Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 5, No. 10. October, 2003

In the News: T-Mobile, WiFi and 802.1X

With file and printer sharing turned on, mobile users with hardware supporting 802.1X (usually enterprise class products) can breathe easier. This month, T-Mobile started to field test this stronger security standard at selected locations out of their more than 3000 hotspots across the United States.

The 802.1X security standard is designed to prevent interception or 'hijacking' of information between the network and hotspot client (mostly laptops and PDAs). The company hopes to increase commercial usage of these public access points by providing greater security. T-Mobile's Hotspot customers who do not activate 802.1X-enhanced security features may still access T-Mobile Hotspot service through their ordinary Web browser interface, and they will continue to have the option of using VPNs and personal firewalls, instead of 802.1X.

The 802.1X standard enhances authentication and encryption via Wireless Provision Services (WPS), a T-Mobile collaboration with Microsoft. This service allows Windows XP users to detect and connect to T-mobile hotspots. Support may be added for non-XP users in the months ahead.

Further details about the 802.1X standards are included in the **October, 2001** issue of *Wireless Security Perspectives*.

IMEI Fraud: Security in GSM

IMEI fraud is the latest problem to hit GSM networks. This does not result in the theft of service. Instead, it allows a stolen phone to be used with a legitimate SIM card ('smart card'). This was originally just a problem for consumers, affecting carriers only after consumer pressure and consequent government legislation. This type of fraud can also be a problem for carriers that provide subsidized handsets.

The IMEI (International Mobile Equipment Identity) is a 14 BCD digit string (56 bits) that permanently identifies the Mobile Equipment (ME – GSM phone). This contrasts with the IMSI (International Mobile Subscription Identity), which is stored in the SIM card – not the phone – and identifies the subscription.

About Wireless Security Perspectives

Price

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

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

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

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

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpsales@cnp-wireless.com

Next Issue Due…

November 26th, 2003.

Future Topics

Wireless Flash Memory Security • Personal Area Network Security • Radius for Wireless • 3G Security • Public Keys & Wireless • 1XEV Security

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.

RFID Journal University
3rd November 2003
Westin Peachtree Plaza
Atlanta, GA
www.rfidjournal-u.com

[Note: this event is being repeated in other locations during November]

RSA Conference 2003 Europe
3rd- 5th November 2003
RAI Congress Centre
Amsterdam, Netherlands
www.rsaconference.com/rsa2003/europe

Next Generation Networks (NGN) 2003
3rd- 5th November 2003
Marriott Copley Place
Boston, MA
www.bcr.com/ngn

The CSI 30th Annual Computer Security Conference
3rd- 5th November 2003
Marriott Wardman Park Hotel
Washington, DC
www.gocsi.com/events/annual.jhtml?_requestid=248470

Satellite Applications Technology Conference & Expo (SATCON)
3rd- 5th November 2003
Hilton New York
New York, NY
www.satconexpo.com

The 14th Annual Northern California Information Security Conference (InfoSeCon 2003)
4th - 5th November 2003
Sacramento Convention Center
Sacramento, CA
issa-sac.org/conferences/2003

11th Annual International Conference on Network Protocols
4th- 7th November 2003
Georgia Tech Hotel and Conference Center
Atlanta, GA
icnp03.cc.gatech.edu/index.html

Adaptive and Resilient Computing Security (ARCS)
5th- 6th November 2003
Santa Fe Institute
Santa Fe, NM
discuss.santafe.edu/bnadaptive

ACM SenSys '03
5th- 7th November 2003
University of California, LA
Los Angeles, CA
www.cens.ucla.edu/sensys03

Angelbeat Regional Technology Forums on Mobility and Wireless
6th November 2003
Baltimore, MD
www.angelbeat.com

[Note: this event is being repeated in other locations during November]

National Wireless Engineering Conference 2003
10th- 13th November 2003
Hilton San Diego Resort
San Diego, CA
www.iec.org/events/2003/natlwireless

Federal CTO Summit 2003
12th- 14th November 2003
Renaissance Hotel
Washington, DC
www.vanheyst.com/CTOSummit

The SC Magazine Conference 2003
13th- 14th November 2003
Millennium Gloucester Hotel
London, UK
www.westcoast.com/conference/programme.html

SANS Network Security 2003
13th- 19th November 2003
Sheraton New Orleans
New Orleans, NC
www.sans.org/ns2003/wirelessnetworks.php

CRA Conference on "Grand Research Challenges in Information Security & Assurance"
16th- 19th November 2003
Airlie House
Warrenton, VA
www.cra.org/Activities/grand.challenges/security/home.html

COMDEX
16th- 20th November 2003
Las Vegas Convention Center
Las Vegas, NV
www.comdex.com/lasvegas2003

Computer Digital Expo
17th- 20th November 2003
Mandalay Bay Convention Center
Las Vegas, NV
www.cdxpo.com

The Conference on Mobile & Wireless Security
25th- 26th November 2003
Conrad Hotel
Dublin, Ireland
www.misti.com

Wireless Broadband Forum
25th- 26th November 2003
De Vere University Arms Hotel
Cambridge, UK
www.wirelessbroadbandforum.co.uk

A Precedent for Location Privacy?

In a move that could set a precedent for wireless location technology, the Finnish parliament is considering a law that would let parents track their children via wireless, even without their consent.

Under the proposal, children younger than 15 could be tracked without their permission. Anyone older than 15 could not be tracked without consent except in emergencies.

A vote will not happen until November, 2003 but the European Union is expected to follow Finland's lead when it crafts laws that set guidelines for wireless location tracking. "Roughly similar legislation will be a reality in the European Union area in the near future," said Juhapekka Ristola, an official in Finland's transport and communications ministry.

The legislation is the latest twist in the debate over privacy, protection and profit. In September, 2003 the Washington State Supreme Court ruled that police cannot attach a GPS-based tracking device to a suspect's vehicle without first getting a search warrant.

But the marketplace has set its own precedents, too. In June, 2003 the Aalborg Zoo in Denmark began selling €3 (US3.50) Bluetooth neck tags so parents could find children who wandered off.

Some countries have embraced tracking. In July, 2003 NTT DoCoMo reiterated its forecast that location-based services such as pet tracking will help drive non-voice services to 80% of the company's total revenue by 2011. One reason for that bullish outlook: In Japan, where wireless is already widely used to track pets, children and the elderly, Secom's pet-tracking service, for example, costs US$7/month.

Other services have used an opt-in approach to avoid privacy infringement. For example, AT&T Wireless' nearly two-year-old Find Friends service uses the same principle as instant messaging buddy lists: Users receive a message that a friend wants to track them, and their choices include a one-time or permanent denial. Those who agree always have the opportunity to hide by blocking tracking.

The use of IMSI is validated by GSM authentication, making it extremely difficult to clone a GSM subscription. Even though an IMSI would be easy to replicate, without the associated root key on the SIM card, the authentication challenges could not be responded to, resulting in the denial of service.

If a phone is valuable, there is money to be made in stealing it and selling it to someone who can then purchase a valid SIM card to use it with. With phones increasingly including photographic, GPS, PDA, music and other desirable capabilities, stealing them becomes more tempting.

GSM has the capability to protect against handset theft by querying each phone for its IMEI and then checking it against the list in an EIR (Equipment Identity Register). An EIR can classify an individual IMEI as Black (denied service) or Grey (tracked). Entire ranges of IMEIs can be classified as White (representing a range of manufactured phones).

In early GSM systems, the EIR was not implemented at all because carriers saw no benefit. Increasingly, however, carriers are being motivated to use it by consumer pressure and direct financial losses from the theft of subsidized phones, or from the theft of phones being sent to distributors, such as the 26,000 Samsung phones that disappeared in 2002 in the UK.

EIRs run separately by carriers do not protect against organized criminals. The theft goes undetected if the phone is used on another carrier's network with a legitimate IMSI. Australia has recently implemented legislation requiring the country's three GSM carriers (Telstra, Optus and Vodafone) to provide a centralized EIR (or other mechanisms) to share the identity of stolen phones.

A criminal may find a way around this by 'cloning' or 'rebirthing' the phone with a new IMEI, similar to the ESN cloning that used to plague analog AMPS systems. The Australian legislation has made this a crime, but this is unlikely to stop the problem.

Another way around networked EIRs is to simply move the stolen phones to another country. This is particularly desirable if they are being moved from a country with subsidies to a country without, where phones are sold for higher prices.

The GSM association is now demanding that all carriers maintain an EIR with weekly sharing of lists of newly stolen phones. Not being an automated system, this relies on efficient reporting by all GSM carriers and quick implementation of all the updates received. A truly centralized EIR would be preferable, but the costs of the necessary international signaling might be prohibitive.

The IMEI problems may soon be experienced by cdma2000 systems, as well. A slightly modified version of IMEI known as the MEID (Mobile Equipment Identifier) is being built into these standards and will eventually replace the ESN. See the **July, 2002** issue of *Cellular Networking Perspectives* for a comparison of IMEI and MEID.

A good question is why authentication is not the answer to this problem. Key distribution is one reason (as well as the fact that no existing GSM phones would have this capability at the time it was invented). Every phone would have to have a secret key embedded in it. Given that the IMEI only identifies a manufacturer, this means that they would have to perform the challenge/response or distribute the keys to carriers upon demand. Manufacturers usually gain no revenues from phones, once they are sold, and therefore have no financial motivation to perform this service. Distributing keys to many carriers would only increase the probability of wholesale theft of the keys, invalidating the authentication. The problem will have to grow significantly in size before such a sophisticated solution becomes worthwhile. Until then, carriers can make it difficult, but not impossible, to use stolen phones.

Creating a Secure and Trusted Environment in Wireless Terminals

Richard York
ARM

Richard York, secure technologies program manager at ARM, looks at the problems of running secure applications in wireless terminals.

The security of a system is only as good as its weakest link. As the consumer electronics industry evolves, the concept of security becomes more blurred, as does the ability to identify that weakest link.

Advances in processing power and memory mean that wireless terminals – from standard GSM or CDMA phones to personal digital assistants and 'smart phones' – are now capable of a wide range of functions. Most of these rely on increasingly complex operating systems and demand several levels of securing data. Unfortunately, current techniques for securing data within a mobile terminal are insufficient for the many new applications operators want to deploy – intended to increase their average revenue per user (ARPU).

The increasing use of standard operating systems such as Symbian, Windows, Java, Palm and even embedded Linux gives developers more tools and a much wider platform for their applications, lowering the cost of deployment and increasing the use of such systems. But this proliferation of large and complex operating systems and the associated software development tools also opens up the risk of attack from viruses and external sources, which makes securing data within the terminal critically important.

Operators want to use the additional capabilities in the terminals for features such as:

- e-commerce, using the phone to make purchases;
- delivery of premium content such as music and video;
- interactive applications such as games;
- updates to the terminal software or configuration data; and
- protection against intrusion.

Security Needs

Each capability needs different types of protection.

Premium content has to be protected, often by encryption. Certificates used by digital rights management (DRM) software must be secured, along with delivery of the conditional access software and encryption keys. This sensitive content may also have to stay protected within phone peripherals such as removable memory cards that have ever-higher capacities. These are often used to store music and video clips needing protection against unauthorized distribution.

Other applications, such as games, have to be purchased and downloaded securely, interacting with the hardware platform and software while not introducing security holes. This is particularly important if elements of the game, such as new characters and abilities, can be loaded into the terminal from other routes, such as a memory card.

Certificates and keys also have to be updated and managed, meaning that part of the system needs the ability to change critical data. A secure system must protect the management code, as well. Having security-critical code sitting in the file system of the operating system and in general purpose memory knocks a huge hole in the overall system security. These issues, which are not being adequately addressed today, are slowing down the deployment of DRM-based applications.

All this has to be handled securely within the terminal without applications compromising each other. Indeed, they may have to be kept totally separate. One DRM company is unlikely to grant a competitor access to its technology within the terminal, even if different systems are used to download things such as video and music. If there is a risk of this, the applications providers will not sign up.

Users will not want applications to have direct access to their data such as credit card numbers and PINs. This should be kept separate from the other areas as well. Without this protection, an attacker could offer a free game which later proves to be a Trojan horse feeding personal and financial information to a network computer as the raw material for identity theft and other crimes.

Ensuring the security of keys, data and applications represents three parts of the same challenge: securing the entire system.

Protecting the Application Chain

At the heart of the challenge for protecting GSM, and some cdma2000, wireless devices is the 'smart card' (SIM or UIM). This has been the stalwart of terminal security since the original specification of GSM, but relies mostly on a restricted physical interface to protect the data within the card. By protecting the software access to the interface, the data can be *de facto* protected. The drawback is that the demands of the average application are so much greater today than when GSM was introduced in the early 1990s. The smart card interface has a low bandwidth of around 30KHz (0.03MHz), orders of magnitude less than the 60MHz to 300MHz provided by the central processor of the terminal. There is also limited memory. High end SIM cards still store only 32Kbytes or 64Kbytes of memory.

With security focussed around PIN numbers, the smart card approach is ideal. Indeed, it is possible and even desirable to store 128-bit encryption keys on a smart card, but those keys are used to decrypt data in the terminal. Once the keys are out of the smart card and into the terminal, they must continue to be protected. The content they decrypt at the wireless terminal must also be protected. It is useless to protect complex keys and decryption architectures if the decrypted content – video or music, for examples – can be simply copied onto a removable memory card!

Providing this will protect data throughout the application chain, rather than at particular points. While operating system vendors have been teaming up with security providers to provide the building blocks of security such as encryption co-processors, a hardware architecture that can assist the end-to-end security of such a system has been lacking.

Today's Security Approaches

Several current approaches attempt to minimize the problems. One of these is the 'sandbox'. This provides a dedicated environment in which the applications runs, and usually including its own area of memory and only limited connections to the outside world. This approach has been taken by Java Virtual Machines running J2ME Java code in terminals.

This approach, unfortunately, suffers from a number of drawbacks. The main objection is that the system cannot be partitioned in this way. Processor cycles and registers are needed for running the system, particularly for the air interface and the GSM or 3G protocol stack. A 'sandbox' cannot provide these.

Using a sandbox approach means having to store all the application data back to memory (which may not be secure) before switching to the real-time portions of the system. The hardware in most terminals is not designed for such context switches, and the memory used to store the data is probably not secure.

What is needed is a way to clearly segregate application code, but this must be coupled with simple hardware protection, so that the code can only access a specified, secure area. The problem is that there is no standard model for doing this.

One way to perform this segregation is with multiple processors, an approach that is becoming common in high-end terminals and smart phones which contain a separate applications processor. The drawback is that this increases the cost of the terminal hardware and makes applications protected in this way inappropriate for low-end terminals, limiting their appeal.

Amiss from the Whole-system Approach

There is a lack of standards for whole-system security. While Java has the **JSR177 format** for defining the interface to the SIM card to access certificates and keys, it does not define how that information is protected. Standards such as IPsec and WPA (WiFi Protected Access – see the **November 2002** issue of *Wireless Security Perspectives*) look at providing a secure connection, but then the terminal becomes the weak point which, when compromised, bores a hole through an entire network's security.

Security and Trust Services API for J2ME (JSR 177)

The objective of the Security and Trust Services API is to define a set of APIs providing security services to J2ME-enabled devices. Such services will rely on interaction with a *security element* in the device, which is responsible for:

- Secure storage, to protect sensitive data such as user's private keys, certificates, and personal information;
- Secure execution, such as cryptographic operations to support payment protocols, data integrity, and data confidentiality.

A security element can be implemented in a variety of ways. Use of smart cards is common. For example, in GSM networks, the network operator puts the network authentication data on a SIM card. When this card is inserted into a mobile handset, it enables the handset to use the operator's network. This JSR will provide an access-model API to enable your applications to communicate with a smart card.

Further information is available at:

wireless.java.sun.com/midp/articles/j2mefuture

and

www.jcp.org/en/jsr/detail?id=177

What is needed is an end-to-end route of trust through the system. If a point in that route is violated, then any data downstream of that point must also be marked as potentially violated.

A Better Approach: Only *One* Secure Processor

The TrustZone approach developed by ARM provides a virtual processor without adding significant costs (see **Figure 1**). This is done through extensions to processor instructions coupled with hardware at various points in the chip, which act as gate-keepers, restricting access to memory and registers when the chip is in secure mode.

This gatekeeper hardware is not just in the processor. It is also in key peripherals around the processor core, such as the boot ROM and a new secure area of memory for storing keys. It also protects access to other areas that need to be in a secure mode, such as the real time clock and the display.

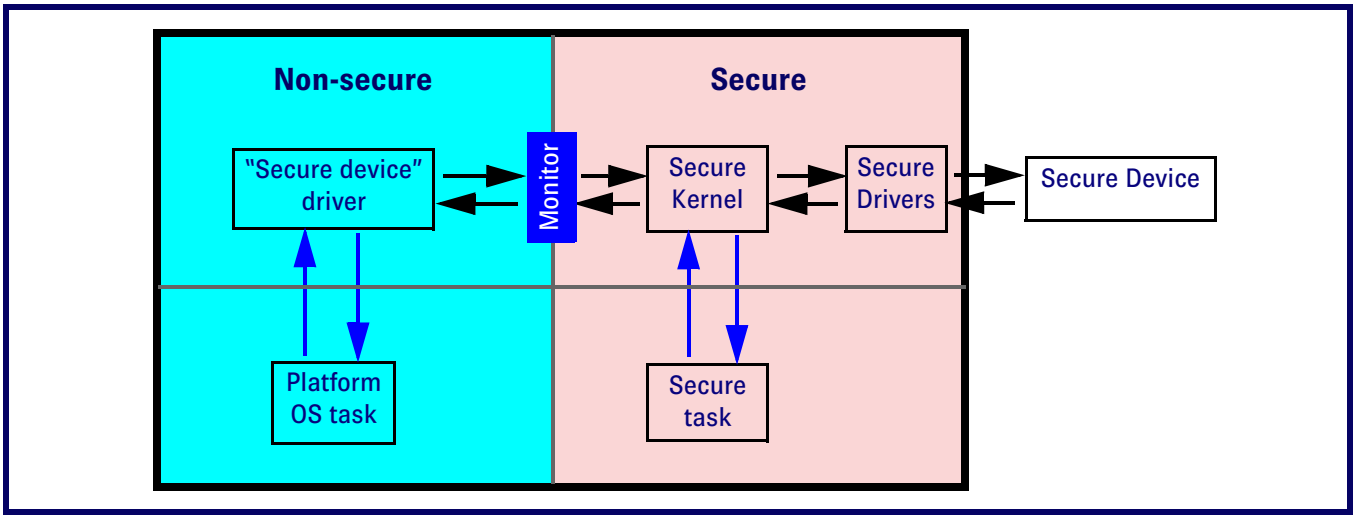
The Secure Monitor Mode allows a limited number of entry points through a dedicated new instruction in the processor and through exception trapping in the operating system. The limited entry allows it to be proved secure. A secure bit in the core indicates when the processor is running in the secured mode. This is visible on the bus to make the memory and peripherals 'security aware'.

However, secure information can still sit in the processor cache when the system switches back to normal mode. TrustZone uses a cache that tags lines with security information to keep the two security domains separate. Each line of the cache has a marker that is checked during a cache compare to prevent a security violation.

Having a secure boot is essential to maintain the integrity of the system during operation, as it can be used to bring the system up in a secure manner – each stage can be controlled by the secure kernel, using signatures and code stored in the secure memory space.

Once the terminal is booted-up, standard applications such as operating systems run as usual. The processor can be put into the secure mode by the operating system so that secure applications such as SSL, JSR177 and TCG run entirely in a secure environment, rather than having elements sitting outside in the relatively insecure operating system.

Figure 1: TrustZone Software System Overview



Limitations of the Approach: The Importance of Multi-layer Protection

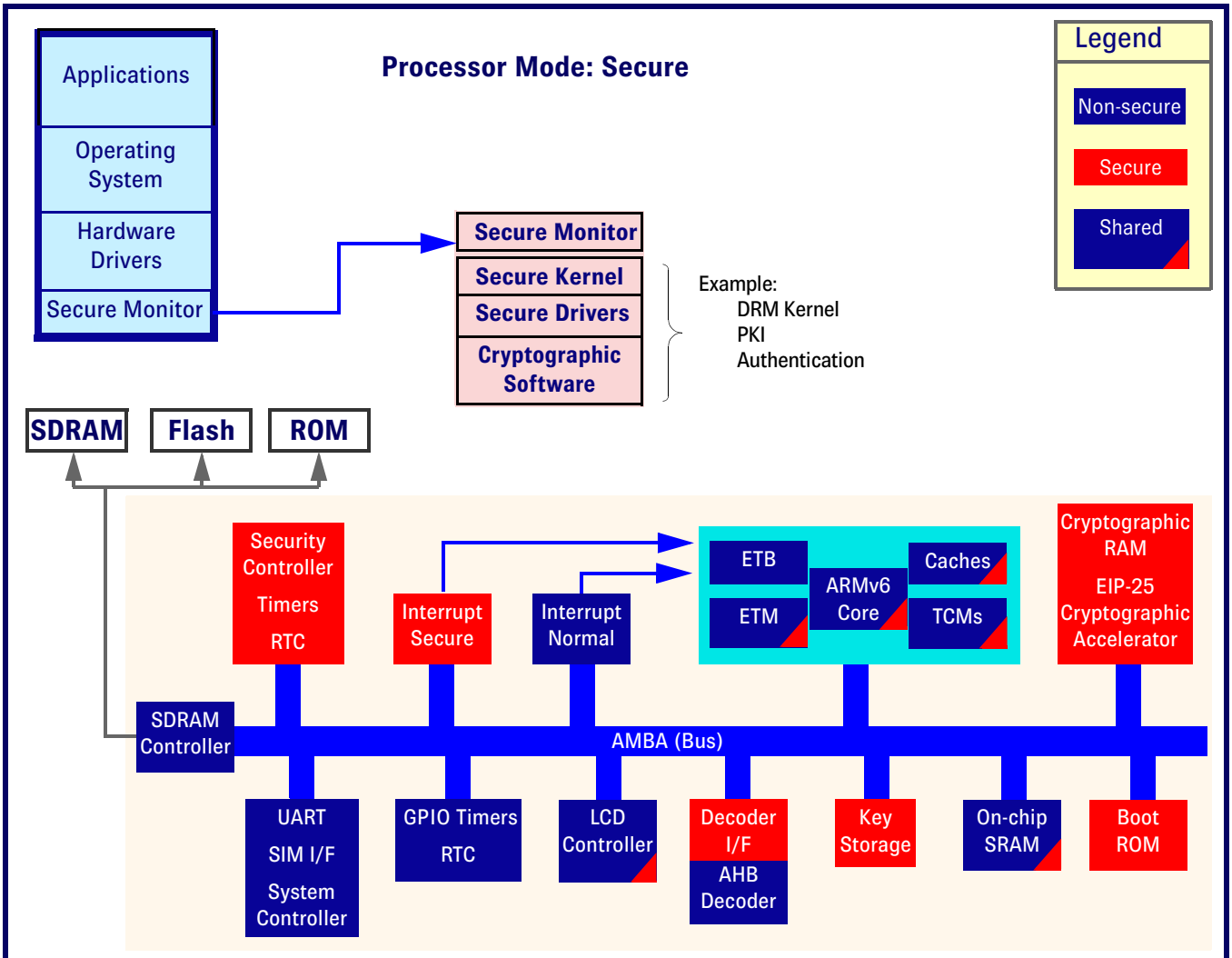
What this system does not do is to protect against malicious applications. The ability to boot securely will stop viruses that try to access the boot ROM and change the start-up configuration, and it keeps the protected data secure, but it will not stop malicious code using or crashing the operating system.

However, terminal and operating system vendors such as Symbian have teamed up with security applications vendors such as MacAfee and Symantec to prevent these types of virus, worms and Trojans from infecting the system.

This approach is also not a 'quick fix' for security. Security certification covers the whole system, from the hardware to the operating system and applications, and TrustZone provides a vital element of this (see **Figure 2** for an example). Lax design in the rest of the system can compromise any security implementation.

Putting security in the processor allows a common platform for security applications, rather than adding additional chips to the system. The existing code needs only minor modification to run on the new secure platforms, using the ARM architecture that is already used for the vast majority of GSM and 3G phones, as well as for many handhelds.

Figure 2: TrustZone Example System



Glossary

AHB	Advanced Hardware Bus	**ETM**	Embedded Trace Module
AMBA	Advanced Microcontroller Bus Architecture	**GPIO**	General Purpose Input/Output
ARMv6 Core	Refer to: www.arm.com/armtech/ARM_Arch?OpenDocument	**SIM I/F**	SIM card Interface
DRM	Digital Rights Management	**SRAM**	Static Random Access Memory: fast (no wait state) memory region; 1 nanosecond access time (one clock cycle)
EIP-25	Safenet's Embedded Intellectual Property (EIP) module – configurable cryptographic engine including design features to resist power and timing attacks.	**TCM**	Tightly Coupled Memory
ETB	Embedded Trace Buffer	**UART**	Universal Asynchronous Receiver/Transmitter

The price of the implementation (i.e, lag in performance speed) is paid in instruction extensions and a few tens of thousands of gates for the peripheral gate-keepers, which in the current 130 nm and 90 nm process technologies is a negligible increase in cost. TrustZone will be implemented in the ARM1176JZ-S processor core in 2004, and can be retro-fitted to other architectures such as ARM9 and even ARM7.

More Than Wireless

This approach is not just limited to wireless terminals, although this is where the need is currently most pressing. A digital TV set top box is another possible venue for it, since these are being considered for interactive applications such as video on demand, betting and home shopping, yet applications are still restricted due to security concerns. These concerns can be addressed by moving the conditional access technology into software – rather than relying on a smart card (which is not usually present in these devices) – and coupling that with a secure area for user data, applications, keys and certificates.

There is increasing demand from equipment makers, network operators, and content and service providers for a secure environment in wireless terminals, and there is currently no commonly available hardware platform to allow this. Creating a secure and trusted environment in an industry-standard and widely deployed processor, beginning at boot up, will open up a wide range of novel, exciting and trustable wireless services.

About the Author

Richard York (richard.york@arm.com) is product manager for security-enabled technology at ARM, including the ARM SecurCore family of microprocessors. He has worked at ARM for over eight years, during which time he has been closely involved with the design of ARM7TDMI core and was an architect in ARM's advanced research and development group. He is also the principal architect of the ARM RealTrace debug system. Before joining ARM, Richard worked in the Amulet group at the University of Manchester, researching asynchronous implementations of the ARM architecture.

About ARM

ARM (www.arm.com) provides 16/32-bit embedded RISC microprocessor solutions. The company licenses its high-performance, low-cost, power-efficient RISC processors, peripherals, and system-on-chip designs to leading international electronics companies. ARM also provides comprehensive support required in developing a complete system.

Secure Mobility Forum

In the summer of 2003, the National Security Agency (NSA) created the Secure Mobility Forum. Its purpose is to exchange ideas and establish partnerships among research communities in government, private industry and academia in support of the classified user. Each alliance member brings with it a distinctly different approach to research. Mobile technology offers significant flexibility and network connectivity, which is driving many user needs and applications. However, these same attributes create unique vulnerabilities. Multidisciplinary research, cutting edge innovation, and partner leveraging are needed to rapidly develop high assurance solutions for mobile tactical and strategic networks. For more information, contact the editors of WSP.

Are you a Mensan?

If so, you should be able to figure this out.

What is the next number in this series:
887, 911, 929, 941, 953?

Are these the ages of the ancient prophets? Cellular frequencies? Encrypted parameters from 802.11's WEP? Or what?!
Submit the first answer and get on WSP's erudite list.

Fraud and Security Patent News

US Patent: 6,636,975

Accessing a secure resource using certificates bound with authentication information

A method and computer program product for accessing a secure resource using a certificate bound with authentication information. In one implementation, the method includes receiving a certificate request from a user, the certificate request including identification information and authentication information associated with the user; verifying the identification information; issuing a certificate to the user when the identification information is verified; and sending the authentication information and a certificate identifier for the certificate to an authentication server. According to one aspect, the sending step includes signing a combination of the authentication information and the certificate identifier to form a unique user identifier; signing the authentication information; and sending the unique user identifier to the authentication server.

Issued: October 21, 2003

Inventor: Yuri Khidekel, *et al*
Assignee: Identix Incorporated (Minnetonka, MN)

Notable References:

[1] Neuman, *et al. Kerberos: An Authentication Service for Computer Networks.* Sep. 1994, IEEE Communications Magazine, p. 33-38.

[2] *Identix Introduces the First Authenticated Certificate – The Next Level of Identity Protection for Internet Security and Secure E-Business.* Company Press Release, 3 pgs, Nov. 16, 1999. URL (discontinued):
biz.yahoo.com/bw/991116/nv_identix_1.html

[3] Wahab, *et al. Biometrics Electronic Purse.* IEEE, 1999, p. 958-961.

[4] Lampson, *Computer Security,* Digital Equipment Corporation, p. 1-54.

US Patent: 6,636,972

System and method for building an executable script for performing a network security audit

A system and method for building an executable script for performing a network security audit. A source program expressed in a network packet simulation language is stored. The same program includes a plurality of statements encoding logic to simulate an exchange of network protocol compliant-packets. Each statement is scanned into a sequence of individual tokens. Each token is parsed into grammatical phrases comprising at least one of an expression and a control construct. Each expression evaluates a data value. Each control construct defines a process flow. The grammatical phrases are compiled into program instructions to execute the logic on a target machine.

Issued: October 21, 2003

Inventor: Thomas Ptacek, *et al*

Assignee: Networks Associates Technology, Inc. (Santa Clara, CA)

US Patent: 6,636,966

Digital rights management within an embedded storage device

A method for enabling locked data stored on a storage medium and accessing it through a data storage engine contained within or connected to a host device. A user selects all or part of the data stored on the storage medium to enable. The host device then connects to a server over a network and completes a transaction. The transaction can be any requirement specified by the supplier of the data selected by the user. Once the transaction is complete, the data storage engine connects to the same or a separate server through the host device and receives a piece of information, known as the content key, necessary to decrypt, read, or otherwise make sense of the data selected by the user. The content key may be, for example, part of a decryption key. The content key is combined with other information stored on the storage medium. The combined information is then used to access the data selected by the user.

Issued: October 21, 2003

Inventors: Lane Lee and Daniel Zaharris

Assignee: DPHI Acquisitions, Inc. (Boulder, CO)

About WSP Patent Listings

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

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

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

US Patent: 6,636,838

Content Screening with end-to-end encryption

A system performing content screening on a message that is protected by end-to-end encryption. The system operates by receiving an encrypted message and an encrypted message key at a destination from a source; the encrypted message having been formed by encrypting the message with a message key; the encrypted message key having been formed by encrypting the message key. The destination forwards the message to a content screener in a secure manner and allows the content screener to screen the message to determine whether the message satisfies a screening criterion. If the message satisfies the screening criterion, the destination receives a communication from the content screener that enables the destination to process the message. In one embodiment of the present invention, the system decrypts the encrypted message key at the destination to restore the message key, and forwards the message key along with the encrypted message to the content screener. This enables the content screener to decrypt the encrypted message using the message key. In one embodiment of the present invention, the system decrypts the encrypted message key at the destination to restore the message key, and then decrypts the encrypted message with the message key to restore the message before sending the message to the content screener.

Issued: October 21, 2003

Inventor: Radia Perlman, *et al*

Assignee: Sun Microsystems, Inc. (Santa Clara, CA)

US Patent: 6,636,689

Data disc modulation for minimizing pirating and/or unauthorized copying and/or unauthorized access of/to data on/from data media including compact discs and digital versatile discs.

A method and system for authenticating a media and/or the data stored on the media in order to prevent piracy and/or unauthorized access and/or unauthorized copying of the data stored on the media, including CDs and DVDs. According to the present invention, there are three ways that authentication keys can be formed and remain hidden without being transferred in the audio/video. These three methods are employed using conventional hardware and/or software in CD or DVD players, which may optionally be modified. Each method of producing authentication keys according to the present invention is a function of the physical characteristics of a disc that does not normally travel with the audio or video or graphics data. Authentication systems of the present invention optionally encompass singular, multiple or multi-level authentication systems, each of which successively must be deciphered before the audio/video is finally available, or alternatively, where each key component must be found in order to build the whole key to perform the entire decryption or authentication process.

Issued: October 21, 2003

Inventor: David Stebbings
Assignee: Recording Industry Association of America (Washington, DC)

US Patent: 6,636,615

Methods and systems using multiple watermarks

Using two or more digital watermarks, with different characteristics, that are embedded in a document, the characteristics are chosen so that the watermarks will be affected in different manners if the document is subsequently copied or reproduced. The detection process or mechanism reads two or more of the watermarks and compares their characteristics. While wear and handling may change the characteristics of the digital watermarks in a document, the relationship between the characteristics of the multiple digital watermarks in a document will nevertheless give an indication as to whether a document is an original or a copy of an original. Document wear can be independently assessed and used as an aid in interpreting the detected watermark characteristics.

Issued: October 21, 2003

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

Notable References:

[1] Winograd, J.M. *Audio Watermarking Architecture for Secure Digital Music Distribution*. A Proposal to the SDMI Portable Devices Working Group, by Aris Technologies, Inc, Mar. 26, 1999.

[2] Mintzer, *et al. Safeguarding Digital Library Contents and Users: Digital Watermarking*. D-Lib Magazine, Dec. 1997, 12 pages.

[3] Vidal, *et al. Non-Noticeable Information Embedding in Color Images: Marking and Detection*. IEEE 1999, pp. 293-297.

[4] Wolfgang, *et al. A Watermark for Digital Images*. Computer Vision and Image Processing Laboratory, Purdue University, Sep. 1996, pp. 219-222.

[5] Cox, *et al. Secure Spread Spectrum Watermarking for Images, Audio and Video*. Proc. Int. Conf. on Image Processing, Sep. 16-19, 1996, Part vol. 3, pp. 243-246.

US Patent: 6,636,592

Method and system for using bad billed number records to prevent fraud in a telecommunication system

A method for using at least one Bad Billed Number Record (BBN) to detect fraud in a telecommunication system. The method includes the steps of generating the BBN for each call attempt made using a billing product, when the call attempt satisfies any one of several fraud criteria; storing the BBN in a storage queue for later retrieval; and retrieving and analyzing the BBN to increment a plurality of fraud control counters according to the analysis.

A system for using several BBNs to detect fraud in a telecommunications system includes a network operator service platform (OSP) for generating BBNs based on received call attempts; a network information concentrator (NIC) for temporarily storing the generated BBNs; and a fraud monitoring system for retrieving the stored BBNs, filtering out unidentifiable BBNs, analyzing identifiable BBNs, and generating alarms based on the analysis.

Issued: October 21, 2003

Inventors: Dean Marchand and Dean Springer
Assignee: Same

US Patent: 6,636,505

Method for service provisioning a broadband modem

A method for automatically provisioning a broadband communication service to a subscriber having a broadband modem. The method includes the step of transmitting a service request from the broadband modem to a central office, which is associated with a network service provider. The network is configured for service in response to the service request. The method further includes automatically configuring the broadband modem by transmitting a configuration signal from the central office to the subscriber. The configuration signal may be transmitted to the broadband modem over a POTS subchannel. Alternatively, the configuration signal may be transmitted to the broadband modem over a subchannel in a broadband service, such as a DMT subchannel for ADSL service.

Issued: October 21, 2003

Inventors: Ray Wang and Paul Shieh
Assignee: 3Com Corporation (Santa Clara, CA)

US Patent: 6,636,502

GPRS-subscriber selection of multiple internet service providers

A switching device (PLMN-SW) in a mobile radio communication system (PLMN) which supports a GPRS-network allows to connect a terminal station of the mobile radio communication network with one of any number of packet data communication networks. The selection of the packet data communication network is based on the transmission of a specific network indication parameter (NIP) from the terminal station. The NIP is transmitted to a serving (GPRS) support node (SGSN) as a special parameter in a PDP context activation procedure. Thus, a large number of internet service providers can be connected to a GPRS-network.

Issued: October 21, 2003

Inventors: Per Lager and Kurt Essigmann
Assignee: Telefonaktiebolaget LM Ericsson (Stockholm, SE)

Notable References:

[1] *Digital Cellular Telecommunications System (Phase 2+); General Packet Radio Service (GPRS); Service Description; Stage 2 (GSM 03.60 proposed version 2.0.0)*. May 1997.

[2] *Digital Cellular Telecommunications System (Phase 2+); General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface; (GSM 09.60 proposed version 1.1.0)*. Jun. 1997.

US Patent: 6,636,491

Access control method for a mobile communication system

A security technique for a communication system. An access point (GGSN) from a mobile communications system to an external system is selected at a service node (SGSN) of the mobile communications system based on at least two or three grounds of selection: a) the subscription data of a mobile subscriber stored in the mobile communication system, or b) an access point selection data given by a user in a service request, or c) other grounds. The serving node sends to the access point (GGSN) selected a further service request which includes indication of the grounds of the selection – i.e, whether the access point is selected by subscription, by a user, or based on any other grounds. Thereby, the access point is able to distinguish and accept service requests in which the rights of the user are already assured by the subscription, without any security problems. When the request is based on the selection of the access point by the user, or on any other insecure grounds, the access point is able to make any further actions to ensure the security. These further actions may include rejection of the service request.

Issued: October 21, 2003

Inventor: Hannu Kari, *et al*
Assignee: Nokia Corporation (Espoo, Finland)

US Patent: 6,636,489

Wireless management system and a method for an automated over-the-air managing process for wireless communication device

In a wireless communication system including a base station, a network and a control unit, a generic network address is initially stored in a communication device, the communication device being activated onto the network utilizing the generic network address. If service is to be provided to the communication device, a control unit of the network provides a unique network address for storage in the communication device for use in subsequent communication between the communication device and the network.

Issued: October 21, 2003

Inventor: Howard Fingerhut
Assignee: Bell South Wireless Data. L.P. (Woodbridge, 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

US Patent: 6,633,981

Electronic system and method for controlling access through user authentication

A Basic Input/Output System (BIOS) device is designed to control access to a portion of BIOS code loaded in its internal memory. For example, during a boot process, an internal state machine permits access to the portion of the BIOS code in response to authentication of a portable token in communication with the BIOS device. Otherwise, the BIOS device precludes access to the portion of the BIOS code until the portable token is authenticated.

Issued: October 14, 2003

Inventor: Derek Davis
Assignee: Intel Corporation (Santa Clara, CA)

Links

As a free service, we provide a spectrum of links to virtually every aspect of wireless communications. Check in at our links page:

- If you need further information about standards and regulatory organizations, technology forums, wireless associations or wireless vendors and service providers;
- If you are seeking a consulting firm or;
- If you desire a broader news perspective by reading reports from other wireless news sources.

www.cnp-wireless.com/links.html

US Patent: 6,633,761

Enabling seamless user mobility in a short-range wireless networking environment

Methods, systems, and computer program instructions for enabling a variety of devices, particularly low-power hand-held devices, to travel seamlessly through a networking environment such as that encountered within a building by establishing connectivity to multiple network access points. The illusion of seamless network connectivity is provided by having these access points coordinate with a core server to perform user authentication, device address assignment, and handoff services.

Issued: October 14, 2003

Inventor: Sandeep Singhal, *et al*
Assignee: ReefEdge, Inc. (Fort Lee, NJ)

www.reefedge.com

ReefEdge is a developer of wireless network infrastructure products that provide security, seamless mobility with session persistence, and management for wireless local area networks. Through a suite of products and technology innovations, ReefEdge enables enterprises, services providers and mobile operators to deploy secure and well-performing wireless networks, while enabling end-users to take full advantage of the benefits of these networks.

ReefEdge
2 Executive Drive
Fort Lee, NJ 07024

Phone: +1-201-242-9700
Fax: +1-201-242-9760