Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 4, No. 2. February, 2002

The ISTPA Privacy Framework in Wireless Environments

John Sabo (Computer Associates)
Michael Willett (Wave Systems)
Michele Drgon (Motorola)
Rick Noens (Motorola)

Introduction

Privacy is sometimes used synonymously with data confidentiality – although they are related, they are really different terms. Data confidentiality is best defined as a security service that protects data against unauthorized disclosure. Privacy is a broader term. We define it as:

> *The proper handling of personal information (PI) consistent with the preferences of the subject.*

A technical framework is needed for the protection of personal information. Historically, it has been treated mostly as a policy issue. Until very recently, little objective research and analysis has occurred on IT-based standards, technical mechanisms or products needed to support those policies.

The Framework Project of the ISTPA (International Security, Trust & Privacy Alliance – www.istpa.org) is developing and promoting an objective framework for achieving security, privacy, integrity, and trust in *all* forms of communications worldwide and it must be applicable to *all* forms of technical and operational infrastructure. Emerging m-commerce business models have exposed technology and operational-based privacy challenges which are distinct from more familiar web and traditional IT issues.

Fair Information Practices have been articulated to describe specific actions necessary to support privacy, including:

- notice and awareness;
- choice and consent;
- access (by the subject of the personal information);
- information quality and integrity;
- update and correction; and
- enforcement and recourse.

> *This is a free country, madam. We have a right to share your privacy in a public place.*
>
> – Peter Ustinov, Romanoff and Juliet (1956)

The ISTPA Privacy Framework Services

The "Fair Information Practices" serve as high-level design points for an embodiment of the proper handling of personal information.

The subject of personal information (e.g., the user of a wireless data device) can agree to various permissible actions that can be applied to the personal information, such as transferring and sharing. A binding mechanism is needed between personal information and

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.

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:

cnpaccts@cnp-wireless.com

Next Issue Due…

March 18th, 2002.

Future Topics

Radius for Wireless • IP Security • Public Keys & Wireless • Security Issues in Ad hoc Wireless Networks • Latest in Watermarking • 3G Security • Blackberry • Security for PDAs • SMS 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**: $300 for delivery in the USA or Canada, US$350 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: Betsy Harter.
Production: Doug Scofield.
Distribution: Debbie Brandelli.
Marketing: Muneerah Vasanji.
Accounts: Evelyn Goreham.
Publisher: David Crowe.

Upcoming Fraud and Security Events

The following upcoming wireless and security conferences may be of interest to our wireless and network security practitioners.

SANS Tysons Corner ISO (Information Security Officer)
3rd – 7th March 2002
Sheraton Premiere at Tysons Corner
Vienna, VA
www.sans.org/TysonsCorner

Instant Messaging Planet Conference and Expo – Spring 2002
7th– 8th March 2002
Omni Parker House
Boston, MA
seminars.internet.com/im/spring02/index.html

Defending Against Information Warfare
12nd– 13th March 2002
Sheraton Crystal City
Arlington, VA
www.srinstitute.com/ck113

Third International System Security Engineering Association Conference
13th– 15th March 2002
Caribe Royale Resort Suites
Orlando, FL
www.issea.org/confs.html

InfoSec World Conference and Expo/2002
18th– 20th March 2002
Disney's Coronado Springs Resort
Orlando, FL
www.misti.com

CTIA Wireless 2002
18th– 20th March 2002
Orange County Convention Center
Orlando, FL
wireless2002.ctsg.com

Note: This event is co-located with *WCNC 2002*

subject permissions. One of the conceptual implications of the transfer or sharing of personal information is a Personal Information Container (PIC) that includes the contract or agreement between the data collector and data subject, as well as the credentials for the subject, held together by the binding mechanism. The *Services Framework* – defined as the collection, processing, storage and ultimate destruction of personal information – requires a life cycle management process. The PIC allows subsequent actions to be based on the agreed-to consumer preferences.

The ISTPA Privacy Framework provides a set of nine privacy services. A *"Service"* is defined as a logically related collection of operational activities. A system designer should be able to integrate them into a functional architecture. The Framework Privacy Services are:

Agent Service. A software process acting on behalf of a data subject or a requestor (as a persona) to engage with one or more of the other Services defined in this Framework.

Audit Service. The recording and maintenance of events in any Service to capture the data necessary to ensure compliance with the terms and policies of an agreement and any applicable regulations.

Certification Service. Validation of the credentials of any party processing personal information.

Control Service. The *repository gatekeeper* that ensures access to personal information stored by a data collection entity complies with the terms and policies of an agreement and any applicable regulations. Control must faithfully enforce privacy policy.

Enforcement Service. Provides redress when a data collection entity is not in conformance with the terms and policies of an agreement and applicable regulations.

Interaction Service. Provides:

- Presentation of proposed agreements from a data collection entity to a data subject;
- Input of the subject's personal information, preferences, and actions; and
- Confirmation of actions.

To the extent the data subject is represented by an Agent, this Service comprises the interface to the Agent.

Negotiation Service. Arbitrates a proposal between a data collection entity and a data subject. Successful negotiation results in an agreement.

Usage Service. The *process monitor* that ensures active use of personal information outside of the Control Service complies

More Conferences . . .

WCNC 2002 (IEEE Wireless Communications and Networking Conference)
18th– 20th March 2002
Orange County Convention Center
Orlando, FL
www.wcnc.org/2002

Note: This event is co-located with *CTIA Wireless 2002*

Information Security in the Age of Terrorism
25th– 26th March 2002
American Management Association
Washington, DC
www.frallc.com

The Information Security Conference
16th– 18th April 2002
McCormick Place
Chicago, IL
www.dci.com/brochure/secchi

Internet World Spring 2002
22nd– 26th April 2002
Convention Center
Los Angeles, CA
www.internetworld.com/events/spring2002

Enterprise Wireless Forum Conference & Expo
29th April – 1st May 2002
Convention Center
Santa Clara, CA
www.imgevents.com

3rd International SANE Conference
27th– 31st May 2002
MECC
Maastricht, The Netherlands
www.nluug.nl/events/sane2002

with the terms and policies of an agreement and applicable regulations.

Validation Service. Checks for correctness of personal information at any point in its life cycle.

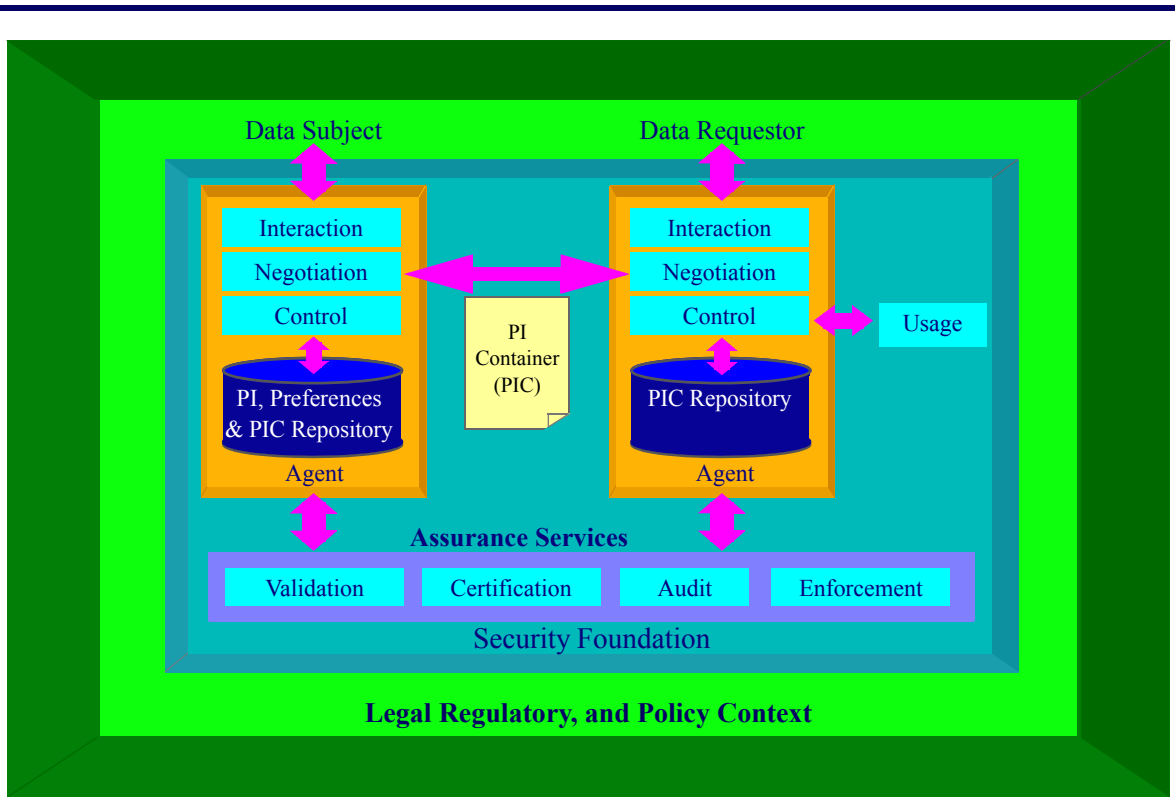
The Privacy Services are shown pictorially in Figure 1.

Typical Configuration

Consider a typical configuration of the Privacy Services, with an Agent Service representing both the Subject and the Data Requestor. Interaction, Negotiation, and Control Services provide a front-end to the secure data repository. The Assurance Services of Validation, Certification, Audit, and Enforcement support both subject and requestor nodes, whereas Usage supports the Data Requestor. It is assumed that security functions are available to all the Privacy Services. The Legal, Regulatory, and Policy Context provide the necessary configuration and parameterization layer.

Note: The ISTPA Privacy Framework empowers a user (subject entity) to exercise strong control over use of their personal information. Trust in the overall system is balanced between the requestors and the subject/users at the edge of the network.

Figure 1: Privacy Services



Privacy Challenges in Wireless Environments

The wireless environment presents additional challenges related to privacy – enhanced, expanded or both. These are created because the user's device is portable, capable of continuous communications and is highly mobile. We focus on six challenges:

- Location Profiling;
- Client Restrictions;
- Client Control;
- Multiple Networks;
- Service Misuse/Multiple Users; and
- Application Policy Granularity.

The ISTPA Privacy Framework in a Wireless Context

For each of the six wireless privacy challenges of a wireless environment we provide a roadmap for developing a more detailed adaptation of the Framework to wireless network infrastructures.

Each of the Privacy Services (and security functions) helps resolve all of the wireless challenges to some degree, but some are more significant to a given challenge. The following sections will describe some of the implications to the Framework Services in the context of the wireless challenges.

Location Profiling

Wireless architectures are increasingly being upgraded with the ability to pinpoint device location. The ability to track someone has obvious privacy implications. It can be an invasion of privacy unless pre-approved by the subject or by laws or regulations, such as the emergency 911 (E911) Phase II positioning service in the United States.

Many services can be implemented with the use of location services, such as intelligent directory assistance and roadside service. Often the user may not be aware that their location is being obtained. And for some services, the client obtaining the location is not the wireless device being pinpointed.

Framework Implications:

Interaction – The Interaction Service deals with all subject dialogue into and out of the Framework structure, including the vicarious dialog to support the Global Positioning System (GPS) or phone cell positioning. Interaction may not always explicitly involve the subject, but it must engage the subject's permission capabilities in the Framework.

Control – The Agent Service will lodge the subject preferences for location profiling with the Control Service. In turn, Control will enforce the subject preferences for the sharing of location information, subject to jurisdictional or legal policies. In the case of location, the act of sharing may be allowed (or denied) by enabling mechanisms in the wireless device or the roaming infrastructure that supports positioning. The heart of the Control Service is a comprehensive privacy policy and subject preferences covering all options.

Usage – If the subject's preferences or negotiated permissions for location profiling allow selective and subsequent access to location information, then it is critical that the Usage Service faithfully enforce the use of such information.

Client Restrictions

The wireless client – for example, a wireless phone, as depicted in Figure 2 – has limited processor power, memory, display size, display clarity and input capabilities. Devices are also usually battery powered. By comparison, a typical client in the wired world is a PC with a display capable of rendering large amounts of information and a CPU and memory far exceeding the requirements to implement most software.

These restrictions on the wireless client tend to make privacy-related software and the human interface a challenge. A privacy agent acting on the user's behalf might have difficulties operating in the wireless client environment, and most certainly, it would have challenges interfacing with the user.

The ISTPA Framework was designed to adjust to these restrictions.

Figure 2: Privacy Constraints on Wireless Devices

The front-end Framework Services of Interaction, Agent, and Control are most impacted by client restrictions. For example, just as the subject interface (Interaction) for mobile applications limits the amount and manner of information exchange for applications, so too are the dialogs concerning personal information limited. The Framework implementation may allow pre-configuration of subject preferences and policies through other channels. The display of website privacy policies will require the simplification and shortening of such policies or the creation of policy symbolism easily understood by the consumer. Choices for opt-in and opt-out will need to be easily communicated.

Framework Implications:

Interaction – The design of the Privacy Interaction Service will be influenced by the design of the Agent and Control structures. A special and easily-understood symbolism for privacy dialog is needed in restricted environments, as is a general transaction grammar. Opt-in and opt-out choices should have a simple encoding.

Agent – Given the memory and computing limitations of some mobile and wireless devices, Agent/Control may need to be split between the device and a central, secure repository (for example, collocated with the wireless gateway, such as the WAP server, as shown in Figure 4). Placing the subject privacy preferences and governing policies on the "wired" side of wireless and mobile communications has advantages in terms of requestor access, but the subject preferences must be faithfully enforced, even with remote Control.

Client Control

Wireless clients are not always controlled by a user. Some may be controlled by devices that may not even be acting on behalf of the user. If a device is in control of the wireless client, even if it is with the express or implicit permission of the user, privacy concerns surface.

While an entity other than the user is controlling the client, the potential exists for information to be divulged which could violate user privacy rights.

Framework Implications:

Control – Since the subject is not always consciously involved in the collection of personal information, the Control Service is paramount for faithfully enforcing the subject preferences, whether local, remote, or split.

Usage – The use of any personal information that is acquired must be governed and managed by the Usage Service. Even though the subject may not be actively engaged, the Agent function will still represent the interests of the subject, and the Control Service will dictate and enforce the subject preferences to and through the Usage Service.

Certification – Given the level of indirection and detachment between the subject and the requestor, proper validation of requestor credentials is vital.

Multiple Networks

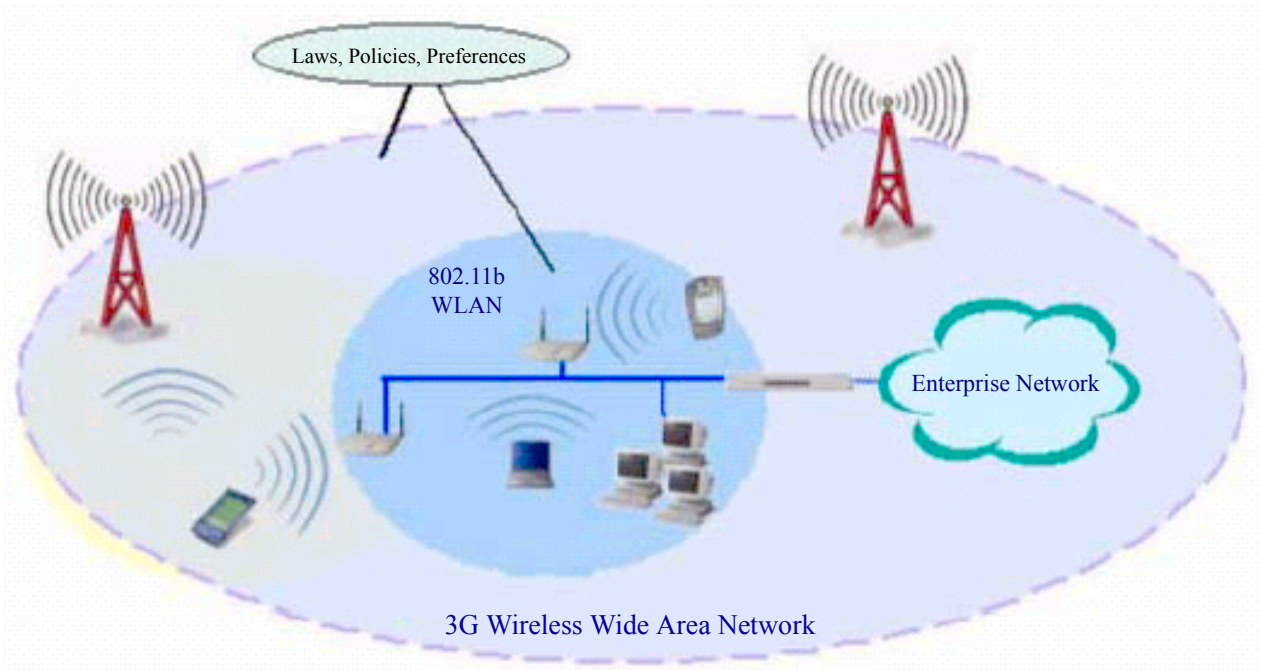
Unlike fixed, wired devices, mobile wireless devices may roam across multiple networks, possibly representing multiple jurisdictions that may have differing privacy policies and governing procedures. For example, users may soon be able to roam from an 802.11b wireless LAN environment into a wide-area 3G cellular environment, as illustrated in Figure 3. Even when a user travels into wireless coverage areas other than that provided by his home carrier, his privacy must still be managed in a consistent manner, and one that is acceptable to the user.

Framework Implications:

Control – The fact that wireless devices roam across multiple networks and even jurisdictions places a specific challenge on the Control Service. Laws or privacy policies. Even the subject's personal preferences may change across such boundaries. Whether physically centralized or distributed, Control must always be enabled to enforce and exercise the right parameters. Most importantly, Control must know the whereabouts of the roaming device, in order to invoke the appropriate action from among the composite policy.

Negotiation – Since the protocol and format for negotiating permissions with the subject may vary across networks, the Negotiation Service and the associated grammars must span the networks.

Figure 3: Privacy Challenges in Wireless Roaming



Service Misuse/ Multi-User

This challenge is partly defined as the theft and misuse of someone's identity for the purpose of stealing wireless access ('airtime'), but it also includes situations when multiple users share a single wireless device. This multiple-user scenario complicates the problem of misuse of service, as we cannot assume that if the owner is not using the device, it is being misused.

Unauthorized use of wireless services – whether in violation of legal, policy, or preference constraints – will invoke the back-end Privacy Services, as will the challenge of multiple users of the same wireless device.

Framework Implications:

Certification – The first defense is the checking of identity and credentials of personal information requestors by the Certification Service.

Audit – All other Privacy Services in the life cycle of personal information, from Interaction/Agent through Control to Usage, are configured to monitor and report violations through the Audit Service. The monitoring function may consist of threshold detectors and triggers placed throughout the Framework infra-structure.

Enforcement – Actions that exceed the misuse/multi-user guidelines of the policy are reported to the Enforcement Service, which can be configured for a variety of reactions, from internal notification to external contact of the proper authorities.

Application Policy Granularity

Historically, privacy preferences have been thought of as constant for a given user. The service provider would provide a suite of applications with a constant level of privacy protection for all the applications offered. In reality, the user may desire different levels of privacy protection, depending on the application. For example, a medical application may require more intimate details from the subject than a banking application.

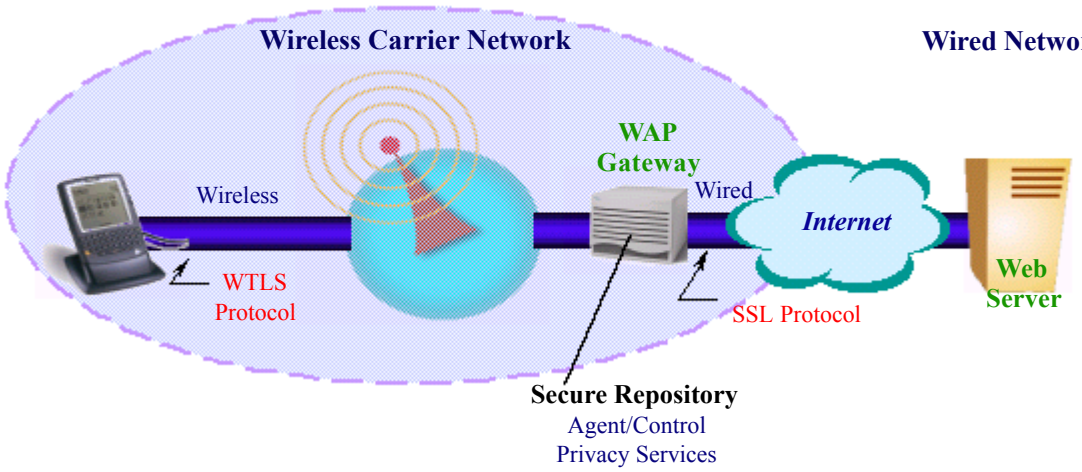
Framework Implications:

Control – Control must be application-sensitive and able to switch dynamically as the subject changes applications.

Usage – Use of personal information must be governed by the original agreed-to permissions of the subject, which were in turn set in an application-specific context.

Validation – Since privacy policy and user preferences can vary with the application, the correctness of the granular personal information should be checked by the Validation Service.

Figure 4: Potential Privacy Architecture with Wireless Application Protocol (WAP)



Summary

Over the years, a large body of technology has been developed to tackle the security challenges of information systems. In the same timeframe, high-level practices have evolved to address personal privacy issues, but very little privacy-related technology has appeared.

The International Security, Trust, and Privacy Alliance (ISTPA) is chartered to define a Privacy Framework providing an operational template for implementing the privacy *"Fair Information Practices."* The resulting Framework consists of nine operational Privacy Services: Interaction, Agent, Control, Negotiation, Usage, Validation, Certification, Audit, and Enforcement.

The wireless and mobile environment offers a number of challenges to personal privacy, some of which are not as novel or challenging in the wired world. These challenges include: Location Profiling, Client Restrictions, Client Control, Service Misuse/Multi-User, Multiple Networks, and Application Policy Granularity.

By choosing specific technologies and appropriate system configurations, the ISTPA Privacy Framework can provide an operational template for implementing the privacy *"Fair Information Practices"* in wireless domains.

To Probe Further

The International Security, Trust, and Privacy Alliance is a global alliance of companies and technology providers working together to provide unbiased research and evaluation of privacy standards, tools, and technologies. The ISTPA has a primary focus on the privacy and protection of personal information (PI).

To learn more about ISTPA and the Privacy Framework discussed herein, visit the ISTPA web-site at

www.istpa.org

You may contact contributors to ISTPA and the authors of this feature article at:

John Sabo (Computer Associates):

John.T.Sabo@ca.com

Michael Willett (Wave Systems):

mwillett@wavesys.com

Michele Drgon (Motorola):

Michele.Drgon@motorola.com

Rick Noens (Motorola):

Rick.Noens@motorola.com

Last, an expanded version of this paper will appear in an upcoming IEEE special issue on wireless security.

IETF Insights

Rindjael in Action

As mentioned in a recent issue of *Wireless Security Perspectives*, the NIST (National Institute of Standards and Technology) has, after a four year process, selected the AES (Advanced Encryption Standard), the successor to the venerable DES. The AES, formerly known as Rijndael, was selected from a field of candidates on the basis of several characteristics, including:

- computational efficiency,
- memory requirements on a variety of software and hardware (including smart cards),
- flexibility,
- simplicity, and
- ease of implementation

The AES is now the US government's designated encryption cipher. Its description is in FIPS 197 (Federal Information Processing Standard). It is expected to be widely adopted by businesses and financial institutions.

The IETF (Internet Engineering Task Force) has recently produced an Internet Draft, titled, "The AES Cipher Algorithm and Its Use With IPsec." It describes the use of the AES Cipher Algorithm in Cipher Block Chaining (CBC) Mode, as a confidentiality mechanism within IPSec. IPSec is the security protocol suite at the foundation of Virtual Private Networks (VPNs) – both wireless and wired. The IETF IPsec Working Group plans for AES to eventually be adopted as the default IPsec encryption algorithm. After its adoption, it will be a required part of any compliant IPsec implementation.

Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working Groups. Other groups may also distribute working documents as Internet Drafts. Internet-Drafts are "works-in-progress" documents that are valid for a maximum of six months. They may be updated, replaced, or obsoleted by other documents at any time.

To obtain the draft on the use of AES for IPSec, click on:

search.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-aes-cbc-03.txt

For information on how the AES will be used elsewhere within the IETF, click on:

csrc.nist.gov/encryption/aes/rijndael/misc/nissc3.pdf

To obtain a copy of FIPS197, the AES specification, click on:

csrc.nist.gov/publications/fips/fips197/fips-197.pdf

MobileIP Security

MobileIP is a proposed standard protocol that builds on the Internet Protocol by making mobility transparent to applications and high-level protocols. MobileIP will eventually allow the seamless roaming of IP-based cellular phones, PDAs, and other handheld wireless devices. Because of concerns about the secure connectivity and scalability of the associated IPSEC processing needed to make network connections truly secure, an Internet draft has been developed. The Internet draft specifies a security "threat model" to allow identification of the security requirements in the MobileIP environment. This ID describes security threats against the MIP v6 protocol and the requirements for a security solution to thwart these threats in environments where it is likely to be deployed.

To obtain a copy of the ID on MobileIP security, click on:

search.ietf.org/internet-drafts/draft-team-mobileip-mipv6-sec-reqts-00.txt

To obtain a copy of the seminar RFC on IP mobility (RFC2002), click on:

www.ietf.org/rfc/rfc2002.txt?number=2002

To obtain other detailed IETF information on IP routing for wireless and mobile hosts, click on:

www.ietf.org/html.charters/mobileip-charter.html

To obtain Charlie Perkins' (Sun Microsystems) MobileIP tutorial and valuable website, click on:

www.computer.org/internet/v2n1/perkins.htm

Fraud and Security Patent News

The US Patent and Trademark Office (USPTO) granted the following fraud and security patents between December 2001 and February 2002.

With these summaries one can see *who* is doing *what* in the world of inventions. It is often instructive to read issued patents, since they include claims of innovations as well as specifications, illustrations, detailed descriptions and references. These references are often useful to broaden one's perspective of wireless communications and security. This more detailed information can be accessed using the patent number in the Search field at the USPTO website:

www.uspto.gov

US Patent: 6,347,373

Method and Device for the protected storage of data from message traffic

A method and processor for setting up a secure telecommunication link between various communication appliances, using both classical and public key cryptography. *Secure* means ciphering and signing of messages, and key management.

Issued: February 12, 2002

Inventor: Hoepman at. al.

Assignee: Koninklijke KPN N.V. (Groningen, NL)

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

US Patent: 6,347,339

Detecting an active network node using a login attempt

A method and apparatus for notifying a network node that a second network node has gone off-line during a communication session. A logical connection is established between the nodes, using a protocol such as Telnet. Randomly generated login information is sent between the nodes, and the response provides indication of an existing connection.

Issued: February 12, 2002

Inventor: Herbert Morris at. al.

Assignee: Cisco Technology, Inc. (San Jose, CA)

US Patent: 6,346,890

Pager-based communications system

A communications system for communicating information to and from recipients scattered over wide geographic areas. The system is suited for applications such as remote reading of utility meters, communication of emergency warnings, bi-directional alarm reporting, time synchronization, and encryption/authentication.

Issued: February 12, 2002

Inventor: Robert Bellin at. al.

Assignee: Same

US Patent: 6,346,886

Electronic identification apparatus

An electronic identification apparatus having memory on board and a removable transceiver device, which also includes a processor and a transponder for receiving information pertaining to the entity to which it is attached.

Issued: February 12, 2002

Inventor: Carlos De La Huerga

Assignee: Same

US Patent: 6,345,358

In-line decryption for protecting embedded software

An in-line decryptor to decrypt software (program instructions) transferred from a read-only memory to a central processing unit. The in-line decryptor comprises a keystream generator that contains a cryptographic algorithm and memory that stores cryptographic keys. This decryptor is used to decrypt the encrypted software in real-time on an instruction-by-instruction basis.

Issued: February 5, 2002

Inventor: Mark Bianco

Assignee: Raytheon Company (Lexington, MA)

Raytheon.com

Raytheon, with 87,500 employees and revenues exceeding $16 billion, is focused on defense, government and commercial electronics, business aviation and special mission aircraft.

US Patent: 6,345,256

Automated method and apparatus to package digital content for electronic distribution using the identity of the source content

A method to automatically retrieve data from a database associated with the content. Data that is associated with the content is retrieved as and it is used to create a version of the content for electronic distribution.

Issued: February 5, 2002

Inventor: Kenneth Milsted et. al.

Assignee: International Business Machines Corporation (Armonk, NY)

US Patent: 6,345,101

Cryptographic method and apparatus for data communication and storage

A new and fast cryptographic method for high volume data communication and storage. The mathematical robustness and simplicity of this method brings an improvement in security and speed as compared to other block ciphers. The data block length or the key length can also be changed without significant redesign in the components of the cipher.

Issued: February 5, 2002

Inventor: Jayant Shukla

Assignee: Same

US Patent: 6,345,043

Access scheme for a wireless LAN station to connect an access point

An access scheme for a wireless LAN station to connect an access point on the network. This scheme allows a wireless station to finish all the processes with an access point – from search to registration – at a very high speed by shortening the beacon interval time and by eliminating the authentication phase.

Issued: February 5, 2002

Inventor: Yi-Shou Hsu

Assignee: National Datacomm Corporation (Hsinchu, TW)

US Patent: 6,343,205

Network operations center for mobile earth terminal satellite communications system

A complete mobile satellite system, including a satellite communication switching office and a network system with satellite antenna for receiving and transmitting satellite messages.

Issued: December 18, 2002

Inventor: Michael Threadgill et. al.

Assignee: Motient Services Inc. (Reston, VA)

www.motient.com

Motient owns and operates an integrated terrestrial and satellite network that stretches across North America. Motient's wireless email or mobile messaging allow mobile users to access information from virtually any location. Motient Corporation was founded in 1988 as American Mobile Satellite Corporation. Its acquisition of ARDIS was completed on March 31, 1998. In April 2000, the company changed its name to Motient.

US Patent: 6,331,974

Chaotic digital code-division multiple access (CDMA) communication systems

The structure, principle and framework of chaotic digital code-division multiple access communication systems. In the systems, a continuous pseudo-random time series is used to spread the spectrum of message signal, and the spread signal is then directly sent through channel to the receiver. Simulation results show that the channel capacity of the system is at least twice as large as that of CDMA.

Issued: December 18, 2002

Inventor: Tao Yang et. al.

Assignee: The Regents of the University of California