An Analysis of
Assigned Access Kiosk Mode
8/6/2021

Assigned Access enables a kiosk user account to only run one application – typically a browser, but it could be any application. It runs full screen and doesn't allow the user to exit the application. How well does it work for self-service kiosk deployments? How does it compare to KioWare?

Comparable to KioWare

1. Elimination of Desktop loading

Both Assigned Access and KioWare run as the User Shell which prevents the Windows Desktop from loading. This immediately eliminates security vulnerabilities associated with the Desktop.

Missing from Assigned Access

1. User Data Security
2. User Session Management
3. Application Restart – Memory Management
4. Windows Popup Dialogs Security
5. Custom Toolbars
6. Printer Security Issues
7. Browser Navigation Management – Domain/Page Allow/Block Lists
8. Full Keyboard Blocking – Virtual Keyboard Support

User Data Security

For most applications, a self-service or public access kiosk needs to clean itself of the current user's data when the user leaves. The next user should never see any of the data of the previous user. How does the kiosk know a user has left? The simplest solution is an inactivity timer, but a user presence sensor (ex, proximity switch or security mat) can also be used. KioWare supports both an inactivity timer and a user presence sensor to know when a user's session is finished and to delete all record of the user. KioWare clears the cache, user session data and the print queue.

User Session Management

It is critical for an application to reset when a user session has completed. There is nothing more confusing to the next kiosk user than to see the last page of content the previous user viewed. The application needs to reset to the Start page of the application when the previous user's session has ended.

Analytical Design Solutions, Inc.
227 W. Market St., Suite 200, York, PA 17401
http://www.kioware.com
717 843-4790 x250

Even better, the kiosk should display content attracting the next user to the kiosk. KioWare both resets the application to the Start page and also can display content to attract the next kiosk user.

Application Restart – Memory Management
There is nothing worse than a user arriving at a kiosk that is either crashed or hung. Kiosks are unlike standard computers in that they are running the same application continuously, and if that application is leaking memory, then it will eventually hang or crash. KioWare has a system service running that does nothing else but ensure the application is functional, and if it determines a performance issue, it will restart automatically. KioWare's goal is to ensure your application is always running.

Windows Popup Dialog Security
Windows has a bad habit of popping up dialog windows for a variety of reasons completely unrelated to the kiosk application. They are at minimum confusing to a kiosk user and serve as a potential security threat because the dialog window can contain links that enable the kiosk user to go places, they should not. KioWare prevents these popup dialogs from being displayed to the user.

One argument to address the security link issue is to make a Group Policy to prevent the user from doing harm. Group Policies do have issues. They are not intuitive, and it will never be clear that all security holes are plugged because the variety of Windows popup dialogs is wide. Perhaps worse is they can be inadvertently and quickly undone by a future kiosk programmer/staff member not familiar with the kiosk requirements, and no one will know there is now a security hole.

Custom Toolbars
Generally, you have two options with Assigned Access: no toolbar or the standard browser toolbar, and there is no easy way to create custom toolbars that strip down a standard toolbar to just what is necessary for a self-service kiosk. Similarly, it is hard to create custom toolbar buttons. It is also difficult to graphically modify a toolbar to work well with a touch screen or be branded to match the application content. In KioWare, you have complete graphical control over the look of custom toolbars as well as their function, including creating custom toolbar buttons.

Printer Security Issues
For security reasons, it is critical to not show the normal Windows print dialog when a user requests a print as the dialog enables access to local disk and network. Even more critically for internet content which may have embedded print buttons, the device must properly handle print button selection when the kiosk has no printer. This needs to be properly handled or else the Windows print dialog will be displayed. This can be both confusing to the user and a serious security risk. KioWare prevents the dialog from being displayed.

Browser Navigation Management
Often a kiosk provides access to a specific website or websites, and it is critical to keep the user on that specific website, or even certain selected pages of that website. In addition, certain allowed website domains/pages may have links to download files. These files can be confusing and distracting at best and serious

security issues at worst. As such, file downloading action needs to be managed. In addition, there may be links to enable the user to send an email using HTML's [MailTo] tags. Clicking this button will attempt to open an email tool which a) likely isn't installed and will error out (again confusing to the user, potential security issue) or b) if an email tool happens to be installed, then this could almost certainly cause a huge security risk. The kiosk needs to prevent [MailTo] tags from being clicked.

KioWare provides the ability to create allow or disallow lists of both domains and pages. We completely control what, if anything, can be downloaded, and we can block HTML [MailTo] tag execution.

Full Keyboard Blocking – Virtual Keyboard Support
Sometimes the kiosk deployment uses the standard computer keyboard. The standard keyboard has many key combinations that a user should not be allowed to use. In particular, the key combination of Ctrl-Alt-Del is particularly dangerous. Alt-F4 is another example.

One argument is to use Group Policies to minimize the Ctrl-Alt-Del hazard, but please refer to the Group Policies discussion under **Windows Popup Dialog Security**. Other problematic key combinations are harder to address using Group Policies. KioWare installs its own keyboard driver that makes it easy for KioWare to completely manage the key combinations you wish to block.

If a physical computer keyboard is not used, then any data entry needs to be using a popup virtual keyboard. KioWare has a built-in virtual keyboard which is secure and easy to configure. The same can not be said of 3rd party virtual keyboard solutions.

Summary
The goals of any self-service kiosk deployment need to include ensuring the kiosk application is always running, preventing the kiosk user from accessing content or resources not necessary to the user experience or is dangerous, ensuring the privacy and security of user data and having the user experience be as clear and simple as possible.

All Assigned Access does is match KioWare's elimination of the Desktop security holes. It does nothing to address the remaining security and useability issues. Assigned Access is not suitable for most self-service kiosk deployments.