Hacking the Kiosk

Managing the Risk of Public Information Systems

Bradford Smith
Consultant
Foundstone Professional Services
A Division of McAfee

March 2008

Table of Contents

Executive Summary

Managing the security of information systems in today's interconnected world is a complex and challenging task. Maintaining an accurate perception of an enterprise's digital security posture is key to understanding what is at risk. Using the case of an interactive kiosk, this paper informs the reader how to identify threats and uncover common vulnerabilities from the perspective of people, process, and technology. It concludes with four timeless information security principles that are specifically applied to kiosks.

Introduction

Interactive kiosks are prevalent in society – in the airport waiting area, the street corner phone booth, the business visitor lobby and national hotel chain. They are often used for commercial purposes, such as the GPS tracking and advertising touch screen in the back seat of a taxi. Other times they provide a public service, such as the ones found at the Hall of Records at the community civic center.

One reason for this proliferation is the efficiency of paperless business processes. Companies can accept job applications or invoice customers without printing a single sheet of paper. As most companies already have web applications that perform these functions, the interactive kiosk is an efficient way to improve accessibility.

But this efficiency does not come without a price. Alarmingly, kiosks are beginning to appear in the news about computer intrusions. This is because kiosks provide temptation to both casual passerbys who attempt to hack the device on impulse and malicious users who might launch sophisticated and targeted attacks against the kiosk infrastructure.

Kiosk Data Breaches

Listed below are some real incidents involving computer kiosks:

- **Automotive Manufacturing** – Six distribution facilities were shut down for over seven hours after an ex-contractor used a kiosk in the visitor's lobby of one of the facilities to delete files and passwords on critical systems, causing more than $29,000 in damage and downtime.[1] This is just one example of a computer kiosk being used in an attack against a company.
- **Metropolitan Transportation** – NYC taxi cabs outfitted with a kiosk in the back seat enable passengers to pay, track their travel via GPS, view advertisements, and watch news. An insecure touch screen gave passengers the ability to surf the internet and gain unauthorized access to the

[1] Computer Contractor Pleads Guilty.
http://detroit.fbi.gov/dojpressrel/pressrel07/de060107.pdf

computer operating system itself. Potentially, malicious software could have been installed to steal the credit card numbers of future passengers. This story ran on WNBC-TV and prompted an investigation by the Taxi and Limousine Commission after a blogger published pictures that documented the compromised system.[2] Although there were no reported cases of stolen credit card numbers, this is a good example of how a computer kiosk might potentially be used to attack others users of the kiosk.

- **Computer Security Vendor** – During a popular computer security conference in 2007, attendees demonstrated how to install adware and examine Google search histories of previous users of a public kiosk. The irony is that the kiosk was part of a display for a security vendor, causing some to assume it had been secured.[3] This is an example of an unsecure information kiosk indirectly damaging a company's reputation.

Anticipating Threats

Many of the threats can be identified by observing the unique aspects of information kiosks and how they are different from other technology. The distinguishing characteristics of the public kiosk are:

- **It is an unattended device –** Users operate it on their own, mostly without staff supervision or intervention.
- **It provides a specific service –** Only the features necessary to complete the task intended by the kiosk are enabled. Typically, users cannot install programs, tamper with kiosk software, access the underlying operating and file system, or view data entered by other users.
- **It is deployed in a variety of environments –** A kiosk could be set-up in the middle of a mall or even on an airplane. It could be set-up at a conference that changes

[2] Cab Computer May Be Vulnerable. http://www.wnbc.com/news/14927577/detail.html
[3] Conference Computers So Faux Secured. *Wired Magazine.* http://blog.wired.com/27bstroke6/2007/02/rsa_conference_.html

locations every month or in of a corporate lobby. Depending on the applications and data it requires, it is often connected to a network.

- **It accepts anonymous access –** Unlike a corporate network where users can be assigned different IT privileges according to groups and based on their identity, a kiosk generally allows all users to operate according to the same access restrictions. Therefore, it is not easy to distinguish between trustworthy and malicious users.

Simple Threat Classification

Based on the above characteristics, which are inherent to the kiosk environment, threats to the security of information kiosks can be classified into three categories: threats to the hardware, threats to the end-users, and threats to the vendor.

1. **Threats to the Hardware** – The biggest threats to the kiosk hardware are *vandals.* These people exploit vulnerabilities in the kiosk's physical access controls. This includes theft of hardware, for example from an unlocked cabinet, stealing accessories like the keyboard or mouse, or physical damage.

   Protecting against this threat is foundational, as stated in the common "law" of computer security that "if a bad guy has unrestricted physical access to your computer, then it's not your computer anymore.[4]"

2. **Threats to End-Users** – The biggest threats to end-users are *identity thieves and fraudsters*. These people exploit vulnerabilities in the kiosk's logical access controls. Their aim, in today's ecommerce-driven world, is to steal credit card numbers and personal information from others. A highly trafficked kiosk is a juicy target for their malicious software.

   At the time of writing this white paper an individual is currently awaiting jail sentencing for having installed malicious software that allowed him to intercept data from customers who used business

[4] 10 Immutable Laws of Security
http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx

kiosks. The stolen data was transferred to a website he controlled. The FBI discovered that he used this information to make over $30,000 of fraudulent charges to these accounts in three days.[5]

3. **Threats to the Vendor –** The biggest threats to the vendor or owner of the kiosk are *competitors and cybercriminals*, broadly defined as anyone who can profit from the obtaining the company's confidential information. These people attempt to exploit vulnerabilities in the implementation of the kiosk. For example, due to the variety of environments in which kiosks are found, it can be difficult to deploy the kiosk on a dedicated network segment. So it is often connected to a shared network. This makes the kiosk into a new-attack vector for gaining access onto other systems on that network.

   The author of this whitepaper encountered this situation while performing penetration testing at a government agency. Not only was the insecure kiosk connected to the internal network, but it had drives mapped to critical servers and unrestricted internet access. Unfortunately, this is a common occurrence. A small vulnerability in the kiosk gives an attacker a large window into an organization's internal network.

   The use of integrated networks in the airline industry has been frequently discussed. Recently, the U.S. Federal Aviation Administration cautioned that the computer networks onboard the new Boeing 787 Dreamliner may not properly isolate the passenger network from the plane's control network.[6] This is an important reminder of the consideration that needs to be given to the kiosk and how it relates to the system as a whole.

This brief survey of the threat landscape shows the potential impact that an insecure kiosk can have. The next section on common "low-hanging fruit" vulnerabilities further refines this understanding.

[5] Man Pleads Guilty to Hacking into Hotel Business Kiosks. http://www.usdoj.gov/criminal/cybercrime/tandiwidjojoPlea.pdf

[6] "Hacking at 36,000 ft." *Special Ops Security*. http://blog.specialopssecurity.com/2008/01/hacking-at-36000-ft.html

Exploiting Vulnerabilities

As mentioned earlier, the purpose of a kiosk is to provide a specific service. This is often enforced by special "kiosk software" that restricts a user from doing anything apart from the allowed function. If users can gain access to the underlying operating and file system, they can potentially bypass the kiosk access controls. Even the simplest application might have features that can give an attacker a foot-hold towards compromising the system. Therefore, the biggest challenge in securing a kiosk is limiting the features on an often feature-rich system. This is often implemented in kiosks by restricting the user to a logical "jail" or "sandbox."

The term used to describe this concept is *reference monitor*. The idea is that the part of the system that governs access control needs to be tamper-proof and impossible to circumvent. The most common ways to circumvent the kiosk access controls are listed below. These are all examples of *privilege escalation* vulnerabilities*.*

- **Word Processors** – On the surface, a word processer seems like a straightforward application. But most enterprise word processors ship as part of a larger suite of products. One of the features included when installing Microsoft© Word is a development environment called the VBA (Visual Basic for Applications) editor. This environment can be activated from a blank word document by pressing **ALT + F11** on the keyboard. Given access to this, a kiosk user could use the VBA editor to write a script that would give him access to computer functions that could be used to break out of the above-mentioned jail or sandbox environment.

  Although not as likely to been seen today, the concept of privilege escalation can also be illustrated in `vi`, a de facto Unix text editor. In `vi`, users can insert text into the document and they can also type commands that `vi` will execute for them. The "!" key refers to a shell escape and will execute a command *using the same privileges as the* `vi` *program!* If `vi` was allowed to execute with higher privileges than the user, access to previously restricted resources could be obtained through the shell escape. For example, executing `sudo vi` and entering the command `:!sh` would escape to the shell with root privileges. Other programs, including `ftp`, also use the `!` key to invoke shell escapes.

- **Web browsers** – Checking to see if a web browser is locked down is one of the first things a tester will do during a kiosk penetration test. It is not enough for the address bar to be disabled. Even if right-click is disabled, simply clicking on a hyperlink and pressing the **SHIFT** key at the same time will open up a new browser window, often with the entire address bar and menu enabled. Once the user has access to the address bar, he can usually access non-approved external websites as well as the file system and all mapped drives by browsing to `C:\`.
- **Calculator** – All Microsoft Windows computers contain a hidden web browser. For this example `Calc.exe` is used, but the following works on any application that has a help screen. This can be accessed by selecting the help item (or press **F1**) from the menu bar of the application. There is a small icon on the program bar that when clicked gives the option to "Jump to URL." Websites and local files can be accessed using this method. This is illustrated in `Figure 1`.

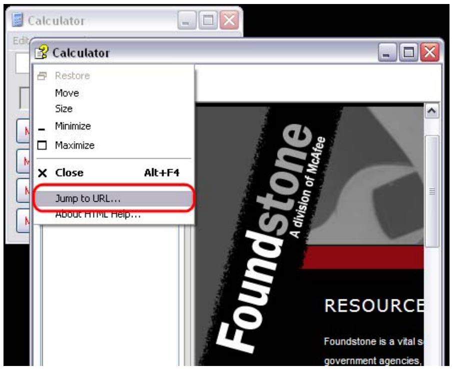
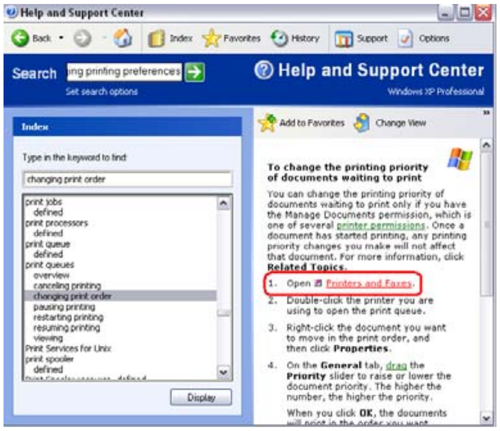


Figure 1: Accessing a hidden web browser in Microsoft Windows

- **Printer –** Another easy way to exploit kiosks using Windows Internet Explorer is through the Print dialogue box. This can be accomplished by pressing **CTL + P** or **CTL + SHIFT + F12**. From within the print dialogue box, there are at least two ways to access the file system. One way is to select the "Print to File" checkbox and then click the "Print" button. This will open up a file browser. The second method is to right-click somewhere in the “Select Printer” area select “Add Printer” or “Properties.” Windows Explorer can then be accessed from the subsequent screens.

- **Help and Support Center** – In addition to the hidden web browser technique described above, the Help Viewer can be used to launch the control panel. This can be accessed by pressing **WINDOWS KEY + F1**. Search for the help page on “Changing printing preferences.” Click “Printers and Faxes.” This is illustrated in `Figure 2`.



Search: ing printing preferences

Type in the keyword to find: changing print order

print jobs
 defined
print processors
 defined
print queue
 defined
print queues
 overview
 canceling printing
 changing print order
 pausing printing
 restarting printing
 resuming printing
 viewing
Print Services for Unix
print spooler
 defined

To change the printing priority of documents waiting to print

You can change the printing priority of documents waiting to print only if you have the Manage Documents permission, which is one of several printer permissions. Once a document has started printing, any printing priority changes you make will not affect that document. For more information, click **Related Topics**.

1. Open Printers and Faxes.
2. Double-click the printer you are using to open the print queue.
3. Right-click the document you want to move in the print order, and then click **Properties**.
4. On the **General** tab, drag the **Priority** slider to raise or lower the document priority. The higher the number, the higher the priority.

When you click **OK**, the documents

Figure 2: Using Help Center to launch the control panel

These four examples underscore the difficulty that kiosk administrators and software developers have with enforcing access restrictions. They also give an idea of how many, some seemingly esoteric, parameters and registry keys must be blocked by an admin who is trying to lock down a kiosk. Missing any one of these can let an attacker in.

Strategic Recommendations

What does it mean for a kiosk to be secure? Often people pursue “security” without a clear idea of what that means. Usually, if the impact of a threat exploiting a vulnerability is negligible, then the kiosk can be called secure. It is important that the answer to that question take into account the context, threat environment, and potential vulnerabilities of the kiosk. Having done so, this paper presents four principles that can be incorporated into the process of securing the kiosk.

Timeless Security Principles

Although these principles were first published in 1970s[7], their application remains relevant to computer systems today.

- **Fail-safe Defaults** – Because a kiosk serves a specific purpose, it is best to specify what actions a user can take, rather than what actions they cannot take. In other words, use a white list instead of a blacklist approach. Not only does this require less complexity, but it prevents failures from going unnoticed because an alert can be sent out when an intrusion is detected. The system can assume that anything not explicitly permitted is a security violation and commit the action to a log file.

- **Least Privilege** – Each component of the kiosk should operate using the least set of privileges necessary for its function. Avoid giving out any unnecessary capabilities. This also limits the damage that can result from accidents or errors.

Component	Example
Internet / Network	Block outbound internet access if the system's job is to provide access to a locally hosted website.
Network	Consider the kiosk an untrusted device and segregate the network it is connected to from the internal networks.
Operating System	Reduce the number of available features by running embedded operating systems or thin clients.
Hardware	Realize where hardware restrictions can be bypassed. The on-screen keyboard is often used to bypass restrictions from a limited or disabled physical keyboard.
Authentication	Access to administration areas should rely on proper credentials rather than obscure key combinations or mouse movements.

- **Least-Common Mechanism** – One of the main features of a kiosk is that it is shared by many users. A certain amount of segregation and isolation is necessary. Potential information paths between kiosk users should be minimal. This might mean wiping the kiosk storage and memory after every session or at the end of the day.

- **Open Design** – It is strongly encourage that the kiosk implementation be subjected to threat modeling, code reviews, or penetration testing. Exposing and fixing the weaknesses of a system

[7] Saltzer, Schroeder. "The Protection of Information in Computer Systems." *Proceedings of the IEEE 63*, 1975.

provides a high degree of confidence and assurance, rather than relying on ignorance of a system's vulnerabilities.

Summary

Many kiosks have faux security and are at risk of being exploited, potentially resulting in reputation damage, fraud and identity theft, all of which can have a financial impact on an organization. By anticipating potential threats and uncovering common vulnerabilities, business's can manage their public information systems with a high degree of confidence that the impact will be minimal should someone hack their kiosk.

About the Author

Brad offers trusted advice to professionals who need to advance their corporate information security strategy. His core expertise as a network and application security professional underpins the broader business objectives of his clients. He is adept at assessing and prioritizing the digital risks an organization faces to their technology, processes, and people. He is based out of Foundstone's southern California office.

About Foundstone Professional Services

Foundstone® Professional Services, a division of McAfee. Inc., offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, Foundstone identifies and implements the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The company's professional services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military.