O MAIOR EVENTO DE HACKING, SEGURANÇA E TECNOLOGIA ~~DO BRASIL~~ DO CONTINENTE

Rage Against the Kiosks

Tiago Ferreira

INTRODUCTION

$ whoami

- Co-founder and security engineer at Blaze Information Security.
- Been around in the security community and industry for 10 years now
- I’ve worked in security companies in Brazil and abroad
- I do security research (exploitation techniques, tools and hacking stuff)
- I am a drummer \m/
- I used to have a cool moustache!

PRESENTATION ROADMAP

$ cat agenda.txt

- A brief overview of kiosk systems and restricted environments
- Understanding the security model of kiosks
- Breaking out of environment restrictions
- Real life kiosk hacking

A BRIEF OVERVIEW OF KIOSK SYSTEMS

KIOSKS

In many cases they sit in public areas but are largely unattended for long periods of time

KIOSKS

Kiosks are popular in airports, waiting areas, hotel lobbies and museums, to name a few.

KIOSKS

Use cases include browsing the web, sending e-mails, printing photos or used to query for information

KIOSKS

Depending on the use case it may be connected to the internal or corporate network

UNDERSTANDING THE SECURITY MODEL OF KIOSKS

Hardware

- In general it is inside a physically fortified box
- Restricts external devices by blocking USB ports (depending on the use case)
- Sometimes it has its own keyboard without special keys like AltGr, Fn, etc.

Software

- Tries to limit a feature-rich environment like an OS into a restricted subset of functionality

- Most restrictions are imposed on user interface

For example: non-existent Start menu, apps execute in full screen with no possibility to minimize, watchdog monitors certain APIs to close modal boxes, disallow right click, etc.

Browser-based

- Many kiosk software monitors the URLs entered into the browser: blacklist approach
- Also, many restrict the users to a certain set of sites (sometimes search engines are allowed)
- Installation of plugins and extensions are forbidden
- File downloads are usually restricted, too

BREAKING OUT OF ENVIROMENT RESTRICTIONS

Break-out overview

- Kiosks and restricted environments are usually not well configured enough, numerous ways to circumvent its security
- Successful exploitation results in effective violations of security boundaries

Break-out overview

- Even if only horizontal privilege escalation (not obtaining admin-level), from restricted to ability to interact with OS and filesystem is a huge step towards full compromise
- Automated tools like iKAT work very well, but newer kiosks patched many of the,vulnerabilities

Rule of thumb

EVEN THE SIMPLEST APPLICATION CAN HAVE FEATURES THAT CAN BE ABUSED TO ESCAPE THE RESTRICTIONS IMPOSED BY THE KIOSK SOFTWARE

High level methodology

- Invoking functionality that can be useful to escape restrictions
- Obtain a dialog box (e.g., Save As, Printer, Open, Tools/Configuration)
- From dialog boxes we can find other intended functionality to abuse and achieve our goal
- Play around with keyboard shortcuts such as CTRL+P, Windows+R (execute), Windows+S (save), etc.

High level methodology

- Map all 3rd party apps that can be called from the browser (Office, PDF readers, etc.)
- Office (MS Word, Excel) contain not only interesting menus but also have the ability to execute documents with active content like macros
- Try downloading files from the browser and see how it goes

High level methodology

- Try to install a browser extension/plugin – a malicious extensions can give you access to the underlying OS.
- Unusual file paths are useful to bypass black-lists used in monitoring watchdogs.
- Protocol handlers like file://, telnet://, ldap://, are your friend.

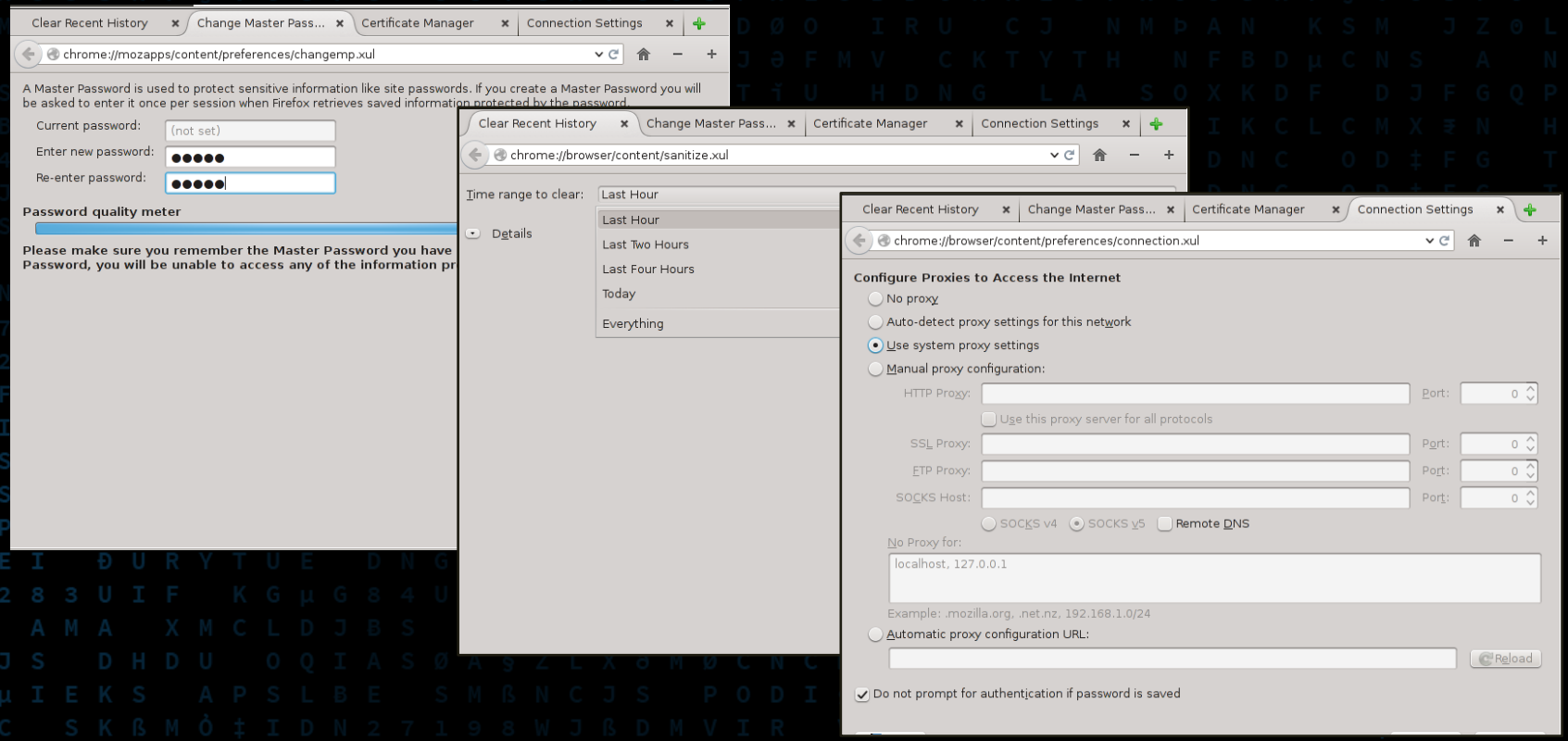
High level methodology

File:/C:/windows	File:/C:\windows\	File:/C:\windows/	File:/C:/windows
File://C:/windows	File://C:\windows/	file://C:\windows	C:/windows
C:\windows\	C:\windows	C:/windows/	C:/windows\
%WINDIR%	%TMP%	%TEMP%	%SYSTEMDRIVE%
%SYSTEMROOT%	%APPDATA%	%HOMEDRIVE%	%HOMESHARE%

High level methodology

- Browser-specific chrome:// URLs are your friend too.
  - Downloads chrome://mozapps/content/downloads/downloads.xul
  - Clear history chrome://browser/content/sanitize.xul
  - Cookies chrome://browser/content/preferences/cookies.xul
  - Connection Settings - chrome://browser/content/preferences/connection.xul
  - Saved Passwords chrome://passwordmgr/content/passwordManager.xul

High level methodology



High level methodology

- Crash the kiosk software and good bye to the monitoring watchdog
- Crash the browser with a client-side exploit and chances are you’ll have access to the desktop

REAL LIFE KIOSK HACKING

Threat Modeling

- Identify potential attack surface
  - Keyboard (physical, virtual)
  - USB device
  - Network Interface Card
  - Browser resources (extension, internals)
  - User input (fuzzing, payloads)

Porteus Kiosk

- It is possible to choose Firefox or Google Chrome
- Pretty well locked down against most attacks
- However, restriction to chrome:// URLs are not properly enforced
- It can be abused by client side attacks

InstantWeb Kiosk

Instant WebKiosk/UB is a **fully customizable** operating system for Internet browsing purposes, which **protects privacy**: users can modify its settings runtime but after a reset the operating system defaults to original values and users' informations are completely destroyed. Closing browser window also resets system – in a less secure but quicker manner. It is hacker proof and completely immune to viruses and malware

Only **persistent settings** are always preserved: network, localization, video, sound and printer configurations persist across reboots. Browser state (custom settings, extension, bookmarks, history and so on) can also be optionally saved by the admin.

Instant WebKiosk/UB makes use of Google Chromium as Internet browser and it features **PDF, images and video** viewing, **office files** and **compressed files** support; it features full "i18n" (**internationalization**) including CJ input methods.

It supports **printing** (plug&print for most common USB printers – network printers need to be manually set) and both **wired** (with DHCP / static) **and wireless networks** (DHCP) in order to access the Internet. System parameters are set by an **user-friendly web interface**. Adobe Flash support has been dropped by latest Chromium version, and HTML5 videos are now used instead.

See download page for free download.

InstantWeb Kiosk

- Based on Chromium
- Claims to be hacker-safe and malware-proof. So let’s debunk the claim.
- Unrestricted access to file:// making filesystem browsing easy
- Allows removal and installation of arbitrary Chrome extensions

Netkiosk

- Based on Internet Explorer
- Unrestricted file access manipulating URI scheme
- It is easy to crash the main process (URI fuzzing)

References

- http://developer.mozilla.org (The chrome URL)
- Paul Craig - Hacking Internet Kiosk’s (Defcon)
- IKAT Tool

Obrigado!

tiago@blazeinfosec.com
http://br.linkedin.com/in/tiagoferreirasecurity

ROADSEC

#dontstophacking