Silverlight Security

OWASP talk, 24. feb 2009

René Løhde, Microsoft
renel@microsoft.com
Agenda

- Silverlight introduction
- Transparency and Fx security
- Connectedness
- Users
Agenda

- Silverlight introduction
  - Transparency and Fx security
  - Connectedness
  - Users
From .Net to Silverlight

- Windows Communication Foundation
- Workflow Foundation
- ... (omitted)
- Windows Presentation Foundation
- Silverlight
WPF is XAML and Code

And

Silverlight is XAML and Code
Managed Code (C#/VB)

HTML
Demo

Hello Silverlight!
Architecture

Code

Controls

Managed Interop

Platform Invoke

CLR

Prop-Sys

Layout

Text

Media

Gfx

Deep Zoom

Image
More famous Silverlight Apps

NBC Olympics (Media streaming)
Blockbuster

Hardrock (Deepzoom)

...see http://silverlight.tenteo.com/
Agenda

- Silverlight introduction
- Transparency and Fx security
  - Connectedness
  - Users
Transparency

1. Transparent
2. SafeCritical
3. Critical

User code (transparent) wants to write a file

System.IO.IsolatedStorageFile
StreamWriter
(SafeCritical code)
verifies the request and calls
Windows API

WINAPI
CreateFile
(Critical code)
creates file without
any validation
Attribute

Agenda

- Silverlight introduction
- Transparency and Fx security
- **Connectedness**
- Users
On first call to **MyBank.com:**
http://MyBank.com/clientaccesspolicy.xml
Does not exist:
SecurityException will be thrown

On first call to **Weather.com:**
http://weather.com/clientaccesspolicy.xml
Exists:
Silverlight will let the call go through (if policy allows)
Cross-Domain Policy Files

- Silverlight looks for two policy files:
  - Silverlight policy: clientaccesspolicy.xml
  - Adobe Flash policy: crossdomain.xml
  - Already used by etc...

- All public services that work with Flash – will also work with Silverlight
What do the Restrictions Really Mean?

- Cross-Domain and HTTP restrictions:
  Some services not accessible from rich browser apps (both Flash and Silverlight)

- Change must come from:
  - Browser APIs - IE, NPAPI (Safari & FireFox)
  - Service Owners
    e.g. Google allows `X-Http-Verb-Override:DELETE` inst. of `HTTP DELETE`

- Can use a proxy:
Cross Domain model

```xml
<?xml version="1.0" ?>
<cross-domain-policy>
  <allow-access-from domain="A" secure="false" />
</cross-domain-policy>
```
Making HTTP Requests

- **WebClient**
  - Simple to use
  - Limited functionality

- **HttpWebRequest**
  - Access to all features

- *Future possibility:*
  *Usability Improvements to HTTP client*
  - *Serializer integration, URI templates, etc.*
  - *Available as a sample*
    - [http://code.msdn.microsoft.com/SilverlightWS](http://code.msdn.microsoft.com/SilverlightWS)
HTTP Requests in Silverlight

High-level components and User Code

HttpWebRequest

Browser Plugin APIs

Web Browser
- Cookies
- Authenticated sessions
- Caching
- Proxy server to use

Windows/Mac Networking Layer

Restrictions

Restrictions
Connectedness Summary

• **Creating** Services for Silverlight
  • Creating and consuming WCF services
  • Securing local services
  • Creating public services (safe for cross-domain)

• Accessing Services that **Describe** Themselves
  • “Add Service Reference”

• Accessing Services that **Don’t Describe** Themselves
  • WebClient / HttpWebRequest, manual work

• Accessing **Feeds**
  • RSS/Atom
Agenda

• Silverlight introduction
• Transparency and Fx security
• Connectedness

• Users
Securing Silverlight Services

- Silverlight will use auth. information in the browser

E.g.: ASP.NET login

User: 
Password: 

YourDomain.com

Credentials

Auth info (e.g. cookie)

Service calls + Auth info

Silverlight code does not normally deal with credentials (user, password)
Securing Silverlight Services

• Silverlight will use auth. information in the browser
• This is exactly what you want!
  • Login once for web page + Silverlight

• To get user identity in WCF Services:
  • Turn ASP.NET Compat Mode on *(template will do this for you)*
  • **HttpContext.Current.User** – current user
Thank you!

“Picking the top RIA toolkit of 2008 was no easy task. Our prize goes to Silverlight because it beats Flash in runtime performance; it has a modest download size; the design tools are good; it boasts wonderful .Net language support and a best-of-breed development environment in Visual Studio 2008...”

Infoworld, Jan 2009