WICKSoft Mobile Documents™ for the BlackBerry

Security white paper – mobile document access for the Enterprise

WICKSoft Corporation
http://www.wicksoft.com

Table of Contents

Introduction

Mobile document access technology – which allows users to remotely access important documents and information from their wireless handheld – greatly improves both employee productivity and convenience by freeing users from having to carry laptops when traveling, and by allowing immediate response and action to issues in real-time.

However, there are certain unique security concerns that are inherent to the operating environment. Due to the fact that data travels over-the-air, and that mobile assets can be easily lost or misplaced, special care and attention must be given when considering any solution for the mobile enterprise.

Security Issues facing the mobile Enterprise

There are four major security challenges facing the mobile Enterprise.

1. Data travels over shared, public, and sometimes open networks.
2. Mobile handhelds may be misplaced or stolen, exposing sensitive information.
3. The mobile device represents a potentially unmanaged point-of-entry in to the network.
4. Worms and viruses may be transferred to the corporate internal network via tunnels created in the mobile VPN technology[1].

WICKSoft, makers of WICKSoft Mobile Documents™ for the BlackBerry, offers technology to combat the aforementioned problems and enables mobile remote access to be achievable in a secure way from anywhere.

[1] The Cabir virus and BBProxy are just two examples of the kinds of malware that can be propagated though Email and Bluetooth enabled devices. According to antivirus maker F-Secure, there are already more than 370 different wireless threates in the air, including attacks that attempt to delete data stored on handhelds and even record end users' phone calls.

Summary

WICKSoft Mobile Documents™ approaches the issue of security from three distinct levels. The first is the data-transfer level, the second is at the application level, and the third is at the handheld level.

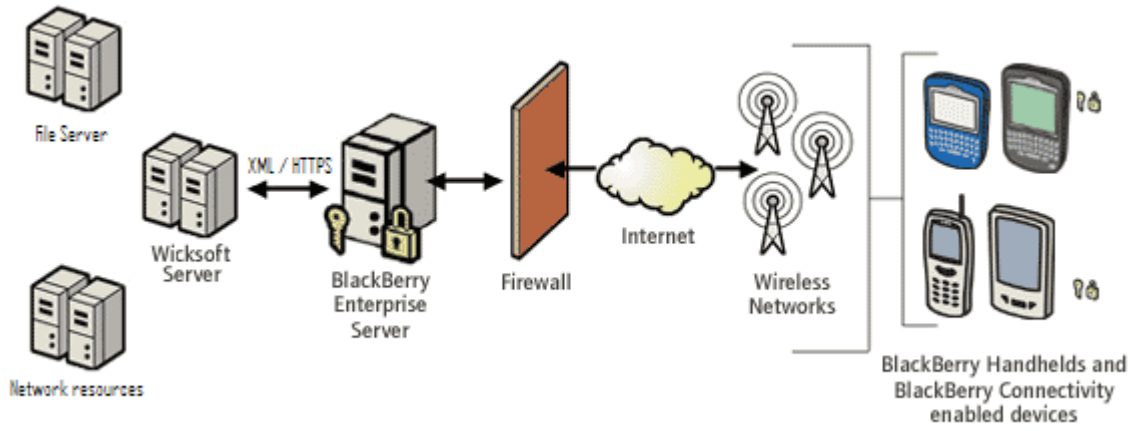
- Security at the data transfer level--where traffic may be susceptible to monitoring, and where worms, viruses, and attackers may attempt to gain a remote point of entry--ensures that a secure tunnel is created and maintained from the handheld directly to the Enterprise.
- Application level security is a policy-based approach to ensure sensitive data never leaves the office, and that only operations deemed 'safe' from a mobile device are possible. Mobile VPN technology must ensure that users cannot accidentally distribute, remove, or otherwise tamper with sensitive information and other network resources.
- At the handheld level, the mobile VPN solution must be able to effect changes immediately, even if a handheld is turned off. This provision is necessary to ensure that stolen or misplaced assets can be disabled immediately, and that no sensitive information is ever left behind.

Combined, these three levels provide a secure channel between the BlackBerry and the Intranet, and also a secure platform through which to operate.

General Network Architecture

WICKSoft Mobile Documents™ is built on, leverages, and extends the inherent security built into the BlackBerry infrastructure.

When used in conjunction with BES and MDS (BlackBerry Mobile Data System™), the WICKSoft Mobile Documents™ Server does not need to be accessible from the Internet—the connection will originate from BES. In other words: no additional ports or entry points need to be opened into the network in order for WICKSoft Mobile Documents™ to function.



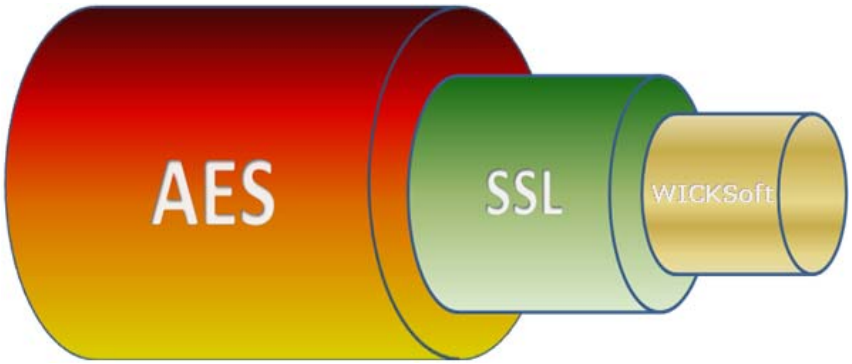
By using BES with Enterprise-activated handhelds, a secure connection is already present. Data is transmitted over an encrypted channel from the handheld to the BES, which is located in the intranet.

Additional security measures, which are discussed later in this document, ensure additional levels of security and integrity are achieved at both the data transmission levels, as well as the application layer.

Data transfer layer

WICKSoft Mobile Documents™ communicates over a secure channel which is comprised of the three security layers. This secure channel ensures that:

- External threats cannot monitor, intercept, or modify data going between the handheld and the Intranet.
- Hostile internal processes, such as worms, users, or other programs introduced via some other means, cannot monitor, intercept, or modify data going between the wireless infrastructure and internal resources.
- Rogue applications, such as Trojans, worms, viruses, and unauthorized user applications cannot hijack or exploit the mobile VPN tunnel.



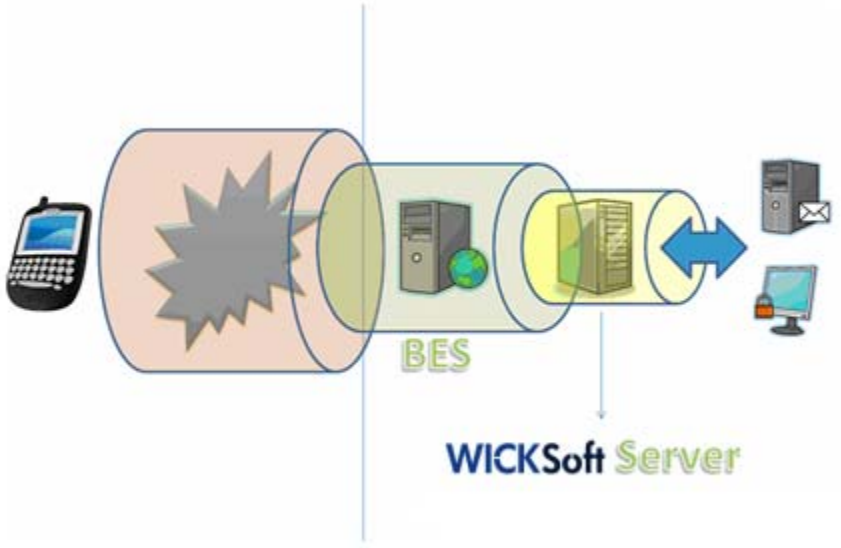
WICKSoft Mobile Documents™ creates a secure channel to the Intranet

Two separate layers of cryptography move the WICKSoft Mobile Documents™ protocol across the wireless network. The addition of an extra cryptography layer ensures that even traffic within the Intranet is secure.

A proprietary protocol is used to transmit instructions from the WICKSoft Mobile Documents™ client, running on the BlackBerry, to the WICKSoft Mobile Documents™ Server that resides within the Intranet.

The three security features that make up the secure channel used by WICKSoft Mobile Documents™ are:

- AES cryptography from the handheld to the BES Server (or wireless carrier if no BES is present)
- SSL cryptography from the handheld to the WICKSoft Mobile Documents™ Server, through the AES tunnel.
- A proprietary protocol designed exclusively for the application of mobile document access.



Two layers of cryptography

The first two layers, the AES and SSL cryptographic layers, protect network traffic all the way from the internal WICKSoft Mobile Documents™ server out to the handheld. These layers ensure that data to and from the handheld always remains secure.

- The AES layer provides a secure tunnel from the handheld up to the BES server (or to the carrier, if no BES is present). With BES, this prevents any monitoring or tampering of the network traffic while it moves over-the-air and over open networks.
- The SSL layer increases the security of the AES layer while at the same time protects the tunnel while it moves through the internal Intranet.
- *When used in conjunction with BES the WICKSoft Mobile Documents™ Server never needs to be accessible via the Internet, or even internal computers*. In this way you can restrict the point-of-entry to verified assets (Enterprise activated handhelds) over a secure and encrypted source. This is similar to restricting an IPSEC VPN to a specific MAC address, only with a higher level of obfuscation.

WICKSoft Mobile Documents™ proprietary protocol

WICKSoft Mobile Documents™ employs a proprietary communications protocol that protects internal resources from Trojans, viruses, rogue devices, and careless end users. This protocol operates over a standard HTTPS connection, so can work with your existing security infrastructure.

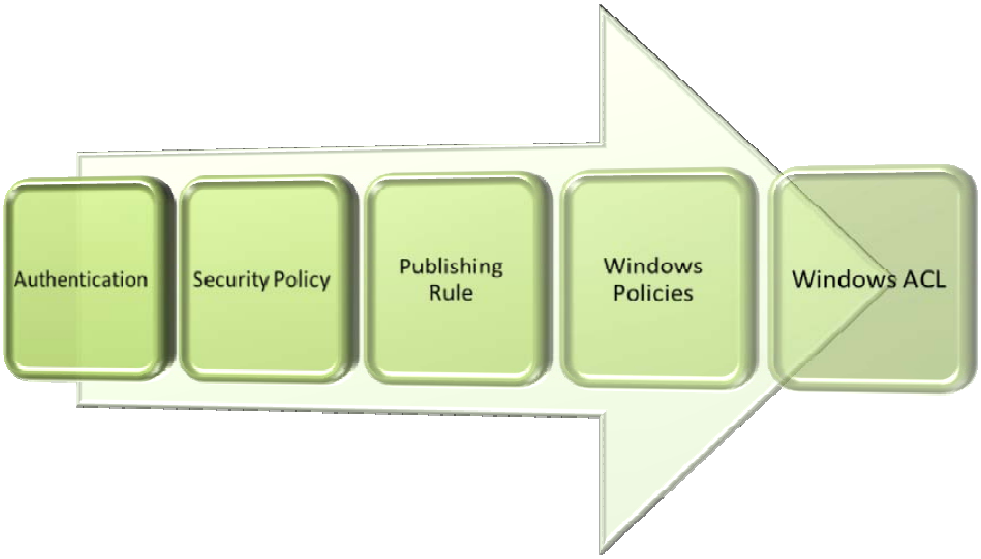
This protocol provides no mechanism to execute remote programs or manipulate a database, and can only convey simple end user operations such as 'List the contents of a folder'.

Using such a protocol provides the following benefits:

- Existing security resources, such as content scanners, MDS, Microsoft ISA Server, and other Firewall products continue to take effect.
- Deployment requirements-- and therefore the security impact—are reduced because the protocol tunnels through standard HTTPS.
- The limited scope of the WICKSoft Mobile Documents™ protocol makes it almost impossible for a standard Windows worm (like an SQL injection exploit) or Trojan to propagate through the system.
- The WICKSoft Mobile Documents™ protocol is exclusive to WICKSoft Mobile Documents™ —in other words, other applications cannot use the protocol. The result is that WICKSoft Mobile Documents™ is highly resistant to tunneling efforts, such as running a torrent, remote desktop application, or some other network utility across the same protocol. For example: an end user could not setup a program like VNC within the Intranet and then use WICKSoft Mobile Documents™ to access VNC , thus circumventing security measures. The WICKSoft Mobile Documents™ protocol will not facilitate tunneling or hijacking by other applications.
- The protocol is highly conducive to policy enforcement. In this way WICKSoft Mobile Documents™ provides additional layers of security which will be discussed later, that are context and content sensitive.

Application level security

All data that moves through WICKSoft Mobile Documents™ goes through the same set of checks and balances before being passed on to the internal network. Only after these checks and balances have been satisfied will WICKSoft Mobile Documents™ perform a given operation on the internal network.



Authentication

The first check is authentication. All WICKSoft Mobile Documents™ users must login to WICKSoft Mobile Documents™ using their BlackBerry. This authentication data is checked by the WICKSoft Mobile Documents™ server for each and every operation before being processed. Once authenticated, all processes within WICKSoft Mobile Documents™ are undertaken as if the user were logged in to the local network as that user. If an account is disabled or modified in Active Directory, or Novell eDirectory, then the changes will be reflected in real-time and rejected by both WICKSoft Mobile Documents™ and the Operating System.

Security Policy

The second check is against the security policy. WICKSoft Mobile Documents™ contains its own patent-pending security policy technology that has been designed for remote access applications. Policies can be customized to restrict access by users and groups to:

- Machines
- Shares
- Files and Folders
- Web resources
- File types

Additionally, all requests must pass a basic sanity test which guards against certain intrusion attempts.

Publishing Rule

The third check is against publishing rules. Administrators must explicitly allow network resources to be made available to end users. In this way the risk of accidently exposing sensitive resources is mitigated. Keep in mind that security policies (mentioned earlier) override publishing rules, so mistakenly providing access to an explicitly denied resource (or user) will not compromise the system.

Windows and Novell Policies

The fourth check is against your Windows or Novell Security Policy. Once a user logs in to WICKSoft Mobile Documents™ they are subject to all of the security constraints implemented at the Intranet level. In this way a Microsoft Security Policy will affect and constrain a WICKSoft Mobile Documents™ user as if the user were accessing the Intranet locally.

Windows and Novell ACLs

The fifth check is against your Windows or Novell ACLs. At no point will WICKSoft Mobile Documents™ ever grant a user access to something they do not have sufficient rights to access. WICKSoft Mobile Documents™ honors all Microsoft Windows and Novell ACLs at both the share and folder level. These ACL checks guarantee that the end user will never be able to do something that they couldn't do from the office.

Application layer security summary

The application security layer, with its multiple checks and balances, makes it very easy to lock down the mobile enterprise.

Basic built-in sanity checks, which cannot be overridden, ensure that relative path referencing, local paths, and certain other aberrant access types are never permitted to flow throughout the rest of the system.

A failure at any one point along the sequence immediately invalidates a client request and is logged to a special security log.

The entire secure channel ultimately provides a level of data and application control that facilitates only the operation of WICKSoft Mobile Documents™ , but no other applications.

Handheld level security

The BlackBerry Wireless Handheld is a very secure operating environment and WICKSoft Mobile Documents™ leverages and enhances this inherent security.

WICKSoft Mobile Documents™ provides the following security features on the handheld:

- At no time is sensitive data ever stored on the handheld, a SIM card, or other portable storage device[2].
- All e-mail messages sent using WICKSoft Mobile Documents™ are sent from within the corporate intranet, and do not travel over the air. When used in conjunction with Microsoft Exchange, WICKSoft Mobile Documents™ acts as if the user sent an email message from their desk, even leaving a copy of the outgoing message in the user's 'Sent Items'.
- WICKSoft Mobile Documents™ honors the automatic lock-out during periods of inactivity that is provided by the BlackBerry.
- WICKSoft Mobile Documents™ provides an independent automatic lock-out so that WICKSoft Mobile Documents™ will become locked after a period of inactivity.
- Data cannot be transferred from an external source, through the BlackBerry, through WICKSoft Mobile Documents™. This makes WICKSoft Mobile Documents™ immune to Bluetooth born viruses and worms, and protects against MIDP and handheld based Trojans.

[2] File downloading is disabled by default. If administrators choose to enable downloading in both the server-wide security policy, and specific publishing rules, then clients may store information on their PDA. Security policies and publishing rules can restrict downloading to documents deemed safe for transfer to a PDA.

Conclusion

WICKSoft Mobile Documents™ delivers a secure channel to the enterprise that facilitates mobile document access without exposing the corporate network to external threats.

Enterprise security management features allow administrators to control mobile access to network resources.

Extensive logging allows for continuous auditing of many aspects of the WICKSoft Mobile Documents™ deployment. Full access traces and security notification permit the administrator to closely monitor activity.

By leveraging existing infrastructure WICKSoft Mobile Documents™ can seamlessly integrate with the mobile enterprise while providing an enhanced level of security and access control.

Sensitive data is never stored on the handheld, and data transfers (such as file management, and e-mail attachments) do not travel over-the-air. Existing security infrastructure is applied to mobile user.

A proprietary protocol ensures existing security threats, such as worms and viruses, do not hijack or tunnel through the secure WICKSoft Mobile Documents™ channel.

For more information about WICKSoft Mobile Documents™ for the BlackBerry please visit http://www.wicksoft.com