Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: wsp@cnp-wireless.com Vol. 3, No. 7. August, 2001

Security - The Key to m-commerce

Guy Singh
Baltimore Technologies

The global m-commerce market is expected to be worth a staggering US $200 billion by 2004. During this time, phones and other mobile devices are going to get smarter, evolving into *lifetools* that deliver personalized local goods and services — anywhere, anytime — while also working as digital diaries, payment systems, wallets and passports. But the marriage of the mobile phone and the Internet will never be as fruitful as analysts predict unless a manageable and scalable end-to-end wireless security system is adopted by mobile commerce vendors.

Nobody questions the mobile mantra anymore. Through the deployment of third-generation networks and devices, organizations and their customers, suppliers, partners and staff all stand to benefit from this brave new mobile world. Benefits, including streamlined business processes, reduced sales cycles and increased revenue streams, are expected. Durlacher detailed in its recent mobile commerce report the following: E-bills; e-salaries; security services (for instance, using the mobile device to gain access to buildings); shopping; retailing; ticketing; auctions; reservations; postcards, advertising; dynamic information management; membership schemes; loyalty programs; medical records; and passports. The possibilities are truly endless.

Products supporting mobile commerce are also as pervasive as the hype around the mobile world. Equipment vendors of WAP (Wireless Application Protocol) gateways and Web-enabled smart phones have been out in force, demonstrating their commitment to this new delivery mechanism — by pushing new mobile technology ahead of existing successful products. Analyst reports have fueled the fire further with predictions of exponential growth of WAP phones and other Web-enabled wireless devices — devices to enable people to do business totally untethered while on the move. The Yankee Group, for instance, predicts there will be 21.3 million mobile data users in the U.S. by the end of 2001. Another pundit, Strategy Analytics, predicts that 'about 95 percent of smart phones shipped to the United States and Western Europe in 2003 will be Wireless Application Protocol (WAP)-Enabled, and 70% will have Bluetooth technology.'

Consider for a moment — how much of this will become a reality without trust in the devices? This type of trusted transaction environment can only become possible with the wide scale adoption of an airtight security infrastructure. A single publicized significant breach of mobile security is all that is needed to shake the foundation of the wireless industry.

About Wireless Security Perspectives

Price

The basic subscription price for *Wireless Security Perspectives* is $300 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$350 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…

September 17th, 2001.

Future Topics

Wireless Packet Data Security • AES (Rijndael) • IP Security • Public Keys & Wireless • IP Mobility Security • Security Issues in Ad hoc Wireless Networks • Electronic Signatures in Wireless • Latest in Watermarking

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**: $300 for delivery in the USA or Canada, US$350 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: Les Owens.
Article Sourcing: Betsy Harter.
Production: Doug Scofield.
Distribution: Debbie Brandelli.
Marketing: Muneerah Vasanji.
Accounts: Evelyn Goreham.
Publisher: David Crowe.

Upcoming Fraud and Security Events

The following are some upcoming conferences and security events that may be of interest to the wireless and network security practitioners.

Infowarcon
5 - 6 September, 2001
Washington, DC
www.interpactinc.com/infowarcon.html

New England SANS
5 - 12 September, 2001
Park Plaza Hotel
Boston, MA
www.sans.org/newengland/boston.htm

Cyber-Sabotage 2001
18 - 19 September, 2001
Delta Hotel
Ottawa, Ontario
www.iqpc.com/cgi-bin/templates/9977569962842407226550002/genevent.html?event=1775&topic=82

The Conference on Mobile & Wireless Security
24 - 25 September, 2001
Atlanta
www.misti.com/conference_show.asp?id=MWS

Developing Winning Strategies to Combat Fraud
15 - 16 October, 2001
Berkeley Hotel
London
www.iir-conferences.com/site/_prod-grp.cfm?DirName=KJ1823&ConfCode=KJ1823&iv=23

VPN Conference 2001
15 - 18 October, 2001
Hilton Alexandria at Mark Center
Alexandria, VA
www.vpncon.com/2001events/fall/fall2001index.htm

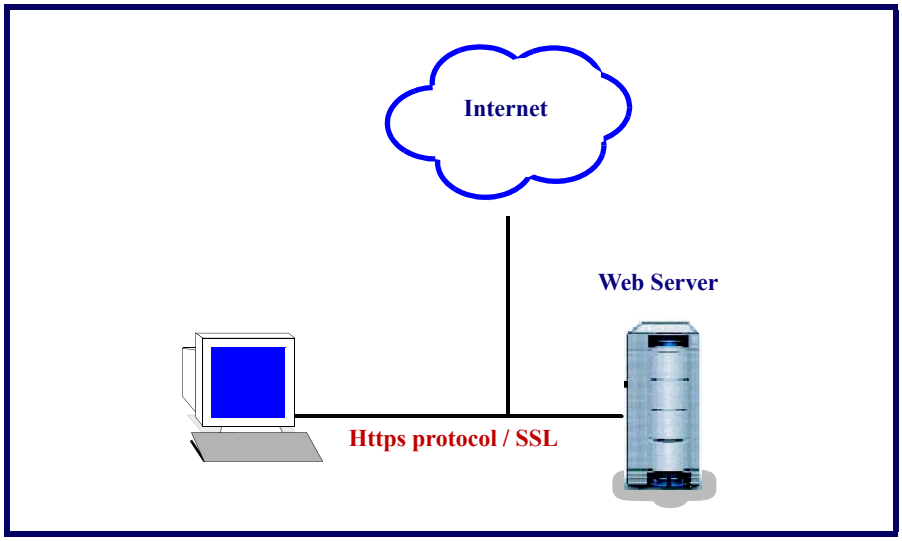
3G Technical Fraud Forum
30 - 31 October, 2001
The Forum Hotel
London
www.iir-conferences.com/site/_prod-grp.cfm?DirName=cg1074&ConfCode=cg1074&iv=23

Without security, the wireless industry is at serious risk. We have already witnessed the destructive effects of the numerous accounts of attacks on 802.11b wireless LAN security. Fortunately, financial losses have not been reported — yet.

But, a little known fact — one that has not been as widely publicized as the various predictions of market size and activity — is that the wireless world presents a far greater security risk than the wired world. There are two primary reasons for this: First, the encryption — used to render information unreadable except for legitimate parties — in mobile communication links has frequently proven vulnerable and inherently weak. Second, the WAP access to the Internet over mobile device — the so-called *Gap in WAP*.

Before discussing the problems with WAP security, it is helpful to begin with a discussion of the security of PC access to the web. This architecture is sometimes referred to as being *two-tiered*, as depicted in Figure 1.

Figure 1: Two-tiered PC-to-Web-Server Architecture

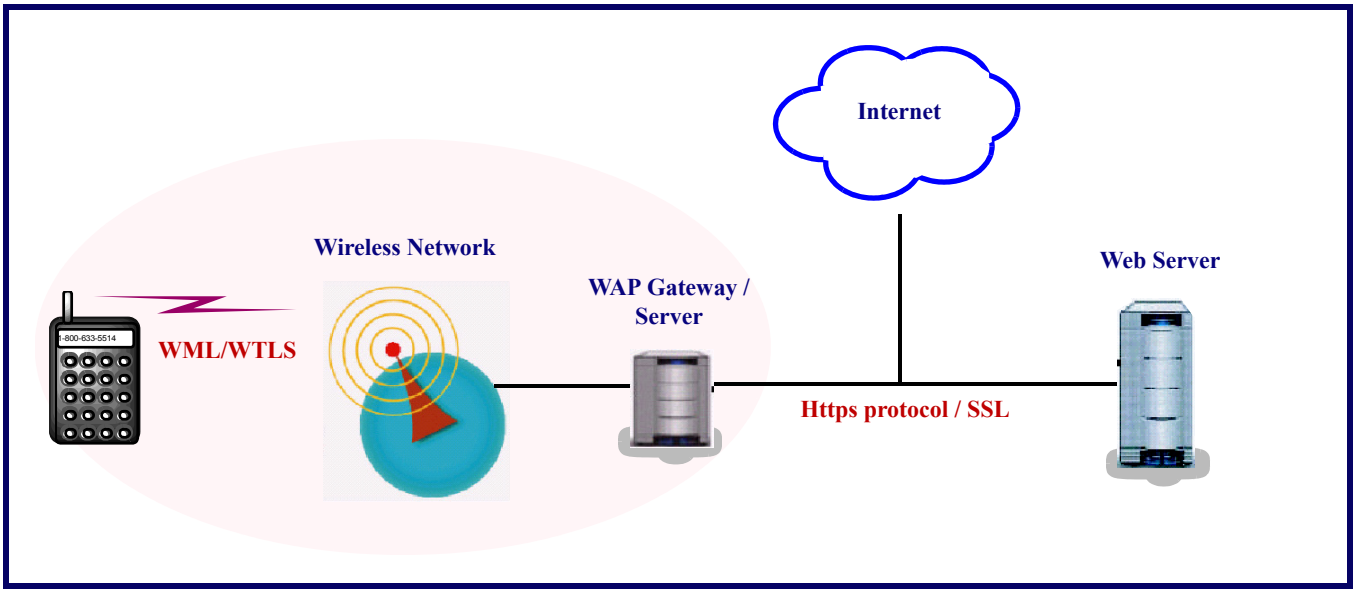


As shown, the architecture is very simple — it comprises a PC and the Web server. When, for example, someone wants to make an electronic purchase or enter some form of personal information, they generally get a pop-up window that "you are about to enter a secure site." At this point, from a technical perspective, the PC is requesting a "server certificate" from the server. The PC's browser uses this certificate — a cryptographically encoded data structure issued by a trusted certificate authority, or CA — to validate the authenticity of the server and to gain assurance that it is bona fide. For more details on the message flow, security services and mechanics of this procedure — namely on the SSL (Secure Sockets Layer) procedures — refer to February, 2000 *Wireless Security Perspectives*.

In contrast, the architecture of WAP Internet-access, as depicted in Figure 2, is three-tiered — comprising a mobile access device, a WAP Gateway and a Web Server. The scenario described above for wired SSL access works similarly in the mobile environment. However, in this mobile scenario, the "WAP gateway" performs the function of the web-browser. It issues up a certificate for validation by the wireless device. The WAP gateway and the web-server also authenticate each other, mutually, as discussed above in the two-tier scenario.

Because of the introduction of the WAP gateway in the middle — a sort of bridge between the wired and wireless worlds — a break is made in the end-to-end security. This breakpoint invokes Wireless Transport Layer Security (WTLS), securing the connection between the mobile access device and the WAP Gateway, and Secure Socket Layer (SSL), securing the connection

Figure 2: Three-tiered Wireless-Device-to-Web-Server Architecture



between the WAP Gateway and the Web Server. All points, including this break-point, require tamperproof security to enable trusted transactions and secure communications.

From an understanding of the preceding discussion, it is clear that the success of mobile commerce depends upon a security infrastructure relying upon a solution that provides end-to-end security. Digital signatures used within a Wireless Public Key Infrastructure (PKI) meet these requirements. By moving the security up to the application layer, the reliance on WTLS (and the associated weaknesses) is removed.

This is why, according to Durlacher Research, PKI will emerge as the *de facto* mobile commerce security standard. It is also why organizations such as Baltimore Technologies have been working with the WAP Forum and other industry forces to create a definitive set of global industry standards and protocols to ensure a trusted environment in which mobile business can flourish.

Wireless PKI provides such a secure and trusted trading environment by meeting the four key requirements of electronic security using cryptography, digital signatures and digital certificates.

The four key requirements are:

- **Confidentiality** — assurance that only the intended recipients can read the message transactions.
- **Authentication** — assurance that the identities of parties with whom you are doing business can be verified.
- **Integrity** — assurance that the information you send or receive is not tampered with on its journey.
- **Non-repudiation** — assurance that agreements are legally binding.

Each of these elements is fulfilled by providing each individual with a pair of keys — comprising a private key and a public key. These 'key pairs' are linked mathematically using asymmetric cryptography, and each key pair is unique. The originator uses the private key to digitally sign the message. This digital signature serves as proof of that user's identity — the equivalent of a legal handwritten signature. The recipient of the message uses the corresponding public key to verify the signature. Because it is the one and only matching key, only it can verify the signature and provide proof that the originator is who she claims to be (authentication), as well as checking that the data has not been changed in any way (integrity). The public key is stored in the user's digital certificate. The trusted "certificate authority" issues the digital certificate the same way a passport is issued by a government body. Refer to June, 2001 *Wireless Security Perspectives* for more on public key cryptography and certificates.

Encryption of data using the user's public key (or keys derived from it) can be used to protect the data (confidentiality). Finally, non-repudiation is achieved by being able to prove an identifiable user conducted a transaction. This can only be fully accomplished with support from national or international legislature. Many countries' governments support this already.

But what actually happens during a PKI-centric wireless transaction? Starting with the vendor setting up a secure WAP site, the following occurs: A mobile commerce vendor sets up a WAP site using Wireless Markup Language (WML) pages. Inside these pages, a vendor specifies tags, which call the signing function. The customer uses her WAP-enabled device — probably a phone — to access this Web site. She downloads a page, fills in a form and clicks on a button associated with the signing function.

This action will call the signing function. The customer will then be asked to enter her PIN (personal identity module). This PIN code unlocks her 'private key' stored in her Wireless Identity Module (WIM). The WIM is a specification for tamper-resistant storage. It can be implemented on any device, but it is

typically the SIM (Subscriber Identity Module). The private key is used to sign the form before it is sent back to the mobile commerce vendor. It is worth mentioning that unlocking a private key with a PIN code is already accepted as part of digital signature legislation in many countries.

When the mobile commerce vendor sees the signed data, it needs to verify that the signature is from an identifiable source in order to verify the authenticity of the user and to check the integrity of the data. It can do this by retrieving the digital certificate from a repository owned by its CA. Wireless PKI allows mobile merchants to set up their own trust domain, so they may even retrieve the certificate from their own repositories. In many countries, legislation has made this certificate legally binding. By validating digital signatures, laws provide assurance of non-repudiation.

There are many types of mobile transactions — some already taking place, others simply predicted. Wireless PKI-based technology enables secure mobile business across all of these transactions and across all wireless platforms. Additionally, building a completely new security infrastructure is not required. This will be an extension of the wired trust model of the wired organizations today.

Even though the infrastructure will remain the same, organizations need to exercise extreme caution when selecting their solution provider. The wrong decision could be the difference between an investment that will future-proof an organization's e-business infrastructure, and a substantial investment in a solution that does only part of the job. For the future-proof option, organizations should ensure the solution provides scalability, end-to-end security and compatibility, as discussed below:

- **Scalability —** Given the predicted growth rate of mobile subscribers (more than one billion by 2003), any solution must be capable of making the millions of connections the market will demand in years to come. The WAP Forum's new security standards, for instance, are designed to ensure such scalability.
- **End-to-end security** — Secure transfer from the mobile customer to the m-commerce vendor is absolutely essential. Without it, the 'Gap in WAP' may seriously compromise the security. Only a PKI-centric solution can provide such end-to-end security.
- **Compatibility** — With today's mobile access devices, as well as with evolving technology, standards and protocols must work with an organization's existing security infrastructure or any future infrastructure. There are many approaches to PKI implementation, with just as many incompatible solutions available from different vendors. It is prudent to look for a solution that guarantees interoperability. Many organizations have already signed an interoperability pact for their PKI products, so optimal solutions will be available.

Furthermore, the security framework that a wireless PKI provides creates a trusted environment for all wireless communication, whether it is via WAP, i-mode, wireless IP, mobile IP or HDML. Even if WAP doesn't survive, wireless PKI is the true key to a secure mobile economy. Without security, all the hype surrounding m-commerce will never amount to anything.

About the Author

Guy Singh is a product manager at Baltimore Technologies. He is responsible for Baltimore Telepathy, wireless e-security products that secure mobile commerce. Guy is an official representative and speaker for Baltimore at the WAP forum. He has been involved in the IT industry for 10 years, working in a wide range of environments including the European Space Agency, telecoms, brokerages, hardware/software OEMs and mobile communications. During this time he has held posts in research and development, engineering, product marketing and product management. He is a regular speaker at public and commercial events including the first World Wide Web Conference, RSA 2000, Java 98, Intranet Expo, Internet World, Global e-Security 99 and is an official speaker for the WAP Forum. Guy holds degrees from Kings College, London and the University of Liverpool.

Fraud And Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following 10 fraud and security patents. The patent number, invention title, inventor, and assignee (owner) are provided. All of these patents were granted in either July or August 2001.

These may be of interest to some of our wireless security practitioners. 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, the references cited or other references included in the patent. For select patents provided below, we provide the URL and contact information for the assignee.

US Patent: 6,272,536

Issued: August 7

Title: System and method for the distribution of code and data

Inventor: Arthur van Hoff et. al.

Assignee: Marimba Inc.
www.marimba.com

Contact:
Marimba, Inc.
440 Clyde Ave.
Mountain View, CA 94043

Telephone: (650) 930-5282

US Patent: 6,270,011

Issued: August 7

Title: Remote credit card authentication system

Inventor: Ofer Gottfried

Assignees: Benensen Tal; Mimoun Elie

US Patent: 6,269,348

Issued: July 31

Title: Tokenless biometric electronic debit and credit transactions

Inventor: David Pare et. al.

Assignee: Veristar Corporation
www.smarttouch.com

Contact:

VeriStar Corporation
Tenth Floor
155 Grand Avenue
Oakland, California 94612
Telephone: (510) 268-8900
(or toll-free: 866-VERISTAR)

US Patent: 6,269,164

Issued: July 31

Title: Method of and system for encrypting messages

Inventor: Paul Pires

Assignee: same

US Patent: 6,266,430

Issued: July 24

Title: Audio or video steganography

Inventor: Geoffrey Rhoads

Assignee: Digimarc Corporation
www.digimarc.com

Contact:

Digimarc Corporation
19801 SW 72nd Ave. Suite 100
Tualatin, OR 97062

Telephone: (503) 885-9699
(or toll-free at 800-DIGIMARC)

US Patent: 6,263,447

Issued: July 17

Title: System and method for authentication of network users

Inventor: Jennifer French et. al.

Assignee: Equifax Inc.

US Patent: 6,263,438

Issued: July 17

Title: Method and apparatus for secure document timestamping

Inventor: Jay Walker et. al.

Assignee: Walker Digital, LLC.
www.walkerdigital.com

Contact:

Walker Digital
5 High Ridge Park
Stamford, CT. 06905

Telephone: (203) 461-7000

US Patent: 6,260,146

Issued: July 10

Title: Method and apparatus for securing and authenticating encoded data and documents containing such data

Inventors: Robert Mos and Clay Von Mueller

Assignee: Semtek Innovative Solutions, Inc. www.semtek.com

Contact:

Semtek Innovative Solutions Corporation
4217-A Ponderosa Avenue
San Diego, California 92123

Telephone: (858) 278-6003

US Patent: 6,259,907

Issued: July 10

Title: System and method of retrieving and formatting data from cellular telephone switches

Inventor: Gary Bellamy et. al.

Assignee: GTE Wireless Service Corporation

US Patent: 6,256,741

Issued: July 3

Title: Specifying security protocols and policy constraints in distributed systems

Inventor: Stuart Stubblebine

Assignee: AT&T Corporation

To review the specification and claims of these patents visit the US Patent and Trademark Office web-site at www.uspto.gov. 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