Kiosk Security

Peleus Uhley
Principal Security Consultant
August 1, 2006

Agenda

- Why Kiosk Security?
- Physical Security
- Network Security
- Active Directory Tools
- Application Security
- Software Solutions
- Operations Security
- Summary

Kiosk - Definition

- “a small stand-alone device providing information and services on a computer screen” – Mirriam Webster
- “Self-service” devices:
  - Airline check-in
  - Tourist information (museums, etc.)
  - Retail services enrollment, gift registries, online shopping
  - Employment applications
- Methodologies also apply to:
  - Public access terminals
  - Cash registers
  - ATMs

Example: Sample Store Connectivity

- The store's kiosks deliver multimedia from a combination of three places: the kiosk's internal drive; samples stored on a server at a company datacenter served through a T1 connection; and multimedia third party sites streaming content to the kiosk from the Internet.

Why Kiosks? – Corporate Perspective

- Everyone has them
  - Drive revenue, improve customer experience, speed checkout lines, reduce employee labor
- PCI Compliance
  - Often deployed on the same networks as cash registers so they are in scope
  - Kiosks that accept credit cards
    - For identification
    - For online purchases

Why Kiosks? – IT Perspective

- Ultimate lock down challenge for admin
  - Advanced AD settings
  - Tricky network segmentation
  - No onsite technical presence
- Redefines levels of risk with web application vulnerabilities

Why Kiosks? – Hacker's Perspective

- Advanced skill set not needed
- Potential access to the information of many users from a single point
- Attacker gets direct feedback on whether they have successfully compromised the machine.
- Public kiosks exist on private, internal networks
  - Same networks as cash registers
  - Unmonitored access to the system
- In many scenarios, it is an anonymous attack.

Physical Security Risks

- Media devices
  - CDs, USB, etc.
- Peripherals
  - Keyboard recorders
- Network jacks
  - MITM
  - Attach own device
- Theft
  - Hardware
  - Hard Drives
- Shoulder surfing
- Reboot (unplug & re-plug or power/reset switch)

Physical Security - Protections

- Custom built cases, custom keyboards
- Cabinets, locks
- Thin terminal desktop cases, diskless CPUs
- BIOS passwords
- Disable F8 during boot sequence
- Employee education. store placement
- Alarms, cameras, privacy screens
- Floor mats to key resets of the application

Physical Security - Cabinets

Physical Security – Custom Kiosks

Physical Security – Custom Kiosks

Network Security Risks

- Two attack scenarios
  - Hacker starts at the kiosk and goes into the internal network
  - Hacker starts in the internal network and owns the kiosk
- Compromise leads to:
  - Access to internal network access of physical location
  - Access to corporate internal networks
  - Access to Internet for download of tools
  - Access to the AD domain
  - Ability to generate wireless traffic to facilitate WEP cracking

Network Security Protections

- DMZ setup for kiosks
  - Egress filters for internal network access
  - Egress filters for public Internet sites
  - Ingress filters for corporate administration
  - NIDS
- Logging to centralized corporate website
- Secure wireless deployment
- Traditional desktop protections such as AV, firewalls, spyware, etc.

Host & OS Application Security Risks

- Help functionality to launch browser
- Abusing search functionality
- Using systray functionality for odd functions
- “Open With” functionality
- Local file access (temporary files, cache directory, etc.)
- Autorun

Active Directory & Group Policy

- Custom shell
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
- Microsoft Computer Access Toolkit
  - http://www.microsoft.com/windowsxp/sharedaccess/default.mspx
- Windows XP Registry Tricks
  - http://www.kellys-korner-xp.com/xp_tweaks.htm
- Windows CE Kiosk Mode
  - http://blogs.msdn.com/mikehall/archive/2005/08/03/447386.aspx

Active Directory & Group Policy

- Disable keyboard and mouse functions
- Limit file system access for application and user
  - Read-Only access if possible
- Disable application launch (software restriction policy)
- Auto-login and auto-launch during reboot
- Hide/Limit Start Menu, shortcut bars, systray
- Lock down IE (covered in depth later)
- Remove unnecessary software
- Remove permissions to install certificates

Active Directory & Group Policy (cont.)

- Login with non-privileged user in separate group
- Logging with IDS
- Disable USB, CDROM and other unused peripherals
- Locking down “Print to File”
- Disable ability to modify shortcuts
- Disable “Windows Explorer” features even if you normally don’t allow users access.

Limitations of SRP

- White list is the best solution
- Hashes can be bypassed by downloading freeware with similar functionality.
- Paths may be bypassed by loading into temp directories.
- Certificates may still allow access to such things as WMP which may allow access to File->Open

OS Keyboard Shortcuts (Partial List)

- Flying Windows + *, F1-F12, Menu Key
- Alt-Esc, Alt-Tab (task switching)
- Ctrl-Esc (start menu)
- Ctrl-Shift-Esc (Open Task Manager)
- Right click
- Num Lock + (+,-,*) – Windows Explorer
- http://support.microsoft.com/default.aspx?scid=kb;en-us;301583

Web Application Security Risks

- Many developers consider XSS attacks to be of lower importance unless they are a target of phishing attacks. With kiosk deployments, a XSS attack can lead to the compromise of a corporate asset.
- Authentication timeouts, session cache, and cookie expiration become a greater concern when the company deploys kiosks since the company now encourages shared workspace interactions.

WhiteHat Security's Black Hat Presentation

- Using "safe" JavaScript with no browser exploits, it is possible to:
  - Establish the URLs of visited web sites
  - Conduct a NMAP-esque scan for other web servers in the internal environment including those for network devices
  - Establish a frameless window to capture keystrokes
  - Control an Intranet browser from an Internet site
- No need to install code on the machine
- Evidence is wiped with the browser cache

Unplanned Functionality

- “I broke into a banking kiosk last week by accident ;-). I changed the URI on the browser by having a configured exit URI in the banking application. The bank's firewall prompted for a password and I just clicked cancel since I don't have one. It then connected me to the external location and let be browse.

  I then discovered I could ignore all the warning messages and the browser still worked. I then tried poking around on the 10.0.0.0 address space and found a link to the corporate internal home page.”

- http://www.securityfocus.com/archive/101/319780

Amazon Sign – Off Policy

If you are using a public terminal, you will want to log off, or sign out, before you leave the computer. Here's how:

1. Click the link near the top of the home page that says "If you're not (your name), click here."
2. On the next page, leave the e-mail and password spaces blank and click the Amazon.com tab at the top of the page.
3. Close the browser to prevent your name or 1-Click settings from appearing on the public terminal.

Once you have done this, your name will be removed from the home page, and your 1-Click ordering settings will be inaccessible to anyone using the same computer after you.

http://www.amazon.com/exec/obidos/tg/browse/-/515722/ref=br_bx_c_2_3/103-1847008-1815859

Internet Explorer Risks

- Cross-site scripting on primary website
- Abuse of multi-media plugins
- Printing to File
- Finding cached documents/temporary files
- Non-terminated sessions
- Running untrusted scripts or ActiveX controls
- File system access

Methods for Securing IE

- Kiosk mode
  - *iexplore.exe –k http://www.site.com*
  - No navigation buttons
  - Use frames with JavaScript navigation
  - Still have to lock down IE
- IEAK/Group policy
  - There is more flexibility
  - Contains most of the controls you need
- Wrapper Application
  - Prevents direct interaction with Internet Explorer
  - Still need to lock down Internet Explorer

Locking Down IE Controls

- Trusted sites
- ActiveX & Java controls
- Auto-complete
- Browser history
- Temp files
- Read-only or removed address bar
- Cookie settings
- Connection settings
- Script debugger
- Full screen mode
- Save passwords
- File://, ftp://, mms://,mmst://,pnm://
- File downloads
- Certificate controls
- Right-click
- Media players
- Disable SSLv2
- View source

Internet Explorer Navigation

- CTRL+B (Open the Organize Favorites dialog box)
- CTRL+E (Open the Search bar)
- CTRL+F (Start the Find utility)
- CTRL+H (Open the History bar)
- CTRL+I (Open the Favorites bar)
- CTRL+L, CTRL+0 (Open the Open dialog box)
- CTRL+N (Start another instance of the browser with the same Web address)
- CTRL+P (Open the Print dialog box)
- CTRL+S (Save the current page)
- CTRL+W (Close the current window)

Internet Explorer Keyboard Shortcuts

- Alt – F, E, V, T, H
- Alt – Space
- Alt – F4
- F1, F3, F11
- Shift + Left mouse button
- Right Click

Application Security Controls

- Reboot application after period of inactivity or shutdown
- Wiper software after period of timeout
- Forced re-authentication
- Utilize a custom application
- Run application as non-privileged user
- Conduct a web site penetration test
- Custom web site (no links to third parties, limited functionality)

Kiosk Commercial Solutions (Partial List)

- Entry level software ranges from $80-$250
- KioWare
- SiteKiosk
- Kiosk Logix
- Kiosk Information Systems

Open Source Solutions

- Open KDE Kiosk
  - Clients for Windows or Linux
  - Kiosk Admin Tool
- Kiosk
  - Custom chrome to limit functionality of the Mozilla browser
  - Still in early stages of development
- Diskless Linux install
  - Doesn’t solve every problem, but reduces the ability of an attacker to write to the disk
  - Instant Kiosk, KioskCD, BoothBox

Operations Security

- Employee education
- Regular monitoring
- Regular updates/patches
- Testing integrated into the web application SDLC
- Integrate kiosks into backup/recovery plans and incident response plans
- Conduct periodic security assessments of the kiosks

Kiosk Security Headlines

- "…planted a copy of the commercial keyboard sniffing program Invisible KeyLogger Stealth on computers at thirteen Kinko's stores sprinkled around Manhattan."
- Occurred over a period of two years
- At the time, Kinko's completely re-imaged their kiosks on a weekly basis

http://www.securityfocus.com/news/6447 - 7/18/2003

Summary

- Kiosks can be a major risk
- Lock down is a non-trivial task
- Requires security at every level
- Redefines levels of risk associated with web app vulnerabilities

Questions?

Thank You!

Peleus Uhley
peleus_uhley@symantec.com