

EXECUTIVE INSIGHT

Securing the mobile enterprise

Strategies for minimizing security vulnerabilities and risks

Security challenges for computers, users, applications and data have evolved over the past several years. In the current environment of mobile computing, bring your own device (BYOD), cloud services and smartphone apps, it is important to focus not just on point solutions for specific problems but on a holistic “security in depth” strategy that protects all areas of the enterprise.

This has always been true of enterprise IT security, but now the stakes are higher because users are demanding access from any place, at any time, with any device and over any network.

This paper explores the vulnerabilities and risks of the mobile IT ecosystem and shares best practices to minimize the likelihood of your enterprise losing valuable data to an attacker.

Table of Contents

OVERVIEW	3
THE MOBILE ECOSYSTEM	3
VULNERABILITIES AND RISKS	4
User failures	5
Authentication attacks	5
Local data storage	6
Session hijacking.....	6
Poor data transmission security	7
Poor server security	7
SECURITY STRATEGIES	7
Training	8
Endpoint protection.....	9
Strong cryptography	9
Multi-factor authentication.....	9
Data center security.....	10
Good coding practices	11
Mobile device management tools	11
IMPLICATIONS AND TRADEOFFS.....	12
FUTURE THREATS.....	12
CONCLUSION	13

Overview

Enterprise IT security in the “mobile age” is not what it used to be. The differences we see today primarily stem from the evolution from personal computers to truly personal devices, such as the iPhone, iPad and Android devices that users expect to purchase with their own money (or corporate allowances) and bring to the workplace as either auxiliary computers or even their primary work platform. The velocity of hardware and software development has increased remarkably in the past decade, and users are increasingly unwilling to wait for corporate IT departments to catch up with the latest gadgets. These days, users want to purchase the device themselves, often within days or even hours of its release, and bring it to work immediately.

This scenario carries with it a large number of risks. First, users think of the device as their personal property, rather than something used to access sensitive corporate systems and information. This generally means that they are more cavalier towards security issues than they might be with company equipment. Second, the user is likely to install various personal apps and games, and is much more likely to visit questionable web sites that may attack the device. Finally, because the device accompanies the user everywhere he or she goes, it is much more likely to be lost or stolen.

It is critically important to understand the scope of the problem before proceeding to remediation strategies. In the first section of this paper, we will explore the entire ecosystem of the mobile enterprise. Then, we will move on to discover some of the vulnerabilities this ecosystem presents, followed by the risks created by those vulnerabilities. In the final section, we will explore some mitigation and defense strategies that will help fix the vulnerabilities and reduce the impact of the risks.

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

The mobile ecosystem

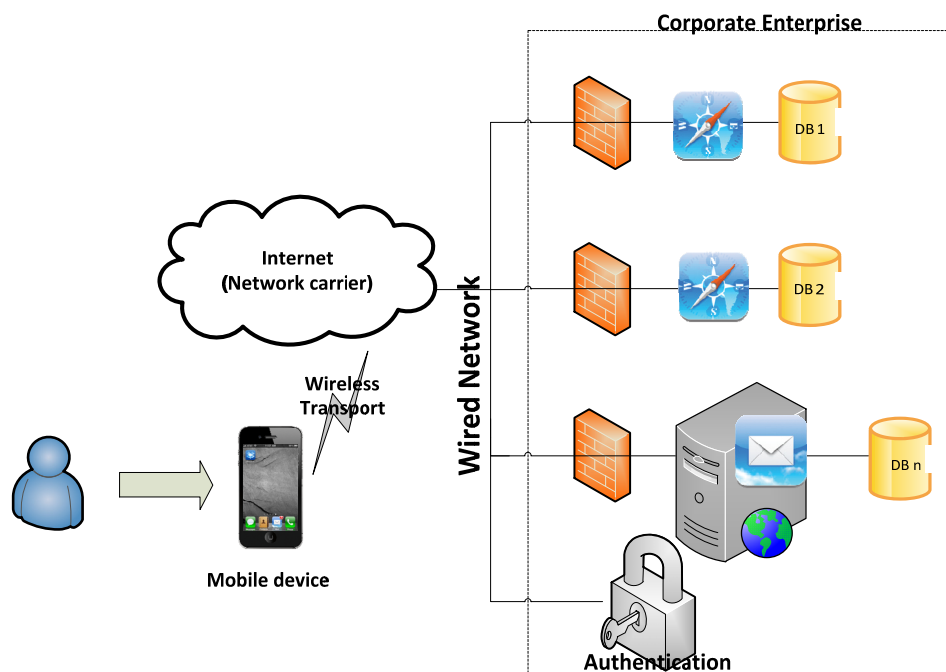
The enterprise ecosystem for mobile users and devices is complex and must be understood before a complete security approach can be designed.

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 WiFi 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 one requires a security solution that addresses that subsystem's special needs.

Figure 1: The mobile enterprise ecosystem



Vulnerabilities and risks

The table below lists some common vulnerabilities in the mobile ecosystem and where those vulnerabilities occur.

Table 1: Vulnerabilities in the mobile ecosystem

	End user	Mobile device	Network path	Corporate enterprise
User failures	•			
Authentication attacks	•	•	•	•
Local data storage		•		
Session hijacking		•		•
Poor data transmission security			•	•
Poor server security				•

Let's take a quick look at each of these vulnerabilities and their associated risks. Some of these vulnerabilities differ between mobile platforms and "fixed" platforms such as laptops and desktops. Where this is true, we will discuss the differences as needed.

USER FAILURES

When users take actions that compromise overall security, the results can be disastrous. These actions can range from sharing account passwords to installing unapproved software to saving sensitive data, unencrypted, on local devices that can be lost or stolen. Some actions are unintentional or result from not following corporate policy, but others are the result of malicious intent on the part of an attacker (e.g., phishing attacks).

User failures frequently result in a compromise of system security, leading to data loss or attacker penetration of a system that stores sensitive data. The worst case for data loss is an ongoing attack in which a “keylogger” or other Trojan software is installed that gives the attacker persistent access to the enterprise network. These attacks can yield not just a snapshot of valuable data, but also long-term visibility into how such data evolves and where it is stored. Long-term visibility might also give the attacker clues that might lead to other sensitive data stored on the network.

Another major type of user failure is losing a mobile device or having it stolen. When this happens, the data stored on the device is at risk. At a minimum, this probably means locally stored email history, but it can also include business contacts, working documents (especially on tablets), and potentially locally cached data pulled from enterprise servers (see the “Local data storage” section below).

User failures can occur regardless of platform. Arguably, user failures occur more often—and with more catastrophic consequences—on “traditional” computers such as laptops and desktops. For one thing, these environments are more likely to have software components with a history of vulnerability, such as Adobe Flash or Acrobat, Java, etc.¹ In addition, phishing emails that lead to drive-by attacks commonly exploit vulnerabilities in these components. Platforms that do not support such components are consequently less vulnerable to simple exploits of user failures of this type.

AUTHENTICATION ATTACKS

When an attacker tries to compromise system security by stealing user authentication data, this is called an authentication attack. Simple one-factor authentication (e.g., user name and password) has been vulnerable for decades. Attack vectors include brute-force attacks, targeted guessing, social engineering, advanced tools such as keyloggers, and more.

Brute-force attacks usually rely on attackers stealing hashed password data from compromised systems. Recent technological developments have made the task of recovering plain-text passwords from hashed databases fast and easy. Rainbow tables frequently allow recovery of a large fraction of passwords with no computation, and GPUs (graphics processing units) found on modern gaming video

User failures can occur regardless of platform. Arguably, user failures occur more often—and with more catastrophic consequences—on “traditional” computers such as laptops and desktops.

¹ Kaspersky Labs IT Threat Evolution Q3 2012:
http://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012

cards have the computational power to process tens or even hundreds of billions of password guesses per second.² This can reduce the task of recovering an eight-letter password to something that can be done in hours or minutes on a home computer that costs under \$2,000 to build.³ Worse still, computing power can be “rented” on demand from cloud vendors such as Amazon. Anyone with a credit card can use hundreds or thousands of CPUs by the hour; this can be done at extremely low cost, if rented at off-peak times. Cloud computing of this nature puts virtual supercomputers in the hands of attackers, with low risk and low cost.

The obvious risk associated with a successful authentication attack is that the attacker gains potentially unrestricted access to any information that the user is entitled to access. In the case of trusted users with elevated privileges, the data exposure could be devastating. Authentication attacks can occur regardless of platform.

LOCAL DATA STORAGE

On mobile devices, most users do not consider what data is stored on the device locally by the applications they use. Most apps store at least basic configuration data, but some create local caches of downloaded data in order to reduce network usage and/or latency. In mobile operating systems, data is generally sandboxed. This means that data can be accessed only from the application used to store it. If the device’s operating system is compromised, however, the sandboxes can be broken, which gives attackers complete access to data from all applications on the device. Even if this is configuration data, the breach can be serious. Consider the implications if the application stored user names and passwords locally!

If a mobile app caches downloaded data locally and the sandbox is broken, the attacker may have access to corporate information downloaded in the application. While this vulnerability is not as great as losing log-in information, it still can result in large data leaks.

Vulnerabilities associated with local data storage are much greater on fixed platforms than mobile platforms, given that sandboxing architecture has generally been implemented on mobile platforms since they first appeared on the market (not so with fixed platforms). Some web browsers (notably Google Chrome) were designed with a sandbox architecture from the start, but this only protects against exploits delivered through the browser. Breaking sandboxes generally requires sophisticated rooting malware, which in turn reduces the number of attackers who have the technical skills required to attack the platform.

SESSION HIJACKING

Session hijacking can occur when session identifiers are used in a web-based application after the user is authenticated and those session identifiers are exposed to an attacker. This most frequently occurs when the web app writes the session identifiers into a URL used after the authentication. Users then have access to the

² <http://blog.cryptohaze.com/2012/07/154-billion-ntlmsec-on-10-hashes.html>

³ <http://hashcat.net/oclhashcat-lite/>

session identifier and can (intentionally or inadvertently) send this data to others by copying and pasting the URL into an email or text message. It's also possible for attackers to read the URL on a compromised device by accessing the browser history. Session hijacking vulnerabilities are present in both mobile and fixed environments.

POOR DATA TRANSMISSION SECURITY

Simply put, all web-based APIs should be using transport layer security (TLS), formerly known as secure sockets layer (SSL). This commonly available technology encrypts communications between client and server. While the security of this technology is currently under debate, it is much better than nothing, and may in fact be good enough. At a very minimum, use of TLS/SSL raises the bar for attackers, making it difficult to gain any information from network sniffing and other related attacks on the network path.

POOR SERVER SECURITY

Securing the server side of a client-server application is a necessary condition for overall effective security. This means applying all relevant operating system and application stack patches, hardening outward-facing servers, configuring firewalls and intrusion detection systems, etc. It also means considering proper system design so that access to data must go through well-defined interfaces on hardened machines so as to prevent large-scale breaches that expose entire databases.

If the server side of the application is not properly secured, the “keys to the kingdom” are available to attackers, who can then potentially have unlimited access to the enterprise network and its data stores. Ultimately, any discussion on overall security architecture must start with how to secure the server(s).

Securing the server side of a client-server application is a necessary condition for overall effective security... If the server side of the application is not properly secured, the “keys to the kingdom” are available to attackers, who can then potentially have unlimited access to the enterprise network

Security strategies

The only strategy that is likely to be successful is one that addresses all of the vulnerabilities directly. Such a strategy would combine technology, training and process in a managed effort to secure vulnerable systems, reduce the attack surface exposed to potential attackers and limit the damage from a successful attack.

History has shown that no network-connected computer system can ever be 100% secure. Therefore, a good security paradigm begins with acknowledging that a successful attack is possible and making sure there are built-in defenses to recognize when a successful attack has occurred (or, better still, to recognize when one is currently in progress!) and subsequently to stop the attack, isolate the affected systems and prevent ongoing data loss.

Maintaining system integrity is also important for forensic purposes, so that the attack vector can be identified and steps can be taken to fix the vulnerability against future attacks.

Table 2 below lists strategies that can be used to mitigate each of the vulnerabilities discussed in the previous section. Some strategies apply to more than one vulnerability, as shown by the “•” in the intersecting cell.

Table 2: Mitigation strategies

	Training	Endpoint protection	Strong cryptography	Multi-factor authentication	Datacenter security	Good coding practices	Mobile device management tools
User failures	•	•					•
Authentication attacks			•	•		•	
Local data storage		•	•			•	•
Session hijacking	•		•	•		•	
Poor data transmission security	•		•				
Poor server security					•	•	

Now let’s look at each of the mitigation strategies to understand how they help reduce the attack surface or mitigate damage from a successful attack.

TRAINING

This is probably the single most important strategy that can be employed to increase enterprise security. The most secure system in the world is vulnerable if its users write down their passwords, share accounts, connect to untrustworthy networks, transport data between devices using an infected USB drive, install malware or expose their computers by responding to phishing attacks. Even IT personnel are a vulnerability if they are not wary of social engineering attacks.

The only way to close many of these attack surfaces is to train users to follow good security practices and recognize (and avoid!) potential attacks in progress. Most organizations have policies in place to forbid users from innocent but misguided actions regarding enterprise IT assets, but many training programs do not cover the reasons *why* these actions are dangerous, so users frequently 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. Also, in a world where the security threat evolves rapidly, security training needs to be updated frequently; users need to be on guard against the current threats in addition to those of the past.

Finally, IT security professionals need to communicate with the users on a regular basis, especially when dangerous exploits appear out of the blue. Many zero-day exploits can be avoided simply by communicating the nature of the threat to users and asking them to be alert until a patch is deployed to close the hole.

ENDPOINT PROTECTION

“Endpoint protection” encompasses a range of technologies intended to help secure the user’s device. Traditionally these technologies have been available only for desktop and laptop computers, but we expect to see a market for them on handheld devices before long. Endpoint protection includes anti-virus and anti-malware features, but also data loss prevention, policy enforcement and general content filtering and/or firewall support.

It is not reasonable, however, to expect that all of these features will be available for mobile devices any time soon. The operating systems on these devices sometimes do not support the types of low-level access needed to perform some of the necessary tasks (e.g., network packet inspection, file scanning, etc.), and the computing power of the devices is not great enough to carry out some of these tasks without placing a heavy burden on the user’s device. However, we do note some basic anti-virus and anti-malware tools for mobile devices and recommend that enterprises consider deploying them on company-owned devices. Clearly, expecting to be able to deploy such software on personally owned devices is on the optimistic side.

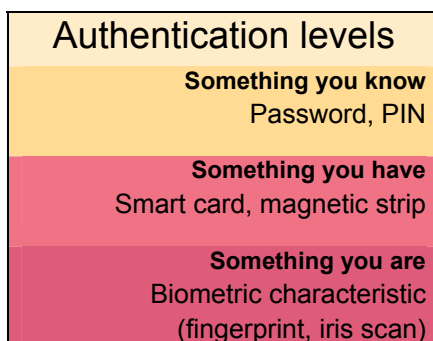
STRONG CRYPTOGRAPHY

Solid cryptography, applied routinely, can help close many of the threats presented in this paper. A well-designed cryptographic solution can protect data in transit and data at rest, which would reduce the surface of attacks against local data storage or the network layer. But good 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 AUTHENTICATION

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 authentication is critical to reducing or eliminating the likelihood of attackers successfully penetrating systems by stealing or cracking user log-in information.

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-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 iris photographs. Migrating these systems to the electronic world is unwieldy for the user but has been done, most notably by the U.S. government in the form of the Department of Defense’s Common Access Card (CAC) program. This program requires users to insert a card in a smart card reader even to use their computers, but can also be used in conjunction with small fingerprint readers to provide all three factors for logical access control.

This heavy approach to three-factor security is probably not tenable for enterprises that wish to authenticate mobile users, but there are new technologies on the horizon that offer three-factor authentication to mobile users without requiring the user to carry additional hardware. CGI offers one such solution, QuadroVoice™.

DATA CENTER SECURITY

It would be easy to fill several volumes with advice on how to achieve good datacenter security, so we will not attempt to address this topic fully in this paper. Suffice it to say that if the servers that store and make available sensitive corporate data are penetrated, it is game over. The attackers win. Like the old joke about why the thief tried to rob a bank (“That’s where they keep the money!”), hackers attack corporate servers because that’s where the valuable information is stored.

Moreover, server and datacenter configurations (to include physical location, IP addresses, security practices, etc.) change slowly, making it possible for attackers

to reconnoiter the target, develop an attack strategy and continue to attack the target until they achieve success. Mobile devices change location frequently and have IP addresses that change frequently—as often as several times per hour for someone driving down the highway! These changes make it difficult for hackers to attack mobile devices with the same tools they use to attack datacenters.

Good datacenter security involves firewalls, intrusion detection systems, network monitors and other tools. It also requires good configuration practices, including keeping operating systems and application stacks updated with the latest security patches, exposing minimum ports and services, and proper layering of servers and APIs. Any enterprise intending to make sensitive data available over the Internet must hire security professionals to oversee the security of their datacenters in order to ensure that these systems are adequately protected.

GOOD CODING PRACTICES

Software developers rarely consider security unless they are forced to do so. 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. Good coding practice is absolutely critical for avoiding SQL injection attacks, buffer overrun attacks, attacks against local caches, authentication attacks, session hijacking, etc.

A full treatment of this topic is beyond the scope of this paper, but several excellent books on the topic are available, and technical training is available from several reputable firms.

If your company is doing in-house development of applications to be deployed on Internet-facing systems (clients or servers), training your developers and ensuring that they follow the policies is a necessary step. If you are outsourcing the development, reviewing the security policies and strategies of your development provider is just as important.

MOBILE DEVICE MANAGEMENT TOOLS

Mobile device management (MDM) tools allow enterprises to monitor the status of mobile devices in terms of installed applications, security posture, allowable web sites, etc. Perhaps the most important feature that MDM tools provide is the capability to remotely wipe a lost or stolen device. It may not be possible to convince users to allow enterprises to install MDM software on personally owned devices, but sensible corporate policies can help alleviate user concerns. Enterprises that provide mobile devices for their workers should definitely consider deploying an MDM solution from an established provider such as Good, ManageEngine, Airwatch or IBM.

In addition to MDM solutions, an interesting new technology appeared in 2012. AT&T offers a context-switching application called Toggle. This tool allows the user to divide the mobile device into Personal and Work partitions. Apps and data installed in one partition are not available or visible from the other. The idea is that users can install Angry Birds, Facebook and other personal-interest applications in the Personal partition, but work-related apps and data go in the Work partition.

Software developers rarely consider security unless they are forced to do so. 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.

Since the two partitions are completely separate, a rogue application in the Personal partition would be unable to access data or settings from the Work partition. The Work partition would also be controllable by the enterprise IT shop so that it is possible to lock down user permissions in this partition—something that users will typically not agree to allow on their personal phone.

Enterprises that support the BYOD scenario are well advised to consider deploying Toggle or one of its future competitors to their users' devices. This technology will act as one more way to reduce the impact to the enterprise of malicious activity on end-user mobile devices.

Implications and tradeoffs

Securing mobile platforms completely probably requires a security-enhanced operating system image, such as SE (Security Enhanced) Android, in combination with other special tools such as Toggle, a mobile anti-malware solution, etc. The challenge for the enterprise support staff is that users always want the latest and greatest software, including operating systems and specialized operating system images can lag the off-the-shelf images by 12 months (or longer). In addition, the processing overhead of anti-virus software can be debilitating to an underpowered computing device like a phone. When coupled together, these approaches are generally not acceptable to users—especially if the user owns the device!

Enterprise IT shops instead need to rely on a combination of techniques that address as many of the vulnerabilities as possible but do not impede users' ability to use their devices. This means user training, containerization, best practices in design and coding of all components of the enterprise solution, etc. When followed well, this approach will lower the threat surface and minimize the impact of a successful attack but mostly be transparent to the user.

Future threats

The threat environment is constantly evolving. Even as we guard against current threats and vulnerabilities, we must remain aware of emerging technologies and the potential for vulnerabilities that emerge with them. For example, it seems clear that near-field communications (NFC) will become common on mobile devices in the next few years. Although this technology is mostly intended for payment solutions, it means that another radio will be present on user devices, and this radio will be used to send and receive data. Aside from the vulnerabilities associated with those transmissions, one has to assume that attackers will want to exploit the mobile platform itself in hopes of capturing information that will allow them to attack the user's financial accounts directly. While this may not be a concern for the enterprise IT environment, it will certainly increase malware authors' interest in mobile platforms, which will in turn make the devices more likely to be attacked.

It will be critical for enterprise IT staff to pay attention to the threat surface of mobile platforms and to help users understand how to defend their devices. Just as

protection measures for corporate laptops and desktops evolve, so must they evolve for mobile devices.

Conclusion

The modern workforce expects to be able to work from any place at any time and wants access to enterprise resources and data from any device and platform. Most corporations today understand the value of supporting this model, but are concerned about the possibility of malicious actors stealing sensitive corporate data.

To reduce the threat to manageable levels, enterprise IT organizations should adopt a holistic “defense in depth” strategy that addresses the entire vulnerability chain. These vulnerabilities include the user, the device, the network, the datacenter server and application stacks that run on datacenter servers.

Each of these links in the chain presents a different set of vulnerabilities, which in turn require specific strategies to reduce the threat surface. The strategies include user training, endpoint protection, strong cryptography, multi-factor authentication, datacenter security, coding practices and mobile device management solutions.

Bottom line: Establishing a good security posture while still supporting the mobile worker requires considering the vulnerabilities across the entire mobile ecosystem and adopting elements of all the strategies described in this paper.

ABOUT CGI

With 71,000 professionals operating in 400 offices and 40 countries, CGI fosters local accountability for client success while bringing global delivery capabilities to clients’ front doors.

Founded in 1976, CGI applies a disciplined delivery approach that has achieved an industry-leading track record of on-time, on-budget projects.

Our high-quality business consulting, systems integration and outsourcing services help clients leverage current investments while adopting new technology and business strategies that achieve results.

As a demonstration of our commitment, our average client satisfaction score for the past 10 years has measured consistently higher than 9 out of 10.

For more information about CGI, visit www.cgi.com or contact us at info@cgi.com.