

Vigilus

Security Overview

Vigilus White Paper





Vigilus Security Overview

Wireless mobility solutions will transform the way enterprises conduct day-to-day business. Savvy enterprises will utilize wireless mobility solutions to create unprecedented process efficiency, resource accessibility, and cost-effectiveness. These improvements in business functionality will yield greater revenue, increased productivity, streamlined operations, and improved customer service. Commenting on this trend, Gartner estimates that by 2008, 65% of Global 2000 companies will provide their workforce with wireless mobile access to business-critical applications.

Along with the benefits of wireless mobility solutions, however, comes a whole new set of security issues that are more complex than those found in the traditional wired environment. This new set of security issues presents new challenges, but these challenges can be overcome with the right solution to ensure total enterprise security.

This document provides an overview of the critical enterprise security issues arising from wireless mobility solutions. It discusses two of the most common wireless mobility solutions and explains why they fail to provide adequate enterprise security. Finally, it presents the solution offered by the Vaultus Mobile Platform (VMP)¹ and explains how the VMP delivers complete enterprise security.

Challenges of End-to-End Mobile Application Security

Since data may be accessed over wireless networks and stored on mobile devices in a mobile application, corporate security officers must concern themselves with tracking and protecting data wherever it is transmitted or stored. The scope of data security has broadened from securing data in a database or application server to securing data wherever it resides, especially on devices such as PDAs (including BlackBerry, and Windows Mobile devices) and mobile phones.

When data exists primarily on a server behind the corporate firewall, securing that data is relatively straightforward. Data exists from the time it is placed on the server until the time it is removed from the server, so data security in the context of a server is based on efforts to restrict physical and network access to the server. Since this aspect of data security is well understood, data is often allowed to reside on the server for extended periods of time. In a mobile application, maintaining the physical security of corporate servers and restricting network access to those servers remain key components of a prudent security effort, but the proliferation of mobile information devices has broadened the scope of information security.

Mobile applications, by nature, introduce additional areas of vulnerability. Because mobile devices send data over public wireless networks, applications on these devices require an additional level of technical sophistication to be secure from malicious attacks. To maintain end-to-end security, corporate security officers must consider all aspects of security along the path from the device to the backend server. These areas include: authentication and authorization, firewall security, over-the-air security, and offline security.

¹ BizMobile and Vigilus Mobilization are products of Vigilus LLC built on the Vaultus Mobile Application Platform (VMAP) from Vaultus Mobile Technologies

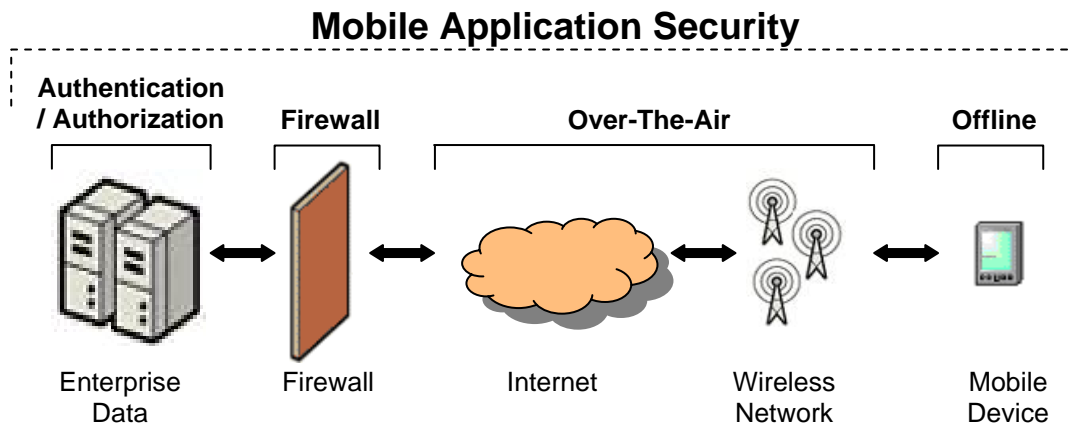


Figure 1: Components of Mobile Application Security

AUTHENTICATION AND AUTHORIZATION

Authentication is the process of verifying a user's identity, and authorization is the process of identifying the user's rights to access data and applications. User authentication and authorization ensure that only designated corporate users can access enterprise data and applications. In a mobile world, the need to establish and maintain a secure connection over a public wireless network further complicates the authentication and authorization process. In addition, access to data, applications, and updates need to be centrally managed for geographically distributed users who rarely enter a physical office.

FIREWALL SECURITY

Because mobile devices are on public wireless networks outside of the corporate firewall, additional ports must be opened in the firewall to allow mobile applications to access enterprise data. With each additional port opened to the outside, the risk of firewall compromise increases. Minimizing the number of open ports and ensuring that only secure protocols can traverse the firewall thus become important factors in maintaining firewall security.

OVER-THE-AIR SECURITY

Data security during transmission is normally not a significant concern in LAN applications since the transmission medium is a wired network in the corporate office behind the firewall, so hacking or eavesdropping would require physical access to the premises. However, because wireless signals can travel through walls and are accessible to the public, they are more susceptible to hacking. Hackers can use the public nature of wireless networks to gain access to a corporate network by disguising themselves as legitimate members of the network (known as spoofing), to eavesdrop on unencrypted transmissions (known as sniffing), to decrypt the content being transmitted wirelessly (known as cracking), or to perform various other attacks.

OFFLINE SECURITY

Because mobile applications transfer data over a relatively slow and sometimes unavailable wireless network, any successful mobile application framework will need to incorporate some form of offline data storage on the mobile device. Whether it is in the form of a web browser cache, a mobile data store, or a document attached to an email, corporate data will be present on mobile devices, and enterprises should take care that such data is properly secured. The presence of enterprise data on devices that can be easily lost or stolen creates a unique challenge for corporate security officers.

Current Approaches to Data Security on Mobile Devices

In the past, very little was done to secure data on mobile devices beyond a password lock that would engage after a certain interval of inactivity. The end user typically could enable or disable the password lock, and the user has complete control over choosing the password. Since most users find this password lock to be inconvenient, they tend to bypass the password lock or choose a password that is easy to enter rather than one that meets corporate security requirements.

Some recent approaches have taken a more active role in securing mobile devices. These approaches recognize the need to take some responsibility for data security even after the data has been handed off to a mobile device. Research In Motion's BlackBerry handheld devices and BlackBerry Enterprise Server (BES) permit an administrator to set a password policy that will be enforced on the mobile device. This policy can include password strength characteristics and device inactivity timeout intervals. With the introduction of Microsoft's Messaging and Security Feature Pack (MSFP) for Windows Mobile 5.0 in combination with Microsoft Exchange Server 2003 Service Pack 2, Windows Mobile devices also have this functionality. However, since the password is for the whole device and is triggered by inactivity, if a device is lost or stolen just after the password has been entered, a malicious user can have complete access to any applications and data on the device for as long as she keeps using the device.

Another new approach allows IT administrators to send a kill directive to a specific mobile device. When the device receives the kill directive, it will erase all the data that resides on it. This can be useful if the user of a mobile device reports that his device has been lost or stolen, or if a departing employee does not return her device to her employer. This approach can be much more effective than the older password-based approach. However, the following two shortcomings show that it is less than perfect:

- **The device needs to be on the network to receive the kill command.** Pushing a kill command to a mobile device is reminiscent of the cell phone heritage of many of today's mobile devices. When a cell phone is lost or stolen, a customer's primary concern is to prevent the charges resulting from unauthorized use of the phone. Since a cell phone has to be on the network to be used, it is sufficient to render a lost or stolen device useless once it is detected on the network but before charges can be incurred. However, when mobile devices used in enterprise applications are lost or stolen, the cost of unauthorized use of the device on the network pales in comparison to the value of the enterprise data stored on the device. Most devices are designed to be easily used in an offline mode. For example, Blackberry and Windows Mobile devices can be used for their PDA features in communications-constrained environments such as airplanes. Unfortunately, the ability to use a device while it is offline allows a malicious user to avoid a kill command, allowing all of the data on the device can be compromised unless mobile applications take special precautions. On many popular devices, this means that names, phone numbers, and corporate data can be obtained by anyone who possesses the device and takes it offline before it receives the kill command.
- **Data needs to be repopulated in the event that a lost device is recovered after it has been killed.** If a device that was reported as lost or stolen and therefore killed was instead merely misplaced, all the data that was on the device must be reloaded. Since wireless networks tend to be bandwidth-constrained when compared to wired networks, replacing the data on the device may require downloading a large amount of data over a slow network or sending the device back to an administrator for configuration. Though this is a minor inconvenience compared to the costs of allowing a malicious attacker to have access to sensitive applications and data, it can be a significant effort to reload data onto a device. This effort will only increase as the memory capacities of devices increase and more enterprise data is stored on devices.

Common Solutions – Overview and Challenges

VIRTUAL PRIVATE NETWORK (VPN)

A VPN provides general-purpose secure network connectivity between a mobile device and the enterprise network. VPNs have gained industry acceptance for remote access over wired networks because of their operational savings and relative ease of use. The most popular VPN implementation standards over wired networks include Point to Point Tunneling Protocol (PPTP), proposed and implemented by Microsoft; IPSec (IP Security), proposed by the Internet Engineering Task Force (IETF); and Layer 2 Tunneling Protocol (L2TP), also proposed by the IETF.

Providers such as Microsoft and Certicom offer VPN products for a multitude of device and server platforms. However, several issues surrounding security and performance continue to prevent overall traction of VPN among enterprises for mobile device connectivity. VPN is bandwidth-intensive, so it is not suitable for wireless networks where bandwidth is much lower than in wired networks. Therefore, VPN-based solutions exhibit noticeable performance degradation and usability problems.

In addition, the security of a VPN solution is heavily dependent on the specific implementation for the particular combination of device and server platforms used. Since the VPN software that runs on each type of mobile device and on the server may come from a variety of vendors, interoperability and configuration issues can create management headaches for administrators trying to ensure the overall security of the corporate network. As the variety of mobile devices continues to grow, interoperability and configuration issues will only get worse.

VPN is a general networking technique that is meant to provide access to the corporate network for a wide variety of applications. Once a VPN connection is made between a device and the corporate network, any application running on that device has complete access to the corporate network. Combined with the fact that network administrators have less control over mobile devices than they have over desktop computers connected to the corporate LAN, VPN reduces the ability of network administrators to ensure the security and integrity of the network.

Lastly, of the four components of mobile application security, VPN only addresses firewall and over-the-air security. Depending on the VPN implementation, it may be configurable to provide authentication in order to establish a VPN connection, but because a VPN connection is not application-specific, it does check to see if a user is authorized to use a particular application. Most significantly, VPN does not protect any mobile application data that is resident on a device should the device fall into the wrong hands.

HTTP AND WEB APPLICATIONS

Because web applications are so prevalent in today's enterprise, it is tempting for an enterprise in need of a mobile application solution to simply use web browsers on mobile devices with existing web applications. In the web application model, data is stored on a server and is only sent to a client web browser in response to a user request. Since data only exists on a server, the application security model is simple and easily understood.

However, the greatest advantage of this model from the application development and security points of view is its greatest weakness from the usability point of view. In web applications, usability is strongly tied to having a fast network that is constantly available. Wireless networks are notorious for high latency, low bandwidth, and inconsistent coverage, so a good mobile application solution should optimize use of the wireless network and provide an offline usage model for times when the network is unavailable. The web application model, with its reliance on verbose, text-based protocols and standards such as HTTP, HTML, and XML, and its lack of offline data storage, is not well suited for the wireless world.

There are a few common techniques that are used to make HTTP-based web applications more suitable for wireless world, such as caching and prefetching, but these techniques introduce new security issues. Most browsers implement caching by downloading HTML files to a local directory and storing them in case a user accesses them again. If a browser caches pages from a website that contains enterprise data, the security of that data is dependent on the security of the cache. Most desktop browsers typically do not cache pages for HTTPS connections because of the difficulty of maintaining security, and that problem is even harder on mobile

devices.

Prefetching involves loading a large number of web pages from the network before a user requests them and storing them locally so that the user's request can be satisfied without the user having to wait for network latency. Prefetching involves storing more data on the device, so it exacerbates the security concerns of caching, and it introduces the problem of synchronizing all of the prefetched data.

Another approach, WAP, was introduced to leverage the web application model while keeping in mind the resource constraints of mobile devices and wireless networks. The main difference between the WAP model and the standard web model is that a mobile user views content using a WAP browser, and web content is transcoded from HTML to WML and from HTTP to WAP by a WAP gateway. The WAP gateway sits between the wireless network and the enterprise web server, and WML and WAP are designed to be more efficient than HTML and HTTP. Because the protocols between the WAP browser and the WAP gateway (WAP) and the WAP gateway and the web server (HTTP) are different, the WAP gateway must decrypt and transcode all content before it is sent to a mobile device. The brief time interval during which data is unencrypted and exposed outside of the enterprise firewall is known as the WAP Gap, and since most WAP gateways are located outside an enterprise firewall, the WAP Gap can be a serious security concern.

Of the four components of mobile application security, the web model completely ignores offline security. Authentication and authorization can be handled by integrating a web application with an enterprise authentication source, and the using HTTPS as a network transport maintains firewall security and provides over-the-air security. However, the only way to ensure offline security with a standard web browser on a mobile device is to disable caching and prefetching entirely. Because of the high latency and low bandwidth inherent in wireless networks, this will make a web application difficult to use.

The Vaultus Mobile Platform

The Vaultus Mobile Platform provides customers with a robust, highly flexible development platform that simplifies the task of mobilizing applications, and offers IT administrators the enterprise-grade tools they need to fully manage users, devices, security and applications. Unlike most other platform solutions, the Vaultus Mobile Platform provides true end-to-end security covering all four areas of enterprise security concern and a meaningful and robust end-user experience.

The VMP consists of a client application that runs on a mobile device and communicates with a server that accesses enterprise data, as well as development and management tools that allow enterprises to mobilize their applications using the VMP. Additional applications, including a client and server, can be added and managed as part of one VMP installation. In order to maximize application usability in a mobile environment, the Vaultus application model relies on the VMP to constantly synchronize an offline data store with an enterprise data source, such as a CRM, helpdesk, or reporting system.

Because actions that a user takes on the mobile device operate on the local offline datastore, users see a responsive application that is not constrained by the latency or availability of wireless networks. Vaultus' patent-pending compression technology makes it possible to keep a large amount of data on a mobile device, so that a user can access most or all of their dataset while working offline. The proprietary Vaultus synchronization technology ensures that whenever a network connection is available, the data store on the mobile device is transparently synchronized with the enterprise data source. The synchronization process ensures that any changes that a user might have made to the local data store are reflected in the enterprise data source, and updates to the enterprise data source are available on the mobile device. The Vaultus synchronization protocol is optimized to use network bandwidth effectively – more than fifteen times more efficiently than XML over HTTP – to maximise the data that can be transmitted over a low-bandwidth wireless network. For more information about the Vaultus Mobile Platform synchronization process, please see the *Vaultus Synchronization Overview* white paper.

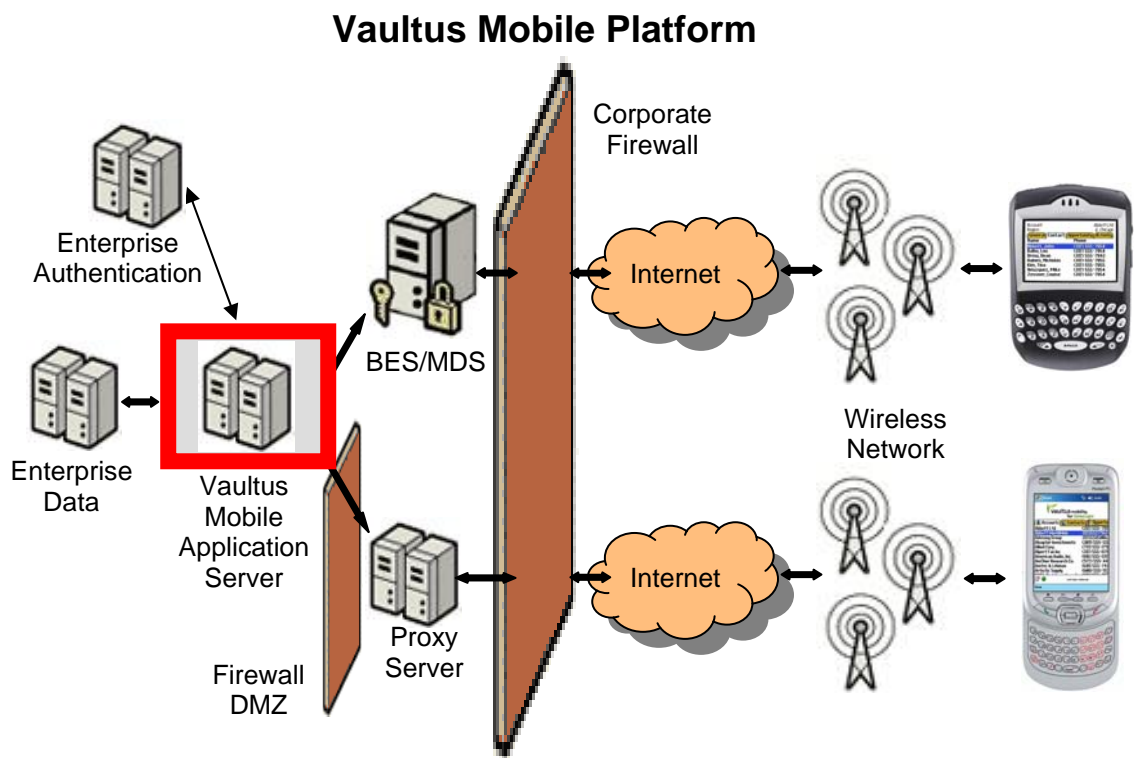


Figure 2: Security Architecture of the Vaultus Mobile Platform

AUTHENTICATION AND AUTHORIZATION

The VMP makes mobile user authentication simple and secure by utilizing the existing enterprise authentication scheme for LAN applications. When a user tries to gain access from a mobile device, the user's login information will be passed to an existing enterprise authentication scheme, such as Microsoft Active Directory, LDAP, or NIS, which is responsible for validating the user. This means that users can use the same account name and password for logging in whether they are using mobile applications or LAN applications. VMP also supports more advanced authentication schemes including RSA SecurID Authentication, a two-factor authentication mechanism that requires an authenticator token as well as a password.

Once a user has been authenticated, she must be authorized to access an application. The VMP maintains a database of user permissions that is managed through a web-based administration tool, the Vaultus Management Console. The Vaultus Management Console allows an administrator to manage the users, user groups, devices, servers, and applications that are part of this installation of the VMP.

The VMP goes to great lengths to keep login information secure. To prevent the compromise of a password if a mobile device is lost or stolen, the VMP does not store any passwords, either as plaintext or in an obfuscated or encrypted form, on mobile devices. To protect login information when it is being sent over a wireless network, all login information is encrypted before transmission using an ECC public key encryption algorithm provided by Certicom².

FIREWALL SECURITY

Although the same Vaultus Mobile Application Server can service all types of devices that are supported by the VMP, the network architecture as it relates to an enterprise firewall varies depending on the capabilities offered by each device platform. For RIM BlackBerry devices, no additional ports need to be opened in the enterprise firewall. All traffic between the BlackBerry device and Vaultus Mobile Application Server is tunneled through the BlackBerry Enterprise Server (BES) and Mobile Data Service (MDS).

For other devices, the Vaultus Mobile Platform minimizes the risk of firewall compromise by only requiring a single port to be opened. The VMP Proxy Server can be placed in the firewall DMZ while the Vaultus Mobile Application server, which directly access enterprise data sources, can be placed securely behind the firewall. By tunnelling all VMP traffic through a single port in the firewall, the VMP Proxy Server allows monitoring of access to enterprise data and control over user connections. The VMP provides an administrator the flexibility to cater to the specific firewall requirements of the enterprise.

OVER-THE-AIR SECURITY

The ECC public key encryption used to encrypt login information is also used to bootstrap the VMP network security model. Public key encryption is well suited for an asymmetric situation, such as when a user needs to make a connection to a server and provide login credentials, but it is not efficient for encrypting a large volume of network traffic.

Symmetric key algorithms³, on the other hand are far more efficient. The Vaultus Mobile Platform uses the

2 In public key encryption, a pair of keys, a public key and a private key, is used for encryption and decryption. The public key is made known to all parties, while the private key is kept secret. Any message encrypted with a public key can only be decrypted by the corresponding private key. Certicom's public key encryption uses an Elliptic Curve Cryptosystem (ECC) algorithm to encrypt and decrypt data. ECC has been researched widely and proven to provide the most security per bit of any known public key scheme, making it ideal for constrained environments. For more information about ECC, see <http://www.certicom.com/index.php?action=ecc,home>

3 In symmetric key encryption, one key is used to both encrypt and decrypt a message. This key is shared by both parties who exchange an encrypted communication. The Vaultus Mobile Platform uses the ARC4 (sometimes known as RC4) algorithm provided by Certicom. ARC4 is used to secure data transmissions in SSL, WPA, and WEP.

initial public key encryption to exchange symmetric keys which form the basis for a secure client-server session for as long as a user's login is valid on the server. All data sent by the VMP is encrypted with a symmetric key algorithm before it is sent over TCP/IP and decrypted it once it arrives at its destination. This ensures that no malicious intruder can access sensitive corporate data while it is transmitted even if he were able to eavesdrop on the network connection.

The second way that the VMP uses cryptographic algorithms to ensure data safety is by preventing data from being tampered with in transit. Using a cryptographic checksum known as a message authentication code (MAC)⁴, the VMP can detect and recover from attempts to modify enterprise data in transit over a public wireless network even if a malicious attacker were able to gain control over the network.

The level of encryption employed by the VMP ensures that should a malicious third party intercept packets during wireless transmission they would not be able to see the contents of the transmission or corrupt the data being transmitted. Therefore, should the TCP/IP connection become visible to third parties during transmission due to a network failure, the data will remain secure.

Because public keys, just like SSL certificates, can occasionally become compromised, the VMP supports a public key expiration interval and the automatic distribution of new public keys. As the public and private key pair for the VMP nears its expiration time, an administrator will be notified by email that she must generate a new public and private key pair and install it in the Vaultus Mobile Application Server by the key expiration date. Once the administrator does so, the server will automatically distribute the key to all mobile devices in the system.

Finally, the VMP allows administrators to change the key lengths of every algorithm in our encryption scheme and therefore adjust the encryption strength of the system to suit the level of security required by the enterprise. The key length of the ECC public key encryption algorithm can vary from 163 to 512 bits (equivalent to 1024 to 3076 bit RSA keys) with the default being 163 bits. The key length of the symmetric key encryption algorithm can vary from 8 to 2048 bits, with the default being 128 bits.

OFFLINE SECURITY

Since the Vaultus Mobile Platform is designed around an offline data store and data synchronization, offline security is the paramount aspect of security for the VMP. In order to complement the existing security features of the RIM BlackBerry or Microsoft Windows Mobile platforms, the VMP offers two important features that keep enterprise data secure on a mobile device.

The first of these features is seamless client-side data encryption. Because the VMP is able to store so much enterprise data on a mobile device, it is important to prevent that data from being compromised in the event that a malicious attacker finds or steals a user's mobile device. An additional challenge when implementing an encrypted data store on a mobile device is to ensure that the added security does not detract from application usability. The VMP client data encryption scheme balances these concerns by leveraging the enterprise login credentials required for authentication, so that a user will only need to remember one password to use the Vaultus application while on the network and to access encrypted data while off the network. Also, the data is encrypted such that a user can change the encryption password when the user's enterprise login password changes.

The second major area in which the VMP improves upon mobile device security is through application leasing based on a lease key. A simple way to understand the concept of application leasing is to think of a hotel key card system. While a hotel guest may possess a key card and keep it even after his reservation expires, the card only allows access to the hotel room while the reservation is valid. In the same way, even if a user has a Vaultus application installed on her device, it will only allow the user to use the application and access enterprise data while the user has a valid application lease. The lease begins when a user logs in to the

⁴ In a MAC, a shared secret is used with a cryptographically secure hash function to ensure that data is not modified. This secret is shared by both parties who exchange an encrypted communication. The Vaultus Mobile Platform uses the HMAC algorithm provided by Certicom.



Vaultus server, but because the application lease key is stored on the device, the lease is enforced even if a user is not logged in, or even not on the network.

The lease key contains sufficient information to grant that device access to the Vaultus application and data for a specific amount of time. The lease key is persistent across restarts of the application and reboots of the device. Precautions are also taken to prevent the lease key from being used inappropriately due to a manual clock rollback on the device, and to prevent a lease key from one device being copied or moved to another device. The lease interval can be configured to be any length of time, but it is typically in the range from one day to one week. It is configured on the Vaultus Mobile Application Server and can be determined by the administrator.

The following steps in the lifecycle of an application lease will help illustrate its value in mobile application security:

- **Application Installation.** When the Vaultus Mobile Application Studio generates an installable application package, it does not include any data. Therefore, when an application is first installed on the mobile device, the local data store is empty. At this point, all of the application data still resides in the enterprise data source.
- **Initial Data Population.** In order to obtain access to enterprise data, a mobile user will need to connect to the network and log into the Vaultus Mobile Application Server. At this point, the user's login information will be validated against an enterprise data source and the VMP user database. If her login is valid and she has permission to use this application, the server will begin synchronizing the initial data set to her device, and the server will grant her a lease key for this application.
- **Application Usage and Data Access.** Access to the Vaultus application and data in an offline or online mode is allowed only when a valid lease key is present on the device. The lease key is validated whenever the application starts and whenever the lease key timer fires to notify the application that the lease has expired. For example, if a user started the Vaultus application for the first time, logged in to download her data, and received a lease for 24 hours, the user has complete access to the application and data for one day. Even if she were to lose her network connection or intentionally disconnect from the network, the lease key would allow her to access the application and data for one day after her initial login.
- **Lease Expiration.** At the end of the lease interval on the device, the key will expire. If the user is currently using the Vaultus application, she will see a screen that prompts her to re-enter his login information to continue to use the application, and she will be unable to access the application or its data without a valid login. If she is not currently using the Vaultus application when the lease expires, the next time she launches the application she will be prompted to log in. Her data is still present on the device, but her access to it is restricted until the server grants her a valid lease key.
- **Lease Renewal.** To renew the application lease, a user will need to present valid login credentials when the application prompts her for it. After every successful login, the server will grant a new lease key for the full lease interval. Because lease renewal happens on login, it is typically not something that will require a user to go out of her way in order to use the Vaultus application. For example, if a she typically logs in every day, then a lease key duration just over a day (say 26 hours) would let her receive a new lease just before the previous day's lease key would expire. She would never notice the presence of the lease key, yet her data would be secure if she were to lose her mobile device. As a result, she would rarely need to take action just to renew the key.

Because application leasing only grants a user the ability to use an application temporarily, it overcomes the shortcomings of built-in device security. If the lease key expires while the device is not connected to the network, the Vaultus application and data becomes immediately inaccessible to the user. Unlike a kill command that requires network access to be pushed to a device, the application leasing protects enterprise data even



when devices are offline. The expiration of the application lease does not delete the data on the device but simply makes the data inaccessible. For example, if the lease expired because the user misplaced a device, as soon as the user finds the device and connects to the network, and successfully logs in, a new lease key will be granted and the application and data will be available for use without any additional work on the part of the administrator. In contrast, if the device really were stolen, since the thief would not be able to log in as the device owner to obtain a new application lease. The enterprise data would remain secure, since the lack of a valid lease key would prevent the thief from getting access to the application and data.

Conclusion

Enterprise demand for increased productivity and competitive advantage virtually guarantees that wireless mobility solutions will make their way into the core of enterprise IT infrastructure. Wireless mobility solutions promise a host of benefits both at the top and bottom line of the balance sheet. However, outstanding security concerns about wireless technology have been one of the main reasons why these solutions have not gained greater acceptance thus far. Recognizing the limitations and shortcomings of existing wireless mobility security schemes, the VMP is engineered to be a secure and robust environment in which to build, deploy, and run mobile solutions for the enterprise.

Unlike other security schemes, the Vaultus Mobile Platform (VMP) has been designed from the ground up to tackle the entire range of security issues present in a wireless mobility solution architecture. VMP also gives developers the tools to build solutions that measure up to corporate-wide security policies without compromising usability or performance. By addressing all four key areas of wireless mobility security – authentication and authorization, firewall security, over-the-air security, and offline security – the VMP provides IT administrators with peace of mind because they know that enterprise data is secure in their mobile application.