



# SystemEXPERTS

LEADERSHIP IN SECURITY

---

*A Perspective on  
Practical Security  
2004*

---

## Appreciating the Security Threats Associated with your Handheld Device

### SystemExperts Corporation

*Brad C. Johnson & Richard E. Mackey, Jr.*

---

#### Abstract

Handheld devices are not only as important as other computing resources like desktop and laptop systems in today's business environment, but they have essentially the same functional capabilities. It is quite possible that handhelds are actually even more problematic than those other systems and may require a higher degree of vigilance and management to use safely.

Using them safely requires a critical review of the types of threats that are inherent to them and dealing with each and every one in a thoughtful way.

Deploying handheld computers in a corporate environment requires substantial thought and planning. It also requires understanding the sensitivity of your data, the strengths and weaknesses of your current infrastructure, and the needs of your administrative team in managing these devices.

There are no easy answers. It is important that you allow yourself latitude in the policies you define and the mechanisms you choose. Like any new technology, you will find that your initial decisions or plans may need to change after you have lived with them for awhile.

#### Inside

- Accepting that handhelds are functionally equivalent to other key computing resources
- Understanding all the places that handheld data may reside (it is not just on the handheld!)
- Thinking about wireless connections when your handheld is within range of "hostile" networks
- Synchronization and authentication risks

### SystemExperts Corporation

**Boston    New York    Washington D.C    Tampa**

**San Francisco    Los Angeles    Sacramento**

Toll free (USA only): +1 888 749 9800

From outside USA: +1 978 440 9388

[www.systemexperts.com](http://www.systemexperts.com)

<mailto:info@systemexperts.com>

## Introduction

Handheld devices are not only as important as other computing resources like desktop and laptop systems in today's business environment, but they have essentially the same functional capabilities. Because of this, they are exposed to the same types of threats and vulnerabilities and need to be managed at the same level as those other devices. Handhelds can be even more problematic than those systems and may require a higher degree of vigilance and management. Therefore, using them safely requires a critical review of the types of threats that are inherent to them and dealing with each and every one in a thoughtful way.

For each threat, you need to think about what policies, procedures, or mechanisms (or all three) that need to be considered within your business context to decide how to appropriately mitigate the risks that each threat represents. Keep in mind that security is all about making tradeoffs. There is a limit to the amount of time, money, or energy that you can or want to spend on each issue. A threat that is vital for you to deal with may be a second or third-level concern for somebody else. Because of that, we cannot tell you how to "solve" any of these threats. It depends on your particular environment, constraints, usage model, and risks. But the first step is to identify the threats and how they might affect you.

## Accessing data after it has been "synchronized"

The most common way to populate handhelds with contacts, documents, and email is by using synchronization software. These packages copy data from a system (typically a PC) to the handheld and copy data from the handheld to directories on the system. The data copied during this procedure is configurable, but for convenience, it happens automatically every time you place the device in its cradle. Once the handheld has been synchronized, anybody with access to the computer the handheld synchronizes with can view the copy of the handheld's contents! When the handheld is inserted into the cradle, it first performs a simple device authentication (including the system name) with the desktop and then requires the password to begin the synchronization process. Once these authentication tests are successfully passed, in a Windows environment the handheld now exists as an object under "My Computer / Mobile Device" and the synchronization process creates a duplicate copy of the handheld contents on the local file system.

Remember, one could access the files by having direct access to the system or by using a remote network management program (e.g., PCAnywhere or Microsoft Remote Assistant).

## Active content modification

Two of the most insidious types of network attacks are an attacker changing data while it is on the network or stealing control of a session away from an authorized user. As with any type of real-time modification of network traffic, the attacker can accomplish these feats if he monitors network traffic with a sniffer, intercepts packets (by a variety of methods), and inserts modified packets for his own purposes. Using this technique, the attacker can modify important transactions or gain control of a session (essentially impersonating the user for the length of the session). Once the attacker owns the session, he can carry out any operation the session privileges permit.

These attacks are possible because a majority of the traffic that flows over networks has no integrity protection built into the underlying communication protocols. In fact, unless a user has installed a VPN or is operating secure versions of application protocols, services like email, remote login, web transactions, and calendar can fall victim to modification attacks. While this same problem exists for laptop and desktop computers, the likelihood of handhelds being used in unprotected networks is higher.

## Exploiting bundled cell phone services

Applications on combined cell phone/handheld devices can often be configured to use SMS message reception to trigger activity in other programs. This behavior may allow an attacker to trigger activity that could expose the device to attack or force communications that disclose sensitive information. If an application is designed to exchange cryptographic keys, download mail, or synchronize with a system at the office based on reception of a particular SMS message, an attacker could send that message and exploit a weakness in the communications used by the device.

This would be a particularly dangerous attack if the attacker had physical access to the system and could monitor all network traffic to and from the device. The consequences could be severe if the triggered functionality depends on the obscurity of timing to protect the transaction. For example, if the protocol used to fetch email, login, or update encryption keys were triggered by an event from a centralized server in the form of an SMS message and the protocols were not encrypted themselves, an attacker could force the event and monitor the network for passwords or other sensitive information.

## Automatic wireless network connections

Let us assume that the handheld is set up to have 802.11 wireless connections enabled and that it has IP addresses assigned automatically by DHCP. These are reasonable assumptions as most handhelds are configured to do this by default. When this device comes into range of another access point, it will automatically try and “connect” to it.

The owner of the handheld may be completely unaware that the device is now under the “control” of an unknown 802.11 access point. In addition, if the access point is using DHCP and the handheld is configured to acquire IP address dynamically, the device is now a known resource on this unknown network and can be interrogated or sent packets by any other device on that network. This could leave the device vulnerable to either data mining or direct attack from the foreign network.

The problem here is that through automatic connections, the handheld may be passing network traffic to an unknown and hostile network. With such an environment, the attacker has the potential to impersonate all services that do not require authentication, including DNS, and web sites. In other words, the device is virtually surrounded.

## Cradle synchronization without authentication

As we pointed out previously, synchronizing the handheld with the base system (usually a desktop PC) is a common way to get the latest data, programs, or configuration changes. Given that it is a frequent task, users typically setup their synchronization process to be easy. This usually implies that they have selected to save the password to fully automate the process. This also makes it easier in case they “lend” their device to somebody else to use.

The problem is that if the base system sync files have been tainted, the handheld is going to be loaded with whatever the base system has in place and it will now inherit whatever those problems are: insecure configuration options, trojan programs, malicious code, or modified data files.

If the device contains sensitive information, it is not protected by the security mechanisms, policies, or procedures that we assume are present. Insecure applications, files, or extensions may now be loaded onto the handheld. These same programs may subsequently introduce security problems onto other handhelds in your environment.

## Starting to think about what to do

Let us outline some of the simple steps you can take to address many of the threats described above.

First, make sure your handheld has password protection enabled and the screen lock timer is set to an appropriate value. These two steps will go a long way in protecting your device if it is lost or stolen.

Second, consider your network communications. If you are going to use your handheld in public places, take measures to encrypt your sensitive communications. That might mean a VPN product or may mean enabling encrypted protocols for particular applications like email and synchronization. And, last on the easy to do list, think about your wireless configuration. We have pointed out the dangers of automatic connections. You will have to decide whether the convenience of this capability is worth the risk.

Once you have made choices regarding the easy steps, the more challenging issues remain.

You will need to:

- Assess and address the threats to your corporate infrastructure (e.g., email, calendar) brought about by your handheld deployment
- Develop policies regarding the sensitivity of data you will store and communicate with the devices
- Deploy appropriate security mechanisms for particular data sensitivities
- Select handheld security mechanisms that can be managed across the enterprise
- Educate handheld users regarding threats and their responsibilities

It should be evident that deploying handheld computers in a corporate environment requires substantial thought and planning. It requires understanding the sensitivity of your data, the strengths and weaknesses of your current infrastructure, and the needs of your administrative team in managing these devices.

There are no easy answers. It is important that you allow yourself latitude in the policies you define and the mechanisms you choose. Like any new technology, you will find that your initial decisions or plans may need to change after you have lived with them for awhile.

## About SystemExperts Corporation

Founded in 1994, SystemExperts™ is the premier provider of network security consulting services. Our consultants are world-renowned authorities who bring a unique combination of business experience and technical expertise to every engagement. We have built an unrivaled reputation by providing practical, effective solutions for securing our clients' enterprise computing infrastructures. Through a full range of consulting services, based on our signature methodologies, we develop high level security architectures and strategies, design and implement security solutions, perform hands-on assessments, and provide a wide variety of both on-site and off-site services.

Our consultants are frequent speakers at conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, firewalls, VPNs, and Windows security at USENIX, NetworkWorld-Interop, CSI, and InternetWorld are among the highest rated because our consultants bring years of practical experience to bear. In addition, our consultants have been technical advisors and on-air guests for CNN, Dateline NBC, WatchIT, and CBS News Radio. Every single full-time staff member is certified in some critical security area.

We provide consulting services on both a fixed-price and time-and-materials basis. We are flexible and we can structure any project so that it is just right for you. You will appreciate the difference of working with genuine experts who are committed to earning a long term partnership with you by over-delivering and providing unmatched personal attention.

*Our consultants provide a wide range of services. Below is a sampling of areas in which we advise our clients. [www.systemexperts.com/services.html](http://www.systemexperts.com/services.html)*

### Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. We can perform "White Hat" penetration testing, web application vulnerability assessments, dial exposure ("war-dialing") reviews, firewall analysis, host hardening analysis, IP services inventorying, wireless LAN inventory, VPN assessments, and denial of service reviews to name some of the more frequent testing we do.

### Security Blanket, Emergency Response & Incident Response "Scrimmage"

It is not a question of *if* your organization will be the target of a hacker; it is only a question of *when*. Preparation minimizes the impact of an attack and ensures a rapid recovery. Our security experts will work with you so you'll be well prepared and if you are attacked, we have the experience and expertise to respond to the intrusion in a pragmatic, professional manner. Our emergency response teams quickly assess the situation, properly preserve evidence for use by law enforcement, lock out the attacker, and develop and help implement a plan to quickly regain control of the IT environment. We can also help you prepare for these inevitable events by practicing your response through our acclaimed Incident Response "Scrimmage" Training Exercise.

### Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest intrusion, firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in Windows, UNIX, and other heterogeneous environments. We also provide interim staffing up to the CISO level.

### Interactive Security Workshops & Code Reviews

Using a highly interactive workshop style methodology, our consultants will work with your team to perform a quick but comprehensive review of the security of applications or systems in their full environmental and business context and help you to understand and apply industry best practices. You may use this as the jumping off point for planning and prioritizing security initiatives. Our clients value this Workshop approach because of the knowledge transfer that occurs – the discussions make their team better.

SystemExperts uses this Workshop methodology in a wide range of services including overall security architecture reviews, design reviews, compliance reviews such as CISP or ISO 17799 assessments, Application Service Provider (ASP) reviews, PeopleSoft security reviews, and security code reviews. In the case of code reviews, we perform the detailed analysis of security-critical code modules after completion of the on-site interactive assessment of the application's architecture.

### Security Policy, Best Practices, & Strategy

Security starts with understanding the underlying business and regulatory requirements. Security policy is the means by which these requirements are translated into operations directives and consistent behaviors. We assist organizations in developing and updating policies and identifying where clients' current security practices, policies, or procedures differ from best industry practice. Over the past ten years, we have assisted some of the largest financial institutions in the world in developing overall security architectures.

### Intrusion Detection & Event Management

In security, it is axiomatic that what you can't prevent, you must detect. We have helped dozens of companies (including several of the largest companies in the world) develop comprehensive intrusion detection plans and implement them.

**To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1.888.749.9800**

**Boston**

**Los Angeles**

**New York**

**San Francisco**

**Tampa**

**Washington DC**

**Sacramento**

[www.SystemExperts.com](http://www.SystemExperts.com)

[info@SystemExperts.com](mailto:info@SystemExperts.com)