Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 5, No. 12. December, 2003

China's Home-grown WiFi Security

In the past year, major vendors such as Nortel Networks, Siemens and Samsung have invested in TD-SCDMA to avoid losing the Chinese market. TD-SCDMA is the 3G technology that China favors. With a population of more than 1.3 billion, China is a market too big for any telecom vendor to ignore.

The latest example of China's market power is a new cryptographic standard for all 802.11 equipment sold in the country. On December 1st2003, the Standardization Administration of China began requiring all Wi-Fi equipment sold after June 1st 2004 must support Wired Authentication and Privacy Infrastructure (WAPI), a cryptographic scheme controlled by 11 Chinese vendors.

Little is known about WAPI except that it does not use AES – NIST's Advanced Encryption Standard for civil government and commercial use in the United States. Robust Security Network (RSN) will form ciphertext using TGi's Counter Codebook Mode, CCM (see **Figure 1**). It is unknown at this time exactly how this will be different in WAPI. It could be that AES is simply replaced with another algorithm or the protocol may be changed entirely. *Wireless Security Perspectives* will cover this in more detail in a future issue.

So far, it has not been endorsed by the IEEE or WiFi Alliance. Major WiFi vendors such as Cisco Systems and Intel have made few comments on their plans for WAPI, except to say that they are studying it.

WAPI is literally a state secret, and the only way for a foreign company to incorporate it into WiFi products sold in the Chinese market is to work with one of the Chinese authorized vendors. That has fueled speculation that, like TD-SCDMA, WAPI is intended to ensure that as much revenue as possible flows to domestic vendors. Also, given the suspicion with which the Chinese government views the free exchange of information on the internet, WAPI could also contain a 'back door' allowing Chinese authorities access to all transmissions encrypted by it.

Indeed, when an October 2002 Deutsche Bank Securities report said that TD-SCDMA could be different enough from CDMA that vendors may not have to pay royalties to Qualcomm, the company's stock fell 6 percent. A year later, that possibility is still being debated, and WAPI could have a similar effect on vendors that get a significant amount of revenue from WiFi products. In a December 3rd, 2003 *Wall Street Journal* article, a Dell China spokeswoman said, "According to our current understanding of the [WAPI requirement], we will have to stop shipments" of laptops that use either of Intel's Centrino chipsets after June 1st, 2004.

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…

January 27th, 2004.

Future Topics

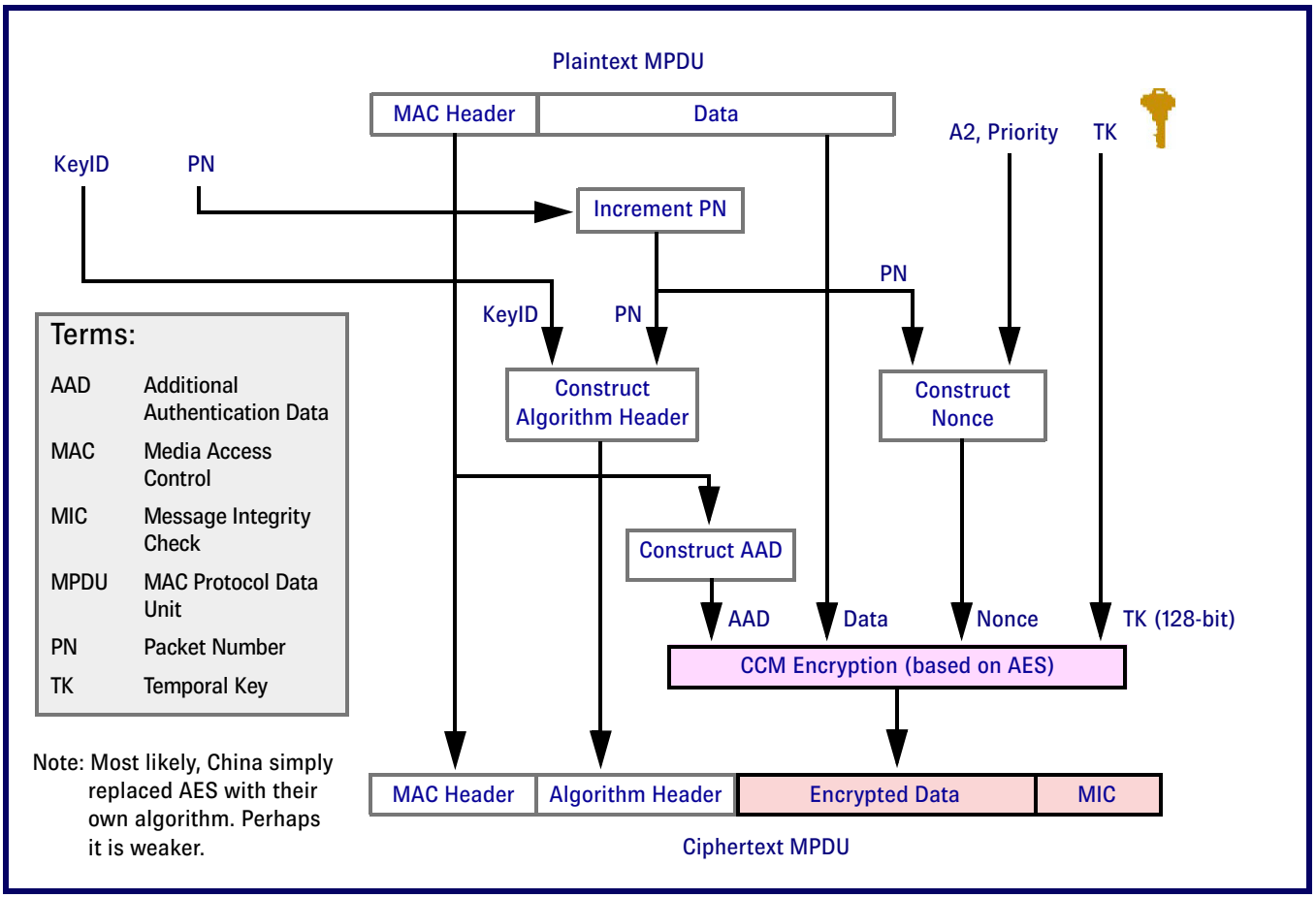
Wireless Flash Memory Security • Personal Area Network Security • Radius for Wireless • 3G Security • Public Keys & Wireless • 1XEV Security

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary, Alberta T2N 3W1, Canada. **Phone**: 1-800-633-5514 (+1-403-274-4749) **Fax**: +1-403-289-6658 **Email**: cnpsales@cnp-wireless.com **Web**: www.cnp-wireless.com/wsp.html **Subscriptions**: $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.

Figure 1: 802.11i RSN Counter Codebook Mode



WSP Erudite Readers get a Financial Break for 2004!

There will be no price increase for *Wireless Security Perspectives or Cellular Networking Perspectives* for 2004, but the July and August issues will be merged. We still expect to exceed our goal of providing, throughout the year, at least 72 pages of up-to-date, accurate and concise information – about wireless security, fraud management and emerging technologies in this publication.

We would also like to wish all our customers and their families "Happy Holidays" and all the best for 2004.

Are you the Arcanist?

For last month's Mathematics Corner, the series goes like this: ... 121393, 75025, 46368, 28657, 17711, 10946, 6765, 4181, 2584 ...

This series is a descending Fibonnaci series, so the next number was 6765 (17711 minus 10946).

Congratulations to Duncan Ho (from Qualcomm), who very quickly submitted the correct answer and was awarded a CNP golf shirt made from environmentally friendly recycled cotton and tagua palm nut buttons.

The question for this month:

What is next in the series:

1, 11, 21, 1211, 111221, 312211?

Submit your answer to wsp@cnp-wireless.com

Thanks to Greg Rose, Qualcomm, for submitting this month's puzzle.

Upcoming Wireless Security and Fraud Conferences & Events

The following are upcoming wireless, wireless security and general security conferences and events that may be of interest to our wireless security and network security practitioners.

CCNC 2004
(IEEE Consumer Communications and Networking Conference)
5th- 8th January 2004
Caesar's Palace
Las Vegas, NV
www.ccnc2004.org

Hands-On Wireless Security
13-14 January 2004
Hilton Scottsdale Resort
Scottsdale, AZ
www.gocsi.com/training/erc/hows.jhtml

MDM 2004
(IEEE International Conference on Mobile Data Management)
19-22 January 2004
Doubletree Hotel
Berkeley, CA
www.cs.duke.edu/mdm2004

Wireless Communications Symposium
20-22 January 2004
Hotel Meridien
Lisbon, Portugal
www.wcs2004.com

DallasCon Network Security Training
21-23 January 2004
Addison Quorum Courtyard
Addison, TX
www.dallascon.com/seminar.asp

WCAI 10th Annual Technical Symposium & Exposition
23-25 January 2004
Fairmont Hotel
San Jose, CA
www.wcai.com

COMNET '04
26-29 January 2004
Washington Convention Center
Washington, DC
www.comnetexpo.com

ISACA National Capital Area Chapter – Wireless Security
27 January 2004
Holiday Inn Capitol
Washington, DC
isaca-washdc.org/content/events/monthly-Jan2004.htm

SICon/04
27-29 January 2004
InterContinental Hotel
New Orlean, LA
www.siconference.org

2004 High Assurance IP Encryption (HAIPE) Symposium
27-29 January 2004
Shelten Point Hotel and Marina
San Diego, CA
www.iaevents.com/haipe04/newinfo.cfm

IT-Defense 2004
28-30 January 2004
nestor Hotel Ludwigsburg
Ludwigsburg, Germany
www.itdefense.de

SANS Honeypots 2004
(Honeypots: Tracking Hackers)
28-29 January 2004
Omni Shoreham Hotel
Washington, DC
www.sans.org/hp_washingtondc04

WHOLES
30-31 January 2004
Sigtuna Foundation
Sigtuna, Sweden
www.sics.se/privacy/wholes2004

The Sound of Security

Michael Paddon, Qualcomm

SonicKey is a research project with a goal of providing a strong authentication mechanism that can be cheaply deployed and used in the real world.

The need for better authentication is manifest; every security professional knows that birth dates, mothers' maiden names and social security numbers are weak authenticators, at best. Yet enterprises and other organizations frequently rely on such information to confirm a person's identity.

A determined hacker can easily ferret out this personal data by using online data-mining techniques. Another common identity validation approach is to send a new PIN or password to the stored e-mail address. This approach works only if we can assume that hackers cannot divert the e-mails of their victim or get read-only access to their e-mail files. The bottom line is that technological progress is rapidly devaluing these authentication techniques from weak to worthless.

Passwords are better, if only because people know that they are supposed to be kept confidential. After all, who keeps their birthday a strict secret? But passwords have vulnerabilities too. They can be overheard, read over your shoulder, intercepted in transit, chosen unwisely (e.g, '123456') or captured from a compromised database.

The biggest inconvenience of passwords is having to remember a different one for every organization with which you interact or for every application you use. Most people either write them down, increasing the likelihood of compromise, or use the same password

for multiple accounts, all of which now can be accessed by a hacker who cracked just a single account. A single compromise can have serious negative consequences.

A better alternative is public key authentication. This uses a pair of keys: one that only the user has – called the private key, and one that is broadcast or otherwise openly provided – called the public key. Keys are typically thousands of bits longs, so they are stored in the user's terminal, handheld device or token rather than memorized. The **October 2000** issue of *Wireless Security Perspectives* includes more about public-key cryptosystems, with a basic description and a comparison of three of them.

Private keys can be used to digitally sign a message. Anyone with the user's public key can decode it to check if the signature is valid. It is virtually impossible to forge a digital signature without access to the private key. To authenticate the user, a challenge (any unique message) is sent to the user's device, which digitally signs it to create a response.

By checking that signature, the challenger can confirm that the user holds the private key and, by extension, is most likely who they claim to be. An eavesdropper gains nothing by recording the exchange, because next time there will be a different challenge.

Public key authentication is widely used. For example, the popular SSL security layer used by many Web sites uses public key authentication to give surfers confidence that the sites they are viewing have not been spoofed or forged.

So Secure, You Can Hear It

In other applications, public key authentication can be more challenging to implement. For example, how do users perform a challenge-response exchange with a bank teller or stock broker? This is the problem that SonicKey tackles.

SonicKey makes strong authentication more flexible by encoding authentication messages (such as public key challenges and responses) as bursts of audio that sound like a second or two of white noise. SonicKey involves both transmitting and receiving sound. In a classic challenge-response scenario, a SonicKey device does both. When running a simpler protocol, it is possible to have one device only emitting and one only listening.

To send or receive a SonicKey message, all that is needed is a device with modest computing power, a speaker and a microphone. Most notebooks, and many desktops, meet these requirements. If not, the cost of adding them is minimal.

All cell phones have speakers and microphones, and some even have speakerphone capabilities that work from several feet away. More and more PDAs are gaining communications capabilities, and with them a speaker and a microphone.

By performing public key authentication via audio bursts, SonicKey solves the biggest problem of all: deployment. Many people are already carrying a SonicKey-capable device – everyone with a cellphone that is software upgradeable, for example. No expensive hardware upgrades are necessary – just the enabling software.

Although the same approach could be applied to transmission by radio waves or infrared, SonicKey's audio transmission has some interesting advantages. SonicKey works across any audio medium, including telephones. Thus, users can authenticate themselves to their Swiss bank just by phoning it. The user is aware when authentication is requested and responded to, simply because they can hear it, and they have an intuitive grasp of the distance that the audio signal will cover.

One of the biggest problems with using public key authentication systems is the distribution of public keys. How does your bank, your broker or your airline get your public key, and how do they really know it is yours?

The traditional solution has been the Public Key Infrastructure (PKI), as typified by the X.509 international standard. In this world, public keys get digitally signed by a Certification Authority (CA) that confirms the user is who they claim to be. At that point, the bank needs only the CA's public key, with which they verify the user's public key.

In practice, however, that scenario does not always work well. One problem is whether a user's bank, broker and airline all trust the same CA. That rarely happens, mostly because CAs are notorious for being happy to accept fees but loathe to accept liability for signing keys. Another problem is that the system is more complicated than most users can or will deal with.

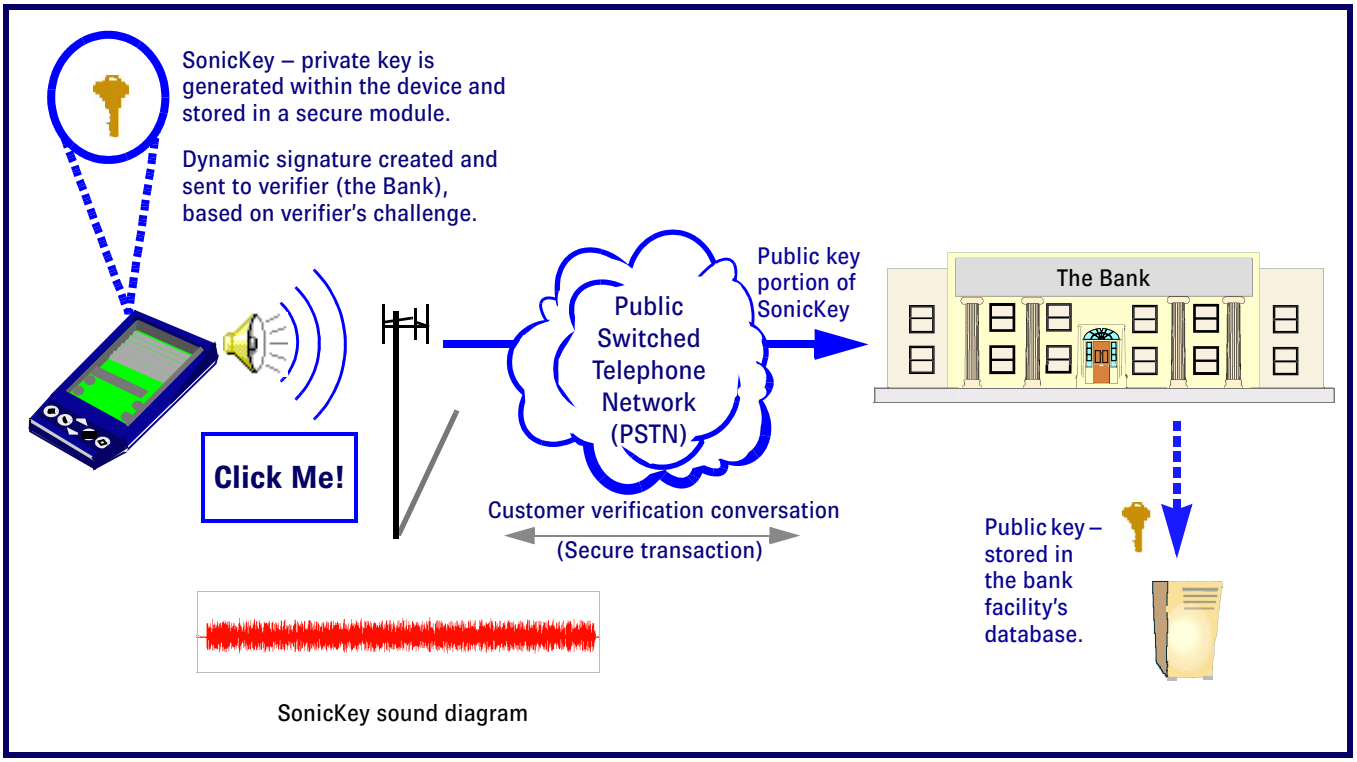
SonicKey solves this key distribution problem neatly by letting users control the process directly. They simply give the bank their public key by walking into a branch, showing several forms of ID and playing the key into a speaker. A similar process can apply to all the organizations that a person might interact with. Users also can even authenticate over the phone by simply engaging in a conversation to demonstrate their identity (as illustrated in **Figure 2**).

Users can afford to take the time to do this, because it only needs to happen once. Thereafter, they use their SonicKey.

In security parlance, this technique is called "out-of-band" key distribution, and it works extremely well in practice.

The bank could also transmit a public key to the client, which would allow the client to authenticate the bank at a later time. This, of course, requires that the user's device stores a distinct public key for each party that the user wishes to authenticate. Often this additional complexity is undesirable because the user initiates each conversation and places some trust in the communication medium. For instance, a user phoning their bank usually would not require additional authentication on their behalf.

Figure 2: SonicKey 'out-of-band' Key Distribution



Private keys must never be transmitted by either entity.

What happens if a private key is lost or stolen? First, the private key would be protected by a PIN or pass-phrase to prevent casual misuse, just like a cell phone is often protected with a PIN. This requirement gives users time to contact organizations with which they have registered their key, to tell them it has been revoked. Users can then acquire a replacement device, generate a new key pair and re-register it with their organizations.

SonicKey Options

SonicKey has been successfully implemented as a BREW application, allowing it to be loaded on to a wide range of cell phones. There are also Java and C implementations, making it portable to just about any modern programmable device. Although classic public key authentication has been the primary production goal with SonicKey, research continues to experiment with alternative, domain-specific, light-weight authentication protocols.

SonicKey's security is still user-friendly. The most natural way of using public keys is for users to generate them and then give them to companies and other organizations with whom they want to do business. For many users, this means they need just one key, although nothing stops a user from deciding to use several. In this model, the private key is never transmitted and may even be stored in a secure module inside the phone, thus making its compromise much less likely. Although SonicKey does not preclude hierarchies such as X.509, its design is intended to let users manage their own key distribution. It seems this is the easiest, most intuitive approach for most people.

SonicKey can transmit in three different modes:

1. The user is physically present and plays the audio directly from the speaker of the SonicKey device into the authenticating device.
2. The user places a landline phone call to the institution's authentication system and plays the sound from the speaker of the SonicKey device into the microphone of the landline telephone.
3. The user transmits over the radio interface of a cell-phone. Currently this is possible only in old analog phones, as newer digital phones apply voice coders that garble a SonicKey audio burst. It is intended that SonicKey-compatible cell-phones will simply decode the burst, transmit the frame digitally and recode the burst at the far end. Such cell-phones could either act as authentication end-points themselves, or simply as audio relays for other SonicKey-compatible equipment. The audio might still be played through the speaker to let users know that authentication is occurring.

SonicKey is implemented with any mix of functionality, depending on what the device requires. Some provide transmit support – some receive. In general, a phone is expected to need both types of modules to participate in challenge-response-type exchanges. More specialized devices, on the other hand, may be configured just to transmit.

One example of a specialized implementation that we have built is a door wired to unlock when presented with a signed time-stamp. Because this is a unidirectional protocol, only the transmit code is in that phone.

Other applications using SonicKey could include point of-sale transactions, computer log-in, and e-commerce. SonicKey is being demonstrated around the world, at technical conferences and elsewhere – and many observers have come up with applications that we had not thought of.

About the Author

Michael Paddon (mwp@qualcomm.com) is a researcher at Qualcomm, specializing in information security. He is a computer scientist with over 16 years of commercial experience, with a primary focus on security, networking and open systems. He has worked for several multi-nationals and a number of startups, including 6 years as CTO of a successful internet security startup.

About Qualcomm

Qualcomm (www.qualcomm.com) is a leader in developing and delivering innovative digital wireless communications products and services based on the company's CDMA digital technology. The company is headquartered in San Diego, California.

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.

Fraud and Security Patent News

US Patent: 6,665,692

Method for updating a linear feedback shift register of a code generator

Three different methods for updating a linear feedback shift register of a code generator, and code generators applying the methods. In the basic method a Galois-type linear feedback shift register of a code generator is updated to a target state which is at a known offset from a unit state. The basic method comprises the following: generating a binary offset number illustrating the offset; generating a counter showing the number of bits in the binary offset number; initializing a temporary state with the unit state; iterating as long as the counter value is higher than zero; multiplying the temporary state by itself by applying a Galois Field multiplication; shifting the temporary state one state forward from the current temporary state if the value of the bit shown by the counter is one; and decrementing the counter value by one; in the end, when the counter has reached the value zero, setting the temporary state as the target state. The described basic method is also employed in methods for updating a Galois-type/Fibonacci-type linear feedback shift register of a code generator to a new state which is at a known offset from a current state.

Issued: December 16, 2003

Inventor: Esko Nieminen
Assignee: Nokia Mobile Phones Ltd. (Espoo, FI)

US Patent: 6,665,530

System and Method for preventing replay attacks in wireless communications

A method and apparatus for confirming the identity of a mobile station in a communication network. A mobile station transmits a security value to obtain access to the network. The system authenticates the mobile station prior to granting it access to the network. The system performs an additional procedure before granting access to the system if the security value sent by the mobile station matches a previously transmitted security value. Using this invention, the system prevents attempts of replay attacks by intruders.

Issued: December 16, 2003

Inventors: Samuel Broyles and Roy Quick
Assignee: Qualcomm Incorporated (San Diego, CA)

US Patent: 6,665,529

System and method of authenticating a subscriber at registration

An apparatus for authenticating a subscriber at registration. It is provided for use in a mobile communications system having at least a switching center communicatible with at least one equipment registry and at least two subscriber registries, wherein, for each system subscriber, data associated with that subscriber is stored at a unique address in one of the subscriber registries. The apparatus includes:

- Switching apparatus for requesting and receiving an equipment identity number from a mobile communications device attempting to use the communications system,
- An equipment registry storing, for each mobile communications device posted with the system,
- The equipment identity number and the unique address in the subscriber registries of the data associated with that equipment identity number,
- Apparatus for transmitting a received equipment identity number from the switching apparatus to the equipment registry,
- Apparatus for retrieving a unique address associated with the transmitted equipment identity number and transmitting the unique address to the switching apparatus,
- Apparatus for communicating directly with the unique address in the subscriber registries to retrieve data therefrom to the switching apparatus and,
- Apparatus for determining whether to authorize use of the system by the mobile communications device attempting to use the communications system, based on the retrieved data.

Issued: December 16, 2003

Inventor: James Mills
Assignee: Ericsson Inc. (Research Triangle Park, NC)

US Patent: 6,665,420

Message authentication code with improved error tolerance

A method of generating an authentication code ("MAC") with improved error tolerance that exhibits improved survivability against acceptable signal distortions such as recompression. A method of generating a message authentication code associated with an image includes receiving blocks of image coefficient data where each coefficient has an original value falling within a range of values. The range of values is divided into first and second regions, both having allowed coefficient values, and an error tolerance buffer region formed between the first and second regions having disallowed coefficient values. The original values of DC coefficients from each block of the image coefficient data is mapped to a modified value contained in one of the first and second regions, but not contained in the error tolerance buffer region. A MAC is generated as a function of the most significant bits of the modified image coefficient values.

Issued: December 16, 2003

Inventor: Liehua Xie, et al
Assignee: Verizon Laboratories Inc. (Waltham, MA)

Notable Reference:

L. Xie, et al. *Secure MPEG Video Communication by Watermarking*, Proceedings of the 3.sup.rd Annual FEDLAB Symposium, Feb. 1999, pp. 459-463.

US Patent: 6,665,405

Cyclotomic polynomial construction of discrete logarithm cryptosystems over finite fields

A system relating to Cyclotomic polynomials. These are used to construct subgroups of multiplicative groups of finite fields that allow very efficient implementation of discrete logarithm-based public key cryptosystems, including public key encryption schemes and digital signature schemes. A field is represented with an optimal normal basis, and a generator of a subgroup of the multiplicative group of the field is used to form a public key.

Issued: December 16, 2003

Inventor: Arjen Lenstra
Assignee: Citibank, N.A. (New York, NY)

Notable References:

[1] Lenstra. *Using Cyclotomic Polynomials to construct Efficient Discrete Logarithm Cryptosystems over Finite Fields*, Jul. 97 ACISP 1997, pp. 127-138.

[2] Taber EIGamal, *On Computing Logarithms Over Finite Field*, CRYPTO 1985, pp. 396-402.

[3] Hellman, M.E, and J. M. Reyneri. *Fast Computation of Discrete Logarithms in GF*(q). In Advances in Cryptography, Proceedings of CRYPTO '82, D. Chaum, R. Rivest and A. Sherman, eds. Plenum Press. 1983.

202.115.65/Cipher/HTML/PDF/C82/3.PDF

US Patent: 6,664,915

Identification friend or foe system including short range UV shield

An identification friend or foe system for use by a weapon to determine whether a target that has been selected is a friendly target. The system comprises a signal source attached to the target and arranged to radiate encrypted signals. A detection system attached to the weapon includes a receiver arranged to receive the encrypted signals when the weapon is within a pre-determined range from the target. Signal processing apparatus is connected to the receiver and arranged to determine whether the encrypted signals identify the target as being friendly. The central processing unit is arranged to decrypt the encrypted signal and produce a disarm signal if the target is identified as being friendly. The central processing unit preferably is also arranged to produce a signal that causes the weapon to perform a collision avoidance maneuver to avoid colliding with the target if the target is identified as being friendly.

Issued: December 16, 2003

Inventor: Daniel Britton
Assignee: The United States of America as represented by the Secretary of the Navy (Washington, DC)

US Patent: 6,654,884

Hardware-level mitigation and DPA countermeasures for cryptographic devices

Countermeasures for differential power analysis, a powerful cryptanalytic method that attackers can use to extract secret keys from cryptographic hardware during operation. To reduce the risk of compromise, cryptographic hardware can employ countermeasures to reduce the amount of secret information that can be deduced by power consumption measurements during processing. Such countermeasures can include balancing circuitry inside a cryptographic hardware device to reduce the amount of variation in power consumption that is correlated to data parameters being manipulated. This can be facilitated by using a constant-Hamming-weight representation when representing and manipulating secret parameters. Low-level operation modules, such as Boolean logic gates, can be built to process input parameters in a manner that balances the number of ON transistors while simultaneously maintaining a data-independent number of transistor transitions during computation. Leakage reduction may be used with other counter-measures, including introducing noise, unrelated to data being processed, into the power measurements.

Issued: November 25, 2003

Inventor: Joshua Jaffe, et al
Assignee: Cryptography Research, Inc. (San Francisco, CA)

US Patent: 6,654,883

Device authentication and encrypted communication system offering increased security

A system composed of a plurality of user devices, each storing unique secret information, a system device and a control unit. The control unit produces key capsule data by performing a digital signature conversion with message recovery on the unique secret information for each user device and distributes the unique secret information to the user devices. When device authentication and encrypted communication is performed, each user device transmits the key capsule data distributed by the control unit to the system device. The system device receives the data and recovers the unique secret information from the key capsule data by a digital signature verification conversion with message recovery, which uses the verification key distributed in advance by the control unit. Thus, the user device and the system device can share unique secret information and, using it as a key, perform device authentication and encrypted communication by performing encryption and decryption based on a secret key encryption algorithm.

Issued: November 25, 2003

Inventor: Makoto Tatebayashi
Assignee: Matsushita Electric Industrial Co., Ltd. (Osaka-fu, JP)

US Patent: 6,654,465

Method of implementing a key recovery system

A method of generating a recovery key encryption key (RKEK) in a secure manner by an integrated circuit (IC) and a key recovery escrow agent includes the steps of generating, by the IC, a first number having a private component and a public component, and generating by the escrow agent a second number having a private component and a public component. The public component of the first number is provided to the escrow agent, and the public component of the second number is provided to the integrated circuit. A Diffie-Hellman modulo-exponentiation mathematical operation is performed by the integrated circuit using the private component of the first number, the public component of the first number and the public component of the second number to create the RKEK. A similar operation is performed by the escrow agent using the private component of the second number, the public number of the second number and the public component of the first number to create the RKEK at its end.

Issued: November 25, 2003

Inventors: Timothy Ober and Peter Reed
Assignee: SafeNet, Inc. (Baltimore, MD)

US Patent: 6,651,171

Secure Execution of Program Code

A curtained operation that allows trusted execution of code and secrecy of data in a secure memory. Curtained code can only be executed from within certain address ranges of a curtained memory region secure against access by code from without the region. Code entry points are restricted, and atomic execution is assured. The memory is organized into multiple hierarchically curtained rings, and peer subrings are denied access to each other as well as to more secure rings.

Issued: November 18, 2003

Inventors: Paul England and Butler Lampson
Assignee: Microsoft Corporation (Redmond, WA)

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