Hacking Internet Kiosk’s

Paul Craig
Principal Security Consultant
Security-Assessment.com
Bio

Who am I?

- Paul Craig
- Principal Security Consultant.
  Security-Assessment.com, Auckland, New Zealand
- Published Security Author.
- Active Security Researcher.
- Devoted Hacker.

Comments, Feedback?

- Email: paul@ha.cked.net
- Website: http://ha.cked.net
Hacking Kiosks:

- What is an Internet Kiosk.
- Kiosk Software Security Model.
- Vulnerabilities in Kiosk Software.
- Vulnerabilities in the Kiosk Security Model.

“Hack any Windows Kiosk in less than 120 seconds!”

- Tool Release.
- Live Demo’s: Hacking (Two) Commercial Internet Kiosks.
- More 0day than you can shake a stick at.
What Is An Internet Kiosk

- Last Year I Was Sitting in an Airport…
  - 8 hour stop-over in Hong Kong.
  - Queue of people waiting to use a hub of Internet Kiosks.

- “Damn, those kiosks sure are popular…”
- “I wonder if I could hack it?.”

- Kiosks are popular, and rarely appear in security publications.
- Popularity + Poor Security Visibility = Good Attack Target

- Personal Objective:
  - Find every possible method of hacking Internet Kiosk terminals.
  - Become the King of Internet Kiosk Hacking!
What Is An Internet Kiosk

- Kiosks are everywhere
  - Airports, Train stations, Libraries, DVD Rental Stores, Corporate Building Lobbies, Convenience Stores, Post Office, Café’s, Hospitals, Motels, Hotels, Universities.
  - Cheap technology has made Internet Kiosks very common.
What Is An Internet Kiosk

Initial Observations of Kiosks

Hardware.

- Kiosks built in tough hard-shell cases.
- Fibreglass, Steel, Thick MDF.
- Lack of physical access to the underlying computer.
- Input devices inaccessible (Floppy/DVD/USB/FireWire)
- Kiosk bolted to the ground (padlocked).

- General public are not trusted.
- Kiosks are designed to prevent physical theft or malicious use.
What Is An Internet Kiosk

**Software.**

- Majority of Kiosks run commercial Windows Kiosk software.
- Linux/BSD Kiosks exist, Windows more popular.
- 44 commercial Windows Kiosk products in the market.
- Marketed as: “Turn that old PC into instant revenue!”
- Buy $59.99 Shareware -> Install -> Instant Kiosk!

**Kiosk Software Essentially Skins Windows:**

- Kiosk browsers based on standard Internet Explorer libraries.
  - WINHTTP.DLL/MSINET.OCX
- Its Windows and Internet Explorer, highly customized.
“Kiosk Software Is The Best Attack Target.”
- Hardware hacking is too obtrusive for public locations.

“I Need to Walk up to Any Internet Kiosk and Pop Shell, Quickly.”
- Explorer.exe, cmd.exe, command.com.
- Time limited, 2 minutes or faster.

16 Months of Kiosk Software Penetration Testing Later…
- Virtualized ten of the most popular Windows Kiosk platforms.
- Researched methods of compromising each Kiosk.
- Developed Kiosk Attack Methodology.

Startling Results: 100% success rate!
Kiosk Security Model
Kiosk Software Implement Security in Two Approaches.

#1 - Reduce Available Host Functionality.
- Disallow native OS functionality that can be used maliciously.
- “Command Prompt has been Disabled”
- “File Downloads Have Been Disabled”
- Implemented through native ACL’s.

#2 - Graphically Jailed Into a ‘Secure Kiosk Browser’.
- Kiosk users are stuck inside a Kiosk browser.
- Kiosk browser ran in full screen, no ability to close, minimize.
- Start Bar/Tray Menu removed or hidden.
- Only thing you can do is browse the web.
Example #1: Site Kiosk.

- Looks similar to Windows.
- Custom Tray Menu/Task Bar.
  - Only one option, ‘New Window’
  - Real Windows ‘Start’ bar is hidden from view.
- Trapped inside the Kiosk browser.
Example #2: NetStop Kiosk

- Custom task bar.
- Kiosk application ran as a full screen desktop.
- No ability to close the browser.
- Only permits internet browsing.
Kiosk Security Model

- Kiosk Browsers Proactively Monitor Your Activity.
  - Kiosks contain multiple blacklists of prohibited activity.
  - Try to do something sneaky, the Kiosk will stop you.

- Try to Browse C:\ with the Kiosk browser:

- Blacklist in-focus Modal Dialogs.
  - Block dialogs by Window Title or Window Class.
  - “Save File As”, “Open With”, “Confirm File Delete”, “Print”.
  - WM_CLOSE Window message sent to the blacklisted dialog.
  - Dialog closes.
API Hooking.

- Hook native OS API calls which can be used maliciously.
- `KillProcess()`, `GetCommandLineW()`, `AllocConsole()`
- “Unauthorized Functionality Detected, Process Killed”.

Kiosk Browser ran in ‘High Security Zone’

- File downloads disabled.
- Browser scripting, pop-ups, ActiveX, all disabled.

Watchdog Timer.

- Every 5 minutes the Kiosk will enumerate all active processes.
- Terminate any unauthorized activity.
- Custom Keyboard Driver.
  - Disable Windows shortcut key combinations.
  - Modifier Keys Unmapped.
    - CTRL, Tab, ALT, ‘Start’, Function, F1-F12.
    - Custom Keyboard with missing modifier keys!
  - Custom Mouse.
    - No right click button.
  - All Methods of reducing functionality!

<table>
<thead>
<tr>
<th>Modifier Keys Unmapped</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTRL-SHIFT-ESC (Task Mgr)</td>
</tr>
<tr>
<td>ALT-TAB (Switch Task)</td>
</tr>
<tr>
<td>CTRL-ALT-DELETE (Task Mgr)</td>
</tr>
<tr>
<td>CTRL-ESC (Start Menu)</td>
</tr>
<tr>
<td>Alt-F4 (Close Application)</td>
</tr>
</tbody>
</table>
Hacking

Kiosk Software
Hacking Kiosk Software

- Kiosk Security Model is Based on Reducing Functionality.
  - Limit functionality which can be used to escape the Kiosk browser.

- Exploiting A Kiosk Requires **Invoking Functionality**.
  - Cause applications/functionality to spawn, popup on screen.
  - Use the invoked functionality to escape the Kiosk jail.
  - Spawn a command prompt, get back to Windows.

- Kiosk Security Is Implemented Through Blacklists.
  - Blacklists (by nature) are never 100%.
  - We only need one method of escaping the software jail.
Lets Say You Find a Kiosk in Your Local Mall.
- ‘10RM for 1 hour of internet usage’
- Insert money.

You Find You are Trapped Inside a Kiosk Browser.
- Only one visible button to ‘Start Browsing’
- Start Browsing...
Hacking Kiosk Software

- Browse The Local File System Using The Kiosk Browser.
  - Local Windows users are capable of browsing the file-system.
  - Kiosk software must explicitly block local browsing attempts.

- Windows Is Designed For Idiots.
  - Caters for mistypes/fat-fingers.
  - C:\windows\ maybe blocked.

<table>
<thead>
<tr>
<th>File:/C:/windows</th>
<th>File:/C:\windows\</th>
<th>File:/C:\windows/</th>
<th>File:/C:/windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>File://C:/windows</td>
<td>File://C:\windows/</td>
<td>file://C:\windows</td>
<td>C:/windows</td>
</tr>
<tr>
<td>C:\windows\</td>
<td>C:\windows\</td>
<td>C:/windows/</td>
<td>C:/windows\</td>
</tr>
<tr>
<td>%WINDIR%</td>
<td>%TMP%</td>
<td>%TEMP%</td>
<td>%SYSTEMDRIVE%</td>
</tr>
<tr>
<td>%SYSTEMROOT%</td>
<td>%APPDATA%</td>
<td>%HOMEDRIVE%</td>
<td>%HOMESHARE%</td>
</tr>
</tbody>
</table>

- Blacklists start failing about now.
Using Common Dialogs To Hack Kiosks.

- Windows contains ‘Common Dialogs’ libraries.
- Saving a file, opening a file, selecting font, choosing a colour.
- COMDLG32.DLL (Common Windows Dialogs Library).
- COMDLG32.DLL Implements Common Windows Controls.
  - From COMCTL32.DLL (Common Windows Controls Library)

File/Open, File/Save Dialog’s Contain ‘File View’ Controls.

- File view control provides full Explorer functionality.
- Same control that Windows Explorer uses.
- File-Open Dialog = Explorer
- Can be used to launch processes.
Systematically Click Every Button, Graphic, Icon In The Kiosk

- Can we invoke a File - Open Dialog? “Attach File”
- Browse the file system
- Right Click cmd.exe: Open / Run As
- Spawn cmd.exe

File View Control
• Internet Explorer ‘Image Toolbar’.
  • Toolbar hovers top-left of a large image when clicked.
  • Each icon of this toolbar can invoke a Common Dialog.
    ▪ File/Save.
    ▪ File/Print.
    ▪ File/Mailto.
    ▪ Open “My Pictures” in Explorer.
• Toolbar is present if the Kiosk uses Internet Explorer libraries.
• Click a large image on screen
  ▪ Spawn a Common Dialog, spawn Explorer.
Using the Keyboard.

- Keyboard shortcuts can be used to access the host OS.
- Check if a custom keyboard driver present?
- Are modifier keys enabled?

Keyboard Combinations Which Produce Common Dialogs.

<table>
<thead>
<tr>
<th>Keyboard Combination</th>
<th>Dialog Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTRL-B, CTRL-I</td>
<td>(Favourites)</td>
</tr>
<tr>
<td>CTRL-H</td>
<td>(History)</td>
</tr>
<tr>
<td>CTRL-L, CTL-0</td>
<td>(File/Open Dialog)</td>
</tr>
<tr>
<td>CTRL-P</td>
<td>(Print Dialog)</td>
</tr>
<tr>
<td>CTRL-S</td>
<td>(Save As)</td>
</tr>
</tbody>
</table>

Kiosk Specific ‘Administrative’ shortcuts.

- All Kiosk products contain a hidden Administrative menu.
- Mash the keyboard, CTRL-ALT-F8? CTRL-ESC-F9?
Browser Security Zones

- Browser security model incorporates multiple security zones:
  
  - Restricted Sites
  - Internet Zone
  - Intranet Zone
  - Trusted Sites

Each security zone adheres to a different security policy.

- Internet zone has less ability to interact with a host.
- Trusted Sites, Intranet Zone typically have more access.
Local Users Can Access All Available Security Zones.

- URL’s must be directly typed into the URL entry bar.

Security Zone Escalation. about: pluggable-protocol handler.

- About handler belongs to the ‘Trusted Sites’ security zone.
- Suffers from a Cross Site Scripting vulnerability.
- Local users can render arbitrary content within a trusted zone.
- Spawn a File Open Common Dialog from a trusted security zone.

```
about:<input type=file>
about:<a href=C:\windows>Click-Here</a>
```

- Internet zone cannot follow links to the file system.
- Trusted sites can.
Shell Protocol Handler.

- Shell handler provides access to Windows web folders.

Type Into the URI Bar:

- Shell:Profile
- Shell:ProgramFiles
- Shell:System
- Shell:ControlPanelFolder
- Shell:Windows

Each URL will spawn explorer.exe and browse the web folder.

Is the shell: handler blocked by the Kiosk?
How About This:

- `shell:::{21EC2020-3AEA-1069-A2DD-08002B30309D}`
- Invoke the Windows Control Panel by ClassID.
- Works from common Internet Explorer libraries.
- Bypass native ACL’s that may exist on control.exe
The Downside to Physical Input Vectors.

- Kiosk software is designed to not trust the guy on the keyboard.
- **Kiosk User = Most Obvious Security Threat.**
- My research concluded that physical inputs are not so successful.
  - 40-50% chance of popping shell.
  - Many techniques are already published, unoriginal.

A Subtle Discovery…

- Remote websites **not** factored into the Kiosk security model.
- Websites are trusted **MORE** than a local Kiosk user!

- Kiosks rely on the default web browser security model.
“I Need a Kiosk Hacking Website.”

- An online tool you can visit from an Internet Kiosk terminal.
- Provide all the content you will ever need to escape a Kiosk jail.

iKAT - Interactive Kiosk Attack Tool.

- First of its kind! New method of hacking Internet Kiosks!
- Fast! iKAT can pop shell in less than 30 seconds.
- 95-100% success rate!

- [http://ikat.ha.cked.net](http://ikat.ha.cked.net)
What Can iKAT Do?

Kiosk Reconnaissance: Detect Installed Applications

- JavaScript & res:// (resource) protocol handler.
- Extract bitmap resources from PE executables.
- Verify bitmap presence and detect installed applications.
- Detects all common commercial Kiosk platforms.
- Enumerates locally installed applications.

```javascript
var disk;
disk = 'C:\\';
var test = new Image();
test.src = 'res://C:\\' + fileurl;
if (test.height != 30) {
    return true;
}
```
- Display Local Browser Variables.
  - Determine underlying Kiosk browser technology.
  - MSI.NET.OCX, WINHTTP.DLL display Internet Explorer appVersion
  - Detect the presence of .NET CLR.

- Display Remote Server Variables
  - Discover remote IP address of the Kiosk terminal.
- All Common Browser Dialogs In One Place

- File Open, Save As, Print, Print Preview:
- Click down the list and determine what dialogs are blocked.
- Use the File View control within the dialogs.
Use Flash To Invoke Common Dialogs.

- Adobe Flash is the most widely used browser plug-in.
- ActionScript 3 can invoke three unique File View dialogs.
  - ‘Select File For Upload’
  - ‘Select File(s) For Upload’
  - ‘Select location for Download by iKat.ha.cked.net’

Flash Common Dialogs have Unique Dialog Titles

- Not standard “Choose File”
- Bypass dialog Window title blacklists.
- Still contains the File View control.
- Blacklists fail (again).
Spawning Applications On The Kiosk.

- Can we cause an application/process to spawn on the Kiosk.
- Does the spawned application contains a common dialog?
- Use the application to gain additional access to the Kiosk.

iKAT Invokes Default Windows URI Handlers.

- URI handler applications are spawned for each URI.
- Callto://, Gopher://, HCP://, Telnet://, TN3270://, Rlogin://, LDAP://, News://, Mailto://

**One Click Automation**: One click spawns all default handlers.

3rd party URI Handlers

- MMS://, SKYPE://, SIP://, Play://, Steam://, Quicktime://
Example: HCP://: Help And Support Center

- `<a href=HCP://dummy> Click-me </a>`
- Search HCP for what you want to launch “Command Prompt”
- “Using Command Prompt” provides link to spawn cmd.exe
- Left Click Only!
- iKAT Provides Links to Over 100 URI Handlers.
  - Click, click, click down the list.
  - Determine which handlers are covered by the Kiosk blacklist.
  - Use invoked handler application to escape the Kiosk.

- iKAT Contains Local Security Zone Handlers
  - about:, res:, shell:
  - Lists of URL’s to type in.
  - Remembering ClassID’s is hard.
Invoke Applications Using File Type Handlers.

- Click on test.myfile, Windows will spawn the ‘myfile’ handler.
- iKAT uses DHTML/JavaScript to invoke 108 unique file handlers.

Internet Explorer supports prompt-less handler execution.

- Example: Click test.wmv, Windows Media Player Spawns.
- No Prompt “Are you sure you want to…”.

Kiosk blacklists monitor in focus dialogs for warning prompts.
iKAT & Windows Media Files.

- WMPlayer will silently launch for multiple file types.
- Windows Media Playlist Files (.ASX)
- Supports ‘Web Enhanced Content’.
- Turn Windows Media Player into a web browser!
- Provides a browser without any Kiosk security controls.
iKAT & Office Documents.

- If an Office file viewer is installed on the Kiosk, we win.
- Embed a copy of cmd.exe within an office document.
- Supported by .DOC, .DOCX, .XLS, .XLSB, .XLSM, .XLSX
- ‘Open Package Contents’ dialog not detected by any Kiosk.

iKAT will spawn the most useful file possible.
iKAT & Java Applets:

- Signed Java applets can execute local processes.
- Detect if JRE is installed (iKAT Kiosk Reconnaissance).
- Does the Kiosk detect the Java security warning prompt?
  - “Warning – Security”
  - 0% of tested Kiosks did.

iKAT Contains Signed Kiosk Specific Java Applets.

- Signed applets to spawn command shells.
- Includes Jython by GNUCITIZEN.
- Install a Malicious ActiveX
  - Safe for scripting ActiveX’s can be used to compromise a Kiosk.
  - Unsafe method: object.execute(‘cmd.exe’);
  - Can we install a malicious ActiveX on the Kiosk?

- iKAT ActiveX
  - Safe-for-scripting ActiveX which executes arbitrary executables.
  - Installing an ActiveX requires administrative authority.
  - iKAT ActiveX gives you the ability to spawn a shell.

- ActiveX is changing:
  - IE8 will not require admin rights for installing a new ActiveX.
Hackin
kiosk software

iKAT & ClickOnce Applications

- ClickOnce is .NET 2.0+ technology (.NET CLR 2+ required)
- ‘Online Application Deployment’ .application file handler.
- Unsigned ClickOnce applications execute with full trust!
- Admin privileges are not required!

Users are warned:

- All tested Kiosks fail to detect this warning message!
- Modern Kiosks now developed in .NET (CLR is present!)
The most useful ClickOnce applications for Kiosk Hacking?

- **Embedded Web Browser.**
  - HTTP browser with reduced security settings.

- **Application Executor.**
  - Spawn arbitrary executables.

- **Access Token Pincher.**
  - Access token hijacking is a hip subject, why not!
  - Does the Kiosk user have the SeImpersonate privilege?
  - Impersonate available (privileged) tokens.
  - Spawn cmd.exe under the context of the privileged token.
  - System shell, I win.
Who Here Has Ever Crashed a Web Browser?

- What about crashing a Kiosk: ‘Emo-Kiosking’
- Create an unhandled exception in a Kiosk browser.
- Kiosk browser crashes, We get the desktop, We Win!
- Rare situation: Application crash = highly critical vulnerability.

iKAT Contains Common Browser Crash Techniques.

- Published exploits which results in a crash.
- Fastest, easiest method of escaping a Kiosk.
- Fairly reliable, 40%-50% of tested Kiosks crash.
- Kiosks crash, or reboot.
Crashing Browser Plug-ins.

“Can I create a .SWF file that can reliably crash a browser?”

- Sequential byte file format fuzzing of the .SWF format.
- Found multiple unhandled exception situations.
- Integer Divide By Zero.
- Immediately un-exploitahle, reliably crash any browser.

Created ‘iKAT Auto Magic Flash Crasher’.

Is the Flash Plug-in Installed on The Kiosk?

- iKAT can crash it, guaranteed, oh-day magic.
- Adobe have resolved this issue in Flash Player 10 RC.
• Lets Assume Something Worked.
  • You have access to the Kiosk File system.
  • Command shell spawned, Common Dialog, Java installed, etc

• What Now?
  • Download additional tools/binaries.

• How Do You Download Files In a Tool-less Environment.
  • Kiosk terminal will not have a copy of wget.exe present.
  • Internet Explorer is likely uninstalled or disabled.
  • File downloads disabled.
Old School: Downloading Files In Windows:

Using Common Dialogs
- ‘Attach’ a remote file from a File-Open dialog.
- FPSE/WebDAV to save the file locally, and attach it.

Works From Any File->Open Dialog.
- File saved in a writeable location.
- Temporary internet files.
- Downloads any file type/size.
Use Flash To Download Files.

- Most Kiosk’s disable File Downloads with browser security policy.
- IE: Tools -> Internet Options -> Custom Level
  - Flash can be used to circumvent the browser policy.
    - Download method of the FileReference() object.
  - Flash does not validate browser security policy.
  - Very high success rate against Kiosks.
  - Another unpublished oh-day trick.
- Notepad Can Download and Upload Files.
  - File-> Open
    - http://test.com/trojan.txt
    - Content must be 7bit safe.
  - File-> Save
    - Upload content to a remote site.
    - FPSE/WebDav
    - http://www.ok.com/blah.txt
  - Quickly upload files from a Kiosk.
#1 Problem: Kiosk Hacking is a Tool less Environment

- “iKAT needs to provide tools for Kiosk hacking”.

Assorted Kiosk Hacking Tools:

- Tools available as
  - .exe, .zip, Flash Download, 7bit Safe VBScript (.VBS/.VBE)!
Command Shell Detours:

- How many ways to spawn a command shell on Windows?

<table>
<thead>
<tr>
<th>cmd.exe</th>
<th>command.com</th>
<th>win.com cmd.exe</th>
<th>win.com command.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loadfix.com start.exe</td>
<td>sc create testsvc binpath=&quot;cmd /K start&quot; type= own type= interact</td>
<td>loadfix.com cmd.exe</td>
<td>loadfix.com command.com</td>
</tr>
<tr>
<td>start loadfix.com cmd.exe</td>
<td>start loadfix.com command.com</td>
<td>start loadfix.com cmd.exe</td>
<td>%COMSPEC%</td>
</tr>
</tbody>
</table>

- Win.com? Loadfix.com? Start? Combinations of both?
- Kiosk ACL’s typically block cmd.exe from spawning.
  - What about command.com, win.com?
- CMD Detours attempts 17 methods of invoking a shell.
- Flawless at bypassing Kiosk ACL’s.
iKAT Reloaded

- Officially Released at Defcon 16 Las Vegas.
  - Amazing success!
  - iKAT can pop shell on ANY Vegas Kiosk < 10 seconds

- Who’s Been Using iKAT?
  - 14,000+ unique hits, 10-15% of requests from Kiosks!
    - reception.sitekiosk.com, comm775-kiosknet-dhcp8.bu.edu & comm685-kiosknet-dhcp74.bu.edu
    - 12-46-54-181.seatac.seattwa.wayport.net, Aoc.ppx-bc2.hqda-aoc.army.pentagon.mil
    - Security-lab1.juniper.net, Lan-116.181.coresecurity.com
    - Ustdc1.deloitte.com, Deloitteservices.deloitte.nl, Dh212.public.mod.uk

- iKAT Portable Now Available!
  - Entire iKAT website in a zip file
  - Useful for offsite penetration testers.
Hacking Kiosks: The Demo’s

- Two virtualized (commercial) Kiosk products.
- Recommended Kiosk application configuration.
- Default Windows XP install.

- Using iKAT To Pop a Command shell
  - As Fast As Possible!
Questions?

Email me:

paul@ha.cked.net

paul.craig@security-assessment.com