Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 6, No. 9. October, 2004

RFID – Facts and Myths, Risks and Security

Lukas Grunwald and Boris Wolf

Applications based on radio frequency identification (RFID) are significantly more prevalent. RFID, a short-range wireless technology, is used by access-control systems for authentication such as opening a door or deactivating a car's anti-theft system. In the retail industry, it is used extensively for applications such as self-checkout, intelligent shelf management for misplaced or perishable goods, receipt-less exchange and efficient warranty claim handling. Several governments are considering integrating RFID chips into ID cards.

Although all RFID systems have one thing in common – using wireless to transfer data – the technologies used in each application vary significantly.

For example, some systems embed their own processing logic directly on the chip. These 'active' RFID devices usually require a battery to power the chip. Other types are passive, drawing the energy necessary to transfer data from an RF field generated by a nearby RFID reader. These applications are more common – and less expensive because a battery is not required. Millions of passive RFID tags, for example, are implanted in animals (both wild and domesticated) as a form of identification. In October 2004, the U.S. Food and Drug Administration approved implantable, rice-grain-size RFID capsules for use in humans for health care applications.

The simple passive RFID chips used for animal tags cannot execute computer software. Instead, they can only send their stored number (e.g. serial number). More sophisticated, passive RFID chips contain RAM, allowing for the persistent storage of data. These are typically used in the retail industry.

The ability to access RFID chips from a distance is a major reason why they are used in manufacturing, as well as supply chain management and logistics. Goods can be identified and traced to their origin or to the customer, without the delays and errors inherent in manual handling. Another of the core differences between RFID and bar codes is its ability to provide information about an individual item, rather than just its type. Today's EAN numbers (bar codes) can only identify types or groups of goods. RFID can identify one specific product and provide associated data about it. This enables new applications such as receipt-less transactions, or a smart refrigerator recognizing food turned bad because the RFID tag provides the expiration date.

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…

November 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

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

Technical Editor and Illustrator: Les Owens.

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

Upcoming Mobile & Wireless and Wireless Security Events

The following are mobile and wireless, plus wireless security events, for late September and for October that may be of interest. Provided are the name, dates and venue of the event, plus URL.

MILCOM 2004
1st - 2nd November (and October 31st)
Monterey Conference Center
Monterey, CA
www.milcom.org

SANS CDI (Cyber Defense Initiative) South 2004
1st - 4th November 1-4
Sheraton New Orleans
New Orleans, LA
www.sans.org/cdisouth04

NGN 2004 (Next Generation Networks)
1st - 5th November
Boston Marriott Copley Place
Boston, MA
www.bcr.com/ngn/index.php

Cartes 2004 (Smart Cards)
2nd - 4th November
Paris-Nord Villepente Exhibition Center
Paris, France
www.cartes.com/en/index.htm

DIMACS Workshop on Mobile and Wireless Security
3rd - 4th November
DIMACS Center, Rutgers University
Piscataway, NJ
dimacs.rutgers.edu/Workshops/MobileWireless

Wireless Enterprise Summit
3rd - 4th November
Radisson SAS Hotel
Nice, France
www.oxfordevent.com/oic/wireless/event

Networking Decisions
3rd - 5th November
Hyatt Regency Atlanta
Atlanta, GA
networkingdecisions.techtarget.com

ACM Sensys '04 (Sensor Systems)
3rd - 5th November
Sheraton Inner Harbor
Baltimore, MD
www.cse.ohio-state.edu/sensys04

ISPCON Fall 2004
3rd - 5th November
Santa Clara Convention Center
Santa Clara, CA
www.ispcon.com/fall2004

31st Annual Computer Security Conference & Exposition
8th - 10th November
Marriott Wardman Hotel
Washington, DC
www.gocsi.com/annual

RFID Link
8th - 10th November
The Fairmont
Dallas, TX
www.wbresearch.com/rfidlinkusa/index.html

AFCEA TechNet Asia-pacific 2004 (19th Annual International Conference & Exhibition)
8th - 11th November
Sheraton Waikiki
Honolulu, HI
www.afcea.org/asiapacific/default.asp

WiCon Americas (Wireless Connectivity)
9th - 10th November
Santa Clara Convention Center
Santa Clara, CA
www.wiconamericas.com

GSM Americas Congress 2004
10th - 11th November
Hotel Inter-Continental Rio
Rio de Janeiro, Brazil
www.gsmconferences.com/gsmamericas/main_default.asp

LCN 2004 – 29th Annual Conference on Local Computer Networks
16th - 18th November
Embassy Suites
Tampa, FL
www.ieeelcn.org

1st IEEE Workshop on Embedded Network Sensors
16th November
Embassy Suites
Tampa, FL
www.cse.unsw.edu.au/~emnet

[Note: this event is held in conjunction with LCN 2004]

Upcoming Mobile & Wireless and Wireless Security Events (continued)

WLN 2004 (Wireless Local Networks)
16th November
Embassy Suites
Tampa, FL
wln2004.cs.bonn.edu
[Note: this event is held in conjunction with LCN 2004]

3rd Annual Wireless Broadband Forum
16th -17th November
Hinxton Hall Conference Center
Cambridge, UK
www.broadband-wireless.org/home.htm

Wireless Expo 2004
16th -17th November
On-line Event
Anywhere
www.wirelessexpo.net/wirelessexpo/default.asp

Information Assurance Conference (part of the E-Gov Institute's Homeleand Security Conference & Exposition)
30th November - 2nd December
Ronald Reagan Building & International Trade Center
Washington, DC
www.e-gov.com/events/2004/ia

Wi-Fi Planet Conference & Expo Fall 2004
30th November - 3rd December
San Jose McEnery Convention Center
San Jose, CA
www.jupiterevents.com/wifi/fall04/index.html

Some vendors are experimenting with RFID tags called "Smart Labels," which are attached to consumer goods. RFID tags are assigned different radio frequencies depending on their application. Smart Labels are usually of type ISO 15693 or ISO 14443A and operate in the 13.56 MHz frequency band. By contrast, tags used for access control and to identify animals operate at 156 KHz. Due to standardization efforts by EPC, global, one can expect these Smart Labels to replace current EAN numbers and bar code solutions in the long run.

Quote of the Month

"Time is the most valuable thing that a man can spend."

Theophrastus (371-287 BC)

Technical Issues And Risks

The conversion from classic tracking based on bar codes or block matrix codes to RFID seems tempting. Intuitively, one might think it possible to simply exchange barcode readers for RFID tag readers and keep the same back-end applications, with only a few adjustments to fix compatibility issues. Then the existing software could process the new numbers coming from the RFID tags, just like the numbers read from bar codes.

However, it is not that simple. Using RFID in the supply chain introduces new risks for both the vendor and its customers, as well as new opportunities. These risks need to be evaluated and then minimized or eliminated by adequate organizational or technical measures.

During initial testing of RFID tags, there was an attempt at bulk reading – large quantities of tags being read at once. For examples, bulk reading could immediately recognize all products on a palette upon arrival at a warehouse, and could check-out all the goods in a shopping cart at a supermarket by simply pushing it through an RFID gate. This turned out to be error-prone, however, as only about 70 percent of tags could be recognized reliably.

Sequential reading of tags one after another, on the other hand, does not have that trouble, although problems do remain. For example, some tags attached to metal foil or wrapped around products containing liquids may not be read correctly because of shielding and reflection effects.

RFID readers and gates can also cause problems. There is a certain latency, and this can be unacceptable in rapid throughput scenarios. Tags need to remain in the field for a specific amount of time before reading can finish.

Privacy Problems

Smart Labels may be read at any time, so technically it is not difficult to use them to identify a person. When tags are invisibly integrated into the product and remain active even after the purchase, an abuse scenario does not seem far-fetched. For example, they are often hidden inside the fabric of clothing. With no

Are You the Arcanist?

How many canonical 3x3 magic squares are there? They were to be composed of nine (9) consecutive integers, with every row, column and diagonal adding to the same number.

There is only one such magic square:

```
2 7 6
9 5 1
4 3 8
```

All 3x3 magic squares can be derived from this by rotation or by adding a constant.

No one submitted an answer.

This month ...

What are the next two digits in the following series: 6180339??

Hint: The ancient Egyptians, da Vinci and those learned in classical aesetics would easily recognize.

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

The proof follows:

1. If the magic square has nine consecutive integers, then subtracting the smallest integer less one will result in a magic square containing the digits 1 through 9 (if you're a programmer you can use 0 through 8).
2. Enumerate the number of valid combinations for each integer, “1” through “9”. For example, the digit “1” can only be combined with 6,8 or 5,9 to make 15. If you do this you will realize that only “5” is in 4 combinations, and therefore must be in the center. Only “2”,”4”,”6”,”8” can be in 3 combinations and therefore must go in the corners (one row, one column, one diagonal). This leaves “1”,”3”,”7”,”9” that can only be in two combinations each and therefore must go on the sides.
3. Place “2” in the top left corner (you can obtain any other corner by rotation). This fixes the placement of “8”.
4. Place “6” in the top right corner (you can obtain the other free corner by rotation). This fixes the placement of “4”.
5. The placement of the remaining four numbers is fixed by the need for all rows and columns to add to 15.

Note that you can easily create impossible magic squares in this fashion, e.g.:

```
X 6 X
X 5 X
X X X
```

Try as hard as you like, you will never get this one to work. However,

```
X 6 X
X 8 X
X X X
```

can be shown to work by the simple expedient of subtracting 3 from both known cells and rotating 180 degrees, leaving:

```
X X X
X 5 X
X 3 X
```

which fits the pattern described above and is therefore valid.

read-protection whatsoever, somebody wearing a tagged suit could easily be (re)identified by reading the unique serial number of the tag. This scenario is especially uncomfortable because the bearer would need special equipment to know if and when tags are being read. (For an alternate view on this scenario, see the “The RFID Bogeyman” in the **April 2004 issue** of *Wireless Security Perspectives*.)

Smart Labels contain a segmented EEPROM memory. The serial number (unique identifier) of the tag can be used as a unique database key for identifying a record in a central database. Product metadata (data about the product) or any other arbitrary information can be stored in a RAM area called the User Data Field (See **Table 1**).

Table 1: Memory Organization of the ISO 15693 Tag

Page	Byte			
	0	1	2	3
Administrative Data Field (unique identifier)				
0x00	User Data Field			
...	...			
0x3F	User Data Field			

System designers have good reasons for storing associated data in a database keyed by the serial number of the tag, rather than in the tag itself. For example, this can be used to supply the customer with elaborate background information about a specific product – more data than can be written onto the tag's memory. Another reason for storing information in a database rather than in the tag occurs when there is a need for data security. Access to databases can be much more easily controlled.

The Administrative Data Field (see **Table 1**) is designed to be written only by the manufacturer. This storage area contains the unique and unchangeable serial number. Details are shown in **Tables 2 and 3**.

Table 2: Coding of the Unique Identifier

Byte							
7	6	5	4	3	2	1	0
0xEO	MFR	Serial number					

Table 3: Coding of the Manufacturer ID

MFR-Code	Company
0x02	ST Microelectronics
0x04	Phillips Semiconductors
0x05	Infineon Technologies AG
0x07	Texas Instrument
0x16	EM Microelectronic-Mann SA

If RFID tags in clothing contained only the ID number of the garment itself, with all additional customer and product information stored in a data mining system at the retailer's shop, then there is no direct link between the person and the serial number – assuming access to the database is well controlled. If, however, the person wearing the garment also carries an RFID-based ID card (or embedded in their skin), it would be theoretically possible to read the name, age, address and other information from the card and link this information to the person. In this scenario, it would be possible for a competitor to collect information about "new" or old, "unfaithful" customers.

For good reason, privacy activists ask for ways to protect Smart Labels. However, the ISO15XXX standards do not address this issue. Although it is possible to define tags as read-only to at least prevent unwanted manipulation of data, it is not possible to delete these write-protected areas to protect privacy.

Deactivation

In Germany, the Metro corporation introduced an RFID deactivator after numerous protests from privacy activists and associations. In order for the deactivator to delete labels, the User Data Field must remain writable. Therefore, it is possible to use testing tools such as RF-Dump, originally developed for auditing of RFID integration testing and penetration testing, to modify the User Data Field arbitrarily. This introduces risks for Metro, as well as for the customer. The deactivator's effectiveness must also be questioned because the serial number in the Administrative Data Field is read-only by default and hence can still be used as a database key after the tag is 'deactivated.'

Tag Blocking

RSA Security has developed the "Blocker Tag," a hypothetical technique to effectively block RFID tags. In its initial version, the Blocker Tag was meant to disrupt the Anti-Collision algorithm of the RFID tags to protect the customer's privacy. With this approach, RSA Security would have delivered a denial-of-service tool, free to your door, with which one could have blocked Smart-Labels, as well as paralyzed entire supply chains. (For more information on the Blocker Tag, read "Addressing RFID Consumer Privacy Issues" in the **September 2003** issue of *Wireless Security Perspectives*.)

RSA now suggests "Soft-Blocking" instead. In this scenario, a second RFID label signals to the reader that it should not read the tag. Alternatively, the same results can be achieved by setting a standardized bit directly in the label. However, this concept seems to be marketing-hype, rather than a realistic solution. It just opens new security holes and therefore cannot increase the consumer's privacy in any way. The whole concept is based on complying with a convention. Somebody applying questionable methods for maximizing revenue will most likely not be hindered from abusing information stored on RFID tags by a 'gentlemen's agreement'.

Off-line Solutions

Not all Smart Label applications can make use of the Electronic Product Code (EPC) stored in the Administrative Data Block. Using an off-line system, inventory personnel may, during accounting of incoming items, electronically write product identity and metadata to the item's RFID tag from a database. In such case, the serial number must be stored in the writable User Data Area, but this poses new attack scenarios:

- Product data can be read and manipulated arbitrarily.
- Information such as the expiration date of perishable goods (e.g., foods and medication) can be modified. Therefore, a merchant – or even an attacker passing by the shelves with a bulk-write-capable tool – could change it.

- The smart shelf system (a thing of the future) is designed to recognize misplaced products. It would be possible to virtually misplace goods by modifying the tag data. In this scenario, the shop computer would notify the staff of a misplaced product, even though nothing was moved.

Another problem occurs when pricing or discount information is stored directly in the RFID tag. This design mistake, although well-known, is found frequently in online shopping systems where the price is calculated in the customer's browser. In the case of RFID systems, as well, the customer could manipulate the price, and this attack becomes even simpler when it is possible to transfer the serial number from a less expensive product.

Consumer Concerns

RFID-equipped customer cards also may be modified as well. Modifications to a card's data stored on its embedded chip becomes an issue when selling age-restricted materials such as movies or alcoholic beverages. When purchases are solely controlled by an RFID system, as is the case with self-checkout systems, an underage person could either modify his customer card or the product tag.

When the RFID tag remains active after the purchase, there is a risk for the consumer. The shop, as well as hacker tools, can write information into Smart Labels. As a proof-of-concept, RF-Dump comes with a cookie feature similar to implementations on the Web. With this feature activated, a special signature and a counter are placed in a free data cell as soon as an arbitrary RFID tag enters the realm of a reader running the software. Every time the tag (together with its carrier) re-enters the reader's field, the counter is incremented. This way, one can literally count how often a customer steps into a store. Even if a store does not give out or sell RFID-tagged items, it could easily operate a system for collecting this information – it might be interesting when combined with other data.

Conclusion

Solutions that store all data on the RFID chip ('off line') are vulnerable, since the data is accessible to virtually everyone. Shopping and product tracking systems based on this design have enormous risks unless they are encrypted. These risks may outweigh the advantages RFID technologies may seem to offer, such as greater customer convenience and better inventory management. Systems coupled with a secured online database are much better protected from manipulation and spying.

RFID has potential in emerging technology applications. It remains an open question whether or not smart household appliances (e.g., an intelligent refrigerator ordering food or a washing machine recognizing the red sock in a load of whites) will indeed be killer applications for this technology.

RFID is still at the beginning of a lengthy development period. Without antennas, the tiny RFID chips can neither be powered nor can they send information. This limits their usefulness, although this limitation may be necessary due to cost constraints.

Despite the technology's immense potential, RFID does not (yet) pose a serious risk for your privacy. In this context, it is surprising to hear RFID opponents' wildly exaggerated arguments and their decision to refuse certain products or to boycott stores using RFID technology.

In general, supply chain infrastructures are well-designed and implemented. Audits are performed, as is common for all security-relevant systems, to protect against data pirating, illegal manipulation and hacking attacks. Usually it is necessary to define attack scenarios, which can be analyzed and evaluated.

As long as the industry is reluctant to provide labels with a complete and effective deactivation feature, RFID tags have to be considered risky from a privacy perspective, and consumers should be made aware that they will be potential carriers of freely readable and writable memory.

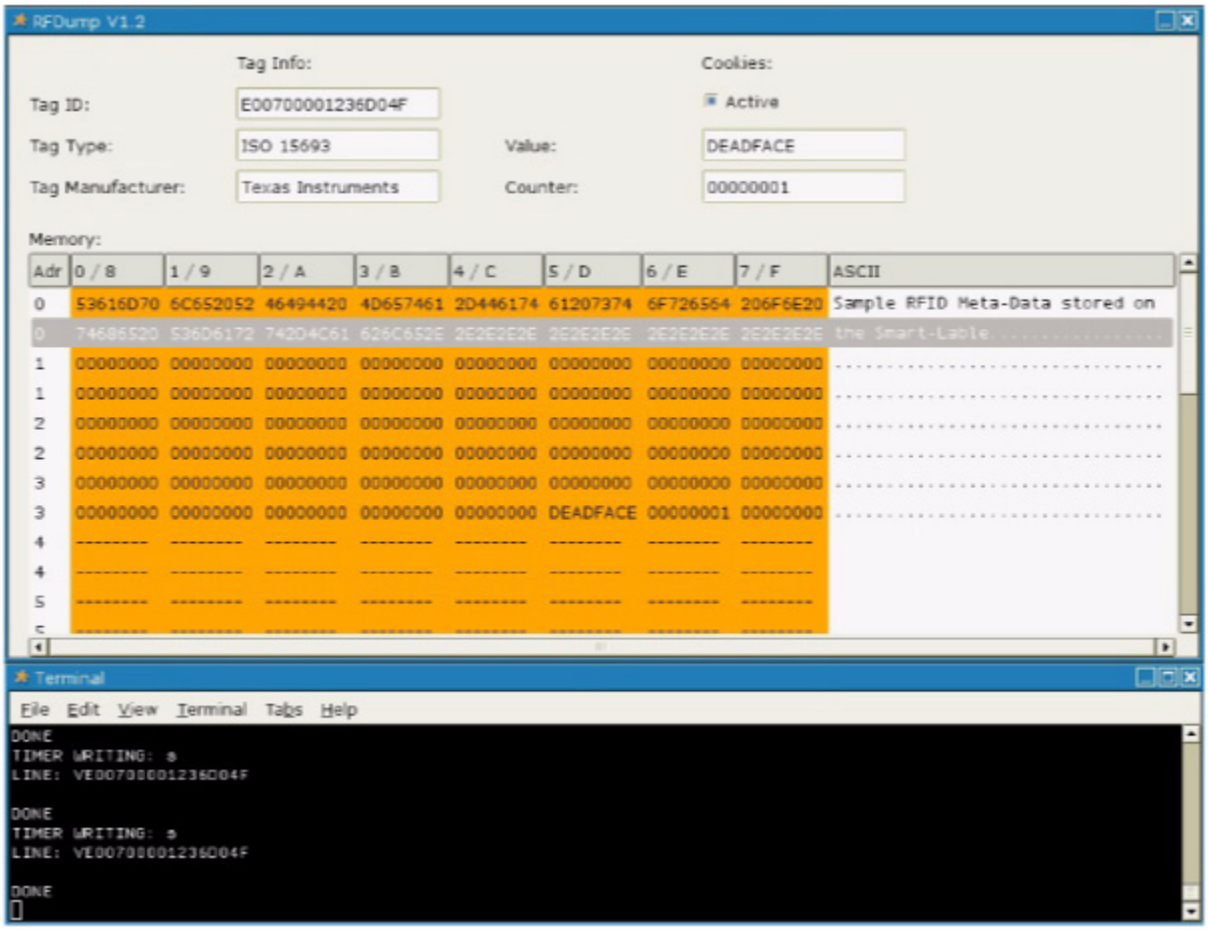
On the other hand, RFID does provide a competitive advantage already, through increased efficiency in logistics. There is the potential for new attacks and sabotage, but these risks can be evaluated and minimized by auditing to determine whether the systems are implemented correctly. For example, one could check whether it is possible to crash a back-end application with RFID tags containing (for proof-of-concept) malicious data sets. Another attack is to try to exploit the system by using specific patterns of invalid data, causing buffer overruns, a common technique used against internet applications.

About RF-Dump

The RF-Dump software developed by German consultant Lukas Grunwald began as a testing tool for auditing RFID integration and penetration testing (for revealing security weaknesses). **Figure 1** shows an example screen generated by RF-Dump. Data in the 'Value' field is shown as having over-written data in the 5/D cell on Memory Address Page 3.

This software was a big hit at the Las Vegas *Black Hat* security conference in July this year. RF-Dump is a free software download for Windows or Linux. Running on a laptop or PDA, this application allows anyone (anywhere) to read and write data within RFID tags of many types.

Figure 1: RF-Dump Screen Display



About the Authors

Mr. Grunwald is CTO of DN-Systems Enterprise Internet Solutions GmbH, a Hildesheim, Germany-based consulting firm specializing in security and Internet/e-commerce solutions for enterprises. Mr. Grunwald has worked in IT security for nearly 15 years and specializes in security of wireless and wired data and communication networks, forensic analysis, audits and active networking. He regularly publishes articles in specialist publications and participates in conferences such as Hackers at Large, Hacking in Progress, Network World, Internet World, Linux World (USA/Europe), Linux Day Luxembourg, Linux Tag, CeBIT and Blackhat Briefings.

Boris Wolf is a consultant at DN-Systems and is currently specializing in supply chain security and emerging RFID technologies. He is holding a master degree from the University of Hannover (Germany) in computer engineering and participated in research projects at Stanford University (California) focusing on peer-to-peer networks. He has been working in the field of designing and implementing database-driven enterprise applications with special focus on their security for more than five years now.

U–R–Linked

www.reed-electronics.com/ednmag/article/CA468418?pubdate=10%2F14%2F2004

A worthwhile link to follow is given above, revealing how very different RFID is from cellular technologies. Catch the latest issues in RFID, including conflicts in technical function, applicability factors, competition, standards-setting groups and opportunities in the ever-advancing technology march of the business world.

This site includes links for getting specific information about RFID-related products and services. A series of news clips provided in the "Applications Teaser" section sheds light on the many types of system designs already in motion.

Fraud and Security Patent News

US Patent: 6,810,250

Method of global roaming services using gateway location register in third generation mobile telecommunication networks

The present invention discloses a method of roaming services for global roaming subscribers in the third generation mobile telecommunication networks in which a visitor network GLR (Gateway Location Register) is connected to a home network GLR so that the home network GLR can download subscriber information from HLR (Home network Location Register) to the visitor network GLR. In this manner, the visitor network GLR is blocked from direct contact to the home network HLR in the roaming service about the terminal moved to other network and downloaded with the subscriber information stored in the home network HLR in which the terminal is registered via the GLR so that the subscriber information stored in the home network HLR can be prevented from being exposed by the visitor network GLR. The visitor network GLR is associated with the home network GLR only in contrast to conventional association with all HLR of the home network so that a signal track can be remarkably reduced. Furthermore, the visitor network GLR can be downloaded with programs for various application or intelligent network services provided in the home network so that the terminal can be provided with the same services in the visitor network as in the home network.

Issued: October 26, 2004

Inventor: Jin Jo, *et al*
Assignee: Korea Telecommunication Authority (Kyunggi-Do, Korea)

US Patent: 6,810,245

Intelligent remote software loading method for wireless portable communication device

This invention discloses a method for a wireless portable communication device having a version of native software to download a second version of native software maintained in a communication network memory by making memory space available in the memory of the wireless portable communication device for the second version of native software while maintaining communication with the communication network.

Issued: October 26, 2004

Inventors: Mark Hinds and Robert Mundschau
Assignee: Motorola, Inc. (Schaumburg, IL)

About WSP Patent Listings

The US Patent and Trademark Office (USPTO) frequently grants fraud and security patents that will be of interest to some of our wireless security practitioners. Each patent includes the invention title – linked to the corresponding USPTO web page. We brief ly describe it and provide, at minimum, its inventor(s) and assignee (owner).

With the listing of patents provided each month, one can see *who* is doing *what* in the world of wireless inventions. Moreover, it is often instructive to read issued patents, since they include patent claims, specifications, illustrations, detailed descriptions and cited references. Patents often include other references, and these are sometimes useful to broaden one's perspective of wireless communications and security.

If the wording in these is difficult to understand, recognize that the patent abstracts are generally provided in their raw legal-jargon form, straight from an attorney's word-processor. Sometimes we edit the abstracts for readability when the legalese is too impenetrable.

US Patent: 6,808,111

Terminal software architecture for use with smart cards

This invention discloses a terminal software architecture that accepts a card with a merchant application implemented. A terminal application is developed independently of the terminal. The terminal has an environment component including terminal hardware, an operating system, and an environment services layer that supplies one or more environment dependent services that are dependent upon at least one of the operating system and the hardware of the terminal. The terminal application is compatible with the card application and has a platform-independent portion that is independent of the environment component and a business logic layer that implements business policies associated with the terminal. The business logic layer makes calls to the terminal application through an access module and an application programming interface. The terminal application makes calls to the environment services layer through an access module and an application programming interface.

Issued: October 26, 2004

Inventor: Forough Kashef, *et al*

Assignee: Visa International Service Association (Foster City, CA)

US Patent: 6,807,633

Digital signature system

This invention is for a digital signature system that includes: (1) a data receiver for receiving an electronic document over a network; (2) an encryption key database and; (3) a signature processor in communication with the encryption key database and the data receiver. The encryption key database includes encryption key records, each being associated with a subscriber of the database and identifying an encryption key uniquely associated with the subscriber. The signature processor is configured for receiving an indicator of one of the subscribers and for deriving a digital signature from the received electronic data and the encryption key associated with the one subscriber. Upon receipt of electronic data and an indicator of one of the database subscribers, the digital signature system derives a digital signature from the received electronic data and the encryption key associated with the one database subscriber. Typically, the database subscriber is the originator of the electronic data, and the data originator identifies itself by providing the signature processor with a personal identification number assigned to the data originator. After the digital signature is derived, preferably the digital signature system then transmits the derived digital signature to the data originator.

Issued: October 19, 2004

Inventor: Patrick Pavlik
Assignee: Xign, Inc. (Pleasanton, CA)

US Patent: 6,807,431

Method and apparatus for integrated wireless communications in private and public network environments

The present invention is a communication system formed by a private network that includes a private wireless network. The communication system includes a public wireless network using a public wireless protocol, such as GSM, and includes public networks, such as PSTN, ISDN and the internet, using a wired protocol, such as IP. The private network also includes a local area network (LAN) and the private network connects to the public networks using a wired packet protocol, such as IP. The public and private wireless networks operate with the same public wireless protocol, such as GSM, and the private wireless network additionally operates with a wired packet protocol, such as IP. The communication system permits users to operate freely in both public and private wireless networks using standard mobile stations while achieving high private network data rates. The communication system uses normal wireless handsets or other mobile or fixed stations without need for any modifications.

Issued: October 19, 2004

Inventor: Leslie Sayers, *et al*
Assignee: Cisco Technology, Inc. (San Jose, CA)

US Patent: 6,807,428

Method and apparatus for time-based reception of transmissions in a wireless communication system

This invention discloses a method for segmented message transmission wherein each message is first divided into segments and the segments are fragmented. A segment parameter is applied to each segment, and a segment identifier to each fragment. The fragments are provided to a lower level for preparation into frames for transmission. One embodiment is applied to the transmission of short duration messages, such as control messages. On receipt of a frame within a segment, a timer is initiated having an expiration period. Receipt of a next frame in the segment stops the timer. Expiration of the expiration period for a timer indicates that a next sequential frame is lost.

Issued: October 19, 2004

Inventor: Lorenzo Casaccia
Assignee: Qualcomm, Incorporated (San Diego, CA)

US Patent: 6,804,376

Equipment employing watermark-based authentication function

This invention discloses means for an image, video or audio data to be encoded with both a frail and a robust watermark. The two watermarks respond differently to different forms of processing (e.g., copying the object may render the frail watermark unreadable), permitting an original object to be distinguished from a processed object. Appropriate action can then be taken in response thereto.

Issued: October 14, 2004

Inventors: Geoffrey Rhoads and Ammon Gustafson
Assignee: Digimarc Corporation (Tualatin, OR)

Notable References:

[1] Bender, *Applications for Data Hiding*. IBM Systems Journal, vol. 39, No. 3-4, 2000, pp. 547-568.

[2] Sharma, et al. *Practical Challenges For Digital Watermarking Applications*. May 3, 2001, pp. 1-10.

US Patent: 6,804,373

Method and system using renormalized pixels for public key and compressed images watermarks on prints

The present invention describes a method (and system) of watermarking a half-toned image, includes grouping pixels of an image into blocks each containing a plurality of pixels, using as many gray levels as there are pixels in a block to halftone the image formed in the same blocks of pixels, based on a data set formed by the gray levels of the blocks of the halftoned image, generating at least one of a digital signature and a compressed version of the image, to form a generated unit, and inserting the generated unit in the halftoned image to form the watermark, by selecting how a predetermined number of pixels in a block are placed in the block.

Issued: October 12, 2004

Inventors: Charles Tresser and Jean-Marc Gambaudo
Assignee: International Business Machines Corporation (Armonk, NY)

Notable Reference:

Fu, et al. *Data Hiding for Halftone Images.* Proceedings of SPIE-Security and Watermarking of Multimedia Contents II, Jan. 24-26, 2000, pp. 228-236.

US Patent: 6,804,357

Method and system for providing secure subscriber content data

This invention is for a personalized smart card, in which public and private cryptography keys are stored. The keys are used to securely request and receive subscriber content data from a service provider using a remote control device.

Issued: October 12, 2004

Inventor: Ari Ikonen, *et al*
Assignee: Nokia Corporation (Espoo, FI)

US Patent: 6,804,331

Method, apparatus, and computer readable media for minimizing the risk of fraudulent receipt of telephone calls

This invention is for a method, apparatus, and computer-readable media for minimizing the risk of fraudulent receipt of telephone calls. The invention provides a method of minimizing fraudulent receipt of telephone calls, with the method including at least the following. One or more authenticated voice samples are associated with at least one person. The person then submits at least one test voice sample during a login process to obtain authorization to receive telephone calls. Each test voice sample is captured and the differences between the test voice sample and the one or more authenticated voice samples is quantified. Depending on the degree of difference between the at least one authenticated voice sample and the test voice sample, the person's request for authorization to receive telephone calls or training is dispositioned. Apparatus and computer-readable media to realize the above function are also provided herein.

Issued: October 12, 2004

Inventor: Jill Vacek, *et al*
Assignee: West Corporation (Omaha, NE)

Notable References:

1) Voicelog. *FCC Acknowledges Validity, Value of Automated Third Party Verification.* Press Release, www.voicelog.com, Aug. 24, 2000.

2) *Fingerprint and Eye Iris Pattern Identification Software.* Libraries and Source Code, Neurotechnologija, Ltd., www.neurotechnologija.com, Apr. 15, 2002.

US Patent: 6,803,851

Method for carrying out a keyless access authorization check and keyless access authorization check device

The present invention describes a method and device for checking keyless vehicle access authorization of an operator. The method includes transmitting a code signal from a base station to a mobile identification (ID) transmitter carried by the operator. In response to receiving the code signal, the ID transmitter performs an action which is indicative of a reply signal that is detectable by the base station. The difference of a signal characteristic between a reference code signal monitored at the base station and the reply signal received by the base station is then determined. The signal characteristic correlates with signal propagation time, changing as a function of the distance between the base station and the ID transmitter. The distance between the base station and the ID transmitter is then determined on the basis of a relative determination based on the difference of the signal characteristic between the reference code signal and the reply signal.

Issued: October 12, 2004

Inventor: Detlev Kramer, *et al*
Assignee: Leopold Kostal GmbH & Co. KG (Ludenscheid, Germany)

Notable Reference:

Merrill, I. Skolnik. *Introduction To Radar Systems*, International Student Edition, Second Edition. McGraw-Hill International Book Co. Copyright 1981, pp. 80-87.

US Patent: 6,802,013

Cryptographic access and labeling system

This invention discloses an integrated, modular computer program for the encryption and decryption of files using conventional encryption algorithms and a relational key generated by the system. The computer program system also generates a series of labels that are encrypted and appended as a trailer to the encrypted message. The encrypted labels provide a history behind the particular encryption and they can be individually selected, separated, and decrypted from the total file. A rule-based expert system is utilized as an intelligent label selection system to minimize message sensitivity. An access control module permits a user with a preassigned passphrase to have access to the encryption or decryption portion of the program by comparing a generated vector or key with a partially decrypted version of a second vector or key stored on a portable storage medium such as a floppy disk. If successful, the access control module creates a main key that is then used throughout the remainder of the program to encrypt or decrypt the labels. Part of the encryption or

decryption process utilizes an internal, reproducible, but irreversible scrambling subroutine in which the bytes of an initializing vector are successively Exclusive 'OR'ed with one another and then the result concatenated to the initializing vector until all of the bytes have been so treated, and then the process repeated an integral number of times depending upon an input variable called a *spinup number*.

Issued: October 5, 2004

Inventor: Roy Follendore III
Assignee: Same

US Patent: 6,802,004

Method and apparatus for authenticating content in a portable device

The present invention discloses a method and apparatuses for authenticating portable device content. First, the portable device receives content from a computer and a signature certificate. The signature certificate is derived from content after the content successfully passes a watermark screening process. The portable device compares the received signature certificate to the received content. The content is only played in the portable device when the received signature certificate authenticates the received content as passing the watermark screening process.

Issued: October 5, 2004

Inventor: Mark Gross, *et al*
Assignee: Intel Corporation (Santa Clara, CA)

Notable Reference:

SDMI Portable Device Specification, Part I, Version 1.0; PDWG Los Angeles; Jul. 8, 1999, pp. 1-35.

US Patent: 6,802,001

Method of incrementally establishing an encryption key

The present invention describes a method for determining an encryption key used by two or more parties for encrypted communications in a manner that prohibits any of the parties from forcing the final value of the encryption key. The encryption key is determined based on numbers exchanged by the parties using a key generation function, such as the Diffie-Hellman algorithm. To prevent any party from forcing the final value of the encryption key to a desired value, a first party divides its number into a plurality of parts, which are transmitted incrementally to the other. After transmitting a first part, the first party waits for receipt of at least a part of a second exchanged number from another party before the first party transmits the remaining parts of its exchanged number.

Issued: October 5, 2004

Inventor: Paul Dent
Assignee: Ericsson Inc. (Research Triangle Park, NC)

Notable References:

[1] Shi, et al. *Signature based approach to fair document exchange.* Communications, IEE Proceedings, Vol. 150, Issue 1, Feb. 2003, pp. 21-27.

[2] Lin, et al. *Three-party encrypted key exchange without server public-keys.* Communication Letters, IEEE, Volume 5, Issue 12, Dec. 2001, pp. 497-499.

[3] Moreau. *Probabilistic encryption key exchange.* Electronics Letters, Vol. 31, Issue 25, Dec. 7, 1995, pp. 2166-2168.

US Patent: 6,801,606

Fraud monitoring system

This invention is for a fraud monitoring system that detects fraudulent or potentially fraudulent usage of a telecommunications network. Each call connected by way of one of the digital main switching units of the network has an associated billing record transferred to a fraud management system. The fraud management system compares the origin and destination of the call with a known usage pattern for the originator. If other indications are that the call is of a fraudulent nature and if the call deviates from the known usage pattern, an alarm can be forwarded to an operator. The user profile used to determine normal calling behavior is updated over a period of time in respect of calls determined as not fraudulent. An initial user profile may be generated from historic billing records.

Issued: October 5, 2004

Inventor: Alexander Edwards
Assignee: Azure Solutions Limited (Ipswich, Great Britain)

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