The Inherent Insecurity of Widgets and Gadgets

Aviv Raff
Iftach Ian Amit
Who are we?

- Aviv Raff
  - Security researcher at Finjan’s MCRC
- Iftach Ian Amit
  - Director of security research at Finjan
Introduction - Widgets?

• What is a widget?
  • Widgets are small applications
  • Provide visual information
  • Provide access to a frequently used functions
  • Hosted in an environment called a “Widget Engine”
Introduction - Types of widgets

- Website widgets
- 3\textsuperscript{rd} party application widgets
- OS integrated widgets
General Issues - Malicious Widgets

- Widgets are applications
- Applications can include malicious code
- Hence, widgets can be malicious
General Issues - Vulnerabilities

• Widgets are small applications

• Often considered too simple to represent a security threat

• Widgets are developed without security in mind

• Hence, widgets probably have security vulnerabilities
General Issues - Attack vectors

• Downloadable malicious widgets

• Email attachments

• Vulnerable widgets
  • Command injection
  • Man in the middle attacks
  • Browser vulnerabilities

• Vulnerable websites
  • XSS
  • CSRF
General Issues - Impact

- Session/Account hijacking
- Remote denial-of-service
- Information leakage
  - Personal
  - Corporate
- Remote code execution
  - Exploiting browser vulnerabilities
  - Download and execute
Web widgets - In the Wild

- Personalized Portals
  - iGoogle
  - Microsoft Live
  - MyYahoo

- Blog systems
  - WordPress
  - TypePad

- Social networks
  - MySpace
Web widgets - iGoogle

- Personalized Portal
- Requires a Google Account
- Based on HTML and javascript
- JS API for widget developers
- Mobile support
Web widgets - iGoogle - Malicious Widget

• Demo
Web widgets – Vulnerable Widget

- Demo
Widget Engines - 3rd party applications

- Yahoo widgets (Konfabulator)
- Google Desktop
- DesktopX
- Opera browser
Widget Engines - Yahoo Widgets

• Previously known as Konfabulator

• Recently released version 4.0

• Based on HTML like Markup Language and javascript

• Some of the widgets require Yahoo account

• Multiplatform API
Widget Engines - Yahoo Malicious Widget

• Demo
Widget Engines - Yahoo Vulnerable Widget

- Demo
OS Widgets - Out-of-The-Box Engines

- Apple OSX
  - Dashboard

- Windows Vista
  - Sidebar

- Linux
  - KDE / GNOME
OS Widgets - Vista Sidebar

- Installed by default on all Windows Vista editions
- Allows installation of external widgets
- Uses Internet Explorer 7.0 for rendering
- **DOES NOT** utilize IE7 Protected Mode!
- JS API for widget developers
OS Widgets - Vista Sidebar Malicious Widget

- Demo
OS Widgets - Vista Sidebar Vulnerable Widget

- Demo
Widgets on Mobile Devices

• iGoogle and Live.com provide mobile interface

• Different widgets display from the PC version

• Only some of the widgets are allowed to be added

• Attack vectors:
  • Session/Account hijacking
  • Exploit mobile browsers vulnerabilities
Widgets and Browser Extensions

• Actually not a lot different

• Browser integration vs. OS/Engine/Site integration

• Firefox browser extensions
  • Run in elevated privileges (Chrome)
  • Firebug

• Internet Explorer ActiveX
  • BHO
  • OS ActiveX
Solutions / Recommendations

• Digital Signing for Widgets

• Trust no one
  • Do not install unofficial/unknown widgets

• If you don’t use, block it!
  • Block .widget and .gadget files

• Use Widget 1.0 implemented solutions
Solutions / Recommendations - Widgets 1.0

- W3C standard for widgets development
  - Last draft version from November 2006
  - [http://www.w3.org/TR/widgets/](http://www.w3.org/TR/widgets/)

- Object model based on Apple’s Dashboard

- Implemented in Opera browser widgets

- Strict security model:
  - No access to user’s file system
  - Explicit declarations of protocol usage
  - Explicit declarations of port usage
  - Intranet IP range restrictions
Questions