Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 5, No. 7. July, 2003

Security and Privacy in RFID

Tim Kridel

June 2003 was a watershed month for RFID (Radio frequency identification) technology. Two of the world's largest companies, Microsoft and Wal-Mart, committed to supporting the nascent short-range wireless technology, whose current applications include tracking inventory, theft prevention and facilitating cashless payments.

RFID uses low power and unlicensed spectrum to transmit a few bytes of information about the object to which the RFID tag is attached. The information is pulled from the tag by a nearby RFID scanner which relays it to a central database which can, for example, track shipments of blue jeans as they leave the factory or as they are received at the distribution center.

Microsoft's initial work on RFID will focus on manufacturing and retail supply chain applications. Wal-Mart has asked its top 100 vendors to add RFID tags to crates and pallets by January 2005. Wal-mart says that requirement translates into about 1 billion tags, five times more than Texas Instruments has shipped since it entered the RFID market. Those volumes should drive the cost of an RFID tag, currently between 30¢ and 50¢, down closer to the 5¢ point where more retailers can make a business case for adopting the technology, partly as an alternative to bar codes.

The announcements by Microsoft and Wal-Mart quickly created a sense of bullishness. Allied Business Intelligence, for example, conservatively estimates the RFID market to be worth $3.1 billion by 2008, up from about $1.3 billion today. One AMR Research analyst went so far as to predict that RFID spending will be "bigger than Y2K. I imagine there will be a rush on investing in RFID."

Even with widespread adoption of RFID years off, some users already are worrying about the privacy implications of any technology used for tracking. Increased focus on security, in response to recent terrorist activity, has citizens watching for needless erosion of their rights and privileges under the guise of advancing technology. In April, for example, Benetton was inundated with calls from privacy advocates after the Associated Press ran a story on the retailer's plans to use RFID to track clothing from factories to stores. "It's a very image-sensitive issue," a Benetton spokesman told the AP.

In early July 2003, Wal-Mart scrapped plans to test an RFID-based "smart shelf" system, which would track products in stores. The company claimed this was not a response to privacy concerns but a decision to focus on RFID in warehouses first. Nevertheless, the issue of privacy and security in RFID will grow as more companies adopt the technology.

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…

August 22nd, 2003.

Future Topics

Wireless Flash Memory Security • Personal Area Network Security • Radius for Wireless • 3G Security • Public Keys & Wireless • Security for Mesh Networks • Security Issues in Ad hoc Wireless Networks • Security for Fixed Broadband Wireless

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.

Defcon 11 (Hacker event)
1st- 3rd August 2003
Alexis Park
Las Vegas, NV
www.defcon.org

iWirelessWorld
4th- 5th August 2003
Hilton Universal City
Los Angeles, CA
www.iwirelessworld.com

12th USENIX Security Symposium
4th- 8th August 2003
DC Convention Center
Washington, DC
www.usenix.org/events/sec03

WirelessWorld and Pocket PC Summit Hong Kong
6th- 7th August 2003
Hong Kong Convention & Exhibition Center
Hong Kong
www.wirelessworld.com

IEEE Radio and Wireless Conference
10th- 13th August 2003
Hilton Boston Logan Airport
Boston, MA
rawcon.org

ECC 2003 (The 7th Workshop on Elliptic Curve Cryptography)
11th- 13th August 2003
University of Waterloo
Waterloo, Ontario, Canada
www.cs.utah.edu/flux/cipher/cfps/cfp-7thECC.html

WESCON 2003
12th- 14th August 2003
Moscone Convention Center
San Francisco, CA
www.wescon.com

SANS Rocky Mountain 2003
14th- 19th August 2003
Hyatt Regency Denver
Denver, CO
www.sans.org/rockymountain03

Crypto 2003 (23rd Annual Cryptology Conference)
17th- 21st August 2003
University of California
Santa Barbara, CA
www.iacr.org/conferences/crypto2003

New Security Paradigms Workshop 2003
18th-21st August 2003
CSF Conference Center, Swiss Institute
Ascona, Switzerland
www.nspw.org/current

WISA 2003 (The 4th International Workshop on Information Security Applications)
25th- 27th August 2003
Shilla Hotel
Jeju Island, Korea
icns.ewha.ac.kr/wisa2003

Mobile Data Services World Forum
26th- 29th August 2003
Grand Hilton
Seoul, Korea
www.mobiledatakorea.com/html/flash_index.htm

WISPCON Euro (Wireless Internet Service Provider Conference)
27th- 29th August 2003
Holiday Inn
London, UK
www.wispcon.info/Euro/sponsorships/badge.html

How RFID Works

RFID systems vary by vendor, but the two key parts are the tag and the reader (also called the scanner). The reader can scan multiple nearby tags simultaneously. Its range varies by application, but generally is between a few inches and 20 feet, depending on factors such as the radio frequency used. An example of range-specific application is FedEx drivers wearing RFID wristbands which automatically unlock their truck doors as they approach, so they do not have to put down their packages.

RFID tag readers are typically linked to a central database maintained by the tag owner (Wal-Mart, for example), but they can also be linked to other organizations, such as banks and credit bureaus.

There are two types of RFID tags: passive and active. With passive tags, which do not need a power source, the tag reader uses RF energy to 'excite' the tag into reflecting back its few bytes of embedded data. Active tags use a built-in power source, usually a battery, to transmit their stored data. Tags can be as small as 0.4 mm square [1], tiny enough that some vendors have proposed embedding them in checks, medical documents and other paperwork.

RFID uses a variety of unlicensed Industrial, Scientific and Medical (ISM) bands, particularly 900 MHz and 2.45 GHz, which are already widely used by other applications. As a result, RFID can leverage ample supplies of low-cost, off-the-shelf hardware, which helps companies make a business case for using the technology. For example, the cost of installing readers at a gas station with four pumps runs about $14,000, and the cost of a RFID-equipped key-ring tag runs about $5, although most retailers give them away in order to encourage use.

Some types of tags are read-only, while others can have data added or updated, such as when a product leaves a clothing manufacturer's distribution center for shipment to a retailer's warehouse, or when a passenger's luggage is transferred between planes during a layover. For example, later in 2003, Delta Air Lines will test an RFID baggage-tracking system in conjunction with the U.S. Transportation Security Administration. The 30-day trial will use more than 40,000 tags in the 900MHz band. Tags will be provided by Matrics and SCS.

For consumer applications such as cashless payments, RFID is a user-friendly technology. One of the most widely used applications is Speedpass. Users wave an RFID-equipped key wand in front of a reader embedded in an Exxon gas pump or a McDonald's cash register. Although the Speedpass wand tells the reader which checking or credit card account to use for the transaction, the account information is not stored in the fob. Users also are not required to enter a PIN as an added security measure, and they can have the wand programmed to tell the reader whether or not a receipt is always necessary.

Is RFID Secure?

RFID's promises of limited human intervention and ubiquity on par with the bar code will raise the eyebrows of any security expert. Examples of potential concerns include:

- Can a retailer walk through a competitor's store with an RFID reader and scan the inventory?
- What happens if an RFID tag is stolen?
- RFID readers are widely available in kit form. How long before hackers scan nearby tags?
- Clothing retailers such as The Gap are testing RFID. If the tags are inexpensive enough to leave in clothes after the sale, could a marketer or researcher put an RFID reader in a public place to study *who* is wearing *what*?
- What type of device is necessary to alter the information in the RFID tag, and how long before RFID cloning devices appear in 2600 Magazine or in Nuts & Volts – for educational purposes, of course?
- At what point will we hear of hi-tech crooks with spoofed tag readers or cloned tags, ripping off innocent folks at the self-service gas pump?
- What happens if RFID tags are switched, such as from luggage that has passed airport security to a bag with a bomb?

Surprisingly, some vendors and users do not see RFID as being inherently risky. "We feel it is secure because of the encryption of the numbering system that's within each transponder," said Rick Ellison, marketing, pricing and technology manager at Mobil, said at a 1998 roundtable. Others show little fear of drive-by hacks similar to those popular today in Wi-Fi. "We have built-in encryption technology to prevent the data from being captured via airwaves," said Joe Pearson, retail program manager at TI.

Balancing Security and Cost

But other RFID vendors argue that security remains the greatest barrier to widespread adoption. The catch is that improved security can increase the cost of RFID. The same challenge hamstrings ubiquitous computing, which also needs to balance security with device costs. See the **May 2003** issue of *Wireless Security Perspectives* for a detailed discussion of ubicomp security.

Part of the challenge is to improve security without requiring expensive processors or extra memory. By some estimates, a coprocessor necessary to handle schemes such as RSA adds about 26¢ to the manufacturing cost of an RFID chip, even in large volumes.

Some early RFID systems used symmetric keys, but all tags were programmed with the same code [2]. The drawback is that an intercepted key or stolen reader can compromise every part of the system that relies on the same key. Re-keying a single device is one thing. Re-keying hundreds of thousands or millions is another.

A public-key approach reduces the chances that theft can compromise the entire system. NTRU Cryptosystems, for example, uses a public-key encryption architecture that the company says is still affordable because it does not require an expensive, dedicated coprocessor to crunch complex algorithms. (Our **October 2000** issue of *Wireless Security Perspectives* includes details about NTRU's 'Lattice' cryptography).

Another, low-tech way to thwart security breaches is to supplement RFID with other technology [3]. Two or more technologies working together could possibly provide better security than any of them could alone. For example, a terrorist posing as a baggage handler is less likely to try using a security-cleared tag (from a piece of luggage) – to get a bag carrying a bomb onto the plane – when it is designed not to be reusable. Characteristics of the luggage, such as its weight, could also be recorded, and bags which did not match could be manually checked.

Conclusion

Like all wireless technologies, RFID is a broadcast radio device that requires a robust, well-engineered and well implemented cryptographic scheme for adequate security. RFID systems in place today may be highly vulnerable and susceptible to fraud and abuse. Existing holes may ultimately drive up the per-tag cost to a point that it breaks the business case for many potential users. However, for some applications, the security threats are not serious enough to stop the use of the technology.

The fact that vendors and users recognize the importance of security is a sign that RFID development will continue. RFID developers will hopefully have learned from the cautionary tale of Wi-Fi, where insufficient attention to security has slowed the technology's adoption, even though equipment prices continue to plummet. Cheaper is not always better.

RFID may be secure for some time into the future, since so much attention is on WiFi insecurity instead – providing a safe haven for the RFID designers and users and the existing 'security through obscurity.' Meanwhile, privacy concerns will mount. History will likely repeat itself again.

Cooking with RFID

According to the CASPIAN newsletter, some consumers, worried about their privacy, are considering ways to disable RFID chips. Cooking them in a microwave for 7 seconds is effective. It doesn't work well for large items, those containing metal or those that are sensitive to heat, however. Also, the chip may be fried, but there is also a risk of personal injury while removing it from the oven, if the item has gotten hot.

CASPIAN speculates that eventually, a hand-held disabler will be developed. But if it is sold by Wal-Mart, will it have an embedded RFID chip?

References

[1] K. Takaragi, *et al. An Ultra Small Individual Recognition Security Chip*. IEEE Micro, Nov.- Dec. 2001, pp. 43-49.

[2] N. Raza, *et al. Applications of RFID Technology.*. Institute of Electrical Engineers, London. 1999, pp. 1-5.

[3] A. Cerino and W. Walsh. *Research and Application of Radio Frequency Identification (RFID) Technology to Enhance Aviation Security.* IEEE, 2000, pp. 127-135.

"Five or ten years from now, we won't worry about communication with wires; you'll just open your laptop or PDA and the data will be there."

— Teresa Meng, Professor, Stanford and Founder of Atheros

Radio Security for Software-Defined Radios

Chih Fung Lam, Kei Sakaguchi, Jun-ichi Takada and Kiyomichi Arakai

Last month, we introduced the concept of SDR (Software Defined Radio), and Thia Rajagopalan gave a perspective on over-the-air (OTA) software download for SDR. He provided an architecture to allow OTA – which was primarily motivated to prevent or reduce costs associated with equipment bug fixes. This month, researchers at the Tokyo Institute of Technology provide a security architecture that includes cryptographic mechanisms and GPS receiver capabilities to ensure that a software-configurable SDR terminal ain't mis-behavin'.

In a software-defined radio (SDR), fundamental attributes (e.g, modulation schemes, frequency, output power and upper-layer protocols) can be changed significantly by loading software that controls, for example, the binary code for baseband modules, upper-layer communication protocols and the settings for IF/RF controllers.

The drawback to SDR's flexibility is the potential security risk of unauthorized or malicious modification of the software. Minimizing that risk is challenging, because current certification methods (developed for non-SDR radios) are not applicable to SDR equipment, and different countries have different radio regulations.

These challenges increase the difficulty of developing a security architecture that accommodates SDR.

An example of this type of challenge is Class III Permissive Change (C3PC), which the FCC proposed in 2001 [1]. C3PC requires testing all combinations of hardware and software. The number of possible combinations, now and even more so in the future, makes performing such a comprehensive test infeasible. C3PC also does not consider the fact that radio regulations vary by country, so a C3PC-certified SDR terminal may be non-compliant when its user roams to a country with different SDR regulations.

Regulatory certification also was not considered during the design of SDR software with reconfigurable architectures such as TRUST [2] and Mobile VCE [3]. The assumption that software is certified before it is distributed by the system does not apply to SDR equipment, such as a set-top satellite TV receiver or a Bluetooth device. These types of devices do not reconfigure through a communication system. They highlight the need for a standardized security system applicable to all types of SDR equipment.

A new SDR security architecture also requires a new software-distribution method. The conventional approach – Secure Download Framework [4] – assumes that, like the firmware in today's radios, SDR software is created and distributed only by the hardware manufacturer. If the market for SDR software flourishes, then third-party vendors should be able to sell their software without depending on hardware vendors. After all, flexibility is part of SDR's *raison d'être*.

An ideal SDR security architecture enables separate hardware and software certification. It also allows flexible software distribution.

The approach described in this article comes from a university research project which proposes migration toward these ideals by requiring architectural changes in all SDR terminals. These changes include addition of system software designated as the Radio Security Module (RSM), [5, 6].

A desktop PC was used to model the complexity of RSM, including encryption. Testing also included a PDA, to show the viability of RSM on handheld devices.

Proposed Hardware Architecture

The proposed SDR terminal contains an Automatic Calibration Unit (ACU) [7, 8] and the RSM. The ACU is essentially an RF manager. Due to the expense of wideband Analog-Digital converters, adjustable analog RF will likely be used for SDR in the near future. The analog RF parameters controlled by the ACU are RF frequency and output power. The RF output signal is fed back into the ACU for runtime radio regulation check. Radio regulation parameters being monitored include:

- Center frequency
- Bandwidth
- Output power
- Adjacent Channel Power Ratio (ACPR)

The ACU checks for compliance with guidelines set by a Telecommunication Certification Body (TCB). The FCC, for example, is a TCB in the United States. Each of the 192 countries currently using wireless have their own TCB.

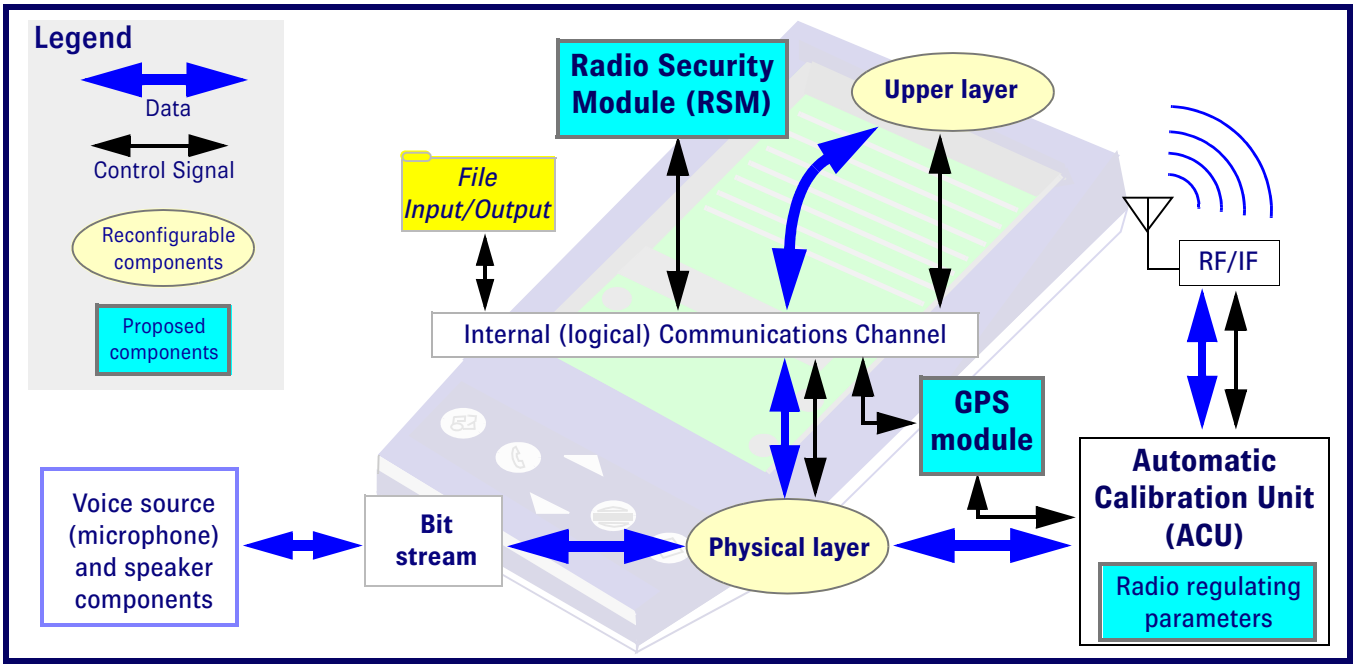
If minor incompliance is found, the ACU uses a built-in pre-processor to adjust it. If major incompliance is found, the ACU will disable the RF output. The RF module in **Figure 1** illustrates an analog module adjusted by parameters under the control of ACU.

The RSM is trusted system software which cannot be reconfigured. It manages the life-cycle of software in the terminal, including installation, storage, operation and termination. To perform these operations, the RSM contains both user-accessible and user-inaccessible components.

User-accessible RSM components are:

- A hardware digital certificate,
- a unique hardware identity (IdHW) and,
- a hardware public-key (PkHW).

Figure 1: RSM in an SDR terminal



User-inaccessible components are:

- A corresponding hardware secret-key (SkHW),
- the public-keys of all TCBs (192 countries),
- GPS range of each country (latitude and longitude values which enclose the area),
- the software's current geographical region and,
- encryption components (encryption algorithm).

User-accessible components would be used to download new software. User-inaccessible components can only be accessible by the RSM and are only updatable by hardware manufacturers.

In the sections and illustrations below:

$DS_A[D]$ represents the digital signature of message *D* signed by *A*.

Example: $DS_{SWM}[IdHW]$ represents the digital signature composed from the Hardware ID, signed by the software maker.

$E_k[D]$ denotes encryption of message *D* by using key *k*.

[D,H] represents the concatenation of messages *D* and *H*.

$V_K[DS]$ expresses verification of digital signature DS, using key K.

During installation, the RSM uses a digital signature to verify the software's source. Following verification, the software remains in storage, where access is limited to the RSM. At the user's command, the RSM activates the software by flashing the FPGA (Field Programmable Gate Array) and DSP (physical layer), and by installing the upper-layer protocol software.

While operating, the RSM uses random GPS position checks to limit the software's operation to the specific geographic region in which it is authorized to operate. If the current GPS position is outside that region, the RSM tells the ACU to suspend the software.

Hardware Certification

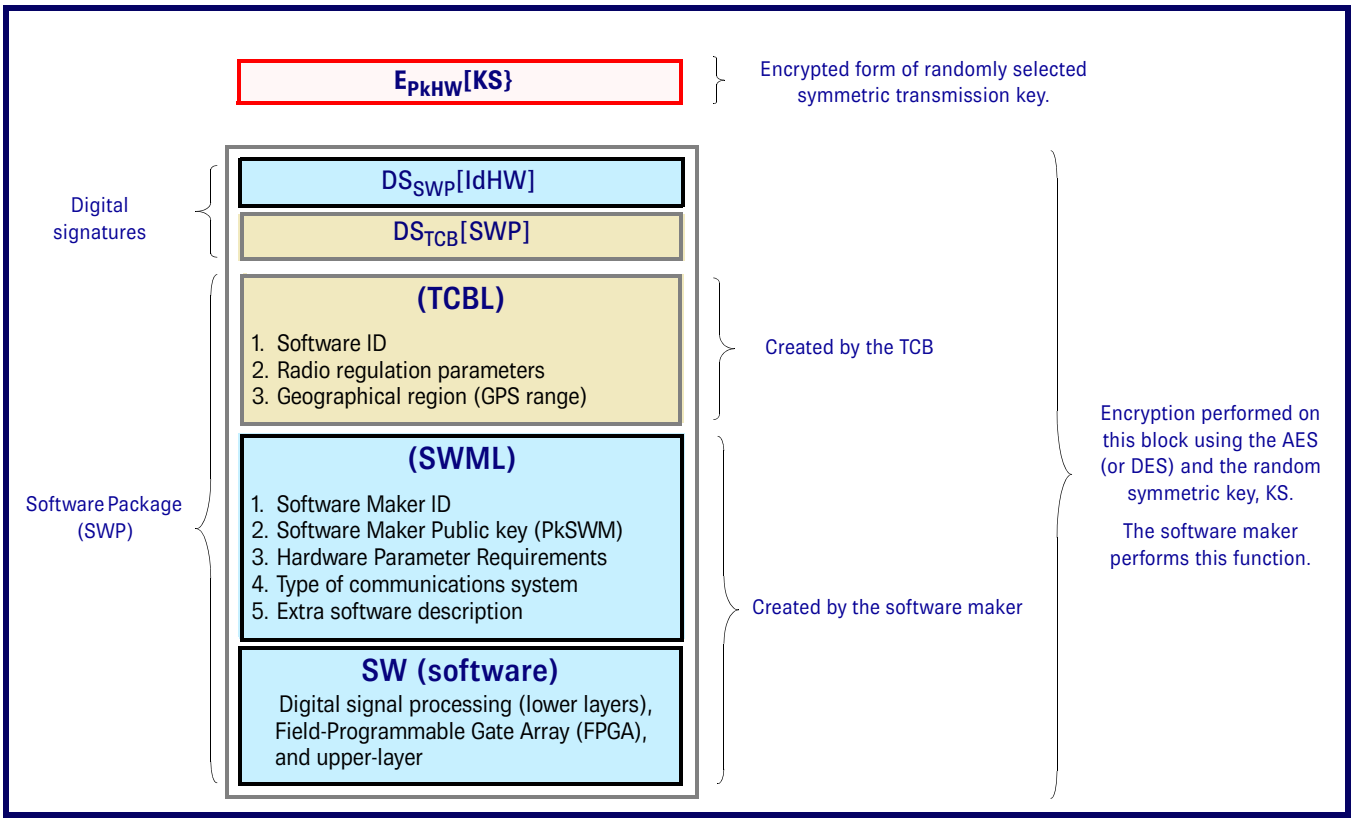
The hardware vendor sends a sample of the SDR terminal to the regulatory bodies (TCBs) in the countries where the device will be sold. The regulators check the RSM and ACU functions, as well as parameters unrelated to the software, such as spurious emissions. After the regulator certifies the terminal, the hardware vendor gives each production unit a unique hardware ID (IdHW) and a set of PkHW and SkHW keys. The regulator creates a unique hardware digital signature for each unit – i.e. $DS_{TCB}[IdHW,PkHW]$ (digital signature comprising the Hardware ID and Hardware Public Key, signed by the TCB) – which is given to the vendor to embed into each terminal.

Software Lifecycle

Each software load gets a software-maker label (SWML) and a TCB label (TCBL) in XML format. Details of these are shown in Figure 2. The SWML contains the software maker's PkSWM and a description of the software. The TCBL contains regulation-related radio parameters and information about the geographical region where the terminal is authorized to operate.

Figure 3 shows the software's life cycle. The software maker submits software and an SWML to regulators in country A, which uses a hardware emulator to test the software. If it complies, the regulator issues a TCBL, which contains the latitude and longitude coordinates for the region where the software is authorized to operate. After certification, the TCBL, SWML and software are called a Software Package (SWP). In the final step of the software-certification process, the regulators create the DS_{TCB}.

Figure 2: Downloaded Software



A hybrid encryption scheme is used during software download, which begins by transmitting IdHW, PkHW and DS_{TCB} to the software maker. The software maker verifies DS_{TCB}, and then uses the IdHW to create a DS_{SWM} and encrypts both digital signatures (DS_{SWM} and DS_{TCB}) together with the Software Package, using AES (or DES) and using a random symmetric key. The symmetric key (KS) is then encrypted using the PkHW and sent with the E_{KS} [DS_{SWM}[IdHW],DS_{TCB}[SWP],SWP] (see **Figure 2**).

The software download is followed by installation, which the RSM does in the following steps (which also are illustrated in **Figure 3**):

- Decryption of KS by SkHW (hardware secret key) in RSM,
- Decryption, using KS, of: E_{KS} [DS_{SWM}[IdHW],DS_{TCB}[SWP],SWP]
- Verify DS_{TCB}[SWP] using $PkTCB_A$,
- Verify DS_{SWM}[IdHW] using PkSWM in SWML,
- Store software (SW), with access rights limited to the RSM.

At the user's command, the RSM performs operating processes in the following manner:

- Operation of the software (flashing FPGA and DSP, etc.)
- Setting allowable geographical region in RSM (in this case, the geographic region of TCB_A)

When the software is running, the RSM checks if the current GPS coordinates are within the allowable GPS range. If any processes malfunction, the RSM tells the user to download the software again.

Global Roaming

When the terminal moves from country A to country B, its current GPS value falls outside the allowable range, prompting the RSM to suspend operation.

[DS_{SWM}[IdHW], DS_{TCB}[SWP],SWP]$_B$ are downloaded (or can be loaded from local storage) in order to operate in country B.

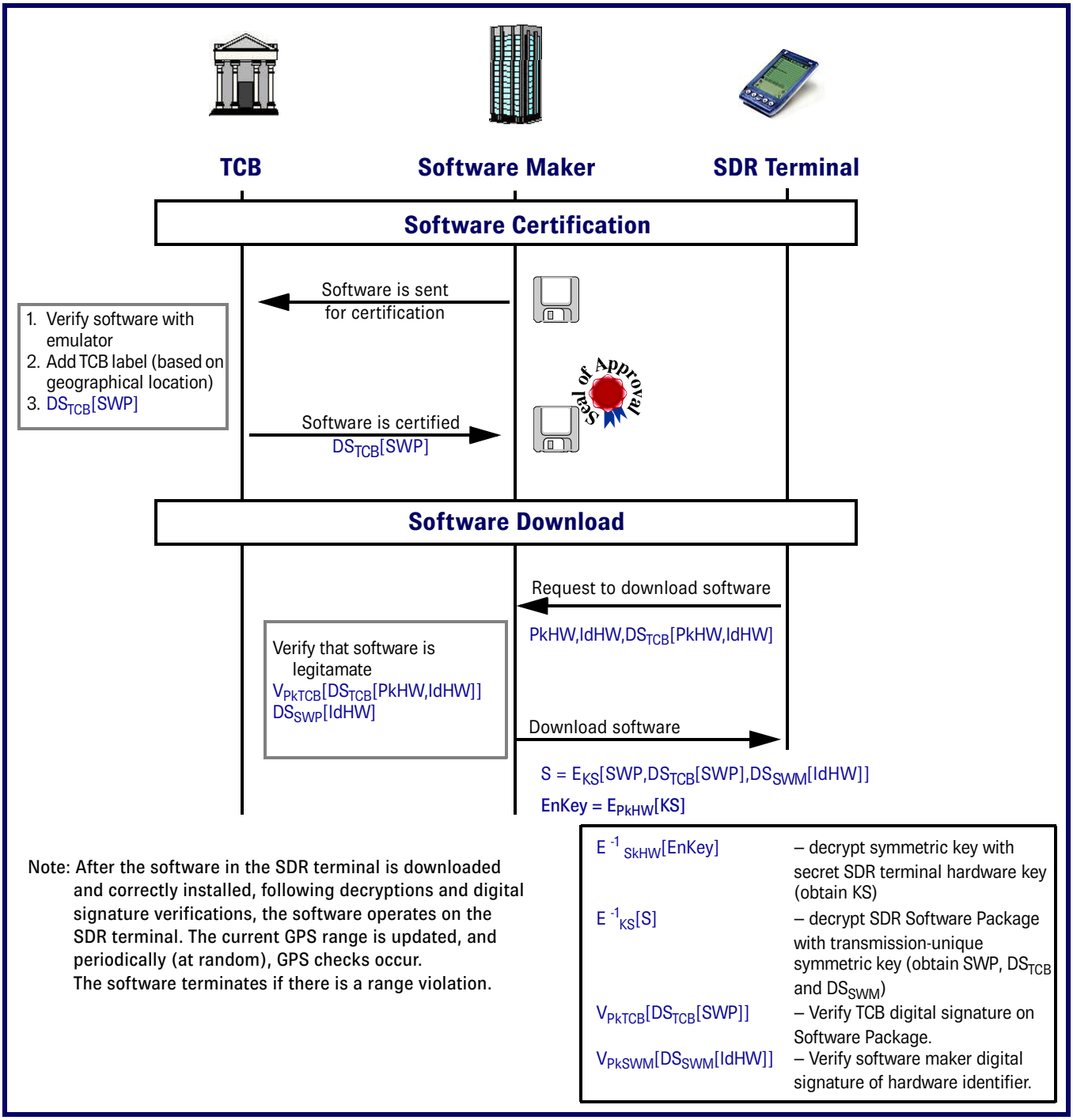
RSM uses $PkTCB_B$, which is already stored in RSM, to verify the DS of SWP_B. For the case where SW_A is the same as SW_B, it is sufficient to download only [DS_{SWM}[IdHW], DS_{TCB}[SWP], TCBL]$_B$. After successful verification of $DS_{SWM}[IdHW]_B$ and $DS_{TCB}[SWP]_B$ by RSM, reinstallation is not needed, since the SW is the same.

RSM Software Complexity: Case study

In order to study the RSM software's complexity, encryption was performed on a PDA and a PC. (The PC's and PDA's specifications are listed in **Table 1**.) On both platforms, DS verification, AES (symmetric) decryption and 1024-bit RSA (asymmetric) decryption were performed on an FPGA binary file using Java code. The file size was 3.8 MB (1 Million gates Xilinx Virtex-II FPGA). Decryptions required 45 seconds of runtime in the PDA, but only 2 seconds in the PC. DS verification required 139 milliseconds in the PDA, as compared to 29 milliseconds in the PC.

Despite obvious differences in operating speed, the PC was configured to emulate an SDR terminal. RSM was implemented using Java2 SE version 1.2.2. The RSM was a Java program with system administrator privileges. A system service was

Figure 3: Details of Software Certification and Download



Note: After the software in the SDR terminal is downloaded and correctly installed, following decryptions and digital signature verifications, the software operates on the SDR terminal. The current GPS range is updated, and periodically (at random), GPS checks occur. The software terminates if there is a range violation.

triggered by the user to initiate software installation using the RSM. All TCB public keys and encryption components were stored as protected files. The RSM Java class file size was 300 KBs and executing memory size was less than 7 MB.

Ensuring Security

Software and hardware certification are separated which simplifies regulators' certification processes. Local radio regulation compliance is assured by random GPS positioning to determine the current country. Hybrid encryption also lets the software maker sell software without depending on hardware vendors.

RSM-based system security, as represented in Figure 4, provides the following allowable and disallowed hardware and software combinations in the proposed SDR architecture:

- A certified terminal does not run uncertified software because of DS_{TCB}[SWP] verification by RSM.
- A certified terminal cannot duplicate software, because only the RSM has access to the corresponding SkHW and can decrypt it.

- Uncertified terminals cannot download SWP, because they do not have DS_{TCB}[IdHW,PkHW]. Even if it was copied, the uncertified terminal will not be able to decrypt SWP, because it does not have the corresponding SkHW.
- Uncertified software will still be able to run on uncertified hardware. Regulators will be responsible for tracking down and seizing these illegal devices.
- Illegal distribution of certified software by parties other than the software maker is prevented by DS_{SWM}[IdHW] verification, where IdHW is a particular terminal's identity number. Note that no one can sign DS_{SWM}[IdHW] other than software makers.

If the same software can be used where the SDR terminal is roaming, only [DS_{SWM}[IdHW],DS_{TCB}[SWP],TCBL] needs to be downloaded. This reduces the need to download and reinstall the same software while still ensuring compliance with local radio regulations.

Modest memory usage and file size show that RSM can be implemented even in a small device such as a PDA. The AES decryption time can be reduced even more through further optimization.

References:

[1] *Authorization and Use of Software Defined Radio*. Federal Communications Commission Report, FCC01-264, Sep. 2001.

[2] D. Bourse, M. Dillinger, T. Farnham, N.Olaziregi. *TRUST System Research – Architectures and UML Modelling*. SDR Forum Document Number SDRF-02-I-0017-V0.00, Jan. 2002.

[3] K. Moessner, R. Tafazolli. *Software Radio Integration and Reconfiguration Management*. SDR Forum Document Number SDRF-01-I-0064w-V0.00, Oct. 2001.

[4] L.B.Michael, M.J.Mihaljevic, S.Haruyama, R.Kohno, *A Framework for Secure Download for Software-Defined Radio*", IEEE Communications Magazine Volume 40 Issue 7, Jul. 2002.

[5] J.J.Fitton. *Security Consideration for Software Defined Radios*. Proceeding of the 2002 Software Defined Radio Technical Conference, Vol.1, Pg.137, Nov. 2002.

[6] C.F.Lam, T.D.Doan, K.Sakaguchi, J.Takada, K. Araki. *Novel Security Architecture that Enables Global Roaming of SDR Terminal*. Proceedings of the 2003 IEICE General Conference, SB-10, Mar. 2003.

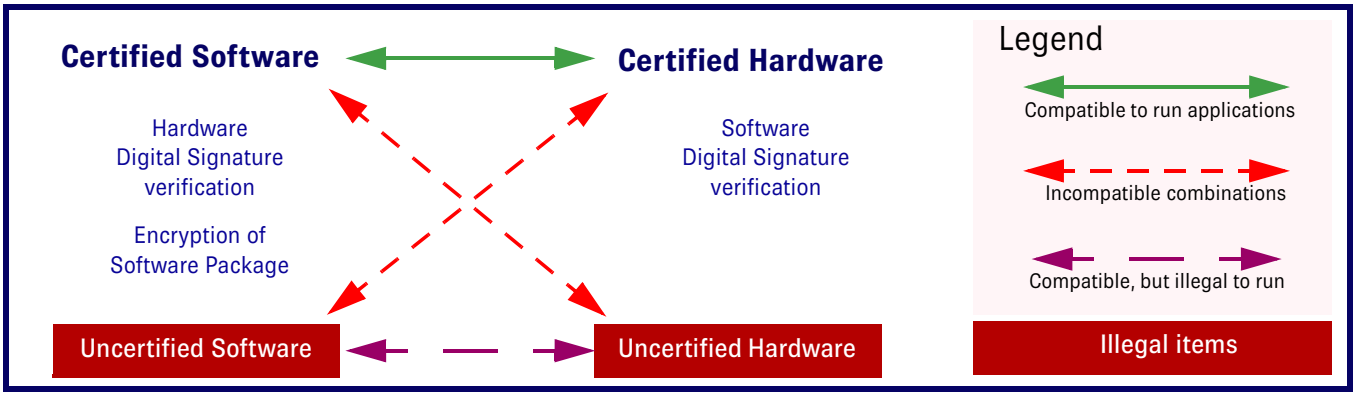
[7] T. D. Doan, C. F. Lam, K. Sakaguchi, J-I Takada, K. Araki. *Digital Pre-distortion Linearizer for a Realization of Automatic Calibration Unit*. Proceedings of the SDR '02 Technical Conference, HW-3-02, Nov. 2002.

[8] M. Togooch, K. Sakaguchi, J. Takada, K. Araki. *Automatic Calibration Unit (ACU) and ACU eMployed Authorization Procedure (AMAP) for SDR*. Software Defined Radio Forum, SDRF-02-I-0020-V0.00, Mar. 2002.

Table 1: Specifications of the PC and PDA used to study the Radio Security Module (RSM)

	PC	PDA (iPAQ)
Processor	Intel Celeron 1 GHz	Intel XScale 400 MHz
Memory	512 MBytes	64 MBytes
OS	Windows 2000	PocketPC 2002
Java Version	JRE 1.2.2 with bouncycastle and cryptix JCE	Jeode JVM with bouncycastle and cryptix JCE
JVM size	22.8 MBytes	3.5 MBytes

Figure 4: Security in All Possible Combinations



About the Authors

Chih Fung, Lam (chihfung@ap.ide.titech.ac.jp) is a M.Eng. candidate at the Tokyo Institute of Technology, Japan. He received a B.E. in computer engineering from Multimedia University, Malaysia, in 2001. His current research interest is SDR's security download architecture. He is a member of IEEE and IEICE.

Kei Sakaguchi has been a research associate at Tokyo Institute of Technology since 2000. He received a B.E. in electrical and computer engineering from Nagoya Institute of Technology, Japan, in 1996 and an M.E. in information processing from Tokyo Institute of Technology, Tokyo, in 1998. He received the Young Engineer Award from IEICE Japan and from the IEEE AP-S Japan chapter, in 2001 and 2002, respectively. His current research interests are mobile propagation measurement, MIMO communication systems and SDR. He is a member of IEEE and IEICE.

Jun-ichi Takada has been an associate professor at Tokyo Institute of Technology since 1994. He received B.E., M.E. and D.E. degrees from Tokyo Institute of Technology in 1987, 1989 and 1992, respectively. In 1992 - 1994, he was a Research Associate in Chiba University, Japan. He received the Excellent Paper Award and the Young Engineer Award from IEICE Japan, in 1993 and 1994, respectively. His current research interests are array signal processing, mobile communication and numerical simulation of waves. He is a member of ITEJ, IEEE, SIAM, AGU and ACES.

Kiyomichi Araki is a professor at Tokyo Institute of Technology. He received a B.S. in electrical engineering from Saitama University, in 1971, and the M.S. and Ph.D degrees in physical electronics both from Tokyo Institute of Technology, in 1973 and 1978, respectively. In 1973 - 1975 and in 1978 - 1985, he was a research associate at Tokyo Institute of Technology, and in 1985 - 1995, he was an associate professor at Saitama University. In 1979 - 1980 and in 1993 - 1994, he was a visiting research scholar at University of Texas, Austin and at University of Illinois, Urbana, respectively. Dr. Araki is a member of IEEE and Information Society of Japan. His research interests are information security, coding theory, communication theory, circuit theory, electromagnetic theory and microwave circuits.

About the Tokyo Institute

Tokyo Institute of Technology was founded in 1881 as Tokyo Vocational School, and it became a university in 1929. Tokyo Tech has five graduate schools, including the Graduate School of Science and Engineering, the Interdisciplinary Graduate School of Science and Engineering and the Graduate School of Information Science and Engineering.

More information is available at:

www.titech.ac.jp

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 were granted in July 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: 6,594,759

Authorization firmware for conducting transactions with an electronic transaction system and methods therefor

The method includes a computer configured to authenticate a user to an electronic transaction system. The computer uses electronic authorization firmware which is in electronic communication with the computer's central processing unit. The electronic authorization firmware includes a non-volatile memory circuit configured to store at least one of the following:

- A user private key;
- user identification data and;
- a firmware identification data.

The electronic authorization firmware further includes decryption logic circuitry functioning between the non-volatile memory circuit and the electronic transaction system. The decryption logic circuitry is configured to prevent unauthorized access to at least one of the following: the user private key and the user identification data in the non-volatile memory circuit. The electronic authorization firmware also includes encryption logic circuit coupled to the electronic transaction system and configured to transmit digital data encrypted using the user private key for transmission to the electronic transaction system. The digital data authenticates the user to the electronic transaction system, wherein the non-volatile memory is inaccessible by the central processing unit without traversing the decryption logic circuitry.

Issued: July 15, 2003

Inventor: Ynjiun Wang
Assignee: **Esignx Corporation** (Cupertino, CA)

www.esignx.com

eSignX **Corporation**
19925 Stevens Creek Blvd.
Cupertino, CA 95014-2358, USA

Telephone: (408) 973-7809
Fax: (408) 973-7289

eSignX is a wireless platform solution provider. It was founded in March 2000 with a mission to enable secure, robust, flexible, convenient, and cost-effective mobile applications in the consumer, enterprise, and government sectors. eSignX has a foundation in patented mobile digital signature technology, based on which they provide a persistent end-to-end wireless security solution. eSignX is currently working with various industry players, such as MSIs (Mobile System Integrators), MAPs (Mobile Application Providers), PKI (Public Key Infrastructure) vendors, trust service providers, smart card and handset manufacturers, network operators, as well as other wireless platform providers.

US Patent: 6,594,498

Communique system for cellular communication networks

The communique system for cellular communication networks operates with existing cellular communication networks to provide communique communication services to subscribers. The communique can be unidirectional (broadcast) or bidirectional (interactive) in nature, and the extent of the communique can be network-wide broadcast or narrowcast, where one or more cells and/or cell sectors are grouped to cover a predetermined geographic area or demographic population or subscriber interest group to transmit information to subscribers who populate the target audience for the narrowcast transmissions. The content of these transmissions can be multi-media in nature, and it may comprise a combination of various forms of media: audio, video, graphics, text, data and the like. The subscriber terminal devices used to communicate with the communique system for cellular communication networks are typically full function communication devices that include:

- WAP-enabled cellular telephones, personal digital assistants, Palm Pilots, personal computers, and the like, or special communique-only communication devices that are specific to communique reception;
- MP3 audio players (essentially a radio receiver or communique radio);
- an MPEG4 video receiver (communique TV) or;
- other such specialized communication device.

The subscriber terminal devices can either be mobile wireless communication devices in the traditional mobile subscriber paradigm, or the fixed wireless communication devices in the more recent wireless product offerings. Furthermore, these communique communication services can be free services, subscription-based services, or toll-based services, while the data propagation can be based on push, pull and combinations of push/pull information distribution modes.

Issued: July 15, 2003

Inventors: Daniel McKenna and James Graziano

Assignee: **Vesuvius, Inc.** (Boulder, CO)

www.vesuviuswireless.com

Vesuvius Inc.
Telephone: (970) 871-4665
Fax: (970) 871-4667

US Patent: 6,594,493

Paging arrangement for wireless communications

Paging areas aligned with wireless terminals are dynamically created. A first base station passes, to the wireless terminal, a list of all the base stations that it knows and that are within a prescribed number of handoffs of the first base station. The wireless terminal uses this list to define its own "personal" paging area. Each time the wireless terminal emerges from a sleep state, it listens for the base station having the best signal and it compares its identification against the list of base stations in its personal paging area. If the best signal base station is on the list, any paging messages for the wireless terminal are automatically broadcast by that base station. Otherwise, the wireless terminal must conduct a handoff to that base station to obtain a new personal paging area centered on that base station, with that base station as paging agent.

Messages originating elsewhere in the network are forwarded to the paging agent for delivery to the wireless terminal. The paging agent then instructs all known base stations within a prescribed number of handoffs of it to page the wireless terminal. The wireless terminal, on hearing the page, will form a connection with the base station having the best signal for communicating. The base station having the best signal for communicating notifies the paging agent that it has established a connection with the wireless terminal, which leaves paging mode and becomes active.

Issued: July 15, 2003

Inventors: Stephen Davies and Michaela Vanderveen
Assignee: **Lucent Technologies Inc.** (Murray Hill, NJ)

US Patent: 6,594,488

Method and apparatus for over-the-air activation of neighborhood cordless-type

A method for providing a neighborhood or local cordless service. The method comprises steps to be followed for receiving subscriber neighborhood zone selection input so that a mobile-telephone-equipped subscriber may place or receive calls for a fixed rate – for example, per month – without having to pay radio frequency air-time charges any time they are located within their selected subscribed-to zones. If the subscribed-to zones are adjacent to one another and if the mobile subscriber roams from one of these zones to another, the subscriber may continue their free call uninterrupted and without paying air time charges. However, when the subscriber roams outside their subscribed-to zones, they may be switched from their neighborhood or local cordless services to conventional personal communications services and pay air-time charges. However for an active call, no air-time charges are incurred as the user transitions between the cellular/DPCS environment and the neighborhood or local cordless service environment. Associated apparatus comprises an IBS for automatically changing radio frequency channels as the subscriber roams within a subscribed-to neighborhood zone, roams to another subscribed-to zone or roams outside a subscribed-to zone. Subscribers may choose to use their mobile identification number, their current directory telephone number for wired public-switched telephone service or obtain a new directory number. Subscribers can actuate their service over-the-air automatically, without service personnel assistance, from their home neighborhood zone.

Issued: July 15, 2003
Inventor: Albert Chow, *et al*
Assignee: **AT&T Corp.** (New York, NY)

Interesting references:

[1] *TIA/EIA Interim Standard.* Addendum No. 1 to TIA/EIA/IS-136.1-A, by Global Engineering Documents with the permission of EIA, pp. 14, 266, 332-40.

[2] *DIVA-2000 Wireless Local Loop.* Diva Communications taken from www.diva.com/product.htm, pp. 1-5, printed Sep. 28, 1998.

US Patent: 6,594,482

Controlled transmission of wireless communications device identity

Selected identifiers belonging to the wireless communications device are provided to a network entity, based upon the control function being processed, or more generally, upon the class of control function being processed. The method for providing device identity includes a system with a Mobile Switching Center (MSC), which receives several identifiers and a control function request from a wireless communications device. The MSC determines which of the identifiers are needed by the network entity to process the requested control function, based on the control function requested. The MSC filters the received identifiers to remove unneeded identifiers, based on its analysis, and forwards the filtered identifiers to the network entity and/or to another network. Another aspect of the invention determines which identifier to send downward to the wireless communications device itself. In these, the wireless communications device is programmed to determine which identifier is needed, and this identifier is transmitted to the MSC with the control function message. This determination by the wireless communications device – of which identifier is needed – is independent of the network, not simply a response to a command from the network.

The method in this invention helps ensure the proper identity is sent by the MSC to other network entities, when the wireless communications device includes more than one fixed identifier. It is particularly adapted for situations where the wireless communications device includes a subscription module having a subscription module identifier and a mobile terminal having a mobile terminal identifier.

Issued: July 15, 2003

Inventor: Nadi Findikli, *et al*
Assignee: **Ericsson Inc.**
(Research Triangle Park, NC)

US Patent: 6,594,481

Apparatus and method for detecting potentially fraudulent telecommunication

An apparatus for credit-based management of a telecommunication system. The apparatus includes an interface for communicating credit information on a particular subscriber and for receiving call records for the particular subscriber, derived from a switch which establishes connections between telecommunication devices. A credit limit device then utilizes the credit information to establish a credit limit for the subscriber. The apparatus also includes a device for comparing the particular subscriber's call usage to a credit limit established for the subscriber, based on information obtained from the credit bureau. An output device is used to provide an indication that the subscriber has exceeded their credit limit. The apparatus includes another device for contacting the credit bureau, upon expiration of a predetermined time period, to obtain a new credit score for a subscriber. The score is used to update the subscriber's credit limit.

Issued: July 15, 2003

Inventors: Eric Johnson and Mark Handzel
Assignee: **Lightbridge, Inc.**
(Burlington, MA)

Interesting references:

[1] Subscriber Computing, Inc. news release entitled, *Subscriber Computing, Inc. Unveils Advanced Version of Fraudwatch.TM.* Mar. 1, 1993, Irvine, California, 3 pages, (no author given).

[2] Cellular Technical Services Company (CTS) product literature on the Clonerwatch.TM.product, (no author, relevant pages, date or place of publication given).

US Patent: 6,591,364

Method for establishing session key agreement

In the method for establishing a session key, a network and a mobile transfer codes between one another. The mobile and the network perform mutual authentication, based on the codes. Besides performing this mutual authentication, the mobile and the network to establish the session key based on the codes. In one embodiment of the invention, the messages forming part of the intended session are sent with the codes, and they form a basis upon which the codes for authentication have been derived.

Issued: July 8, 2003

Inventor: Sarvar Patel
Assignee: **Lucent Technologies Inc.**
(Murray Hill, NJ)

Interesting references:

[1] Bird Fasbender, A., *et al. Systematic Design of Two-Party Authentication Protocols.* Crypto 91, pp. 44-61.

[2] Park, Chang-Seop. *On Certificate-Based Security Protocols for Wireless Mobile Communication Systems.* IEEE Network: The Magazine of Computer Communications, US, IEEE Inc. New York, vol. 11, No. 5, Sep. 1, 1997, pp. 50-55.

[3] S. Patel. *Information Leakage in Encrypted Key Exchange.* Proceedings of DIMACS workshop on Network Threats, 38: 33-40, Dec. 1996.

[4] E. Blossom. *The VPI Protocol for Voice Privacy Devices.* Dec. 1996.

US Patent: 6,591,306

IP network access for portable devices

A guest station on a foreign network is provided IP access by the foreign (i.e., hosting) network without changes to the guest station, including settings for IP address, next-hop-router (gateway), and netmask. An access router automatically detects guests and their home-IP-address, and it assigns a local care-of address to every guest. For outgoing traffic, the router replaces the guest's original/home IP address with the care-of address, and the reverse is performed for incoming traffic. IP traffic may thus be initiated, and responses received, at the temporary current location without having to change its IP address.

Issued: July 8, 2003

Inventor: Jens-Peter Redlich
Assignee: **NEC Corporation**
(Tokyo, JP)

US Patent: 6,591,116

Mobile equipment and networks providing selection between USIM/SIM dependent features

A mobile equipment, such as a cellular radio telephone, includes a controller coupled to a wireless transceiver for bidirectionally communicating with one of several different networks, such as a GSM network and a Universal Mobile Telecommunications System (UMTS) network. A data storage module, such as a SIM/USIM or as a UICC (UMTS Integrated Circuit Card), is readably coupled to the controller. The module stores information for specifying at least an identification and the operational capabilities of the module in each of the different networks. The controller is responsive to a request received from one of the networks. The request, coming through the transceiver, is for accessing the module, to retrieve the stored information. Completion of the request transmits the retrieved information, through the transceiver, to the requesting network.

Issued: July 8, 2003

Inventor: Pasi Laurila, *et al*

Assignee: **Nokia Mobile Phones Limited** (Espoo, FI)

US Patent: 6,591,095

Method and apparatus for designating administrative responsibilities in a mobile communications device

A new process for determining the administrator of a mobile communications device, e.g a wireless cellular telephone, two-way pager, or laptop computer, connectable to a telecommunications network. The system and methods described provide processes for determining whether a Subscriber Entity Module (SIM) is present with a digital certificate for a domain of an administrator, e.g, a network operator, for designating administrative responsibilities in a mobile communications device. A mechanism is provided to designate administrative privileges to an entity by the owner of the mobile communications device.

Issued: July 8, 2003

Inventor: Avinash Palaniswamy

Assignee: **Motorola, Inc.** (Schaumburg, IL)

Interesting references:

[1] *Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module--Mobile Equipment (SIM--ME) interface.* Draft (GSM 11.11 version 5.8.0), Dec., 1997, pp. 1-127.

[2] Fasbender, A., *et al. Any Network, Any Terminal, Anywhere.* IEEE Personal Communications, US, IEEE Communications Society, vol. 6, No. 2, Apr. 1999, pp 22-30.

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