Wireless Security Perspectives

Cellular Networking Perspectives

Technical Editor: Les Owens, Managing Editor: David Crowe Vol. 3, No. 1. January, 2001

Bluetooth: A Global Specification for Wireless Connectivity

"Let all men know empty and worthless is the power of kings. For there is none worthy of the name but God, whom heaven, earth and sea obey."

Many of us are familiar with Canute "the Great" (995? – 1035), the powerful Viking king and imperious ruler of England Denmark and Norway, who said this. Canute was the brutal-turned-wise-and-temperate king from whom many legends come. But, only recently have we heard of his grandfather, Harald Bluetooth, the 10th century Danish Viking credited with bringing the warring factions of Denmark and Norway together.

This month's issue of *Wireless Security Perspectives* covers Bluetooth – the technology named after him. It is an emerging, global, *de facto* standard for connectivity in the burgeoning wireless industry. In this issue, we present a brief technology overview of Bluetooth and provide an introduction to its security features. We do not attempt to provide an assessment of the strength of its security.

Overview of Bluetooth

Bluetooth is a de-facto open standard for short range digital radio. It is touted as a low-cost, low-power, and low-profile technology that provides a mechanism for creating small wireless networks on an ad hoc basis. Bluetooth is considered a personal area network (PAN) technology that offers fast and reliable transmission for both voice and data. Untethered Bluetooth devices will eliminate the need for cables and provide a bridge to existing networks.

According to the leading founders of the technology (Ericsson, Intel, IBM and Nokia), Bluetooth is a standard that will ultimately:

- Eliminate wires and cables between both stationary and mobile devices;
- Facilitate both data and voice communications;
- Offer the possibility of *ad hoc* networks and deliver synchronicity between personal devices; and
- Be competitively priced with alternative wireless data technologies.

Bluetooth is designed to operate in the unlicensed ISM (Industrial, Scientific, Medical applications) band that is available in most parts of the world – with frequency variation in some countries). The characteristics of Bluetooth are summarized in Table 1.

Bluetooth-enabled devices will automatically ("unconsciously") locate each other and form networks. Frequently, the configured networks will comprise only two devices – in what is called a piconet. Devices in a Bluetooth piconet operate on the same channel and follow the same frequency hopping sequence. First generation Bluetooth provides data rates at 1Mbps, with transfer rates up to 2Mbps expected in the next generation.

About *Wireless Security Perspectives*

Price

The basic subscription price for *Wireless Security* Perspectives is $300 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$350 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.

Back issues are available individually, or in bulk at reduced prices.

Our sister bulletin, *Cellular Networking Perspectives*, provides complementary information on wireless standards and technology.

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due…

February 16th, 2000.

Future Topics

More on Bluetooth • IP security • Public Keys & Wireless • Kerberos PKINIT• Public Key Infrastructure (PKI) • IKE • Wireless Data Security • IETF Security Standards • AES (Rijndael)

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: http:/www.cnp-wireless.com/wsp.html. Subscriptions: $300 for delivery in the USA or Canada, US$350 elsewhere. Payment is 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.

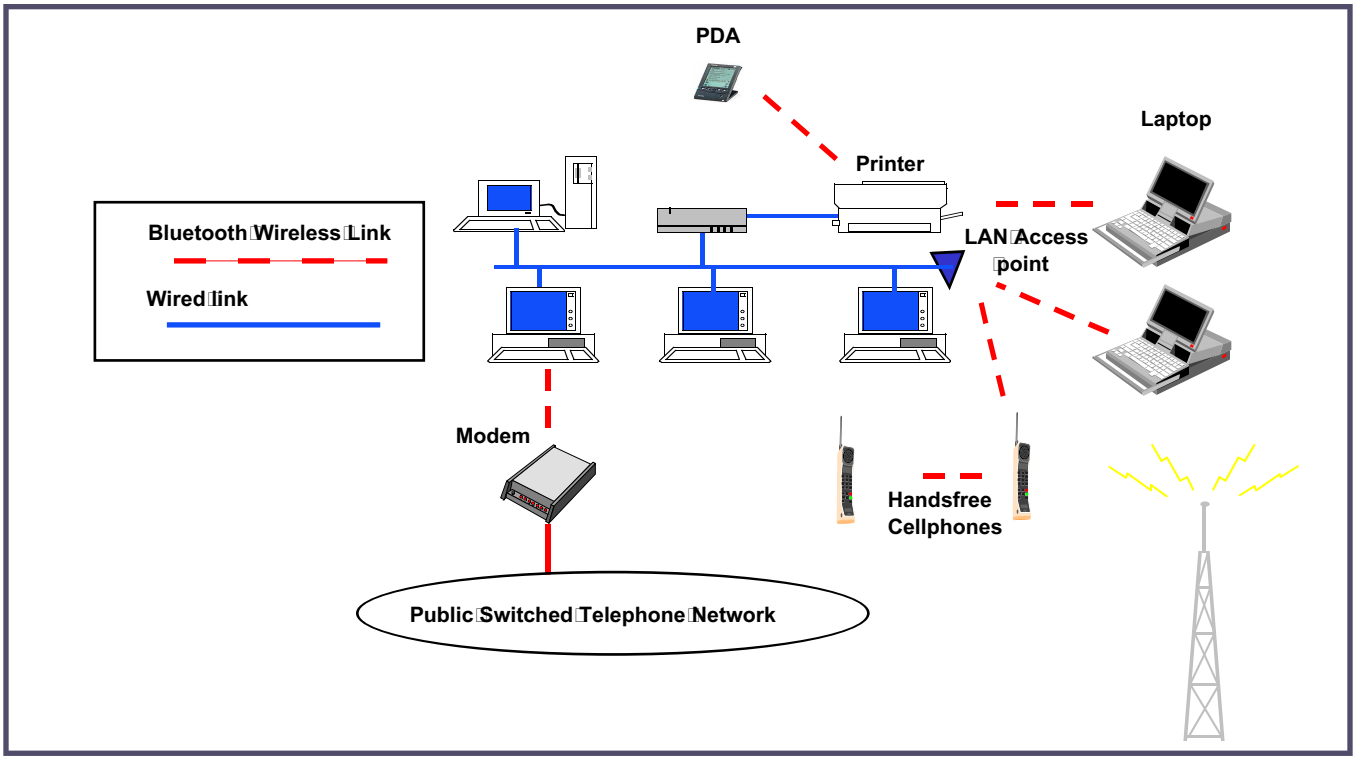
Table 1: Summary of Bluetooth Characteristics

Characteristic	Specification
Physical Layer	Frequency hopping Spread Spectrum (FHSS)
Frequency Band	2.4 - 2.45GHz (ISM Band)
Hop Frequency	1600 hops/ sec
Transmit Power	0 dBm (United States), 100 mW (worldwide)
Data Rates	1 Mbps (gross rate)
Modulation Scheme	Shaped, binary FM
Multiple Device Support	Up to 8 active devices on each Piconet
Operating Range	10m, extends to 100m with more power

Standardization

Bluetooth, originally developed by Ericsson in 1998, is now being standardized within the IEEE 802.15 Personal Area Network (PAN) Working Group that formed in early 1999. Today more than 2,000 organizations are part of the Bluetooth Special Interest Group (SIG) that has since formed. The SIG comprises leaders in the telecommunications and computing industries who are driving development and promotion of Bluetooth technology. These companies have plans to develop a broad-range of Bluetooth-enabled consumer devices to enhance wireless connectivity. Among those anticipated this year are cellular phones, PDAs, notebook computers, modems, cordless phones, pagers, laptop computers, cameras, PC cards, fax machines, and printers. A typical Bluetooth network is shown in Figure 1.

Figure 1: Typical Bluetooth Network



Bluetooth's Competition

Bluetooth is far from the only protocol attempting to provide wireless local area networking. Others are:

- IRDA, an infra-red communications protocol that can transmit data up to 4 Mbps, but is limited to very short distances and line-of-sight communications. See www.irda.org.
- HomeRF is designed to provide communications among home appliances, support voice and video. It provides for speeds up to 10 Mbps, also in the ISM band. See www.homerf.org.
- 802.11 is a wireless LAN protocol that provides data-only communications between computers at 10 Mbps. See:

  grouper.ieee.org/groups/802/11/main.html

Bluetooth is obviously not the highest performance local area wireless proto-

col, but it has been designed to be one of the cheapest. It is hoped that this will encourage its incorporation in low cost devices (such as computer mice) for which other protocols will simply be too expensive, and it does provide good integration of voice and data, and is not restricted to line-of-sight communications.

Overview of Bluetooth Security

Bluetooth will enable many types of devices to "go wireless." As with all wireless technologies that replace cable connections by radio signals, Bluetooth requires built-in security features to prevent unauthorized disclosure of information and usage of the devices. Provisions must exist to thwart eavesdropping attempts (through encryption) and impersonation of a legitimate message originator (through authentication security services).

Bluetooth provides some security due to its frequency-hopping scheme with 1,600 hops per second combined with a limited transmission range of about 10 meters. These characteristics provide Bluetooth with additional protection from eavesdropping and malicious access.

The frequency-hopping scheme makes it difficult for an adversary to locate the Bluetooth transmission. The power control, or range limitation of about 30 feet, require that an adversary be in relatively close proximity to pose a threat to the system.

In summary, the security features provided by Bluetooth are:

- Frequency-hopping Scheme;
- Radio link power control;
- A "challenge-response" authentication scheme; and
- Stream Cipher Encryption.

The encryption and authentication security features are discussed in more detail in the following section.

Upcoming Security Conferences – What's Happening?

Entrust Secure Summit 2001
January 22-25, 2001
San Diego, CA
www.entrust.com

Optimizing Wireless e-Commerce Security
January 23-26, 2001
London
www.iir-telecoms.com

SANS 2001
January 28- February 2, 2001
New Orleans
www.sans.org/NO2001.htm

Black Hat Briefings Win 2K Security
February 13-15, 2001
San Francisco, CA
www.blackhat.com

eSecurity Conference & Exposition
March 26-27, 2001
Boston
www.intmedgrp.com/security

Information Security Managers Symposium
March 27-29, 2001
San Diego, CA
www.misti.com

RSA Conference 2001
April 8-12, 2001
San Francisco, CA
www.rsa.com

Security of Bluetooth – Under the Hood

Bluetooth technology provides three levels of security:

1. A non-secure mode;
2. A service-level security mode; and
3. A less sophisticated, link-level security mode.

Non-Secure Mode

In the non-secure mode, a device will not initiate any security procedures. In this mode, the authentication and encryption functionality is completely bypassed. This mode is provided for applications for which security is not required, such as exchanging business cards.

Service-Level Security Mode

In the Service-level security mode, security procedures are initiated after channel establishment at the Logical Link and Adaptation Protocol (L2CAP) level. L2CAP resides in the data link layer and provides connection-oriented and connectionless data services to upper layers. For this security mode within L2CAP, a Security Manager is introduced to control access to services and to units. The centralized Security Manager, as specified in the architecture, maintains polices for access control and interfaces with other protocols and device users. Varying security polices and "trust" levels, to restrict access, may be defined for applications with different security requirements operating in parallel. Therefore, it is possible to grant access to some services without providing access to other services. Obviously, in this mode, the notion of authorization is introduced – the process of deciding if device A is allowed to have access to services Z. This security mode will be described in a future issue of *Wireless Security Perspectives*.

Link-Level Security Mode

In the Link-level security mode, an authentication procedure in the form of a "challenge response" scheme is provided. Two devices interacting in an authentication procedure are referred to as the Claimant and the Verifier. The Verifier is the Bluetooth device validating the identity of another device. The Claimant is the device attempting to prove its identity.

The Bluetooth device verification scheme involves the following steps:

1. The Claimant transmits its 48-bit address to the Verifier.
2. The Verifier transmits a 128-bit random challenge to the Claimant.

3. The Verifier uses a hash algorithm to compute an authentication response using the address, link key, and random challenge as inputs. The Claimant performs the same computation.
4. The Claimant returns the computed response, SRES, to the Verifier.
5. The Verifier compares the SRES from the Claimant with the SRES that it computes.
6. If the two 32-bit SRES values are equivalent, the Verifier will continue connection establishment.

The Bluetooth standard allows both unidirectional and mutual-authentication to be performed.

The hash algorithm (or function) used for the authentication processing is based on the SAFER+ algorithm. This is one of a family of algorithms developed by James Massey and used in Cylink Corporation products. SAFER stands for Secure and Fast Encryption Routine, and the algorithms are based on iterated block ciphers (IBC), where the same cryptographic function is applied for a specified number of rounds.

Security Parameters

The Bluetooth address is a public parameter that is unique to each device. This address can be obtained through a device inquiry process.

The private key, or link key, is a secret entity. The link key is derived during initialization and is never disclosed outside the Bluetooth device and is never transmitted over the air-interface.

The random challenge, obviously a public parameter, is designed to be different on every transaction. The random number is derived from a pseudo-random process within the Bluetooth device.

The cryptographic response (SRES) is public as well. With knowledge of the challenge and response parameters, it should be impossible to predict the next challenge or derive the link key.

Authentication

The parameters used in the authentication procedure are summarized in Table 2 below:

Table 2: Summary of Authentication Parameters

Parameter	Length	Secrecy Characteristic
Device Address	48-bits	Public
Random challenge	128-bits	Public, Non-deterministic
Authentication Response (SRES)	32-bits	Public
Link key	128-bits	Secret

The simple Bluetooth "challenge-response" procedure is shown in Figure 2. This procedure is similar to the CAVE-based authentication scheme currently used in cellular/PCS systems connected to ANSI-41 networks. Some of the security weaknesses identified in [6], may apply to the Bluetooth implementations. However, the power control and frequency-hopping system reduce this risk of compromise. It is important to note that a complete analysis of the Bluetooth environment and the assets at stake are required before a definitive assessment can be made of the security risk.

In addition to the authentication scheme, Bluetooth provides for a confidentiality security service to thwart eavesdropping attempts on the air-interface. The encryption provided in this service is depicted in Figure3.

Encryption

As shown in Figure 3, the Bluetooth encryption procedure is based on a stream cipher. A keystream output is exclusive-ORed with the payload bits and sent to the receiving device. This keystream is produced using a hash algorithm based on linear feedback shift registers (LFSR). The hash function takes as inputs the master identity, the random number (EN_RAND), a slot number, and an encryption key which initialize the LFSRs before the transmission of each packet, if encryption is enabled. Since the slot number used in the stream cipher changes with each packet, the ciphering engine is also re-initialized with each packet even though the other variables remain static.

The encryption key provided to the encryption hash function is produced using an internal KG (key generator). This key generator produces stream cipher keys based on the link key, random number (EN_RAND again) and the ACO value. The ACO parameter, a 96-bit authenticated cipher offset, is another output produced during the authentication procedure of Figure 2. As mentioned above, the link key is the 128-bit secret key that is held in the Bluetooth devices and is not accessible to the user. Moreover, this critical security element is never transmitted outside the Bluetooth device.

The link key is generated during an initialization phase during which time, two Bluetooth devices that must communicate are "associated." According to the Bluetooth specification, two associated devices simultaneously derive link keys during the initialization phase when a user (or users) enters the same PIN (personal identification number) into both devices. After initialization is complete, devices automatically and transparently authenticate and perform encryption of the link.

Based on this discussion, it is obvious that the number of pair-wise link keys is of the order N^2 for N communicating Bluetooth devices in a piconet (actually, [N x (N-1) / 2]). The Bluetooth specification provides means to share link keys and otherwise reduce the total number of keys required in certain instances.

To be continued…

If Bluetooth has a price/performance equation that brings commercial success,

Figure 2: Bluetooth Authentication Procedure

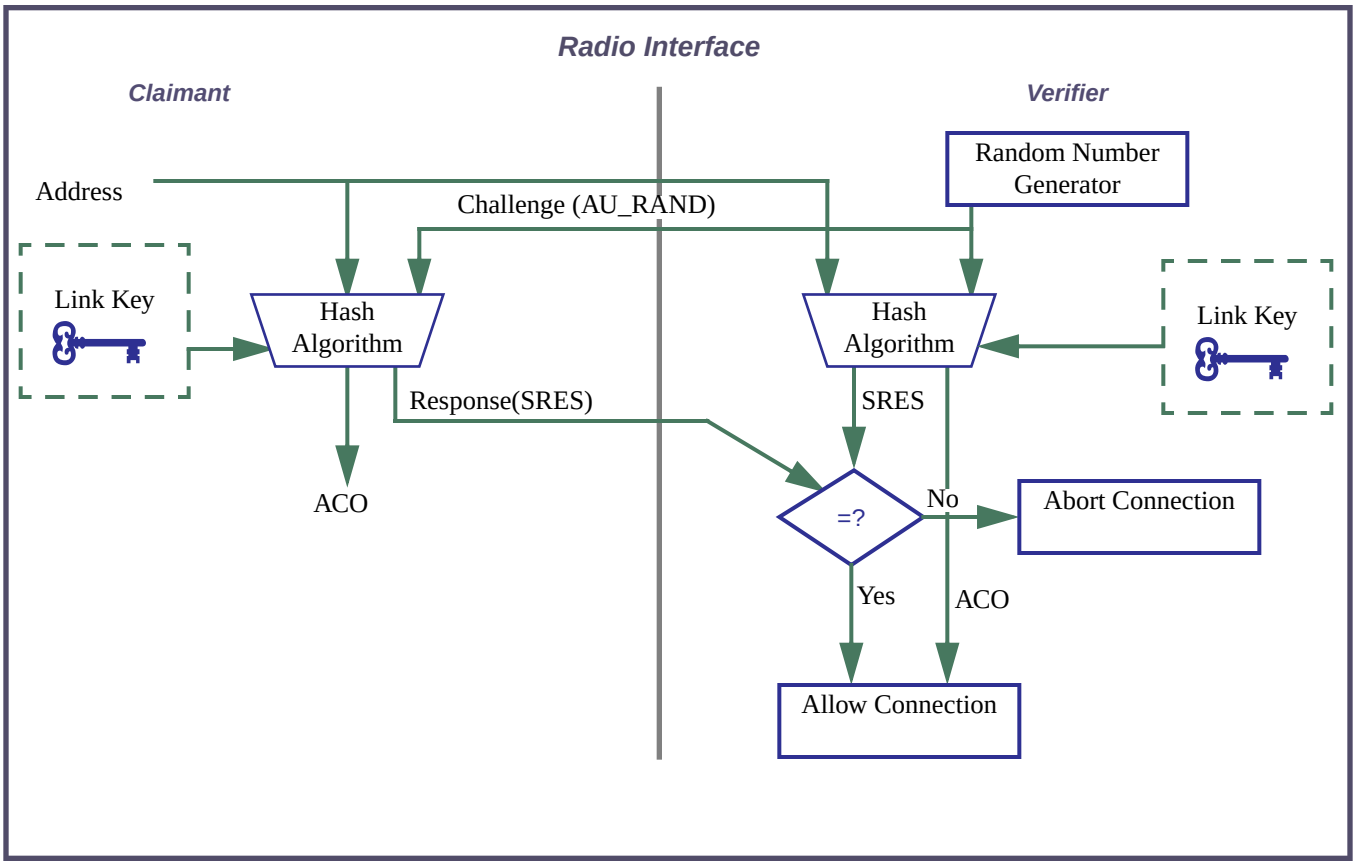
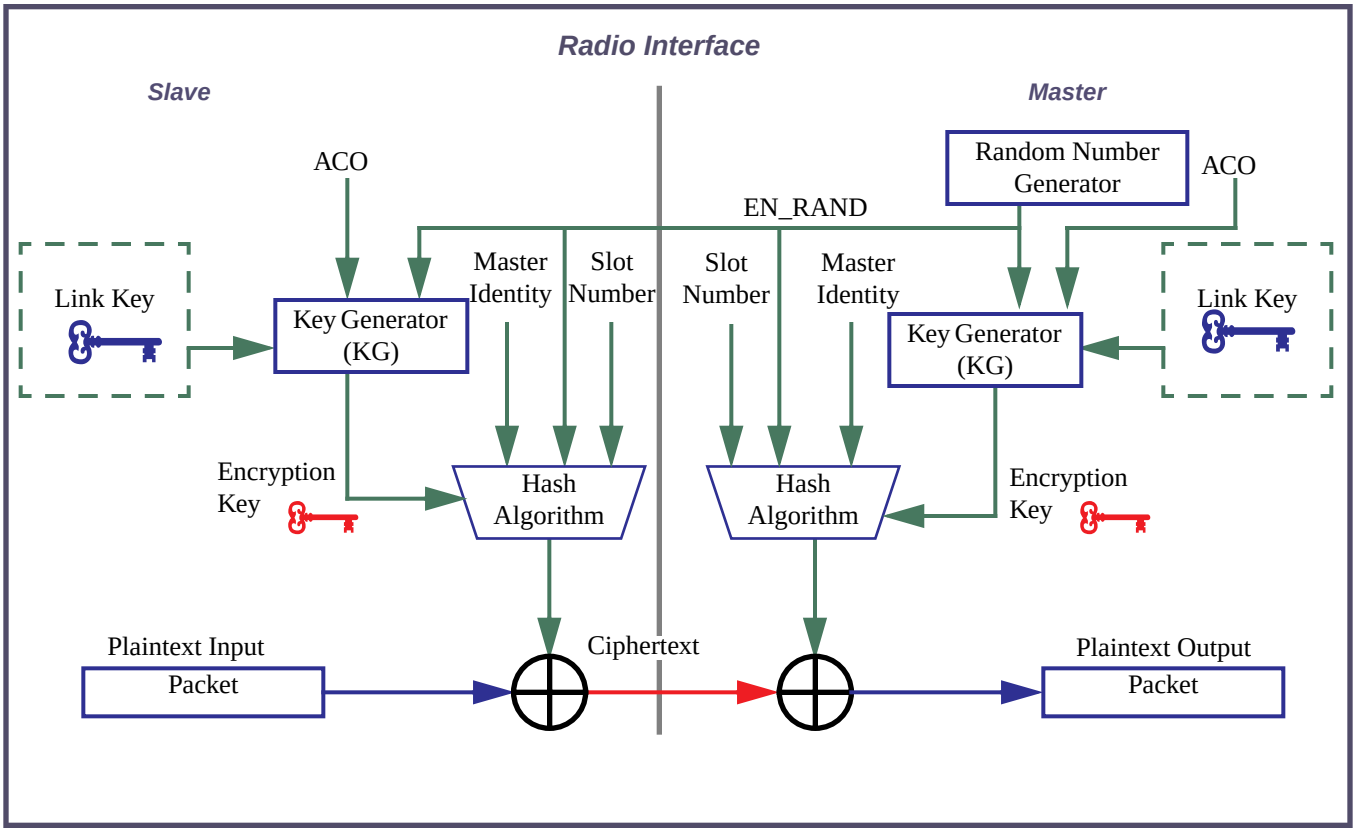


Figure 3: Simplified Bluetooth Encryption Procedure



it may bring freedom from wires and introduce a whole new way of communicating.

In future issues we will discuss a variety of applications of Bluetooth, and their security implications, Service Level Security and will also provide an extensive list of Bluetooth resources.

Selected References

[1]. AU-System, *Bluetooth White Paper 1.1*., January 2000.

[2]. Haartsen, Jaap. *The Bluetooth Radio System*, IEEE Personal Communications, pp. 28 - 36, February 2000.

[3]. Siep, Thomas et. al. *Paving the Way for Personal Area Network Standards: An Overview of the IEEE P802.15 Working Group for Wireless Personal Area Networks*, IEEE Personal Communications, pp. 37 - 43, February 2000.

[4]. Muller, Thomas. *Bluetooth Security Architecture v1.1*, January 2000.

[5]. Schneiderman, Ron. *Bluetooth's Slow dawn*, IEEE Spectrum pp. 61 - 65, November 2000.

[6]. Patel, Sarvar. *Weaknesses of North American Wireless Authentication Protocol*, IEEE Personal Communications, pp. 41 - 44, June 1997.

[7]. Menezes, Alfred et. Al. *A handbook of Applied Cryptography*, New York: CRC Press, 1997.

Fraud And Security Patent News

The following 10 fraud and security patents were issued by the US Patent and Trademark Office (USPTO) since October 2000. They are primarily concerned with fraud and security of wireless communications.

Patent Number: 6,173,174

Title: Method and apparatus for automated SSD updates on an A-key entry in a mobile telephone system

Inventor: Pamela Jacobs

Assignee: Compaq Computer Corp.

Date Granted: 9 January 2001

Patent Number: 6,173,173

Title: Invalid mobile telephone call terminating system and method

Inventor: Lauran Dean, David Jones, and Michael Marcovici

Assignee: Lucent Technologies, Inc.

Date Granted: 9 January 2000

Patent Number: 6,157,825

Title: Cellular telephone anti-fraud system

Inventor: Max Frederick

Assignee: Corsair Communications, Inc.

Date Granted: 5 December 2000

Patent Number: 6,167,251

Title: Keyless portable cellular phone system having remote voice recognition

Inventor: Edna Segal and Alon Segal

Assignee: Telespree Communications

Date Granted: 26 December 2000

Patent Number: 6,163,604

Title: Automated fraud management in transaction-based networks

Inventor: Donald Baulier, Michael Cahill, Virginia Ferrara, and Diane Lambert

Assignee: Lucent Technologies, Inc.

Date Granted: 9 January 2000

Patent Number: 6,161,006

Title: System and method for the early detection of cellular telephone piracy

Inventor: Shridharan Balachandran

Assignee: Ericsson, Inc.

Date Granted: 12 December 2000

Patent Number: 6,157,826

Title: Authentication key generation method and apparatus

Inventor: Jae Lee

Assignee: Daewoo Telecom Ltd.

Date Granted: 5 December 2000

Patent Number: 6,157,823

Title: Security cellular telecommunications system

Inventor: Douglas Fougnies and Dan Harned

Assignee: Freedom Wireless, Inc.

Date Granted: 5 December 2000

Patent Number: 6,154,727

Title: Visit verification

Inventor: Edward Karp et. Al.

Assignee: CyberHealth

Date Granted: 18 November 2000

Patent Number: 6,144,859

Title: Wireless cellular communicator system and apparatus

Inventor: Christoph LaDue

Assignee: Aeris Communications, Inc.

Date Granted: 7 November 2000

Patent Number: H1,918

Title: Integrated authentication center and method for authentication in a wireless telecommunications network

Inventor: Scott Hoffpauir and Steve Liao

Assignee: DSC / Celcore, Inc [Alcatel].

Date Granted: 7 November 2000

Patent Number: 6,141,406

Title: Method and apparatus for detecting a secondary destination of a telephone call based on changes in the telephone signal path

Inventor: John Johnson

Assignee: T-Netix Inc.

Date Granted: 31 October 2000

To review the specification and claims of these patents visit the US Patent and Trademark Office web-site at www.uspto.gov. To obtain a copy of one of these patent number from the US Patent and Trademark Office at the address or telephone numbers below:

General Information Services
U.S. Patent and Trademark Office
Crystal Plaza 3, Room 2C02
Washington, DC 20231

Phone: 800-786-9199 or
+1-703-308-4357