Wireless Security Perspectives *Cellular Networking Perspectives*

California Mulls RFID Privacy Law

California is the latest state to set privacy guidelines for consumer applications of radio frequency identification (RFID) tags. On February 24, 2004, state senator Debra Bowen introduced SB 1834, to amend California's Business and Professions Code to cover RFID. If passed, violations would be considered an act of unfair competition. Key requirements include:

• Obtaining users' written consent before their personally identifiable information – such as name, address or credit card number – could be stored in an RFID tag.

• Getting additional written consent before that information could be shared with a third party.

• "Reasonable measures" to ensure that user data is transmitted and stored securely.

• In retail applications, the RFID tag must be removed or destroyed before the customer leaves the store.

The guidelines would apply to public agencies, too. In a press release announcing the bill, Bowen cited the San Francisco Public Library Commission's plan to tag books, starting in 2005. That is one example of how homeland security agencies could use RFID as an end run around libraries' resistance to turning over patrons' borrowing records.

SB 1834 was born out of two hearings last year in the Senate Subcommittee on New Technologies, which Bowen chairs. The bill also is one of the latest examples of recent concerns about RFID security and privacy. Such concerns have already led to the creation of groups such as Customers Against Supermarket Privacy Invasion & Numbering, and on February 27, 2004, the German retailer *Metro Group* said that it would stop issuing RFID-equipped customer cards due to consumer concerns.

SB 1834 is an attempt to set guidelines before the technology goes mainstream, the point where it is tougher and more expensive to revamp or replace technology that is already deployed. "There's no reason to let RFID sneak up on us when we have the ability to put some privacy protections in place before the genie's out of the bottle," Bowen said.

At least two others states have addressed the concerns with RFID. In Utah, the Radio Frequency Identification Right to Know Act (HB 251) passed the house and a senate committees, but expired March 3, 2004

About Wireless Security Perspectives

Price

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

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

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

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

Complete pricing information for both publications is available at:

   www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

   cnpsales@cnp-wireless.com

Next Issue Due...
   April 29th, 2004.

Future Topics

Light-weight Security Protocols • Security for UWB • MANET Security • Radius for Wireless • Handheld Device Security • 4G Security • Zigbee Security • PKE-enabled Wireless

after amendments stalled hearings. In Missouri, the Senate Commerce and Environment Committee is reviewing the RFID Right to Know Act of 2004 (SB 867).

Legislators are not the only ones who argue that privacy and security need to be addressed sooner rather than later. For example, in August 2003, the analyst firm GartnerG2 warned retailers to begin proactively educating customers about RFID rather than simply responding to their privacy concerns as they come up.

Those concerns could be a boost for companies such as RSA Security, which has developed "blocker tags" that let users thwart RFID transmissions. (As it happens, the prototypes were demonstrated for the first time on February 24, the same day SB 1834 was introduced.) Other vendors offer tags that can be embedded with a "kill feature," which is one way that retailers could meet SB 1834's requirement that tags be removed or destroyed at the point of sale. For more information on techniques for safeguarding RFID privacy and security, see the July 2003 and September 2003 issues of *Wireless Security Perspectives*.

Privacy and Telematics: Driving Ahead of the Law

Kevin J. Kuzas and William J. Sill
Wilkinson Barker Knauer LLP

Careful what you say while driving – your car may be spying on you. And pay attention to the fine print in your next rental car contract, for you may discover it was *you* that authorized the spying.

Every year, more and more cars are equipped with "telematics." The Telematics Research Group estimates that by 2008, over 40% of new cars in the United States will have some form of telematics. [1] Strictly speaking, "telematics" applies to any marriage of location-tracking technologies, such as GPS, with wireless communications, such as cellular, often with advanced computing features added. The most popular applications currently are consumer applications such as General Motors' OnStar, that center around navigation and safety. Business versions of similar services, such as AirIQ, are increasingly used by rental car companies, delivery services and other businesses that own a fleet of vehicles, to monitor usage.

Telematics services are increasingly allowing the collection and use of data some may consider personal information. Typically, users are unaware of the extent of the monitoring and of the data collected. Thus, telematics applications raise several privacy concerns that are only beginning to be understood.

This article looks at the first few instances in which the use of telematics has collided with the U.S. legal system. Perhaps not surprisingly, these cases leave many important issues unsettled. Therefore, we also provide a brief overview of the legal principles in the United States that govern privacy, and we discuss how they might be applied to telematics services when, as is inevitable, further legal challenges arise.

Telematics' First Fender-Benders Hit The Courts

Case #1: In June 2001, a Connecticut man was outraged to learn that his rental car had tattled on him. His contract with Acme Rent-a-Car specified that he would not speed and that should he be caught speeding, additional charges would be applied to his credit or debit card. Imagine his surprise when he opened his bank statement and learned that Acme had debited his account another $450 – for speeding on three separate occasions: $150 each time – even though he had not been pulled over by the police.

Acme vehicles were equipped with GPS technology, and the company had employed AirIQ to monitor its fleet. AirIQ enabled Acme to monitor vehicle speed and location and verify if any accidents had occurred.

When the man complained about the additional charges, Acme was able to point to the three exact times and places where the man was speeding. Although this example does raise substantial privacy issues, it should be noted that Acme fined the driver only when he exceeded 80 m.p.h.

The man sued Acme in small claims court to recover the $450. Importantly from the perspective of setting legal precedent, the Connecticut Department of Consumer Protection reviewed Acme's billing practice. The department found an unlawful "deceptive trade practice" and ordered Acme to refund any money it had charged its customers for speeding. Acme has appealed the ruling, and the appeal is still pending.

The state's decision was not based primarily on privacy grounds. Instead, the department focused on whether Acme had adequately informed its customers in advance of the additional charges and whether or not Acme, as a private company, had any business prohibiting excessive speeding – traditionally a function reserved for the state. Yet privacy concerns clearly played a role. The state attorney general, who is defending the ruling against Acme's appeal, denounced the practice as a "clear violation of privacy." According to the attorney general, "Acme cannot infringe on the privacy rights of its customers or fine consumers with no recourse." [2]

Case #2: Telematics "tattling" is not limited to the private sector. In a widely reported incident in July 2001, a Merced, California man, speeding in his brand new, OnStar-equipped SUV, got into an accident. Rather than stop, the man decided to run for it. However, OnStar had noticed that the car's airbag had deployed, and when it could not reach the driver (to ensure his safety), OnStar called the police. The police were able to connect the hit-and-run incident to the driver.

Most alarming is the fact that it is possible for the government to eavesdrop on discussions you have with your passengers. It did not take long for the Federal Bureau of Investigation (FBI) to discover that with a court-authorized wiretap, it could use the OnStar system to establish a one-way call to a suspect's vehicle without the driver's knowledge and eavesdrop on the conversations taking place in the car. This ability has the potential to turn every car, not just Volkswagen Beetles, into "bugs."

Case #3: OnStar complied with several court-ordered wiretaps, but expressed concerns that the wiretaps were disabling some of the key safety features of the OnStar system. For example, in the event of an accident, the wiretapped vehicle could not call OnStar because the phone line would already be in use. OnStar appealed several court orders requiring it to institute wiretaps, and in December 2002, the case reached the Federal Court of Appeals for the Ninth Circuit in California.

In November 2003 the court issued its decision – the first of its kind. [3] The court first addressed whether the wiretap laws applied to a telematics service such as OnStar. The wiretap law applies to any "wire or electronic communications," and the court noted that the cellular technology used by the OnStar service has traditionally been subject to the law. The court ruled firmly that the wiretap laws apply to services such as OnStar and thus, with proper warrants, law enforcement could require telematics services to monitor users without their knowledge.

However, the wiretap law requires a "minimum of interference" with the service being provided. The court found that the wiretaps at issue were disabling some of the most important features of the OnStar service and thus could not be conducted with a minimum of interference. As a result, the court ruled that these particular wiretaps were unlawful.

The Ninth Circuit ruling is important both for what it did and did not do. Although it established some limits on the government's rights to monitor telematics users, it did not create any privacy right for drivers. In fact "privacy" was not even mentioned in the court's decision. If the government could have found a way to conduct the monitoring without disabling the OnStar service, the court may very well have upheld the legality of the wiretaps.

U.S. Privacy Law: Is the Tank 1/4 Full or 3/4 Empty?

The United States does not have a comprehensive privacy law that encompasses telematics. Instead, there is a patchwork of laws regulating privacy concerns for specific types of information, such as financial or medical records, or for specific industries, such as telephone companies or cable television companies. None of these laws directly apply to telematics.

"Location privacy," though, has been a particularly sensitive topic that has occasionally attracted the attention of regulators and policymakers. Cellular operators, for example, have been prohibited by the Federal Communications Commission from disclosing a caller's location without the caller's permission, except in certain emergency situations. [4] However, an attempt to legislate location privacy on a broader, technologically-neutral basis failed in 2001. The 2001 Location Privacy Act would have required users to grant permission before businesses could use their location information. This law would have applied to telematics services, and might have prohibited Acme Rent-a-Car from tracking its renters. The legislation, like many other privacy-related bills, died in committee after the September 11th 2001 terrorist attacks.

This does not mean that telematics privacy is totally unprotected. The Federal Trade Commission (FTC) and other government agencies have long advocated "fair information practice principles" with respect to the collection and use of personal information. These principles are:

- **Notice** – Consumers should be informed of a company's data collection policies.
- **Choice** – Consumers should have the right to grant or deny permission to certain uses of their personal data.
- **Access** – Consumers should be able to uncover the information about them that a company has in its possession and correct any errors.
- **Security** – Sensitive information should be protected from unauthorized access and disclosure.
- **Redress** – There should be valid enforcement mechanisms against those that do not follow these practices, whether through government action or industry self-regulation.

These principles do not have the force of law. Many businesses, however, make efforts to comply with at least some aspects of these principles. For example, many businesses publish a privacy statement providing consumers with notice of their information practices, and some even provide consumers with the opportunity to opt out of certain uses of information. Many business and consumer groups advocate at least partial compliance with the FTC's fair information practices because they believe it helps convince policymakers that further government regulation is unnecessary.

in determining the extent of a person's expectation of privacy when they use a service capable of collecting personal information. Among the most important issues to consider are:

- Were notices provided to inform consumers that they could be monitored?
- Was the company's privacy policy made available conspicuously?
- Did the privacy policy disclose how the company would use the information gathered?
- Did any of the company's marketing materials or advertising raise consumers' privacy expectations?

The FTC and state regulators have very broad authority to police "unfair" or "deceptive" trade practices. They have used this authority to take action where they perceive consumer expectations of privacy have been breached.

What are the privacy expectations of the average consumer when it comes to telematics? There seems to be at least an initial perception that a driver's car is their "castle" and thus location information is very sensitive. Yet in the **three previously mentioned cases**, privacy was not the determining factor. Perhaps this is due, in part, to the fact that telematics companies do not seem to be creating any unrealistic privacy expectations from their users – at least not among those who read the fine print in their contracts.

OnStar Privacy Agreement

effective as of July 2003 until replaced

This Agreement describes the terms and conditions regarding your receipt of OnStar services. These terms and conditions apply to the OnStar service plan included in the price of a new vehicle ("Standard Service Plan"), any other OnStar service plan selected by you at the time you purchase your vehicle (whether new or used) or any time thereafter ("Extended Service Plan"), additional OnStar services selected by you, and any update or improvement to the OnStar services (all of the above collectively referred to as the "Services"). Your activation and receipt of OnStar Services shall constitute your acceptance to be bound by these terms and conditions.

... OnStar may collect personal information about you or your use of the Services. ... Service Providers may monitor and/or electronically record your conversations with call center representatives, emergency services providers, and law enforcement personnel. ... privacy cannot be guaranteed on cellular telephone systems such as those used for the Services, and OnStar shall not be liable to you for any claims, loss, damages or costs which may result from a lack of privacy experienced.

OnStar reserves the right to modify any and all terms ... at any time during the term of this Agreement upon notice to you.

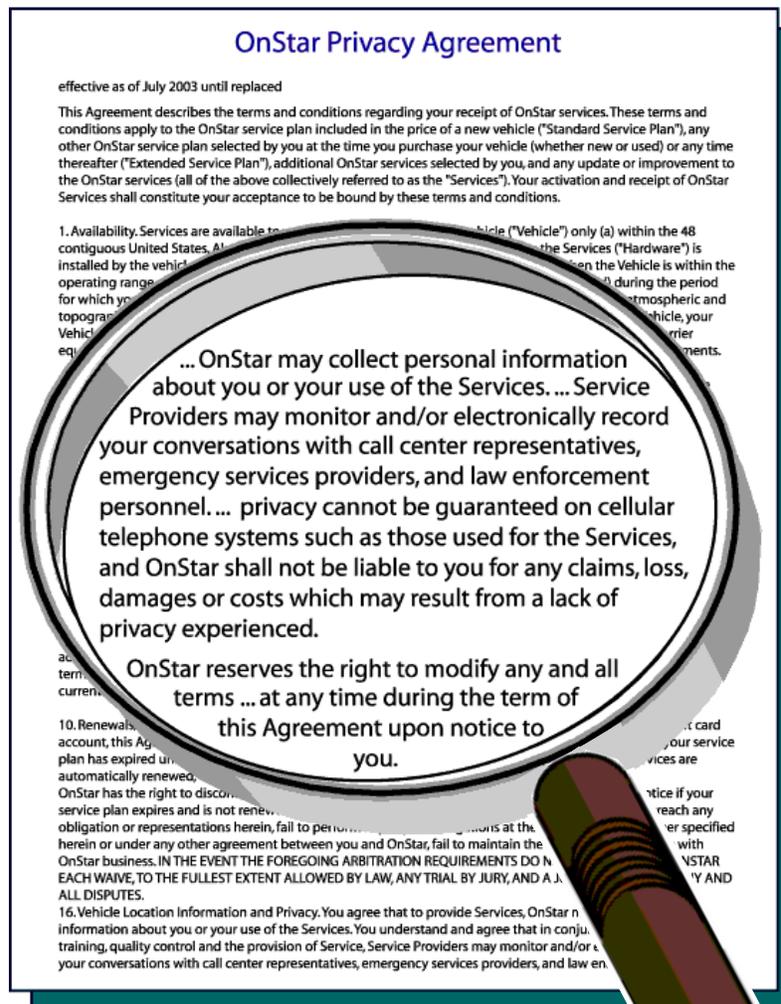## Privacy Expectations for Telematics Services

Consumer expectations of privacy may play an important role in determining the response of policymakers and regulators to privacy issues posed by telematics. Several factors are involved

For example, the "Terms and Conditions" for OnStar state that the customer "consents" to use of vehicle location and other personal information for several purposes unrelated to providing the services, such as:

- "locating your Vehicle if you are in default of this Agreement or any finance or lease agreement,"
- "sharing Information with the Vehicle manufacturer and dealer" and
- "transmitting . . . advertising and promotional materials."

Furthermore, OnStar's published privacy policy **(illustrated above)** also goes out of its way *not* to promise that it will not disclose the information it collects to selected third parties.

It is also important to distinguish consumer expectations regarding private sector uses of personal information, on the one hand, from expectations with respect to government intrusions on privacy, such as law enforcement investigations, on the other. Expectations of privacy from the government and the private sector would clearly overlap in situations where the government sought to monitor activity without suspicion that a crime was being committed.

The Fourth Amendment to the U.S. Constitution protects against unreasonable searches, and this prohibition would generally prohibit monitoring where an individual had an expectation of personal privacy. Importantly, though, if law enforcement authorities can show probable cause of criminal activity and obtain a warrant, privacy expectations can be overcome. As the Court of Appeals decision in the OnStar case shows, the car is not a sanctuary from lawful wiretaps.

Driving Towards an Uncertain Future

A comprehensive body of privacy law has yet to coalesce, particularly as applied to relatively new technologies such as telematics. One can almost guarantee that more legal challenges to the use and disclosure of data collected by telematics services will occur in the future. For example, Acme is not alone in deploying telematics to monitor the use of its vehicles, and it has not ceased monitoring its drivers, although it has ceased charging additional fees for speeding while its appeal is pending.

Also, consumer expectations may evolve with respect to the appropriate level of privacy expected from telematics services. As mentioned above, location privacy was a hot topic prior to the September 11 attacks, and it is likely to receive attention again in the near future as new location-based services continue to be developed and deployed. Several privacy advocacy groups – such as the Electronic Frontier Foundation, the Electronic Privacy Information Center and the Center for Democracy and Technology – have made location privacy a priority. These groups can be expected to increase the level of consumer awareness of privacy issues with respect to telematics and other location-tracking services. In turn, these efforts could change policymakers' assumptions about consumer expectations.

Without a comprehensive federal law, there is always a risk of inconsistent court decisions or a patchwork of state laws, which could hamper the development and roll-out of new services. If a consensus among business, consumers and policymakers could be reached on the level of privacy protection that is appropriate for telematics, a federal law could bring certainty to the industry as to its legal obligations. Based on the few cases that have arisen to date, it is difficult to conclude whether we are driving towards that consensus or whether we are stuck in neutral.

About the Authors

Kuzas (kevin.kuzas@wbklaw.com) and Sill (wsill@wbklaw.com) are partners at Wilkinson Barker Knauer LLP.

References

[1]. Wireless NewsFactor. *Honda, Toyota Add Telematics Features to New Cars,* August 29,2002,
www.newsfactor.com/perl/story/19239.html

[2]. Connecticut Attorney General's Office Press Release dated April 5, 2002 available at:
www.cslib.org/attygenl/press/2002/coniss/acmeappeal.htm

[3]. In re: *In the matter of the Application of the United States for an Order Authorizing the Roving Interception of Oral Communications*, D.C. No. CV-01-01495-LDG, November 18, 2003 (9th Cir.) Although the case was filed anonymously, the description of the service in the decision reveals features used exclusively by OnStar.

[4]. 47 U.S.C. § 222(f), 47 C.F.R.§ 64.2007.

U-R-Linked:

www.elonka.com/UnsolvedCodes.html

An interesting list of unsolved cryptographic codes – some dating from a few years ago and others from a few thousand years ago. Budding cryptographers may want to try out their skills and aim for the fame that can only be obtained by being the first person to do something difficult such as this.

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.

Communications Design Conference
29th March - 1st April 2004
Moscone Center
San Francisco, CA
www.esconline.com/
electronicaUSA/tech_conf/cdc

SANS2004 Annual Conference
1st - 9th April 2004
Walt Disney World Dolphin
Lake Buena Vista, FL
www.sans.org/sans2004

The Wireless LAN Event
6th- 7th April 2004
Olympia
London, UK
www.wlanevent.com/
home/default.asp

SPIE Defense & Security Symposium (Digital Wireless Comms)
12th- 16th April 2004
Gaylord Palms Resort &
   Convention Center
Orlando, FL
www.spie.org

NW Technology Tour Wireless LANs: Gaining Strength — Reaching Farther
13th April 2004
Hyatt Woodfield, in Schaumburg
Chicago, IL
www.nwfusion.com/events/wlan

[Note: Technology tour
planned for several other
locations during April]

3rd International Workshop on Wireless Information Systems (WIS 2004)
13th- 14th April 2004
Porto Center
Porto, Portugal
www.iceis.org/workshops/
wis/wis2004-cfp.html

ISPCON Spring 2004
14th- 16th April 2004
Washington Hilton & Towers
Washington, DC
www.ispcon.com/spring2004/
wisp-workshop.asp

2nd International Conference on Pervasive Computing (Pervasive 2004)
18th- 23rd April 2004
Vienna Hofburg
Vienna, Austria
www.pervasive2004.org

Wireless Security Forum
19th- 20th April 2004
Santa Clara Convention Center
Santa Clara, CA
www.wsfevent.com

Wireless Communications Alliance Meeting
20th April 2004
Santa Clara Convention Center
Santa Clara, CA
www.wca.org

[Note: Co-located with
Wireless Security Forum]

Information Processing In Sensor Networks (IPSN '04)
26th- 27th April 2004
DoubleTree Hotel & Executive
   Meeting Center
Berkeley, CA
ipsn04.cs.uiuc.edu

Security Solutions 2004
26th- 29th April 2004
Tampa Marriott Waterside Hotel
Tampa, FL
security2004.telos.com/agenda

4th International Conference on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks
26th- 30th April 2004
Eldorado Hotel
Santa Fe, New Mexico
ranger.uta.edu/~kumar/
ipdpswman.html

DallasCon Information and Wireless Security Conference
1st-2nd May 2004
Wyndham Hotel
Dallas, TX
dallascon.com/default.asp

Fraud and Security Patent News

US Patent: 6,711,690

Secure write blocking circuit and method for preventing unauthorized write access to nonvolatile memory

A secure write blocking circuit and method of operation thereof. The secure write blocking circuit includes enable and disable block input terminals coupled to a blocking circuit. The blocking circuit, such as a set/reset latch in a preferred embodiment, generates a block signal to prevent write access to a nonvolatile memory device, such as flash memory, in response to signals provided to the enable and disable input terminals. The secure write blocking circuit also includes an interrupt generator (coupled to the disable block input terminal) that generates an interrupt signal in response to a signal at the disable input terminal. In a related embodiment, the secure write blocking circuit also includes a logic circuit, coupled to the blocking circuit, that receives the block signal and a write enable signal and in response thereto generates a control signal to a write enable input of the nonvolatile memory device.

Issued: March 23, 2004

Inventor: Richard Dayan, *et al*

Assignee: International Business Machines Corporation (Armonk, NY)

US Patent: 6,711,689

Interception system and method

An interception system and method for performing a lawful interception in a packet network such as the GPRS or UMTS network. The interception system comprises an interception activation monitoring function, an interception activation and deactivation function, an interception data collection function and an interception data destination function. The interception data collection function can be implemented in an existing network node such as a GPRS support node, wherein an interception information is set in the corresponding PDP context, and the collection of the intercepted data is performed in response to the set interception information. Furthermore, the interception data destination function may be arranged in an interception browsing element arranged for browsing the intercepted database on an external command received from another network element comprising the interception activation and deactivation function. Thereby, browsing and managing of the lawful interception can be separated into different network elements.

Issued: March 23, 2004

Inventor: Martte Lumme

Assignee: Nokia Corporation (Espoo, Finland)

Notable Reference:

[1]   So-Lin Yen and Hong-Kuang Hwang; *Intelligent MTS Monitoring System.* Proceedings of the Annual International Carnahan Conference on Security Technology, Albuquerque, New Mexico, Oct. 12-14, 1994, Conf. No. 28, pp. 185-187.

US Patent: 6,711,680

Method of limiting key usage in a postage metering system that produces cryptographically secured indicium

A method and system for generating messages from which it can be verified that a variable does not exceed a predetermined limit. The message can be a postal indicium. A message originator, which can be a postage metering system, receives a message in the form $R^{-k\,(T)}$, where R is a trapdoor function, K is an integer equal to the limit, and T is a plain text, from a data processing center which maintains the inverse function R^{-1} in secrecy. The message originator computes $S_m=R^m(R^{-k\,(T)})$, where m is a current value of the variable, and incorporates S_m into the message. A verifier verifies that m<K by confirming that $R^{k-m}(S_m)=T$. The verifier cannot compute $R^{k-m}\,(S_m)$ for m<K since it does not have R^{-1}. For the same reason the originator cannot compute $R^{-k'\,(T)}$, k'>K, from $R^{-k\,(T)}$.

Issued: March 23, 2004

Inventor: Robert Cordery

Assignee: Pitney Bowes Inc. (Stamford, CT)

US Patent: 6,711,679

Public key infrastructure delegation

An approach for allowing a server to act on behalf of an original requestor (originator) which includes an approach for indicating the chain of servers through which the original request came. This provides a mechanism for a server to act as a "delegate" for a request made by an originator. This approach uses PKI constructs and relies upon public-private key digital signatures for verifying the validity if the "delegation" information. The approach described here allows the originator some control over the extent to which its identity can be used on its behalf by servers that it contacts and servers that are contacted on its behalf. The entire "delegation chain" is contained within the construct, allowing examination of the "path" that a request has taken in getting to a server from which service was requested.

Issued: March 23, 2004

Inventors: Richard Guski and Timothy Hahn

Assignee: International Business Machines Corporation (Armonk, NY)

Notable References:

[1] Szabo, Nick. *Delegation and Agreement Based Certification Policy.* 1997.

szabo.best.vwh.net/trust.html

[2] Hu, Yuh-Jong. *Agent-Oriented Public Key Infrastructure for Multi-Agent E-Service.* Emerging Network Technology Lab. Dept. of Computer Science, National Chengchi University, Taipei, Taiwan 116, 1999.

[3] Branchaud, Marc. *A Survey of Public-Key Infrastructures*, Department of Computer Science, McGill University, Montreal, Canada, Mar. 1997.

US Patent: 6,711,674

Method of watermarking configuration data in an FPGA by embedding the watermark corresponding to a macro obtained upon encountering a first watermark tag from the macro

A method for watermarking FPGA configuration data. Specifically, if an end user desires to use a macro from a macro vendor, the end user creates a design file containing a marked macro received from the macro vendor, rather than the actual macro. The end user then uses an FPGA programming tool to convert the design file into configuration data. Specifically, the FPGA programming tool processes the design file to detect marked macros. If a marked macro is detected, the FPGA programming tool embeds a watermark corresponding to the macro within the configuration data.

Issued: March 23, 2004

Inventor: James Burnham

Assignee: Xilinx, Inc. (San Jose, CA)

Notable References:

[1] Lach, J., W.H. Mangione-Smith, and M. Potkonjak. *FPGA Fingerprinting Techniques for Protecting Intellectual Property.* 1998, IEEE 199 Custom Integrated Circuits Conference, Proceedings of the IEEE 1998, pp. 299-302.

[2] Kahng, A.B.; J. Lach; W.H. Mangione-Smith; S. Mantik; I.L. Markov; M. Potkonjak; P. Tucker; H. Wang; and G. Wolfe. *Watermarking Techniques for Intellectual Property Protection* . Design Automation Conf., 1998. Proceedings, 1998. Page(s): 776-781.

US Patent: 6,711,414

Wearable computing device capable of responding intelligently to surroundings

Techniques and approaches that enable wireless communication devices, namely, wearable devices, to assist users in new ways by interacting with other devices or surroundings to notify users of things that would be of interest to users. In one aspect of the invention, wearable devices display information for users in response to surrounding signals. The surrounding signals can come from a nearby wireless transceiver that may be included in another wearable device, a terminal device or an isolated device provided in a setting. In another aspect of the invention, wireless communication or computing devices (e.g., wearable devices) can interact and perform social filtering. The users of the devices can then be suitably notified.

Issued: March 23, 2004

Inventors: Alexander Lightman and Thad Starner

Assignee: Charmed Technology, Inc. (Santa Monica, CA)

Charmed Technology, Inc
1431 Ocean Avenue, Suite 600
Santa Monica, CA 90401

Telephone: 310-458-3233

Fax: 310-458-2844

e-mail: info@charmed.com

www.charmed.com/bnuw1.htm

Charmed Technology is an MIT Media Lab spin-off and supplier of wearable Internet products, services and technologies. The Charmed Technology vision is to incorporate the unwired Internet into fashion, lifestyle and health applications by creating inexpensive wireless mobile devices that will allow individuals to access the World Wide Web anywhere and anytime through wireless technology. Charmed Technology will allow individuals to be connected to the Internet via their eyeglasses, necklaces, or lapel pin – or even a child's toy.

US Patent: 6,711,263

Secure distribution and protection of encryption key information

Secure distribution of a private key from a distributing unit to a receiving unit, based on providing each of the distributing unit and the receiving unit with a protecting circuit holding an original private key unique for the protecting circuit. The protecting circuit of the receiving unit is associated with a certificate holding information on the type of the protecting circuit. The protecting circuit of the distributing unit requests this certificate to verify the authenticity by using a public key, of a certificate authority, stored in the protecting circuit. Next, the protecting circuit determines, based on the type information of the certificate, whether the protecting circuit of the receiving unit represents a type of circuit that is acceptable for protecting the private key to be distributed. If the protecting circuit is found to be acceptable, the private key is encrypted and transmitted thereto. The received key is decrypted and stored in the protecting circuit of the receiving unit. In this manner, the private key is protected during transfer and may be distributed to and securely protected in one or more receiving units.

Issued: March 23, 2004

Inventors: Jan Olaf Nordenstam and Allan Hansson

Assignee: Telefonaktiebolaget LM Ericsson (Stockholm, Sweden)

US Patent: 6,711,262

Procedure for the control of applications stored in a subscriber identity module

A procedure for the control of applications stored in a user's subscriber identity module (SIM) in a data communication system that includes a data communication network, a terminal device connected to the data communication network and to which the subscriber identity module is connected, and an application control server that is connected to the data communication network. The SIM contains a stored application that makes use of the data communication network and that is used by way of the terminal device. A key list comprising one or more application-specific keys is stored in the user's SIM, and a corresponding key list is also stored in the application control server which is operable to control applications stored in the SIMs of multiple users of the network. The application stored in the user's SIM is activated or closed (or both) through the transmission, verification and use of keys stored in the key lists at the SIM and at the application control server.

Issued: March 23, 2004

Inventor: Harri Vatanen

Assignee: Sonera Oyj (Helsinki, Finland)

US Patent: 6,708,893

Multiple-use smart card with security features and method

A smart card that is adapted to partially include and employ a triply-secure algorithm for data exchange. The algorithm verifies a user's identity and his simultaneous membership in any groups that he has joined. For this purpose, the algorithm requires only a single insertion of the smart card and only a single input of the user's personal identification number. The algorithm can be used in smart cards or in computer networks for identity verification and membership proof. A combination of three different hard problems is used. The first one is based on integer factorization, such as the RSA authenticating technique. The second one is based on a discrete logarithm, and the third one is based on the coefficients of a polynomial function. In a typical application using smart cards, a certification authority (CA) establishes requirements for preparation and issuance of a multi-purpose card.

Issued: March 23, 2004

Inventors: Shervin Erfani and Jian Ren

Assignee: Lucent Technologies Inc. (Murray Hill, NJ)

Notable Reference:

[1]   Data Encryption Standard (DES) FIPS Pub 46-3, National Institute of Standards and Technology, reaffirmed Oct. 15, 1999, pp. 1-22.

US Patent: 6,708,273

Apparatus and method for implementing IPsec transforms within an integrated circuit

A secure communication platform on an integrated circuit. It is a highly integrated security processor which incorporates a general purpose digital signal processor (DSP), along with a number of high performance cryptographic function elements, as well as a PCI and PCMCIA interface. The secure communications platform is integrated with an off-the-shelf DSP so that a vendor who is interested in digital signal processing could also receive built-in security functions which cooperate with the DSP. The integrated circuit includes a callable library of cryptographic commands and encryption algorithms. An encryption processor is included to perform key and data encryption, as well as a high performance hash processor and a public key accelerator.

Issued: March 16, 2004

Inventor: Timothy Ober, *et al*

Assignee: SafeNet, Inc. (Baltimore, MD)

US Patent: 6,697,944

System and method for intrusion detection using a time domain radar array

A system and method for highly selective intrusion detection using a sparse array of time modulated ultra wideband (TM-UWB) radars. Two or more TM-UWB radars are arranged in a sparse array around the perimeter of a building. Each TM-UWB radar transmits ultra wideband pulses that illuminate the building and the surrounding area. Signal return data is processed to determine, among other things, whether an alarm condition has been triggered. High resolution radar images are formed that give an accurate picture of the inside of the building and the surrounding area. This image is used to detect motion in a highly selective manner and to track moving objects within the building and the surrounding area. Motion can be distinguished based on criteria appropriate to the environment in which the intrusion detection system operates.

Issued: March 23, 2004

Inventors: Larry Fullerton and James Richards

Assignee: Time Domain Corporation (Huntsville, AL)

Notable References:

[1] Harman, R.K. *Intrepid Micro Track leaky cable sensor.* Security Technology, 2002. Proceedings. 36th Annual 2002 International Carnahan Conference on, Oct. 20-24, 2002. pp: 191-197.

[2] Anderson, F., *et al. Ultra-wideband beamforming in sparse arrays.* IEE Proceedings-H, vol. 138, No. 4, Aug. 1991, 8 pages.

[3] Skolnik, M.I., *Introduction to Radar Systems.* McGraw-Hill, 1980, pp. 553-560.

[4] Frazier, *Surveillance Through Walls and Other Opaque Materials.* IEEE 1996 National Radar Conference, Ann Arbor, MI, May 13-16, 1996, pp. 27-31.

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