Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 6, No. 8. September, 2004

In the News: Mosquito Bites

Almost two months to the day the first mobile virus appeared, a second bug has struck. Like the Cabir worm, the new Mosquito Trojan targets handsets running the Symbian Series 60 operating system. Mosquito first appeared in mid-August and takes its name from the Mosquitos game published by Ojom for Symbian-based camera phones. The virus writers hacked the game, embedded a Trojan Horse and then distributed the corrupted version for free on the internet.

The Trojan Horse malware concept is named after the mythical, apparently innocent, wooden horse left outside the gates of Troy. It actually hid soldiers, who emerged after the horse had been dragged inside the city. Trojan software is designed to look like an innocent piece of software, but hidden within it is a malicious software program that can do a great deal of damage once inside the gates of your computer.

Infected handsets send text messages to premium-rate services without the user's knowledge, racking up big phone bills in the process. However, users can easily tell whether their version of Mosquitos carries the Trojan. First, when preparing to download the game, they are warned that the game's supplier cannot be verified. Once installed, the opening screen boasts: "This version has been cracked by Soddom Bin Loader. No rights reserved. Pirate copies are illegal and offenders will have lotz of phun!!!" Symbian says that uninstalling the game should remove the Mosquito Trojan, too.

Although they both target the same type of device, there are some key differences between Mosquito and Cabir, which first appeared on June 14. For example, Mosquito is spread by downloading a game over the wireless network, while Cabir uses Bluetooth to spread. That difference shows how quickly virus writers have found different ways to exploit wireless devices. (For more information about mobile viruses, including the Cabir worm, see the **June 2004 issue** of *Wireless Security Perspectives*.)

Virus writers are already targeting handheld operating systems besides Symbian Series 60. On July 17, the first PocketPC virus, Duts.1520, appeared and is believed to be the product of the same group that created Mosquito. Their decision to target Symbian first may be the same reason why virus writers target Windows: They target the most widely used operating systems in any domain. It is unclear why they chose to piggy-back the Trojan in the Mosquitos game, but it may have been an ironic jab at Ojom, which already offers a game called Attack of The Killer Virus.

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:

cnpsales@cnp-wireless.com

Next Issue Due…

October 21st 2004.

Future Topics

Light-weight Security Protocols • Security for UWB • MANET Security • Radius for Wireless • Handheld Device Security • 4G Security • Zigbee Security • PKE-enabled Wireless

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published **11** times a year 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.

Upcoming Mobile & Wireless and Wireless Security Events

The following are mobile and wireless, plus wireless security events, for late September and for October that may be of interest. The name, dates and venue of the event, plus URL, are provided.

ACM MobiCom 2004

26th September through 1st October
Loews Philadelphia Hotel
Philadelphia, PA

www.sigmobile.org/mobicom/2004

[Note: this event is held in conjunction with WiSe 2004]

ACM MobiWac 2004
(ACM International Workshop on Mobility Management and Wireless Access)

26th September through 1st October
Loews Philadelphia Hotel
Philadelphia, PA

ru1.cti.gr/mobiwac04

[Note: this event is held in conjunction with MobiCom 2004]

HP Wireless and Mobility Roadshow 2004

27th September
Hyatt Regency Austin
Austin, TX

www.winnetmag.com/roadshows/mobilewireless/index.cfm

SANS Network Security 2004

29th September through 4th October
Riviera Hotel & Casino
Las Vegas, NV

www.sans.org/ns2004

WiSe 2004 (ACM Workshop on Wireless Security)

1st October
Loews Philadelphia Hotel
Philadelphia, PA

www.ece.cmu.edu/~adrian/wise2004

[Note: this event is held in conjunction with MobiCom 2004]

Hack In the Box Security Conference 2004

4th- 7th October
The Westin Kulala Lumpur
Kuala Lumpur, Malaysia

conference.hackinthebox.org/index.php

GSM in Middle East, Gulf and North Africa 2004

5-6 October
JW Marriott Hotel
Dubai, United Arab Emirates

www.gsmconferences.com/gsmmeg

ICNP 2004
(12th IEEE International Conference on Network Protocols)

5th- 8th October
Kaiserin-Friedrich-Haus
Berlin, Germany

www.icnp2004.de.vu

TELECOM '04 Annual Conference & Exhibition

9th- 13th October
Venetian Hotel and Convention Center
Las Vegas, Nevada

www.ustelecom04.com

WINMEC RFID Forum 2004

12th October
UCLA
Los Angeles, CA

www.winmec.ucla.edu/rfid/2004

Security Conference & Expo 2004

12th- 13th October
The Westin
Cincinnati, Ohio

www.ccr.com/fw/main/Security_Conference_and_Expo_2004-1584.html

Wireless Industry Congress 2004

17th- 19th October
National Arts Center
Ottawa, Canada

www.wicorg.com

Gartner Symposium ITXPO 2004

17th- 22nd October
Walt Disney World Dolphin
Orlando, Florida

www3.gartner.com/2_events/symposium/2004/asset_59607_1395.jsp

Public WLAN 2004 – Positioning P-WLAN Services in the Wireless Offer

20th- 21st October
Hilton Kensington Hotel
London, UK

www.b2b-conferences.com/Telecoms/130/Public-WLAN-2004.html

Upcoming Mobile & Wireless and Wireless Security Events (continued)

Wireless Connectivity Asia
13th- 14th October
Shangri-la Hotel
Singapore
www.wiconasia.com

[Note: the WiCon Americas event is in November]

2004 NW Wireless and Security Summit
20th October
Oregon Convention Center
Portland, Oregon
www.wliinc3.com/cgi/foxweb.dll/wlx/cal/wlxprofile?caleid=689&cc=PORLMCC

MASS 2004
(1st IEEE International Conference on Mobile Ad-Hoc and Sensor Systems)
24th- 27th October
Hyatt Regency Austin
Fort Lauderdale, FL
www.ececs.uc.edu/~cdmc/mass

SASN 2004
(2004 ACM Workshop on Security of Ad Hoc and Sensor Networks)
25th October
Wyndham City Hotel
Washington, DC
cs.gmu.edu/sasn

[Note: this event is held in conjunction with CCS 2004]

2004 Broadband Summit
24th- 26th October
Crystal Gateway Marriott
Crystal City, Virginia
www.wispcon.info/us/wispconvi/center.htm

CCS 2004
(11th ACM Conference on Computer and Communications Security)
25th- 29th October
Wyndham City Hotel
Washington, DC
www.acm.org/sigs/sigsac/ccs/CCS2004

[Note: this event is held in conjunction with SASN 2004]

WIPSCON VI Vegas
27th- 29th October
Palace Station Hotel & Casino
Las Vegas, Nevada
www.wispcon.info/us/wispconvi/center.htm

Security Leadership Council
28th- 29th October
webinar
Available everywhere
www.tatevent.com/welcome.php

Verizon Wireless Fries Spammer

In one of the first U.S. court cases involving wireless spam, Verizon Wireless won a permanent injunction against a Rhode Island spammer who targeted the company's phones. In August, a U.S. District Judge in New Jersey issued a ruling barring Jacob Brown from sending messages to Verizon Wireless customers. The lawsuit stemmed from unsolicited SMS messages, sent from spoofed IP addresses, offering mortgage loans and links to pornographic Web sites. He had sent these to Verizon Wireless customers in California, Massachusetts, New Jersey and Rhode Island.

Wireless spam is not a new phenomenon, but the ruling may set a legal precedent in the United States. Verizon Wireless has two similar lawsuits pending in federal court in Georgia. In the Brown case, Verizon Wireless also sought $150,000 in damages, which the judge did not award.

Other wireless carriers have had similar results. In March 2003, a Tokyo court ordered a spammer to pay NTT DoCoMo $54,420 for messages that were randomly sent to customers. NTT DoCoMo says that more than 80 percent of the 950 million messages sent each day on its network are unsolicited. Also in March 2003, the U.K. regulator ICSTIS fined Kast Investment $63,000 for unsolicited text messages telling recipients that they had won £400. Claiming it, however, required a call to a so-called "premium-rate" phone number. Worse, the message said that the offer was from the user's wireless carrier rather than Kast.

Quote of the Month

"Success is the child of Audacity."

Benjamin Disraeli

U–R–Linked

www.maawg.org/home

Both wireless and wired networks frequently suffer large loads of unwanted messages. Recently there is offered an holistic problem-solving approach for battling things like virus attacks, spam and DoS attacks. This is available through MAAWG (Messaging Anti-Abuse Working Group). It is a collaboration of industry and government agencies. Their efforts counter obnoxious issues plaguing wireline and mobile applications.

Controlling Wireless Access To Adult Content

Tim Kridel

Sex sells, and wireless is just another channel for those who sell it. The pornography market will be worth $70 billion by 2006, with wireless' share at around $4 billion, according to Visiongain, a research firm. With those kinds of numbers, it is not surprising that some view porn as the ever-elusive killer app that will help justify the hundreds of billions of dollars spent so far on 3G licenses and infrastructure.

"Adult entertainment is what will make money for mobile phones," says Julia Dimambro, commercial director for wireless communications at Private Media Group, which supplies adult content to wireless carriers.

Time will tell whether those bullish forecasts pan out, but one thing is clear: Tapping that market entails a host of thorny issues from legal, technical and business-practices perspectives. Even wireless carriers that do not plan to offer adult content still must grapple with related issues, such as pedophiles using MMS or SMS to target underage wireless users.

Even wireless carriers that do not plan to offer adult content still must grapple with related issues, such as pedophiles using MMS or SMS to target underage wireless users. Those that do not tackle those issues before they flare up run the risk of losing customers, at least among consumers who recognize the risks.

"They are going to have to convince mums and dads that the devices can be used safely and appropriately [by their children]," says John Carr, technical adviser to NCH Action For Children, one of the U.K.'s largest children's welfare organizations. "It's the mums and dads, after all, who are largely going to be buying [3G cellphones] for their children. To achieve that the mobile companies are going to have to provide an array of protective measures and tools that the wired internet companies are only now starting to deploy on a much more widespread basis."

Codes of Conduct

Hutchison 3G UK – usually referred to simply as "3" – is one carrier that has several technical safeguards aimed at preventing underage access to adult content. The "Top Shelf" section of its entertainment services menu features soft-porn-caliber slide shows and video clips from content providers such as Playboy. To access Top Shelf, users must be over 18 and have a PIN code, which is available only through an age-verification process. (One potential draw-back to this and other types of opt-in approaches is stigma: Some users may be too embarrassed to sign up, thus reducing revenue from adult services.) An additional safe-guard is 3's overall walled-garden strategy, which limits access only to content from 3's partners rather than providing full, unfiltered access to any Web site that can be viewed on a handset.

Are You the Arcanist?

Last month's series was:
49921, 49927, 49937, 49939, 49943, 49957, 49991, 49993, ... and the next in the series is the next prime number, 49999.

Simon Arcand (Magma) provided the correct answer, as did Greg Rose also. Good job, fellows! It was so easy, they suspected a trick hidden in it.

This month ...

How many canonical 3x3 magic squares are there? They must be composed of nine (9) consecutive integers, with every row, column and diagonal adding to the same number, and must not be transformable into another magic square by simple transformations (i.e., adding a constant to every cell or by a series of rotations). Describe the unique pattern of each such canonical magic square.

Submit your answer to
wsp@cnp-wireless.com
and if you give the correct answer, we will send you our environmentally-friendly golf shirt, made from recycled cotton – free.

3's strategy exemplifies discreet marketing of adult content. Recent efforts of self-regulation among wireless carriers take it a step further, by offering a code of conduct. The **box** at right summarizes it.

The code of conduct echos Carr's argument about responding to parental concerns, to avoid restricting the growth of the wireless soft porn industry: "Mobile operators recognize that [adult content] may cause some concern to parents whose children have mobile phones," the consortium said in a press release.

Masked Marketing in Wireless?

In 2001, the Netherlands' Tring offered "Een Prettig Pakket," which bundled a Nokia 3300 phone and a vibrator.

Meanwhile, vendors such as Vibelet offer downloadable, vibrator-like ringtones.

No, no. None of that smut will e'er plug up my phone ... It's cool having my phone handy, like ... in my pants pocket.

"The Code requires that content deemed to be unsuitable for consumption by persons under the age of 18 will receive an "18" classification," says Hamish MacLeod, who coordinated the code's creation. "This will be independently assessed and be a common standard across networks. This content will be placed behind access controls (e.g., PINs) and only made available to those that the mobile operator has satisfied itself are at least 18."

To reach this level of satisfaction, carriers do not have to create safeguard tools from scratch. For example, the developer Bango.net already offers a platform that lets a carrier verify the user's age before providing access to adult content.

"Mature" Content Code of Conduct for Wireless

In January 2004, six U.K. carriers – Hutchison 3G, Orange, O2, T-Mobile, Virgin Mobile and Vodafone – created a code of conduct for self-regulating mature content, including pornography. The code calls for:

- All commercial content unsuitable for customers under 18 will be classified "18". Such content will not be made available to customers until the networks, through a process of age verification, are satisfied that he or she is at least 18.
- The classification framework will be in line with comparable standards in other media and will be created by a body that is independent of the mobile operators.
- Chat rooms made available to customers under 18 will be moderated (i.e., monitored to guard against inappropriate use).
- Parents and caregivers will be able to apply filters to the mobile operator's Internet access service so that the Internet content thus accessible is restricted.
- Mobile operators will work with law enforcement agencies to deal with the reporting of content that may break the criminal law.
- Mobile operators will also combat bulk and nuisance communications.
- Mobile operators will provide advice to customers on the nature and use of new mobile devices and services and support other relevant media literacy activities designed to improve the knowledge of consumers.

Another example is Nokia. On September 22, the company announced an addition to its Nokia Intelligent Content Delivery (ICD) platform that restricts access based on subscriber and service recognition. Available in fourth quarter 2004, the module lets subscribers choose the services that can be accessed on their devices based on user-specified criteria such as content type and price. Although the press release used parents as one example of people who might use the filtering system, it also identified enterprises, suggesting that some companies already have voiced concern about access to content that, at the very least, is not work-related or may contain a mobile virus.

The Messaging Loophole

The Code has a few potential loopholes. For example, although it covers chat rooms, it does not address premium SMS services, which will continue to be regulated under the ICST's Code of Practice (ICST: Information and Communications Services and Technologies), nor does it cover peer-to-peer communications. So although consortium members will moderate chat rooms open to minors, it is difficult to see how the guidelines would prevent, for example, a pedophile from using SMS to communicate with a minor.

The Code also does not address content that enters the wireless network in ways outside the operator's control. For example, an under-aged child could bypass the safeguards by using Bluetooth or infrared to load adult content and then share it with friends via MMS. But any attempt to craft tougher restrictions on peer-to-peer communications (such as Vodafone's Flirt) would run afoul of privacy laws. "The code does not involve mobile operators intercepting private communications," MacLeod says. "In the United Kingdom, this can only be done by law enforcement agencies under a warrant. Communication in public chat rooms is not private."

Hamstrung by privacy laws, carriers are in a difficult position when faced with parents who are not aware of the limits on policing messaging services. "I have had complaints from parents" says John Carr, "about the nature of the chat services that their children have been able to access via SMS, and I have had complaints about how MMS has been abused, so these are very real issues."

One technical option is to limit the range of services that a phone can access, based on its user.

"The key to many of these things" continues Carr, "is going to be the age-verification system that all the operators are committed to introducing. The whole point of that system is to allow the operators to distinguish between adults and children. Where a handset is identified as belonging to a child, there will be a range of restrictions applied at the network level that ought to minimize a whole range of risks."

Of course, the potential downside is that by blocking SMS or MMS entirely, the operator also plugs two of the most lucrative revenue streams today, particularly among teenage users.

The increasingly common practice of third-party billing creates another technical option. By adding charges to customers' bills for content provided by its partners – regardless of whether it is accessed by a Web browser or MMS – a wireless carrier has a certain level of control over them, or at least those that want to get paid. As John Maynard, MMS program manager at Vodafone, told *The Register*: "Operators have a liability for content that is monetized. We have become shopkeepers rather than just a payment agency or a common carrier. People are less likely to distribute illegal content because the billing mechanism will catch up with them."

Government Intervention

Besides avoiding the risk that concerned parents will stop buying phones for their children, thus cutting into one of the few remaining growth markets, wireless carriers have another incentive to be proactive: Self-regulation can stave off government regulation. For any business, few things are more embarrassing than having a law nick-named after them.

The U.K. carriers' code of conduct appears to be avoiding that situation. "This is an excellent example of the responsible self regulation we are keen to encourage among the mobile operators to address issues relating to new types of content now available on mobile handsets," Stephen Timms, Communications Minister, said in the January 2004 press release announcing the code. "We believe this approach best meets the needs and expectations of consumers."

Other governments, however, are not waiting for operators to take the lead. For example, in March 2004, the Thailand Culture Ministry announced that it would take legal action against companies that provide pornographic images for wireless. The production, sale or distribution of pornography is already illegal in Thailand, where it carries a maximum penalty of three years in prison.

Although privacy and wiretap laws in countries such as the United Kingdom limit a carrier's ability to police peer-to-peer communications, they often do not limit government oversight. For example, in July 2004, the Chinese government announced plans to expand its Internet and chat room monitoring to include SMS, in an effort to weed out "pornographic, obscene and fraudulent" messages, according to the state-run Xinhua News Agency. A Chinese vendor, Venus Info Tech, is providing real-time SMS-monitoring tools based on filtering algorithms created by the state-run Chinese Academy of Sciences.

Although wireless carriers are encouraged to facilitate the monitoring as part of "self-discipline," the country's largest carrier, China Mobile, already had plans to screen messages for pornographic content. Regardless of whether the government or the carrier is the watchdog, screening SMS is no small task: China's 260 million wireless users sent 220 billion SMS messages in 2003, according to the Ministry of Information Industry.

Lessons Learned

Wireless carriers are not the first service providers to face the issue of controlling underage access to adult content. The wired Internet provides plenty of lessons – and cautionary tales.

"Get a grip of this problem early in the development cycle so that you are not always playing catch up," MacLeod advises. "Make the filtering solution easy to apply. Take-up of filtering in fixed line is very low because customers are left to make their own choices and install it themselves. The [wireless carriers] will apply filtering at the network level to their Internet access service and will make it very easy for customers to invoke."

But wireless faces unique issues, too. For example, the notion of community standards – a key benchmark in the United States for defining obscenity in any medium – becomes a gray area when, for example, the user roams to a country that has stricter prohibitions on pornography. Indeed, when it comes to offering adult content, the cornerstone of wireless – mobility – becomes a stumbling block.

"From a legal perspective," according to Carr, "there is no difference in principle between the wireless world and the wired world. However, the fact that the wireless world makes everything mobile does heighten certain risks and therefore, potentially, the duty of care of the provider increases accordingly. Historically, children and young people have accessed the internet from fixed PCs, generally in their homes, in classrooms at school, in public libraries and so on. There has therefore always been the possibility that a parent, a teacher, a librarian or some other responsible adult could be on hand to supervise the child's access. In the mobile world, that simply no longer exists in the same way. A child might be on-line on the bus to school, in the playground during break or while out in the park. Should they run into difficulties, they are much more likely to be on their own, left to their own devices to try to deal with the situation."

Fraud and Security Patent News

US Patent: 6,792,615

Encapsulated, streaming media automation and distribution system

This invention discloses systems and methods for creating and distributing programming content carried by a digital streaming media to be a plurality of remote nodes located over a large geographic area to create customized broadcast quality programming at the remote nodes. At the remote nodes, a multi-window screen display simultaneously shows different programming, including national programming and local programming content. The remote nodes utilize a remote channel origination device to assemble the customized programming at the remote location that can be controlled from a central location. An encapsulated IP and IP encryption system is used to transport the digital streaming media to the appropriate remote nodes.

Also disclosed is a graphical user interface ("GUI") providing a software control interface for creating and editing shows or programs that can be aired or played on a remote display device having a multi-window display. The intuitive GUI software provides the user the ability to easily manage and assemble a series of images, animations and transitions as a single broadcast quality program to be displayed on a remote display device. Another application software system is capable of automating the production of audio narration reports. The disclosed audio concatenation engine automates the creation of audio narration using prerecorded audio segments to minimize the requirement for live, on-air personnel to record audio narration segments.

Issued: September 14, 2004

Inventor: Lynn Rowe, *et al*
Assignee: New Horizons Telecasting, Inc. (New Town, PA)

US Patent: 6,792,544

Method and system for secure transmission of information

The present invention includes a system and method for secure transmission of information. The system includes a source system for generating, encrypting, and transmitting a data file, and a host system for receiving and decrypting the transmitted data file. Both the host system and the source system include delivery confirmation tools for confirming that the sent files correspond to the received files.

A corresponding method comprises generating a data file at the source system, encrypting the generated data file and sending the encrypted data file. A host system receives and decrypts the encrypted data file. The source system generates a list of sent files and the host system generates a list of received files. Comparison tools verify delivery by comparing the list of sent files with the list of received files.

Issued: September 14, 2004

Inventors: Tony Hashem and Riad Hasan
Assignee: GE Financial Assurance Holdings, Inc. (Richmond, VA)

US Patent: 6,792,542

Digital system for embedding a pseudo-randomly modulated auxiliary data sequence in digital samples

The present invention discloses a system for embedding auxiliary digital information into an existing primary digitally-encoded signal to form an unobjectionable composite digital signal. Auxiliary data bits modulate a pseudo-random (e.g., PN) sequence to provide an auxiliary data sequence that is used to modify the Least Perceptually Significant Bits (LPSBs) of successive multi-bit samples of the primary signal. In a cross-term compensation embodiment, a correlation (V) between the PN sequence and the sample bits is determined, and compared to the auxiliary data bits to determine whether there is

a desired correspondence. The LPSBs in the samples are toggled, if necessary, to provide the desired correspondence. The selection of LPSBs to modify accounts for a desired noise level of the auxiliary data in the primary signal. LPSBs may be selected to be modified based on a sparse PN sequence to achieve the desired noise level and to conceal the presence of the auxiliary data. The data to be hidden can be any digital data, while the primary signal is any uncompressed or compressed digitally sampled process, including, for example, audio or video data.

Issued: September 14, 2004

Inventor: Chong Lee, *et al*
Assignee: Verance Corporation (San Diego, CA)

Notable References:

[1] G. Voyatzis, N. Nikolaidis and I. Pitas. *Digital Image Watermarking: an Overview*. Int. Conf. on Multimedia Computing and Systems (ICMCS '99). Florence, Italy. Jun. 7-11, 1999, vol. 1 pp. 1-6.

[2] P. Bassia and Ioannis Pitas. *Robust Audio Watermarking in the Time-domain.* EUSIPCO '98, Ninth European Signal Processing Conference. Sep. 8-11, 1998.

US Patent: 6,792,112

Encrypting communications between wireless mobile units

This invention is a wireless mobile unit including a voice encoder circuit that receives an analog voice signal and creates digital voice data representing a user's voice. The mobile unit receives an encryption key entered by the user, typically on the keypad or through a voice recognition circuit, and stores the encryption key in a storage device. An encryption circuit encrypts the digital voice data using the encryption key. A transmitter then modulates the encrypted voice data onto an RF signal and transmits the RF signal to a base station in a wireless network. The base station uses the same encryption key to decrypt the signal before transmitting it to another base station or mobile unit. Signals transmitted from the base station to the mobile unit are encrypted and decrypted using a user-selected encryption key in a similar manner.

Issued: September 14, 2004

Inventors: Lowell Campbell and Daniel Robertson
Assignee: DENSO Corporation (Kariya, Japan)

US Patent: 6,792,111

Cryptation system for packet switching networks based on digital chaotic models

The present invention is a cryptation system for information transmitted through packet switching networks that masks digital information data by combining it at the transmitting station with digital data of a certain cryptation code before transmitting the so-encrypted data through the network. The system also performs an inverse decrypting processing at the receiving station using the same code.

About WSP Patent Listings

The US Patent and Trademark Office (USPTO) frequently grants fraud and security patents that will be of interest to some of our wireless security practitioners. Each patent includes the invention title – linked to the corresponding USPTO web page. We brief ly describe it and provide, at minimum, its inventor(s) and assignee (owner).

With the listing of patents provided each month, one can see *who* is doing *what* in the world of wireless 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.

The system generates at a transmitting station and at a receiving station, starting from a given pair of password codes or user key, a certain discrete chaotic model or map of the pair of codes or key, producing dynamically updated pairs of values of codes or keys every certain number of processing steps of the chaotic map. The data to be transmitted is masked by way of a logic combination with the current dynamically-updated keys at the transmitting station. The data is demasked at the receiving station by way of a logic decomposition of the digital data from the current dynamically-updated key, thereby returning the digital data to a normal non-encrypted condition.

Issued: September 14, 2004

Inventor: Francesco Italia, *et al*
Assignee: STMicroelectronics S.r.l. (Agrate Brianza, Italy)

Notable Reference:

[1] Kotulski, et al. *Discrete Chaotic Cryptography*. Polish Academy of Sciences, Institute of Fundamental Technological Research, PL-00-049 Warszawa Swietokrzyska 21, Poland. Jan. 13, 1997. pp. 381-394.

US Patent: 6,792,088

Telephone device capable of preventing unauthorized transmission when sending messages

A cellular phone decides with a transmission category decision portion whether a message is sent from an external device or from the cellular phone. In the case where the message is sent from the external device, a personal identification number (PIN) comparison portion compares the PIN sent from the external device with a predetermined PIN. A control portion permits the message to be sent from the external device only when the two PINs correspond to each other.

Issued: September 14, 2004

Inventor: Nozomi Takeuchi
Assignee: NEC Corporation (Tokyo, Japan)

US Patent: 6,789,202

Method and apparatus for providing a policy-driven intrusion detection system

One embodiment of the present invention provides a policy-driven intrusion detection system for a networked computer system. This system operates by receiving a global policy for intrusion detection for the networked computer system. This global policy specifies rules in the form of a global security condition for the networked computer system and a global response to be performed in response to the global security condition. The system compiles the global policy into local policies for local regions of the networked computer system. Each local policy specifies at least one rule in the form of a local security condition for an associated local region of the networked computer system and a local response to be performed in response to the local security condition. The system communicates the local policies to local analyzers that control security for the local regions. A local analyzer compiles a local policy into specifiers for local sensors in a local region associated with the local analyzer. These specifiers are communicated to the local computer systems in the local region. This allows local computer systems to implement the local sensors.

Issued: September 7, 2004

Inventors: Cheuk Ko and Jaisook Rho
Assignee: Networks Associates Technology, Inc. (Santa Clara, CA)

US Patent: 6,788,928

Cellular Phone

The present invention discloses a cellular phone that is easy to use, featuring a sufficient degree of security preventing unauthorized use by conducting a simple authentication operation, not perceived by the user. As the user holds the cellular phone by hand, the control unit issues an instruction to temperature obtaining units to start detecting the temperature. The temperature obtaining units measure the temperature at regular intervals, and successively transfer the obtained temperature data to a temperature comparator unit. The temperature comparator unit judges whether the temperature data obtained by the temperature obtaining units are lying within a predetermined condition, and issues an instruction to biodata units to obtain fingerprint data of the user depending upon the result of judgment. The biodata obtaining units obtain the fingerprint data of the user and transfer the obtained fingerprint data to a biodata authentication unit. The biodata authentication unit compares the obtained fingerprint data with the fingerprint data of the owner stored in a biodata storage unit, and judges whether the user is the proper user.

Issued: September 7, 2004

Inventor: Nobuaki Kohinata
Assignee: Hitachi, Ltd. (Tokyo, Japan)

US Patent: 6,788,729

Frequency hopping method and base station

The invention relates to a frequency hopping method and a base station including, at the receiver end, a number of baseband processing units and broadband receiver units, which form RF sub-bands and receive frequency hopping signals according to a frequency hopping sequence from the RF sub-bands they have formed. The base station includes, at the receiver end, a switching device and channelling unit, which receive baseband signals from an intermediate band and each of which is connected to a receiver unit forming a particular RF sub-band. The switching device selects, according to the frequency hopping sequence, the channelling unit whose baseband output provides the baseband signal which is connected to the baseband processing unit. The channelling unit places the baseband signals to its baseband output according to the frequency hopping sequence.

Issued: September 7, 2004

Inventor: Harri Posti
Assignee: Nokia Networks Oy (Espoo, Finland)

US Patent: 6,785,823

Method and apparatus for authentication in a wireless telecommunications system

This invention discloses a method and apparatus for allowing a mobile station in a wireless network to perform network authentication in association with mobile packet data services. The packet data serving node (PDSN) does not authenticate the mobile station with an authentication server prior to sending a CHAP (Challenge Handshake Authentication Protocol) success message. Rather, a mobile station is authenticated via an authentication server after the PDSN receives an IPCP message indicating whether the mobile station desires to use Mobile IP in the current session. If the mobile station desires to use Mobile IP, the PDSN uses authentication techniques in accordance with Mobile IP protocols.

In the preferred embodiment, if the mobile station does not desire to use Mobile IP, the PDSN authenticates the mobile station, querying an authentication server with the buffered contents of a previously received CHAP challenge response.

Issued: August 31, 2004

Inventors: Nischal Abrol and Marcello Lioy
Assignee: Qualcomm Incorporated (San Diego, CA)

Notable Reference:

[1] Perkins, Charlie. *Mobile IP and Security Issue: An Overview*. Proceedings of 1st IEEE-RPS Joint Conference on Internet Technologies and Services, Oct. 25-28, 1999. pp. 131-148.

US Patent: 6,785,790

Method and apparatus for storing and retrieving security attributes

This invention is an apparatus for providing security in a computer system. The apparatus comprises an address generator, a multi-level lookup table, and a cache. The address generator is adapted for producing an address associated with a memory location in the computer system. The multi-level lookup table is adapted for receiving at least a portion of said address and delivering security attributes stored therein associated with said address, wherein the security attributes are associated with each page of memory in the computer system. The cache is a high-speed memory that contains a subset of the information contained in the multi-level lookup table, and may be used to speed the overall retrieval of the requested security attributes when the requested information is present in the cache.

Issued: August 31, 2004

Inventor: David Christie, *et al*
Assignee: Advanced Micro Devices, Inc. (Austin, TX)

US Patent: 6,785,256

Method for extending mobile IP and AAA to enable integrated support for local access and roaming access connectivity

The present invention discloses a way to extend Mobile IP Authentication Authorization and Accounting (AAA) signaling to enable a node to request from a network operator combinations of home and local service capabilities (when roaming) in an efficient and scalable manner. It also enables the home and foreign service providers to constrain and account for actual services provided, based on a combination of the foreign and home operator policy.

Issued: August 31, 2004

Inventor: Alan O'Neill
Assignee: Flarion Technologies, Inc. (Bedminster, NJ)

www.flarion.com

Flarion Technologies is developing and deploying FLASH-OFDM®, a mobile broadband system enabling 'LAN-like' communications in a cellular environment. Flarion's product line consists of the RadioRouter® base station, modems (PC Card, CompactFlash Card, and Desktop modem), embedded chipsets, and system software to create an end-to-end FLASH-OFDM network for mobile operators. Flarion also licenses the FLASH-OFDM technology to facilitate the design of FLASH-OFDM enabled networks and computing devices (notebook PCs, handheld PCs, PDAs, web tablets, handsets, etc).

Flarion Technologies, Inc.
Bedminster One
135 Route 202/206 South
Bedminster, NJ 07921
USA

Phone: +1 908-947-7000
Fax: +1 908-947-7090

US Patent: 6,785,366

Scheme for registration and authentication in wireless communication system using wireless LAN

In the disclosed registration and authentication scheme, in the case of carrying out the registration and authentication of a wireless terminal with respect to a wireless base station provided inside the home, for example, a user of the wireless terminal must directly operate the wireless base station. For this reason, it is possible to prevent the registration and authentication of a wireless terminal of an external user who cannot easily operate the wireless base station, and thereby it is possible to realize the secure and easy registration and authentication processing even when the wireless communications are used.

Issued: August 24, 2004

Inventor: Hideaki Nakakita, *et al*
Assignee: Kabushiki Kaisha Toshiba (Tokyo, Japan)

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