

Managing Security in Mobile and
Wireless Services

In the increasingly competitive corporate landscape, the quest for ways to continuously increase revenues, cut costs, speed up transactions and reduce operational errors has meant a flood of technological innovations to support these business objectives. In the cash management industry, from the perspective of both banks as well as corporate treasuries, the highly transaction-intensive nature of the business implies that the potential to reap benefits from such services as automation, instant information access, real-time decision-making and straight-through processing is real and substantial. Moreover, with cash management products and services being fairly commoditised, the opportunity to create unique selling propositions by leveraging new technologies is attractive to banks.

The success and ongoing growth of web-based cash management solutions is evidence of this trend. Although the aggressive projections of past years may have been toned down, the numbers around electronic business-to-business (B2B) payments, electronic information delivery and such metrics, as well as the money invested by banks in making their cash management services web-ready, are significant enough to conclude that banks as well as their corporate customers see this area as adding considerable value.

With the increased benefits and convenience of mobile and wireless applications in the banking industry come increasing risks in security and the need for security solutions.

Three points of security vulnerability exist: the mobile device itself, the wireless channel, and the network connection between the wireless web servers and the back-end transaction servers.

Handheld devices and wireless local area networks (WLAN) are especially vulnerable to potential viruses and the ability for wireless signals to be picked up beyond their intended recipients.

Thus, stricter security policies, WLAN security upgrades, the use of encryption technology such as virtual private networks, and end-to-end security solutions are highly recommended.

Business Logic in Wireless Services

As banks adopt multi-delivery channels in response to customer demands for greater convenience and lower costs, the wireless channel has seen growing acceptance in the retail payments and brokerage segments, although it still varies across geographies. This is being driven by the ubiquitous nature of wireless devices and their consumer acceptance, and the benefits of convenience and low transaction costs. Also, with the intensification of competition, the industry is increasingly feeling the need to equip its mobile workforce with mobile or wireless devices to boost efficiencies and improve customer relationship management (CRM). Wireless local area networks (WLANs) are increasingly becoming popular because of the flexibility and mobility they provide. Similarly, for corporates, the benefits of offering mobile cash management services can accrue in the form of:

- A customer-acquisition strategy to target new segments at a relatively lower cost; e.g. small businesses and corporates that serve large retail bases such as utilities and retail chains;
- A means of fostering customer loyalty and retention especially with the large corporate segment, which is a highly competitive market with large volumes and greater price sensitivity and hence derives greater value-added benefits from real-time information access and decision capabilities;
- Providing a value-added service by using an alternate delivery channel, which could likely complement other low-cost channels, such as the Internet, to provide a full range of services; and
- Personalising services based on individual authority levels for large companies, and offering greater convenience to corporate treasurers, small business owners and other decision makers who are always on the move.

Typical applications are related to:

- Receiving such information as real-time reporting or statements, and account activity alerts to facilitate decision-making;
- Transaction initiation without any lags or delays based on information accessed;
- Improving CRM by mobile-enabling field personnel; and
- Other value-added services such as personalised news updates.

A number of banks in the US and Europe have started launching mobile cash management services in many of these areas, with plans to expand their suite gradually. But, in spite of the evident benefits, it is also a reality that several challenges stand in the way of a large growth in wireless access to treasury tools. These include using the "right" technologies and standards, speed of access or transacting, limited (screen) real estate, which in turn limits functional capabilities and fuels security concerns.

Once these challenges are addressed, the growth of mobile commerce will be an inevitable phenomenon. The challenge of managing security in mobile services is by far the largest concern for the cash management industry. Once banks and corporates address transaction and information security concerns, this should go a long way towards increasing acceptability of mobile cash management solutions as a value-added service or channel to complement all other technology advancements being leveraged by this business.

Security – an Ever-growing Concern

Security requirements in any transaction are directly proportional to the transaction's value, sensitivity and volume. Mobile transactions in the cash management industry typically possess all these characteristics. Indeed, security is a de facto requirement for any transaction channel in the cash management business, and thus most security requirements are fairly generic and independent of the channel. However, the mobile channel has unique characteristics that can result in several new security vulnerabilities. Any end-to-end mobile transaction typically has three points of security vulnerability: the mobile device itself, the wireless channel, and the network connection

between the wireless web servers and the back-end transaction servers.

Handheld Security: the Physical Device itself is Often the Weakest Link The data stored in a mobile device can be as much at risk as the data transmitted over the air. At the handheld device level, security can be compromised either by the loss of the device or the presence of malignant code in the form of viruses. While the virus menace

Key message

There is a need for a clear and strictly enforced security policy, employee awareness and the implementation of a mobile security solution.

Wireless Link: Nobody Owns the Airwaves

The wireless link is sensitive from a security point of view because, unlike wired connections, wireless signals can propagate to places well beyond the intended coverage area. This is true particularly of WLAN communication. If sufficient precautions are not taken, it is not difficult for eavesdroppers inside the campus or outside the campus to snoop on sensitive information with some basic sniffing equipment.

To prevent this, mature authentication, authorisation and encryption techniques need to be used. Locationenabling access control is another technique where selective access controls can be put in place, depending on the location from which access is made. Security breaches in WLANs may potentially arise out of not changing default secure set identifiers (SSIDs), passwords and other access point settings. These can, however, be handled easily by having installation or configuration policies in place. Wired equivalent privacy (WEP) is the standard security protocol in WLAN (802.11x). Besides the many cases where security is compromised when the WEP security setting is left in its default state "off", WEP in itself is not a sufficiently strong security mechanism, particularly when sensitive information is exchanged over the wireless network. WEP has been cracked several times in the past using techniques as simple as playing with driver settings. Therefore, it is recommended that upgrades (typically, firmware) to new IEEE 802.11 security standards be considered. Wi-Fi protected access (WPA) resolves most of WEP's serious problems and can be applied as a software (or firmware) upgrade to Wi-Fi certified devices. Periodic wireless sniffers and scanners can be used to check the airways for

intrusion and security compliance, particularly when a security policy is placed into effect. Also, 24/7 policy-monitoring systems are available.

Mobile wireless networks, such as GSM, GPRS or the 3G networks, provide sufficient levels of access control and data encryption. However, for financial transactions, additional security is recommended using wireless access protocol (WAP) security (wireless transport layer security, or WTLS, end-to-end) by having WAP gateways located at the financial institutions or by employing security solutions based on mobile public key infrastructure (PKI). Transactions based on the use of the short messaging service (SMS) typically rely only on the security provided by the mobile network. For additional security, cryptographic techniques based on the subscriber information module (SIM) toolkit may be employed.

Key message

Configuration, use, and security policies should guide WLAN installation, configuration and usage. The application of WLAN security upgrades, such as WPA, and the use of wireless security technologies, such as WTLS, secure sockets layer (SSL), or other thin-client application layer encryption technologies is recommended for outdoor wireless transactions.

The Back End: the Wireless Service Provider is a Key Entity The wireless service provider often plays a key role in mobile financial transactions. Effectively, the mobile operator mediates the transactions between the mobile end-user and the back-end financial systems, unless end-to-end transactions are employed. Mobile operators not only have a trusted billing relationship with the users but also have access to customer profiles. While this can be used for establishing a secure payment channel, in certain cases end-to-end transactions between the mobile user and the financial systems may be desired in which the mobile network is used just as an access channel. WAP is a popular technology for wireless transactions. Depending on the location of the WAP gateway, transactions occur either using the mobile network as an intermediate entity (carrier hosted) or directly between the user and the financial system using the mobile network as a transmission channel. In a carrier-hosted solution (a low-cost, WAP gateway with the mobile operator), transactions between the mobile network and the back-end financial systems occur

using a SSL, which provides sufficient levels of security. However, it must be understood that in such configurations potential security vulnerabilities, such as the WAP security hole, exist (i.e. the translation of WTLS to SSL, which results in some data being unencrypted for some time).

Therefore, for end-to-end secure transactions, the WAP gateway should be hosted at the enterprise. Next-generation WAP or WAP 2.0 aims to address such security problems. Virtual private networks (VPNs), where practical, are often the most secure way of ensuring end-to-end security for corporate information access from outside the LAN using mobile devices. While full VPN on mobile devices may have its limitations now, VPN vendors are expected to introduce mobile VPN solutions through thin and clientless VPN technologies by 2004.

Key message

There is a need for end-to-end security solutions (i.e. a WAP gateway at the enterprise, WAP2.0, and use of a mobile VPN solution).

The Bottom Line

The mobile channel has potential for being a value-added benefit to the cash management industry in several ways. While security is a concern in any form of electronic transaction, the sensitivity of transactions in this business, and the potential damage that a security breach can cause, means that the issue of security needs to be effectively resolved for the large-scale adoption of mobile services in the cash management industry. Effective enforcement of security policies is as critical to mobile security as is the implementation of comprehensive mobile security solutions.

Authors

Puneet Gupta

Senior Tech Specialist, Software Engineering and Technology Labs
Infosys Technologies Ltd.
India

Sujata Banerjee

Consultant
Banking Domain Competency Group
Infosys Technologies Ltd.
US



Infosys Technologies Limited, Plot No. 44, Electronics City, Hosur Road, Bangalore - 560100. India • Tel.: +91 80 28520261 • Fax: +91 80 28521747
e-mail: finaclemktg@infosys.com • www.infosys.com/finacle

"COPYRIGHT NOTICE: Copyright ©2009 Infosys Technologies Limited, Bangalore, India. ALL RIGHTS RESERVED." Finacle logo is a registered trademark of Infosys and Infosys acknowledges the proprietary rights of the trademarks and product names of other companies mentioned in this document. Infosys believes the information in this publication is accurate as of its publication date; such information is subject to change without notice.