Executive Summary

Research In Motion (RIM) has designed its BlackBerry Enterprise Solution to be resilient to many operational and security risks, including attacks by malicious code. The BlackBerry environment provides top-down control for system managers so that users are protected from attack without having to take individual action. Using several technologies to thwart unwanted intrusion, Research In Motion enables enterprises to extend the perimeter of security to include its mobile computing devices.

Malicious code is the highest-ranked threat priority, according to IDC research. The many direct and indirect costs of an infection are well known in the IT community because of experiences with PCs. Designed for individual management, the PC provides just the uncontrolled environment that malicious code writers seek. The PC’s many interfaces amount to a multitude of doors that might be found ajar, and the user often participates innocently in infecting the machine.

Cognizant of the importance of security in enterprise environments, Research In Motion designed the BlackBerry environment to be manageable and controllable. It features several layers of protection:

- The BlackBerry environment provides restricted functionality by disabling all but the necessary protocols and interfaces. Bluetooth’s discovery capability, which represents a real threat, is not enabled, for example.

- Top-down policies can automatically preclude users from engaging in dangerous behavior. Should system administrators choose, users can be blocked from installing new applications.

- The BlackBerry system uses digital signatures to authenticate executable code and blocks unsigned programs that might somehow find their way inside the system.

IDC believes that these layers of protection represent best practices when countering the risk of a successful malicious code attack. Organizations hesitant to deploy mobile devices and gain the efficiencies that they provide should examine the BlackBerry Enterprise Solution.
Malicious Code and Enterprise Mobile Devices

Malicious code is a well-known problem for most enterprises. In a 2004 study of more than 600 IT managers, IDC research found that IT managers view Trojan horses, viruses, and other malicious code as the greatest threat to enterprise network security. As shown in Figure 1, this threat was ranked significantly higher than all other threats. Experience has shown that successful attacks of malicious code are costly to the enterprise and that defending against this threat is difficult and time-consuming.

FIGURE 1

Threat Priorities

- Trojans, viruses, and other malicious code
- Employee error
- Internet worms
- Spyware
- Hackers
- Sabotage by current employee
- Application vulnerabilities
- Spam
- Cyberterrorism
- Sabotage by former employee
- Inability to meet government standards

n = 606
Source: IDC, 2005

New mobile devices further expand the perimeter of risk for enterprises, a perimeter that last expanded dramatically when enterprise systems were attached to the Internet. To counter Internet threats, companies needed a collection of technologies — firewalls, intrusion detection, VPNs — to ensure that enterprise systems and resources could not be inappropriately accessed or hijacked. Technologies for mobile devices will need to be similarly deployed.
Most malicious code attacks have targeted PCs because they are numerous, most are in the hands of nontechnical users, and they were not designed initially to be a trusted component of enterprise information systems. Email attachments can carry malicious code payloads that infect the PC and exploit its security weaknesses, and they may even depend on naive users to execute the code. In general, people who launch malicious code attacks are looking for computing devices that are numerous, in the hands of nontechnical users, accessible over the Internet, and unprotected.

**Mobile Devices**

Mobile computing devices further expand that security perimeter for the enterprise, as Figure 2 shows. The mobile device, like the PC, is vulnerable to a familiar family of security threats, including eavesdropping, spoofing, and malicious code attacks. These threats also have well-understood countermeasures. The basic tools for formulating countermeasures rest on encryption techniques and basic control over the operating environment of the mobile device.

![Figure 2: The New Enterprise Security Perimeter](image)

Source: IDC, 2005

**The Emerging Threat Environment for Mobile Devices**

Mobile devices, a category that IDC defines as smart handheld devices, mobile phones, and converged devices, are increasingly high-profile targets for various security threats, as follows:

- **Receipt of malicious executable code.** Virus writers often send attachments to email that contain malicious code, and depending on the configuration of the mobile device, this code may be executed either automatically or by the user.
Access to enterprise data at rest. Hackers may target sensitive data stored on the mobile device or even attempt to use the mobile device as an access point to the enterprise network. If this data is sensitive and personal, then the enterprise breach may cause regulatory problems to arise.

Access to enterprise data during transmission. Hackers may also attempt to monitor data transmitted from the mobile device through wireless networks that are not always secure.

User behavior. Users may load and launch malicious applications, attachments, and other executable code either inadvertently or perhaps even intentionally. With the capability to browse and download information from the Internet, these mobile devices are highly vulnerable to user-induced security failures.

Thwarting Malicious Code

Thwarting malicious code is the focus of this white paper. Best practices for defending against the threat of infection by malicious code depend on the ability of enterprise system administrators to take control of the configuration of enterprise mobile devices. Malicious code attacks on mobile devices can be thwarted with four basic technologies, as follows:

Restricted capabilities environment. Mobile devices should be configured with minimal capabilities sufficient to execute solution software. Unnecessary functionality, which can be a vector for malicious code, should be disabled entirely. Of particular concern for wireless devices are self-discovery capabilities, particular for Bluetooth.

Required digital signatures. Mobile devices can be configured to accept executable code only from trusted suppliers. Trusted code is signed with a digital signature that is formed with a private key held by a trusted supplier and matches a public key stored on the mobile device. Unsigned code cannot be executed when digital signature technology is deployed. RIM believes that signing is a strong deterrent. Signed code is analogous to requiring criminals to show identification before committing a crime.

Centralized administration. Strong configuration management support from a centralized server reduces risk of malicious code being loaded on enterprise mobile devices. Corporate policies can be enforced when the IT department has the capability to reset mobile devices to a standard configuration.

Applications control. IT administrators can benefit from controlling the applications environment with the effective use of applications control tools. These tools help shield the environment from malicious code because they allow the IT administrator full visibility into and authority over the applications that users run. These tools include the ability to restrict the types of connections applications can make. IT administrators can disallow the use of applications that connect to the Internet where malicious code resides.
Summary and Implications

Mobile devices and the extended networks that support them pose new threats to enterprise systems, but they can be mitigated. The key to mitigating these new risks is control over the mobile device and its supporting environment.

The RIM BlackBerry

The BlackBerry Enterprise Solution

The BlackBerry Enterprise Solution from Research In Motion is a product designed from the ground up for enterprise deployment. Security capabilities have been put in place to make sure that enterprise network managers can exert the control necessary to keep these mobile devices free from malicious code and other security threats. Figure 3 shows the BlackBerry Enterprise Solution architecture.

FIGURE 3
BlackBerry Enterprise Solution Architecture

Source: Research In Motion, 2005
How the BlackBerry Solution Thwarts Malicious Code

RIM employed four basic controls to protect the BlackBerry handheld device from malicious code attack. First, RIM or a recognized application developer digitally signs all software intended for the BlackBerry. Second, BlackBerry software parses email attachments into binary format before transmitting them to the handheld device. Third, RIM provides for wireless deployment of IT policies to each BlackBerry. Finally, Bluetooth is configured to demand user attention when connections are formed with other devices. More information follows about each of these controls.

Signed Software

BlackBerry mobile devices use a Java operating environment, which provides a standard platform for third-party software developers. To control access to sensitive data on the BlackBerry and avoid the risk of malicious code, RIM designed specific application programming interfaces (APIs) that third-party developers must use. In addition, RIM requires that all software be digitally signed or the BlackBerry device will not execute the code.

Attachment Service

The BlackBerry Attachment Service handles email attachments, which could be scripts or executable code, by parsing the files in a binary format. The Attachment Service does not open the application or render it with other software (e.g., Adobe Acrobat). The BlackBerry Enterprise Server (BES) reformats certain attachments (e.g., documents, spreadsheets, graphics, and Web pages) so they can be easily displayed on the BlackBerry’s screen. BES sends only a static image to the BlackBerry, which virtually eliminates the transfer of malicious code to the device.

Automated IT Policies

The BlackBerry Manager Handheld Configuration Tool, which is a component of the software running on the BlackBerry Enterprise Server, enables system administrators to regulate the use of third-party software on BlackBerry devices. Enterprise IT policies about obtaining and installing third-party software are automatically enforced. If enterprise policy disallows installing new software, then users will be unable to do so. Alternately, the Configuration Tool may specify which applications users may legitimately install. When system administrators update IT policies, the update is immediately and wirelessly transmitted to all BlackBerry handheld devices. By "white listing" only approved applications and executables, administrators limit user flexibility, but this policy sharply reduces the potential for malicious or badly written personal applications to disrupt the device's normal operations. Connection rules supported by BlackBerry administration tools also allow IT managers to prevent applications from connecting to the public Internet where malicious code may reside.
Bluetooth Configuration

Another potential source of malicious code is a nearby device equipped with Bluetooth wireless capability. The BlackBerry mobile device supports Bluetooth access to a serial port. The Bluetooth radio is disabled in BlackBerry devices to ensure that Bluetooth's discovery capability does not compromise security. To connect to a Bluetooth device, users must enable the radio and confirm each connection between the BlackBerry and a Bluetooth-enabled device. IT administrators can also remotely disable Bluetooth.

In summary, RIM has put in place technology to reduce the risk that malicious code can execute on the BlackBerry device. This technology is built into the foundation of the solution architecture and provides system administrators with the capability to configure all BlackBerry devices automatically and wirelessly. RIM participates in the process by providing digital signatures for legitimate third-party software developers.

How the BlackBerry Thwarts the Cabir Virus

The Cabir virus, which appeared in June 2004, infects some mobile devices and uses Bluetooth for propagation. Called a "proof-of-concept" exploit because it demonstrates the potential for attack, Cabir neither carries a payload nor causes any damage to the systems it infects. When installed on a susceptible mobile device, the virus executes each time that the device is switched on. The virus uses Bluetooth to wirelessly look for other susceptible devices within approximately 30 feet. When it finds another unprotected device, it "Bluetooths" a file to its victim.

For a BlackBerry user, the default settings for Bluetooth communication serve as the first line of defense. Before the file can be transferred, the user must agree to create a Bluetooth link. Should that link be formed by the user, then other defenses come into play. The Object Exchange (OBEX) protocol alone would disable Cabir, but RIM does not support OBEX in the Bluetooth stack. Policies managed at the enterprise server can deny the user the right to install the code. If these policies are not enabled and the user agrees to install Cabir, then the final line of defense is reached: The code is not signed by RIM and thus cannot be executed.

IDC Analysis

Situation Analysis

When end-to-end enterprise-class security is needed, control over all subsystems is crucial. Secure systems with a few carefully designed gateways and the leanest possible execution environment will be more resilient to threats than systems with multiple access points and greater flexibility.

Opportunities

RIM’s BlackBerry offers a mobility solution with security capabilities built to enterprise IT standards. As a result, the BlackBerry will be attractive for enterprise deployment, especially in industries such as financial services where security is of great concern to IT decision makers. Network managers will find the ability to set and enforce IT policies particularly compelling. In addition to repelling malicious code, the BlackBerry offers other technologies to protect enterprise data even if a BlackBerry device is lost.

The RIM BlackBerry technologies for repelling malicious code have been successful to date. While viruses have found footholds with other mobile systems, no virus outbreaks have been reported for the RIM BlackBerry solution.
Challenges

As the community of BlackBerry users continues to grow, attackers will increasingly target the security systems that protect RIM's server and handset software, just to test the robustness of the security architecture. As attackers have shown in the past with other systems, new techniques developed in the future may successfully circumvent the RIM security architecture in unanticipated ways.

Some of RIM's potential customers and third-party software providers may struggle with the trade-off between improved security and the controlled architecture of the BlackBerry solution. IDC believes that the requirement that RIM control application software distribution with digital signature technology is crucial to securing its solution. RIM will need to demonstrate quality in order to attract customers who are increasingly interested in open source or multivendor solutions.

Conclusion

IDC encourages IT organizations that intend to deploy centrally managed mobile systems to evaluate the RIM BlackBerry solution. This white paper has focused on how the BlackBerry solution thwarts malicious code, but the product also has a rich portfolio of security and management capabilities that addresses other risks to deploying enterprise mobile systems.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2005 IDC. Reproduction without written permission is completely forbidden.