CGI

Experience the commitment®

Mobile Device Security

Strategies to minimize security risks and vulnerabilities

Solution Brief

May 2019

In the current environment of mobile computing, bring your own device (BYOD), cloud services and smartphone apps, it is important to focus not only on point solutions for specific problems but also on a holistic “security in depth” strategy, that protects all areas of the enterprise.

This has always been true of enterprise IT security. However, the stakes are higher now. Users demand access at any time, with any device and over any network and require security protocols that can keep pace.

THE MOBILE ECOSYSTEM

The enterprise ecosystem for mobile users and devices is complex and must be understood before a complete security approach can be designed.

The ecosystem consists of four major subsystems:

- End user
- Mobile device (hardware, operating system and applications)
- Corporate enterprise (servers, applications and services, and data sources)
- Network path (connects the mobile device to the corporate enterprise, e.g., local Wi-Fi or cellular communications, network carriers, the Internet, routers, etc.)

To achieve sufficient security for the entire mobile ecosystem, it is necessary to secure all four of these subsystems. Each subsystem exposes a particular set of vulnerabilities and, thus, each requires a security solution that addresses the subsystem’s needs.

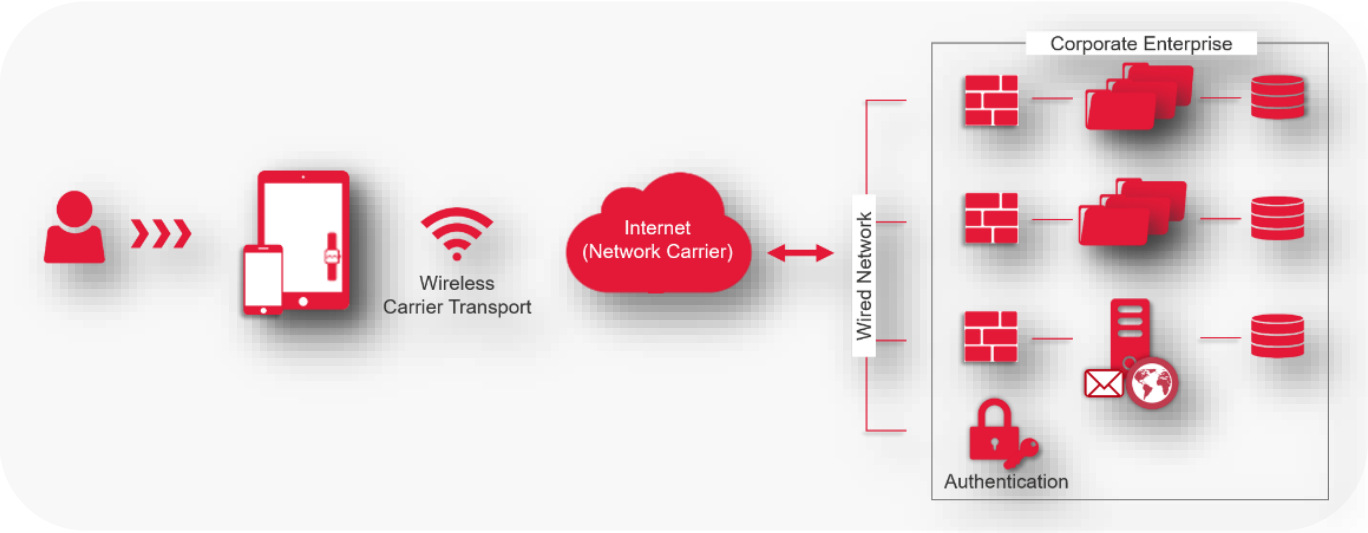


Figure 1: The mobile enterprise ecosystem

CGI's mobile device security solutions address each of these four areas in different ways—according to industry best practices, NIST guidelines and other associated regulatory requirements that may apply in specific customer environments—so each solution is tailored to address and/or mitigate the needs of each agency or enterprise environment.

THE IMPORTANCE OF POLICY

CGI recommends that mobile device security begin with the development and socialization of an organization-wide mobile device policy. Decisions made during the development and documentation of this policy will form the foundation of the resultant solution architecture, application development and testing policies, platform and/or device choices, technical implementation tools, processes, and procedures, acceptable use policies and more. For example, end user service agreements become particularly important in BYOD environments, as certain measures taken to protect organizational data in the event of a lost device—such as a full device wipe—could cause the user to lose personal data and/or pictures that were stored on the personal device when those measures are activated. Organizations should ensure the policy covers topics from all four major areas listed above.

Vulnerabilities, risks and recommended strategies

USER INTRODUCED RISK

A common user introduced risk is losing a mobile device or having it stolen. When this happens, the data stored on the device is at risk, especially if it has not been encrypted. At a minimum, this probably means locally stored emails and/or attachments, but it can also include business contacts, working documents (especially on tablets), photographs/videos and potentially locally cached data pulled from enterprise servers.

CGI recommends developing strong organizational policies covering expected user actions when devices are lost or stolen, mandatory device encryption (often enforced by Mobile Device Management (MDM) solutions) and multifactor authentication, as all will help lessen the outcome of user-introduced risk.

MALWARE ANALYSIS

Malware analysis begins with properly obtaining the malware sample in a way that prevents accidental execution and keeps the sample preserved to ensure sample integrity. Cyber Threat Analysis Center (CTAC) personnel utilize four different methods for malware analysis: static, dynamic, interactive and reverse engineering.

Depending on the circumstances, more than one method may be employed to fully analyze the sample and discover all of the malware capabilities. All four types of analysis take place in either an isolated physical or virtual environment.

- Static analysis involves looking at various aspects of a malware sample without executing the sample.
- Dynamic analysis involves using automated tools in order to execute the malicious code and record its behavior.
- Interactive analysis involves manual execution of the malware in order to observe its behavior, while stepping through each phase of the infection process.
- Reverse engineering of malware samples involves revealing the underlying code of the malware sample for in-depth analysis from a developer perspective and identifying content to build custom defense measures.

CODING PRACTICES AND APPLICATION VETTING

Software developers may not have experience with secure coding practices and, in some cases, they may not be familiar enough with the security implications of their actions to realize they may need to find a better way to implement certain features or retrieve and/or store certain data. Therefore, it is critical for enterprises that develop solutions in-house to conduct regular training on good security practices and conduct reviews of the security design of solutions before they are deployed.

For organizations doing in-house development of applications to be deployed on internet-facing systems (clients or servers), training developers and ensuring that they follow the policies is a necessity. Reviewing the security policies and strategies of a development provider is just as important if the development will be outsourced.

MOBILE DEVICE MANAGEMENT TOOLS

Mobile device management (MDM) tools allow enterprises to enforce organizationally-defined policies as well as monitor and maintain the organization's devices in a number of ways. For example, operating system management on mobile devices is extremely important but, depending on the platform(s), there could be additional challenges for the IT staff with maintaining and validating the proper OS versions and checking for unauthorized changes or certain types of system privileges not allowed or supported within the organization. A strong MDM solution will help organizations centrally manage supported operating systems at current organizationally-approved levels across devices, helping to mitigate impacts associated with policy enforcement (mandatory encryption, multifactor authentication, password complexity, remote wipe capability, etc.), OS updates, OS fragmentation, EOL/EOS hardware and software, rooting and more.

Organizations that provide mobile devices for their workers should definitely consider deploying an MDM solution from an established provider.

TRAINING

Good end-user training is probably the single most important strategy that can be employed to increase enterprise security. Even the most secure system in the world is vulnerable if its users are not familiar with good security practices.

Most organizations have policies in place to forbid users from innocent but misguided actions regarding enterprise IT assets. However, many training programs do not cover the reasons why these actions are dangerous so users often think the policies are unreasonably restrictive. If employees are to take the policies seriously, they must first understand the nature of the vulnerabilities caused by their actions. Security training needs to be updated frequently to ensure users are aware of the current threats in addition to those of the past.

STRONG CRYPTOGRAPHY

Applied routinely, solid cryptography can help close many threats. A well-designed cryptographic solution enforced by MDM solutions can protect both data in transit and data at rest, which reduces the attack surface of the device(s) in question. Strong cryptography is also important in preventing authorization attacks (by avoiding the transmission of log-in information in the clear) and can be a key factor in preventing session hijacking (by requiring properly encrypted data communications for all sessions). Cryptographic solutions can also be used to bind data to applications, sessions and strong authentication of users and devices, further enhancing the sandbox to ensure that only appropriate applications can access data.

MULTI-FACTOR AUTHENICATION

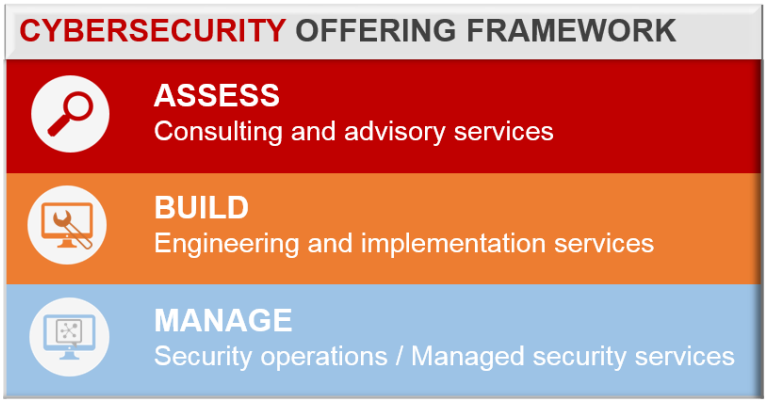
Good security starts with good control over access to resources. This requires confidence in the identities of the users accessing the system. To this end, single- factor authentication (e.g., user name and password) is inadequate in today's environment of advanced persistent threat.

Two- or even three-factor Something you know authentication is critical to Password, PIN reducing or eliminating the likelihood of attackers Something you have successfully penetrating Smart card, magnetic strip systems by stealing or cracking user log-in information.

Two-factor systems rely on authenticating the user not simply by a shared secret (as in the "something you know" approach); they add "something you have" or "something you are" to the formula, forcing attackers to gather information or a physical object in order to log in successfully. The classic examples of this approach are ATM cards, which require a log-in candidate to have a physical magnetic stripe card and the four- or five-digit number that unlocks the card. Another example is the cryptographic token approach (RSA, SafeNet, Entrust, etc.) which requires the user to type in a multi-digit number displayed on a small electronic device carried by the user. The token's number reflects the "something you have," while the user's password or PIN reflects the "something you know."

Three-factor systems are available in today's physical security world. They utilize the "something you know" and "something you have" approaches described earlier, but also add "something you are," usually in the form of fingerprints or facial recognition. It is worth noting the fingerprint/facial recognition technologies are still relatively new and—with hardware and software capabilities varying widely between device models and versions as these capabilities continue to evolve—they may not yet be quite ready for mandatory organizational deployment. However, these technologies should be watched for and evaluated periodically as they continue to mature.

PROTECTING AMERICA'S ASSETS



The CGI Cybersecurity Offering Framework provides an end-to-end portfolio of enablement and transformation solutions that assist clients through the journey of becoming a highly secure organization.

CGI's mobile device security solutions address each of the four areas that comprise a mobile device ecosystem, according to a combination of NIST guidelines, other associated regulatory requirements that may apply in specific customer environments and industry best practices, so that each solution is tailored to address and/or mitigate the needs of each agency or enterprise environment.