# Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 7, No. 1. January, 2005


## Thank You Readers!

*David Crowe, Editor*

Thank you, loyal readers, for your support of *Wireless Security Perspectives* during its five-year history. We appreciate all the positive feedback we received over the years. This is our last issue. Those whose subscriptions have not ended will be receiving refunds over the next few weeks.

The staff of *Wireless Security Perspectives* wishes you the best in your endeavors, especially those involving the wireless world. There is much fertile ground for wireless innovations, including those needing greater security.

We hope that your back issues of WSP will remain a useful resource to you. Back issues will still be available for US$25 each if you wish to fill out your library with a complete set of issues back to 1999.

## The Latest in WiFi Certification ... and WAPI

Last summer, the IEEE ratified the 802.11i amendment. The result is stronger security for users of 802.11 wireless systems (even those including legacy products).

The WiFi Alliance is coordinating certification testing for 802.11i. Protection in compliant devices is based on RSN (Robust Security Network), often informally called WPA2 (WiFi Protected Access 2).

Security in networks using WPA2 with 802.11a, b and g devices will be similar to that which is applied to much of the U.S. government's encrypted information. The WiFi Alliance targets 2006 as the year when WPA2 security will replace WPA as mandatory for manufacturers wanting to boast of WiFi Certified devices.

WPA2 employs AES encryption supporting 128-bit, 192-bit, and 256-bit keys. This improves the modestly secure encryption of WPA, which uses TKIP. Both WPA and WPA2 are using CCMP. For more information about WPA, TKIP and CCMP, refer to the **November 2002** and the **November 2003** issues of *Wireless Security Perspectives* or the WiFi Alliance website.

Six companies (working with eight product entries) are currently participating in the WPA2 security test-bed which began in September. These are Realtek, Atheros, Instant802 Networks, Cisco Systems, Broadcom and Intel. Mostly, they are focusing on WPA2 support, but one is going a step further. Taiwan-based Realtek Semiconductor Corporation's entry, the 8255 combo RFIC, includes an option allowing the user to choose between WPA2 or China's WAPI security standard.

Companies with connections to China may be looking for marketing advantages, although support of WAPI (Wireless Authentication and Privacy Infrastructure) may not help elsewhere. Even the Chinese admit WAPI has little chance of acceptance in the world market.

## The Chinese Saga

WAPI supporters tried to make a comeback last summer. Chinese delegates at meetings with the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) complained of known defects in the 802.11 security standard. Their proposed remedy included a WAPI security mechanism. The events following their complaint could be interpreted as retaliation against the Chinese. For example, the U.S. embassy in China blocked them from getting visas necessary to attend a pivotal conference held on November 11th, 2004 in the U.S.


*Wireless Security Perspectives* (ISSN 1492-806X (print) and 1492-8078 (email)) is published **11** times a year by Cellular Networking Perspectives Ltd, 2636 Toronto Cresc. NW, Calgary, Alberta T2N 3W1, Canada. **Phone**: 1-800-633-5514 (+1-403-274-4749) **Fax**: +1-403-289-6658 **Email**: cnpsales@cnp-wireless.com **Web**: www.cnp-wireless.com/wsp.html **Subscriptions**: $350 for delivery in the USA or Canada, US$400 elsewhere. **Payment**: accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery**: Email or 1st class mail. **Back Issues**: Available individually for $35 in the US and Canada and US$40 elsewhere, or in bulk at reduced rates. **Discounts**: Educational and small business discount: 25% off any order. **Copies**: Each subscriber is licensed to make up to **10** copies of each issue or back issue. Call for rates to allow more copies.

Technical Editor and Illustrator: Les Owens.

Article Sourcing: Tim Kridel.
Production: Doug Scofield.
Distribution: Debbie Brandelli.
Accounts: Evelyn Goreham.
Publisher: David Crowe.

## Upcoming Mobile & Wireless and Wireless Security Events

Below are mobile & wireless and wireless security events (or events with sessions on these topics) for early 2005. These upcoming events may be of interest to the theoretician and to the practitioner. The name, dates and venue of the event, plus URL, are provided.

*International Conference on Consumer Electronics*
January 8th- 12th
Las Vegas Convention Center
Las Vegas, NV
www.icce.org

*DoD Cyber Crime Conference*
January 10th- 14th
Westin Innisbrook Resort
Clearwater, FL
www.technologyforums.com/dodcybercrime

*Wireless Communications Association's 11th Annual International Symposium & Business Expo*
January 12th- 14th
Fairmont Hotel
San Jose, CA
www.wcai.com/event/05/ts11gen.htm

*Certified Wireless Network Administration Training*
January 17th
LLC International, Inc.
McLean, VA
www.securityuniversity.net/classes_wireless_CWNA.php

*2nd Annual Lone Star Network Security Forum*
January 19th- 20th
American Airlines Training and Conference Center
Fort Worth, TX
www.ianetsec.com/data/forums/Forum_Program3.pdf

*SECURECOMM Wireless Forum – Securing the 3G Infrastructure, GSM Operators, and Wireless Networks*
January 19th- 21th
Central London, UK
www.marcusevans.com

*Wireless Technology Forums (various wireless events)*
January 20th (and other dates in 2005)
Crowne Plaza Ravina Hotel
Atlanta, GA
www.airmagnet.com/company/shows.htm

*ICPWC 2005 (7th IEEE International Conference on Personal Wireless Communications)*
January 23rd- 25th
Kennesaw State University
New Delhi, India
www.elitexindia.com/icpwc2005/index.asp

*PKC 05 (8th International Workshop on Practice and Theory in Public Key Cryptography)*
January 23rd- 26th
Congress House
Les Diablerets, Switzerland
lasecwww.epfl.ch/pkc05/index.html

*RFID Lab @ WINMEC : Hands-on Workshop on RFID Application Development*
January 25th
UCLA
Los Angeles, CA
winmec.ucla.edu/rfid/experience

*Wireless Broadband – WiFi, WiMax and UWB*
January 25th- 26th
Hilton Hotel
Barcelona, Spain
www.telecoms.com

*Wireless Security Bootcamp*
February 3rd- 4th
Plano Center
Dallas, TX
www.airscanner.com/wireless

*RSA Conference 2005*
February 14th- 18th
Moscone Center
San Francisco, CA
2005.rsaconference.com/us

*"Making Tracks" (A conference on RFID, sponsored by CWTA)*
February 16th
Marriott Chateau Champlain
Montreal, Quebec
www.cwta.ca/CWTASite/english/conference/program.html

*4th Annual Mid-Atlantic Network Security Forum*
February 28th - March 1st
Wardman Park Marriott Hotel
Washington, DC
www.csoonline.com/events/viewevent.cfm?EVENT=8856

## Upcoming Mobile & Wireless and Wireless Security Events (continued)

*Mobile Convergence: MINMEC Annual Forum 2005*
March 8th
UCLA
Los Angeles, CA
www.wireless.ucla.edu/2005/enterprise

*WCNC 2005 (IEEE Wireless Communications and Networking Conference)*
March 13th- 17th
Ernest N. Morial Convention Center
New Orleans, LA
www.comsoc.org/confs/wcnc/index.html

*IEEE INFOCOM 2005 (24th Annual Event)*
March 13th- 17th
Hyatt Regency Hotel
Miami, FL
www.ieee-infocom.org/2005

*43rd Annual ACM Southeast Conference*
March 18th- 20th
Kennesaw State University
Atlanta, GA
acmse.kennesaw.edu

The Chinese delegation eventually did gain admittance to the U.S., arriving late to the conference. While attending, they presented a speech that seems to have resulted in an ISO resolution, submitted in December, to uphold WAPI as an alternate security model. The February 21st - 25th 2005 plenary meeting of the ISO/IEC JTC1 SC6 WG1 will address the possibility of making WAPI an international standard alongside 802.11i. Not everyone is happy about this. The IEEE, for example, opposes this dual standard scenario.

## Progress in Hashing Cryptanalysis

*Arjen K. Lenstra*


**Abstract.** Due to newly discovered weaknesses in the MD5 secure hash algorithm, all new designs should use SHA-1, until even stronger hashes become available. Existing systems using MD5 should confirm that they only need target collision resistance, not random collision resistance.

Several new hash function results were presented at the most important cryptology conference, Crypto 2004, held each August in Santa Barbara, California. Before the meeting there were two kinds of common hash functions – the known-to-be-weak ones, and the believed-to-be-good ones. Right now the former category is known-to-be-very-bad, but the latter category has hardly been affected.

If the security of your design relies on a formerly known-to-be-weak hash function such as MD4 or MD5, you most likely do not have to rush out and replace it, depending on what is required for a successful spoofing attempt. For instance, an existing digital certificate may contain the hash $H(b)$ of a bit string $b$. To spoof it, the attacker has to find a bit string $b'$, different from b, but with the same hash as b. Given $H(b)$, and possibly $b$ itself, finding a $b'$ whose hash value collides with it (i.e., $H(b) = H(b')$) is still considered to be sufficiently hard for all common hash functions.

This property of hash functions, that they are hard to invert, is their most important design criterion. This property is often referred to as *second pre-image resistance* or *target collision resistance*. Hash functions with n-bit values are designed in such a way that inverting them (or finding a second pre-image, or constructing a target collision – whatever one prefers to call it) should take on the order of $2^n$ operations. All common hash functions such as MD4 and MD5 (both with $n = 128$) or SHA-0 and SHA-1 (with $n = 160$), still offer more than adequate protection against spoofing attempts that target an existing hash value.

Therefore, against such attacks the security relies on the fact that for a given particular hash value it is hard to come up with a bit string that hashes to that value. Unfortunately, there are also applications of hash functions where the hash value is not given in advance. That gives the attacker a much larger degree of freedom. For instance, in digital signatures one customarily signs the hash $H(d)$ of a document $d$ (a bit string). In this scenario an attacker may construct a pair of different bit strings $d,d'$ such that $H(d)=H(d')$, but without any further restrictions on the particular value $H(d)$. The attacker then digitally signs $d$ (using $H(d)$), but later claims that not $d$ but $d'$ was signed. Since $H(d) = H(d')$, there is no way to deny

### Quote of the Month

*"It is the mark of an educated mind to be able to entertain a thought without accepting it."*

*Aristotle*

the attacker's claim. Therefore hash functions must be *collision resistant*: it must be computationally infeasible to construct different bit strings that hash to the same value.

Collision resistance puts a much heavier demand on the design and length of hash functions than target collision resistance. This is due to the so-called *birthday paradox*: the probability that among a group of 23 randomly selected people, at least two people have the same birthday is more than 50%. Because this probability is much higher than most people expect, it is referred to as a paradox. In reality there is no paradox at all. It can be proved mathematically and verified empirically that if elements are drawn at random from a collection of N objects (with replacement), then $k$, the expected number of draws before an element is drawn twice, is approximately:

$$k = 1.26\sqrt{N}$$

In the birthday example, $N$ would be 365. In the context of $n$-bit hash functions, there are $N = 2^n$ different objects (i.e., hash values). After hashing about $1.26 \times 2^{n/2}$ randomly selected different bit strings, one may expect – under reasonable assumptions about the random behavior of the hash function – that two bit strings are found with the same hash value. Therefore, for the digital signature application sketched above, the effort required by an attacker to successfully create a collision is only on the order of $2^{64}$ if a 128-bit hash function is used, and only about $2^{80}$ for a 160-bit hash.

## Are You the Last of our Arcanists?

Last month, we asked: What's next in this series? 9, 10, 11, 11, 12, 11 ...

Zero (0) is the answer. No one submitted the correct answer, but it's so easy! Why, this is the series showing the number of issues of *Wireless Security Perspectives* published each year. That number for next year was expected to be zero.

### Our last question ...

184,756; 167,960; 125,970; 77,520; 38,760 .... what is the next number?

***Clue:*** *Newton may have figured this out first.*

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

From a security point of view, collision resistance effectively doubles the hash length requirement as compared to target collision resistance. This is a general fact that applies to all hash functions, past and future. The results presented at Crypto 2004, however, made clear that for many common hash functions, the situation is much worse with respect to collision resistance. It was shown that random collisions (not target collisions) can be found by hand for MD4 and computed in a matter of minutes for MD5. With $n = 128$, both were designed to resist an effort of $2^{64}$. Furthermore, for SHA-0, with $n = 160$, collisions can be found with effort $2^{40}$, much lower than the intended design effort $2^{80}$.

For practical applications, this means MD4, MD5, and SHA-0 should no longer be used when an attacker is free to choose the value to be hashed. But because MD4 and MD5 have been known for a long time to be weak with respect to collision resistance, and because SHA-0 should never have been used anyway, the impact of the new findings should be very limited.

Nevertheless, the cryptographic community was astonished to see how much weaker MD4, MD5, and SHA-0 turned out to be. SHA-1 (with $n = 160$), and its recent extensions SHA-$i$ for $i = 256$, 384, and 512, are not affected by the methods presented at Crypto 2004.

So, what should be done in practice? For existing applications of affected hash functions, one should consider if the random collision attack scenario applies. If it does, a proper risk analysis should be carried out. If there are mitigating factors that may render the likelihood of successful attacks sufficiently low, one may decide not to take action; otherwise replacement of the hash function may be in order.

For new applications, the affected hash functions must not be used. For the moment, this limits the choice of hash functions mostly to SHA-1 and its extensions. This is not different from the situation before the new findings were announced.

Is this the end of the story? Should we now all happily use SHA-1 or its extensions and hope for the best? Or should we go for an overhaul and total redesign of our hashing methods and come up with something better?

Consider the situation in more detail. All common hash functions, including MD4, MD5, and SHA-0, 1, 256, 384 and 512, follow the same basic design principle, with just a single, relatively minor change setting apart SHA-1, 256, 384 and 512 from MD4, MD5, and SHA-0. Apparently this particular new feature offers adequate protection against the new collision attacks. But with the rest of the basic design already completely picked apart, how long will this last?

Adi Shamir, one of the world's most dreaded cryptanalysts and most respected cryptographers, recommends starting afresh. Given how long the Advanced Encryption Standard (AES) process took, it may be a while before a better hashing standard emerges. For the foreseeable future, however, SHA-1, 256, 384 and 512 remain the hashes of choice.

## Folklore about Hash Functions

Independent of the commotion caused by the new collision attacks, there was a very elegant and surprisingly simple result by Antoine Joux about the concatenation of hash functions.

If the results of two independent $n$-bit hash functions are concatenated, then according to cryptofolklore, the result is as good as a $2n$-bit hash function: finding a target collision should take effort $2^n \times 2^n = 2^{2n}$, and the effort of finding a random collision should take effort $2^{n/2} \times 2^{n/2} = 2^n$.

It was shown that if one of the hash functions is a so-called iterative hash function – and all common hash functions are iterative – then concatenation leads to hardly any additional security, refuting, for all practical purposes, the folklore assumption.

The most remarkable aspect of Joux's result may be that it took so long for such a straightforward argument to be published, strongly suggesting that hash-research is still in its infancy.

**A deeper look at Joux's argument.** An $n$-bit iterative hash function splits the input into a number of fixed size blocks, say $B_1, B_2, ..., B_r$. The hash is calculated in $r$ rounds as a function of the $r$ blocks and a fixed $n$-bit *initialization vector* $R_0$ that depends only on the hash function: for $i = 1, 2, ..., r$, a round function is applied to $R_{i-1}$ and $B_i$ and produces an $n$-bit value $R_i$. The resulting hash is the $n$-bit value $R_r$. Therefore, in the $i$th round, the round function is applied to the result of the previous round (or the fixed initial value $R_0$ if $i = 1$) and the $i$th input block.

Now construct a collision for an $n$-bit iterative hash function $H$: values $x_{11}$ and $x_{12}$ with $x_{11} \neq x_{12}$ such that $H(x_{11}) = H(x_{12})$. This takes at most about $2^{n/2}$ operations. Denote $H(x_{11}) = H(x_{12})$ by $C_1$. Similarly, it takes at most about $2^{n/2}$ operations to construct a collision for $H$ where its initialization vector is replaced by $C_1$: $x_{21}$ and $x_{22}$ with $x_{21} \neq x_{22}$ such that:

$$H_{C_1}(x_{21}) = H_{C_1}(x_{22})$$

where the subscript $C_1$ indicates usage of $C_1$ as an initialization vector as opposed to the default initialization vector.

It then follows, from the way iterative hash functions work, that $H$ applied to the concatenation of $x_{1i}$ and $x_{2j}$ – with $i, j \in \{1, 2\}$ – always results in the same value, say $C_2$, independent of the choices of $i$ and $j$.

So, the two pairs $(x_{11}, x_{12})$ and $(x_{21}, x_{22})$ result in a four-way collision, and therefore four distinct values that all have the same hash value $C_2$:

$$x_{11}||x_{21} \quad x_{11}||x_{22} \quad x_{12}||x_{21} \quad \text{and} \quad x_{12}||x_{22}$$

(with '||' denoting concatenation)

Furthermore, this four-way collision can then be concatenated with a newly constructed collision for $H_C$ resulting in an eight-way collision to $C_3$, and the eight-way collision can be concatenated with a collision for $H_C$ for a sixteen-way collision, etc. Repeating this construction $m/2$ times, we find that a $2^{m/2}$-way collision for $H$ can be found after at most about $(m/2) \times 2^{(n/2)}$ operations – that is, $2^{m/2}$ different inputs that all hash to the same value under $H$.

For any $m$-bit hash function G, one may expect, based on the birthday paradox, that among those $2^{m/2}$ different inputs that collide for $H$, there is a pair that collides for $G$ as well. This implies that a collision can be found for the hash function consisting of the $n+m$-bit concatenation of the hash functions $H$ and $G$. This takes, essentially, only $m/2$ times the effort to find a collision for $H$, plus about $2^{m/2}$ applications of $G$ to identify the $G$-collision. That is much less than the effort $2^{(n+m)/2}$ that one would expect for a decent $m+n$-bit concatenation of the hash function. Note that the argument works for any m-bit hash function $G$, and that only $H$ has to be iterative.

## About the Author

Arjen K. Lenstra is Distinguished Member of Technical Staff at Bell Laboratories, Lucent Technologies. Before joining Bell Labs in 2004, he was Vice President at Citibank's Information Security Office, Citibank, New York, Senior Scientist at Bellcore, Visiting Professor at The University of Chicago and he held visiting positions at IBM's Thomas J. Watson Research Center, AT&T Bell Labs, and DEC Systems Research Center. Furthermore, since May 2000, he is professor of cryptology at the Technical University Eindhoven, The Netherlands. His main research interest is cryptanalysis of public key cryptosystems, in particular the RSA cryptosystem. Lenstra wrote the software that was used to break the famous 1977 Scientific American RSA challenge, and he was involved in the first successful attack on a 512-bit RSA modulus in 1999. He is co-inventor of the public key cryptosystem XTR. He received his Ph.D. from the University of Amsterdam, The Netherlands.

## The Hunt for Stolen Handsets

*Tim Kridel*

Just how bad is handset theft in Europe? In London alone, a handset is stolen in more than half of the 4,000 street crimes that occur each month. In more than 1,200 cases so far, victims were singled out for their phones. In response, the U.K. government created the National Mobile Phone Crime Unit in December 2003.

In the Netherlands, 240,000 handsets are stolen each year. In response, Vodafone Netherlands announced (October 29th 2004 press release) that beginning in first quarter 2005, it would block service to stolen and lost handsets owned by its customers. For years, the carrier has tried to block service to lost and stolen handsets based on the SIM. However, thieves can bypass this by selling the phone without a SIM, making the theft undetectable, when the user of the stolen phones use it with a legitimate SIM with a different IMSI. The new policy expands that ability to the handsets themselves by using the International Mobile Equipment Identity (IMEI), the 56-bit code used in GSM-based phones, including UMTS devices. In the next year or two, a close relative of the IMEI, the MEID, will also be used in TDMA (TIA-136) and cdma2000 phones as well.

Although IMEIs can be altered, the Netherlands' Minister of Justice has proposed making that illegal as another theft deterrent. In February 2004, the GSM Association and seven handset vendors announced plans to begin configuring new handsets so that IMEIs cannot be reprogrammed.

By adding support for IMEI-based blocking, Vodafone Netherlands is able to join its parent company's Equipment Identity Register (EIR), a database used by Vodafone carriers in 11 countries and by five roaming partners. Once a lost or stolen handset is logged into the EIR, it is permanently blocked from service on networks operated by the participating carriers.

Even so, loopholes remain. For example, it is still possible to use a stolen Vodafone device on a non-Vodafone network. Although the GSM Association's Central Equipment Identity Register (CEIR) is another way to identify and block lost or stolen handsets on a wider range of networks, it is possible to bypass that system by cloning the IMEI of a good handset and then applying it to a stolen one (even assuming that the IMEI was reported lost or stolen to the EIR).

Enterprise customers have a particular concern about their proprietary company information stored on or made accessible through handsets. JP Mobile's SureWave Mobile Defense is used by individuals, healthcare providers, financial services and government agencies to remotely implement security measures, such as a device wipe, device lock, securing of specific files or types of data, and provision for workgroups (e.g., passwords).

Some carriers are responding to the issue of handset theft by 'reaching out and cleaning up.' In November 2004, Sprint announced Managed Mobility Services, which can remove all data in a lost or stolen handset in under three minutes by sending a "poison pill" that will be activated when the device connects to the network.

But when one hole is plugged, another one opens. For example, some GSM and CDMA handsets now include 802.11, and more are planned for 2005. As a result, unless the poison pill can be fed over a public or private Wi-Fi network, it will still be possible to use a stolen dual-mode handset as long as it is not connected to the cellular network.

Even the poison pill has to be implemented with good security to prevent unauthorized users from sending it and erasing all the data on a device that it is in the hands of the legitimate user.

## Fraud and Security Patent News

### US Patent: 6,836,862

***Method of indicating wireless connection integrity***

This invention discloses a method and system thereof for monitoring the data transfer integrity of a wireless connection between two devices, in particular two Bluetooth-enabled transceivers. A number of data packets are transmitted from one of the two devices to the other in a first-occurring transmission. The receiving device indicates to the transmitting device whether any of the data packets were not successfully received. Any data packets that were not successfully received are retransmitted. The integrity of the wireless connection is measured, for example, by determining the number of data packets successfully transmitted in the first-occurring transmission relative to the total number of data packets transmitted and retransmitted. The measure of wireless connection integrity can be provided to a user via either a visual or audio indication, or it can be provided to another device such as a computer system, so that corrective actions can be taken if needed in order to improve the data transfer integrity of the wireless connection.

Issued: December 28, 2004

Inventors: Rich Erekson and Darrell Goff
Assignee: 3Com Corporation (Santa Clara, CA)

*Notable Reference:*

[1] Excerpts from "Specification of the Bluetooth System." Compiled by Dan Sonnerstam, Pyramid Communications AB, V 1.0 B, Dec. 1, 1999. Pages 1-13, 70, 71, 527, 686,691, 693.

**US Patent: 6,836,845**

***Method and apparatus for generating queries for secure authentication and authorization of transactions***

This invention discloses 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 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.

December 28, 2004

Inventor: Robert Lennie, *et al*

Assignee: Palm Source, Inc. (Sunnyvale, CA)

*Notable Reference:*

[1] Samar, Vipin. *Single Sign-On Using Cookies for Web Applications.* Jun. 19, 1999, IEEE.

**US Patent: 6,836,655**

***Secure interlink receiver for remote programming of wireless telephones***

This invention describes an interlink receiver system and receiver unit for remote encoding wireless phone units. The invention includes a host computer that communicates with the interlink receiver unit over telephone lines or airways to encode wireless phone units with the key code for authentication of the phone unit and encryption of communications from the phone unit during use, the interlink receiver unit connecting to the host computer for data exchange and controlling the encoding of a connected phone unit.

Issued: December 28, 2004

Inventor: Theordore Watler, *et al*

Assignee: Telemac Corporation (Los Angeles, CA)

**US Patent: 6,834,112**

***Secure distribution of private keys to multiple clients***

This invention discloses means for securely distributing a private key to a user of a remote client computer over an insecure channel. The user's private key is transmitted to the client from a remote server in an encrypted format. A first hash of the user's password is transmitted to the remote server and is used to authenticate the user. A second hash of the user's password remains with the client computer and is used to decrypt the user's private key. The user only has to remember one login name and a single associated password. Thus, the private key can be securely distributed from the remote server to the client computer system. The distribution does not require the user to carry any special hardware devices and only requires a single password. Because the private key is not permanently stored at the client computers, even if an unauthorized user has access to the client computers, they are not likely to be able to obtain the private key. Similarly, because the remote server only has access to an encrypted version of the private key, and because the remote server does not store and has no way of uncovering the user's password, the remote server, even if broken in to, is not likely to compromise the user's private key.

Issued: December 21, 2004

Inventor: Ernie Brickell

Assignee: Intel Corporation (Santa Clara, CA)

*Notable Reference:*

[1] Kaufman, Perlman, Speciner, *Network Security Private Communication in a PUBLIC World.* Prentice Hall PTR, 1995. p. 433-38, 443-47.

## 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: 6,832,314

***Methods and apparatus for selective encryption and decryption of point to multi-point messages***

This invention discloses methods and systems for selectively encrypting and decrypting messages transmitted on a channel of a communication network, such as a broadcast channel. Group encryption keys are provided for one or more services utilizing the broadcast channel to communicate messages. A message associated with a particular service first receives an error check value, such as a cyclical redundancy check (CRC) value generated from the unencrypted message. The message is then encrypted using the group encryption key for the service and the CRC is added to the encrypted message and transmitted with a broadcast address of the communication network. A receiver then receives the message and determines that the CRC indicates an error (as it is generated from the encrypted message rather than the unencrypted message). The receiver then decrypts the message using the group encryption key for the service (assuming the receiver is authorized to receive the service, i.e., has access to the group encryption key) and generates a CRC from the decrypted message. If this CRC matches the CRC received with the message, the receiver recognizes the message as being associated with the corresponding service and processes the message accordingly. Where multiple services are supported and the receiver has a corresponding plurality of group encryption keys, each encryption key can be tested until a CRC without error is provided thereby indicating the service with which the message is associated.

Issued: December 14, 2004

Inventor: David Irvin
Assignee: Ericsson, Inc. (Research Triangle Park, NC)

*Notable Reference:*

[1] Li Gong and Nachum Schacham, *Multicast Security and its Extension to a Mobile Environment*, Wireless Networks, vol. 1, No. 3, Oct. 1, 1995, pp. 281-295.

### US Patent: 6,832,313

***Migration from in-clear to encrypted working over a communications link***

This invention discloses a system involving a central computer and a remote computer, which can communicate over a link, is migrated from in-clear working to encrypted working automatically as the computers receive and install long term keys necessary for encrypted communication. When migration is required, the settings at both ends of the link need to be changed to "encrypt" simultaneously and, particularly, if there are numerous remote computers and the possibility of connection of a remote computer to different central computers, as is possible in virtual private network (VPN) scenarios, severe problems can ensue. Hence, as well as the normal two modes of working "in-clear" and "encrypt", a third mode in which "initiate encryption" is set at one end of the link and "accept encryption" is set at the other end of the link is proposed. This third mode ensures that working in-clear can continue over a particular link, such as between a particular VPN server and a particular gateway PC, until a long term key required for encrypted working is installed at both ends of the link, but that once key installation is complete, only encrypted working is possible over that link.

Issued: December 14, 2004

Inventor: Thomas Parker
Assignee: Fujitsu Services Limited (Slough, GB)

### US Patent: 6,832,251

***Method and apparatus for distributed signal processing among internetworked wireless integrated network sensors (WINS)***

This invention discloses means for a Wireless Integrated Network. Wireless Integrated Network Sensor Next Generation (WINS NG) nodes provide distributed network and Internet access to sensors, controls, and processors that are deeply embedded in equipment, facilities, and the environment. The WINS NG network is a new monitoring and control capability for applications in transportation, manufacturing, health care, environmental monitoring, and safety and security. The WINS NG nodes combine microsensor technology, low power distributed signal processing, low power computation, and low power, low cost wireless and/or wired networking capability in a compact system. The WINS NG networks provide sensing, local control, remote reconfigurability, and embedded intelligent systems in structures, materials, and environments.

Issued: December 14, 2004

Inventor: David Gelvin, *et al*
Assignee: Sensoria Corporation (San Diego, CA)

*Notable References:*

[1] Asada, G., et al. *Wireless Integrated Network Sensors (WINS)*. Proceedings of the SPIE, SPIE, Bellingham, VA 3673:11-18 (1999).

[2] S. Natkunanathan, et al. *A Signal Search Engine for Wireless Integrated Network Sensors.* ASFL Annual Symposium, Mar. 2000, pp. 1-4.

[3] Michael J. Dong, et al. *Low Power Signal Processing Architectures for Network Microsensors.* 1997 International Symposium on Low Power Electronics and Design; Digest of Technical Papers (1997) pp. 173-177.

[4] G. Asada, et al. *Wireless Integrated Network Sensors: Low Power Systems on a Chip*. Proceedings of the 1998 European Solid State Circuits Conference (ESSCIRC), pp. 1-8. The Hague, The Netherlands, Sep. 22-24, 1998.

[5] Gregory J. Pottie, et al. *Wireless Integrated Network Sensors: Towards Low Cost and Robust Self-Organizing Security Networks.* SPIE Conference on Sensors, C3I, Information and Training Tech. for Law Enforcement, Boston, MA. pp. 1-10; Nov. 3-5, 1998.

[6] Tsung-Hsien Lin, et al. *Wireless Integrated Network Sensors (WINS) for Tactical Information Systems.* Rockwell Science Center, Thousand Oaks, Jan. 1998, pp. 1-6.

[7] K. Sohrabi, J. Gao, V. Ailawadhi, G. Pottie. *A Self-Organizing Wireless Sensor Network.* Proc. 37.sup.th Allerton Conf. On Comm., Control, and Computing, Monticello, IL, Sep. 1999.

### US Patent: 6,832,082

***Initialization of handsets in a multi-line wireless phone system for secure communications***

This invention discloses means for a wireless telephone system, having one or more wireless handsets and a base unit. Each handset has a handset transceiver, and the base unit has a base transceiver and a handset docking station, which has a wired interface. The base unit digitally communicates over an RF channel with a handset via its handset transceiver only if the handset has previously been initialized by the base unit. The handset is initialized via the wired interface when it is physically docked in the docking station.

Issued: December 14, 2004

Inventor: Kumar Ramaswamy, *et al*
Assignee: Thomson Licensing S.A. (Boulogne, FR)

### US Patent: 6,831,979

***Cryptographic Accelerator***

This invention discloses means for a cryptographic accelerator for handling instruction-intensive bit permutations. The cryptographic accelerator comprises a selector and a plurality of buses coupled to the selector. Herein, at least one of the plurality of buses includes signal lines routed to perform a bit permutation operation incoming data. The bit permutation operation is one of a plurality of operations associated with a symmetric key function.

Issued: December 14, 2004

Inventor: Roy Callum
Assignee: Intel Corporation (Santa Clara, CA)

## 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