Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 4, No. 8. September, 2002

Draft of U.S. Cyberdefense Strategy

September 18 began the two-month public comment window for the Draft Strategy to Secure Cyberspace, 65 pages drafted by The President's Critical Infrastructure Protection Board (PCIPB), established under U.S. Presidential Executive Order 13231 on October 16, 2001. The draft was produced with the assistance of the SANS Institute.

In March 2002, SANS requested cooperation from leaders and experts in the private and public sectors. The result of their efforts is the draft proposal being presented, which is a first step in maintaining a living document on the subject of U.S. policy for internet security.

If implemented in its current form, the draft does not increase federal regulation, but it does call for action from users at home, in business and in government. There are concerns, however, that the document is being watered down. Reports indicate there were last-minute changes before the draft's release, and these softened the potential impact.

What is likely to be effective? Voluntary implementation, with its lack of any definite liability (e.g., no defined illegal practices are identified) has its implications. Strict regulations, together with its red tape, would bring on yet another dimension of complexity.

It is possible (likely?) that this draft is an attempt to 'test the waters', and thus determine how much agency involvement the public and private sectors are willing to tolerate in order to prevent and possibly prosecute internet terrorist attacks.

The stated purpose of the Strategy, as defined in the draft, is to "engage, empower and establish efforts to secure cyberspace." Policies and procedures are taking shape, and these may affect the way homes, the business world and government, connected to all types of wireless devices, will operate in the future.

Public comments, including questions and recommendations, are sought concerning the draft's content and approach. Does it reflect key issues? Should other issues be included? Agenda boxes in the draft include specific questions for promoting discussions.

Wireless security practitioners should especially consider the portions of the draft listed below:

- "Securing Emerging Systems"on page 47,
- Items R4-12 and R4-13, on page 51,
- Items D4-5, D4-6 and D4-7, on page 53.

The draft advises agencies to carefully review the recently released NIST report findings (R4-12), which focuses on 802.11, Bluetooth and hand-held device developments. Our **July 2002 supplement** to the *Wireless Security Perspectives* provides an overview and quick access to the NIST report.

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…

October 24th, 2002.

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**: $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.

The draft Strategy is available at no charge from:

www.whitehouse.gov/pcipb

Submit feedback and comments to:

feedback@cybersecurity.gov

A series of eight meetings over the next few weeks will be held at various locations across the U.S. to discuss the Strategy draft. Locations of these meetings are listed on page 8 of the draft, and more information about these will become available at:

www.securecyberspace.gov

Errata in Mathematics of RSA

In the article about primality testing, featured in our **August, 2002 issue** of *Wireless Security Perspectives*, the equation in Figure 1 for calculating **d** included an error. This equation should have looked like this:

$$\mathbf{d} = \mathbf{e}^{-1} \mathbf{mod} \phi(\mathbf{n})$$

Clearly, there is a difference between this exponential relationship as opposed to the simple subtraction erroneously included in the equation last month.

Our apologies for any confusion this caused.

Prime Factoring Results Insignificant?

by Greg Rose
Qualcomm Australia

In this author's opinion, the Indian factoring result (presented in the **August issue** of *Wireless Security Perspectives*), while fascinating for theoretical mathematics, has no cryptographic significance at all. We already had algorithms that prove primality (Solvay-Strassen, for example) but they only "probably" finish in polynomial time . . . they aren't guaranteed to.

So, to generate a prime to be used, e.g., in RSA, you first do trial division on the candidate with the first few hundred

Upcoming Wireless Security and Fraud Events

The following are some upcoming conferences and security events that may be of interest to the wireless and network security practitioners. Once again, from the number of conferences planned for the month of October, it is clear that wireless and security are definitely topics of immense interest these days.

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

Wireless Edge Conference & Expo 2002
1st- 3rd October 2002
San Jose Convention Center
San Jose, CA
www.sys-con.com/wirelessedge2002

ITEC Conference & Expo / Austin Wireless
2nd- 3rd October 2002
Austin Convention Center
Austin, TX
www.austinwireless.net
events.goitec.com/home

An Ultra Wideband Technology Workshop: From Research to Reality
3rd- 4th October 2002
Radisson Hotel Mid-town
Los Angeles, CA
commsci1.usc.edu/INTEL-USC/index.html

Wireless Security Boot Camp
14th- 23rd October 2002
Intense School
Fort Lauderdale, FL
www.intenseschool.com

WPMC 2002 (The 5th International Symposium on Wireless Personal Multimedia Communications)
16th- 18th October 2002
Sheraton Waikiki
Honolulu, HI
www.wpmc02.gatech.edu

Federal Wireless User's Forum (FWUF) Workshop
16th- 18th October 2002
Sands Expo and Venetian Hotel
Las Vegas, NV
is2.antd.nist.gov/fwuf/oct02_pan.html

(This conference to be held in conjunction with the CTIA event below)

CTIA Wireless IT and Internet 2002
16th- 18th October 2002
Sands Expo & Venetian Hotel
Las Vegas, NV
www.wirelessit.com/registration/conference_schedule.cfm

(This conference to be held in conjunction with the FWUF event above)

SANS Network Security 2002
18th- 25th October 2002
Renaissance Hotel
Washington, DC
www.sans.org/NS2002

(This conference to be held in conjunction with the NIAL conference)

National Information Assurance Leadership Conference
24th- 25th October 2002
Renaissance Hotel
Washington, DC
www.sans.org/NS2002/nial.php

(This conference to be held in conjunction with SANS NS 2002)

Enterprise Wireless Forum Conference & Expo
28th- 30th October 2002
World Trade Center
Boston, MA
www.jupiterevents.com/ewf/fall02/index.html

Federal Information Assurance Conference (FIAC) 2002
29th- 31st October 2002
University of Maryland
University College
Adelphi, MD
www.fbcinc.com/fiac

primes, to get rid of the obviously composite ones. Then you run a couple of rounds of Miller-Rabin checking, which leaves you with a "strong pseudo-prime".

Most packages leave it at that, but if you care, spend a few hours doing one of the prime-proving algorithms; if it doesn't terminate in a few hours, discard the number and try again. (This has never happened . . . finding a number that has this behaviour would be very interesting. There's no proof that they exist, but neither is there proof that they don't.)

All this beats spending a year or two running the new algorithm on a 512-bit number.

Fraud And Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following fraud and security patents that may be of interest to 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 August and September 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: 6,457,099

Programmable dedicated application card

A programmable dedicated application card is invented comprising one or more EPROMs for storing a software application, an EEPROM storing a Host Control Program (HCP) for interfacing with a Client Interface Program (CIP) executing on a host computer system, an appropriate amount of SRAM for executing and shadowing the software application, a small amount of DRAM for use as a cache for user-data during execution of the software application, and a reduced instruction set code (RISC) processor that accesses the SRAM to execute the software application and send the results to the user via the local computer system. The PDAC is simply "plugged into" a host computer system such that, when desired, the user accesses and executes the software application directly from the PDAC, thereby saving local computer resources, e.g., processor and memory, and making those resources available for other tasks. The CIP of the host computer system makes available to a user the different software applications of the local PDACs, as well as the software applications available from remote PDACs.

Issued: September 24, 2002

Inventor: David Gilbert (Charleston, West Virginia)

Assignee: Same

Interesting Reference:

Caron, *et al*. "New architectures for smart cards: the ocean approach". 1994. p 148-155, IEEE.

US Patent: 6,456,976

Mobile terminal provided with speech recognition function for dial locking

A mobile telephone is composed of an antenna, a sending/receiving section, an automatic response control section, a memory, a key input section, a dial locking control section, a control section, a speech recognition section, a timer, a display section, a speech input section, a counter and a speaker. A character code from the key input section is stored in the memory. The control section determines if an aural signal is coincident with the character code stored in the memory. If there is coincidence, dial locking is set by the dial locking control section.

Issued: September 24, 2002

Inventor: Takehiko Kuita

Assignee: NEC Corporation (Tokyo, Japan)

US Patent: 6,456,839

Method and apparatus for billing a neighborhood cordless service

A method for providing a local cordless service comprises the steps of receiving subscriber neighborhood zone selection input so that a mobile telephone-equipped subscriber may place or receive calls for a fixed rate, for example, per month without having to pay radio frequency air time charges any time they are located within their selected subscribed-to zones. If the subscribed-to zones are adjacent to one another and the mobile subscriber roams from one zone to another, the subscriber may continue their free call uninterrupted and without paying air time charges. However, when the subscriber roams outside their subscribed-to zones, they may be switched from the present local cordless services to conventional personal communications services and pay air time charges. However for an active call, no air-time charges are incurred as the user transitions between the cellular/DPCS environment and the local cordless service environment.

Associated apparatus comprises an IBS for automatically changing radio frequency channels as the subscriber roams within a subscribed-to neighborhood zone, roams to another subscribed-to zone or roams outside a subscribed-to zone. Subscribers may choose to use their mobile identification number, their current directory telephone number for wired public switched telephone service or obtain a new directory number. Subscribers can actuate their service over-the-air automatically without service personnel assistance from their home neighborhood zone.

Issued: September 24, 2002

Inventor: Albert Chow, *et al*

Assignee: AT&T Corp. (New York, NY)

US Patent: 6,456,822

Electronic device and method for blocking cellular communication

A method and device for achieving reliable prevention of cellular telephone calls, within a given area. In the preferred embodiment, the device and method operate to block the control frequencies of the cellular system within a given area. The device broadcasts a blocking signal with a low power output, which interferes with the reception ability and decoding of signals and commands broadcast at the control frequency. Thus, the handshake routine of the telephone/cellular subscriber with the local cellular system is prevented. Operation of the device is achieved in several ways, manually, automatically, and/or by remote control.
Its operation prevents cellular communication ability by subscribers within the area or within the effective blocking range, which is derived from the effective radiated power (ERP) of the blocking signal, its type and the type of communications/or blocked system. Using the inventive device, a given area normally accessible by cellular communications is blocked from such access, thus providing a security-related, cultural or other safe-guard. The given area is thereby isolated from cellular communications, and access can only be achieved by physically relocating the user of a blocked cellular telephone.

Issued: September 24, 2002

Inventors: Yossef Gofman and Ofer Yarden-Zaslavsky

Assignee: Netline Communications Technologies (NCT), Ltd.
(Tel Aviv, Israel)

Contact:
Selpro are Hong Kong-based importers, distributors and dealers of quality law enforcement products. Selpro represents manufacturers as exclusive or authorized dealers, and markets their products in Hong Kong, Macau, China, the Philippines and other countries and territories throughout the Australasian region. Selpro, founded in 1985, is licensed by the Hong Kong Police to deal in firearms, is registered with the Hong Kong Department of Trade and Industry as an importer of strategic commodities, and is a registered and approved supplier to the Hong Kong Government.

Interesting Reference:
Robinson, M.P., *et al.* "Interference to medical equipment from mobile phones". Journal of Medical Engineering & Technology. Vol. 21; Nos. 3-4; pp. 141-146; May-Aug. 1997.

US Patent: 6,456,698

System and method for identifying an unidentified caller

A system for identifying an unidentified caller includes a database that contains utterance data corresponding to a known caller. A data communications system is coupled to the database and receives utterance information corresponding to the unidentified caller. The data communications system compares the utterance information with the utterance data to identify the unidentified caller as the known caller.

Issued: September 24, 2002

Inventor: Sanford Morganstein

Assignees: Distributed Software Development, Inc. (Lisle, IL); Morganstein; Sanford J.
(West Dundee, IL)

Interesting Reference:
Sadaoki Furui. "Speaker-dependent-feature extraction, recognition and processing techniques". Elsevier Science Publishers B.V. pp. 505-520, Mar. 1991.

US Patent: 6,454,173

Smart card technology

The present invention is an electronic card for use in a secure data inter-change system having a terminal adapted to receive and communicate with said electronic card, said card having means for communicating with said terminal and having a memory for storing program algorithms and data therein including valid terminal verification data and valid user identification request data. The electronic card comprises:

a. A microprocessor for monitoring for a predetermined period of time, immediately following insertion of said card in said terminal, an output from said terminal for a terminal verification message and being operable to erase said memory when said terminal verification message is not received within said predetermined period of time and being responsive to said terminal verification message received within said predetermined period of time, by comparing said received terminal verification message to said stored valid terminal verification message and being operable to erase said memory when said received terminal verification message is not valid; and means for monitoring – following receipt of a valid terminal verification message – the output from said terminal for a user identification request and being responsive to said user identification request by comparing said received user identification request to said stored valid user identification request and being operable to erase said memory when said user identification request is not valid and being operable to erase said memory when said received request is an attempt to read data from said memory before receipt of said valid user identification request.

b. said electronic card further storing the majority of application algorithms in the e-squared portion of the integrated circuit, thereby providing a dynamic set-up structure such that said card can be dynamically programmed for each unique application.

Issued: September 24, 2002

Inventor: Marcel Graves
(Ontario, Canada)

Assignee: Same

US Patent: 6,453,416

Secure proxy signing device and method of use

A digital signature of a document is formed in a digital signing device by using a private key stored in the digital signing device. A number of data items are supplied to the signing device. The signing device uses the data items to derive and authenticate a document hash. The digital signature is only formed if the derived document hash is authenticated.

Issued: September 17, 2002

Inventor: Michael Epstein

Assignee: Koninklijke Philips Electronics N.V.
(Eindhoven, Neatherlands)

US Patent: 6,453,159

Multi-level encryption system for wireless network

A multi-level encryption scheme for a wireless network. A first level of encryption is provided, primarily for wireless communications taking place between a mobile terminal and an access point. In addition, a second, higher level of encryption is provided, which is distributed beyond the wireless communications onto the system backbone itself. Through a key distribution server/access point arrangement, the second level of encryption provides a secure means for distributing the encryption scheme of the first level without compromising the integrity of the network.

Issued: September 17, 2002

Inventor: Daniel Lewis

Assignee: Telxon Corporation (Akron, OH)

Contact:

Symbol Technologies announced the acquisition of Telxon in a stock-for-stock merger in December 2001. The acquisition created a global leader in wireless handheld computing systems across many industries and vertical applications. Telxon's business is operated as a wholly owned subsidiary.

US Patent: 6,452,910

Bridging apparatus for interconnecting a wireless PAN and a wireless LAN

A Wireless bridge conjoins two previously incompatible technologies within a single device to leverage the strengths of each. The Wireless bridge marries the Personal Area Network (PAN) technology of Bluetooth as described in Bluetooth Specification Version 1.0B with the Wireless Local Area Network (WLAN) technology described in the IEEE802.11a specification to provide a wireless system level solution for peripheral devices to provide Internet service interactions. The invention brings together, in a single working device, implementations of these technologies so they do not interfere or disrupt the operation of each other, and instead, they provide a seamless transition of a Bluetooth connection to Wireless Local Area Network/Internet connection. From the Wireless Local Area Network perspective, the inventive wireless bridge extension allows a Bluetooth-enabled device to roam from one Wireless Access Point (bridge) to the next without losing its back-end connection. To inter-operate, the invention takes into account the minimum separation and shielding required of these potentially conflicting technologies.

Issued: September 17, 2002

Inventor: Vikram Vij

Assignee: Cadence Design Systems, Inc. (San Jose, CA)

Interdigital.com

Contact:

Cadence Design Systems is the world's largest supplier of electronic design technologies, methodology services, and design services. Its solutions provide a way to design high-performance electronic systems and integrated circuits (ICs). Cadence offers end-to-end solutions for system, digital, analog, and printed circuit board (PCB) design. It also helps companies augment their design teams.

US Patent: 6,449,367

Steganographic techniques for securely delivering electronic digital rights management control information over insecure communication channels

Electronic steganographic techniques can be used to encode a rights management control signal onto an information signal carried over an insecure communications channel. Steganographic techniques ensure that the digital control information is substantially invisibly and substantially indelibly carried by the information signal. These techniques can provide end-to-end rights management protection of an information signal, irrespective of transformations between analog and digital. An electronic appliance can recover the control information and use it for electronic rights management to provide compatibility with a Virtual Distribution Environment. In one example, the system encodes low data rate pointers within high bandwidth time periods of the content signal to improve overall control information read/seek times.

Issued: September 10, 2002

Inventor: David Van Wie, *et al*

Assignee: InterTrust Technologies Corp. (Santa Clara, CA)

Numerous interesting references are provided.

US Patent: 6,445,794

System and method for synchronizing one-time pad encryption keys for secure communication and access control

A method for generating an identical electronic one-time pad at a first location and a second location, the method comprising the steps of:

a. Providing a first electronic device at the first location and a second electronic device at the second location, each of the first and the second electronic devices having:

(i) a non-volatile memory;

(ii) a processor;

(iii) at least one table of true random numbers being stored on the non-volatile memory, the table being identical for the first and the second electronic devices; and

(iv) at least one software program for obtaining a true random number from the table, the software program being stored on the non-volatile memory and the at least one software program being operated by the processor;

b. providing a communication channel for communication between the first electronic device and the second electronic device;

c. selecting a selected true random number from the table at the first and the second electronic devices according to a selection procedure, the selection procedure being identical for the first and the second electronic devices, the selection procedure including exchange of at least a portion of a key between the first and the second electronic devices over the communication channel, such that the selected true random number is identical for the first and the second electronic devices; and

d. forming at least a portion of the identical electronic one-time pad at

the first and the second locations with the selected true random number.

Issued: .September 3, 2002

Inventor: Adam Shefi

Assignees: Benyamin Ron (Tel Aviv, Israel); Worcop Investment Ltd. (Tortola, West Indies)

Interesting Reference:

Menezes, A., *et al*. "Handbook of Applied Cryptography". CRC Press LLC. 1997. CIP 1996. pp. 20-21 and 169-175.

US Patent: 6,442,276

Verification of authenticity of goods by use of random numbers

A method of verifying the authenticity of goods, which includes generating one or more random codes and storing the one or more random codes in a database. The goods are then marked with one of the generated random codes such that each of the goods contain their own unique random code. Upon field checking and inventory of marked goods and comparing the codes on the marked goods to codes within the database, the authenticity of goods may be verified. Also, the invention includes a system for verifying the authenticity of goods which includes a database containing a plurality of unique random codes, and an indication whether or not each of the unique random codes has been read, and a code reader or scanner for reading the code affixed to a good. The system further includes a computer apparatus or other electrical mechanism for comparing a read code to the unique random codes contained within the database, such that upon comparison, the comparing means indicates whether the read code is valid and if valid, whether it has been read previously on another good, thereby indicating the good's authenticity.

Issued: August 27, 2002

Inventor: Frank Doljack

Assignee: Assure Systems, Inc. (Pleasanton, CA)

Assure Systems is a product security company specializing in detecting and deterring product fraud including counterfeiting, gray market diversion, and tax evasion. Its information-based solution is a departure from methods that use sophisticated images.

Assure Systems implements innovations in the following:

- Cryptography;
- 2-dimensional bar codes and readers;
- small, powerful hand-held data terminals;
- high-speed variable data printing engines;
- increased computer processing power; and
- worldwide access to the Internet.

These make possible the creation of a digital signature system for physical products.

Interesting Reference:

Tygar, J.D., *et al.* "Cryptographic Postage Indicia". Lecture Notes in Computer Science. Springer Verlag, New York, NY, US. Vol. 1179, Dec. 1996, pp. 378-391.

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