Wireless Security Perspectives

Cellular Networking Perspectives

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

Cryptography In The News

At an IEEE (Institute of Electrical and Electronics Engineers) standards committee meeting in New Jersey on June 24, the IEEE ratified the 802.11i security specification for 802.11 wireless LANs. The specification, which has been much anticipated by vendors and consumers around the world, contains the standard replacement for current "Wi-Fi" networks with the fatally flawed and frequently vilified Wired Equivalent Privacy (WEP) security mechanism. Weaknesses were discovered in WEP nearly five years ago and it has been the subject of considerable press and industry activity. See the **November 2002** and **November 2003** issues of *Wireless Security Perspectives* or download special publication 800-48 (a PDF file) from NIST for more information on WEP.

At the heart of the 802.11i specification is the NIST's Advanced Encryption Standard (AES) for the encryption of data between client stations and access points. AES will provide very robust cryptographic protection for 11i networks, to guard against unauthorized viewing of packets that flow through the ether. The use of AES in the new 11i networks – so-called Robust Security Networks – should render Kismet, Airsnort and other hacker tools useless. This will come as a welcome relief to those network administrators who still rely on WEP, with its improper use of the RC4 algorithm.

On the negative side, however, the use of AES may require that consumers totally replace their existing APs and network interface cards. This "fork-lifting" of Wi-Fi equipment is because many vendors plan to implement AES in custom, dedicated hardware to efficiently perform the encryption and decryption processes. We shall see.

See also www.wi-fiplanet.com/news/article.php/3373441

Quote of the Month

"Science is built up of facts, as a house is built of stones; but an accumulation of facts is no more a science than a heap of stones is a house."

Henri Poincarè

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…

July 15th 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.

Getting Ready for Harmful Content on Mobile Terminals

Matias Impivaara, F-Secure Corp.

June 14th 2004 marked a milestone in wireless history: the first real mobile phone virus, a worm named Cabir infecting Symbian mobile phones that support the Series 60 user interface platform. Although there have been no reports of the worm spreading in the wild or that it poses a direct threat to phone users, it clearly shows there are virus writers who can now create viruses for mobile devices.

Just how great a threat mobile viruses will become is difficult to predict. Nevertheless, it is safe to assume that this incident will not be the last, as others refine Cabir and introduce more sophisticated ones to catch some of the fame of Cabir's writers.

Before this first mobile phone worm there were some denial-of-service (DoS) attacks through, for example, bad SMS messages, malformatted WAP pages or reverse-engineered over-the-air messages. (See the **March 2003** *Wireless Security Perspectives* for information about the Nokia 6210's vulnerability to a DoS attack via a malformed vCard). SMS messages have been used to deliver unwanted and harmful content, and settings of mobile phones have been changed with smart messages (Smart Messaging is a concept for sending and receiving ring tones, picture messages, operator logos, business cards, calendar requests, and Internet settings over the Short Message Service (SMS)).

Some problems are by-products of other trends. Manufacturers are rapidly releasing new mobile devices, but that can lead to inadequate testing, making them more vulnerable to malfunctions, including security weaknesses. At the same time, standards are not complete, which allows room for misinterpretation in their design. These defects are not always severe, but they are still annoying and unpleasant for users.

So far, the smartphone developer community has been relatively small and business-oriented, but it is steadily expanding to new applications areas. Just as anti-virus software vendors have gained experience and knowledge of virus protection over the past years, so, too, have the virus writers. Their capabilities should not be underestimated. Virus evolution in the mobile environment could be faster than in the traditional PC world. The misuse possibilities are considerable.

Challenge spurs on many virus writers. It is unfortunate that there are many who would like to become famous as the creator of the first real widely spread and damaging virus for handheld devices. Their opportunities increase with each new advanced handheld device that hits the market.

Wireless offers new motivations for virus writing. Due to the direct link between mobile devices and billing, financially driven viruses may appear, causing significant costs for users, operators and service providers.

Prerequisites for a Large-Scale Virus Incident

When comparing the vulnerability of operating systems, the main criteria are the openness of the platform and the functionality it offers. In this sense, there are no major differences between the most common handheld platforms.

In general, the following conditions need to be met before a large-scale malware outbreak on an open platform can occur:

Scale – To be an interesting target for virus writers, a platform must running on enough devices.

Functionality – A device must have enough functionality for the virus to exploit. In a simple device, viruses cannot be sophisticated, so the possibilities to generate a big virus incident are limited. That situation is changing as devices add intelligence and functionality. Meanwhile, as users become more comfortable with wireless data, they are demanding more from their devices and services. The marketplace responds by spawning value-added services to attract people to download and share applications – potentially including viruses. Finally, mobile devices are replacing laptops for some business users, creating more opportunities for virus writers.

Connectivity – Network technologies such as CDMA2000 1X and GPRS can provide an "always-on" connection. The potential for spreading viruses is further magnified when devices have multiple communications capabilities such as Bluetooth, infrared, WiFi and SMS. Indeed, Bluetooth was a key medium for the Cabir worm. For more information on Bluetooth-related vulnerabilities, see the **February 2004** and **November 2003** issues of *Wireless Security Perspectives*.

These requirements are starting to be met for the major open handheld platforms, such as Symbian OS and Windows Mobile.

Possible Threats

Security challenges to be expected in the mobile environment are similar to those already encountered in the PC and Internet worlds. The Cabir worm gives us a good preliminary indication. It was packed in a Symbian installation file (.sis) named *caribe.sis*. When installed in the phone, the worm activated automatically and started looking for new devices that use

Bluetooth. It continued even if the user tried to disable Bluetooth via the phone's system settings. Once it found Bluetooth phones in discoverable mode, the worm tried to replicate by sending itself to them.

The Cabir worm's ability to spread hinges on whether the receiving phone's user chooses to accept and install the received file. F-Secure has already seen vulnerabilities in some Bluetooth implementations, so it is possible that in future versions, the spreading could be more automated.

It is also possible to send messages and open TCP/IP connections directly from applications which, when misused, could offer additional ways for the malware to spread. Should it manage to send MMS or SMS messages, it would result in unexpected usage charges. The technology for this kind of virus is available, and as the PC environment has shown, even when it is not, a convincing message can trick users into helping spread a virus.

Another possible threat comes from Trojan horses in games, screensavers and other applications. These could result in false billing, unwanted disclosure of stored information, and deleted, corrupted, modified or stolen user data. Similar applications can also be used for eavesdropping and gaining unauthorized access to corporate networks.

In addition to malicious, actively spreading applications, it is likely that we will see DoS and system-unavailable attacks, too.

Challenges may also emerge with cross-platform software, such as BREW and J2ME, although the basic design of these is usually considered to be secure. As the number of applications and phone models that can download executable code increases, it is no longer possible to thoroughly verify the behavior of all content on all device models before publishing.

When applications are pre-tested and signed, the signing process must be light in order to maintain the attractiveness of the distribution channel in comparison to open systems. This approach leaves room for vulnerabilities and undocumented features that can spread regardless of the control.

In open systems, where a large community of independent software vendors offer applications to mobile phone users without pre-testing, antivirus software and on-the-fly incompatibility scanning of the content help ensure the functionality of the downloaded applications. With Java, the biggest risks from harmful content relate to vendor-specific extensions that let applications access personal information and communication channels in the device.

Mobile Spam

The most worrisome malware scenarios in the mobile environment are not coming from the stereotypical virus writers, such as teenagers, but from more organized parties. In the PC world, spam and online crime currently are behind most of the largest worm outbreaks. The same phenomenon could be repeated in the mobile world.

In the PC world, spammers are outsourcing virus creation to virus writers in order to infect large numbers of machines. The machines are then used to send spam and host Web sites for the spammers' purposes, hiding their identities. Looking at the future of SMS/MMS spamming, one credible scenario is that mobile spammers would spread viruses to infect large amounts of handsets. Then those handsets would silently start to send SMS/MMS spam to all the numbers in their phonebooks. In this scenario, the handset's owner would bear the cost of spamming – and hide the identity of the spammer.

It is almost certain that something like this scenario will happen in the future, but estimating when is much more difficult. With PC spam, this phenomenon appeared roughly eight years after the first spam attacks occurred. Now that the business model has been established in the wired networks, the first attempts in wireless may occur much sooner after the first virus.

Are You the Arcanist?

Our question last month (for which there was no winner) gave: [616, 150, 634]; [600, 250, X] and asked for "X".

These are each a series of "Pythagorean Triplets." Remember $a^2 + b^2 = c^2$? In the first triplet, a=616, b=150 and c=634. There are an infinite number of these!

To complete the second triplet:

Since a=600 and b=250, then the third term is derived by solving for c :

$$\mathbf{c} = \sqrt{600^2 + 250^2} = \mathbf{650}$$

The question for this month:

For the series: 9, 45, 161, 405, 825, (N) ....
What is (N)?

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

Required Solutions

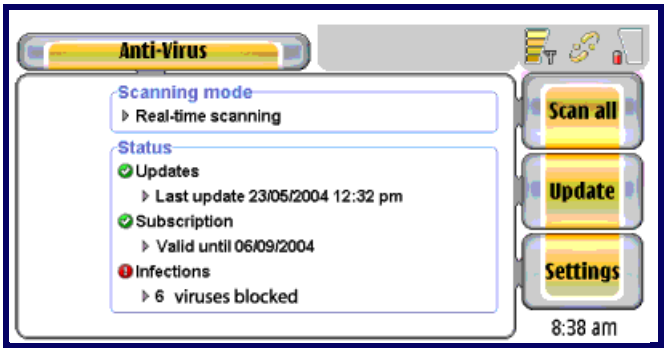
The good news is that wireless operators are well positioned to offer safeguards to their customers. The success of security services offered by European operators shows that PC users prefer subscription-based security services over traditional software licensing.

For a complete content-security solution, the operating system (OS) and device vendors will have to work together to implement a security-focused OS hot-fix process. Service providers should establish a two-tier reactive protection mechanism against new threats:

- A real-time, up-to-date antivirus product in the handset, with a mechanism for automatically delivering updates directly to the device.
- A gateway-level mechanism in the network for flexibly filtering the traffic.

There are several mobile-security solutions already on the market, ready to be implemented by handset manufacturers and mobile operators looking for ways to differentiate their offering as a secure solution. One example is F-Secure's Mobile Anti-Virus, which provides on-device protection for Symbian OS terminals and a hosted update service with over-the-air anti-virus updates through a specific SMS update mechanism or HTTPS connections. It has already been tested in several operator networks.

Figure 1: Mobile Anti-virus Scan Screen



Another option is a network solution like the F-Secure Mobile Filter, which is a security proxy that lets operators filter content. It has been delivered to several operators to block harmful software and incompatible Java applications in the network before they are download to users' devices.

In corporate environments, the emerging mobile security challenges call for a new security policy. Given handheld devices' unique issues, existing corporate security polices usually do not cover all the aspects of their protection. Enterprises should expand security policy guidelines to cover handheld devices or establish a separate handheld device security policy. At the very least, all mobile devices running an open OS should be required to use an automated anti-virus solution.

Future of Mobile Content Security

In the future of mobile content security, it is likely that anti-virus clients will evolve toward general security clients, which may offer, for example, combined application control and firewall functionality. In the long term, features may include other content security functions, such as intrusion prevention, parental control and spam filtering.

The evolution from simple solutions toward integrated, multi-functional entities will be necessary to ensure compatibility and interoperability in the terminal. Other key aspects will continue to be automation, ease of use and timeliness of updates. The ideal product should be automated and easy to manage, providing reliable and transparent on-device protection. Innovative and advanced solutions, as well as business and service models with over-the-air update mechanisms, will be necessary to ensure that mobile devices are protected at all times.

With the debut of the first real mobile worm, wireless users should be concerned about the security of their devices now, even if they were not before. Users should not be troubled with security any more than is absolutely necessary. The burden of managing and updating security applications should be taken out of their hands.

For wireless operators and device manufacturers, a wireless anti-virus service is insurance against end-user support loads, terminal downtime, negative user experiences and bad publicity. Like all insurance investments, those companies need to weigh the risk and the cost of preparing. If ignored or overlooked, harmful content in mobile terminals can cause severe damage to their customers and to their reputation as a carrier. The solutions are already available.

About the Author

Matias Impivaara (matias.impivaara@f-secure.com) is owner of a mobile anti-virus business and head of product management in the mobile security unit of F-Secure Corporation. He is also responsible for the company's joint activities with mobile device manufacturers. He joined F-Secure in 2000 and worked in business development and product marketing positions in the company's mobile security business.

Impivaara has several years of experience in the mobile phone business on all major markets. Prior to joining F-Secure, he worked at Nokia, where he held several positions in the product creation and business development departments in its Mobile Phones unit. Mr. Impivaara has a M.Sc. (Tech.) degree from Helsinki University of Technology in Finland.

About F-Secure

Founded in 1988, F-Secure Corp. (www.f-secure.com) specializes in centrally managed security solutions for the mobile enterprise. The company's award-winning products include anti-virus, file encryption and network security solutions for all major platforms, from desktops to servers and from laptops to handhelds.

F-Secure is headquartered in Helsinki, Finland, with offices in California (San Jose), Germany, Sweden, Japan and the United Kingdom. Customers include Cap Gemini, Barclays Bank, Deutsche Telekom, Honda, Sonera and Verizon.

Swiss Track Prepaid Users

Switzerland is famous for its neutrality, but after this summer, it will not be known as a haven for anonymity. In an attempt to thwart terrorists, Swiss regulators have expanded rules for prepaid telecom services, including those sold nearly two years ago.

Beginning July 1, service providers must collect information about buyers before selling them prepaid products, including wireless. The new rules also require that they track down the name, address and occupation of persons who bought prepaid cards within the past two years. Beginning in October, service providers also must provide the same information for people who bought prepaid cards after November 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.

Prepaid is popular in Switzerland. Swisscom is the country's largest wireless operator, and about half of its 3.7 million customers use prepaid. The upshot is that the new rules could cause a last-minute flood of customers trying the beat the deadline. "Imagine more than a million customers running to our shops in the next few months," spokeswoman Pia Colombo told Dow Jones News wires.

The irony is that because Swisscom is partially state-owned, the government effectively is making work for itself. Time will tell whether or not the new rules are effective: Just because buyers now have to divulge information about themselves does not mean that they will provide anything more than an alias and a fake address.

Wireless Insecurity

The invitation is still open:

Do you know of any less than brilliant ideas (or worse) in wireless security (or any other type of security). Maybe you have results from a security design that failed miserably. If you prefer, we will publish your account anonymously. The idea is a light-hearted Wireless Insecurity piece that does not slam or menace any person or organization.

Submit your story to wsp@cnp-wireless.com and, if we decide to print it, you will become the proud owner of one of our eco-friendly golf shirts.

Fraud and Security Patent News

US Patent: 6,754,834

Technique for generating correlation number for use in lawful interception of telecommunications traffic

The present invention is a technique for generating a correlation number for use in lawful interception of telecommunications traffic by handling one of either a "PDP (Packet Data Protocol) context activation" or a "Start of intercept(ion) with PDP context active" event and generating a unique PDP-ID (PDP Context Identifier) in response.

An MCC (*Mobile* Country Code) and an MNC (*Mobile* Network Code) of a network operator is identified, as is a DF-ID of a DF (Delivery Function). The MCC and MNC are combined to generate an Operator-ID. The generated PDP-ID and the generated Operator-ID and the DF-ID are combined to generate the correlation number.

Issued: June 22, 2004

Inventors: Kari Miettinen and Joonas Pylkkanen
Assignee: Nokia Corporation (Espoo, Finland)

US Patent: 6, 754,825

Secure authentication and authorization for transaction processing

This patent describes a method and apparatus for authenticating and authorizing online transactions. An authentication cookie is transmitted to a client system. The authentication cookie includes a user encryption key and an encrypted buffer that contains user identification data and a profile code. Subsequent requests for the particular service use the authentication cookie to generate a query that includes the encrypted buffer and user identification data entered by the user. Portions of the query are encrypted using the user encryption key. Queries received at each authentication and authorization server are authenticated by reconstructing the user encryption

Upcoming Wireless and Wireless Security Events

The following are upcoming wireless and wireless security events for July that may be of interest. The name, dates and venue of the event, plus URL, are provided.

USENIX '04 Annual Technical Conference
1st– 2nd July
Boston Marriott Copley Place
Boston, MA
www.usenix.org/events/usenix04

SANSFIRE 2004
6th– 11th July
Monterey Conference Center
Monterey, CA
www.sans.org/sansfire2004

WNET 2004 – Wireless Networks and Emerging Technologies
8th– 10th July
The Banff Center
Banff, AB, Canada
www.iasted.com/conferences/2004/banff/wnet.htm

Wireless LANs: Gaining Strength, Reaching Farther (Westin Buckhead)
13th July
Marriott Wardman Park Hotel
Atlanta, GA
www.nwfusion.com/events/wlan

[Note: this WLAN event occurs on other dates and at other locations during July]

ALGOSENSORS 2004 – the 1st International Conference on the Algorithmic Aspects of Wireless Sensor Networks
16th July
Turku University
Turku, Finland
ru1.cti.gr/algosensors04

[Note: this event is held in conjunction with the 31st International Colloquium on Automata, Languages and Programming]

4th Annual iWireless World 2004
21st– 22nd July
Hilton Universal City
Los Angeles, CA
www.iwirelessworld.com

Wireless and Mobile World Expo
21st– 22nd July
National Trade Centre at Exhibition Place
Toronto, CA
www.worldexpos.wowgao.com

HP Wireless and Mobility Roadshow 2004
27th July
The Westin San Francisco Airport
San Francisco, CA
www.winnetmag.com/roadshows/mobilewireless

ADHOC NOW '04 – 3rd International Conference on Ad Hoc Networks and Wireless
22nd– 24th July
University of BC, Harbor Center Campus
Vancouver, BC
www.cs.ualberta.ca/adhocnow04/Default.htm

Blackhat Briefings and Training
24th– 29th July
Caesars Palace
Las Vega, NV
www.blackhat.com

PODC 2004 – 23rd Annual Symposium on Principles of Distributed Computing
25th– 28th July
The Fairmont Newfoundland
St. John's, Newfoundland, Canada
www.podc.org/podc2004

SPECTS '04 – 2004 International Conference on Performance Evaluation of Computer and Telecommunication Systems
25th– 29th July
San Jose Hyatt
San Jose, CA
www.scs.org/confernc/ssimc/ssimc04/cfp/spects04.htm

U-R-Linked

Wireless Security: An Oxymoron!?

Soft rock, small crowd, jumbo shrimp, act naturally, almost exactly, silent scream and wireless security. Huh? Click on the URL below to hear what the Internet Caucus Advisory Committee and a panel of experts said about wireless security ... is wireless security truly an oxymoron? Hear also Congressman Honda (D-CA) share some precautions and tips for securing Wi-Fi networks.

www.netcaucus.org/events/2003/wireless

key using information transmitted in the clear and decrypting the query using both the reconstructed user encryption key and the secret key. The user identification data entered by the user is then compared with the user identification data in the encrypted buffer for further authentication. The profile code is analyzed for determining authorization. If the query is authenticated and authorized, the authentication and authorization server forwards the request to a server that provides the desired service.

Issued: June 25, 2004

Inventor: Robert Lennie, *et al*
Assignee: Palm Source, Inc. (Sunnyvale, CA)

US Patent: 6,754,824

Modulated message authentication system and method

This invention is a telecommunications system and method for implementing a message authentication code (MAC) for transmitted digital information signals. Digital information signals typically include an error detecting code, such as a Cyclic Redundancy Check (CRC) code, to ensure reliable delivery of the information. In order to verify the identity of the sending node, the CRC code can be modulated by a sequence known only to the participating nodes. Thus, the CRC code not only provides an error detecting function, but also serves as a message authentication code.

Issued: June 25, 2004

Inventors: Joakkim Persson and Ben Smeets
Assignee: Telefonaktiebolaget L M Ericsson (Publ) (Stockholm, Sweden)

Notable References:

[1] Krawczyk, Hugo. *LFSR-based Hashing and Authentication.* Proceedings of the Annual International Cryptology Conference, vol. Conf. 14, Aug. 21, 1994, pp. 129-139.

US Patent: 6,754,822

Active watermarks and watermark agents

This invention presents techniques for protecting the security of digital representations, and of analog forms made from them. The techniques include authentication techniques that can authenticate both a digital representation and an analog form produced from the digital representation, an active watermark that contains program code that may be executed when the watermark is read, and a watermark agent that reads watermarks and sends messages with information concerning the digital representations that contain the watermarks.

The authentication techniques use semantic information to produce authentication information. Both the semantic information and the authentication information survive when an analog form is produced from the digital representation. In one embodiment, the semantic information is alphanumeric characters and the authentication information is either contained in a watermark embedded in the digital representation or expressed as a bar code. With the active watermark, the watermark includes program code. When a watermark reader reads the watermark, it may cause the program code to be executed.

One application of active watermarks is making documents that send messages when they are operated on. A watermark agent may be either a permanent resident of a node in a network or of a device such as a copier or it may move from one network node to another. In the device or node, the watermark agent executes code which examines digital representations residing in the node or device for watermarked digital representations that are of interest to the watermark agent. The watermark agent then sends messages which report the results of its examination of the digital representations. If the watermarks are active, the agent and the active watermark may cooperate and the agent may cause some or all of the code that an active watermark contains to be executed.

Issued: June 22, 2004

Inventor: Jian Zhao
Assignee: Fraunhofer-Gesellschaft zur Forderung der angewandten forshung e.v.

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 briefly 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: 6,754,821

System, method and article of manufacture for transition state-based cryptography

This invention is a system, method and article of manufacture provided for transition state-based cryptography in an application including at least one state having a state key associated with it. A request for access is sent to a server utilizing a network *upon reaching a state in the application* [emphasis added]. The request includes a state key associated with the state. A reply is received from the server in response to the request. The reply includes an access key for providing the access if the state key is valid.

According to another embodiment of the present invention, a method is provided for transition state-based cryptography in an application including at least one state having a state key associated with it. A request for access is received from a *client to a server* utilizing a network [emphasis added]. The state key is verified at the server. A reply is sent from the server in response to the request. The reply includes an access key for providing the access if the state key is verified.

In one aspect of the present invention, the request for access is for a subsequent state in the application.

Issued: June 22, 2004

Inventor: Thomas Berson, *et al*

Assignee: Xerox Corporation (Stamford, CT)

US Patent: 6,754,819

Method and system for providing cryptographic services in a distributed application

This patent describes a data security system that provides cryptographic services in a multiprocessor platform supporting a distributed application. The distributed application includes a cryptographic object that is executable exclusively on the data security system. An input interface object, a cryptographic function, and an output interface objection form the cryptographic object.

The data security system includes a first processor element for executing the input interface object, a second processor element for executing the cryptographic function, and a third processor element for executing the output interface object. The combination of data security system and cryptographic object ensures the separation of plain text data from cipher text data.

Issued: June 22, 2004

Inventor: Jonathan Wootten, *et al*

Assignee: General Dynamics Decision Systems, Inc. (Scottsdale, AZ)

Notable References:

[1] Gutmann, Peter. *An Open-source Cryptographic Coprocessor.* 9th USENIX Security Symposium Paper 2000, pp. 97-112 of the Proceedings.

[2] T. Peacock. *Features and Utilization of Motorola's Advanced INFOSEC Machine, AIM, in Embedded Encryption Applications.* IEEE 2000 International Performance, Computing and Communications Conference, Feb. 20, 2000, pp. 423-429.

US Patent: 6,754,488

System and method for detecting and locating access points in a wireless network

This invention is a method and computer program product for ascertaining the location of an access point in a wireless network. Initially, a strength of a radio frequency signal of an access point of a wireless network is monitored at a position utilizing a wireless network analyzer. Next, the wireless network analyzer is moved about the position. The foregoing operations may be repeated to allow the location of the access point to be ascertained based on the monitored strength of the radio frequency signal.

Issued: June 22, 2004

Inventor: King Won, *et al*

Assignee: Networks Associates Technologies, Inc. (Santa Clara, CA)

US Patent: 6,754,483

Method and system for generating a secure wireless link between a handset and base station

This patent discloses methods and an apparatus for establishing secure wireless links between a handset and a base station in cordless telephone systems. A method of generating a secure wireless link between a handset and a base station includes initiating a linking procedure, generating a security code, displaying the security code at the base station, entering the security code into the handset and then establishing a radio frequency link between the handset and the base station utilizing the security code.

A cordless telephone system capable of generating a secure wireless link includes both a handset and a base station. The handset includes a control circuit, a transmitter and a receiver coupled to the control circuit along with a keypad also coupled to the control circuit. The base station includes a control circuit, a code generation circuit coupled to the control circuit, a display coupled to the control circuit for displaying a code generated by the code generation circuit, and a transmitter and receiver coupled to the control circuit.

Issued: June 22, 2004

Inventor: Norman Beamish

Assignee: Skyworks Solutions, Inc. (Irvine, CA)

US Patent: 6,754,482

Flexible access authorization feature to enable mobile users to access services in 3G wireless networks

The invention is a flexible access authorization feature for wireless telecommunication systems that enables network operators and/or service providers to dynamically authorize a user to receive services for which the subscriber has not previously subscribed or which are not supported in the user's home network. This is accomplished by enabling a user to expand and contract their portfolio of available communication services on an as-needed basis to enable wireless users to use their user mobile terminals and obtain the services which they need, regardless of the user's location in the wireless communication network and regardless of the present set of services for which the

user is authorized. The flexible access authorization feature is accomplished by real time interaction among the relevant functional entities of the wireless telecommunications system to obtain new or additional user information to execute the flexible access authorization logic to decide on access authorization to a selected service. The flexible access authorization logic can reside in any of a number of network entities and can examine a number of conditions to determine access authorization for a user with respect to a selected service, including: time-dependency, location-dependency, account billing limitations, and other factors.

Issued: June 25, 2004

Inventor: Mohammed Torabi
Assignee: Lucent Technologies Inc. (Murray Hill, NJ)

US Patent: 6,754,214

Communication network having packetized security codes and a system for detecting security breach locations within the network

This patent describes architectures, systems, and methods for securing and prioritizing packets of data sent through a communication network. Each packet is assigned a security code and priority code as it enters the network. The security code or priority code may remain the same or change as it travels from node-to-node across the network. By assigning security and priority codes to each packet, maximum bandwidth allocation can be achieved among the nodes in a packet-switched environment.

The assigned security and priority codes enter and travel through the network according to modules which have a hierarchical class or grouping. Thus, the security and priority information may be sent solely within one class or among classes, depending on where within the classes the data path exists. In this manner, a specified quality of service can be achieved to ensure the data path is secured dynamically as it travels from node to node, and also to determine which packet among several is to be forwarded across a shared resource of that network.

Issued: June 22, 2004

Inventor: Rupaka Mahalingaiah
Assignee: Dunti, LLC (Austin, TX)

US Patent: 6,751,734

Authentication executing device, portable authentication device, and authentication method using biometrics identification

The present invention is an authentication method using biometrics identification, comprising the following steps:

- Identifying a user by biometrics entered from a portable authentication terminal;
- When the user has been registered previously, establishing communication between the authentication terminal and an authentication executing device independent of the authentication terminal, and calculating a common secret key for use in transmission of an authentication message;
- Encrypting an authentication message including the user's inherent information in the authentication terminal based on the secret key;
- Sending the encrypted authentication message from the authentication terminal to the authentication executing device, and;
- Decrypting the authentication message in the authentication executing device based on the calculated secret key, thereby executing an operation depending on the user- inherent information included in the message.

Issued: June 15, 2004

Inventor: Kaoru Uchida
Assignee: NEC Corporation (Japan)

US Patent: 6,751,729

Automated operation and security system for virtual private networks

This patent reveals a node device for providing secure communication services over a data network, such as the Internet or another public or private packet switched network, to multiple computers that are coupled through the node device and multiple other node devices. The node device includes a network communication interface for coupling the node device to the data network. The node device includes a data storage containing cryptographic information, including information that is unique to the node device. The node device also includes a tunneling communication service coupled to the network interface configured to maintaining an encrypted communication tunnel with each of multiple other node devices using the cryptographic information. For example, the encrypted communication tunnels are implemented using the IPsec or PPTP protocols. The node device includes a routing database for holding routing data and a router coupled to the tunneling communication service and to the routing database. The router can pass communication from one communication tunnel to another. A centralized server can be used to control the node devices in a centralized manner, thereby reducing or eliminating on-site administration of node devices.

Issued: May 25, 2004

Inventors: Michael Giniger and Warren Hilton
Assignee: Spatial Adventures, Inc. (Ashburn, VA)

www.spatialadventures.com

Spatial Adventures
21392 Chickacoan Trail Drive
Ashburn, VA 20148

Tel: (866) 858-2133

US Patent: 6,751,318

Method and apparatus for digital signature authentication

The present invention improves speed and reduces complexity in a digital signature scheme that uses elliptic algebra. The signature scheme generates two points that are compared. If the points do not match, the signature is not authentic. The present invention reduces computations by comparing only the *x*-coordinates of the two generated points. The invention provides a scheme for deducing the possible values of the x-coordinate of a sum of two points using only the x-coordinates of the original two points in question. The present invention provides a scheme that limits the possible solutions that satisfy the equation to two (the authentic signature and one other). Because of the large number of possible inauthentic solutions, the chance of a false authentic signature is statistically insignificant.

Issued: June 15, 2004

Inventor: Richard Crandall
Assignee: NeXT Software, Inc. (Redwood City, CA)

US Patent: 6,749,115

Dual processor trusted computing environment

The present invention relates to an architectural development of a monolithic integrated circuit with dual public key cryptographic protected central processing units in a computing device, with large external non-volatile reprogrammable memory enabled to perform cryptographically controlled transactions for identification of persons, computers, and or mobile devices, for controlling access to physical and computational devices, for multi-vendor monetary transactions, and to serve as a safe depository of data, especially useful for encapsulating applications, programmed and updated by varied entitled programmers such that one or many vendors' applications are mutually exclusive, and virtually unable to corrupt, infringe, change or affect other vendor applications.

Issued: June 15, 2004

Inventor: David Gressel, *et al*
Assignee: M-Systems Flash Disk Pioneers Ltd.
(Beer Sheva, Israel)

www.m-sys.com

M-Systems (Nasdaq: FLSH) develops, manufactures and markets flash memory solutions to a variety of markets including mobile handsets, keychain storage, embedded systems, military and aerospace. M-Systems flash-based data storage products known as flash disks, provide the functionality of a mechanical hard drive in a silicon chip.

M-Systems Inc.
8371 Central Ave., Suite A
Newark, CA 94560

Tel: (510) 494-2090
Fax: (510) 494-5545

US Patent: 6,748,532

Universal smart card access system

The present invention is a universal secure token scheme that provides two-way authentication, credit, debit, and stored-value operations. The invention permits the use of universally available networks to access corporate, private, and proprietary devices. The invention provides strong authentication, offers optional encryption of the established session, and operates without requiring special permission to reconfigure firewalls. One application of the invention provides a universal token scheme that can be used in debit and stored-value transactions. In one embodiment, devices and services are treated as URLs and a smart card is configured to perform the necessary HTTP protocol to access the URL.

Issued: June 8, 2004

Inventor: Rinaldo Digiorgio
Assignee: Sun Microsystems, Inc. (Santa Clara, CA)

Notable Reference:

[1] T. Verschuren. *Smart access: Strong authentication on the Web, Computer Networks and ISDN Systems.* Holland Publishing, Amsterdam, The Netherlands. vol. 30, No. 16-18, Sep. 30, 1998, pp. 1511-1519.

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