:	Tim Kridel.
Production:	Doug Scofield.
Distribution:	Debbie Brandelli.
Accounts:	Evelyn Goreham.
Publisher:	David Crowe.

Upcoming Fraud and Security Events

The following are some upcoming conferences and security events that may be of interest to the wireless and network security practitioners.

Internet Untethered – Denver Wireless Trade Show/Seminar
6th August 2002
Westin Tabor Center
Denver, CO
www.angelbeat.com/Denver86.shtml

SANS Parliament Hill
7th- 12th August 2002
Ottawa, Ontario
www.sans.org/ParliamentHill02

Meeting IT Security Benchmarks through Effective IT Audits
8th- 9th August 2002
American Management Association
Washington, DC
www.frallc.com/infotech.asp#2

RAWCON2002 - IEEE Radio and Wireless Conference
11th- 14th August 2002
Hilton Boston Back Bay
Boston, MA
rawcon.org

Network Security Conference
12-14 August 2002
Caesars Palace
Las Vegas, NV
www.isaca.org/nsc2002.htm

Crypto 2002
18th- 22nd August 2002
Santa Barbara, CA (UCSB)
www.iacr.org/conferences/crypto2002

Secure i-World (Online Privacy and Websec)
19th- 21st August 2002
Manchester Grand Hyatt
San Diego, CA
www.secureiworld.com

Internet World Fall 2002
30th September - 3rd October 2002
Jacob J. Javits Convention Center
New York, NY
www.internetworld.com/events/fall2002

What is meant by *protection*?

The A5/3 ciphering algorithm, a complex set of mathematical operations, is designed to provide the confidentiality security service – it is designed to *protect* against unauthorized disclosure of information. Although an adversary may be able to eavesdrop or "sniff" the wireless interface, the algorithm's scrambling will transform the traffic to gibberish, rendering it totally unintelligible to the adversary.

Background of A5 ciphering

A5/3 is the latest in encryption algorithms for the protection of GSM traffic. Several versions of the A5 ciphering algorithm are used in the various GSM networks worldwide because of export control restrictions on cryptographic systems:

- A5/0 – provides no encryption – used mainly in third-world countries,
- A5/1 – provides the strongest encryption – used in North America and Western Europe,
- A5/2 – provides weaker encryption – used in Asia.

Where does it fit into the picture?

According to people involved in the development of A5/3, there are several reasons for making it available to GSM operators, including the desire to replace the other aging algorithms, the availability of significantly stronger cryptographic algorithms since the release of the A5 family in the 1980's, and relaxation of worldwide export control laws. Moreover, James Moran, Director of Fraud and Security at the GSM Association, noted that continued deployment of the A5/2 cipher in GSM networks presents a security risk. Although the algorithm has not been "cracked" in a live network, the algorithm has already been compromised under test conditions.

More Upcoming Events

Telecoms Fraud & Security Seminar
23rd- 25th September 2002
Courtyard Marriott Kopenick
Berlin, Germany
www.iir-conferences.com

CTIA Wireless IT and Internet 2002
16th- 19th October 2002
Sands Expo & Convention Center
Las Vegas, NV
www.wirelessit.com

Development and usage

A5/3 was designed by the Security Algorithm Group of Experts (SAGE) of ETSI (European Telecommunications Standards Institute). The 3GPP (Third Generation Partnership Program) Working Group SA3 provided the requirements specification for the algorithm's development.

The new algorithm can also be used for GPRS (General Packet Radio Service) and other GSM modes, such as HSCSD (High Speed Circuit Switched Data) and EDGE (Enhanced Data Rates for GSM Evolution). The A5/3 algorithm will be available to wireless infrastructure developers and handset vendors for GSM systems in 3Q2002. Unlike the details of the other A5 versions, the defining specifications of A5/3 are publicly available on the 3GPP website:

www.3gpp.org

The developers invite others to evaluate the strength of the algorithm – gone is the "security through obscurity" of the past.

Fraud And Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following fraud and security patents. These may be of interest to some of our wireless security practitioners. Each patent includes the patent number, the invention title – linked to the corresponding USPTO web page – a brief description, the inventor(s), and the assignee (owner). These patents were granted during June and July 2002.

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.

US Patent: 6,421,781

Method and apparatus for maintaining security in a push server

A secure Push Server is disclosed. The Push Server is used for sending notifications to different wireless clients on different wireless networks. The Push Server allows Information Service Providers to send notifications to the wireless clients. The Information Service Providers initiate a request to the Push Server that includes updated information. The request also includes a certificate from the Information Service Provider. The Push Server authenticates the request from the Information Service Provider by verifying the certificate. The Push Server also determines if the certificate was issued from an acceptable certificate authority by examining an acceptable certificate authority list. Finally, the Push Server checks the content of the notification to be sure it does not interfere with other Information Service Providers. After performing the security checks, the Push Server processes the notification request.

Issued: July 16, 2002

Inventor: Mark Fox et. al.

Assignee: Openwave Systems Inc. (Redwood City, CA)

US Patent: 6,421,727

Inter-networking system and method for a global telecommunications network

A method and system for providing service activation capability from Service Providers to end-customers in a global Iridium-type telecommunications system. The inventive method includes the steps of utilizing a browser to download a program and executing the program to provide for service provisioning. In the illustrative embodiment, the browser is a Web browser, the program is a Java application and the inventive method further includes the steps of providing service activation, suspension, reactivation and deactivation. Telephony services are provisioned, along with paging and roaming. Capcode generation, allocation and ordering are also supported, along with tracking and maintenance of capcode status.

Issued: July 16, 2002

Inventor: Abraham Reifer et. al.

Assignee: Same

US Patent: 6,421,714

Efficient mobility management scheme for a wireless internet access system

A wireless data network providing communications with a Point-to-Point Protocol (PPP) server is disclosed. A home network includes a Home Mobile Switching Center and a Wireless End System. The Home Mobile Switching Center includes a Home Registration Server and a Home Inter-working Function. The Wireless End System includes an End Registration Agent which is coupled to the Home Registration Server. The wireless data network also includes a PPP server, wherein a message can be coupled from the End System through the Home Inter-working Function to the PPP server.

Issued: July 16, 2002

Inventor: Girish Rai et. al.

Assignee: Lucent Technologies (Murray Hill, NJ)

US Patent: 6,421,707

Wireless multi-media messaging communications method and apparatus

A wireless multimedia messaging communications method and apparatus permitting a subscriber to a wireless telecommunications service to receive and generate multimedia messages from known wireless personal communications devices, – i.e. cellular/PCS telephones. A multimedia message may be received by the network and selectively delivered to a subscriber of the wireless service. Upon receipt of the message, the network determines an appropriate action to take with respect to the message, based upon a profile of the subscriber. The subscriber is then notified by the network of the message, and it then delivers the message – and any multimedia attachments to the message – to the subscriber, according to a delivery indication sent by the subscriber to the network. Advantageously, the method allows for the conversion of messages as appropriate – i.e., text-to-speech, text-to-fax, provides gateways to varieties of multimedia information such as that found on the Internet, and provides an active messaging format wherein message templates are stored on a mobile device that interprets the active messages, thereby permitting a subscriber to quickly compose a message by supplying simple, dynamic components of the message.

Issued: July 16, 2002

Inventor: Scott Miller et. al.

Assignee: Lucent Technologies (Murray Hill, NJ)

US Patent: 6,421,537

Method and apparatus for providing switch capability mediation in a mobile telephone system

An improved Home Location Register (HLR) that includes a Switch Capability Mediation Module for implementing switch capability mediation between different mobile switching centers (MSCs). According to the invention, when one MSC (home MSC of a receiving party) attempts to communicate with another MSC (serving MSC) via the HLR serving the home MSC, the Mediation Module determines whether the two MSCs are provided by different vendors and whether they implement different capabilities, based on the MPCM (MSC ID Point Code Map) file records of both the originating and the serving MSC. The MPCM files store MSCs' network configuration information. For each capability involved, the Mediation Module determines which one of the three situations are present:

1. The originating MSC has this particular capability, but the serving MSC does not.
2. The originating MSC does not have this capability, but the serving MSC does.
3. Both the originating and the serving MSC have this capability, but each implements it in a different way.

Depending on which situation is present, the Mediation Module provides appropriate capability mediation between the two MSCs.
In any of the above three situations, if the Mediation Module determines that it cannot mediate between the two different MSCs, based on the particular capability involved, it may deny the call entirely. Thus, by using the improved HLR of the invention, the communication between two different MSCs may be properly established and optimized.

Issued: July 16, 2002

Inventor: James Lamb et. al.

Assignee: Compaq Computer Corp. (Houston, TX)

US Patent: 6,421,368

Spread-spectrum wireless communication system

A system for accessing a telephone system, in which a set of user stations are matched with a set of base stations for connection to a telephone network. Each base station may be coupled directly or indirectly to the telephone network, and each may be capable of initiating or receiving calls on the telephone network. Each user station may comprise a spread-spectrum transmitter or receiver, and each may be capable of dynamic connection to selected base stations. A plurality of base stations may be coupled to a private exchange telephone system for coupling user stations in calls outside the telephone network. User stations may use CDMA, FDMA, TDMA or other multiple-access techniques to obtain one or more clear communication paths to base stations. User stations may make and break connections with base stations as the user station moves between service regions, or as it is otherwise more advantageously serviced by base stations. User stations may direct requests to and receive information from an enhanced telephone services processor, so as to obtain enhanced telephone services within the telephone network. Base stations may be coupled to each other by means of a private exchange telephone system or other small business telephone system (such as a PBX, Centrex, or key-type system) so as to couple user stations in calls outside the telephone network. User stations may also be coupled directly or indirectly to the telephone network on their own or by another access path, such as narrowband or spread-spectrum cellular telephone circuits.

Issued: July 16, 2002

Inventor: Jeffrey Vanderpool

Assignee: Xircom Wireless, Inc. (Colorado Springs, CO)

US Patent: 6,418,224

Method and apparatus for self-inverting multiple-iteration CMEA crypto-processing for improved security for wireless telephone messages

A self-inverting enhanced CMEA encryption system suitable for use in wireless telephony. An unprocessed text message is introduced into the system and subjected to a first iteration of a CMEA process, using a first CMEA key to produce a first intermediate message, a first intermediate processed text message, a first intermediate ciphertext message, or the like. The first intermediate processed text message is subjected to a further iteration of the CMEA process, using a second CMEA key, to produce a second intermediate processed text message. The second intermediate processed text message is subjected to a final iteration of the CMEA process, using the first CMEA key, to produce the final processed text message. Security may be additionally enhanced by subjecting each message to an input/output transformation before and after each iteration of the CMEA process. In a three-iteration process, a total of four input/output transformations are used with the first and fourth input/output transformations being identical, and with the second and third input/output transformations being identical.

Issued: July 9, 2002

Inventor: Mark Etzel et. al.

Assignee: Lucent Technologies (Murray Hill, NJ)

US Patent: 6,418,130

Reuse of security associations for improving handover performance

In a radio telecommunication system, the performance of a mobile unit can be significantly improved during a hand-over procedure by reusing existing security associations corresponding to the mobile unit. By reusing existing security associations, a mobile unit can begin secure communications immediately following the hand-over. Otherwise, and in accordance with conventional practice, the mobile unit will have to undertake the time consuming task of renegotiating the required security associations before it can begin transmitting and receiving secure communications.

Issued: July 9, 2002

Inventor: Yi Cheng et. al.

Assignee: Telefonaktiebolaget L M Ericsson (publ) (Stockholm, SE)

US Patent: 6,415,142

Prepaid smart card in a GSM-based wireless telephone network and method for operating prepaid cards

Description of a smart card which, in normal use in a network, allows the transfer of goods/services to a user of the card from a network operator by subtracting prepaid units of value stored in the card. The card has an embedded integrated circuit with a serial number unique to each card. The circuitry includes a prepaid units register for storing a value for remaining prepaid units. In response to an interrogation, the serial number and the remaining prepaid units may be read out.

A key number is also stored in the circuit. It has a first portion unique for each card, and a second portion which is common to a plurality of cards, but unique for a network operator. The key number, in normal use of the card, cannot be read from the card. An algorithm is also stored in the card, and in normal use, it also is not readable from the card. A microprocessor calculates a certificate in accordance with the algorithm as a function of the key number and the number (currency value) in said prepaid register, and the certificate is readable from the card.

Issued: July 2, 2002

Inventor: Philippe Martineau

Assignee: Gemplus S.C.A. (Gemenos, France)

US Patent: 6,411,807

Roaming authorization system

A Roaming Restriction System permitting a wireless carrier or a subscriber to set a profile that identifies a chosen time window within which the subscriber's wireless calls originated from one or more selected roaming areas are not allowed to be completed, while calls initiated either from authorized roaming areas or from outside the chosen time window are allowed to be completed. The Roaming Restriction System allows a wireless carrier to either suspend or grant roaming privileges for a given subscriber within one or more location areas, and for a particular time window.

Issued: June 25, 2002

Inventor: Umesh Amin et. al.

Assignee: AT&T Wireless Service, Inc. (Kirkland, WA)

US Patent: 6,411,715

Method and apparatus for verifying the cryptographic security of a selected private and public key pair without knowing the private key

Methods and apparatus are disclosed for demonstrating that a public/private key pair is cryptographically strong without revealing information sufficient to compromise the private key. A key pair can be shown to be cryptographically strong by demonstrating that its modulus N is the product of two relatively large prime numbers.
In addition, a key pair can be shown to be cryptographically strong by demonstrating that N is cryptographically strong against Pollard factoring attacks, Williams factoring attacks, Bach-Shallit factoring attacks, and weighted difference of squares factoring attacks.

Issued: June 25, 2002

Inventor: Moses Liskov

Assignee: RSA Security, Inc.
(Bedford, MA)

US Patent: 6,408,074

Hardware architecture for a configurable cipher device

A cipher device that can be configured to execute different types of cryptographic algorithms and perform more than one algorithm simultaneously. The device is operated from an external source. It is implemented with a hardware architecture exhibiting the efficiency of conventional hardware-based cipher devices while also employing the flexibility of software-based solutions.

Issued: June 18, 2002

Inventor: Kevin Loughran

Assignee: Lucent Technologies
(Murray Hill, NJ)

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