KIOSK SOFTWARE: WHAT IS IT AND WHY DO I NEED IT?

Learn about the kiosk-specific security features that Kiosk System Software covers.

KIOSK SYSTEM SOFTWARE: WHAT IS IT AND WHY DO I NEED IT?

The need for application protection is critical, but unfortunately it is usually an afterthought. Kiosk system software ensures that your application is secured and always running, preventing misuse and allowing kiosks to remain unattended. Specifically, kiosk system software protects the application by blocking users from ever reaching the Operating System (OS) or desktop and limiting browser use. This prohibits users from changing systems settings, surfing the Internet, overwriting files stored locally on the kiosk and accessing sensitive company, employee and user information.

APPLICATION SOFTWARE VS. SYSTEM SOFTWARE

There are two types of kiosk software: application software and system software. The application software is designed specifically to interact with users and provide the kiosk functionality, while the system software protects the application. The kiosk system software wraps around the application, rendering all else inaccessible to users, while providing kiosk managers access to the entire system with a passcode, mouse sequence or key combination.

The two types of software can be separate or the system security can be programmed into the application. The latter requires the application to be custom developed, which is often more expensive and time-consuming as the developer must be involved anytime a change needs to be made.

KIOSK SYSTEM SOFTWARE BEST PRACTICES

Kiosk System Software best practices include taking advantage of kiosk-specific security features, which are listed below.

Keyboard Filtering: For applications that have a keyboard available to the user, it is critical to disable certain specialty keys and key combinations. The keys could open a new window, dialog box, menu, or allow users to escape the application altogether. This allows access to the OS where users can easily navigate to anywhere on the kiosk. Specific keys and key combinations that should be blocked are:

- CTRL+ALT+DEL – allows access to the task manager
- F1, F2, F3...F12 – can open a new window and can be customized to load windows that are not appropriate to the kiosks function
- Pause – a user could hit this and walk away from the kiosk, leaving an inappropriate screen on the kiosk
- Esc - can allow the user to escape the entire application
- Windows – opens the start menu
- CTRL+P, CTRL+N, etc. – opens the print dialog, opens a new window
- ALT+F4 – exits the application
- Menu – opens a pull down menu of the application

Virtual Keyboard: The virtual keyboard, which works with touch screen hardware, reduces hardware vulnerability by eliminating the need for a physical keyboard and mouse. The keyboard is kiosk-specific, meaning certain keys (such as CTRL+ALT+DEL) are not programmed into the virtual keyboard.

Attract Screens/Session End Features: Attract screens essentially replace the Windows screen saver, which would allow access to the OS, by rotating through images, ads or URLs instead. This feature can also be used to end a user's session, by logging a user off after a certain period of idle time and beginning the attract screen loop. The previous user's history, including the cookies, cache and print queue are then cleared. Clearing the previous user's history is imperative in making both the previous and potential user feel safe, and securing their personal information from the next user or any passerby.

File Download Blocking: Kiosk system software can prevent dialog boxes from being shown and ultimately prevent file downloading altogether. It is important to block dialog boxes from being shown; eventually a user could navigate to a Microsoft help link allowing access to browser windows and function-critical C: drive files.

External Device Support: Kiosk system software also supports the integration of external devices for added security. Session end devices, such as retractable printers, retract printed materials immediately back into the kiosk at the end of a session. Security devices, such as security mats or proximity switches, sense whether users are standing at the kiosk, and will reset the application and clear the previous users' history as soon as the user steps away.

Remote monitoring: From a central server, kiosk system software can manage multiple kiosks, specifically through remote monitoring and content updating. Remote monitoring supervises the kiosk's health by sending regular heartbeats to ensure the kiosk is up and running, as well as alerts for anomalies such as a paper jam. This feature also produces usage statistics and survey data for analysis.

WHY NOT RUN IE IN KIOSK MODE?

The problem with using IE in kiosk mode is that many kiosk-specific security features are lacking. Many of the key combinations will still allow users to open a new window or close the kiosk window. This allows access to the entire machine, where users can overwrite files critical to the function of the kiosk. Additionally, IE in kiosk mode does not clear the history of the previous user, which is especially important when the user is entering or accessing any personal information. Lastly, IE in kiosk mode does not return to the start page after the session end and does not rotate through attract screens, which show users how to use the kiosk and explain its purpose.

CONCLUSION

If the kiosk is not secured, it can be hacked, either maliciously or unintentionally, and costs will be incurred. The kiosk may be inoperable, users may feel unsafe, or sensitive information may be stolen from the kiosk. Protecting your kiosk application with kiosk system software protects potential victims, your application, and your bottom line.

ACTION STEPS

Download a free demo

Most kiosk system software companies offer free trials to test with your application. Use this time to contact their support staff to ensure any problems or questions you may have can be answered prior to purchase. This is also a good test to see how the company will handle any issues after purchase. Also test thoroughly with your application and make sure the system software was designed for your intended use. For example, if you plan to have your kiosk accept payments, make sure the kiosk software can be configured with a mag stripe reader, which is used to swipe credit cards. Otherwise, you will need to build this ability into your application.

I recommend: Test a demo of any kiosk software before you purchase. KioWare Kiosk Software, which specializes in browser lockdown security as well as server-based remote monitoring, offers a 500 hour fully functioning free demo. Sitekiosk also offers a limited trial.

Use best practices

Do your research. Pick the brains of the kiosk software company you are testing; they have likely worked with hundreds of clients before that have encountered your same issues. Scour the Internet for blogs, articles and reports on kiosk best practices. Information on hacking kiosks is easily attainable, but the information to prevent hacking is just as attainable.

I recommend: Some kiosk software, like KioWare, offers a security audit feature. This feature contains the best practices for kiosk-specific security, allowing you to pick and choose which settings you would like to change. Summit Research, a company dedicated to kiosk consulting and developing reports on the kiosk industry, also published a very thorough report on kiosk project best practices: http://www.summit-res.com/bestpracticesreport.html, which you can purchase for $695. Or you can download this Kiosk Marketplace publication on software security for free, it does require you to register your email: http://www.kioskmarketplace.com/white_paper.php?id=69. There are also bi-annual kiosk tradeshows, called Kioskcom, that are held in NY and Las Vegas every year: http://www.kioskcom.com/.

Pilot – test with employees and end-users

Pilot a small number or a single kiosk with employees and end-users alike. The test will likely reveal changes needed to make the application more user-friendly and to better secure your kiosk. Take your time testing, the last thing you want is to rush to push out a kiosk that is not secured properly, leaving the OS, desktop and browser vulnerable.

I recommend: Never stop testing, even after the pilot is done. You can always research on Kiosk Marketplace how to continually improve your project.