KiOWARE®
kiosk system software

Call: 717-843-4790
Email: Sales@Kioware.com
Visit: www.KioWare.com

WHITE PAPER

James S. Kruper, President
Analytical Design Solutions, Inc.
KioWare Kiosk Software
July 2011

KIOWARE SECURITY FEATURES

INTRODUCTION

KioWare displays browser based content in a self-service environment. By its nature, self-service implies a public facing computer being used by an unsupervised member of the general public. As such, there are significant security issues for KioWare to handle that range from protecting the computer and underlying infrastructure to protecting innocent users of the system from malicious users.

KioWare has many features designed to target the wide range of security risks to the deployed computer.

FULL SCREEN MODE

KioWare consists of a full screen browser window that may include a toolbar at the top, bottom, right or left screen position. As such, the user never has an opportunity to interact with any GUI other than the browser based application that KioWare is displaying or the configured toolbar(s).

KIOWARE SYSTEM SHELL

The biggest security threat occurs when the malicious user gains access to the underlying operating system. KioWare works very hard on many levels to prevent this from ever happening. The most important is to run KioWare as the System Shell. By default, Windows Explorer is the System Shell which means that if somehow a malicious user were able to exit KioWare abnormally, they would have access to the normal Windows Desktop, and while it is possible to use Group Policies to lock down the Desktop, a far better solution is to run KioWare as the System Shell. With KioWare as the System Shell, any abnormal exit from KioWare deposits the malicious user to a login prompt as there is no Windows Desktop to display – as it was never loaded at PC boot time. Due to a significant reduction in overhead, KioWare as the System Shell has the added benefit of booting the PC more quickly and also increasing execution speed of your application.

SOFTWARE WATCHDOG

KioWare has a system service that's sole purpose is to assess the health of the KioWare executable. When the Watchdog determines that KioWare is not performing properly perhaps due to an application memory leak finally using too many resources, or that KioWare has exited abnormally, it will immediately restart KioWare. So in essence, even if a hacker were able to exit KioWare abnormally, they would have no time to attempt to logon to the operating system.

HARDWARE WATCHDOG

An optional PCI card can be installed to perform the role of a Hardware Watchdog that's job is to ensure the Software Watchdog is performing properly. Should it sense a problem, it will cycle power on the computer.

ACCESS CONTROL LISTS

KioWare has numerous Access Control Lists that can be used to prevent user actions that may have security implications.

Protocol ACL

Especially useful for public websites, KioWare can prevent navigation to URLs based on the protocol of the URL. This is useful to prevent users from going to unsafe URLs.

Browsing ACL

Especially useful for public websites, KioWare can prevent navigation to URLs based on the domain or individual page. Access can be limited based on a white or black list. This is useful to prevent users from going to unsafe URLs and to URLs not pertaining to the application.

Scripting ACLs

KioWare has its own library of scripting commands that are useful for custom application development, and KioWare has the ability to block KioWare Scripting commands based on the Scripting ACLs. This helps to prevent a rogue site from running KioWare commands. Some KioWare commands have significant security implications and will not function unless a Scripting ACL is defined. The Scripting ACL is configured similarly to Browsing ACL.

Input Device ACL

KioWare provides an interface layer to many peripheral input devices such as magstripe readers, barcode scanners, check readers, etc, and it is important to be able to control on which URLs the device is able to input data. The Input Device ACL is configured similarly to Browsing ACL.

USB LOCKDOWN

For deployments which have public facing USB ports, KioWare can disable the ports (Note: in Win7, this requires a Group Policy setting) and also log port usage to the Windows Event Log.

ALT-F4/CORNER EXITING

To thwart a malicious user from eventually guessing the KioWare exit passcode, there are two methods for initiating a normal exit from KioWare from which the user must enter the passcode. For deployments where there are no keyboards with function keys and no access to easily add a keyboard, KioWare can be configured to use Alt-F4 to initiate exit. Otherwise, the user is required to touch all four corners in the proper sequence to initiate exit. In the first case, the malicious user has no means of initiating exit, and in the latter the cycle time to initiate exit will prove a significant deterrent to randomly guessing the passcode.

EVENT LOGGING

KioWare makes extensive use of the Windows Event Logs, so while not technically a feature to prevent a security incident; it is a very useful feature for debugging hardware and application issues as well as provides an audit trail for security incidents. Event Logs can be uploaded to KioWare Server and used for automatic changing of a kiosk status.

PRINT DIALOG BLOCKING

A hacker will want to gain access to the file system, and the standard Windows print dialog is a perfect entry to the file system. KioWare can block embedded JavaScript print commands as well as provide a safe printing command as a replacement accessible either via a toolbar button or scripting.

MAILTO LINK BLOCKING

A user clicking on a Mailto link will cause the PC to load the default email tool which will likely provide a hacker an access point to the file system. KioWare has the ability to block all Mailto Links.

BROWSER FEATURES

KioWare can prevent file download links from functioning as well as manage popup windows – either preventing outright or limiting how many can open at a time. In addition, KioWare can prevent right mouse clicks from opening application (ex. Flash) context menus (ex. Flash) which often have security holes.

DIALOG BLOCKING

Windows is known to popup miscellaneous dialogs. This can be confusing to a self-service user, and it can also be a security risk depending on what actions the dialog allows. KioWare constantly checks for open dialogs and has a long list of known dialogs to block; however, KioWare can also be configured to block any additional dialogs a particular deployment may require.

SCHEDULED SHUTDOWN AND DISPLAY SLEEP

Sometimes an effective security measure is to simply remove the temptation. KioWare can shutdown the PC and turn off the monitor on a daily schedule.

SESSION END ACTIONS

KioWare has two primary modes of operation: User Mode when the user is interacting with the system and Attract Screen mode when there is no user. To provide security for users, KioWare completely erases any trace of the user when the user's session ends and KioWare transitions into Attract Screen mode. KioWare can clear cache, cookies and print queues. KioWare can also retract any untaken prints. In addition, a session end URL can be executed if additional custom user cleanup is required.

SECURITY DEVICES

Instead of relying on user interaction to begin a user session and an inactivity timer to end a user session, KioWare supports numerous security devices such as security mats and proximity switches which are used to control the start and end of a user session to only when the user is directly in front of the kiosk.

.NET ADDINS

KioWare is architected to enable custom .NET libraries to be integrated at runtime. This enables KioWare to be extended with a broad range of custom security functionality unique to a particular deployment.

CONCLUSION

KioWare has been battle tested since 2003 in roughly 50,000 deployments across 70 countries and in that time we have learned that providing security is a constantly evolving task, so it is important to never rest on one's laurels. Properly configured, we are confident that KioWare will provide a secure self-service experience; however, with an eye always to the future, we also work closely with a prominent kiosk security consultant who enjoys trying the latest hacking techniques on KioWare.