Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 5, No. 6. June, 2003

In The News: 3G Phones Banned at Italian Polls

The BBC reported that Italian authorities plan to ban 3G video phones from their polling booths, fearing the Mafia will force their "bought" voters to prove they delivered. The voter would bring the phone into the polling booth and transmit, to the gangsters, video of themselves while voting.

There are a few problems with this scenario, however. First, it will be a long time before everyone has a 3G phone with a still camera built in, let alone a video camera. Second, this scenario implies that the phone will have to be lent to the voter for the duration. If this was the case, a non-wireless digital camera would probably do just as well. This approach would also reduce the considerable costs of video transmission over a public wireless network (even the Mafia must have a budget for vote buying exercises).

Another problem is the difficulty of photographing yourself while voting, given that in many countries the ballot is just a scrap of paper that needs to be held still with one hand while writing with the other. Furthermore, this supposed security flaw has its own built-in flaw – the voter could vote correctly, then carefully erase the "X" and vote again. The only way to prevent this would be for the voter to continually photograph himself or herself from the time of entering the booth to the time of exiting, which would likely be a bit too obvious.

Until these flaws can be worked out, manipulators will likely continue employing the more traditional options: bussing in voters; plying them with beer or intimidation; stuffing the ballot box after regular voting hours (or, the converse, selectively destroying ballots); making seductive promises that the politician has no plans on keeping; or having partisan control over the vote counting system.

The original BBC report is at:

news.bbc.co.uk/2/hi/technology/3033551.stm

Software Defined Radio: Some Basics

Software Defined Radio (SDR) – or simply software radio – is an emerging technology intended to build highly flexible radio systems – perhaps multi-service, multi-standard, multi-band – that are reconfigurable and reprogrammable by software. SDR, extending back to the early 1990's, has been recognized as one of the most important new technologies for wireless communications today. It is a means to "future-proof" radios.

Dr. Jospeh Mitola, considered the "father of SDR," offers this definition: *SDR is a cognitive radio that intelligently senses its environment, interacts with its user, and adjusts as necessary to maintain ubiquitous communications.*

Hence, an SDR is basically a radio that changes its personality depending on its resident software. It can take on any number of air-interfaces, depending on

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…

July 24th, 2003.

Future Topics

UWB Security • Secure RFID • Security Aspects of Adaptive Radio • Wireless Flash Memory Security • 802.16 Security • Radius for Wireless • 3G Security • Public Keys & Wireless • Security for Mesh Networks • Security Issues in Ad hoc Wireless Networks

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

Technical Editor and Illustrator: Les Owens.

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

Upcoming Wireless Security and Fraud Conferences & Events

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

802.11 Planet Conference & Expo
25th- 27th June, 2003
World Trade Center
Boston, MA
www.jupiterevents.com/80211/spring03/index.html

Computer Security Foundations Workshop
29th June - 2nd July, 2003
Asilomar
Pacific Grove, CA
www.csl.sri.com/programs/security/csfw/index.html

ConVurge GOV 2003
29th June – 3rd July, 2003
Homestead Resort
Hot Springs, VA
convurgegov.com

The 2nd European Conference on Information Warfare and Security
30th June - 2nd July, 2003
University of Reading
Reading, UK
www.mcil.co.uk/2m-eciw2003-home.htm

WCA 2003 – "Capitalizing Your Connections"
8th- 11th July, 2003
DC Convention Center
Washington, DC
www.wcai.com/events.htm

Homeland Defense Training Conference – Mobile and Wireless Solutions
9th July, 2003
DC Convention Center
Washington, DC
www.homelanddefensejournal.com/conf_mobile_2003.html

The Eighth Australasian Conference on Information Security and Privacy
9th- 11th July, 2003
University of Wollongong
Wollongong, Australia
www.itacs.uow.edu.au/research/NSLabs/acisp03

Twenty-Second ACM Symposium on Principles of Distributed Computing
13th- 16th July, 2003
Sheraton Needham
Boston, MA
www.podc.org/podc2003

57th IETF
13th-18th July, 2003
Austria Center Vienna
Vienna, Austria
www.ietf.org/meetings/IETF-57.html

17th Vanguard Enterprise Security Expo
13th-17th July, 2003
J.W. Marriott Grande Lakes Resort
Orlando, FL
www.go2vanguard.com/expo

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

The Fourth Wireless World Conference
17th- 18th July, 2003
University of Surrey
Guildford, UK
www.surrey.ac.uk/dwrc/ww4

GOVSEC 2003
23rd- 25th July, 2003
DC Convention Center
Washington, DC
www.govsecinfo.com

Blackhat USA 2003 Briefings and Training
28th- 31st July, 2003
Caesars Palace
Las Vegas, NV
www.blackhat.com

the availability of the code. For instance, imagine the ability to use the same cellphone as you travel across the United States – crossing different service providers and switching automatically from AMPS to ANSI-136 to ANSI-95 as needed. Or, imagine a device that can be a 2G cellphone, an 802.11b WiFi device and a Bluetooth device, all in one, depending on the need – using one basic DSP (Digital Signal Processing) hardware platform, but using software that reconfigures the multi-purpose wireless machine. Better still – imagine an SDR packaged in a PDA form-factor that can be an AM/FM radio, a pager and a satellite Smartphone, all in one. Sound cool?

Well, this rather utopian vision for SDR is still a few years away because of several limitations --- but, it is coming.

Secure downloading of the air-interface software is a key component of the complete SDR solution. Researchers and SDR proponents have generally envisaged software downloading through three means: from the Internet, from a smart card, and from over the air. Over-the-air (OTA) means – simply and elegantly – over the wireless interface.

There is a bootstrap problem, however. Before the device can be loaded with new software using OTA updates, the SDR has to have at least one workable radio interface software module loaded, and the sending network must provide coverage at the location of the device, of course.

Quote of the Month

"Whenever you have a secret, you have a vulnerability."

— Whitfield Diffie, Chief Security Officer, Sun Microsystems Inc. (Infosecurity Canada, 2003)

Mr. Diffie discovered public key cryptography more than 25 years ago. His perspective on wireless security includes solutions using the new advanced encryption standard (AES), Rijndael, although at least one other expert feels AES is theoretically vulnerable.

Besides numerous radio-link challenges – such as transmission logistics and failure contingencies – the OTA update approach has the most security risks, since "workable software" could mean different things in different countries, social contexts and budget parameters.

There are a considerable number of security concerns, including: compromise of the manufacturers' software, malicious tampering with the code while it is being transmitted over the radio interface, bogus software introduction, and rogue, unauthorized terminals. In this month's issue of *Wireless Security Perspectives*, Insignia offers insights on OTA Firmware Updates of wireless terminals. Their article points out the very important and practical use of OTA – a major driver for SDR today – as a means for bug fixes. Even so, OTA mechanisms do not fully clear all SDR hurdles.

'Over-the-Air' Firmware Updates of Mobiles

Thia Rajagopalan
Insignia

As wireless technology evolves, mobile operators and terminal manufacturers face a dilemma. Competitive pressure forces operators to generate more revenue from data services to keep average revenue per user (ARPU) high. In order to sell new services, their subscribers must have terminals capable of delivering them. But when terminal manufacturers respond by adding features such as MMS, Java, PIM and WAP browsers, the software becomes more complex, setting the stage for bugs and other problems. Compatibility between devices is often a big problem, particularly with pre-standard or early standard implementations of complex protocols.

Glitches increase costs for customer care, including those related to upgrading phone firmware to fix software problems. Customers either have to ship their phones to a fulfillment center, where they are re-flashed with the new version of the firmware, or they have to take them to a retail store. Both methods are expensive for operators and time-wasting and aggravating for customers.

A solution is Over-the-air (OTA) Firmware Updates, which ensure that customers get timely updates without any inconvenience. OTA updates can often be distributed at off-peak hours and transparently, so users do not need to be aware that their phones have been updated.

OTA updates are far less expensive than current methods. However, there are many technical challenges in providing a flexible and robust OTA Firmware Update solution. Operators are especially worried about OTA's reliability and security. This article examines how the key challenges of deploying an OTA Firmware Update system can be overcome.

How OTA Works

A typical OTA Firmware Update system consists of two elements: The server and the client. The server typically resides in the operator's data center. It is responsible for managing each supported terminal's software image – tracking the software versions of the terminals in the network and managing the transmission of Firmware Updates to the terminals. The client, embedded in the terminal's software, is responsible for downloading each Firmware Update and for applying it to the terminal's flash memory.

A typical OTA upgrade, illustrated in **Figure 1**, involves the following steps:

1. **Package Generation.** Because the bandwidth of wireless networks is limited, it is impractical for the terminal to download a new version of the entire software image. Downloading a 2 MB image over a 9.6 kbps connection would take nearly 30 minutes, and the terminal also would have to support a large "scratch" space for storing the downloaded software. To use network and terminal resources more efficiently and to provide a better user experience, a better alternative is to generate upgrade packages, containing instructions for transforming the current image to the new version. These are generated when a new version of software is available, and a server administrator specifies the existing versions that can be upgraded.

OTA or DOA?

The term "3G" is supposed to be synonymous with marketing-friendly buzzwords such as "streaming multi-media," but judging by launches so far, "buggy" and "recalled" seem more accurate.

The latest examples are from a June 12 Reuters article, *3G Handsets Unfit for Consumers, Operators Say*.

"We had 10 Nokia 6650s, but they had to be sent back for software upgrades," said Rudi Westerveld, an assistant professor at the Technical University of Delft, which is conducting tests for T-Mobile.

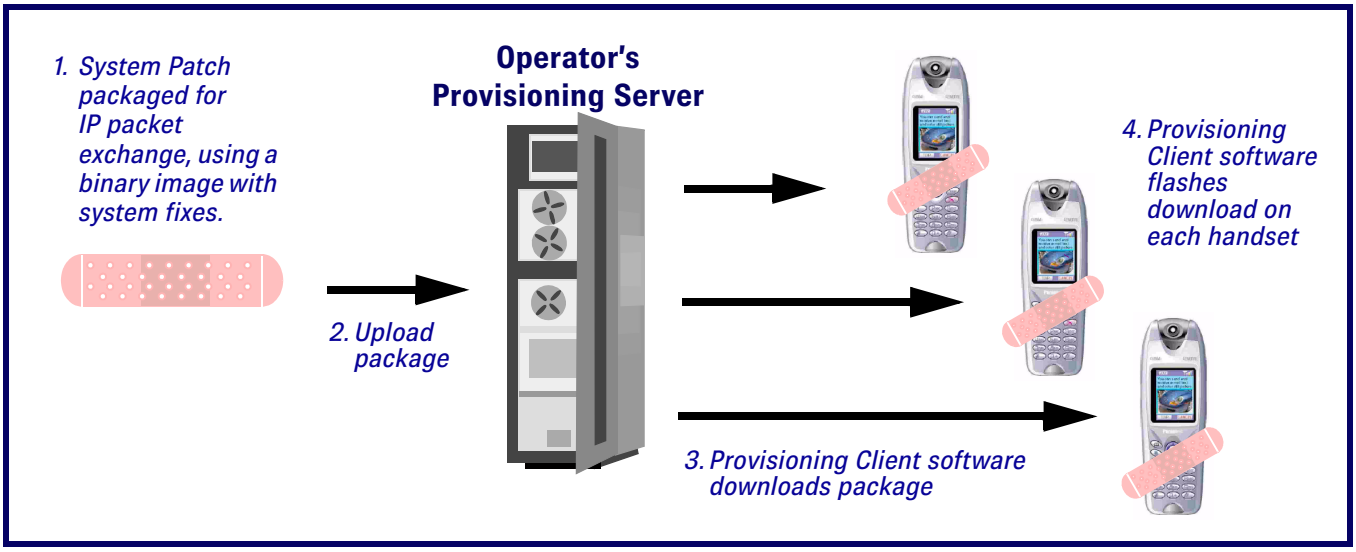
"We're debugging," said Pietro Porzio Giusto, VP at Telecom Italia Mobile. "They're just not stable enough."

Upgrades are even tougher when the phones are in customers' hands.

An alternative is Over-the-air (OTA) Firmware Updates, which reduce the cost and hassle of disseminating bug patches. Although OTA technology has been around for years, security concerns are one reason why most operators have been reluctant to use it. But until 2.5G and 3G phones can deliver a flawless out-of-box experience, biting the OTA bullet might be necessary.

2. **Testing and Certification of Packages.** Once the upgrade packages are created in the server, they go through the operator's testing process, which certifies them for deployment.
3. **Provisioning of Packages to Mobile Terminals.** Upgrade packages can be distributed in two ways: Operator Push or User Pull. In Operator Push, the operator specifies the upgrade packages to be deployed by creating provisioning requests identifying: the devices to be upgraded; when the upgrade should occur; and how devices should be notified. In User Pull, subscribers select an update from a list for their handset model.

Figure 1: OTA Upgrade Provisioning



4. **Downloading Upgrade Packages.** Once a new software version is selected, the client communicates with the server and each authenticates the other. After this, and when a secure channel is established, the upgrade package is downloaded to the terminal.
5. **Application of Upgrade Packages to Terminals**. At the end of the download, the client software follows the instructions in the upgrade package. Once the changes are applied, the upgrade is complete.

OTA's Technical Challenges

There are several technical issues and challenges in providing flexible, robust OTA Firmware Updates.

- **Reliability.** A new version of software must be installed on the device in a predictable, reliable manner. Operators, terminal manufacturers and subscribers must be confident that the technology works and that an update will never render the terminal unusable.
- **Fault Tolerance.** With millions of terminals relying on the OTA Firmware Update server, it must have built-in fault tolerance and a design with no single point of failure. The client-server protocol should be robust enough to support loss of network connectivity. In case of network failure, the download should resume where it left off, instead of starting all over again. The client also must be able to tolerate failures such as lost network connections and batteries that run out while updating the flash memory.
- **Scalability.** As the size and complexity of mobile networks continue to grow, the OTA solution must be scalable enough to support millions of terminals on a variety of networks. The operator should be able to start with a small configuration and grow the system rapidly as the OTA Firmware Update capability is rolled out to more and more subscribers.
- **Open Standards.** Standards-based technologies such as HTTPS, TCP/IP and certificate-based private/public keys should be used wherever possible.
- **Limited Client Resources.** Today's terminals have less than 10 MB of flash memory, and the processor speed is as much as two orders of magnitude less than those in PCs. The challenge is to provide all the necessary levels of security, robustness and fail-safe operation in as little space as possible, using as little processing power as possible. An intimate understanding of the underlying real-time operating system, hardware and processor is key.
- **Security.** Comprehensive, standards-based security is critical so that malicious forces cannot penetrate the provisioning server in any way. The solution also must guarantee that a rogue server cannot spoof the terminals and provision them with unsafe software.
- **Carrier-Grade Solution.** The OTA server must have the characteristics that operators expect in telecom hardware and software. The server should work reliably under all failure conditions, so that it can guarantee software integrity on the terminals. It must be available 99.999% of the time and should include comprehensive administrative and troubleshooting tools. These tools should be capable of monitoring (trace logging) and upgrades, with easy-to-use system utilities. Preventive maintenance and repairs should both be possible without interrupting service.
- **Bandwidth Utilization.** Minimizing download time is important, particularly on lower speed networks. Using data compression, or by highly localizing changes and additions, the server can provide software upgrades in a download package several times smaller than the full new image.
- **Integration with Existing Infrastructure.** To provide a seamless operation, the server should support integration with existing systems such as customer care, billing and MIDlet provisioning systems. This should include the provision of APIs based on industry standards such as SOAP and XML.

  Note: A MIDlet is an application designed for mobile devices that complies with the J2ME (Java 2 Micro Edition) Mobile Information Device Profile (MIDP) standard.

OTA Security 'Must-Haves'

Security is one of the biggest concerns for operators considering OTA. Several points of vulnerability need to be considered.

All human access to the server must be restricted by user name and password. This includes Web access to the server and access from a client device.
To minimize the risk of intrusion, only a small number of tries for a username and password combination should be allowed before the user is blocked from accessing the server. SNMP alarms should be triggered whenever an intrusion attempt is detected. All access must be logged so any break-in attempts are detected quickly, allowing the administrator to rapidly identify and plug security holes.

The servers must only accept software update packages from a trusted list of device suppliers. Digital certificates are a good way for the server to authenticate the supplier.

The server should include comprehensive role-based security so that several levels of administrative privileges can be assigned, based on each administrator's role. At a minimum, functions protected by access-control lists should include: Upload Image, Create Update, Approve Update, Update One Device, Update Multiple Devices and Manage Console User.

The administrator should be able to configure the server to encrypt all communication between the client and the server using HTTPS. Mutual authentication must be used, so that neither the client nor the server will be able to spoof the other party.

Figure 2 illustrates the end-to-end security infrastructure required for an OTA Firmware Update system.

Ten Key OTA Security Questions

Answers to ten basic questions are helpful for understanding OTA security.

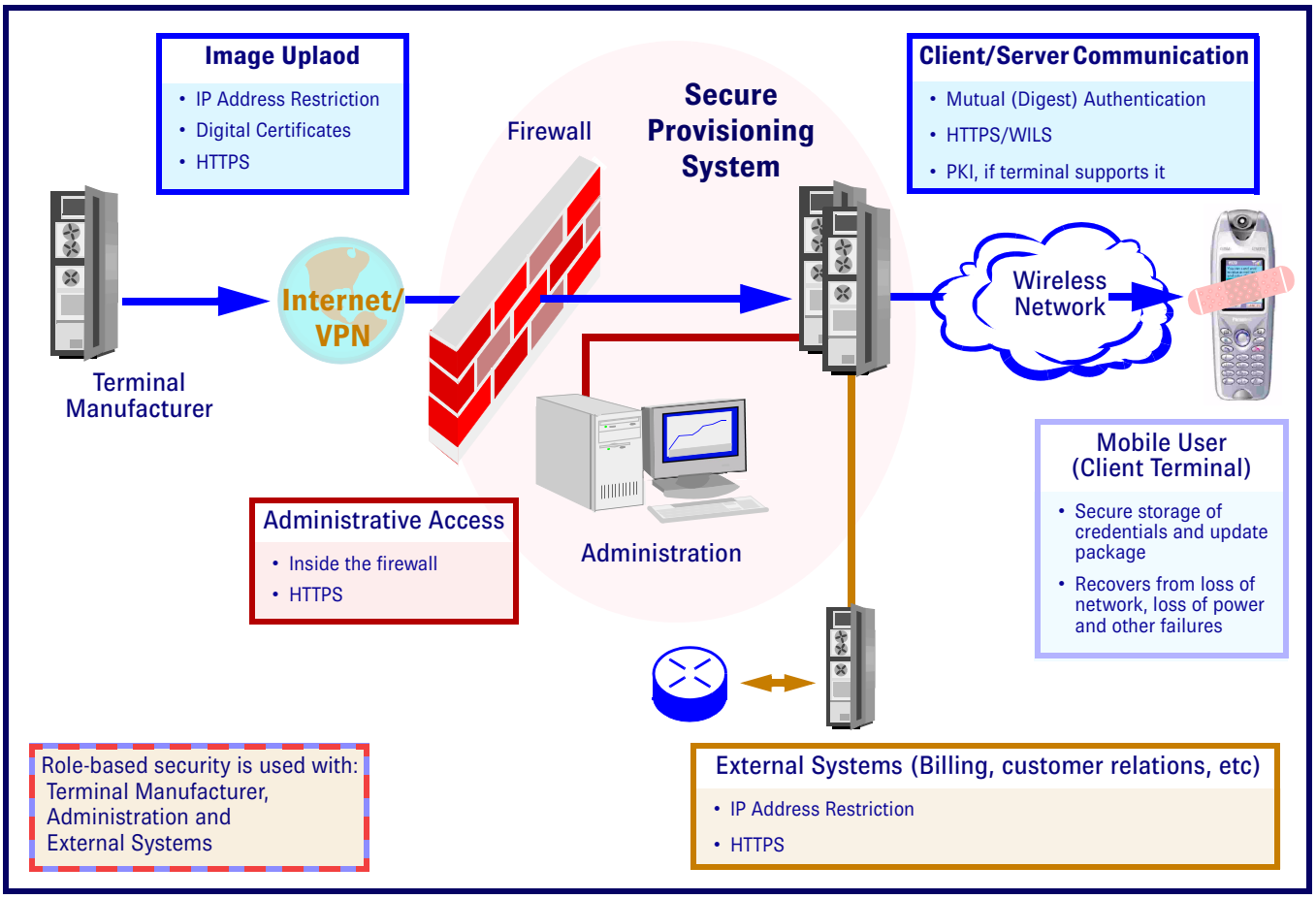
How can unwanted downloads be prevented?

The operator should have the flexibility of determining whether each update is mandatory or optional. With mandatory updates, subscribers may decide *when* to install the update, but they cannot refuse to install it. With optional updates, subscribers may choose whether to install it.

How can downloads be secured to prevent freeloaders?

Strong authentication and authorization schemes must be built into the system to ensure that only authorized terminals can access updates. At a minimum, Digest Authentication should be used to establish a mutually secure channel between the client and the server. If the terminal supports digital certificates, they should be used to authenticate a client before provisioning an update.

Figure 2: Features of End-to-end Security in an OTA Firmware Update System



How can unauthorized modification of data be prevented?

Images submitted to the server must be digitally signed to validate their authenticity. When an upgrade package is sent to a terminal, a cryptographic checksum is included. This allows the client to validate the package before applying it to flash memory.

How do you authenticate the person trying to download?

Strong authentication mechanisms must be in place to validate the user's credentials, which must be verified before upgrades can be downloaded.

How do you prevent malicious, unwanted downloads and denial-of-service (DoS) attacks?

Access to the server can be limited to terminals on a particular operator's network. This limitation prevents access by non-subscribers. The strong mutual-authentication mechanism also will prevent unauthorized access to updates. DoS attacks can be prevented by limiting the number of Firmware Updates for a terminal to a small number per day.

If OTA upgrades are done without user intervention, how is a security association established?

The client credentials can be stored securely in the terminal. When an automatic update without user intervention is desired, an upgrade notification (e.g, SMS, WAP Push) from the server will automatically launch the Firmware Update client. This client software will communicate with the server, authenticating itself by presenting the credentials stored in the flash memory. Once mutual authentication is done, the download and update phases will continue as in the user-assisted scenario.

How is a software load minimized in size to avoid over-whelming the radio interface?

Sophisticated differencing-engine technologies, developed specifically for in-place updates of terminal software, are used to generate compact upgrade packages. By deploying these instead of the entire software image, OTA Firmware Updates can be performed without over-whelming the radio interface.

How big are the files? How much bandwidth is necessary?

A good OTA Firmware Update system should operate in limited bandwidth networks, including those with data rates as low as 9.6 kbps. To make the update process user-friendly, the download time should be kept under two minutes, which implies that the upgrade package size should be less than 100 KB. For larger updates, the system should support multi-step updates involving multiple smaller downloads instead of one large download. This approach reduces the client requirements for flash space and memory, and enhances the user experience.

Can OTA Firmware Update be done when a terminal is roaming?

It is technically possible to perform updates when a terminal is roaming. The operator must allow terminals on a different network to communicate with the server in their data center. All the security implications need to be considered before configuring the network to allow a roaming subscriber to access the Firmware Update server.

What recovery procedures will be in place if a software upgrade fails?

The system should anticipate failure and have recovery mechanisms in place. If a failure occurs, the client software should resume the download or update operation from where it left off.

Rollback mechanisms should be supported. If the operator determines that a new version has problems after an upgrade is complete it should be possible to roll back the software on the terminals to a known good version. They should be able to create an upgrade package to transition the terminal software from the (bad) new version to the good (old) version.
If something goes wrong during the update and it cannot be completed, the updated client software must be able to roll back the firmware to the version in use before the update process started.

Standards that Aid OTA Security

To protect the operator's investment and enable multi-vendor interoperability, an OTA Firmware Update system must be based on industry standards, including:

- **SyncML-DM.** This is a standard for device management functionality, especially for mobile terminals. In its current form, it is geared toward managing the assets in a mobile device, especially applications and configuration data. It is expected to evolve (rev 2.x) to incorporate provisioning of firmware through cooperation between OMA and SyncML More information is available at:

  www.openmobilealliance.org/syncml

- **IOTA.** IOTA is used primarily in CDMA to provision data elements such as WAP configuration parameters and roaming lists. It also is used as the basis for other proposals for provisioning various other elements, such as applications and firmware. It might evolve to incorporate Firmware Update in one of the IOTA extensions. See:

  www.cdg.org

- **SDR Forum.** The SDR Forum is an international, non-profit organization dedicated to promoting the development, deployment and use of Software-Defined Radio (SDR) technologies for advanced wireless systems. Some of the working groups in the forum are in the process of defining standards relevant to OTA Firmware Update systems. See:

  www.sdrforum.org

- **JSR 124 - Client Provisioning Specification.** JSR 124 is a standard proposal administered by the Java Community Process (JCP) as a "J2EE Client Provisioning Specification." It defines an extension to the Java 2, Enterprise Edition (J2EE) platform to provide J2EE application servers with facilities for building provisioning applications. Even though it was proposed for the purpose of provisioning content such as Java MIDlets, screensavers and ringtones, this framework can be extended for use in Firmware Updates. See:

  www.jcp.org/en/jsr/detail?id=124

- **CC/PP.**
  Composite Capabilities/Preferences Profiles is a way to specify what a user agent is capable of doing. This enables sophisticated content-negotiation techniques between servers and clients, producing

optimized XML-based markup for display and use on a wide variety of Web user agents, including mobile terminals. See:

www.ccpp.org

- **UAProf.** The Open Mobile Alliance created the User Agent Profile, which sets a framework for specifying and exchanging capability information about mobile terminals. The UAProf file is stored in a repository server, and the URL pointing to the file is sent in the HTTP header from the mobile device to the server when requesting content. Using UAProf information, the content server can deliver content most suited to the capabilities of the terminal. See

  www.openmobilealliance.org

Recognizing OTA's Opportunities

The ability for mobile operators and terminal manufacturers to perform OTA Firmware updates is a major technological advancement. It reduces customer care costs and enables a wide range of services that operators can use to generate revenue and differentiate themselves in the marketplace. It advances technology beyond the fixed-function phone paradigm, which must be bypassed to make full use of the potential mobile data services and network infrastructure capabilities both currently available and being planned for future network developments.

About the Author

Thia Rajagopalan (thiar@insignia.com) is Insignia Solutions' Product Manager for the Secure System Provisioning product, an end-to-end system for performing Over-the-air Firmware updates for mobile phones. He has over 12 years of product development and product management experience in various companies providing infrastructure products for the wireline and wireless telecommunications industries. He has a Masters degree in Computer Science from Kansas State University.

About Insignia Solutions

Insignia Solutions (www.insignia.com) specializes in Over-The-Air (OTA) Repair Systems for wireless carriers and mobile device vendors. Their product, the Insignia Secure System Provisioning (SSP), is designed for implementation in cost-reduction and revenue-increasing programs.

The configuration of SSP, as illustrated in **Figure 2**, furnishes software for both the server and the client. The SSP Server manages OTA Firmware updates through a secure, standards-based approach. SSP Client provides a simple and secure mechanism for caching the update, after which it performs the update using BrickProof™, a client-side security architecture which tracks each operation. The Server and the Client both tolerate loss of power or loss of network coverage during software updating.

Founded in 1986, Insignia (INSG on NASDAQ) is headquartered in Fremont, Calif., with R&D and European operations based in the United Kingdom.

Insignia is a member of the JCP executive committee. It is one of fifteen companies – worldwide – voting on all JSRs for wireless, such as the J2EE Client Provisioning Specification discussed in the article.

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 June 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: 6,581,162

Method for securely creating, storing and using encryption keys in a computer system

A secure environment for entering and storing information necessary to conduct encryption processes. The method maintains session keys, passwords, and encryption algorithms in a secure memory space such as System Management Mode (SMM) memory, in a computer.

One disclosed embodiment of the invention allows for entry of a user password via a secure keyboard channel. The password is maintained in a secure memory space that is not accessible during normal computer operation. In addition to the user password, optional node identification information is stored in secure memory. The node identification information is appended to the user password, and both are subsequently encrypted. An encryption algorithm and encryption keys are also stored in secure memory. Following the encryption process, the encrypted password and node identification information are communicated directly from secure memory to network interface circuitry for communication over a network.

In addition, an encryption key that is no longer needed can be safely destroyed in secure memory, using this method, without the danger of unidentified copies of the key remaining in computer memory.

Problems associated with key renegotiation and destruction are alleviated, since the encryption keys used for the encryption process cannot be appropriated during normal computer operation.

Issued: June 17, 2003

Inventor: Michael Angelo
Assignee: Compaq Information Technologies Group, L.P. (Houston, TX)

US Patent: 6,581,059

Digital persona for providing access to personal information

A method and system providing a structured and accessible information repository for an entity's personal information. A database, containing personal information and a set of information preferences associated with the personal information database, is controlled on an information server. The personal information database contains personal information about an entity, such as name, phone number, address, etc. The information preferences define an entity's preference regarding the conditions of use under which the personal information will be released. When another computer or user of another computer – a requestor – requests personal information from the information server, the requestor then identifies the information it is requesting and provides the conditions under which the information is to be used. The received conditions of use are compared to the set of information preferences to determine if the received conditions of use are acceptable. If the received conditions of use are acceptable, the information is retrieved and provided to the requestor. If the received conditions are unacceptable, the requestors request is denied. The requestor and the freely addressable access interface may then negotiate the conditions of use until acceptable conditions are reached, or until it is determined that acceptable conditions cannot be obtained. Encryption and third party certification are used to provide security to the system. Records of the transactions are maintained to provide a "paper trail" in case the agreement is broken.

Issued: June 17, 2003

Inventors: Robert Barrett and Paul Maglio
Assignee: International Business Machines Corporation (Armonk, NY)

Interesting reference:

Lee, J.G. *et al. ICOMA: An Open Infrastructure for Agent-based Intelligent Electronic Commerce on the Internet.* International Conference on Parallel and Distributed Systems, Seoul, Dec. 10-13, 1997, pp. 648-655.

US Patent: 6,580,906

Authentication and security in wireless communication system

A communication system having a wireless trunk for connecting multiple phone lines over wireless communication links to a cellular network.

The system comprises a central telephone switch, such as a private branch exchange or key system, connected through one or more trunk lines to a wireless access communication unit. The wireless access communication unit preferably comprises a separate subscriber interface for each trunk line from the central telephone switch.

The wireless access communication unit collects data from each of the subscriber interfaces, formats the data into a format compatible with an over-the-air protocol, and transmits the information over one or more wireless channels to a cellular base station.

A controller within the wireless access communication unit interfaces the *subscriber* interfaces with a radio transceiver. It also assists in the conversion of data from a format suitable for wireless transmission.

Authentication is carried out separately for each of the subscriber interfaces, which allows the wireless access communication unit to represent itself as multiple individual subscribers to the network. At each initial registration, each subscriber interface derives its own ciphering key from a stored user key, which is used for all subsequent encryption and decryption.

Issued: June 17, 2003

Inventors: Izzet Bilgic and Narayan Menon
Assignee: Intel Corporation (Santa Clara, CA)

Interesting references:

[1] Charles Brookson, *GSM (and PCN) Security and Encryption.* 1994. Internet:
www.brookson.com/gsm/gsmdoc.htm

[2] Racal Research Ltd., *Technical Information: GSM System Security Study.* June 1988. Internet:
jya.com/gsm061088.htm

[3] John Scourias, *A Brief Overview of GSM*. Internet:
kbs.cs.tu-berlin.de/.about.jutta/gsm/js-intro.html

[4] Philip Cox, *GSM Security.*. Internet:
www.alanta.demon.co.uk/GSMPaper/Chapter4.html

US Patent: 6,578,143

Method for negotiating weakened keys in encryption systems

A method for permitting encrypted communications between two stations which are operable with encryption algorithms that accept encryption keys having work factors (WFs) with different values. The method proceeds using the following steps:

1. A first determining step identifies which of the keys has the lower WF (represented as WF_{low}).
2. Provide an initial encryption key(KEY_i) having a work factor value, WF '.
3. Compare WF ' with WF_{low} determined in Step 1.
4. When, in Step 3, WF ' is greater than WF_{low} , the following steps occur:
   a. Perform a first hash function on KEY_i to produce a first output, and derive from the first output a first intermediate key (KEY_{mid}) having a work factor value not greater than WF_{low}.
   b. Perform the first hash function on (KEY_{mid}) to produce a second output, and derive from the second output a final encryption key (KEY_f) having a work factor value not greater than WF_{low}.
   c. Use (KEY_f) to encrypt communications between the two stations.
5. When, in the comparing step, WF ' is found not to be greater than WF_{low} , use (KEY_i) to encrypt communications between the two stations.

Issued: June 10, 2003

Inventor: Gregory Rose
Assignee: Qualcomm Incorporated (San Diego, CA)

US Patent: 6,577,865

System for intercept of wireless communications

The system includes an HLR of a wireless communications system configured to associate one or more flags with each subscriber. The HLR notifies an Intercept Server, each time it detects a call event for a subscriber under surveillance, as indicated by the flags.

The Intercept Server includes a Gateway Delivery Function module and one or more Delivery Function modules. The Gateway Delivery Function module provisions the appropriate Delivery Function module~~s~~, depending on the location of the subscriber, to deliver call content or data from an MSC to a Collection Function operated by a law enforcement agency. Non-call associated data is also provided to a Delivery Function module for delivery to a Collection Function.

Issued: June 10, 2003

Inventors: Cemal Dikmen and Murat Karabatur
Assignee: Ulysses Holdings, LLC (Shelton, CT)

US Patent: 6,577,614

System and method for OTA over CDMA data channel

The system comprises a CDMA data network, a server, and a base station in communication with the data network and configured to receive an update parameter from the server. The base station is further configured to establish a CDMA data channel between the mobile client and the base station, and the base is configured to send the update parameter from the base station to the mobile client over the data channel. The update parameter is sent in accordance with a CDMA air interface standard (such as ANSI-95) and a CDMA data channel standard for data services (such as ANSI-707).

Issued: June 10, 2003

Inventor: Charles Cook, *et al*
Assignee: Qwest Communications International Inc. (Denver, CO)

US Patent: 6,577,299

Multiple protocol smart card communication device

A communication link is established between the smart card and a computer, using a valid smart card communication protocol. A smart card communication device determines the valid smart card communication protocol used by a smart card by polling a communication channel using various smart card communication protocols until a valid acknowledgment message is received. A radio frequency circuit is configured to communicate with the smart card using the valid smart card communication protocol. A digital signal processor having at least two demodulators demodulates an incoming data stream produced by the receiver in accordance with the valid smart card communication protocol in a dynamically reconfigurable manner.

Issued: June 10, 2003

Inventor: Walter Bonneau, *et al*
Assignee: Cubic Corporation (San Diego, CA)

www.cubiccomm.com

Cubic Communications, Inc.
9333 Balboa Avenue
San Diego, CA 92123

Telephone: (858) 277-6780

Cubic Communications, Inc. (CCI) provides Radio Frequency (RF) and Digital Signal Processing (DSP)-based wireless communications equipment to government and commercial customers worldwide.
CCI, headquartered in San Diego, has served the domestic and international communications and signal intelligence markets for more than four decades. Traditional products include receivers, exciters, antennas and direction-finding equipment.

US Patent: 6,575,361

System and method for managing stored-value card data

A computerized system and method for managing stored-value card data over a communications network between various terminals and a central processor. Each of the terminals is accessible to respective users. The central processor is remote from the terminals.

The stored-value card data is configured to securely process, in real time, stored-value cards transacted at the terminals, to enable charging prepaid stored-value services to a recipient of the transacted stored-value card.

The method allows for providing a database coupled to the central processor. The method further allows for storing various types of records in the database, comprising stored-value card data for each stored-value card.

An associating step allows for associating each stored record to identifiers so that the record uniquely matches a respective stored-value card and a respective terminal. The associating step is enabled by assigning a "setup" card to the location and capturing the terminal information when a transaction utilizing that card is made. A transmitting step allows for transmitting a request of stored-value card activation to the central processor from a respective requesting terminal.

The central processor is configured to accept the transmitted activation request, based on whether the associated identifiers for the stored-value card to be activated match identifiers actually transmitted by the requesting terminal for that stored-value card and terminal.

Issued: June 10, 2003

Inventors: Phillip Grave and Merrill Smith
Assignee: E-2 Interactive, Inc. (Atlanta, GA)

US Patent: 6,574,730

User authentication in a communications network

An authentication system of a terminal on a public switched telephone network, providing a security node associated with a local exchange and a network terminal.

For one-way authentication, the terminal responds to a call initiation by sending a unique authentication code comprising a number and a secret key encrypted according to a first algorithm. The secret key is specific to the terminal. The security node constructs the expected authentication code from the number, using the first algorithm and a second key which is a function of a terminal

identification number, and compares the expected code with the received code.

In two-way authentication, the security node responds to the call initiation by sending a transaction number to the terminal encrypted according to a second algorithm. The terminal generates the authentication code as a function of the first algorithm, the secret key and the transaction number.
The authentication code is sent back to the security node. An expected code is compared with the received one in the same way.

In both cases, a match between expected and received authentication codes constitutes authentication of the terminal, allowing the user access to the network.

Issued: June 3, 2003

Inventor: Robert Bissell, *et al*
Assignee:
British Telecommunications plc (London, GB)

Interesting reference:

Walker, Michael. *Security in Mobile and Cordless Telecommunications*. Proceedings of the 6.sup.th Annual European Computer Conference, May 4, 1992, pp. 493-496.

US Patent: 6,574,466

Method of securing transmission of information utilizing time variant techniques with error detecting code

A process for establishing secure communication between particular communicating units via a channel of a telecommunication network. Using an error detecting code, the process encodes data prior to its being selectively transmitted to one or more particular receivers. This code enables reliable recovery of the information on reception.

For security reasons, the error detecting code used to *encode* the information is encrypted using an enciphering key defined by application of a time-dependent variation law. Alternatively, the error detecting code used to *transmit* information can be selected by application of a time-dependent variation law.

Issued: June 3, 2003

Inventors: Helen Papini and Fran Simon
Assignee: Alcatel (Paris, FR)

Interesting reference:

Hwang Tzonelih, et al, *Secret Error-Correcting Codes (SECC)*. Advances in Cryptology, Santa Barbara, Aug. 21-25, 1988, Jan. 1, 1988, pp. 540-563.

US Patent: 6,574,455

Method and apparatus for ensuring security of users of Bluetooth-enabled devices

Rather than including a static network descriptor in messages transmitted between master and slave Bluetooth-enabled devices communicating on a piconet, the network descriptor is changed each time a new session brings on one of the devices. Ordinarily, the network descriptor is computed as a known function of the master's Bluetooth address (BD_ADDR). The descriptor change prevents an intentional eaves-dropper – who may be in proximity to the piconet and who may be listening for and detecting the network descriptor included within these messages – from associating a detected network descriptor with a particular device of a user, which could lead to the use of the descriptor for tracking the location of the user who is carrying and using that device.

The network descriptor, the Channel Access Code (CAC), is changed each time a new session begins by computing it as a known function of a seed and the master's BD_ADDR. The seed is a random number chosen at the beginning of each new session by the master.

For further security, the CAC is changed not only when a new session begins, but within each session on a periodic basis. For the latter, the seed is a combination of the random number generated for each session by the master and a time parameter associated with the master.

Issued: June 3, 2003

Inventors: Bjorn Jakobsson and Suzanne Wetzel
Assignee: Lucent Technologies Inc. (Murray Hill, NJ)

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