Wireless Security Perspectives

Cellular Networking Perspectives

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

In The News: Automated Intelligence Systems

The U.S. Information Awareness Office (IAO) under the Defense Advanced Research Project Agency (DARPA) is developing a comprehensive program to detect and protect against terrorists – the Terrorist Information Awareness (TIA) program. This includes massive collection of data from a wide variety of sources, automated analysis and coordination of the groups who will provide or use some of the data.

The IAO's TIA intelligence strategy includes twelve integrated systems, each with a focus in one of three general categories:

1. **Data collection.** Goals would include quick and transparent collection which does not disrupt the normal flow of recorded incidents. Data might require conversions, for example from voice to text or from foreign languages to English. All data would be routed to massive database systems.

   IAO's computer-assisted data collection systems would utilize data such as:

   - Human identity, based on biometric data such as distance monitoring using face recognition or gait recognition technology (involving computer-linked infra-red or visible light video cameras). Currently, computer-assisted face recognition is possible from a distance of 25 to 150 feet, but the projected capability is to achieve recognition at a distance of 500 feet,
   - Market transaction data in all possible markets, ranging from the stock market to the 'black market',
   - Communication exchanges at all possible levels – including those occurring within homes,
   - Hospital data and data from labs or chemical and biological agent production sites (for assessing the threat of bio-terrorism),
   - Event sequences in micro and macro environments (e.g, within businesses or across the entire Internet),
   - Changed data detected at monitored websites and,
   - Managerial plans or policies of suspected support groups (at commercial or industrial enterprises, for instance) or of suspected targets (such as government agencies or industrial facilities which, if disabled, would cripple the economy).

2. **Data analysis.** New database technology, from developments directed by the IAO, would support automated restructuring, improved automation in time and location stamping of data, and protection of the privacy of innocent parties by obscuring their identity or by removing their communications from analysis. All of this would be integrated with new simulation modeling technologies intended for predicting suspicious activity at business sites, public areas and within government networks. Adaptable model-building engines would analyze scenarios based on broad-context data (behavior data in foreign nations under 'normal'

About Wireless Security Perspectives

Price

The basic subscription price for *Wireless Security Perspectives* is $350 for one year (12 issues) for delivery by emailed PDF file or by first class mail within the US or Canada. International subscriptions are US$400 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees to allow more readers.

We provide discounts to educational institutions and small businesses (less than 10 employees).

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

Delivery is by first class mail or by email (Acrobat PDF file).

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due…

June 18th, 2003.

Future Topics

Wireless Flash Memory Security • Software-defined Radio Security • 802.16 Security • Radius for Wireless • 3G Security • Public Keys & Wireless • Security for Mesh Networks • Security Issues in Ad hoc Wireless Networks

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

Technical Editor and Illustrator: Les Owens.

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

Upcoming Wireless Security and Fraud Conferences & Events

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

Supercomm 2003
1st – 5th June 2003
Georgia World Congress Center
Atlanta, GA
www.supercomm2003.com/wirlesnet.cfm

The Gartner IT Security Summit
2nd – 4th June 2003
Washington Hilton
Washington, DC
www.gartner.com/us/itsecurity

Infosecurity Canada
3rd – 5th June 2003
Sheraton Center Hotel
Toronto, Ontario, Canada
reedexpo.ca/infosec

Wireless LAN Security Workshop: Security for 802.11 networks
5th June 2003
DoubleTree Hotel
Tysons Corner, VA
www.itvshop.com/wlan-security

SummerCon (Hacker conference!)
6th – 8th June 2003
The University Club of Pittsburgh
Pittsburgh, PA
www.summercon.org

2003 USENIX Technical Conference
9th – 14th June 2003
Marriott Rivercenter
San Antonio, TX
www.usenix.org/events/usenix03

SANSFIRE 2003
14th – 19th June 2003
Hilton Washington & Towers
Washington, DC
www.sans.org/sansfire03

15th Annual Computer Security Incident Handling Conference
22nd – 27th June 2003
The Westin Ottawa
Ottawa, Canada
www.first.org/conference/2003

IEEE Workshop on Internet Applications (WIAPP '03)
23rd – 24th June 2003
DoubleTree Hotel San Jose
San Jose, CA
www.cs.ucdavis.edu/~aksoy/wiapp03

NetSec 2003 Conference and Exhibition
23rd – 25th June 2003
Hyatt Regency New Orleans
New Orleans, LA
www.gocsi.com/netsec/03

Satellite Workshop on Foundations of Computer Security
26th – 27th June 2003
University of Ottawa
Ottawa, Canada
theory.stanford.edu/~iliano//fcs03

2nd Annual Government Symposium on Information Sharing and Homeland Security
30th June – 2nd July 2003
The Philadelphia Marriott
Philadelphia, PA
www.federalevents.com

circumstances, for example), and this would be used to predict suspect behavior which is statistically shown, from historical data, to precede an attack. Models would be automatically updated as new data arrives. Other predictive models would analyze wireless and wired network patterns, to reveal changes in security architectures or methods used by suspected terrorists.

Inter-agency collaboration would collate information to produce both classified and declassified reports for distribution to appropriate teams in agencies and private-sector partners. Analysis systems are intended to be capable of rapid response, even when the data is nebulous, and built-in system flexibility features would enable distribution of updated reports as the risk of attack waxes or wanes.

3. **Synthesis of strategy**. The IAO is developing systems for centralized data presentation among agencies and organizations committed to resolving terrorist threats. Automated planning systems would allow human teams and machines to 'think' together about complex problems. These would be designed to help team members overcome biases and limitations. They would provide improved decision support to foster coordinated response efforts from appropriate agencies. They would perform certain administrative tasks, such as risk analysis and maintaining accountability. Strategy adjustment recommendations could occur as new data strengthens or weakens decisions made throughout the entire process.

The IAO does not expect these automated processes will ever identify terrorists by themselves. The programs are being developed to allow human intervention in all processes.

Securing Networks with "Cyber Panel"

Part of the strategy for countering terrorist threats would employ components of an advanced cyber defense system. The "Cyber Panel Program," would be an integrated set of developing technologies which together would provide theater-level capabilities similar to those described for Therminator in the **November 2002** issue of *Wireless Security Perspectives*. The IAO intends this program would allow operators (or agency-authorized IT personnel), in public and private

sectors, the ability to continuously monitor multi-layered networks.

Cyber Panel is aimed at providing the operator:

- Capability to observe patterns of data indicative of an impending attack,
- Recommended actions to avert or counter a developing attack situation,
- Tools for impact assessment and attack tracking,
- Tools for assessing network health under various 'what if' response scenarios,
- Tools for dynamically reconfiguring security and survivability systems during an attack or recovery,
- Real experiences in the concept of NetOps (network operations), which could facilitate rapid and wide-ranging information exchange among backbone network operators,
- Broadened security in the general network environment, since attacks would be less likely because adversaries would have little or no hope of getting the results they want.

Conclusion

If this program works, it could provide more protection to Americans against terrorist threats. However, it could also threaten their right to privacy. Such an enormously complex system could incur massive costs and provide a steady stream of false alerts, while missing the truly major threats, which may be instigated by a handful of people using a low-tech approach. Those who have criticized the U.S. intelligence community for relying too much on computers, and too little on traditional intelligence techniques such as infiltration of radical groups, will not be big fans of this proposal.

Security for Ubiquitous Computing

By Tim Kridel

Peer pressure can be a bad thing – and not just for adolescents. In ubiquitous computing, where any device can use wireless to communicate with any other device in a peer-to-peer relationship, not being able to withstand pressure from dubious sources can be disastrous.

Ubiquitous computing, or "ubicomp" is a rapidly growing area of academic research today. According to the researchers, ubicomp will come of age in the next 5 – 10 years. It has two primary characteristics, according to current researchers: Physical integration and spontaneous operation. With ubicomp, therefore, computing nodes will be integrated into our physical world and they will inter-operate extemporaneously and naturally, anytime and anywhere. Ubicomp is the result of three trends:

- The declining cost of hardware for wireless technologies such as Bluetooth and WiFi,
- Increasing coverage (indoors and out) of packet-based wireless networks, which provide an "always-on" connection and,
- A belief that automating certain types of communications reduce an application's costs or at least make it more user-friendly.

Ubicomp is characterized by a highly embedded architecture supporting a high degree of mobility, as depicted in Figure 1. Ubiquitous computing means not only mobility like we are starting to see today with WiFi and have had for many years with cellular and PCS, but also integration into our environment – into common, everyday items and our clothing and even into ourselves.

As one ubicomp architect describes the near future:

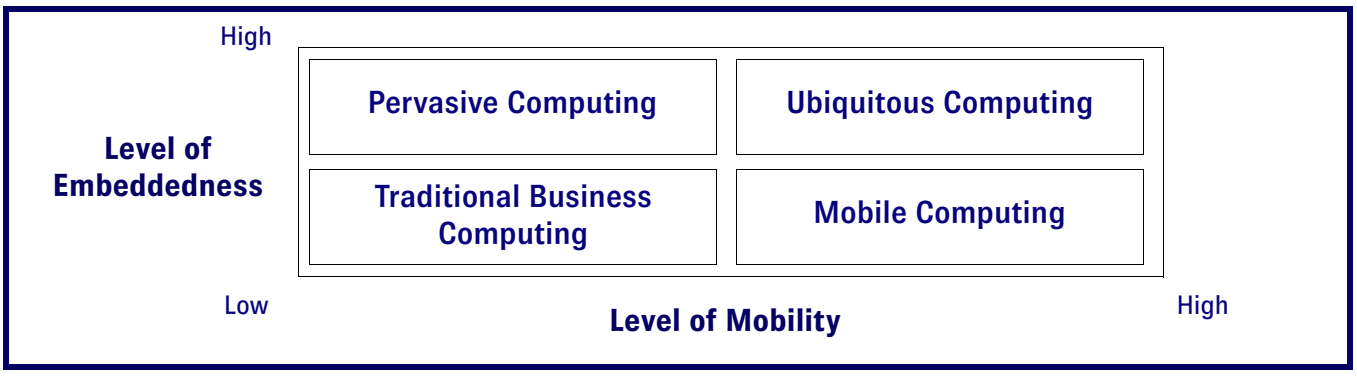
> "Within a few years, we will see many of the world's fridges, heart monitors, bus ticket dispensers, burglar alarms, and electricity meters sending messages to each other. Networked processors will be extremely cheap commodities embedded in everything from furniture to clothes. On the nanotechnology front, swarms of microscopic robots will cooperate in decentralized federations of autonomous agents that will give the terms "distributed system" and "peer-to-peer" entirely new meanings."[1]

With their Orwellian overtones, such scenarios inevitably raise questions about privacy and security. In fact, almost every paper or journal article on any aspect of ubicomp eventually makes the same observation: The issue of security in ubicomp has not been fully researched, let alone addressed. Worse yet, researchers have shared this refrain for more than five years, which suggests that security for ubicomp has not advanced at the same pace as the technologies that enable ubicomp.

Some of the common security questions that arise in ubicomp are:

- How do you deliver data securely over insecure wireless channels?
- How do you protect ubicomp devices from one another and from hostile entities?
- How do you provide access control to and from the Internet and other networks?

Figure 1: Ubiquitous Computing – Both Highly Embedded and Highly Mobile.



- How do you obscure the user's location?
- How do you verify the identity of a spuriously appearing ubicomp device?
- What does trust mean in an ubicomp environment?

Where Ubicomp Is Vulnerable

One of ubicomp's weakest points is the embedded portion of the device that sends and receives data. However, no manufacturer will want ubicomp to increase the cost of a device so that potential buyers will find it unattractive, so – as with Bluetooth or infrared – ubicomp modules have to be relatively inexpensive.

Low-cost (and the small footprint of an embedded device) usually means there is a limited amount of memory and processing power, which in turn means the available security resources also are limited. Disparate ubicomp devices often have different operating systems or different levels of memory and processing power, all of which combine to make a one-size-fits-all security platform a tall order.

With multiple potential communications technologies – including Bluetooth, GPRS, WiFi, and infrared – ubicomp security also has to be addressed above the network layer.

Security is further encumbered by the nature of a ubicomp device's power source, since this determines its ability to support features for protecting itself, and by extension, this limits the amount of protection passed along to the other devices and networks to which it connects.

Battery life can be a major weakness in some ubicomp environments. If the attacker's intent is to disrupt or disable the network rather than to steal data, one method is to attack one of the battery-powered nodes through a technique known as "sleep-deprivation torture," where the attack forces the device to perform functions that quickly drain its battery [1].

Anecdotal evidence suggests that most WiFi users, whether they are consumers or enterprises, are not aware of or do not bother to turn on basic security features such as WEP or to disable security holes such as ad hoc networking.

Educating users about security in ubicomp may be even more of a challenge than it is with WiFi, especially when the devices involved are not those usually associated with communications. For example, even novice WiFi users understand a laptop uses WiFi to communicate, but that level of understanding cannot be assumed when the devices can include everything from digital cameras to refrigerators to home entertainment systems.

A user may never even have an opportunity to configure some devices. An example is an automobile system that periodically looks for a network with which to relay information, such as an alert that maintenance is overdue. If part of ubicomp's purpose is to let devices communicate with little or no user intervention – either initially or occasionally – then its greatest strength is also its greatest weakness.

As the designers of one proposed ubicomp-security solution bluntly put it:

> "Clearly, we cannot expect ordinary individuals to tinker around with netmasks, default gateways, and MTU sizes. A robust and fast plug-and-play solution is needed which provides reconfiguration when nodes exhibit individual or collective mobility (e.g., when moving nodes to new rooms)."[2]

Potential Security Methods

For devices using low-power sources, one option is to use symmetric-key cryptography, since it generally requires less power than asymmetric-key cryptography. Security Protocols for Sensor Networks (SPINs), for example, use symmetric-key cryptography [3].

Ubicomp security solutions, however, are not often characterized by such simple and straight-forward answers. In one respect, security concerns in WiFi today foreshadow those of ubicomp tomorrow: Connecting to a network or to another device is easy even for novice users, so *what* will prevent unauthorized access, regardless of whether it is unintentional, intentional or malicious?

In WiFi, one possible solution is to add a layer of protection called location-enabled networking (LEN), where access to certain types of information or even the network itself is determined by the user's location. For example, if access is not allowed from outside the building, a LEN would not allow a WiFi user in the parking lot to log on. Or if a user is in the lobby, access to the network would be possible, while access to, for example, a database of sales leads would not be allowed. (See the **March 2003** issue of *Wireless Security Perspectives* for a detailed discussion of WiFi LENs.)

The drawback is that location information can be spoofed. Data which appears to be GPS information can be provided as proof of the device's location, even though it was not calculated by a GPS receiver. Furthermore, the complexity of location-determining equipment would likely antagonize system designs meant to be simple, which typically employ low cost, small, robust and lower-powered devices.

Authentication using short-range technology is one option – at least in devices with multi-mode ubicomp modules and in applications where proximity is a measure of trustworthiness. The short-range of Bluetooth or infrared or even ultrasound are physically constrained channels of communication, and therefore, signal interception by those outside their range is limited [4]. Two devices, communicating over a short range which does not extend to the parking lot, for instance, could exchange a shared secret key and transfer data over the link or they could switch to another link, such as 802.11g, for a large file transfer. Signal leaks to the outside could occur from reflection of the signal out through a door or from signal forwarding via covert operations, and its detection would require additional system configuration. This also will increase the complexity of the devices, and the result may only be 'good enough', rather than truly strong security.

Outside of or in addition to these approaches, security in ubicomp systems may need to have more manual intervention, such as only allowing new devices to communicate when a central controlling device is temporarily set into a mode to allow it, and with every application to join the network being manually approved. This, unfortunately, would oblige home owners to do network management tasks, and it could prove to be an unmanageable burden for corporate installations.

Some location-based ubicomp-security methods are designed to balance security and privacy. The authentication process in Mist, for example, uses an hierarchy of routers and contact points to reduce the amount of information that the device has to reveal in order to get access [5]. That approach could be a good fit for services where users are willing to receive advertising information automatically pushed to their ubicomp devices as long as no information about them is collected.

One of the better known ubicomp-security proposals, if only for its name, is "Resurrecting Duckling," which was inspired by an animal behaviorist research into why a newborn goose assumes that the first moving object that it sees is its mother [1]. In ubicomp, a device such as a digital camera stands in for the duckling, which is imprinted by the Mother Goose, such as a PDA, through a symmetric key. The Duckling device will then follow instructions only from the Mother Goose or from devices which have received the symmetric key from the Mother Goose. One benefit of this concept is that the Mother Goose can order the Duckling to commit suicide so that it can be reborn later, so that it can be imprinted by another Mother Goose. Even this is not without problems. How would a Duckling be resurrected if the Mother Goose's motherboard burns out?

Each ubicomp-security method has its advantages and disadvantages, and the chances that a one-size-fits-all method exists are as slim as ubicomp applications are many. The good news is that ubicomp is still in its nascent stages, when there is no better time to address security.

References:

[1] F. Stajano and R. Anderson. *The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks.* Security Protocols, Lecture Notes in Computer Science, vol. 1796, Springer-Verlag, Berlin, 1999, pp. 172–194.

[2] A. Misra, *et al.* *Autoconfiguration, Registration, and Mobility Management for Pervasive Computing.* IEEE Personal Communications, August 2001, pp. 24-31.

[3] A. Perrig, *et al.* *SPINS: Security Protocols for Sensor Networks.* Proceedings of the 7th Annual International Conference. Mobile Computing and Networks (MobiCom 2001), ACM Press, New York, 2001, pp. 189–199.

[4] T. Kindberg, *et al.* *Context Authentication Using Constrained Channels.* Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications, 2002.

[5] J. Al-Muhtadi. *Routing Through The Mist: Privacy Preserving Communication in Ubiquitous Computing Environments.* Proceedings of the 22nd International Conference on Distributed Computing Systems, 2002.

Talk About Wireless Security!

With cell phone thefts now accounting for more than 50% of all street crime in London, England, U.K. carriers such as Vodafone have launched technology that remotely disables stolen phones. Police, meanwhile, are taking a low-tech approach: Marking phones with ultraviolet ink to make them easily identifiable when recovered.

> "Mobile phone robbery is rapidly becoming a very risky crime to be involved in," Metropolitan Police Commissioner Sir John Stevens told the BBC.

It is particularly risky for a thief who targets someone with a Motedo MTD-125, which looks like a cell phone but is actually a 180,000-volt stun gun. (The antenna is one of the prongs, which poke through the included leather carrying case.) If that does not do the trick, the MTD-125 also includes a 130-dB alarm. It is all powered by a 9-volt battery.

Although Motedo says the design "has won many patents from various countries and areas," the Taiwan-based company is silent on where it has been approved for sale. If U.K. regulators will not allow it, Motedo might try Japan, where groping on trains is rampant. Last August, a Yokohama teen used an MMS phone (multimedia messaging service phone) to snap evidence of a man fondling her before pulling out a stun gun.

> "I knew it was all over the moment she whipped the thing out," the groper told police.

There is no word from Motedo on whether or not it plans to put its stun gun technology in a real cell phone.

IREAN Workshop Papers Online

Often, forces coming from university research programs help shape emerging technology. The IREAN (Integrated Research and Education in Advanced Networking) Research Workshop – sponsored by the Alexandrian Research Institute of Virginia Tech – sheds light on many emerging aspects of wireless communication systems. Presentations at the workshop provided snapshots of some of the issues faced.

Summaries of all 20 presentations given at the workshop are freely available in a list at:

www.irean.vt.edu/research_workshop_april2003

The list of presentation abstracts includes several on wireless security. For example, one of them analyzes IPSec routing problems, and another discusses fraud control in WiFi, Bluetooth and in other wireless activities (including a taxonomy of wireless attack showing a classification scheme for the spectrum of known types of attack). The summaries indicate each researcher's intent regarding further explorations. Some include illustrations (e.g, models and analysis diagrams), research data, valuable observations, and suggested strategies and recommendations for wireless security practitioners.

The list also includes several interesting topics involving wireless, but not wireless security, such as: Innovations for dealing with FCC Regulations, Biologically Inspired Cognitive Wireless, Wireless Interactive Teaching, Ultra-wideband Technology Application, Mobile Ad hoc Network (MANET) Routing Protocols, and Intelligent Online Routing.

For additional information about IREAN, contact:

Alexandria Research Institute
206 N.Washington Street, Suite 400
Alexandria, VA-22314

Telephone: (703) 518-8080
Fax: (703) 518-8085
Email: ari-info@vt.edu

Fraud And Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following fraud and security patents. These will be of interest to some of our wireless security practitioners. Each patent includes the patent number, the invention title – linked to the corresponding USPTO webpage – a brief description, the inventor(s), and the assignee (owner). All of these patents, except the last one, were granted in May of 2003.

With the listing below, one can see *who* is doing *what* in the world of 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: 6,567,915

Integrated circuit card with identity authentication table and authorization tables defining access rights based on Boolean expressions of authenticated identities

This invention concerns an integrated circuit (IC) device, such as smart cards, electronic wallets, PC cards, and the like, and various methods for authenticating identities and authorizing transactions based on the authenticated identities. The IC device has a memory and a processor. It maintains an identity authentication table in the memory to hold an arbitrary number of identities. This table correlates identities with authentication protocols, so that different protocols can be used to authenticate associated identities. It also correlates counts with the identities. Individual counts specify a number of uses of the IC device for a corresponding identity, without requiring the IC device to authenticate the identity for each use. The IC device also maintains an authentication vector in memory, which tracks identities in the identity authentication table that are currently authenticated by the IC device. The IC device further maintains authorization tables in the memory and in association with particular files used in transactions. Each of these tables defines authorization for a particular transaction as a Boolean expression of the identities listed in the identity authentication table.

Issued: May 20, 2003

Inventor: Scott Guthery
Assignee: Microsoft Corporation (Redmond, WA)

US Patent: 6,567,511

System and method for real-time fraud detection within a telecommunications system

Real time detection of the fraudulent use of a telecommunications network is accomplished by analyzing data for each call that is occurring within the network. A signal protocol receiver is used to collect signaling protocol for each call that is occurring within the network. The Signaling protocol data is collected, decoded and formatted into call information records (CIRs). The CIRs contain various operator-specified parameters for each call that is occurring within the network. The CIRs are compared to operator-defined thresholds. If any of them exceeds the thresholds, an alert is generated, which is then stored in a database where the operator can analyze them and take the appropriate corresponding action to resolve the alert. The alerts and the CIRs are archived in a database so that trends of fraudulent use can be detected and prevented. This method of fraud detection provides for effective analysis of every call that occurs within the network. Ideally, no fraudulent call goes undetected. Additionally, the method does not impose an additional load on the network switching equipment, and it therefore results in a better quality of transmissions.

Issued: May 20, 2003

Inventor: Judy Betts, *et al*
Assignee: Ameritech Corporation (Hoffman Estates, IL)

US Patent: 6,564,322

Method and apparatus for watermarking with no perceptible trace

A watermark in the form of an added message is attached to a digital recording so that a significant content of the recording is completely unchanged by the process in the sense that any reader commonly used for such recording will extract from the recording exactly what would have been extracted in the case when the added message had not been attached. This is done by hiding the added message in the error correcting code (ECC) for the significant content of the recording.

Issued: May 13, 2003

Inventor: David Jameson, *et al*
Assignee: International Business Machines Corporation (Armonk, NY)

US Patent: 6,564,261

Distributed system to intelligently establish sessions between anonymous users over various networks

A network provides users with a simple and secure way of establishing communication sessions with other users or services, running either over IP networks or other networks, (e.g, PSTN). In a sense, the network can broker communication services between two or more users (e.g, people) and/or services. Several different clusters of servers are provided, and each of the clusters may be linked together. Also, each cluster may include multiple servers. Users are registered within some specific cluster and given a unique system/network ID. The system may be configured such that messages are not sent directly between users, but instead through at least one intermediate routing service (RS) provided on a server of one of the

users. Thus, with this configuration, a user may hide or mask his/her personal information from other users even when communicating with them. The configuration may also allow a user to establish a communication session with another user without knowledge of the client device (e.g, PC, mobile phone, etc.) being used by the other user, as the network arranges for communication (e.g, text chat session, voice chat session, PC to PC, PC to PSTN, or PC to mobile phone), web conference, or pages (PC to PC, PC to SMS) between the users, regardless of the client device being used by the called user. Thus, the network enables any of the above communication services between users, and the initiating user's knowledge is limited concerning the types of other devices connected.

Issued: May 13, 2003

Inventor: Gudjon Gudjonsson
Assignee: Telefonaktiebolaget LM Ericsson (publ) (Stockholm, SE)

Interesting references:

[1] *Using Hyperflow for Secure Internet Server Clusters.* Cyber IQ Systems, Dec. 1998, pp. 1-16.

[2] Handley, *et al. SIP: Sessions Initiation Protocol.* Mar. 1999, RFC 2543 (153 pages printed).

US Patent: 6,560,581

System and method for secure electronic commerce transaction

An electronic commerce system for facilitating secure electronic commerce transactions among multiple participants. Each electronic commerce transaction involves at least one commerce document defining the transaction, and at least one commerce instrument defining a payment for the transaction. The electronic commerce system has a credential binding server at a trusted credential authority, multiple computing units at associated participants, and a communication system interconnecting the credential binding server and the multiple computing units. The electronic commerce system operates in two phases: A registration phase and a transaction phase.
During the registration phase, each of the computing units generate and send a registration packet over the communication system to the credential binding server. Unique credentials are produced by the credential binding server, based upon the registration packets sent back to the computing units.
During the transaction phase, an originating computing unit initially requests, receives, and verifies the credentials of expected recipient computing units to ensure communication between authenticated participants. Thereafter, the originating computing unit signs and encrypts the commerce document(s) and the commerce instrument(s) in a manner which ensures that only the intended recipients can decrypt them. The originating computing unit then sends both the commerce document(s) and instrument(s) over the communication system to a first recipient computing unit. The first recipient computing unit decrypts and verifies the commerce document(s) and/or instruments intended for it. The first recipient computing unit then passes the balance of the encrypted commerce document(s) and/or instrument(s) over the communication system to a second recipient computing unit, which decrypts and verifies the commerce document(s) and/or instrument(s) intended for it.
This process is continued until all commerce documents and commerce instruments are distributed, decrypted, and verified by their intended recipients.

Issued: May 6, 2003

Inventor: Barbara Fox, *et al*
Assignee: Visa International Service Association (Foster City, CA)

Interesting references:

[1] Rubin, Aviel D. *Secure Distribution of Electronic Documents in a Hostile Environment.* Computer Communications, Elsevier Science Publishers, Amsterdam, vol. 18, No. 6, pp. 429-434. Jun. 1, 1995.

US Patent: 6,560,340

Method and apparatus for geographically limiting service in a conditional access system

A cable television system provides conditional access to services.
The cable television system includes:

- A head-end from which service "instances", or programs, are broadcast and,
- Several set-top units for receiving the instances and selectively decrypting the instances for display to system subscribers.

The service instances are encrypted using public and/or private keys provided by service providers or central authorization agents.
Keys used by the set tops for selective decryption may also be public or private in nature, and such keys may be reassigned at different times to provide a cable television system in which piracy concerns are minimized.

Issued: May 6, 2003

Inventor: Gendon Akins III, *et al*
Assignee: Scientific-Atlanta, Inc. (Lawrenceville, GA)

Interesting references:

[1] Coutrot, *et al. A Single Conditional Access System for Satellite-Cable and Terrestrial TV.* IEEE Transactions on Consumer Electronics, vol. 35, No. 3, Aug. 1989, pp. 464-468.

[2] Louis Claude Guillou and Jean-Luc Giachetti. *Encipherment and Conditional Access.* SMPTE Journal, 103 (1994) Jun., No. 6, White Plains, NY.

[3] Menezes, Alfred J. Handbook of Applied Cryptography, pp. 506-525.

US Patent: 6,560,338

Limiting delays associated with the generation of encryption stream ciphers

A method and an apparatus for generating encryption stream ciphers based on a recurrence relation designed to operate over finite fields larger than GF(2). A non-linear output can be obtained by using one or a combination of non-linear processes to form an output function. The recurrence relation and the output function can be selected to have distinct pair distances, such that,

as the shift register is shifted, no identical pair of elements of the shift register are used twice in either the recurrence relation or the output function. Under these conditions, the recurrence relation and the output function also can be chosen to optimize cryptographic security or computational efficiency. To assure processing quality, the ciphering delay is measured to provide an estimate, according to a provided measuring method, and a second ciphering method is employed to limit the accumulated delay of the ciphering operation, if the delay estimate exceeds the predetermined bounds.

Issued: May 6, 2003

Inventors: Greg Rose and Frank Quick.

Assignee: Qualcomm Incorporated (San Diego, CA)

Interesting references:

[1] D. Coppersmith Handley, *et al. The Shrinking Generator.* Proc. Crypto '93, Springer-Verlag, 1994.

[2] K. Shaheen, *Code Book Cipher System.* 1994 IEEE, pp. 66-71.

[3] Lee, Handley, *et al. BRM Sequence Generators Based on the Field GF(2) for DSP Implementations.* Proceedings of 1995 IEEE International Symposium on Information Theory: p. 48 (Sept. 17-22, 1995).

US Patent: 6,560,337

Systems, methods and computer program products for reducing effective key length of ciphers using one-way cryptographic functions and an initial key

Effective key length of a symmetric key cipher is reduced by deriving an intermediate value from an initial key. Predetermined bit locations of the intermediate value are selected to obtain an intermediate key. An intermediate shortened key is derived from the intermediate key by setting predetermined bit locations of the intermediate key to predetermined values. A diffused intermediate shortened key is derived from the intermediate shortened key using the one-way cryptographic function. Predetermined bit locations of the diffused intermediate shortened key are then selected to obtain a shortened key. In first embodiments, the one-way cryptographic function is a one-way hash function. Second embodiments use the symmetric key cipher itself to perform the one-way cryptographic function.

Issued: May 6, 2003

Inventor: Mohammad Peyravian, *et al*

Assignee: International Business Machines Corporation (Armonk, NY)

Interesting references:

[1] *X9.69 Key Management Extensions.* Accredited Standards Committee X9, American Bankers Association, Aug. 6, 1998.

[2] Harney, *et al. Group Key Management Protocol (GKMP) Specification*, IETF RFC-2098, Jul. 1997.

[3] Massey. *SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm.* Fast Software Encryption, Cambridge Security Workshop Proc., Springer-Verlag, 1994, pp. 1-17.

US Patent: 6,557,103

Spread spectrum image steganography

Spread Spectrum Image Steganography (SSIS) provides the ability to hide a significant quantity of information bits within digital images (a cover signal). The message is recovered with low error probability, due to the use of error control coding. SSIS payload is, at a minimum, an order of magnitude greater than that of existing watermarking methods. Furthermore, the original image is not needed to extract the hidden information. The proposed recipient need only possess a key in order to reveal the secret message. The very existence of the hidden information is virtually undetectable by human or by computer analysis. SSIS also provides the advantage of resiliency to transmission noise, like that found in a wireless environment and low levels of compression.

Issued: April 29, 2003

Inventor: Charles Boncelet, *et al*

Assignee: The United States of America, as represented by the Secretary of the Army (Washington, DC)

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