Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 6, No. 10. November, 2004

Our Swan Song

David Crowe
Editor and Publisher

I have made the difficult decision to suspend publication of both *Wireless Security Perspectives* and *Cellular Networking Perspectives* with our December 2004 issue, after more than a decade of publication of the former and five years of the latter.

Subscriptions to the newsletters have not recovered from the telecom crash of a few years ago, and other commitments, such as my consulting engagement with Qualcomm, IRM and SID management responsibilities in IFAST and my chairmanship of TIA subcommittee TR-45.2, have made it more difficult to produce the newsletters.

The publication of a monthly newsletter has been a wonderful experience for me, and for those who have worked with me. I am very proud of what I have produced along with the help of editor Les Owens and with Doug Scofield's desktop publishing talents, Tim Kridel's writing and article sourcing expertise, and the invoicing and accounting assistance of Debbie Brandelli and Evelyn Goreham. Earlier in the production of the newsletters, Jordene Fletcher and Muneerah Vasanji also provided valuable assistance.

Back in 1992 when I first started *Cellular Networking Perspectives* I did not consider myself a writer, and still do not know where I found the confidence to offer my amateur writings publicly. I have concluded that one of the secrets of writing is practice (another is to always critically review your own writing at least twice), and with over two hundred newsletter issues under my belt, I certainly have had a lot of that! Only a couple of years after starting my newsletters, I found myself writing for an industry magazine (*Cellular Marketing*). Then *Cellular Business* actually wanted to pay me to write columns. All of this came as a great shock. Like riding a bicycle for the first time, suddenly you realize that it's really happening, although you do not quite understand how and are scared to think about it in case the magic comes undone.

I hope I do not sound too much like a defeated politician, but now it is time for me to move on to other challenges. Memories will not fade – the favorite issues, the struggle to fill in for promised articles that never materialized, and the joy of publishing something professional that only a short time before was a messy draft. In fact, with age, the memories may even improve!

Most of all I would like to thank you, our loyal readers, who inspired and encouraged me for so many years. I count many of you among my friends and colleagues, and appreciate the praise and encouragement that you gave us over the years (yes, and your occasional criticisms as well). Feel free to continue to contact me at David.Crowe@cnp-wireless.com.

As a parting offer, and to help to clear out our closets, we would like to offer you our remaining company golf shirts at $20 ($25 for shipment outside North America) each, including shipping. Please contact us at cnp-sales@cnp-wireless.com to make a purchase before it is too late!

Refunds to our subscribers will be processed in January, 2005.

The final issue of *Wireless Security Perspectives* is due …

December 30th 2004

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 **Payment**: accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery**: Email or 1st class mail. **Back Issues**: Available individually for $35 in the US and Canada and US$40 elsewhere, or in bulk at reduced rates. **Discounts**: Educational and small business discount: 25% off any order. **Copies**: Each subscriber is licensed to make up to **10** copies of each issue or back issue. Call for rates to allow more copies.

Technical Editor	Les Owens.
Article Sourcing:	Tim Kridel.
Illustration and Production:	Doug Scofield.
Distribution:	Debbie Brandelli.
Accounts:	Evelyn Goreham.
Publisher:	David Crowe.

Upcoming Mobile & Wireless and Wireless Security Events

Below are mobile & wireless and wireless security events (or events with sessions on these topics) for late November and December. Some of these upcoming events may be of interest to both the theoretician and to the practitioner. The name, dates and venue of the event, plus URL, are provided.

IEEE Globecom 2004

November 29th - December 2nd
Hyatt Regency Dallas
Dallas, TX

www.comsoc.org/livepubs/ci1/public/2004/nov/ciconfp.html

Wi-Fi Planet Conference & Expo Fall 2004

November 30th - December 3rd
San Jose McEnery Convention Center
San Jose, CA

www.jupiterevents.com/wifi/fall04/index.html

5th E-Gov Institute Information Assurance Conference

November 30th - December 2nd
Ronald Reagan Building & International Trade Center
Washington, DC

www.e-gov.com/events/2004/ia

Infonex – Deploying Wireless LAN

December 1st- 2nd
Delta Chelsea Hotel
Toronto, Canada

www.infonex.ca/inx/644/daytwo.html

Government Solution Summit

December 1st- 3rd
Hyatt Regency Coconut Point
Bonita Springs, FL

www.governmentsolution.com

SecureGOV 2004

December 5th- 7th
Homestead
Homestead Resort, VA

www.convurge.com/securegov2004/index.html

RTSS 2004 – 25th IEEE International Real-time Systems Symposium

December 5th- 8th
SANA Lisboa Park Hotel
Lisbon, Portugal

www.cs.unc.edu/~anderson/meetings/rtss04

Asiacrypt 2004

December 5th- 9th
Shilla Jeju Hotel
Jeju Island, Korea

www.iris.re.kr/ac04

2004 Advanced Technical Security Symposium

December 6-7
Quality Inn Hotel Conference Center
Columbia, Missouri

www.more.net/conferences/symposium2004/schedule.html

20th Annual Computer Security Applications Conference

December 6th- 10th
Hilton Tucson El Conquistador
Tucson, AZ

www.acsac.org/2004/glance.html

Wireless Community Networks Summit

December 7th- 8th
Inter-Continental Hotel
Miami, FL

www.wcai.com/event/05/w_gen.htm

Joint Wireless Working Group Fall 2004 Conference

December 7th- 9th
Atlantic City Hilton
Atlantic City, NJ

www.iaevents.com/JWWG/Info.cfm

US IPv6 Summit 2004

December 7th- 10th
Hyatt Regency
Reston, VA

www.usipv6.com

SANS CDI (Cyber Defense Initiative) East 2004

December 7th- 14th
Hilton Washington & Towers
Washington, DC

www.sans.org/cdieast04

Infosecurity New York

December 8th- 9th
J. K. Javits Convention Center
New York, NY

www.infosecurityevent.com

Building, Breaking, and Securing WiFi: Hands-on

December 10th
Wyboston Lakes, UK

www.7safe.com/wireless_security_training_course.htm

Upcoming Mobile & Wireless and Wireless Security Events (continued)

WITSP 2004 – The 3rd Workshop on the Internet, Telecommunications and Signal Processing
December 20th- 22nd
Stamford Grand Hotel
Adelaide, Australia
www.dspcs-witsp.com/WITSP_04/CFP.html

3rd International Trusted Internet Workshop
December 22nd
Taj Residency Hotel
Bangalore, India
vulcan.ece.iastate.edu/~gmani/tiw-2004

Plan ahead for ...

RFID: Impact on Supply Chain Management
March 8th- 9th
Toronto, Canada
www.informationexchange.ca/RFID

Japan Mulls Prepaid Ban

Japan is the latest country to crack down on prepaid wireless in an attempt to thwart crime. Under a proposal by the ruling Liberal Democratic Party, prepaid phones would be banned to halt scams. One example is calls made to elderly people, who are told that a relative is in trouble and can be saved only by an immediate transfer of money into the caller's bank account.

Not surprisingly, the proposal has encountered a backlash, particularly from Vodafone's Japanese unit, where 10 percent of customers are prepaid. Its largest rival, NTT DoCoMo, opposes the ban even though less than 1 percent of its customers use prepaid. The European Business Community, a trade group representing 3,000 companies, argues that the ban would stymie free trade and investment – and put U.K.-based Vodafone at a competitive disadvantage.

The ban's effect also is debatable. For example, extortionists could just as easily buy prepaid wireline cards and make calls from payphones. And although eliminating prepaid wireless would reduce their options, it would not reduce their victims' gullibility.

Japan's proposal comes on the heels of Switzerland's new rules for prepaid telecom services, aimed at thwarting terrorists. Prepaid is popular in Switzerland. Swisscom is the country's largest wireless operator, and about half of its 3.7 million customers use prepaid.

On July 1, Swiss service providers began collecting information about buyers before selling them prepaid products, including wireless. The new rules also require that operators track down the name, address and occupation of persons who bought prepaid cards within the past two years. In October, Swiss service providers also had to provide the same information for people who bought prepaid cards after Nov. 1, 2002. In cases where that information was not collected, service for that device or card must be blocked.

The June 2003 amendment to the Federal Mail and Telecommunications Monitoring Act is a response to what Swiss regulators and police say is "the increasingly anonymous use of prepaid cards by criminals, as well as the fact that Swiss prepaid cards are also being used in terrorist circles." One example: Senior members of al-Qaeda used prepaid cards bought in Switzerland to help plot the September 11 attacks, according to the Swiss Justice Ministry.

(For more on Switzerland's new prepaid regulations, see the **June 2004** issue of *Wireless Security Perspectives*.)

Mobile Viruses and Trojan Horses – Perspectives and Opportunities

Tom London and Patrick Townsend
InnoPath

Wireless users are becoming aware that viruses, Trojan horses and other threats to their PCs are migrating to their handsets. The first mobile virus – a worm named Cabir – appeared in June 2004 and targeted handsets running the Symbian Series 60 operating system. Cabir was soon followed by other attacks on Symbian-based handsets and on devices running the Pocket PC OS. (For more information on mobile viruses and related attacks, see the **September 2004**, **June 2004** and **March 2003** issues of *Wireless Security Perspectives*.)

Wireless data provides fertile ground for malware for several reasons. These include the number and sophistication of mobile devices, the highly-connected and distributed network in which they operate (especially when unfettered Internet access is included) and the burgeoning market for downloadable features and services. Fortunately, the viruses that have appeared so far have not been dangerous or destructive to the infected devices nor to the networks they exploited en route to the devices.

Independent software vendors (ISVs) have responded quickly and appropriately to the threat, but their work has only begun. Moreover, the ISVs are only part of the solution.

Unlike the PC world, wireless service providers will shoulder more of the burden of preventing virus propagation. While PC users have corporate networks, personal firewalls and secure log-ins, only the wireless carrier security infrastructure stands between most mobiles and the Internet. The PC world has taught us that these countermeasures are not always sufficient. Rather, mobile devices will only approach being adequately secured when they have anti-virus clients and mechanisms to update their virus definitions.

Enablers and Contributing Trends

The enablers for virus propagation are becoming commonplace. For example, the wide availability of 2.5G and 3G services, along with the ability to download applications and content, increases not only handset capabilities, but also the opportunities for viruses to spread. From increased memory capacity – to faster processors – to open file-based Operating Systems, handsets are increasingly vulnerable to processing intrusions.

Are You the Arcanist?

Last month, the question was: What are the next two digits in the series: 6180339 __ __? A hint mentioned the ancient Egyptians and da Vinci.

Greg Rose and David Ott, both from Qualcomm, submitted the correct answer, which was ... 88.

The series in its entirety, (.6180339887498948482045868343656 4), is the "The Golden Mean" (or Golden Ratio) – the number is found in nature and used in architecture, and is very pleasing to the eye. As a term applied in mathematics, it raises some fascinating questions and studies.

This month ...

What's next in this series?
9, 10, 11, 11, 12, 11 ...

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.

U - R - Linked:
GSM Security

www.gsm-security.net/gsm-security-faq.shtml

This is a nicely organized FAQ – a concise but thorough overview of GSM security, including cryptography for voice and data, and some non-cryptographic security topics such as TMSI (identity hiding) and SIM locking. Step-by-step details of GSM authentication are described, and also some GSM weaknesses, including how some of the security algorithms have been broken.

Information at the URL (above) is maintained by Network System Architects, Inc. Their sidebar includes links to GSM-related news, standards and more.

In proprietary and closed handset environments, software security is often simpler to implement. The 'walled garden' approach to guard content and access will eventually give way to the increased availability and exchange of applications and content. Open OSs, Java and BREW, for example, will create more uniform environments that could allow a single virus or Trojan to infect different handset models.

Because cell phones and other mobile devices typically connect to multiple networks (e.g., voice telephony and IP-based data networks), virus-like agents can cause damage including unauthorized access to premium resources, unauthorized communication with other devices, and unauthorized modifications to subscriptions. Such unauthorized activities could leave unsuspecting users footing the bill.

It took years for the PC world to mobilize against these threats, but then the rapid growth of viruses prompted a host of companies to provide a range of support capabilities. This legacy bodes well for mobile device protection. However, virus protection is currently available for less than 10 percent of handsets – those with open OSs. More than 90 percent of handsets today are unprotected.

Until operators, handset manufacturers and the application and content vendors jointly address the issue of security for all handsets, the larger issue of protection will remain unaddressed.

Cyberthreat Vectors

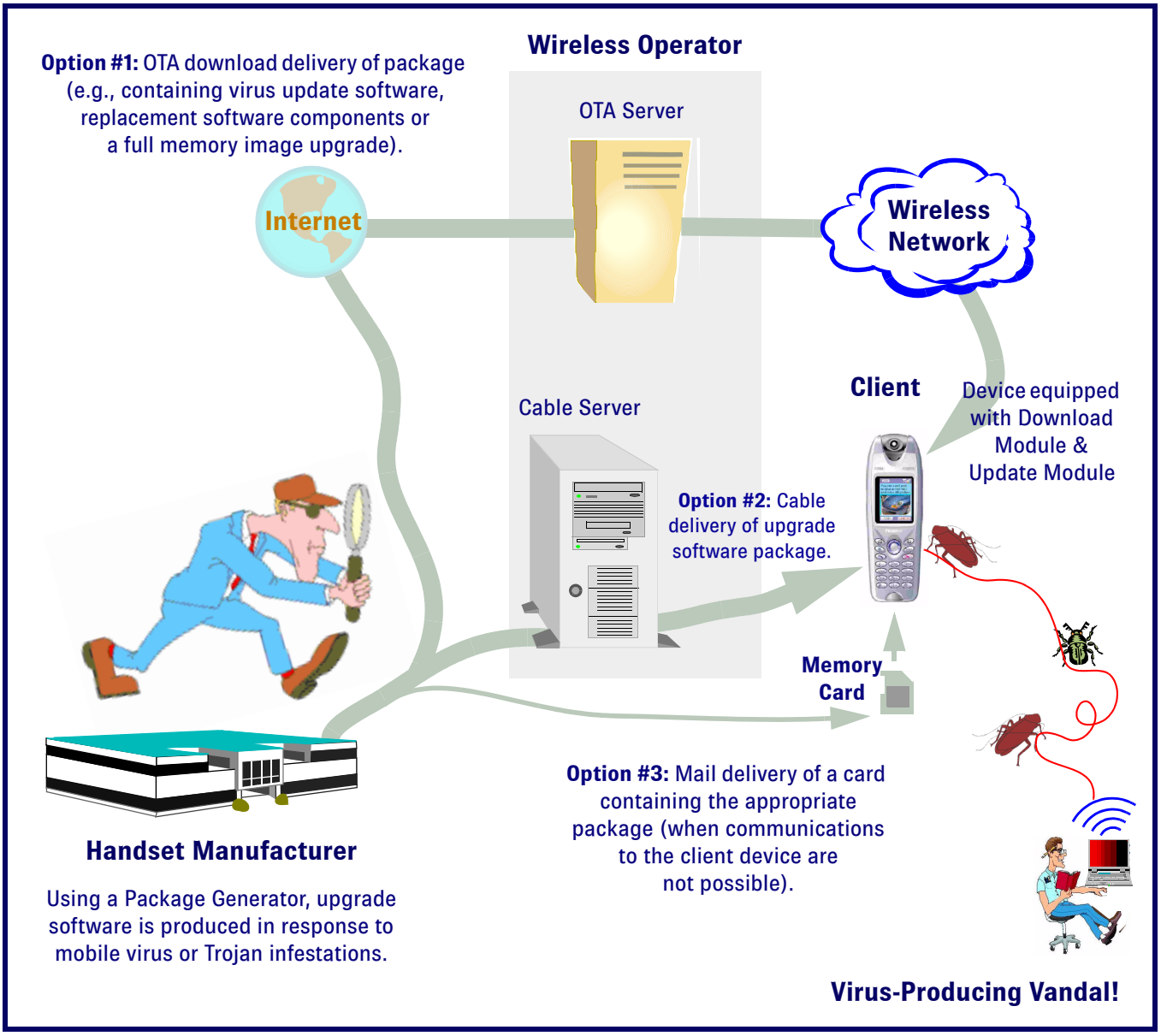
To date, mobile viruses appear to be only proofs-of-concept. That is, they have demonstrated only their ability to propagate. They have not caused any damage, nor turned mobile phones into spam-bots.

Even the ability of viruses to change a mobile device's configuration – a seemingly harmless occurrence – could reap havoc and increase subscriber dissatisfaction. As many handsets use standards based on configurations, parameters could be altered to maliciously switch users to other operators, roam on costly partner networks, and worse. For example, settings could be changed to allow the download and installation of applications.

As in the PC world, another cyberthreat is that of malware grabbing information such as account numbers during m-commerce transactions. This scenario, and those causing parameter changes, could occur without the user's knowledge.

Cures for these threats can be quite complex. At the point-of-sale, the customer is given no means for restoring virus-damaged software embedded in the device. Removal of a virus or Trojan from a cell phone is not the same as their removal from a PC. The wireless operator or handset manufacturer could repair it, of course, although this option would often be expensive and time-consuming. A better solution, however, is to leverage from a wireless service provider offering an over-the-air (OTA) upgrade capability, as illustrated in Figure 1.

Figure 1: Three Ways to Find and Swat the 'Bugs' in a Mobile Device



Native Code Complications

Most handsets today run only native code applications, which present some unique challenges. Although Java and BREW applications are becoming more common, it will be many years before these outnumber native code applications.

Installing anti-virus protection after handsets using native code architectures have left the factory is nearly impossible. Handsets do not support the installation of applications separately, nor do they support after-manufacture update, because of various handset limitations.

Recently, firmware-update technology has become pervasive in the Japanese market. This technology can be leveraged to install and update anti-virus applications and their definition files used to recognize viruses. (For a look at how OTA firmware updates can be delivered securely and efficiently, see the **June 2003** issue of *Wireless Security Perspectives*.)

This approach kills two birds with one stone. OTA updates let operators fix security holes in the handset while at the same time installing and updating virus protections.

Solution Framework

From the subscriber's point of view, the handset is supported by the wireless service provider. The logo on it is usually that of the service provider, rather than the manufacturer. Intuitively, the logo identifies who to contact when problems occur.

This can provide a giant opportunity. It can also become a customer support headache that drains off profits. Service providers who address security pre-emptively can protect their marketing success. Failure to provide adequate protection may deter new prospects and disillusion current customers whose devices suffer virus attack. Many customers purchase long-term service contracts, but if anti-virus solutions are not part of the deal ... many will say "no deal," especially as virus problems become more prevalent. The door to increased revenue, then, is opened by offering anti-virus solutions.

Best practices require that ASPs providing applications and content support methods of protection and barriers against hackers and viruses. These protections will have to be scalable and standardized. Methods to deal with unauthorized programs and catalysts have been developed during the past few years. Three inter-connected techniques are typically used:

- Network detection and filtering;
- Client detection and;
- Removal and cleansing of the client.

By far, the most effective way to prevent the spread of viruses is to prevent them from passing through a network. Most networks filter and screen message content, especially at network gateways. It is clear that mobile network operators will need to keep abreast of best practices in this field. In fact, there is evidence that doing so reduces customer care and network bandwidth costs, and is especially well received by subscribers.

Quote of the Month

"In the land of the blind the one-eyed man is king."

Niccolo Machiavelli, 1469 -1527
Florentine statesman and philosopher

It has not been possible for wireless operators to eliminate all messages carrying viruses. The release rate of new viruses is so high that there is often a time lag before operators can deploy anti-virus measures. Client devices need to be made resistant to attacks, or at least not contagious. Methods of hardening the base system software include removing buffer overruns and other bugs, and ensuring appropriate controls on changing or adding capabilities.

Maintaining up-to-date software, especially the essential definition files, requires an on-going distribution infrastructure. The logical structure is well developed for the Internet and will likely require little modification to function effectively in the mobile world. For quality and performance reasons, few wireless operators can tolerate reflashing the entire handset storage memory image.

Update technologies, such as those deployed by InnoPath, allow applications and software to be delivered over the air to handsets currently in use. The update software is then installed with little to no impact to the remaining device firmware. Update technologies will enable wireless operators to respond to new threats and provide their subscribers with up-to-date protection.

Infection Response Scenarios

In a best-case infection scenario, handset anti-virus software recognizes and removes corrupted application or data software, and the device is restored to full operation. However, once corrupted software has been removed, full operation may not be restored. Consequently, the anti-virus software may need to perform a second task of recognizing degraded operation and components.

Another layer of protection that will likely be implemented is diagnostic software with the ability to track core operational functions of a device and responding to abnormal patterns.

Function call patterns can be more readily monitored when all calls between components are routed through a specialized component, such as InnoPath's Dynamic Addressing (DA) Manager component. This method was originally developed to prevent changes in one software component from cascading and

causing changes in the code of other components. DA drastically reduces the size of upgrade package files that represent the difference between two versions of mobile device software. In fact, DA makes upgrade time-independent of mobile device memory image size.

The next level of infection severity would result in degraded components after anti-viral cleansing. This damage could be countered by OTA downloading and re-installation of all affected software components. OTA re-installation could stop an infection cold, without subscriber intervention.

The worst infection scenario would involve a brand new virus. Device diagnostic alerts could be the first indication of trouble. Because the severity of disruption would vary with the attack method, service support will need a variety of counter-methods to bring devices back from the brink. Critical operational areas include the device core, communication and upgrade functions.

Currently, if core functions are corrupted in this worst scenario, the device must be returned to a point-of-sale, which is an ideal place to capture brand new viruses infecting the storage memory image. For the wider mobile community, later analysis will yield the cure. The wireless service provider would offer a solution for the ailing device, which would be a full memory image upgrade to restore full health.

The recovery scenario improves significantly if core and upgrade functions remain healthy. If communication is still intact, OTA software component replacement may fully restore the device with minimal disruption. If communication is not possible, a full image upgrade could be loaded onto a memory card and mailed to the customer (Option #3 in **Figure 1**).

Challenges and Opportunities

Factors complicating the deployment of solutions range from fragmented handset technologies to the growth in mobile-to-mobile communication. Handsets, which are embedded devices by design, will need extensive testing so that security updates do not impact more than this peripheral function. Security products and services in mobile networks must address these complications.

Complete solutions will include protection contained in the network and on the handset. Given the state of the art in handset technology, these solutions must involve handset manufacturers, wireless operators, and ISVs providing software to these parties. OTA firmware update technologies are best positioned to deliver security solutions by providing the fastest and most secure, flexible, and convenient delivery of any type of software to existing mobile customers.

About the Authors

Tom London is VP of R&D at InnoPath Software. He has held a variety of management and lead technical positions with companies such as Concert, AT&T and Bell Laboratories. Most recently, London was CTO and founding partner of Aruba Media. London holds numerous U.S. and global patents and was a major contributor to the early versions of UNIX, where he helped create the first versions of UNIX for the DEC VAX-11 computer line. He co-authored *Networks in a Flash – Making Broadband for You*, which simplifies the broadband installation process.

Peeping Tom Camera Phones

Tim Kridel

With multiple hinges, the Sharp V602 camera phone is already a contortionist. Thanks to an infrared filter accessory, it now has privacy advocates bent out of shape.

Dubbed the "pervert filter," the device attaches to the camera and turns it into the equivalent of night-vision goggles, capable of seeing through clothes. The filter works by detecting infrared radiation, which includes body heat. A body is hotter than clothing, so the filter provides a rough, X-ray-like view of the wearer. By some accounts, the filter offers the best resolution through dark-colored underwear.

A Tokyo-based defense contractor, Yamada, manufactures the filter, which was designed for military applications. How the filter wound up in the gray market as a camera phone accessory is not clear, but word quickly spread over the Internet. Although Yamada says that the filter should be used only for "academic purposes," it has not blocked sales despite the hoopla.

"We only sold these filters because we expected the night shot function would be used for taking pictures such as a baby asleep in bed, or the fine details of a leaf," a spokesman told the *Times* newspaper in London.

Although the $180 filter is available for shipment to most countries, so far, the privacy concerns are limited to Japan, the only market where the V602 is sold. But in theory, the filter should work with any phone that has a high-resolution camera and auto-focus, so it may become a PR nightmare for more than Vodafone, whose Japanese unit sells the V602. "We would never go to market with a phone with any kind of capacity to see people naked," a Vodafone spokeswoman told CNET.

Nor would most companies – at least not intentionally. But two years ago, Sony had to stop selling a video camera after word spread that the built-in night filter could see through clothing. People who work in the nude also find camera phones irritating. For example, the Bazooka's Showgirls strip club in Kansas City uses a sledgehammer to disable camera phones caught photographing its dancers.

London holds a B.A. from the University of Pennsylvania, and earned graduate and doctorate degrees from Cornell University.

Patrick Townsend-Wells is senior technical writer at InnoPath Software, where he oversees the documentation department. Prior to joining InnoPath, Townsend was the senior technical writer in charge of documentation and patents for U.S. Wireless, a geolocation telecommunications company.

About InnoPath Software

InnoPath Software (formerly DoOnGo Technologies) provides an easy, cost-effective way to deliver the best possible user experience on handsets through faster updates and by enabling better personalization. InnoPath is the only over-the-air mobile device management company actively updating handset software in commercial deployments. Its flagship product, DeltaUpgrade Plus, helps wireless operators and handset manufacturers keep mobile device software and firmware current and functional. Today, more than 35 million active subscribers are experiencing the value of patented InnoPath update-ready technology. For more information, see www.innopath.com.

Fraud and Security Patent News

US Patent: 6,823,520

Techniques for implementing security on a small footprint device using a context barrier

This invention discloses means for a context barrier. By the inclusion of a context barrier, isolating the execution of the programs, a small footprint device (such as a smart card) can securely run multiple programs from unrelated vendors. The context barrier performs security checks to see that principal and object are within the same namespace or memory space, or to see that a requested action is authorized for an object to be operated upon.

Issued: November 23, 2004

Inventor: Joshua Susser, *et al*
Assignee: Sun Microsystems, Inc. (Santa Clara, CA)

Notable References:

[1] Cordonnier, et al. *The concept of suspicion: a new security model for identification management in smart cards.* 1997.

[2] Sun Microsystem. *Java Card 2.0 Programming Concepts.* Oct. 15, 1997. Revision 1.0 Final.

[3] Gong, L., et al. *Going beyond the sandbox: an overview of the new security architecture in the JavaDevelopment Kit 1.2.* Proc. Usenix. Sym. Internet Technologies and Systems, Dec. 8, 1997.

[4] Islam, et al. *A Flexible Security Model for Using Internet Content.* IBM Thomas J. Watson Research Center Papers, Jun. 28, 1997.

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.

US Patent: 6,823,461

Method and system for securely transferring context updates towards a mobile node in a wireless network

This invention discloses a method and system for transferring contexts from a previous access router (PR) to a new access router (NR) that is subsequently associated with a Mobile Node (MN). For example, transferred contexts may include, but are not limited to, Security, Quality of Service (QOS), Header Compression, and Buffers. A context is transferred from the PR to the NR. Any change in an element of the context is conveyed by the NR to the MN in a secure fashion, even though a Security Association does not yet exist between the NR and MN. The NR provides an authenticated security context update to the MN, e.g., advising when the type of encryption has changed from Triple Data Encryption Standard (DES) to DES. The NR utilizes the Security Association between the PR and the MN to provide such an authenticated security context update to the MN over a RAN or a wireless LAN.

Issued: November 23, 2004

Inventor: Lakshmi Narayanan, *et al*
Assignee: Nokia Corporation (Espoo, Finland)

Notable References:

[1] Hamer, et al. *Issues In IPSec Context Transfer.* Internet Draft, Internet Engineering Task Force (IETF), Feb. 2002.

[2] Kempf. *Problem Description: Reasons for Performing Context Transfers Between Nodes In An IP Access Network*. Internet Draft, IETF, Sep. 2002.

[3] Tsirtis, et al. *Fast Handovers for Mobile IPv6*. Internet Draft, IETF, Sep. 30, 2002.

US Patent: 6,823,189

System and method for identifying mobile communication apparatuses proximal with an identification locus

The present invention is a system for identifying at least one selected mobile communication apparatus proximal with an identification locus which includes: (a) a mobile communication base facility in communication with a plurality of mobile communication apparatuses that include the selected mobile communication apparatus; (b) at least one location-indicating device emitting a location-indicating code and is installed in each of the selected mobile communication apparatus; the location-indicating code relates a geographic location and an individual identification of a respective selected mobile communication device; and (c) at least one supported unit in communication with the mobile communication base facility. At least one of the mobile communication base facility and the supported unit have on-line access to an information store and a locator. The information store cooperates with the locator in receiving the location-indicating code to relate the individual identification with respective contact data for a respective selected mobile communication device.

Issued: November 23, 2004

Inventor: Akhter Akhteruzzaman, *et al*
Assignee: Lucent Technologies Inc. (Murray Hill, NJ)

US Patent: 6,823,185

Systems and methods for performing authorized intercept in a satellite-based communications system

This invention discloses means for performing Authorized intercepts of communications in a satellite communications system. By this means, a law enforcement agency (LEA) can request the intercept of communications to and/or from subscriber units (SUs). In one embodiment, an LEA intercept request causes an intercept order for a particular target SU to be transmitted to one or more satellites, where the intercept order is stored in an intercept table. Any communications traffic involving the target SU results in an intercept by a satellite, which routes a copy of the intercepted communications to the requesting LEA, either directly or via an associated intercept facility.

Issued: November 23, 2004

Inventor: Erwin Comer, *et al*
Assignee: Motorola, Inc. (Schaumburg, IL)

Further information on these patents:

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

US Patent: 6,823,068

Denial cryptography based on graph theory

This invention discloses an encryption method that is based on charting a path on a graph, where the graph is the encryption key. The plaintext expresses that path through a sequence of graph vertices, and the ciphertext expresses the same through a sequence of edges between these vertices. There are numerous ways to construct the graph to match a choice of plaintexts with a single ciphertext.

Issued: November 23, 2004

Inventor: Gideon Samid
Assignee: Same

Notable References:

[1] British General Staff, *Manual of Cryptography*, Aegean Park Press (1919).

[2] Yasuhiro, et al. *Dual reduction Method of Random Keys for Encryption by Graph transformation*. 1988.

[3] Gaines, *Cryptanalysis*, 1956.

[4] Gideo Samid. *Cryptographic Possibilities Suggested by Certain Expansion-Reduction Algorithms.* AGS Encryptions, Ltd., Jul. 4, 1999, pp. 1-23.

US Patent: 6,819,244

Chipless RF tags

This invention is a method of marking an article to enable its identification, by applying to the article a conductive path, which is at least partially coated with a dye layer of at least one compound selected from: voltage sensitive fluorescent dye (VSFD); mixture of VSFD dyes; electro luminescent (EL) compound; OLED compound; or mixtures thereof. The dye layer is excitable to emit fluorescent radiation, which serves to identify the article.

Issued: November 16, 2004

Inventor: Shlomo Dukler, *et al*
Assignee: Inksure RF, Inc. (Tenafly, NJ)

US Patent: 6,819,219

Method for biometric-based authentication in wireless communication for access control

This invention discloses means for biometrics access control. Smart cards systems that are used in biometric authentication are slow in processing and the cards themselves have the added disadvantage of being misplaced or lost. Moreover, storing biometric data (on a database) over a network poses security issues that can be compromised in extreme instances. Significant security can be achieved if the biometric templates are stored locally in a portable device. A user can use the portable device to either transmit wirelessly the stored biometric for authentication purposes, or a user can locally measure a biometric using the portable device and match it against a biometric which is also stored locally (in the portable device).

Issued: November 16, 2004

Inventor: Rudolph Bolle, *et al*
Assignee: International Business Machines Corporation (Armonk, NY)

US Patent: 6,816,969

Digital signature generating method and digital signature verifying method

In a signature generating method where not necessarily all of a plurality of signature generating devices work together each time to generate signatures, the present invention seeks to correctly and securely reflect data relating to previous signatures. When generating signatures, the data used for the next signature is sent beforehand to the other signature generating devices. Also, when generating signatures, at least one of the devices is used consecutively, thus allowing history data to be shared during signature generation.

Issued: November 9, 2004

Inventor: Kunihiko Miyazaki
Assignee: Hitachi, Ltd. (Tokyo, Japan)

Notable References:

[1] Campbell. *Supporting Digital Signatures in Mobile Environments.* Twelfth IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises, Jun. 9-11, 2003, pp. 238-242.

csdl.computer.org/comp/proceedings/wetice/2003/1963/00/19630238abs.htm

[2] Wong, et al. *Digital Signatures for Flows and Multicasts.* IEEE/ACM Transactions on Networking, vol. 7, Issue 4, Aug. 1999, pp. 502-513.

US Patent: 6,815,722

Detecting and preventing fraudulent use in a telecommunications network

The invention relates to a method and an arrangement against fraudulent use in a telecommunications network. The invention is based on the idea that at least one fraud profile identified by an identifier is created and the identifier is included in the subscriber data of some subscribers. Based on this identifier, the fraud restriction parameters of the subscriber are retrieved from the subscriber's fraud profile, and these fraud restriction parameters are used in detecting and indicating possible fraudulent use. The fraud restriction parameters include values for different service limits, such as the maximum number of call forwarding requests and/or the maximum number of location updates during a certain period, and possibly, at least for some features, an action parameter related to a service limit and implemented when the service limit is reached.

Issued: November 9, 2004

Inventor: Vesa Blom, *et al*
Assignee: Nokia, Inc. (Espoo, Finland)

Notable References:

[1] Eleftheriadis, et al. *User profile identification in future mobile communications system.* IEEE network, Sep./Oct. 1994, pp. 33-39.

[2] Japanese Laid Open Patent Application No. H-9-121-387, entitled "Mobile Communication Network and a Method of Locking a Selected Mobile Phone in the Mobile Communication Network." May 6, 1997, Paul S. Meche, et al.

US Patent: 6,816,090

Mobile asset security and monitoring system

The present invention is a mobile asset security system that enables remote tracking and monitoring of the asset. The security system is equipped with a control and intelligence unit, a position determining device and a number of intrusion detection devices. The control and intelligence unit processes information from the position determining device with the help of an in-built virtual mapping system to obtain geographic information of the vehicle in the form of name of place, street, coordinates, etc. The control unit may be remotely configured and controlled through a built-in voice recognition and DTMF tone detector. The geographic information and information regarding any violation of intrusion detection devices is converted to synthesized speech using a text to speech system. The text to speech system converts the speech to a language desired by the user. The synthesized speech is transmitted to the user's communication device over an existing communication network.

Issued: November 9, 2004

Inventor: Ashok Teckchandani
Assignee: Ayantra, Inc. (Fremont, CA)

US Patent: 6,813,625

Method and device for self-clock controlled pseudo random noise (PN) sequence generation

The present invention is a method and device for use, e.g., in a mobile telephone, for self-clocked controlled pseudo random noise (PN) sequence generation, which comprises a plurality of sequence generator units for outputting a plurality of sequence values (Z_t) on the basis of a plurality of clock values (Ct), and step pattern generators for selecting a step pattern, comprising said plurality of clock values (C_t), from a plurality of possible step patterns on the basis of a step pattern select signal (W_t). Thus, a flexible and efficient self-clocked controlled pseudo random noise (PN) sequence generation is obtained.

Issued: November 2, 2004

Inventor: Ben Smeets
Assignee: Telefonaktiebolaget L M Ericsson (Publ) (Stockholm, Sweden)

US Patent: 6,813,491

Method and apparatus for adapting settings of wireless communication devices in accordance with user proximity

This invention discloses improved approaches for adapting settings of wireless communication devices based on estimated proximity to respective users. In accordance with one aspect, one or more settings of a wireless communication device can be automatically altered in accordance with motion (if any) of the wireless communication device. Consequently, settings of the wireless communication device can be dynamically adapted based on the proximity (e.g., motion) of the wireless communication device to its user.

Issued: November 2, 2004

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