white paper

phone.com

Understanding Security on the Wireless Internet

How WAP Security Is Enabling Wireless E-commerce Applications for Today and Tomorrow

About Phone.com

Phone.com, Inc. is a leading provider of software that enables the delivery of Internet-based services to mass-market wireless telephones. Using its software, wireless subscribers have access to Internet- and corporate intranet-based services, including email, news, stocks, weather, travel and sports. In addition, subscribers have access via their wireless telephones to network operators' intranet-based telephony services, which may include over-the-air activation, call management, billing history information, pricing plan subscription and voice message management. Visit http://www.phone.com for more information.

Part Number WPSE-R4-001 January 2000

UNDERSTANDING SECURITY ON THE WIRELESS INTERNET

How WAP Security Is Enabling Wireless E-commerce Applications for Today and Tomorrow

Executive Summary

With the advent of e-commerce and e-banking, the Internet has changed the way many people purchase goods and manage their finances. Online trading, banking and shopping are available today to millions of Internet users. These services are now emerging on the *wireless* Internet, allowing subscribers to access bank accounts, trade stocks and purchase goods right from the screen of their wireless phone. This new avenue onto the Internet has been made possible in large part by the Wireless Application Protocol (WAP), a de-facto standard developed by the WAP Forum, a group of over 200 telecommunications and software companies. According to Strategy Analytics, there will be over 525 million WAP-enabled handsets in the marketplace by the year 2003.

WAP has stimulated application development by providing a common, secure protocol that allows applications to be written for use across existing wireless networks. Hundreds of applications that take advantage of this common application environment are now available. Many of these applications use WAP's security mechanism to ensure that transactions over the wireless Internet are safe and secure. Examples include wireless banking from Bank of Montreal, wireless stock trading from Ameritrade and Charles Schwab Canada, and wireless e-commerce from Amazon.com.

This paper explains the WAP security model and the Wireless Transport Layer Security (WTLS) mechanism, which provide a safe and secure environment for wireless Internet transactions today. It explains the key issues that any data security system must address and it describes how the WAP model addresses these issues. It also presents ideas for future improvements that the WAP Forum is considering for the next generation of WAP security. A final section discusses how Phone.com provides solutions today that offer complete WAP security for network operators, subscribers and content providers.

The Wireless Internet Is Already Here

Wireless Internet access represents the next wave of the Internet. This trend is being spurred by the mobile phone industry's widespread support of the Wireless Application Protocol. By enabling WAP applications, a full range of wireless devices, including mobile phones, smartphones, PDAs and handheld PCs, gain a common method for accessing Internet information.

Strategy Analytics has reported that in 2003, ninety-five percent of all handsets shipped will include WAP support. According to The Strategis Group, there are more than 32 million professional mobile data users in the U.S. marketplace today and demand in this segment will continue to grow. With expanding subscriber bases and demand for new wireless data services driving phone sales, operators and manufacturers expect increased revenues from the sale of wireless Internet services and devices.

Analysts expect dynamic growth in the mobile market, with a forecast of more than one billion mobile phones in use within the next three to four years. According to Gartner Group, mobile phones are expected to be the most common client device accessing the Internet worldwide by 2005. Ovum has reported that smartphones and data-centric terminals will account for as much as two-thirds of the estimated USD $67 billion handset market in 2004.

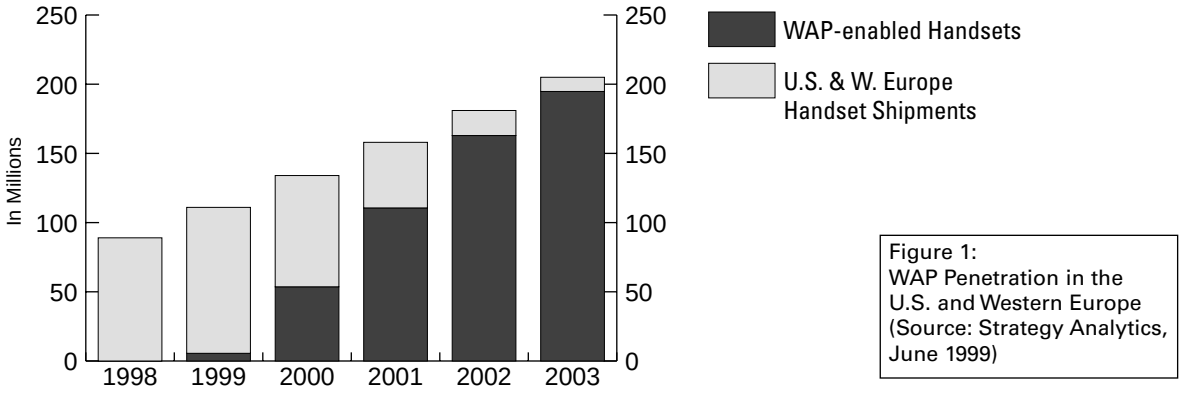

Figure 1:
WAP Penetration in the U.S. and Western Europe (Source: Strategy Analytics, June 1999)

All of these statistics demonstrate the enormous demand for wireless Internet services and applications. WAP enables rapid application deployment and provides access to the broadest consumer base possible because WAP was designed to operate on top of any type of wireless data network. Whether network operators are deploying CDMA, CDPD, GPRS, GSM, iDEN, PDC or TDMA data solutions, application providers can reach subscribers across multiple operator networks with a single application.

Sparked by an open, Web-based protocol, network operators, handset manufacturers and content developers have all implemented solutions that have led to a groundswell of support for WAP deployments around the world. Applications exist today to view a variety of Web content, manage email from the handset and gain better access to network operators' enhanced services. Beyond these information services, content providers are now developing solutions for the latest Internet opportunity—wireless e-commerce.

Recently, Ameritrade made its service WAP-capable for U.S. mobile phone users. Thomas K. Lewis, Jr., co-chief executive officer of Ameritrade Holding Corporation, noted in a recent press release that the addition of wireless Web access is another step in Ameritrade's continuing effort to extend the ability of its customers to invest when and how they choose. "Ameritrade is a customer-oriented organization," Lewis said. "We know that our customers want to be empowered to act on their investment decisions at any given moment."

As more subscribers demand WAP services, the need for wireless Internet security will continue to grow. In the mid-nineties, a push to provide strong encryption occurred in hopes of fostering electronic commerce. For years, the “next killer app" hype surrounded electronic commerce. But until Secure Sockets Layer (SSL) and encryption became widespread de-facto security standards, electronic commerce was only a curiosity, not a mass-market opportunity. By 1998, the security infrastructure was in place, triggering a dramatic increase in electronic commerce transactions. Nineteen ninety-eight became the year of e-commerce, with Internet operations challenging traditional "brick and mortar" operations for the first time. Now the industry is poised to take its next big leap forward—into the wireless world.

In June of 1999, the WAP Forum formally approved WAP Version 1.1. WAP 1.1 includes the Wireless Transport Layer Security (WTLS) specification, which defines how Internet security is extended to the wireless Internet. WTLS is poised to do for the wireless Internet what SSL did for the Internet—open whole new markets to e-commerce opportunities. Network operators providing application developers and end users with effective WAP-based wireless security are capitalizing on this emerging trend.

Security on the Internet

A first step to understanding how the WAP security model works is to review how SSL security makes e-commerce secure over the Internet. Today's security solutions keep information away from individuals that should not have access to confidential or financial data. Security protects mission-critical information that can be used against a corporation or used to create fraudulent transactions. Additionally, security provides peace of mind, ensuring that individuals and institutions are comfortable conducting business and exchanging information online.

There are four different concerns that a security system can address: privacy, integrity, authenticity and non-repudiation.

Privacy ensures that only the sender and the intended recipient of an encrypted message can read the contents of that message. To guarantee privacy, a security solution must ensure that no one can see, access or use private information, such as addresses, credit card information and phone numbers, as it is transmitted over the Internet.

Integrity ensures the detection of any change in the content of a message between the time it is sent and the time it is received. For example, when a user instructs a bank to transfer $1000 from one account to another, integrity guarantees that the account numbers and dollar amount in the user's message cannot be altered without the bank or the user noticing. If the message is altered in any way during transmission, the security system must have a way of detecting and reporting this alteration. In many systems, if an alteration is detected, the receiving system requests that the message be resent.

Authentication ensures that all parties in a communication are who they claim to be. *Server authentication* provides a way for users to verify that they are really communicating with the Web site they believe they are connected to. *Client authentication* ensures that the user is who they claim to be. Examples of authentication in the real world include presenting a driver's license to verify that a consumer writing a check is the person named on that check, and presenting a corporate photo ID to prove that a telephone technician really works for the telephone company.

Non-repudiation provides a method to guarantee that a party to a transaction cannot falsely claim that they did not participate in that transaction. In the real world, handwritten signatures are used to ensure this. When a consumer writes a check, presenting a driver's license ensures the identity of the writer (authentication), while the signature on the check ensures that the consumer was in fact present and agreed to write the check (non-repudiation).

Over the Internet, the Secure Socket Layer (SSL) protocol, digital certificates and either user name/password pairs or digital signatures are used together to provide all four types of security. The following explains these different techniques.

Public key cryptography is an encryption method that is a key component of SSL. It uses pairs of keys and mathematical algorithms to convert clear text into encrypted data and back again. The pair consists of a registered *public key* and a *private key* that is kept secret by its owner. A message encrypted with the public key can be decrypted only by someone with the private key. Likewise, a message encrypted with the private key can be decrypted only by someone with the public key.

Public key cryptography uses very advanced algorithms to encrypt small amounts of information but is impractical for encrypting large quantities of data. Faster *bulk encryption algorithms* use a *shared secret key* between the communicating parties to encrypt most secure messages on the Internet. These algorithms are extremely difficult to decode when the shared secret key contains a large number of bits. SSL uses public key cryptography to exchange this key at the beginning of a secure Internet conversation, thus ensuring that it remains a secret for the duration of the conversation.

SSL uses public key cryptography, bulk encryption algorithms and shared secret key exchange techniques to provide privacy over the Internet. To provide integrity, SSL uses *hashing algorithms* that create a small mathematical fingerprint of a message. If any part of the message is altered, it will not match its fingerprint when the message is checked at the receiving end. In this case, the sender is asked to resend the message.

Because anyone can generate key pairs, it is possible for a malicious party to put up an impostor Web site and then falsify information in a transaction by providing a public key to a user. To prevent this kind of fraud, *digital certificates* are used to provide an authenticated way to distribute public and private keys. Digital certificates are also used to authenticate the parties of an Internet conversation so that users and content providers can both be confident they know who they are communicating with.

There are two different kinds of digital certificates—*server certificates* and *client certificates*. Server certificates are used to authenticate that a Web server is what it claims to be. Client or personal certificates are used to authenticate the identity of an individual user on the Internet. Both types of certificates include the certificate holder's identity and public key, and other information used to authenticate the certificate. Most importantly, the certificate is itself encrypted with the private key of a *certificate authority*, creating an independent binding of the public key and the certificate holder. Third party companies like VeriSign and RSA Security operate as certificate authorities, providing a respected, independent resource to issue keys and certificates to their holders.

When a Web browser requests a secure conversation with a Web server, the server provides the browser with its server certificate. The browser authenticates the Web server by confirming that a valid certificate authority encrypted the certificate. It then uses the public key stored in the certificate to encrypt a shared secret key to send to the Web server. The shared secret key is used to encrypt the rest of the conversation. By using a server certificate, the Web server and browser can have a secure conversation that is private and authenticated, with guaranteed integrity.

Note that in this example only the server has been authenticated. Client certificates can be used to authenticate a user to the Web server but today most Web applications rely on a simple user name and password to authenticate the user of the browser client.

The remaining issue to address is non-repudiation. As with client authentication, most Web applications today simply rely on the entry of a user name and password to provide non-repudiation. Applications can request a *digital signature* from a client, which requests that the user specifically authorize a transaction. The authorization is then encrypted utilizing the user's private key from their client certificate. Not surprisingly, a digital signature is analogous to a real signature on a check and serves the same purpose. So far though, the adoption of client certificates for use by individuals on the Internet has been slow.

Good network security solutions require that content providers and clients manage and maintain their digital certificates and other security information carefully. *Public Key Infrastructure (PKI)* solutions help companies manage this information so that it is secure and easy to organize. PKI contains three common functional components: the certificate authority to issue certificates (in-house or outsourced); a repository for keys, certificates and certificate revocation lists on an LDAP-enabled directory service; and a management function, typically implemented via a management console. Additionally, PKIs can provide key recovery in case a user loses their private key due to a hardware failure or other problem.

Different combinations of all of these security techniques are used for different applications, depending on which forms of security are important and the degree to which the solution needs to be balanced with the convenience for the user. For example, certificate-based client authentication and non-repudiation are not widely used on the Web today because most users don't want to be bothered with the administrative tasks of obtaining and safely maintaining a client certificate.

Security in a WAP Environment

There are three parts to the WAP security model, as shown in the figure below. On the right, the WAP gateway simply uses SSL to communicate securely with a Web server, ensuring privacy, integrity and server authenticity.

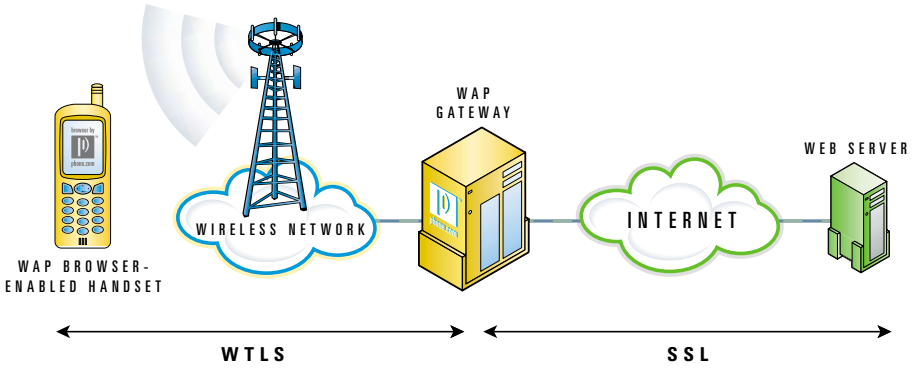

Figure 2: The WAP Security Model

On the left side of Figure 2, the WAP gateway takes SSL-encrypted messages from the Web and translates them for transmission over wireless networks using WAP's WTLS security protocol. Messages from the handset to the Web server are likewise converted from WTLS to SSL. In essence, the WAP gateway is a bridge between the WTLS and SSL security protocols.

The need for translation between SSL and WTLS is incurred by the very nature of wireless communications: low bandwidth transmissions with high latency. Because SSL was designed for desktop and wired environments with robust processing capabilities connected to a relatively high-bandwidth and low-latency Internet connection, cell phone users would be disappointed by the delays required to process SSL transactions. Furthermore, to put SSL functionality into handsets would raise cell phone costs and destroy the low-cost pricing paradigm that is driving industry growth.

WTLS was specifically designed to conduct secure transactions without requiring desktop levels of processing power and memory in the handset. WTLS processes security algorithms faster by minimizing protocol overhead and enables more data compression than traditional SSL solutions. As a result, WTLS can perform security well within the constraints of a wireless network. These optimizations mean that smaller, portable consumer devices can now communicate securely over the Internet.

The translation between SSL and WTLS takes milliseconds and occurs in the memory of the WAP gateway, allowing for a virtual, secure connection between the two protocols. Suppliers of the WAP gateway and network operators take every measure possible to keep the WAP gateway itself secure by:

1. Ensuring that the WAP gateway never stores decrypted content on secondary media.
2. Using a process of decryption/re-encryption that is security conscious and optimized for speed so that the unencrypted content of a message is erased from the volatile internal memory of the WAP gateway as quickly as possible.
3. Securing the WAP gateway physically so that only authorized administrators have access to the system console.
4. Limiting administrative access to the WAP gateway so that it is not available to any remote site outside the carrier's firewall.
5. Applying all other security precautions used to protect billing systems and the Home Location Register to the WAP gateway.

On the wireless side of the transaction (the left side of Figure 2), the WAP gateway uses WTLS to provide privacy, integrity and authentication between itself and the WAP browser client. It is based on the Internet standard security protocol TLS 1.0, which in turn is based on SSL 3.0, providing the functionality of a strong Internet security standard over a wireless airlink. WTLS goes beyond TLS 1.0 by incorporating new features such as datagram support, optimized handshake and dynamic key refreshing.

Although the WAP security model does not call for non-repudiation or client authentication, a particular gateway provider's implementation can provide this with the use of client certificate and digital signature technology. Applications can implement client authentication and non-repudiation by following the standard Web development practice of requiring users to enter a username and password.

WTLS and the WAP security model provide an extremely secure solution that leverages the best technologies from the Internet and wireless worlds. When the WAP gateway is deployed in an operator environment according to standard operator security procedures, subscribers and content providers can be assured that their personal data and applications are secure.

Next Generation WAP Security

The current WAP security model requires a strong relationship between the network operator and the content provider to implement the most secure solutions possible. The WAP Forum has recognized that as the market for highly secure applications increases, a more flexible and extensible solution will be needed. When working across many different wireless networks, application developers must be assured that their content remains encrypted from the time it leaves their application server until it arrives at the WAP handset. Phone.com has been participating in the WAP process to develop this more advanced security solution, which must address the enterprise's need for higher security and the operator's need for proper integration with WAP gateways in the wireless network.

Solutions are now coming to market before the WAP Forum has established a standard approach to providing end-to-end secure content. Besides being proprietary, these solutions promote installing a WAP Gateway at a content provider or in an enterprise. Since WAP Gateways were designed for use in an operator's network, this creates a number of difficulties for content providers, subscribers and wireless network operators.

- Operating a WAP gateway at the content source places a burden on the content provider to maintain a system that is compatible with a variety of network protocols and SMSCs. For each network and SMSC combination, the content provider will have to support a different configuration on their gateway. This goes against one of the original goals of the WAP Forum to provide content solutions that are network independent and increases the effort required for the content developer to deliver services to the wireless Internet.
- Content providers are burdened with handset provisioning and activation issues. The content site must either limit their offering to a small number of handset models or take on the burden of supporting a broad array of devices.
- Because these solutions are proprietary, they do not work across all WAP handsets. In some cases, they work with only a single handset model, limiting the subscriber population that content providers can reach.
- Subscribers will find it difficult to switch between an operator's network-based WAP gateway and the content provider's or enterprise's gateway. This manual switching requires changing raw handset parameters each time the subscriber wishes to contact a different site. Furthermore, when the subscriber experiences difficulty, both the network operator and the content provider will experience increased support costs.
- Subscribers will have more difficulty getting quality of service issues resolved. Where does a subscriber call to report a problem with a handset that was supplied by a content provider and is connecting to the content provider's WAP gateway but service is being provided by a network operator? The operator? The content provider? The handset manufacturer?

- Operators must trust equipment operated outside their network that interacts closely with their network elements. This can lead to traffic management problems, for example systems out of their control could flood their networks with SMS messages. This has an adverse effect on the content provider as well because their system must compete with others like it for an unknown amount of network resources, which may lead to poor quality of service for the subscriber.

A solution intended for enterprises and content sites should be designed to meet their unique needs and address the real issues of offering seamless, quality service that integrates well with an operator's WAP gateway. A well-designed enterprise WAP solution should:

- Insulate the content site from the implementation details of the wireless network so that applications remain network- and SMSC-independent.
- Leverage the existing activation and provisioning systems in the operator's network to shield content developers from these issues.
- Enable access from any WAP-compatible handset.
- Provide a simple, transparent way for subscribers to access enterprise WAP sites. It should be as easy to access one of these sites as it is today to access a standard WAP content site.
- Make it easy to identify whether a quality of service issue lies with the operator's network systems or the content provider's Web server. This allows network operators and content providers to ensure customer satisfaction by helping to quickly resolve service issues.
- Allow the network WAP gateway to work closely with the enterprise WAP solution so that network resources can be properly utilized and shared across the wireless Internet subscriber population.
- Allow application developers to integrate WAP technology that can encrypt content using WTLS and send it through the Internet to operators' networks.
- Offer the proper interfaces to integrate with the content provider's existing Public Key Infrastructure (PKI) solution, allowing for ease of integration into the provider's existing e-commerce systems.
- Provide a clear upgrade path from existing WTLS 1.1-compatible applications to this new grade of WAP security.

Enabling content developers to build solutions that are network independent and secure from end-to-end is essential. With a high-quality, well-designed solution that integrates seamlessly with network WAP gateway solutions, both content developers and network operators will benefit from the continued growth of value-added subscriber applications.

WAP Security: Today and Tomorrow

Application providers and wireless network users should feel confident that today's transactions leverage the best security provisions that SSL offers through the robust WTLS implementation. Already, key Internet applications for handsets have been deployed, including e-banking, stock trading, e-commerce, and other exchanges of private and mission-critical data.

With WTLS optimized to ensure transactions are conducted in a secure and user-friendly way, and WAP-capable handsets reaching the market, subscribers are beginning to embrace wireless e-commerce in the same fashion that consumers adopted wired e-commerce over the last 18 months. As application developers realize returns on WAP applications, the market is expected to grow rapidly, leading to a wealth of secure, wireless e-commerce applications. Application developers are further assured of their investment since the WAP Forum is already working to develop even more secure solutions for the future.

Please continue on for an overview of Phone.com's wireless security solutions.

Phone.com Extends WAP Leadership with Advanced Security Solutions

Phone.com has developed its security solutions as part of its commitment to lead the convergence of wireless phones and the Internet. Since 1996, Phone.com has been developing and deploying wireless Internet solutions, giving the company unmatched experience in the field. This extensive market experience has already helped wireless operators around the world, such as AT&T, DDI, IDO, SFR and Sprint PCS, launch commercial wireless Internet services.

Phone.com is a founding member of the Wireless Application Protocol (WAP) Forum, the industry organization that delivered the de-facto worldwide standard for wireless Internet solutions. Given Phone.com's experience in leveraging WAP, application developers and network operators can feel confident in the company's ability to provide secure transactions on the variety of handsets that are compliant with the WAP standard.

Phone.com was the first to provide secure wireless Internet communication to browser-enabled handsets with its HDTP 2.0 standard, made commercially available in 1997. More recently, Phone.com was the first to provide commercial availability of a WAP 1.1-compliant gateway with a complete implementation of WTLS 1.1.

As a result of this work, Phone.com has developed a deep understanding of security issues and the highly successful UP.Link™ WAP Gateway includes security features unmatched in the industry. For example, UP.Link WAP Gateway provides client certificate support that allows Web servers to authenticate UP.Link WAP Gateway on behalf of its subscribers. With the existing Internet standard use of user names and passwords, content providers can already implement secure applications that offer privacy, integrity, authentication and non-repudiation.

UP.Link WAP Gateway offers flexible certificate authority support, including pre-configurations to support server certificates authenticated by VeriSign, Thawte and RSA. This flexibility allows network operators to add other certificate authorities so they can support their own internal certificate authority if desired.

UP.Link WAP Gateway supports standard RSA_anon algorithms for public/private key encryption, available with both 1024-bit (U.S. domestic) and 512-bit (export) key lengths. In addition, UP.Link WAP Gateway offers support for both the 56-bit (export) and 128-bit (U.S. domestic) RC4, RC5 and DES encryption standards for bulk encryption. UP.Link WAP Gateway also supports the MD5 and SHA-1 hash standards.

UP.Link WAP Gateway is the only WAP gateway to offer both RSA and Diffie-Hellman key exchange algorithms as part of its WTLS implementation. This allows it to provide secure connections to the broadest selection of WAP handsets in the industry, including all handsets that use the UP.Browser™ microbrowser, as well as other popular handsets, such as the Nokia 7110.

To address the need for strong security in the international market, Phone.com recently established a major development center in Northern Ireland. In the near future, Phone.com expects to be shipping 128-bit security solutions for use in countries outside the United States.

In the data exchange between SSL and WTLS protocols described earlier in this document, the payload transmitted between the handset and the Web server is unencrypted for a very brief moment inside the UP.Link WAP Gateway. Besides the suggestions recommended earlier, the UP.Link WAP Gateway takes additional steps to make it extremely difficult to access messages while they are being translated. The following are a series of additional measures UP.Link provides to enhance security.

1. The UP.Link's encryption/decryption algorithm operates in a single UNIX process. This guarantees that unencrypted data never leaves the particular server processing the transaction and even within that single server, data is never passed through an insecure inter-process communication (IPC) mechanism between processes. The algorithm has been optimized to minimize the time unencrypted data is stored in memory and it explicitly erases the contents from memory when the security protocol translation is completed.
2. Only the UNIX root account can attempt to view an unencrypted message.

3. The root password can be used only from the physical console; remote logins using the root password are not allowed.
4. A strong background in UNIX system administration and memory architecture is needed to even attempt to grab unencrypted data. UP.Link Administration does not include any tools that could be used to view unencrypted data.
5. It is extremely difficult to find unencrypted data in memory. Special UNIX tools available only to the root account would be needed to view memory and even then a large amount of data sifting is required to figure out where and when a transaction occurred. Since transactions are in memory only a short time, this approach becomes extremely difficult.
6. Access to WTLS transmissions requires extensive knowledge of Phone.com's WAP implementation. Some of the information required to attempt a WAP gateway penetration is not provided in any documentation that a network operator receives from Phone.com.

Even if these six protections were overcome, attempting to inject a fraudulent transaction into the gateway from the console is even less likely. Phone.com's additional security guards provide a secure solution, suitable for many classes of wireless applications.

Any WAP solution designed for providing secure transmissions on wireless networks must address equally the needs of subscribers, network operators and content providers. This solution must be an open, accepted standard so that all industry participants can implement interoperable solutions. Phone.com is actively developing the strongest security standards possible. In addition, Phone.com is working closely with the WAP Forum to assure these standards of excellence become the next generation security solution that will take wireless e-commerce to the next level of mass-market acceptance.

With more commercial deployments of wireless Internet solutions than any other provider, Phone.com has the experience and expertise to provide network operators, content providers and subscribers with robust, secure solutions today. Contact your Phone.com™ representative for more information on how your company can become a part of the next wave of e-commerce - *wireless* e-commerce.

Phone.com, Inc.
800 Chesapeake Drive
Redwood City, CA 94063 USA
Americas: +1 650 562 0200
Europe: +44 (0)1707 828 051
Asia Pacific: +81 3 5325 9211
http://www.phone.com