# Security in a Mobile World

## Security is a concern with wireless services and businesses who take full advantage of the wireless Internet.

By John Mennel, 724 Solutions

As mobile Internet-enabled devices become more pervasive in the homes and working lives of consumers, the demand to provide services traditionally available on desktop computers grows as well. Instant-on access to the Internet as well as increasing bandwidth and full-time connectivity will soon be challenging the dominance of the PC as our Internet appliance of choice. Companies recognize the potential of delivering new and existing services over these new channels. According to Jupiter Communications, there will be 79.4 million browser-enabled mobile phones in operation by 2003. Meridien Research states there will be 500 million potential consumers of digital wireless device users by 2003. These are the users that will drive the demand for wireless Internet banking, stock trading and retail transactions.

Security is the most commonly cited reason for consumers' hesitation to use online services such as banking and shopping. It's not surprising, then, that concerns become even greater as we move from the wired desktop to portable devices. In a study done by Ipsos Reid in 2000, 10 percent of the respondents interested in wireless services were highly concerned about security. And as the security of these services increased in 2001, the change in reply by respondents declined to seven percent. However, it won't be enough for businesses to simply assure their partners and customers that they have a secure mobile infrastructure; they must be able to demonstrate that they have the technology in place to meet security challenges.

Mobile transactions use many of the same security building blocks as the wired Internet. However, there are some significant differences in implementation and architecture, and it is crucial that business and IT decision-makers understand these differences as they build secure mobile applications.

**Managing the Risks**

It is imperative that businesses understand the security threats posed by the Internet and wireless environments, and implement specific safeguards that can mitigate risk exposure. In order for consumers to routinely use mobile transactions, they must first accept the fundamental principles of security:

&#149Respect for privacy;
&#149Protection of confidential information;
&#149Assurance of business integrity;
&#149Validation of identity; and
&#149The ability to prove that a transaction has occurred based on agreed terms (this proof is particularly important where a settlement is not instantaneous).

For both businesses and end-users, this means:
&#149Financial and personal information should never be disclosed to unauthorized parties;
&#149All information should be protected to prevent others from stealing or modifying that information;
&#149User and service identities must be verified; and
&#149Personalized privilege and authority policies should be enforced, and the wireless platform should have a mechanism (e.g., a &quotdigital trail&quot) that prevents repudiation.

Security is a matter of risk management, with the objective being mitigation according to acceptable risk criteria. With wireless devices receiving considerable attention, a new set of security concerns are raised.

**Security Zones**

Wireless solutions can be separated into different areas and managed as three different security zones: the Device Zone, the Network Infrastructure Zone and the Enterprise Zone. Each zone is a distinct trust domain with its own security policies and practices.

*Zone 1: Device Zone*

The Device Zone is comprised of the actual devices &#151 mobile phones, personal digital assistants (PDAs) or pagers &#151 used for wireless transactions. These devices are the &quotfront end,&quot and a key component in the user experience; this is where the user interacts with an application. Therefore, device designers and makers must consider including security safeguards for wireless data on their devices.

The easiest way to secure wireless data is to encrypt it, though most devices have their own security capabilities. Examples include:
&#149On Wireless Application Protocol- (WAP)-enabled devices, security algorithms enable WTLS between the device and the WAP gateway;
&#149On the Palm VII, Elliptical Curve Cryptography (ECC) is embedded in the Palm operating system to enable secure communications between the device and the Palm.net gateway; and
&#149Using smart cards on Global System for Mobile Communications (GSM) handsets, public key infrastructure (PKI) functionality enables transaction confidentiality and digital signatures for non-repudiation and strong authentication.

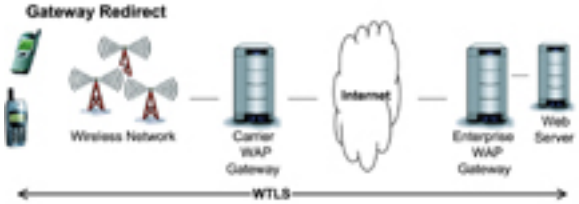
Security companies have developed, or are developing, products to enhance device security. One example is a wireless VPN solution that allows IT professionals to extend their VPN to the wireless world. Others provide a user-friendly method for maintaining encrypted data on PDAs or have biometrics &#151 integrated authentication included in the device and/or application.

*Zone 2: Network and Carrier Infrastructure Zone*

The Network and Carrier Infrastructure Zone is comprised of the device's network delivery and carrier infrastructure providing the communications channel into the business.

Information transmitted by the mobile device and received from the business passes through a secure communications channel that ensures both confidentiality and data integrity. Generally, sensitive information is encrypted at the transport

layer for communication using a strong 128-bit cipher, the strongest cryptographic technology exportable for commercial use.
It is important to note that the transport layer security is not continuous between some devices and the business. In these instances, the exposure can be addressed through best-practices security safeguards at the mobile network service provider's gateway site. Organizations, including financial institutions, enact a service-level agreement with the carrier(s) for physical security of the gateway and related information assets hosted at the carrier site.




Wireless Application Protocol (WAP) has two scenarios to consider. The first is the carrier model, in which the enterprise uses the carrier WAP gateway to terminate the WAP protocol. It receives the hypertext transfer protocol (HTTP) traffic from the Internet or a VPN. The advantage of this model is that the enterprise does not have to operate a gateway onsite or provide devices; the disadvantage is the existence of the two-zone security exposure, for which the enterprise will need to perform extra due diligence to ensure the security of the gateway operating at the carrier site.
The other model for WAP gateway operation is the enterprise model, in which the enterprise operates its own WAP gateway on its own premises. One advantage of this model is true end-to-end security, since the WAP (and, thereby, the WTLS session) terminates at the enterprise. Additionally, it is network- and carrier-independent, and the enterprise has control of service levels. The disadvantage is that it is technically harder to configure devices.
*Zone 3: Enterprise Zone*
A business' wireless solution includes its mid-tier transaction system, wireless platform, network infrastructure, and content aggregation services for delivering stock quotes, news, weather and other lifestyle information, as well as the user experience and transaction processing systems. All of these components are situated behind the company's firewall.
When choosing a secure mobile infrastructure, a company should select a vendor with a product portfolio that contains the following components:
&#149Device adapters that transform business data, optimizing for specific device display limitations and interface;
&#149Back-end gateways that act as a message switch for servers at the enterprise;
&#149Wireless applications;
&#149Application framework; and
&#149A platform for high availability, scalability and performance of mobile transactions.

The application framework allows for rapid development of mobile applications, and provides session, user and device data management, policy management, logging,

and presentation. It is the common architectural framework for customer-developed applications and includes:
&#149Session management - supports secure wireless cookies and tokens in uniform resource locators (URLs) or in the HTTP header;
&#149Privileged management infrastructure (PMI) - allows management entitlements and enforcement policies for access control according to business rules and object permission attributes; this limits access to services and administration functions, and applies risk management policies to map transactions to device capabilities;
&#149Authentication service - must be flexible to support various enterprise authentication requirements;
&#149Contract management service - allows the business to specify the content and format of the contract to be signed by the end-user for non-repudiable transactions; and
&#149Secure transaction processor - responsible for verifying digital signatures.

In addition to the above security services, the product portfolio should provide mechanisms for logging system events and transactions without capturing sensitive transaction data. These logs can be used to detect security incidents such as attempted intrusions or unauthorized use. Moreover, they may serve as evidence in legal cases involving fraud (i.e., transaction repudiation), embezzlement, theft or mischief.
The components in the product portfolio should be on-premise software solutions for the enterprise. This is the recommended deployment scenario, as the enterprise zone is assumed to be an environment that is deemed trustworthy &#151 where recommended policies and industry best-practices for ensuring operating system platform, network, and physical security are implemented and access to the environment is limited to specific authorized individuals. This deployment scenario also gives the business control over service levels.
Many companies choose to operate security features behind the firewall. However, these components can also be operated by a carrier or by a trusted third party, which means transactions must be carried over the Internet &#151 making part of this zone much less trustworthy. Two security options are available to mitigate the risks in this circumstance: (1) the back-end gateways should be configured to use a secure RSA-based 128-bit secure socket layer (SSL) connection; or (2) a secure leased line &#151 ideally, with VPN firewall routers &#151 between the mid-tier and the business' system should be constructed.

**Public Key Infrastructure**

Support for strong authentication and non-repudiation using digital signatures, and for end-to-end confidentiality, requires a full PKI implementation for the management of public keys and certificates. A digital certificate is a digitally signed electronic document issued by a trusted certification authority (CA) attesting to the logical binding of a public key to the identity of its owner.
Most companies have deployed, or will deploy, a PKI solution from a vendor of choice. To leverage its existing infrastructure, a business needs a solution that can extend the same level of security offered by PKI to wireless devices. The PKI Gateway is designed to handle and route certificate requests from supported end-user devices to one or more CA/RA (registration authority), regardless of the CA/RA product vendor(s) and technologies used in the PKI.

PKI allows users to strongly authenticate themselves to an organization. By unlocking their key, the user is telling the business he is communicating with that he is indeed who he says he is, and he is supposed to have access to those accounts. PKI also allows a business to extend its basic wireless offerings to include high-value transactions such as the down payment on a home, or commercial banking.*

The digital signature legislation that has been passed in various countries around the world recognizes that contracts that are digitally signed are legally binding &#151 that means that a digitally signed transaction cannot be repudiated. PKI also delivers end-to-end confidentiality by employing element-wise encryption of transaction data, as well as by enabling certain parts of the communication &#151 such as the transaction data (i.e. credit card and account numbers, etc.) &#151 to be encrypted right through to the business' back-end system, regardless of what gateways it must go through to get there.

An increasing number of device and browser manufacturers are building PKI support into their products. Current examples include the Neomar browser for a variety of PDAs and smart phones, and handsets that support Subscriber Identity Module (SIM) cards or Subscriber WAP Identity Module (SWIM) cards in GSM phones.

**Voice Authentication**

The convergence of voice and data will also have important implications for many aspects of wireless applications, security notwithstanding. Voice recognition will be used to gain an added degree of authorization for high-value transactions, especially in business-to-business commerce, treasury and investment banking applications. For example, completion of a transaction request in a wireless data application will trigger a telephone session in which the user will be asked to provide a &quotvoiceprint.&quot Initially, the voice interaction will be accomplished by the system calling the handset after the data session is finished. Eventually, voice and data interaction will be enabled as part of the same call. Because the voiceprint will be made over the same handset on which the transaction was requested, this feature would add a powerful new level of authentication and authorization.

**Conclusion**

Security remains of primary importance for consumers and businesses that are using wireless services. To take full advantage of the wireless Internet, businesses must understand the fundamental principles of security and be able to implement a full range of wireless security measures. To do so, companies must recognize that wireless solutions are separated into three zones &#151 the Device Zone, the Network Infrastructure Zone and the Enterprise Zone &#151 each requiring unique security policies and practices.

Proper security implementations will enable businesses to support their security claims and demonstrate to consumers that wireless transactions can be performed in a secure manner with respect to user validation, confidentiality, privacy, fraud and theft. It also lessens the business' exposure to extra costs incurred for offering services where, for instance, there are card-not-present transactions, making the wireless channel a much more compelling one on which to extend its service offering.

**John Mennel is the vice president for product management at 724 Solutions Inc. Mr. Mennel can be reached at jmennel@724.com.**

* *It isn't non-repudiable simply because the user has been authenticated &#151*

*non-repudiation occurs when the buyer/user digitally signs the transaction. Must be aware that usually, separate keys are issued for authentication and to digitally sign transactions.*

**Source URL (retrieved on *09/30/2014 - 5:47pm*):**
http://www.wirelessdesignmag.com/product-releases/2001/10/security-mobile-world