finjan
Vital Security™

The Inherent Insecurity of Widgets and Gadgets

Aviv Raff

Iftach Ian Amit

Who are we?

finjan
Vital Security™
securing your web

- Aviv Raff
  - Security researcher at Finjan's MCRC
- Iftach Ian Amit
  - Director of security research at Finjan

Introduction - Widgets?

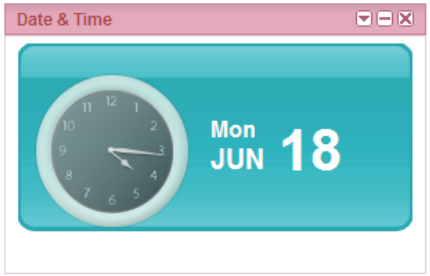
finjan
Vital Security™
securing your web

- 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

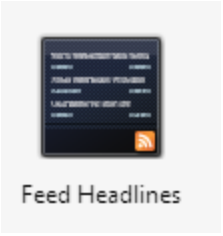
finjan Vital Security™
securing your web

- Website widgets



- 3rd party application widgets

- OS integrated widgets



General Issues - Malicious Widgets

finjan
Vital Security™
securing your web

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

General Issues - Vulnerabilities

finjan
Vital Security™
securing your web

- 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

finjan Vital Security™ securing your web

- Downloadable malicious widgets
- Email attachments
- Vulnerable widgets
  - Command injection
  - Man in the middle attacks
  - Browser vulnerabilities
- Vulnerable websites
  - XSS
  - CSRF

General Issues - Impact

finjan Vital Security™
securing your web

- 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

finjan Vital Security™
securing your web

- Personalized Portals
  - iGoogle
  - Microsoft Live
  - MyYahoo
- Blog systems
  - WordPress
  - TypePad
- Social networks
  - MySpace

Web widgets - iGoogle

finjan
Vital Security™
securing your web

- Personalized Portal
- Requires a Google Account
- Based on HTML and javascript
- JS API for widget developers
- Mobile support

Web widgets - iGoogle - Malicious Widget

finjan
Vital Security™
securing your web

- Demo

Web widgets – Vulnerable Widget

finjan
Vital Security™
securing your web

- Demo

Widget Engines - 3rd party applications

finjan Vital Security™
securing your web

- Yahoo widgets (Konfabulator)
- Google Desktop
- DesktopX
- Opera browser

Widget Engines - Yahoo Widgets

finjan
Vital Security
securing your web

- 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

finjan
Vital Security
securing your web

- Demo

Widget Engines - Yahoo Vulnerable Widget

finjan
Vital Security™
securing your web

- Demo

OS Widgets - Out-of-The-Box Engines

finjan Vital Security™
securing your web

- Apple OSX
  - Dashboard
- Windows Vista
  - Sidebar
- Linux
  - KDE / GNOME

OS Widgets - Vista Sidebar

finjan Vital Security™
securing your web

- 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

finjan
Vital Security™
securing your web

- Demo

OS Widgets - Vista Sidebar Vulnerable Widget

finjan
Vital Security
securing your web

- Demo

Widgets on Mobile Devices

finjan Vital Security™ securing your web

- 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

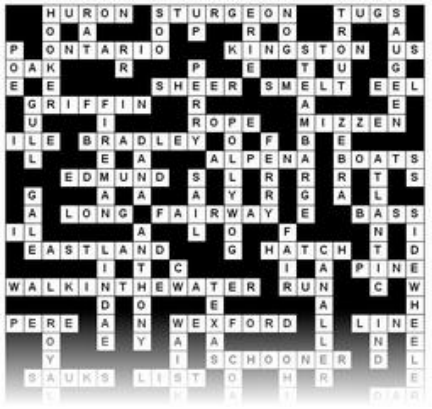
finjan Vital Security™
securing your web

- 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

finjan
Vital Security™
securing your web

- 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

finjan Vital Security™
securing your web

- W3C standard for widgets development
  - Last draft version from November 2006
  - 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

finjan
Vital Security™
securing your web