Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 6, No. 4. April, 2004

Crypto In The News – PKIX Working Group Message Digest Specification

The IETF (Internet Engineering Task Force) PKIX Working Group has developed a new specification for a 224-bit one-way hash function. A hash function is a cryptographic primitive known also as a message digest. It is typically used in numerous applications for integrity protection to detect unauthorized message modifications. The specification, titled, *A 224-bit One-way Hash Function: SHA-224,* is based on NIST's SHA-256, the 256-bit one-way hash function.

The computation of a SHA-224 hash value is performed in two steps. First, the SHA-256 hash value is computed, except that a different initial value is used, then the resulting 256-bit hash value is truncated to 224 bits. The document is currently available at:

www.ietf.org/internet-drafts/draft-ietf-pkix-sha224-01.txt

NIST is developing guidance on cryptographic key management. Five security levels are discussed in their recent draft for comment *NISTGUIDE*: 80, 112, 128, 192, and 256 bits of security. One-way hash functions are available for all of these levels except 112. SHA-224 provides 112 bits of security, therefore it completes these NIST recommendations. It is especially useful for Triple-DES [3DES], which has a generally accepted strength of 112 bits of security.

The use of a different initial value ensures that a truncated SHA-256 message digest value cannot be mistaken for a SHA-224 message digest value computed on the same data.

China WAPI Update

Chinese wireless device manufacturers will be working with international standards-setting bodies, rather than going the lonely path of implementing WAPI (Wired Authentication and Privacy Infrastructure). During China-U.S. trade talks on April 21, China agreed to table their WAPI June 1st deadline. It would have imposed a Chinese proprietary encryption standard on all WLAN devices destined for the Chinese market. Read more about WAPI in our **December 2003** issue of *Wireless Security Perspectives.*

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…

May 27th, 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.

The news about WAPI was met with mixed emotions. Several leading global WLAN vendors were actually looking forward to having the WAPI standard set in motion, especially after Intel announced they would not comply, supported by Broadcom and the SIA (Semiconductor Industry Association). China is the world's third largest chip market. At least two Taiwanese chip design companies, and others working alongside them, already have WAPI certification and will continue WAPI-based developments, in spite of China's recent concession at the Joint Commission on Commerce and Trade (JCCT) meeting.

China plans to continue developing WAPI, but it has agreed to do so in conjunction with international standards bodies, hoping to integrate it into those standards. WAPI was developed to address weaknesses in the original WiFi security specification.

Eleven Chinese telecom equipment makers currently have free access to China's proprietary WAPI technology. Their plan seeks revision of WAPI to take into account various recent comments received from Chinese and non-Chinese companies.

The immediate effect of putting WAPI aside for now is expected to be increased sales of 802.11-based WLAN equipment to China.

The RFID Bogeyman

New technologies typically attract two groups. The first is investors, who see the next big thing, followed by legislators and worrywarts, who also see the next big thing – albeit more as a problem than an opportunity.

Radio frequency identification (RFID) is no exception. "The RFID train is beginning to leave the station," said Sen. Patrick Leahy (D-Vt.) in a March 23rd speech. "Now is the right time to begin a national discussion about where, if at all, any lines will be drawn to protect privacy rights. We are on the verge of a revolution in micro-monitoring – the capability for the highly detailed, largely automatic, widespread surveillance of our daily lives."

Created largely as a medium for cashless payments and inventory tracking, RFID has prompted fears of corporate espionage, Big Brother-style surveillance and mark-of-the-beast scenarios from the Bible's book of Revelations. Granted, there are plenty of proposals out there to inspire such concerns, ranging from RFID chips implanted in humans to RFID tags sewn into clothing and capable of surviving multiple runs through a washing machine.

But every scenario that is possible in theory also bears the burden of making a business case for it. In that respect, RFID's privacy fears mirror those of E-911 Phase II in the late 1990s: Yes, a carrier could use location technology to track every subscriber every moment, perhaps for reasons as innocuous as using them to collect network-performance data.

Are You the Arcanist?

Last month's question was:

Show the next two in this series:
5, 25, 61, 113, 181, (?), (?).

The next two numbers are: 265 and 365.

Explanation: For the series above, denoted as k, take two series i and j, where i=(1,3,5,7,9,11,13) and j= (2,4,6,8,10,12,14).

$$k = (i)^2+(j)^2$$

Simon Arcand (from Canada) was very quick to reply with the correct answer, and his win was a free CNP golf shirt, made from environmentally-friendly, recycled cotton. Our aptly named winner found a different formulation of the series:

$$k = 8(i)^2 - 4(i) + 1$$

for i = (1, 2, 3, 4, 5, 6, 7)

Now here is the next question: What comes next in this series ... 58, 108, 145, 228, 778, 1426, ...?

Submit your answer to wsp@cnp-wireless.com

But that business case looks iffy because that information is already gathered through drive testing. Such intensive use of location technology would redirect network resources that otherwise could be generating revenue.

Even if RFID tags were embedded in everything from people to blue jeans, their range is so small that tracking would be ineffective unless tag readers were ubiquitous – not just on every street corner but every few feet. Installing readers just in, say, the world's 100 largest shopping malls would be so expensive and provide demographic data so spotty that it is tough to envision a business case to fund it. Making this even more difficult is the proliferation of proprietary RFID formats, meaning that multiple readers or multi-protocol readers would be required, causing costs of such a project to sky-rocket.

The worst part about positioning RFID as a 'bogeyman' is that it distracts from legitimate security and privacy issues. (For some examples, see the **September 2003** and **July 2003** issues of *Wireless Security Perspectives*.) There are plenty of those to keep everyone busy, just as there are plenty of other, more practical ways that Big Brother can track us – and already does.

Upcoming Wireless & Wireless Security Events

The following are upcoming wireless and wireless security (and general security) events in May that may be of interest to security practitioners.

DallasCon Information and Wireless Security Conference
1st- 2nd May 2004
North Wyndham Hotel
Dallas, TX
dallascon.com/conference.asp

6th Wireless Internet Data and Enterprise Applications Conference
4th- 5th May 2004
Covel Commons, UCLA
Los Angeles, CA
www.wireless.ucla.edu/2004s/home.asp

Government Enterprise Architectures Conference
5th- 7th May 2004
Sheraton National Hilton
Arlington, VA
www.dci.com/events/goveac

Bluetooth Wireless
5th May 2004
Webcast
Anywhere
www.sans.org/webcasts/show.php?webcastid=90473

TeleStrategies Billing & OSS World
5th- 7th May 2004
DC Convention Center
Washington, DC
www.tsnn.com/partner/listings/evitem_techweb.cfm?ID=349644

2004 IEEE Symposium on Security and Privacy
9th- 12th May 2004
The Claremont Resort
Oakland, CA
www.cs.berkeley.edu/~daw/oakland04-cfp.html

SANS Computer Security Bootcamp 2004
9th- 16th May 2004
Wyndham Baltimore – Inner Harbor
Baltimore, MD
www.sans.org/bootcamp04

Networld+Interop
9th- 14th May 2004
Las Vegas Convention Center
Las Vegas, NV
www.interop.com

12th IEEE MELECON 2004 – Special Session on Wireless Protocols Security
12th- 16th May 2004
Old town Dubrovnik
Dubrovnik, Croatia
www.melecon2004.org/index.html

WTS 2004 – Wireless Telecommunications Symposium
14th- 15th May 2004
Kellogg West Conference Center, Cal Poly
Pomona, CA
134.71.194.20/wtsi2004

The Security Professionals Workshop
16th- 18th May 2004
Fairmont Hotel
Washington, DC
www.educause.edu/conference/security/2004

13th International World Wide Web Conference
17th- 22nd May 2004
NY Sheraton
New York, NY
www2004.org

2004 Southeast Security Forum
19th- 20th May 2004
Marietta Conference Center & Resort
Marietta, GA
www.ianetsec.com/forums/se_forum/se_intro_2004.htm

Wireless Communications Alliance (WCA) Meeting
20th May 2004
HP, Cupertino– Oak Room Audiorium
Cupertino, CA
www.wca.org

Cyber Security Group 2004 Training Conference
25th- 27th May 2004
Sheraton Overland Park Hotel
Overland Park, KS
cybertrain.labworks.org/conferences/may2004

PET 2004 – Workshop on Privacy Enhancing Technologies
26th- 28th May 2004
Radisson Plaza Hotel Admiral
Toronto, Canada
petworkshop.org/2004/index.html

Advances in Wireless Fraud Detection

Scott M. Zoldi

As new wireless data technologies become available, operators grapple with ways to bill customers for the new services and to provide adequate fraud detection. Areas of concern include new GPRS, UMTS and CDMA packet data premium content services, micro-payments and m-commerce. With the introduction of m-commerce, wireless fraud will likely evolve to mimic credit card fraud, exposing operators to new fraud scenarios and larger fraud losses.

Currently, fraud losses are estimated to be as much as 4% of wireless revenue, with much of the fraud being mis-classified as bad debt. Although subscription fraud is a major portion, the expanding capabilities of wireless devices will enable new types of technical fraud such as handset takeover. Operators will increasingly rely on advanced analytic tools and traditional wireless fraud detection techniques to predict fraud with their new offerings.

Predictive Profile Variables

The first task in detecting fraud is identifying the relevant data sources. Call detail, billing, payment, application, promotions and customer information records all help predict wireless subscription fraud, whereas technical fraud detection relies most heavily on call event records. Once data sources are determined, it is important to assemble a concise set of predictive variables that summarize the entire data history of the customer and line of service (IMSI or MIN), rather than storing the raw records. Fair Isaac Corporation assembles these predictive variables in patented transaction profiles. These transaction profiles are not "mini databases." Instead, they are an adaptive set of variables individualized to a particular line of service or customer. They are updated with each new piece of data.

To make fraud predictions in real time, the profile variables are defined using recursive-analytic formulas that allow a summarization of the most important fraud predictors over arbitrary time scales. Transaction profiles typically contain a few hundred variables summarizing the entire data history, and they allow profiles to be retrieved and the variables to be updated in real-time.

Some example variables include:

- Geo-velocity (successive calls made a large distance apart) and call-collision variables (two overlapping calls from the same device),
- Increase in the volume of calls to numbers outside those most frequently dialed, increase in calls made from outside the most frequently visited cell sites or packet data sessions outside the most frequently visited IP addresses,
- Increase in the packet data-download volume and number of sessions established,
- Severity of change and rate of change in customer information,
- Ratio of unbilled usage to past bill amount,
- Time of day and day of week premium rate service frequency changes.

As discussed in more detail later, only metrics required to compute the fraud model score are calculated and stored. This approach drastically reduces the memory requirements of the fraud system while maintaining the highest levels of fraud prediction at the line of service level. Traditionally, neural networks are one of many statistical tools that are used to perform variable selection on the hundreds to thousands of variables initially used in fraud model development. Like other statistical modeling techniques, neural networks require historical wireless fraud data on which to perform the variable selection.

Wireless Fraud Consortium Data

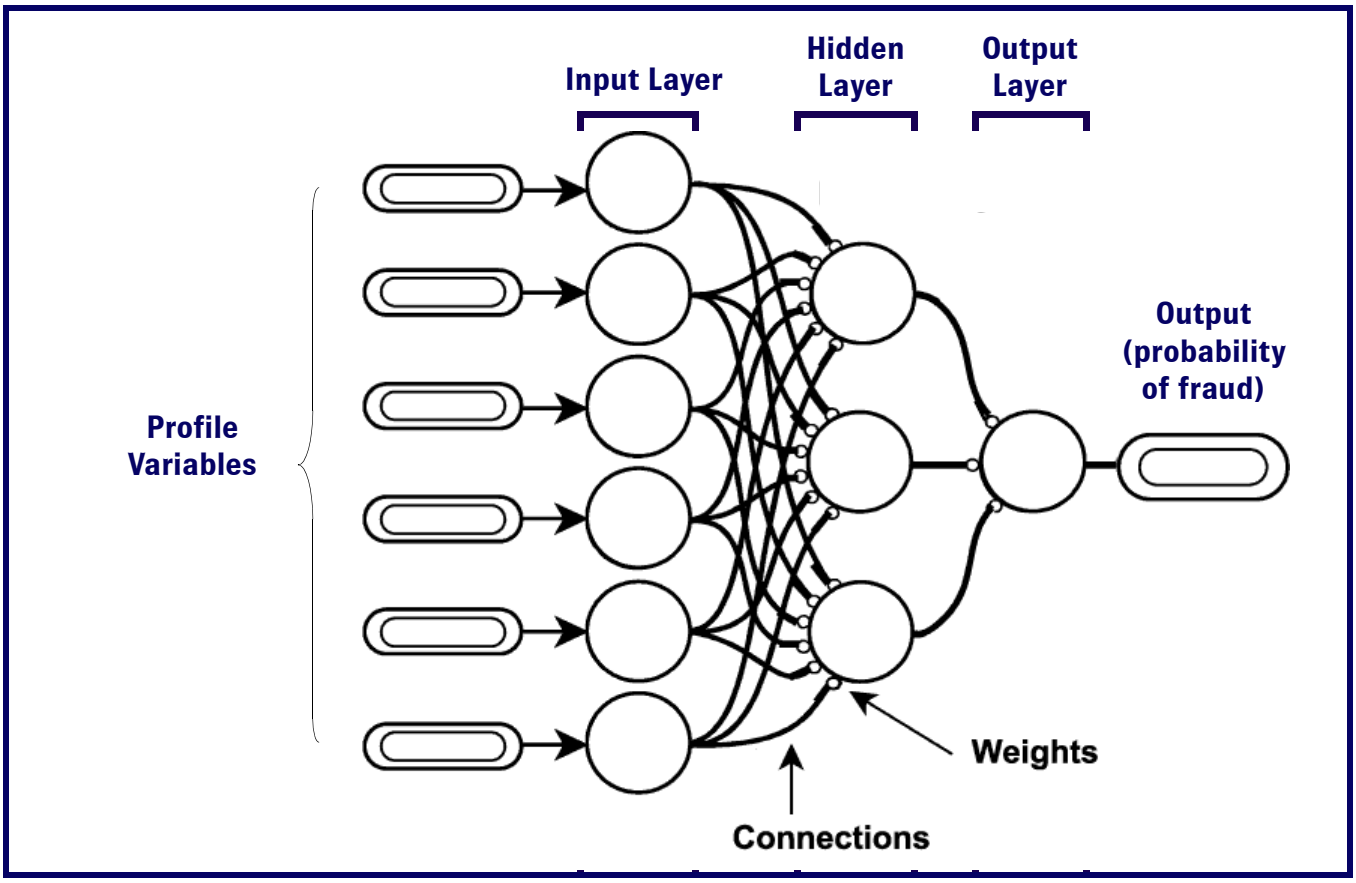
Very often the lack of historical fraud data prevents an operator from building statistical fraud models, despite the huge improvement in fraud prediction compared to notional methods such as rules and scorecards. To solve this industry problem, Fair Isaac uses a data consortium consisting of telecom data (e.g., call detail records, application records, billing records, SS7 records) from a number of telecom operators. This consortium is not a negative file but rather the complete data histories of fraud and non-fraud customers. The data consortium provides a far larger set of fraud patterns than any single operator's historical data. It also allows more robust models to be constructed based on the larger number of wireless fraud patterns. Although models are based on the operator's historical data, the consortium can be leveraged to enhance the quality of the fraud data, include data on new services and include fraud data on moving and evolving fraud trends.

Neural Networks

Neural network training requires adequate historical data from good, fraud and suspected fraud customers – for which the data consortium is often leveraged. Once these data are assembled, they are processed through the model to compute and update each line of service exactly as they would be in production. The process of generating profile variables to be used in fraud models starts with hundreds to thousands of possible predictive variables. Although predictive, the profiles at this stage are too large for a real-time production system and need to be refined to reduce false positives.

To train the model, profile variables (derived from the raw data) are presented to the input layer of the neural network (Figure 1).

Figure 1: Neural Network



Training of the neural network involves an iterative optimization of the connection weights within the network. By continuously adjusting the weights on the processing units, neural networks are able to learn non-linear relationships between input variables to provide the best prediction of the probability of fraud at the output layer. The hidden nodes consist of processing units that combine the weighted input connections to derive an optimal output signal to pass to the next layer. The neural network's hidden nodes essentially become "super variables" used in the final layers of the network to determine the probability of fraud.

As training evolves, the weights of the input variables adjust to a point where the scientists can review the weights to determine which variables are redundant or do not contribute to enhancing the prediction of fraud. Then it is necessary to remove variables, re-train and continue pruning the number of variables. The smaller the set of variables, the lower the false positives associated with the prediction. Because the model weights are derived based on historical fraud data, an accurate determination of the return on investment of the model in production can then be performed, based on a validation sample of the customer's historical data that was not used to train the neural network. This validation scoring will provide statistics on the cases generated at different score ranges, the percentage of fraud detected, the false positive ratio, the days to detect risk and the average dollar savings attributed to the model.

Real-Time Link Analysis

Link analysis involves computing attributes that can link different phones based on the shared values of the attributes. For example, one may analyze dialed numbers to group customers that have either called or received calls from a recently-shutdown fraudster.

Another common form of link analysis is to report all IMSIs (subscription identifiers) associated with a single IMEI for fraud purposes.

Most fraud departments would like to combine link analysis with real-time predictive scoring, but given the large volume of call event records its use is often reserved for manual or police investigations. To accomplish real-time link-like analysis, the effort is distributed across the service level profiles using specially defined *number patterns* that are updated with each new call event record. These assemble pertinent patterns in usage that uniquely identify each subscription. For example, phone numbers uniquely identify each of us (dialing family, friends, and business associates). These number patterns can also be more generic, such as visited IP or cell site patterns. Based on distributed computation, these number patterns can be updated and compared against previous fraud number patterns in real time.

Link analysis is extremely valuable for detecting repeat subscription/identity fraud and for bringing down fraud rings. Repeat fraudsters will often continue dialing the same number patterns once they obtain a new service. As they begin to use their service and visit premium content sites or call international numbers, their "premium content site number pattern," "international country number pattern" and "visited cell site number pattern" will begin to exhibit linkages with their previous fraudulent number patterns. This enables a quick removal of repeat identity fraudsters.

Link analysis is also useful for identifying members of fraud rings by analyzing weaker links between their number patterns and those of caught fraudsters. Once a fraudster is caught using the traditional neural network model, members of the same fraud ring can be quickly identified based on weaker number pattern linkages. Because this technique relies on number patterns that are continually updated in real time, wireless operators are able to use link analysis and model scores to refine the prediction for wireless fraud in real time.

Global Network Monitoring

Although fraud detection has traditionally focused on creating profile variables at the customer and line-of-service levels, collective fraud patterns frequently arise that can cost operators millions in fraud losses over a single weekend. Global profiling involves monitoring call event records associated with network components to detect deviations and abnormalities indicative of compromised network elements or collective attacks on network elements.

Global profiling can be used to monitor network elements such as international switches, serving GPRS service nodes, service control points in the SS7 network and cell sites, as well as roaming partners. By creating variables that determine deviations from the normal over different time-scales and time periods, the fraud system can point to network problems or suspected global hacks and attacks. Although these techniques border on network assurance, they become a necessity to detect collective fraud patterns, such as rapid rises in hot country volumes or premium content access through compromised nodes in the network. Monitoring is also essential for detecting denial- of- service attacks, which may become even more prevalent as cellular packet data services evolve.

Wireless Data: A New Frontier for Fraud

Wireless operators recognize that data services will provide a significant portion of their future revenue. The types of fraud that operators will experience may be quite different than traditional wireless voice fraud. Much of it will take advantage of vulnerabilities in current wireless devices. A recent example of wireless device vulnerability is bluejacking, where Bluetooth users can send anonymous messages to nearby Bluetooth devices. A more serious example of device vulnerability is bluesnarfing, which consists of a data attack that allows the attacker to access telephone numbers and diary entries on the victim's device. (For more information on bluejacking and bluesnarfing, see the **November 2003** and **February 2004** issues of *Wireless Security Perspectives*.) As mobile devices increasingly maintain an always-on connection to the Internet, it is conceivable that various back doors and Trojan horses will be designed to attack them.

One potential Trojan horse that could be applied to wireless packet data phones would be a variant of "Back Orifice," which would allow for easy device take-over via the Internet. Once this virus was inadvertently downloaded into the wireless device, a hacker could open programs, delete files, download premium rate service (PRS) content and send messages, all undetected by the user. Even more menacing are variants on programs that we already see in the ISP space that disconnect modems and reconnect them to PRS services. In a wireless data environment, rogue programs could access PRS sites or dial PRS numbers without the user's consent. Virus programs could also be coordinated to attack networks or premium content sites in a collective fashion using thousands of phones.

Constructing the appropriate predictive variables to detect take-over will depend on the data sources provided by each wireless data operator. In situations where only upload and download data volume is readily available, predictive variables would monitor statistics such as typical data volumes, deviations in the data volume, download time stamps (time of day and day of week), averages and changes in the size of downloads, frequency of data requests, upload-vs.-download data ratios and quality of service requested. If more detailed information is available, sample variables could include link analysis of

"IP patterns," requesting content from frequently visited content providers, time delay between upload/download requests vs. premium download requests, and change in MMS/SMS usage time of day and day of week patterns.

Voice and customer-level variables will also continue to be available in the prediction of fraud. Customer-level variables are those which are based on the billing system (e.g., number of billing address changes within the last 30 days) or detail about the customer (e.g., the number of services attached to an account). Data fraudsters will also commit fraud on the voice system. Subscription fraud detection is drastically improved with use of information about the early-life behavior for a customer account. This includes how the account was set up, the number of other devices attached to the wireless device and risk associated with the dealer from whom the customer purchased the device. Early detection using customer-level variables can also limit loss from "call/data sell fraud."

If the SIM card evolves into a credit or debit card, m-commerce will more closely resemble traditional e-commerce credit card fraud, where credit cards are used on the internet to fraudulently obtain services (e.g., music downloads, or chat sessions on the Internet) or goods (e.g., airline tickets). However, credit card account takeover and card-not-present models can easily be applied to the m-commerce area. Also, the level of sophistication in current credit card models will help protect m-commerce revenues. The extent of the similarity between e-commerce and m-commerce fraud will depend heavily on the credit/debit policies that telecom operators extend to their lines of service, as well as the extent of goods and services that can be purchased with the phone.

Link analysis and global monitoring of the network will continue to be valuable technologies in the wireless area. Link analysis based on IP patterns, dialed numbers, m-commerce merchants and cell sites will continue to drive the detection of repeat fraudsters and fraud rings. Global monitoring will also be necessary to detect collective denial-of-service attacks on the cellular data networks where rogue programs could target a specific operator's network or premium content providers. Given that phones are becoming more programmable, networks should be continually monitored utilizing analytic techniques to detect abnormalities and failures early enough so measures can be taken to secure the network.

Quote of the Month

Only two things are infinite: the universe and human stupidity, and I'm not sure about the former.

Albert Einstein

A View to the Future

Wireless devices are advancing by leaps and bounds with the acceptance of UMTS/CDMA2000 networks and the associated increased goods and services. Ultimately, subscription fraud and device take-over will be the two dominant types of fraud on new generation wireless networks. As more users adopt data services and utilize connections to the Internet, virus writers will target mobile devices to commit fraud or to disrupt networks. Telecom operators that implement analytic techniques for their new data service offerings will gain a competitive advantage by being able to more quickly and reliably pinpoint fraud on their data networks from the huge volume of data generated by these services. The next few years will prove to be a highly dynamic and exciting time for the builders of fraud-detection systems, due to newly deployed data event records and m-commerce records, in addition to the roll-out of new wireless devices and services.

About The Author.

Scott Zoldi, Ph.D., is an Analytic Science Director at Fair Isaac Corporation. Scott directs the telecom Fraud and Risk Management Analytic Modeling Group. Prior to joining Fair Isaac, Scott served as a Postdoctoral Director's Fellow at Los Alamos National Laboratory, where he worked on modeling problems related to solution propagation, weak turbulence, parallel computing and chaos theory. Scott received his Ph.D. in Theoretical Condensed Matter Physics from Duke University.

About Fair Isaac.

Founded in 1956, Fair Isaac (www.fairisaac.com) specializes in predictive modeling, decision analysis, intelligence management, decision management systems and consulting services. More than 100 telecom providers worldwide are Fair Isaac customers, including eight of the top 10 U.S. wire-line providers and all of the top 10 U.S. wireless providers. The company's RoamEx® solution is used to exchange more than 90% of roaming detail records for North American wireless carriers, for use in fraud prevention.

Fraud and Security Patent News

US Patent: 6,728,553

Subscriber identity module mobile station and method for performing a smart card function

A subscriber identity module that makes it possible to integrate different smart card functions for use in a mobile station. New diversified service combinations are enabled, to be implemented so as to allow them to be used via a data communication device, such as a mobile station. A feature characteristic of these service combinations is that a part of the series of actions is carried out in a system and/or application external to the data communication system and the data communication device in addition to or instead of wireless communication between the mobile station and the data communication system/application.

Issued: April 27, 2004

Inventor: Marja Leena-Lehmus, *et al*
Assignee: Sonera Oy (Helsinki, Finland)

US Patent: 6,728,529

Preventing excessive use of security keys in a wireless communications security system

A. technique for initializing a cryptographic algorithm in a wireless system. A start value is x-bit in size and is used to provide an initial value to an n-bit security count value. A wireless communications device establishes channels with a compatible device, and releases channels established with the compatible device. For every channel established by the wireless communications device, a corresponding terminal value is obtained. A terminal value for a channel is the highest value reached by the x most significant bits of an n-bit security count value associated with the channel. The security count value is used to encipher data transmitted along the channel. A final value that is obtained is the greatest value of all the terminal values. Finally, a start value is stored in the memory of the wireless device that is at least as large as the final value.

Issued: April 27, 2004

Inventor: Richard Lee-Chee Kuo, *et al*
Assignee: ASUSTeK Computer Inc. (Taipei, Taiwan).

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

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: 6,728,514

Scalable wireless network topology systems and methods

A means for wireless broadband data access to and from a plurality of locations distributed randomly over a large geographic area. The network can be deployed one node at a time, with a new node incorporated into the network if within radio frequency range of any existing node in the network. The newly incorporated node can then be the attaching point for another new node that requires incorporation into the network. Data can be forwarded over multiple hops to reach its destination in the network, with the data-polling scheme self-synchronizing with minimal transmission overhead.

Issued: April 27, 2004

Inventors: Nuno Bandeira and Lars Poulsen
Assignee: Wi-Lan Inc. (Calgary, Canada)

Contact:
2891 Sunridge Way N.E.
Calgary, Alberta, Canada T1Y 7K7
Tel: (403) 273-9133
Fax: (403) 273-5100
info@wi-lan.com
www.wi-lan.com

US Patent: 6,711,690

Methods and Systems Using Multiple Watermarks

A method for using two or more digital watermarks, with different characteristics, in a document. The characteristics are chosen so that the watermarks will be affected in different manners if the document is subsequently copied or reproduced. The detection process or mechanism reads two or more of the watermarks and compares their characteristics. While wear and handling may change the characteristics of the digital watermarks in a document, the relationship between the characteristics of the multiple digital watermarks in a document will nevertheless give an indication as to whether a document is an original or a copy of an original. Document wear can be independently assessed and used as an aid in interpreting the detected watermark characteristics.

Issued: April 27, 2004

Inventors: Geoffrey Rhoads and Ammon Gustafson
Assignee: Digimarc Corporation (Tualatin, OR)

Notable References:

[1] Cross, et al. *Watermaking for Self-Authentication of Compressed Video*. Motorola Corporation, IEEE Jun. 2002, pp. 913-916.

[2] Winograd, J.M. *Audio Watermarking Architecture for Secure Digital Music Distribution.* A Proposal to the SDMI Portable Devices Working Group, by Aris Technologies, Inc., Mar. 26, 1999.

[3] *Audio Watermarking System to Screen Digital Audio Content for LCM Acceptance.* A Proposal Submitted in Response to PDWG99050504-Transition CfP by Aris Technologies, Inc., May 23, 1999, Document Version 1.0, 15 pages.

[4] Gabor, et al. *Theory of Communication* J. Inst. Elect. Eng. 93, 1946, pp. 429-441.

[5] Luc. *Analysis of Spread Spectrum System Parameters for Design of Hidden Transmission.* Radio engineering, vol. 4, No. 2, Jun. 1995, pp. 26-29.

[6] Machado. *Announcing Stego 1.0a2, The First Steganography Tool for the Macintosh.* Internet reference, 3 pages, Nov. 28, 1993.

[7] Macq. *Cryptology for Digital TV Broadcasting.* Proceedings of the IEEE, vol. 83, No. 6, Jun. 1995, pp. 944-957.

[8] Pickholtz, et al. *Theory of Spread-Spectrum Communications –A Tutorial.* Transactions on Communications, vol. COM-30, No. 5, May, 1982, pp. 855-884.

[9] Pitas, et al. *Applying Signatures on Digital Images.* IEEE Workshop on Nonlinear Image and Signal Processing, Neos Marmaras, Greece, Jun., 1995. pp. 460-463.

[10] Gruhl, et al. *Information Hiding to Foil the Casual Counterfeiter.* Proc. 2d Information Hiding Workshop, LNCS, vol. 1525, Apr. 15, 1998, pp. 1-15.

US Patent: 6,728,378

Secret Key Messaging

Computer-enabled methods and systems for the secure transmission and platform-independent receipt and decryption of encrypted messages. Messages are encrypted by a symmetric encryption algorithm using a secret key that is, or is based on, a password known to the intended recipient. The recipient is also sent a computer program which, upon input of the correct password, uses the password to generate the secret key, or alternatively, uses the password as the secret key. The program then uses the secret key to decrypt the encrypted message. The invention further provides for ensuring the integrity and authenticity of sent and received messages. The communications medium over which messages are sent according to the invention may be a communications network such as the Internet, and the messages may be electronic mail messages and MIME messages. The invention also provides for the secure delivery of statement and transaction information pertaining to an account.

Issued: April 27, 2004

Inventor: Marco Garib
Assignee: Eversystems Information Comircio Representagco, Importageo e Exportagco (Sao Paulo, Brazil)

US Patent: 6,726,100

Method for spreading parameters in offline chip-card terminals as well as corresponding chip-card terminals and user chip-cards

A method for updating time-limited parameters, in particular lists of blocked user chip-cards, in off-line chip-card terminals, in which said parameters are updated with the user chip-cards used in the off-line chip-card terminal. Advantage: The off-line terminals do not have to be inspected manually.

Issued: April 27, 2004

Inventors: Eric Lauper and Reanto Cantini
Assignee: Swisscom Mobile AG (Bern, Switzerland)

US Patent: 6,725,374

Method for the execution of an encryption program for the encryption of data in a microprocessor-based portable data carrier

A method for the execution of an encryption program for the encryption of data in a microprocessor-based portable data carrier, with the encryption program comprising several parallelisationable subprograms. The serial order of execution of at least two of the subprograms is randomly permuted in the execution of the encryption program under the consideration of at least one random number.

April 20, 2004
Inventor: Michael Jahnich, *et al*
Assignee: Orga Kartensysteme GmbH (Paderborn, Germany)

US Patent: 6,725,056

System and method for secure over-the-air provisioning of a mobile station from a provisioning server via a traffic channel

A provisioning system for use in a wireless network, comprising a group of base stations that communicate with mobile stations. The provisioning system provisions unprovisioned mobile stations and prevents unprovisioned mobile stations from accessing an Internet protocol (IP) data network through the wireless network. The provisioning system comprises a provisioning controller that retrieves provisioning data from a provisioning server associated with the IP data network and causes a first base station to transmit the retrieved provisioning data to a first unprovisioned mobile station in a first traffic channel established between the first base station and the first unprovisioned mobile station. The provisioning system prevents any unprovisioned mobile station from accessing the wireless network except by means of a traffic channel, thereby preventing the unprovisioned mobile station from making an unauthorized access to the Internet via a data call to a base station.

Issued: April 20, 2004

Inventors: Bryan Moles and Sudhindra Herle
Assignee: Samsung Electronics Co., Ltd. (Suwon, Korea)

US Patent: 6,724,895

Electronic identification system and method with source authenticity verification

An RF electronic identification (RFID) system with at least one transponder encoder for writing data into a memory arrangement of a selected transponder or a plurality of transponders adapted to receive data from the at least one encoder. The system further includes at least one verifier for interrogating a selected transponder and to read data stored in the transponder. The encoder includes a controller for providing an identification code characteristic of the encoder to form part of the data to be written into the transponder. The verifier includes computing means for extracting the identification code from the data read thereby and for comparing the code to authorized codes. An indicator provides an indication whether or not the identification code corresponds to any of the authorized codes. The system also includes a method of verifying the authenticity of a transponder.

Issued: April 20, 2004

Inventors: Christopher Turner and Johan Kruger
Assignee: Supersensor (Proprietary) Limited (Goodwood, South Africa)

US Patent: 6,724,310

Frequency-based wireless monitoring and identification using spatially inhomogeneous structures

Wireless tags that have a plurality of non-equivalent current pathways, each of which responds differently to an interrogation signal and collectively represent encoded information. The element is subjected to the signal, stimulating the current pathways, each of which contributes to an overall element response. The individual contributions and, hence, the information may be recovered from this overall response. The response of each of the pathways to the signal may vary in terms of one or more of: resonant frequency, amplitude, damping, and Q factor.

Issued: April 20, 2004

Inventors: Neil Gershenfeld and Richard Fletcher
Assignee: Massachusetts Institute of Technology (Cambridge, MA)

US Patent: 6,721,771

Method for efficient modular polynomial division in finite fields f(2 m)

A method for performing an inversion and multiply, in a single operation, as a polynomial divide operation. As a result, the method reduces the number of mathematical operations needed to perform point doubling and point addition operations. An elliptic curve cryptosystem using the polynomial divide operation can be made to operate more efficiently. An elliptic curve crypto-accelerator implemented with the polynomial divide operation can dramatically enhance the performance of the elliptic curve cryptosystem.

The invention uses five registers A, B, U, V, and M, to accomplish a polynomial divide operation. Four registers A, B, U, and V are initialized with values so that the registers maintain a number of invariant relationships. The registers store initial values a(t)=x(t), u(t)=y(t), b(t)=prime(t), and v(t)=0. Here the polynomials in registers A, U, B, and V are denoted as a(t), u(t), b(t), and v(t), respectively. Register M stores the irreducible polynomial prime(t). By applying a series of invariant operations to the registers, the register values are systematically reduced until registers A and B have a value of one. At that point, register U stores a value which represents y(t)/x(t) mod prime(t), solving the polynomial division.

Issued: April 13, 2004

Inventor: Sheueling Chang
Assignee: Sun Microsystems, Inc. (Santa Clara, CA)

US Patent: 6,721,555

System and method for facilitating device authentication in a wireless communications system

A system for efficiently accommodating an authentication protocol in a communications system. The system includes a first mechanism for establishing a first communications interface between a first device and a second device, and for establishing a second communications interface between the second device and a third device. A second mechanism selectively relays authentication signals received by the second device between the first device and the third device. A third mechanism employs the third device and the second mechanism to authenticate the first device via the first communications link and the second communications link.

Issued: April 13, 2004

Inventor: Marc Phillips, *et al*
Assignee: Qualcomm Incorporated (San Diego, CA)

Wireless Insecurity

Do you know of any less than brilliant (or worse) ideas for wireless security (or any other type of security)? Perhaps you would like to share them, even if you have to keep your name and the company it involves anonymous!
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.

Though it is not squarely on the topic of security, the Norwegian tax collectors' SMS tax return plan (below) seems open to abuse:

---

mTaxPayer

This year in Norway, an estimated 36,000 tax payers filed their returns by SMS. They were allowed to do so only if there were no changes to the documents they received in the mail. They contacted the Norwegian Inland Revenue office using their wireless device, and then entered a code word, their identity number and a pin code.

This means that the government essentially did their taxes for them. All the Norwegian taxpayers did was approve the final result via SMS. Even if this system can be kept free from hackers, it is hard to imagine that many other countries would trust the government to get their taxes right!