Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

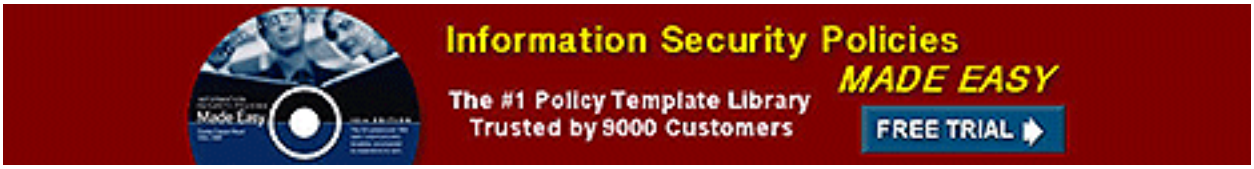
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Kiosks: The Interactive Media Solution, or is it?

With any new implementation of a media solution, come potential security risks that should be addressed prior to the implementation of this solution. The implementation and operation of kiosks is no exception. This paper addresses the topic of kiosks utilizing computers require information systems support and security to protect both the business and the customer.

Copyright SANS Institute
Author Retains Full Rights

AD



Kiosks: The Interactive Media Solution, or is it?

Lisa T. Evans

Version 1.2e

October 1, 2001

E-commerce kiosks are popping up everywhere and in different forms: interactive, information, touch screen, and Web-based. Retail stores such as Kmart (3,500 kiosks), Staples (2,500 kiosks) and Barnes & Noble have kiosks for the benefit of shoppers checking the availability of products both in-store, and products that can be shipped. Rental car agencies, such as Alamo Rent A Car, encourage customers to utilize their kiosks to rent cars on-line for faster service. Airports, too, are installing kiosks to help customers bypass long lines, while hospitals install interactive touch-screen kiosks to provide visitors with general patient information. [1]

But is this new interactive media a solution for both customers and retailers. Will it aid in customers locating products or accessing services in a more convenient, efficient manner. Or is it merely another "toy" that could lead to other technology security issues that, in the long run, will not pan out?

What is a kiosk?

A "kiosk" can be considered any vertical display unit that contains a touch screen allowing individuals to view information and possibly interact with it in some way. [2] There are several types of kiosks ranging from a simple display case to help a user locate information or products to a very complex unit such as an ATM in which an actual transaction takes place (e.g., making purchases, depositing or withdrawing money). The simplicity or complexity of a kiosk is according to the desires of the kiosk owner.

Globally, more and more businesses are considering kiosks as a means to increase sales. Some companies, such as Kmart have explored this territory as early as the 1990's. However, due to expensive network maintenance costs, and poor systems that would frequently crash, they decided to postpone this consideration until more recently. [1] Now, with the option of Web-based kiosks, this has become a popular tool. With a carefully developed kiosk display and program, businesses can replace a salesperson with a less expensive communication tool. Yes, even the most complex version may cost less than $10,000, and this would include such features as a couple of printers, a digital video camera, a fingerprint reader, a scanner and a keypad. [3]

Companies that have deployed kiosks are definitely reaping the benefits. From the time that BlueLight.com has deployed their kiosks in January, they have seen 20% of their site traffic coming through the kiosks. [1] Other retailers are hoping for similar results. "Jupiter Media Metrix, Inc. in New York predicts that consumers will purchase almost $200 million in goods and services through kiosks this year and $6.5 billion by

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

2006." (ComputerWorld, 18). This demonstrates that companies have the potential to profit from kiosks, but with these potential profits come potential problems.

Security Issues and Vulnerabilities

With any new implementation of a media solution, come potential security risks that should be addressed prior to the implementation of this solution. The implementation and operation of kiosks is no exception. When considering kiosks with a computer running behind it (as opposed to a kiosk playing a CD or video), there is a need for information systems support and security to protect the business and the customer.

One main security concern is since kiosks are in a public access environment the next user has the ability to follow the trail of a previous user. This could allow the next user to gain access to confidential files of the previous user. How is this possible? Well, take the example of Microsoft's Office 2000. Users with Microsoft Windows 2000 have the ability to install Office 2000 in public places such as an airport kiosk or an Internet café. The user connects to the company network or Web site to access Office documents and then logs off. According to the Microsoft Tips & Trick site "if the Windows registry settings that preserve the most recently used file history are enabled," the next user can come in and access the previous user's confidential files. Of course, Microsoft offers a solution for this that will preserve the customer's security. But it's also up to the customer/user to ensure that steps are taken and that controls are in place to ensure that his/her privacy, moreover, the privacy of the company, is not loss. (www.microsoft.com/office/ork/2000/journ/KioskMode.htm) [4]

With the recent terrorists attacks that occurred on September 11, airports, and possibly other retailers, need to consider the potential physical security risks that may result from kiosks. In fact, since the occurrence of the terrorist attacks, the AFA (Association of Flight Attendants) has requested that their be a ban of all remote check-in locations, including self-service kiosks since the safety guidelines administered by the FAA (Federal Aviation Administration) did not seem to be strong enough. This was of concern to the AFA since kiosks give passengers the ability to check in without being identified by airline personnel. Moreover, where airline kiosks are present, passengers can obtain boarding passes, check in luggage, and access flight information. However, AFA requested that all passengers check in at the counters and present identification to airline staff. [5]

Although some airlines have opted to discontinue kiosk operations altogether, many North American-based airlines have taken it a step further by developing a number of different strategies to integrate kiosks into the new security regulations outlined by FAA. Most airlines have decided to keep the kiosks operating. However, there are some, such as Air Canada, that have opted to shut down its kiosk system.

Some kiosk designers are planning to improve security on their kiosks. According to Robert Pratt, CEO of SMO Multimedia Corporation, "we plan to work closely with airline

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

and airport executives, federal agencies and security offices to incorporate into our kiosks any tools or technology that could be useful in deterring further terrorist attacks and providing public service announcements to passengers." [6]

It is important to note that the level of risk associated with a kiosk depends on the type of kiosk being utilized. If we categorize the kiosks into Internet, interactive, information and touch screen, the high-risk kiosks would probably be Internet and interactive since these kiosks would be connected to a server and have to access the server to retrieve, edit, and update customer requests and confidential information. Therefore, in dealing with an Internet kiosk, the kiosk owner must be aware that one of the biggest concerns a customer would have would be providing a kiosk with a credit card number. This is not something that the kiosk owner would want to view lightly. On the contrary, this should be a major consideration for the kiosk owner.

To mitigate some of these potential risks, the kiosk owner should ensure that appropriate controls are in place. Many software companies offer secure software solutions for Internet kiosks. Some of these packages have an option in which a file can be built with a list of credit card numbers that should be rejected. Moreover, some vendors such as Surf-Timer develop packages in which a company can access the Web site and download the software for installation. Packages such as these have more specialized built-in support options for kiosks that have the ability to accept credit cards as a means for identification or even as a means for payment.

Other kiosks owners such as Radio Shack have found success in other vendor packages such as those developed by Kiosk Advantage. Visible Advantage, developed by Kiosk Advantage, contains an interface with a high level of security to prevent customers from accessing corporate information, but still allowing them to check product descriptions and inventory levels at Radio Shack stores.

Security can also be beefed up on kiosks by establishing a centralized account system. First, a kiosk can be controlled by requiring customers to have a pre-established account. Then, when the user uses the kiosk, he or she is required to provide a user name and password to access the account located on the centralized account system. The benefit of this is that another layer of security is added preventing the next user from coming behind the previous user and accessing the confidential customer files without proper forms of identification.

Even better, another layer of security can be provided if the kiosk owner issues a card to the customer. At this point, extra security is provided since in addition to something the customer knows (password), and something that identifies the customer (user name) is required, something the customer owns (card) is also required to gain access to confidential customer information. This not only provides the customer with security, it also provides the kiosk owner with security of its reputation.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Taking the level of security to another level, consider the option of biometrics. Once a concept that would only be seen in a science fiction flick, biometrics is no longer something that is overlooked. In fact, there are recent indications that airport security may be improved using biometrics. Many leaders in the airport security equipment industry work closely with labs that are developing technologies like non-magnetic scanning (performs a whole body scan), retinal, voice, and fingerprint scanning. Some airlines are already using facial biometrics to check passenger identities as part of check-in procedures. [7]

Even some designers have chosen biometrics as its means for security. Mike Stinson and John Templer of Mr. Payroll Corporation developed a self-service check-cashing kiosk. Their kiosk uses biometric face-recognition technology. With this security element, their goal is to gain the customer's ultimate confidence and to deter fraud. [8]

The reason that facial biometrics is so much more secure is because a password, or card can be stolen. With the software that Stinson uses, the software forms a three dimensional image of the user based on the views taken by the cameras located at the kiosks. Moreover, during initial enrollment, a customer must provide a company representative with personal information via a phone located right next to the kiosk. The system stores up to eight images of the customer that cashes a check. Since the system has neural network technology, the computer learns a face from prior experience. Thus, the more a customer uses the kiosk, the better the system recognition of the customer cashing the check.[8]

However, there are several considerations that need to be addressed before jumping into biometrics. Specifically, with facial biometrics, a very complex and integrated database would need to be designed, one that could be shared by all airports, globally. Moreover, those that currently have deployed facial biometrics in kiosks, have to deal with the fact that the database only allows for a limited number of images. Additionally, there is the risk of identity fraud. Although the system improves as more pictures of a customer are taken, there is the possibility that the system may not recognize a person based on changes in makeup or hairstyle. Thus, the customer may not be able to perform a transaction if unrecognized by the system. And, if that is the case, under extreme circumstances the system may accept another individual that may portray to be the registered customer. [7]

Kiosk Infrastructure

For an Internet-based kiosk to work effectively, it must be connected to a high-bandwidth reliable network. Moreover, an ultra-reliable network is also a must since few customers would be unwilling to tolerate slow response times from a store kiosk when they can sit at home in front of the computer and wait at the Web site instead. Another infrastructure consideration is the presence of a robust data network. Since other store devices such as phones, cash registers, and back-office software will need to connect

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

to the main system, an excellent data network can be a significant factor in the successful operation of a kiosk. [1]

From a personnel perspective, the technical support should also be present. The technology department should constantly monitor the network in the effort to avoid system downtime. They should also be responsible for maintaining hardware and Internet connections with the stores. Moreover, store sales associates should be trained to assist customers with kiosk operation; and to handle such things as changing the printer paper and rebooting when necessary. [1]

Something that does not appear to be a topic of conversation regarding kiosks is backup and recovery procedures. This probably is not a significant topic for conversation since it is "understood" that in order to even have a Web-based kiosk, there needs to be a connection to the corporate LAN or WAN in which the data for that particular server is backed up according to the corporate policy.

However, this is not something that should be assumed or taken lightly. Just as it is important that the confidentiality of customer and corporate information is maintained, it is also important that information submitted by the customer is retained, in other words, appropriately backed up to the corporate server. The risks the kiosk owner takes in not ensuring that backup procedures are in place and practiced is a change in customer perception. This could eventually lead to a loss in customer market share since most customers would be disappointed to hear that their information was lost.

The Future

So what does the future hold for the Internet kiosks? The future looks quite promising. Kiosks that contain product information and the ability to order products are a real benefit to stores that may not be able to house as many products, but want to remain competitive.

Check-cashing is another option already mentioned. These can be much cheaper than setting up check-cashing stores and hiring employees. However, the security would have to be as complex, if not more than the face biometric security used by Mr. Payroll Corporation kiosks.

Another possibility for kiosks is kiosk Internet voting. Kiosk Internet voting entails the placement of voting machines in locations other than the traditional voting locations (i.e., schools, libraries, and malls). This would be a possibility only after poll site Internet voting (enabling users to cast votes from numerous traditional polling locations using an Internet connection) is in place. The benefit would be that votes could be counted faster and more accurately. However, the Internet Policy Institute (IPI) is encouraging caution before rushing into this option. There are still many issues and potential risks that need to be considered: technological, security, secrecy, fraud, and even sociological. [9]

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Regardless, of what the potential future uses for kiosks are, there is still work to be done in the world of "kiosk deployment" for the operation of kiosks, particularly Internet-based kiosks, to be successful. Based on demographics many customers will have to be familiar with on-line shopping and maneuverability on a computer to even consider utilizing a kiosk. Moreover, as we discussed, it is very important for the security of both the kiosk owner and the customer to be in place to ensure that there is confidentiality of information. Additionally, maintenance of the kiosk, from an infrastructure standpoint, has to be continuous for the kiosk to work properly. These are not unrealistic steps that need to be taken in order to have a functional and reliable kiosk. However, to satisfy the customer, and to be a success in the eyes of the kiosk owner, these steps cannot be overlooked.

References

[1] "Retailers, Travel Companies Deploy Thousands of Kiosks." ComputerWorld, Stacy Collett. August 6, 2001. Page 18.

[2] "kiosk." Whatis?com. URL: whatis.techtarget.com/definition/0,,sid9_gci212445,00.html

[3] "Brazilian Project Shows Internet's Promise for the Masses." Gartner, Waldir Arevolo De Azevedo Filho. January 25, 2001. URL: www3.gartner.com/DisplayDocument?id=320136&acsFlg=accessBought

[4] "Enhance Security in Public Access Environment." March 21, 2000. URL: www.microsoft.com/office/ork/2000/journ/KioskMode.htm

[5] "Flight Attendants Union Calls for Kiosk Ban." September 18, 2001 URL: www.kioskmarketplace.com/news_story.htm

[6] "SMO to Update Airport Kiosk Systems." URL: www.kioskmarketplace.com/news_story.htm?i=10751

[7] "Airport Technology to Improve in Attack Aftermath." InfoWorld, Ed Scannell and Cathleen Moore. September 14, 2001. URL: www.cnn.com/2001/TECH/ptech/09/14/airport.technology.idg/index.html

[8] "Face It." Security Works. January 1998 URL: www.securitymanagement.com/library/000467.html

[9] "Caution on Net Voting." ComputerWorld, Eric J. Sinrod. April 2, 2001. URL: www.computerworld.com/cwi/story/0,1199,NAV47_STO59077,00.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 1st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced