Kiosk Marketplace .com

SPECIAL REPORT

Software Security: The Importance of Locking Down Your Self-Service Kiosk

SPONSORED BY:

KIOWARE® kiosk system software

Keeping a self-service kiosk safe goes beyond the enclosure. Learn measures that can protect kiosk software.

By Richard Slawsky | Contributing writer, KioskMarketplace.com

It is a self-service kiosk deployer's worst nightmare: Doing nothing more complicated than unplugging a kiosk and plugging it back in, a hacker accesses the kiosk's operating system and wreaks havoc on it and the accompanying self-service network. Equally as frightening, through various keystrokes or touching different parts of the screen, a user burrows into a device's file system, tapping into sensitive data.

It's a fact of life in the world of technology. For every technological application designed to benefit society, there are people who want to use that technology to cause damage.

In June 2012, a breach at kiosks deployed in Ontario, Canada, by the provincial government exposed debit card and personal information of thousands of citizens. All 72 of the kiosks, which allowed users to renew drivers' licenses and health insurance cards, were taken offline after the incident.

TJX's data breach in 2006 — which reportedly originated at in-store job application kiosks — was one of the largest breaches of customer data in U.S. history. The snafu, which TJX (parent company of T.J. Maxx and Marshall's) has spent tens of millions of dollars investigating, prompted the retail industry and legislators to take a closer look at data security for businesses that handle payment card information and reinforce the Payment Card Industry's Data Security Standard.

Sometimes the least visible component (of a kiosk) — the operating system— can create the most dangerous vulnerability.

Kiosks can be surprisingly easy for hackers to access, leaving private information vulnerable and costing a deployer money and his reputation. In addition to kiosk system software, hardware provides an additional layer of security to protect a deployer's intended user experience.This kiosk by EuroTouch for the Community Health Partnership is one example.

Kiosks can be surprisingly easy for hackers to access, leaving private information vulnerable and costing a deployer money and his reputation.

Unfortunately, kiosk hacking is an ongoing problem. A quick Internet search yields hundreds of pages devoted to showing methods to access the operating system of a variety of kiosks and how to manipulate them to a hacker's advantage.

The rewards of hacking a kiosk vary. Often, hackers disrupt a kiosk simply for the challenge. Some vending units contain expensive merchandise, such as mobile phones or electronics. But the most valuable reward to a hacker may be the information contained within a kiosk. A loss of this kind not only can cost retailers money but also damage their reputation.

An attack on a public-access kiosk's software could result in the theft of a user's personal data, such as passwords to various websites, if that information is not cleared immediately after the user leaves.

And an attack on a kiosk deployed by a company to provide human resources services could result in the loss of Social Security numbers, as well as medical information, family history and names of associates and former employers. The scope of a theft in this regard is potentially even more staggering, since a company's self-service kiosk may be connected to the company network, containing the information for dozens, if not hundreds, of employees.

Finally, the deployer himself may be the victim since confidential information, ranging from sales numbers to the accumulated data of users, may be stolen, damaging a company's reputation and infrastructure.

Manufacturers and deployers of self-service devices spend significant resources securing their technology. Enclosures are designed to keep the machine in place and guarded against thieves and vandals. Cash acceptors can be configured to work with armored-car carriers. Even surge protection and communications vulnerabilities are addressed in hardware security.

But sometimes the least visible component — the operating system — can create the most dangerous vulnerability.

Danger comes not only from miscreants. A power outage can expose the same weaknesses as unplugging the kiosk. Sometimes, a frustrated user who pokes wildly at the interface can hit a single button or a combination that allows system access. Malicious intent aside, even a well-meaning user can download a virus, reset the system, or access private information if the kiosk application is not secure.

By keeping a kiosk's application software secure with lockdown software, deployers will save themselves time, money and an immeasurable amount of aggravation.

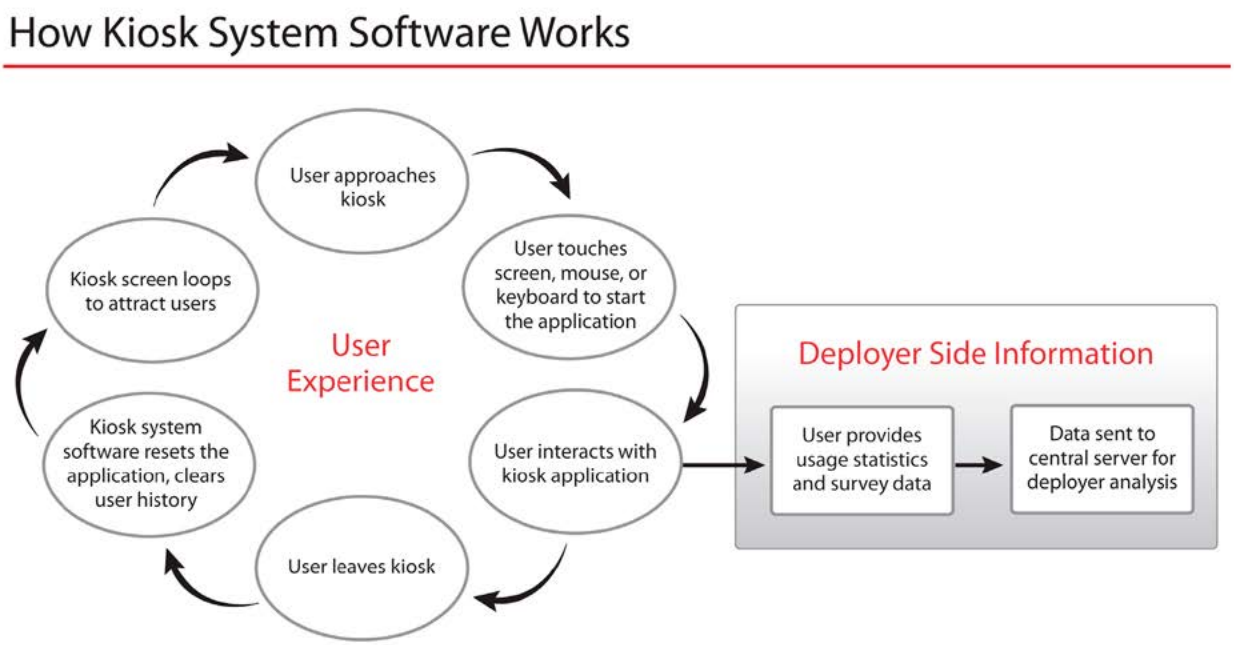
And just as attacks — intentional or accidental — can have many sources, the potential damage is multifaceted as well. Along with misuse of sensitive customer or corporate information, the kiosk might be taken offline for hours or even days, resulting in a significant impact on sales. Inappropriate material may be displayed on the kiosk for all to see, resulting in a public relations nightmare.

"If kiosk system software isn't being used, then yes, it is that easy to access anything and everything on the kiosk," said James Kruper, president of York, Pa.-based KioWare, a provider of kiosk system software. "Using software lockdown protection is extremely important," he said. "You always want your kiosk to be used for its intended purpose."

Point of vulnerability

Kiosks generally employ two kinds of software: application software and system software, Kruper says. The former may create vulnerability, while the latter should protect against it.

Application software controls the task the user wants to perform. Kiosks may contain several different applications, i.e., see if an item is in stock, sign up for a loyalty program or check for a wedding registry.



Kiosk system software supports the deployer's intended user experience by addressing kiosk-specific issues and securing the kiosk application.

A virtual keyboard can prevent the intentional or inadvertent access to system files associated with certain keystrokes on traditional boards. In addition, since they have no moving parts, virtual keyboards reduce upfront and maintenance costs.

Each application is presented as an array of tasks the user may want to perform.

System software addresses kiosk-specific issues, securing the kiosk application and end-user information. Application software is a function of system software. When a consumer decides she wants to join a retailer's loyalty program, it is the system software that directs that program to start.

The main function of lockdown software is to ensure that access to an application on the kiosk is restricted to its intended use. Software must be properly designed to ensure misuse doesn't compromise data that is stored locally.

Lockdown software may lock down as many or as few aspects of a computer as a deployer prefers. Protection may be added or enabled as time passes, also at the discretion of the deployer.

Protecting a kiosk is relatively inexpensive, especially when looked at in relation to the time spent repairing it or the cost of covering damages. Depending on the provider and the functionality of the security software, Kruper says, prices range anywhere from $39 to $500 or more.

One popular product from KioWare, KioWare Lite, Kruper says, is $70 per license. The software includes the basic browser, OS and desktop lockdown service, as well as a security audit feature that provides industry best practices and points out features a deployer may have missed, such as catching certain keystrokes that could be dangerous. Other KioWare products feature usage statistics and server-side management capabilities. KioWare is available for the Windows and Android OS.

By keeping a kiosk's application software secure with lockdown software, deployers will save themselves time, money and an immeasurable amount of aggravation.

"This type of software, it just puts its own shell up there," said Vincent Giardina, systems administrator for the Greater New Orleans Federal Credit Union. "There's not much [an attacker] can do."

Giardina says lockdown software has been installed on two public-facing computers that may be used by any member of the credit union. No attempts have been made to attack the computers, but Giardina says the credit union decided to be proactive.

"That's what you need to do when you're dealing with computers, especially in the banking industry," Giardina said.

Kiosk system software locks down and disables as many key combinations as the deployer wants.

Disabling specialty keys and key combinations

Kruper tells the story of an Internet provider who set up shop in a mall to demonstrate the difference between high speed and dial-up Internet. Typically, hundreds of tech-savvy teenagers a day visited the computers and gained access to the system through key combinations. And at the end of each day, the provider had to re-set his computer settings because he had neglected to use any kind of software protection.

Key combinations may be gateways to a kiosk attack since they allow access to certain functions. The combinations may be entered deliberately by a hacker hoping to gain access to the kiosk's operating system and software, or inadvertently by a child who cannot see the screen but can reach the keyboard.

A virtual keyboard can prevent the intentional or inadvertent access to system files associated with certain keystrokes on traditional boards. In addition, since they have no moving parts, virtual keyboards reduce upfront and maintenance costs.

On many machines, the combination of 'Ctrl'-'Alt'-'Delete' allows access to the computer's task manager and essentially holds the power to shut down the computer, lock its functions or log off. 'Alt'-'F4' allows the user to quit the current program while 'Ctrl'-'Esc' opens the Start menu. Although relatively harmless on a home or office PC, these key combinations, if enabled on a kiosk's keyboard, could open the virtual doors to a self-service network.

Since many kiosks use Windows as the operating system for their computers, many also may have embedded commands that are unique to Windows and could expose the system's software. Any Windows or generic key combination, no matter how minor, should be disabled completely before the self-service kiosk is deployed. This cuts off the ability of an experienced hacker to obtain access to applications, stored files and information while making it impossible for a user to inadvertently trigger a shut-down or similar event.

Software security locks down and disables as many key combinations as the deployer wants. Other features, which may be common to computers' operating systems, may also be disabled by lockdown software.

Deployers may choose to have some security features added, depending on the type of self-service deployment. Deployers may opt to further increase security with the use of touchscreens and virtual keyboards, possibly eliminating the need for a keyboard entirely. Specialty keys and key

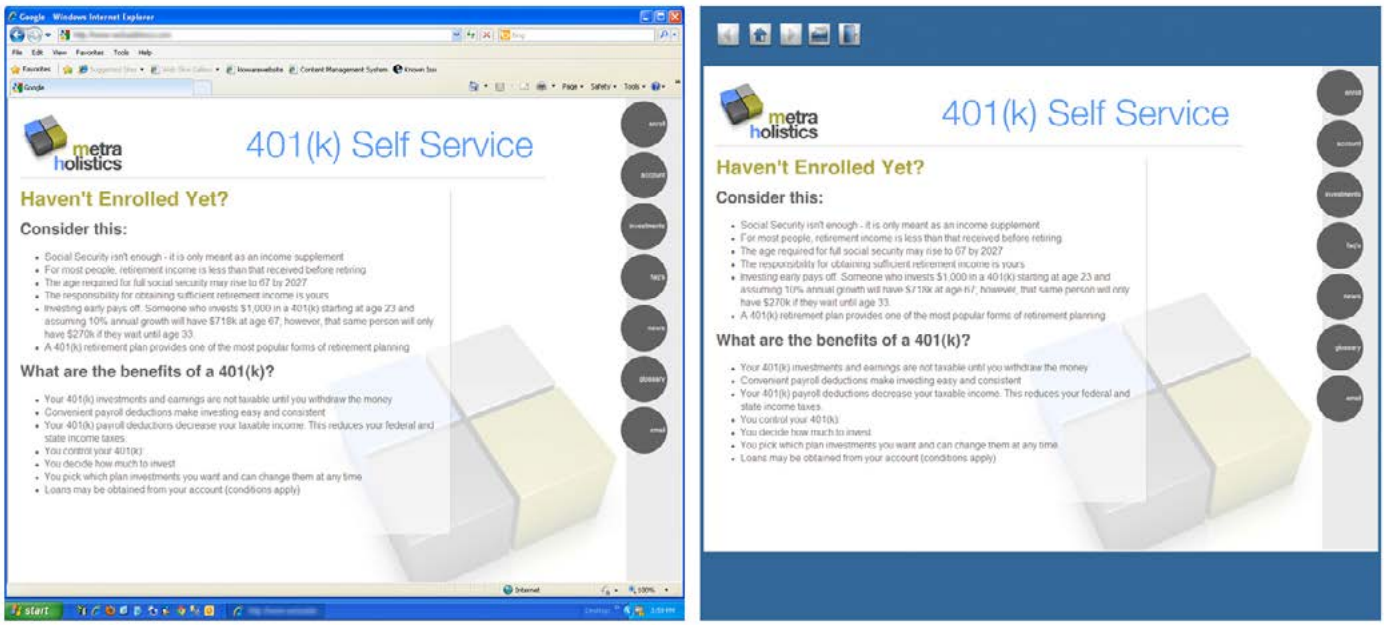
combinations are no longer available because virtual keyboards are kiosk specific, and there is no longer the cost of maintaining a physical keyboard.

Attract screens

The attract screen is used to attract attention to a kiosk when it's not in use. Through the use of basic graphics and instructions, attract screens can show users how the kiosk may be used and how to operate it. As soon as a user touches the screen or keypad or swipes a magnetic stripe, the attract screen is deactivated and the application takes over. Soon after a kiosk becomes idle, software should end the previous user's session, clear all cookies and cache, and initiate the attract-screen loop.

The time-out function is activated by the user once he starts to use the kiosk. If the user takes too long to answer a question or enter information, a prompt will appear on the screen asking the user if he is ready to proceed or needs more time. If the user is still there, a simple touch of the screen or a prompt deactivates the function and he may continue, but if the user has left, the application can be reset.

An additional reason for attract screens is to replace the Windows screensaver, which allows access to the entire system and leaves the kiosk vulnerable



Two screen shots with a hard-to-see but very important difference. The one on the left leaves buttons exposed that could allow someone to hack the machine. The one on the right conceals the vulnerable features. It replaces the standard internet Explorer toolbar with a kiosk-specific custom toolbar.

to security threats. Adequately secure system software supplants the role of screensavers and performs these additional, security-enhancing tasks.

Attract screens also can serve as embedded advertising platforms, offering an additional revenue stream. The kiosk can display the name of the deployer or can feature paid advertising from third parties.

Ending the session

Once an application has completed its task, it is essential that it logs the user off and then re-starts with all evidence of the previous session or transaction erased. Many Internet browsers come with a feature that automatically saves passwords and other personal information in order to save the user time. At home or at the office, this is a practical feature. But if enabled on a publicly accessed self-service kiosk, it may allow follow-up users to see and use previously entered data.

Security software for HR kiosks

Employees use HR kiosks to log into their HR accounts, which contain confidential and private information, so it is essential that an HR kiosk's physical design and placement, as well as programmatic function, are secure. Not only does the kiosk need to be equipped with vision barriers and placed so that other staff cannot easily see the display screen, it also needs to have the perception that the information is safe and secure. The most well-guarded kiosk will be wasted if no one uses it because the perception of safety is missing.

The kiosk system software needs to ensure that the user's session is automatically ended when the user leaves the kiosk. Typically, this is accomplished using a security mat or proximity switch that initiates the log-on screen when a user arrives at the kiosk. Such technology sequentially flushes local variables and resets the application immediately upon the user leaving the kiosk.

In HR applications, users often want a printout of their changes and records. Many times, users will print their information and then proceed with other HR activities. If the user then forgets about the printout, there is a risk of other employees removing the printout and viewing the user's private information.

Kiosk printers with retracting capabilities are a must for user privacy. Now, if forgotten by the user, the document is retracted back to an internal disposal box, thus maintaining the user's privacy. Kiosk printers generally retract after a designated amount of time, but that does not ensure complete privacy. What if a new user approaches the kiosk immediately after the first user and takes the printout before the printer has been set to retract? The most reliable way to make certain that the user's printout is protected is by conjoining the retract event with the security device's termination of the user's session. Such a conjoining means that if a user steps off the security mat without taking her printout, it will instantly be retracted, thus ensuring the user's complete privacy. ■

Enabling an application to log the user off, clear history and reset immediately is crucial in preventing this kind of theft, says KioWare's Kruper.

Control of dialog boxes

Dialog boxes also represent opportunities for an attacker to wreak havoc on a self-service kiosk.

A print box is an example of a dialog box. Other dialog boxes may ask the user if he wishes to use a particular function. Lockdown software can limit the role of dialog boxes, turning them on or off based on the preference of the deployer, and even altering the functionality and appearance of OEM versions to suit the security preferences of the deployer. Deployers can permit only limited dialog boxes to appear and permit only yes or no answers to questions, for example.

And in addition to enhancing security, this functionality also can save money by limiting print functionality — preventing users from, say, sending too many copies to an attached printer.

It is important to limit the ability to access dialog boxes, as they can open the file menu, allowing access to the entire file system. Eventually, users can access a Windows help menu that automatically opens Internet Explorer. From there, a user can navigate wherever he chooses.

Kruper says blocking file downloads is another part of dialog box blocking that should be considered. Downloads from outside sources may contain viruses that can cripple the kiosk and a business' self-service strategy.

Allow/revoke lists

"Allow" or "revoke" lists also are key features of lockdown software. Installed on computers with Internet access, these two security functions work much the same way. A deployer may choose to allow access to a selected list of pre-approved domains or pages, such as his own bank's homepage or a retailer's website. Other domains or individual pages may be blocked ahead of time. While there are specific programs, such as Net Nanny, to accomplish limitations to pornographic websites in general, kiosk system software can allow or revoke specified websites, allowing for comprehensive control over the user's online activity.

Remote monitoring

Lockdown software also offers the deployer the option to remotely monitor his self-service kiosk or network from a central location.

Tablets and self-service

Mobile tablet devices and self-service

The self-service industry has another new technology to absorb: mobile tablet devices. As companies seek new technology opportunities, devices such as the iPad and similar tablets are being used for self-service. Unfortunately, these devices come with the same security issues as kiosk self-service applications.

Why deploy tablets as self-service apps?

Mobile tablet devices are easy to connect to Wi Fi or cellular data networks. They have mature and intuitive touch screen interfaces. They also have the flexibility to be mounted in a fixed kiosk pedestal or be deployed as a true tablet.

What applications are well suited for tablets?

Healthcare providers have begun offering paperless check-ins using mobile tablet devices, and hotels have used them to display all of their services electronically within each room. In retail, tablets are used for POS, price checks, and loyalty card administration. Marketers are using tablets for survey data collection. The list is growing and the sky's the limit.

The Apple iOS iPad was the initial breakthrough device, but since its introduction there have been many Android and Windows 8 tablet devices announced. Despite being first to market and whose subsequent market success opened the self-service industry to the possibilities of tablets, the iOS operating system is surprisingly not well suited for self-service.

Self-service imposes many demands on an operating system that are far different from the standard consumer use of the device; unfortunately, by having a closed operating system, Apple has tied the hands of anyone wishing to write robust self-service applications.

On the other hand, Android has an extremely open operating system that is well suited for self-service. Similarly, Windows 8 is also a viable platform for self-service especially when a broad range of external device support is necessary. Another

key issue is the iPad is only available in a consumer quality device, whereas Android and Windows 8 devices are becoming available in higher quality OEM configurations which are designed to run 24x7 in a self-service environment.

Similar to the PC used in a self-service kiosk, the tablet needs to be protected from abuse, nefarious or not, by the self-service user. The user's personal information needs to be similarly protected, since the device will be used next by a complete stranger. This protection takes many forms.

The desktop/launcher

It is critical to prevent the user from accessing the Desktop/App Launcher. The user should be allowed to run the specified application, but prevented from configuring or executing any other applications as well as downloading and installing any new applications.

Browser lockdown

If the application uses a browser, and most will, it is important to ensure the user is limited only to the domains or pages allowed. In addition, if displaying Web pages, then links such as mailto tags or file downloads need to be blocked.

When the user has finished, all traces of that user's presence on the device must be removed.

Remote monitoring

An important aspect of any self-service deployment is the ability to remotely monitor the device to determine its current status. Is your application running? Are any components reporting errors? For a tablet, the requirements can expand to also include the physical location of the device and the battery life remaining.

Device security

Tablets have one major drawback: they are mobile. It is important for the software to a) let the user know the device needs to be returned, b) indicate to the user when the device is about to leave an approved operation area, and c) lockdown the device and provide retrieval information to the deployer when the device has left the approved operation area.

Mobile tablet devices have great promise to improve the self-service experience; however, there are challenges to mobility that must be addressed and today the Android OS and Windows 8 are the best platforms for self-service. KioWare offers a full line of kiosk mode software for the Android and Windows OS that ranges from basic browser lockdown to server based remote monitoring/management.

Source: KioWare

About the sponsor:

Founded in 1991 to provide client server software development, Analytical Design Solutions Inc. (ADSI) developed KioWare (www.kioware.com), award winning kiosk system software, in 2001, and KioWare for Android software in 2012. KioWare deploys browser-based applications into a kiosk mode environment easily and inexpensively, securing the operating system, and allowing users to access only the application. Each client has the ability to customize KioWare to his or her needs, appealing across multiple vertical markets. The KioWare product line ranges from basic browser-lockdown to server based remote monitoring.

For applications where reliability is crucial, kiosk system software has both hardware and software watchdog capability. The software watchdog constantly monitors the health of the kiosk system software .exe and restarts the .exe when necessary. The hardware watchdog constantly monitors the health of the software watchdog and restarts it when necessary.

In addition, a daily update of the kiosk's activity may be viewed, and e-mail or text alerts may be received if there is a kiosk error, such as a printer jam or loss of functionality.

Remote monitoring allows the deployer to update software without sending a technician to the location and to monitor performance statistics such as usage.

External security device support

External devices that work in conjunction with lockdown software may be an option. Security mats are weight activated and close down or reset the application if the user steps away.

If a retractable printer is used, kiosk system software can support the integration of the device. This option senses when printed information is not taken and retracts it back into the kiosk, preventing the wrong eyes from seeing it.