Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 4, No. 11. December, 2002

Biometric Security For Wireless Device

Tim Kridel

Despite the work being done to secure the air link portion of wireless communications, user devices remain a the weak spot. Improving the security features built into handheld devices such as smart phones and wireless PDAs will help to convince business and enterprise users to adopt wireless data. They need to be convinced that is if a handheld is lost or stolen, it will be is difficult for an unauthorized user to access information stored on the device or to use it to access a network containing sensitive data, such as a corporate intranet.

One traditional approach to security is the use of passwords or PINs. Aside from the fact these are prone to theft and hacking, one of their biggest drawbacks is the inconvenience of repeatedly keying them in, which often leads to users figuring out a way to bypass them or just avoiding services requiring them.

For the enterprise, the former problem (user bypassing) compromises security and increases costs by increasing the resource requirements of help desks. Nearly 40% of calls to corporate help desks are about lost or missing passwords, according to Compaq. For the operator, the latter problem (avoidance of services) is a barrier to acceptance that reduces revenue.

A viable alternative to achieve an acceptable balance between security and convenience is biometric security. This is particularly true when the device includes built-in biometric data collection features. Design includes an authentication system requiring a user's physical attribute such as a fingerprint, retina, iris or voice. The illustration on this page shows a device with a built-in fingerprint scanner – the black square located below the screen. With this alternative, if a wireless device is lost, there is less risk of security breaches because the user's authentication information – such as his fingerprint – is not stored on the device, so the finder – possibly a criminal – cannot get access.

Research suggests that most people are comfortable with biometrics, at least when it is used for securing public places, such as airports. An October 2002 survey by Harris Interactive found that 82% of respondents would allow their fingerprints to be scanned for airport security. It is unclear whether their tolerance will extend to, for example, wireless devices and mobile e-commerce applications, but it is reasonable to think that they will if it is convincingly shown to thwart fraud and identity theft while not noticeably increasing the difficulty of using the device.

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…

January 23rd, 2003.

Future Topics

802.11 Wireless LAN "Hotspot" Roaming Security • Wireless VPNs • 3G Security • Public Keys & Wireless • Wireless Flash Memory Security • Radius for Wireless • Security Issues in Ad hoc Wireless Networks • 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**: $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.

Biometrics for Thin Clients

Voice-recognition is among the least expensive biometric types to add to a wireless device, while the cost of hardware and software for fingerprint recognition has dropped significantly over the past few years. Four years ago, peripheral fingerprint-recognition devices for laptops and desktops already retailed for well under $100, and prices have continued to fall.

Over the past few months, several vendors have launched PDAs with built-in biometrics. The BioAPI Consortium maintains a list of biometric devices and peripherals at:

www.bioapi.org/BioAPI_products/products.htm

Hewlett-Packard, for example, in November, began selling the iPAQ Pocket PC h5450, which is wireless enabled (Bluetooth, 802.11b) and also includes a thermal biometric fingerprint reader. Although it is priced at $699, the h5450 is a high-end model and the high cost is not due to fingerprint recognition alone.

"The typical cost of adding biometric security to a wireless device is about $100 for hardware," says Cuong Do, CEO of Consumer Direct Link (CDL), whose Linux-based Paron MPC PDA includes built-in fingerprint recognition, Bluetooth and GSM. "The main cost is software to do remote enrollment and remote identification from device to backend."

One obvious challenge to adding biometric security to a wireless device is that thin clients have limited memory and processing power. CDL's system gets around that hurdle by limiting the tasks the handheld must perform.

"The bulk of the processing is provided by the backend server," says Do. "The wireless device captures the fingerprint biometric that is transformed into an encrypted format. This encrypted information is sent to the backend server via a secured wireless link (i.e., using a Virtual Private Network) for processing and matching. The operating system also plays an important role since lifting the finger image, extracting it and converting it requires a fast process." One CDL system user is the Hong Kong Air Cargo Terminal.

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.

International Workshop on Practice and Theory in Public Key Cryptography (PKC 2003)
6th- 8th January 2003
Hyatt Regency Miami
Miami, FL
www.sait.fsu.edu/pkc2003

Secure and Survivable Software Systems
6th- 9th January 2003
Hilton Waikoloa Village
Big Island, HI
www.cs.uidaho.edu/~krings/HICSS36/HICSS36-cfp.htm

2003 International Consumer Electronics Show (CES)
9th- 12th January 2003
Las Vegas Hilton and Convention Center
Las Vegas, NV
www.cesweb.org

SANS Cyber Defense Initiatives 2003 – Fighting Back
12th- 17th January 2003
Crowne Plaza Austin Hotel & Executive Meeting Center
Austin, TX
www.sans.org/CDI03Austin
[See dates for New Orleans and San Antonio locations also]

Security and Watermarking of Multimedia Contents V
20th- 24th January 2003
Santa Clara Convention Center and Westin Hotel
Santa Clara, CA
www.ssie.binghamton.edu/fridrich/Research/ei23.pdf

How to Perform a Technical Vulnerability Assessment
27th- 28th January 2003
Fort Lauderdale, Fl
www.gocsi.com

7th Annual Financial Cryptography Conference
27th- 30th January 2003
La Creole Beach Hotel
Gosier, Guadeloupe, France
ifca.ai/fc03

COMNET Conference & Expo
27th- 30th January 2003
Washington Convention Center
Washington, DC
www.comnetexpo.com/comnetexpo/V33/index.cvn

7th Annual Information Assurance (IA) Workshop – Leveraging the Power of Information
28th- 30th January 2003
Williamsburg Marriott Hotel
Williamsburg, VA
iac.dtic.mil/iatac/announcement.htm

SPACECOM 2003
28th- 30th January 2003
Broadmoor Hotel
Colorado Springs, CO
rockymtn-afcea.org/2003

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

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

Biometrics in General

A variety of factors affect the costs of biometric authentication. One factor affecting the cost of fingerprint recognition, for instance, is the quality of the scan. Fingerprint recognition, from a quality perspective, can be classified into two types: Commercial grade and Forensic grade.

In commercial grade recognition, a scanned fingerprint is simply compared to one in a database.

With forensic grade recognition, a much finer scan of the fingerprint is created, allowing investigators, for example, to match it with a database of hundreds or millions of other fingerprints.

Further information about factors affecting accuracy is available from the Biometric Systems Lab at the University of Bologna, Italy, at:

bias.csr.unibo.it/research/biolab/bio_tree.html

Wireless applications always transmit a device or user identity, apart from the biometric information. Consequently, the system knows the single fingerprint to match against for authentication. This allows commercial grade recognition to be used, significantly speeding up the process, and reducing its cost.

Dual-technology authentication also decreases the chance that the user can breach security. "We have several applications where a biometric sensor is needed in conjunction with, for example, a smart card reader for the highest level of security," says Marinda Gansmoe, a development engineer with IBM Engineering & Technology Services, who helped CDL develop its Pervasive Network 3P system. Their system includes a wireless PDA with a biometric system. The ordinary user of this type of PDA configuration is less likely to try to bypass authentication, since the password hassle is eliminated.

Standards Bodies

The American National Standards Institute (ANSI) and National Institute of Standards and Technology (NIST) are among the better-known standards bodies working on biometrics. A list of others is available from the U.S. government Biometric Consortium Web site at:

www.biometrics.org/html/standards.html

One example is the BioAPI Consortium (www.bioapi.org), which has nearly 100 members. Founded in April 1998 by Compaq, IBM, Identicator Technology, Microsoft, Miros and Novell, the group focuses on standards for face, fingerprint and voice recognition. Its goals include developing standards that work with any operating system and APIs that work with any recognition technique.

The group's most recent major accomplishment was in April 2002, when ANSI published BioAPI Specification Version 1.1 as ANSI/INCITS 358. The specification is compliant with the Common Biometric Exchange File Format. ANSI/INCETS 358 defines an open API for a variety of biometric technologies.

The irony is that, although that biometric security has progressed to the point that it is a viable option for mobile devices, the technology still faces plenty of hurdles to wide adoption. For example, despite the push to improve security, North American airports and airlines have been slow to adopt biometrics, mainly because the U.S. Transportation Security Administration has not issued recommendations for how and where biometrics could be used.

Such delays create a ripple effect in other sectors because airport deployments would be an opportunity for a wide range of companies to learn about how biometrics can be used to improve security. Nevertheless, vendors of mobile devices seem confident enough in the technology. They are forging ahead on their own, and in the end, that pioneering work could wind up making the wireless sector into a model of how other sectors can use biometrics to improve security without compromising user-friendliness.

References

[1] C. Do, and M. Furusawa, *Application of Biometric Fingerprint in m-Commerce*. Jan., 2001.
www.cdlusa.com/is/releases/Fingerprint_Paper.pdf

[2] *82% of Americans Endorse Airport Use of Fingerprint Scanning to Increase Security.* Harris Interactive press release. Oct. 3, 2001.
www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=380

[3] E-mail interview with Cuong Do, CEO, Consumer Direct Link. Dec. 16, 2002.

[4] Telephone interview with Marinda Gansmoe, a development engineer with IBM Engineering & Technology Services. Nov. 25, 2002.

[5] *Compaq Introduces Mobile Biometrics Technology.* Compaq press release. Oct. 16, 2000.
h18020.www1.hp.com/newsroom/pr/2000/pr2000101601.html

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 November and December of 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.

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: 6,496,936

System and method for authentication of network users

A network authentication system providing verification of the identity or other attributes of a network user to conduct a transaction, access data or avail themselves of other resources. The user is presented with a hierarchy of queries based on wallet-type (basic identification) and non-wallet-type (more private) information designed to ensure the identity of the user and prevent fraud, false negatives and other undesirable results. A preprocessing stage may be employed to ensure correct formatting of the input information and to clean up routine mistakes (such as missing digits, typos, etc.) that might otherwise halt the transaction. Queries can be presented in interactive, batch processed or other format. The authenticator can be configured to require differing levels of input or to award differing levels of authentication according to security criteria.

Issued: December 17, 2002

Inventors: Jennifer French and Jone Wilder

Assignee: **Equifax Inc.** (Atlanta, GA)

US Patent: 6,496,928

System for transmitting subscription information and content to a mobile device

A system controlling access to broadcast messages received by a plurality of mobile devices. Selected mobile devices are provided with a broadcast encryption key (BEK). The broadcast messages are encrypted using the BEK prior to broadcasting so that the selected mobile devices containing the BEK can decrypt the broadcast messages. The broadcast messages are then broadcast.

Issued: December 17, 2002

Inventor: Vinay Deo, *et al*

Assignee: **Microsoft Corporation** (Redmond, WA)

US Patent: 6,496,690

Prepaid subscriber service for packet-switched and circuit-switched radio telecommunications networks

A system and method of providing a prepaid subscriber service to a mobile subscriber in an integrated wireless telecommunications network having a circuit-switched portion and a General Packet Radio Service (GPRS) packet-switched portion. A prepaid subscriber class (PPSC) is stored in a home location register (HLR), and the PPSC is sent from the HLR to a serving mobile switching center (MSC) when the subscriber registers in the circuit-switched portion of the network. The PPSC is sent from the HLR to a serving GPRS support node (SGSN) when the subscriber registers in the packet-switched portion of the network. Also, the PPSC may be sent from the SGSN to a Gateway GPRS Support Node (GGSN) in order to indicate that the subscriber is a prepaid subscriber. When the mobile subscriber begins a packet-switched data session, the SGSN, GGSN, or both periodically send partial call data records (CDRs) to a prepaid center (PPC). When the mobile subscriber begins a circuit-switched call, the MSC periodically sends partial CDRs to the PPC. The PPC calculates in near real time, a new account balance for the prepaid subscriber. The current call is disconnected, and prepaid services are stopped when the account balance is reduced to zero.

Issued: December 17, 2002

Inventors: Miguel Cobo and Betty Lee

Assignee: **Telefonaktiebolaget LM Ericsson (publ)** (Stockholm, SE)

US Patent: 6,496,595

Distributed biometric access control apparatus and method

An access control apparatus and method is described. Enrollment is conducted at a centralized server, and enrollment data – such as identification data – is downloaded to plural local access units at respective entrances to a restricted area. The local access units then collect data of a person upon an attempted entry into the area, and they compare the data with downloaded enrollment data to determine if the person is authorized for access. If the person is authorized, an access control device is operated to open a door, gate, or the like of the entrance. The enrollment data can be biometric data and the same type or different type of biometric data can be collected at the local access units. If a different type of data is collected at the local access units, and if it is correlated to data stored on the local access unit, data of the same type as the downloaded data is collected and compared to the downloaded data for access control. The enrollment data can be non-environmentally-affected data, such as fingerprint parameter data and the different type of data can be environmentally-affected data, such as facial parameter data.

Issued: December 17, 2002

Inventor: Daniel Puchek, *et al*

Assignee: **Nextgenid, Ltd.** (San Antonio, TX)

Nextgenid.com

NextgenID is located in San Antonio, Texas and their mission is to make biometric products for everyday use. NextgenID's scientists have been involved in the development of biometrics since the early days of facial recognition, and they have developed state-of-the-art EigenPlus™ biometric facial recognition and FingerMatch™ fingerprint recognition applications. NextgenID develops, manufactures and sells its own products. They also work directly with customers to meet special or unique requirements, and they work with OEM's to develop proprietary or private label products. NextgenID may be reached at (210) 494-5399.

US Patent: 6,493,551

GSM MoU Bypass for delivering calls to GSM subscribers roaming to CDMA networks

Method and system integrating wireless/wireline and circuit/packet networks (to bypass GSM Memorandum of Understandings) for cellular/PCS services so that GSM subscribers roaming into CDMA networks can be provided with basic wireless call delivery services as long as the roamers can pay the bill with their valid credit card. This is achieved by integrating wireless and wireline networks, as well as circuit and packet networks, using IP networks and protocols as an alternative to the existing telephony-based approach.

Issued: December 10, 2002

Inventor: Jin Wang, *et al*

Assignee: **Lucent Technologies Inc.** (Murray Hill, NJ)

Interesting References:

[1] Diffie, W. and Hellman, M. *"New Directions in Cryptography."* IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp. 644 - 654.

[2] Perkins. *"IP Mobility Support."* Network Working Group, RFC 2002, Oct. 1996.

[3] Droms. *"Dynamic Host configuration Protcol."* Network Working Group, RFC 2131, Mar. 1997.

[4] *"A Primer of the H.323 Series Standard."* DataBeam Corporation, May 15, 1998.

US Patent: 6,490,357

Method and apparatus for generating encryption stream ciphers

A method and an apparatus for generating encryption stream ciphers based on a recurrence relation designed to operate over finite fields larger than GF(2). A non-linear output can be obtained by using one or a combination of non-linear processes to form an output function. The recurrence relation and the output function can be selected to have distinct pair distances such that, as the shift register is shifted, no identical pair of elements of the shift register are used twice in either the recurrence relation or the output function. Under these conditions, the recurrence relation and the output function also can be chosen to optimize cryptographic security or computational efficiency.

Issued: December 3, 2002

Inventor: Gregory Rose

Assignee: **Qualcomm Incorporated** (San Diego, CA)

Interesting References:

[1] D. Coppersmith, *et al*. *"The Shrinking Generator."* Proc. Crypto '93, Springer-Verlag, 1994.

[2] K. Zeng, *et al.* "*Pseudorandom Bit Generators in Stream-Cipher Cryptography."* 1991 IEEE, pp. 8-17.

[3] W. Meier, *et al*. *"The Self-Shrinking Generator."* Communications and Cryptography: Two Sides of One Tapestry, R.E. Blahut *et al*, eds. Kluwer Academic Publishers, 1994.

US Patent: 6,490,352

Cryptographic elliptic curve apparatus and method

An apparatus for operating a cryptographic engine which may include a key generation module for creating key pairs for encrypting substantive content to be shared between two users over a secured or unsecured communication link. The key generation module may include a point-doubling module as part of an elliptic curve module for creating and processing keys. Hash functions may be used to further process ephemeral secrets or ephemeral keys that may be used for transactions, sessions, or other comparatively short time increments of communication. The keys generated by the key generation module may be configured to be processable by an encryption system for divulging independently to two independent parties a secret to be shared by the two independent parties. A single-inversion, point-doubling algorithm may be provided to reduce the operation count of a cryptographic process.

Issued: December 3, 2002

Inventor: Richard **Schroeppel** (500 S. Maple Dr., Woodland Hills, UT 84653), *et al*.

Assignee: **Same**

Interesting References:

[1] Vanstone, S.A, *et al*. *"Elliptic Curve Cryptosystems Using Curves of Smooth Order Over the Ring Zn."* IEEE Trans. on Information Theory, vol. 43, No. 4, Jul. 1997, pp. 1231-1237.

[2] *"New Public-Key Schemes Based on Elliptic Curves over the Ring Z.sub.n."* 1991 Kenji Koyama excerpt, Advances in Cryptology – Crypto 1991, Springer-Verlag, pp. 252-266.

US Patent: 6,487,403

Wireless universal provisioning device

The system includes at least one wireless communications device having a standard wireless interface and a wireless provisioning device that provisions the wireless communications device. The wireless provisioning device uses the standard wireless interface to transfer the provisioning information, including an authentication key, to the wireless communications device when both devices are interconnected via a wireline link between a transceiver antenna of the wireless communications device and a communication unit of the provisioning device.

Issued: December 12, 2002

Inventor: Christopher Carroll, *et al*

Assignee: **Verizon Laboratories Inc.** (Waltham, MA)

US Patent: 6,484,260

Personal identification system

A portable, hand-held personal identification device for providing secure access to a host facility, which includes a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative of the sensed biometric trait. A processing unit responsive to the biometric signal is adapted: 1) to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person – a unique trait to the enrolled person; and 2) to provide a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person. The verification signal includes information indicative of the enrolled person or the device. A communication unit, including a transmitting circuit, is adapted to transmit the verification signal to a host system.

Issued: November 19, 2002

Inventor: John Scott, *et al*

Assignee: **Identix, Inc.** (Los Gatos, CA)

US Patent: 6,483,930

Iris imaging telephone security module and method

The invention is a compact, handheld imaging apparatus which can be used to capture high-quality iris images for identification of a person. The hand-held iris imager is non-invasive and non-contacting. It comprises a camera, a cold mirror, a lens, and an illuminator. The imager has sensors and indicators which assist a user in aligning and focusing the device. The imager also automatically captures the image when proper positioning is achieved. A template of the image is then compared to a database of previously stored templates of images to identify the person. The imager is

integrated into a telecommunications device as a security module. The telecommunications device cannot be unlocked and used unless a user has been identified and authorized by the imager.

Issued: November 19, 2002

Inventors: Clyde Musgrace and James Cambier

Assignee: **Iridian Technologies, Inc.** (Moorsetown, NJ)

iridiantechnologies.com

Iridian Technologies, Inc. of Moorestown, NJ and Geneva Switzerland is involved in research, development and marketing of authentication technologies based on iris recognition – one of the most accurate biometric identifiers. Iridian is a holder of exclusive U.S. and international patents on the core concepts and technologies behind iris recognition, and it is committed to providing the authentication infrastructure critical for secure physical access, today's rapidly evolving e-commerce and information access needs, and for tomorrow's wireless world. The company markets its hardware and software products to: The Fortune 1000; the government, including public safety and justice; and the transportation, healthcare, and financial service industries. Iridian can be reached on 1-866-IRIDIAN or 1-856-222-9090.

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