

Securing Microsoft Silverlight

Web and User Experience



Level 300



Rudi Grobler

Barone, Budge & Dominick



Blog

<http://www.rudigrobler.net>



Twitter

@rudigrobler

DTL323 - Using the MVVM Design Pattern with the Microsoft Visual Studio 2010 XAML Designer
Mon, 18 Oct 2010 (10:45 - 11:45) | Breakout Session | Sessions Room C3 | Level: 300 - Advanced

WTB312 - Powering Rich Internet Applications: Windows Server AppFabric, Web Services, and Microsoft Silverlight
Tue, 19 Oct 2010 (14:30 - 15:30) | White Board | Session Room D2 | Level: 300 - Advanced

WUX310 - Securing Microsoft Silverlight
Tue, 19 Oct 2010 (17:15 - 18:15) | Breakout Session | Session Room A3 | Level: 300 - Advanced

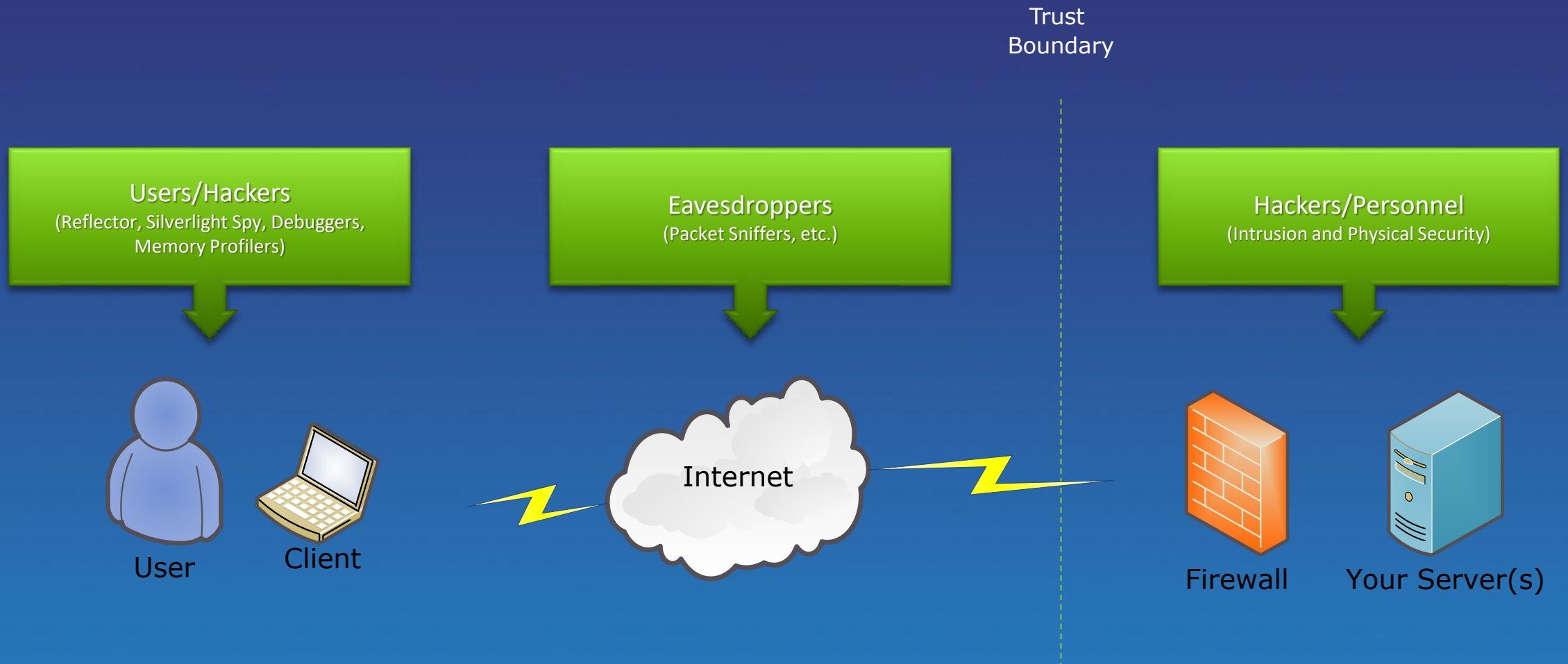
WUX407 - Best Practices: Building a Real-World Microsoft Silverlight Line-of-Business Application
Wed, 20 Oct 2010 (08:30 - 09:30) | Breakout Session | Session Room D4 | Level: 400 - Expert



A close-up, high-contrast photograph of a person's face, partially obscured by a black mask. The person is wearing black gloves and is turning a silver, circular dial on a white surface. The dial has markings for 0, 90, and 180 degrees. The lighting is dramatic, with strong highlights and deep shadows.

Know thy
ENEMY

Silverlight Security Vectors

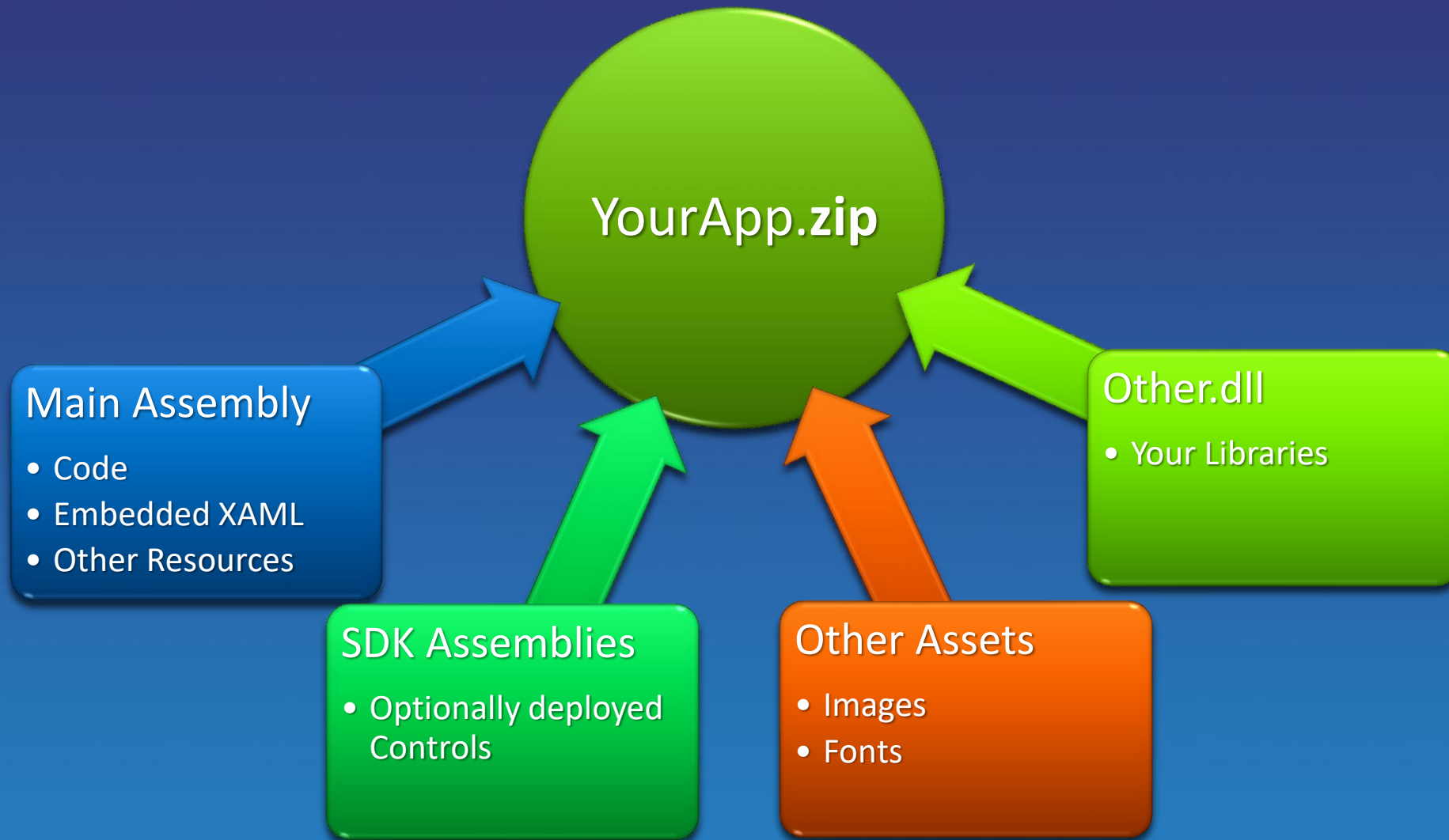


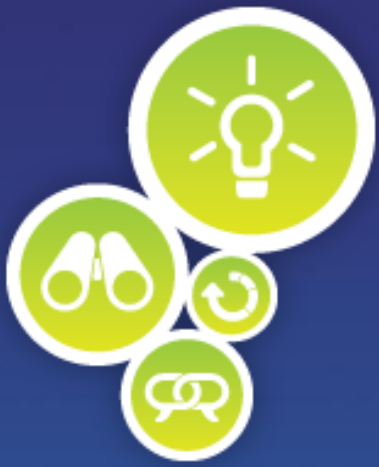
*"It's a basic truth of the human condition that **everybody lies**. The only variable is about what."*

House M.D.



Securing the Client





Hacking Silverlight

DEMO



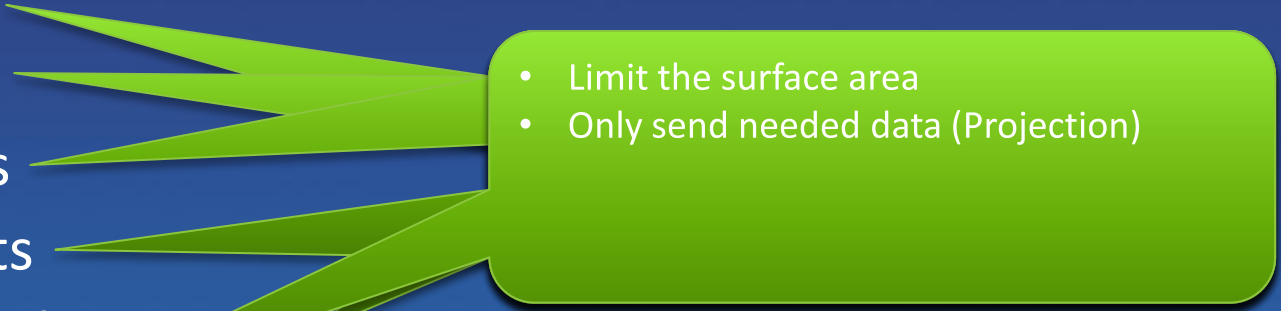
Are you
Scared yet?



Securing the Client

- Client Security Considerations

- Code
- XAML
- Assets
- Secrets
- Isolated Storage
- Data

- 
- Limit the surface area
 - Only send needed data (Projection)



Protecting Your Intellectual Property

- What is worth protecting?
 - Labor? No...
 - Unique implementations? Yes...
 - Sensitive data? Yes...
- Silverlight does not protect your Algorithms
 - Obfuscation only protects against decompilation
 - Code runs in the client
 - Client must be able to download assemblies
- Hide it on the Server
 - Generate the XAML on the Server
 - Send only summary data to the client



Obfuscation

“Obfuscation is the concealment of intended meaning in communication, making communication confusing, intentionally ambiguous, and more difficult to interpret”

- dotfuscator
 - Silverlight XAML Obfuscation
 - With XAML Obfuscation, developers can protect Intellectual Property and prevent tampering by renaming XAML resources, trim and compress Silverlight assemblies to optimize load time and performance, and automatically re-sign assemblies. Developers can fully obfuscate and instrument Silverlight XAP files resulting in a streamlined automated build process.
- CodeFort
 - .NET & Silverlight Obfuscator
 - CodeFort is an advanced obfuscator and protection tool for Microsoft .NET and Silverlight applications.





Obfuscation

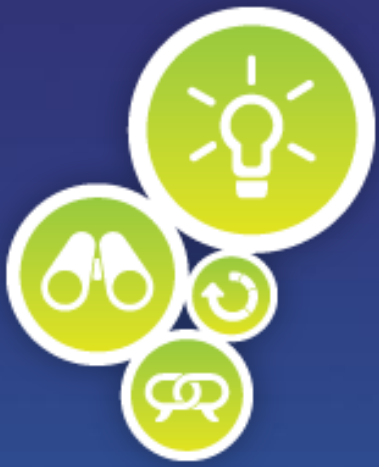
DEMO



Protecting Your XAP

- Silverlight Apps Are **Just** Files
 - Protect like any other web file
 - Forms Authentication
 - Windows Authentication
 - Token-based Authentication





Protecting your XAP

DEMO



Protecting Your XAP



Forms Authentication

- Cookie based
- Custom Encrypted Cookies
 - Never decrypt on client
 - Expire Cookies Frequently



Windows Authentication

- Just Works
- Assumes NTLM on the Platform
 - OSX is Problematic



Token-based Authentication

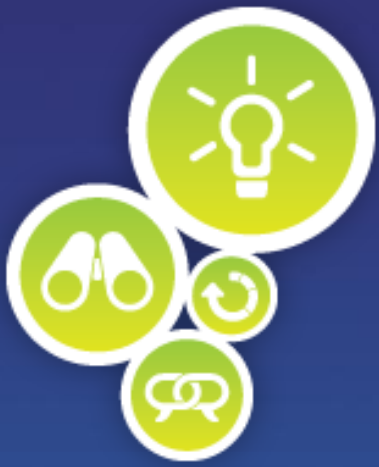
- Can use expiring tokens
- Pass them in on web services
- Not foolproof or 'secure'
- Must also expire



Protecting Your XAP

- For Apps with Login
 - XAP needs to be accessed anonymously
 - Compose at Runtime
 - Bootstrapper
 - PRISM
 - SLExtensions
- Tamper detection
 - Sign your XAPs or check their MD5 checksum





Protecting your XAP

DEMO



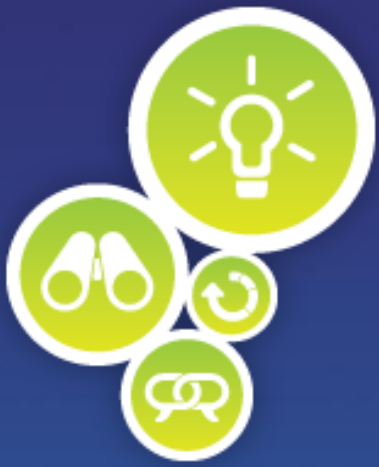
ASP.NET Application Services

- Using Forms Authentication Service
 - AuthenticationService (pre-built WCF)
 - Simple SOAP call to authenticate

```
<%@ ServiceHost Language="C#"
    Service="System.Web.ApplicationServices.AuthenticationService" %>
```

```
var proxy = new AuthenticationServiceClient();
proxy.LoginCompleted += (s, args) =>
{
    if (args.Result)
    {
        // Succeeded
    }
};
proxy.LoginAsync("Frank", "P2ssw0rd", null, false);
```





ASP.NET Application Services

DEMO



Isolated Storage

- Do NOT save secrets here... and if you do, at least encrypt it
- Can be disabled by user
- Is limited in size (1MB) but can be increased
- Discoverable (not encrypted)
 - %userprofile%\AppData\LocalLow\Microsoft\Silverlight\is
 - %userprofile%\Local Settings\Application Data\Microsoft\Silverlight\is
- Encryption
 - Symmetric Encryption: AES
 - Needs key and initialisation vector, both must be stored somewhere safe
 - Key can be derived from password or other known value





Isolated Storage

DEMO



Securing Services

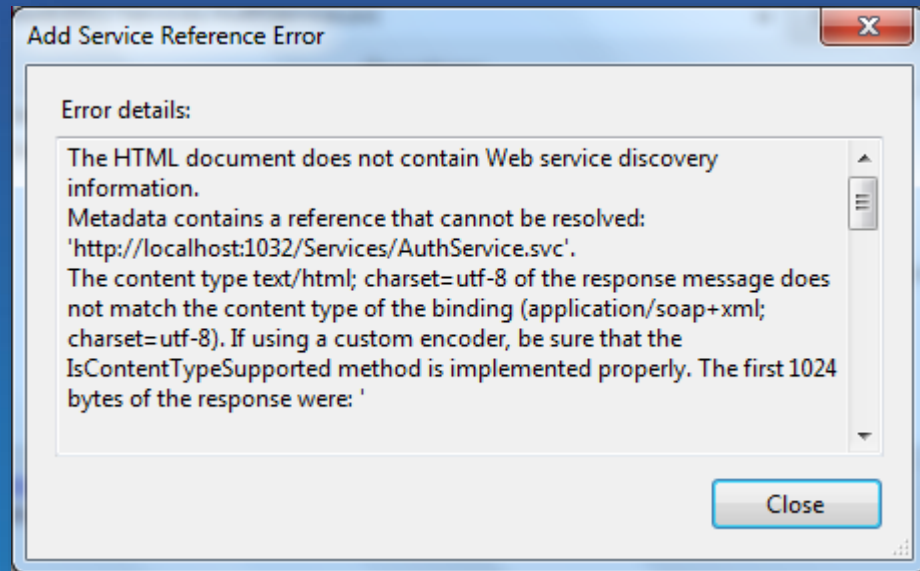
- Secure service same way you would secure the XAP
 - Token Based
 - Cookie Based
 - NTLM Based
- Also consider securing each method

```
if (HttpContext.Current.User.Identity.IsAuthenticated)
{
}
}
```



Securing Services

- Add Service Reference Problem
 - Doesn't play well with security
 - Must disable security when adding/refreshing
 - Trouble for building references at build-time



Securing Services

http://www.rudigrobler.net/MyCoolApp.xap



User



Client

https://www.rudigrobler.net/foo.aspx



Firewall



Your Server(s)



Securing Services

- To enable a Silverlight control to access a service in another domain, the service must explicitly opt-in to allow cross-domain access.

```
<?xml version="1.0" encoding="utf-8" ?>
<access-policy>
  <cross-domain-access>
    <policy>
      <allow-from http-request-headers="SOAPAction">
        <domain uri="*" />
      </allow-from>
      <grant-to>
        <resource path="/" including-subpaths="true" />
      </grant-to>
    </policy>
  </cross-domain-access>
</access-policy>
```

clientaccesspolicy.xml



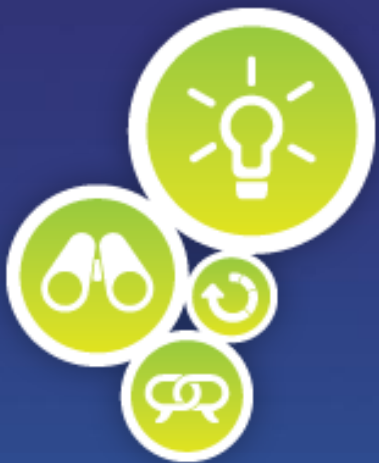
Securing WCF DataService

- Entity Set Access Rules

```
public class QuizDataService : DataService<GiveAQuizEntities>
{
    public static void InitializeService(DataServiceConfiguration config)
    {
        config.SetEntitySetAccessRule("QuestionDefinitions", EntitySetRights.All);
        config.SetEntitySetAccessRule("Quizzes", EntitySetRights.ReadSingle);
        config.SetEntitySetAccessRule("QuizTakers", EntitySetRights.WriteAppend);
        config.SetEntitySetAccessRule("QuizResults", EntitySetRights.WriteAppend);
        config.SetEntitySetAccessRule("QuizAnswers", EntitySetRights.WriteAppend);
    }
}
```

- Also supports Query Interceptors





WCF DataService

DEMO



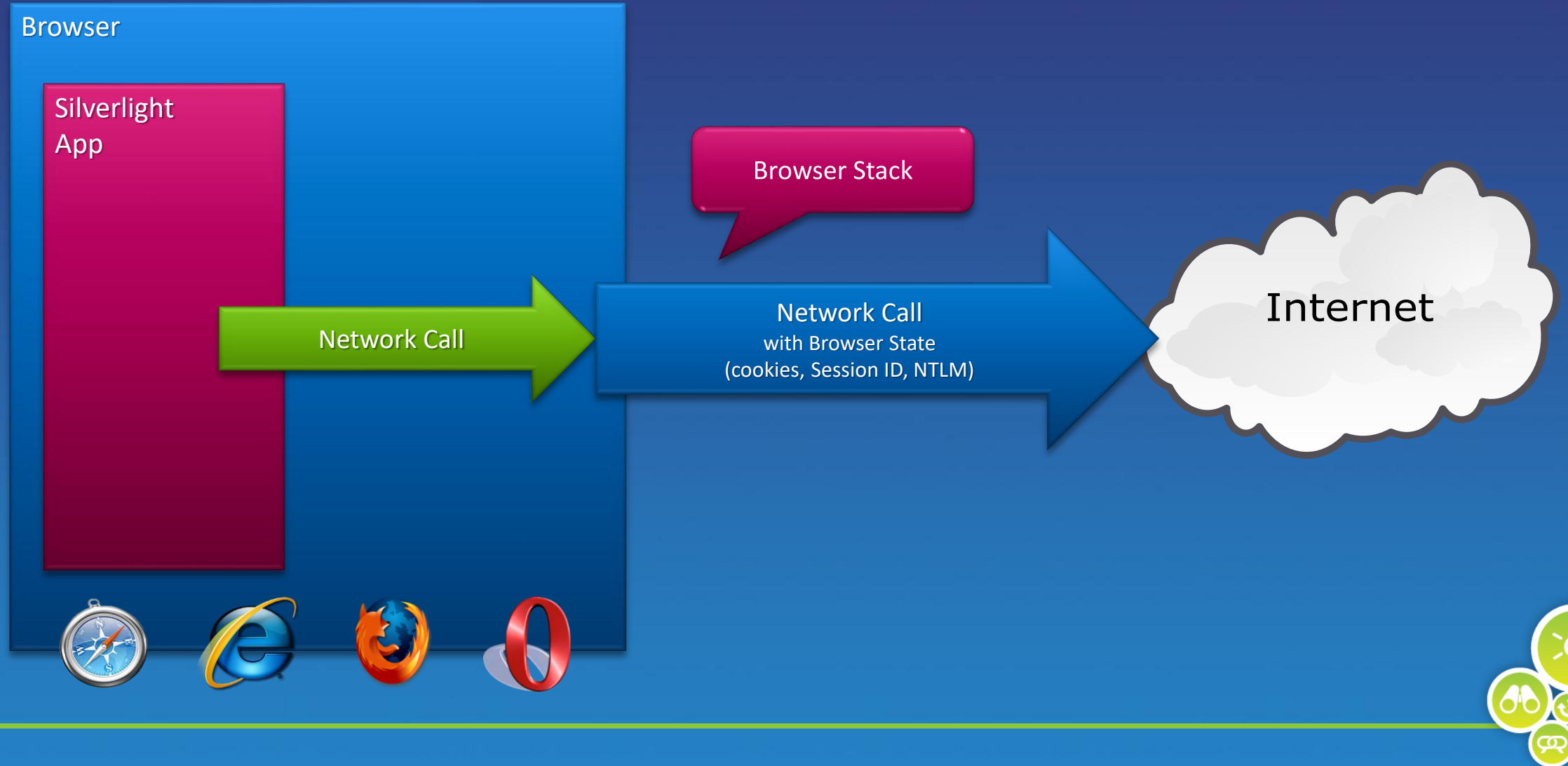


<http://giveaquiz.codeplex.com/>

GiveAQuiz.com is a new web site that allows users to create quizzes and have other users take the quizzes. This is differentiated from polling web sites as this project will allow the creator of a quiz to view the each individual user's results instead of just summary information (which is especially important for grading contextual results like essay questions). This web site is aimed squarely on users that need to create quizzes and give grades on the results.



Browser HTTP Stack



Browser HTTP Stack

- Standard network stack goes through Browser
 - Good:
 - Uses cookies and NTLM
 - Looks and feels like the browser
 - Bad:
 - Only GET/POST are supported
 - Typically limited to two outbound requests
 - Incomplete status codes





404

DEMO



Client HTTP Stack

- Alternative: Client HTTP Stack
 - For specific scenarios:
 - Need PUT/DELETE
 - Need Custom Cookies
 - Need more control
 - Status codes, bodies and headers
 - Only status code 404 (Not Found) and 200 (OK)
- Only stack available out-of-browser



Client HTTP Stack

- Create New Request
 - Use WebRequestCreator's ClientHttp property:

```
WebRequest req = WebRequestCreator.ClientHttp.Create(new  
    Uri("http://api.search.live.net/qson.aspx?query=Silverlight",  
        UriKind.Absolute));
```



Client HTTP Stack

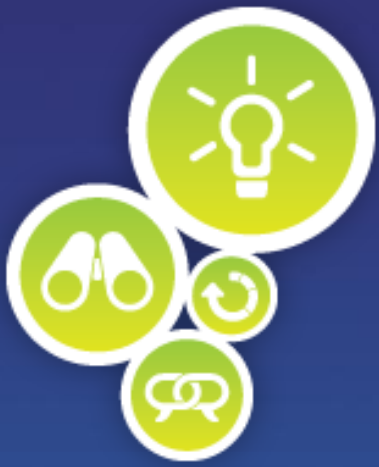
- Specify all Client HTTP Stack
 - Call WebRequest's RegisterPrefix to specify:

```
bool httpResult =  
    WebRequest.RegisterPrefix("http://",  
                             WebRequestCreator.ClientHttp);
```

- Then all calls become client, even WebClient:

```
WebClient client = new WebClient();  
client.DownloadStringCompleted += new  
    DownloadStringCompletedEventHandler(OnDlComplete);  
  
client.DownloadStringAsync(new Uri("/template.xaml",  
                                   UriKind.Relative));
```





Client Http Stack

DEMO



Browser Stack vs. Client Stack

| Feature | Browser Stack | Client Stack |
|------------------|---------------------------|---|
| Authentication | Handled by browser | Not supported |
| Content caching | Handled by browser | Not supported |
| Cookies | Handled by browser | Handled by CookieContainer (Cannot be shared with browser) |
| HTTP methods | GET and POST only | All methods provided by server options in ClientAccessPolicy.xml |
| Proxy info | Uses browser proxy info | Uses OS proxy info |
| Request headers | Supported on GET requests | Supported on all requests |
| Response headers | Not supported | Fully supported in HttpWebResponse |
| Status codes | 200 and 404 only | All status codes supported |



Questions?



Blog

<http://www.rudigrobler.net>



Twitter

@rudigrobler

And don't forget
to poken me



Resources

Microsoft®
tech·ed
Online

Sessions On-Demand & Community

www.microsoft.com/teched

Microsoft® | Learning

Microsoft Certification & Training Resources

www.microsoft.com/learning

Microsoft® TechNet

Resources for IT Professionals

<http://microsoft.com/technet>

msdn®

Resources for Developers

<http://microsoft.com/msdn>

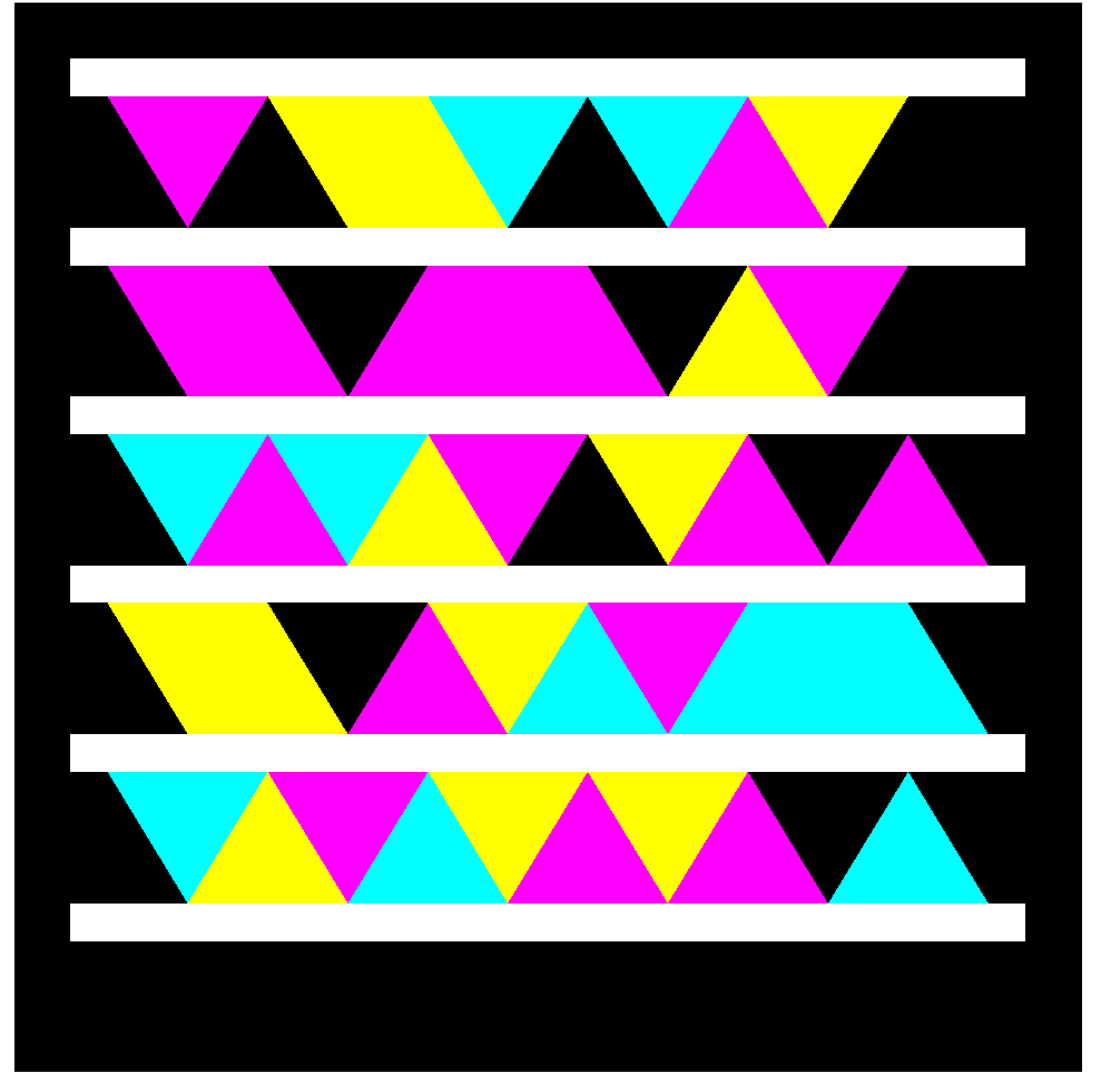
Need more Information?

SMS [Your Name] and the word “Web” to 41491





Complete an evaluation
via CommNet and Tag
to win amazing prizes!



Microsoft®

© 2008 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.