

Secure Smart Client ClickOnce Deployments

Brian Noyes

IDesign, Inc. (www.idesign.net)

brian.noyes@idesign.net

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

About Brian

- Chief Architect, IDesign Inc. (www.idesign.net)
- Microsoft Regional Director / MVP
- Writing
 - Data Binding in Windows Forms 2.0, Addison Wesley, January 2006
 - Smart Client Deployment with ClickOnce, Addison Wesley, Summer 2006
 - MSDN Magazine, MSDN Online, CoDe Magazine, The Server Side .NET, asp.netPRO, Visual Studio Magazine
- Speaking
 - Microsoft TechEd US, Europe, Malaysia, Visual Studio Connections, DevTeach, INETA Speakers Bureau, MSDN Webcasts
- Participates in Microsoft Design Reviews
- E-mail: brian.noyes@idesign.net
- Blog: <http://www.softinsight.com/bnoyes>

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

Agenda

- Quick Intro to ClickOnce
- Code Access Security at a Glance
- ClickOnce Security Protections
- User Prompting Privilege Elevation
- Configuring Trusted Publishers

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

Quick Intro to ClickOnce

- Smart Client deployment technology
 - Automatic deployment
 - Automatic / on-demand update
- Trustworthy deployment mechanism
 - Prevent harm to other apps or data on machine
 - At deployment
 - At runtime
- Best of two worlds:
 - Rich client user experience
 - Ease of maintenance and deployment of web applications

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

How ClickOnce Works

- Build Client App
- Publish it to deployment server
 - Visual Studio wizard
- Provide link to users
- User clicks on link
 - App downloads and caches on user machine
 - App executes in secure sandbox
 - App updates based on update policy if new version available

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

Agenda

- Quick Intro to ClickOnce
- Code Access Security at a Glance
- ClickOnce Security Protections
- User Prompting Privilege Elevation
- Configuring Trusted Publishers

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

Code Access Security

- Component oriented security
- Restricts operations or resources that executing code may perform/access
- Based on identity or origin of code, not user
- Managed programmatically and administratively
- Complex permissions schema
 - PermissionSet + Evidence = Code Group
- Several built-in origin-based code groups

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

Agenda

- Quick Intro to ClickOnce
- Code Access Security at a Glance
- ClickOnce Security Protections
- User Prompting Privilege Elevation
- Configuring Trusted Publishers

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

ClickOnce Deployment

- Application executable and supporting files downloaded and cached on client
- Placed under user profile
 - Isolated by user
 - Isolated by application
 - Isolated by version
- Cannot perform any custom install steps
 - Use bootstrapper for pre-requisites
- Manifests are signed
 - Provides authentication and tamper detection

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

ClickOnce Deployment

- Two deployment modes
 - Launched
 - Like No-Touch Deployment in .NET 1.X
 - Must be connected every time app runs
 - Files cache on machine
 - No other artifacts added to machine
 - Installed
 - Supports disconnected operation
 - Files cache on machine
 - Start menu shortcut added
 - Add/Remove Programs Control Panel item added

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

ClickOnce Execution

- User assumed to be non-administrator
- Protected by Code Access Security
- Permissions Determined By:
 - Address of deployment manifest (origin)
 - Code Access Security Policy for origin
 - Application manifest permission specs
 - User prompting or trusted publishers
- ClickOnce creates Application Trust

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

Agenda

- Quick Intro to ClickOnce
- Code Access Security at a Glance
- ClickOnce Security Protections
- User Prompting Privilege Elevation
- Configuring Trusted Publishers

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

User Prompting Permissions

- Configure security settings for application
- Publish application
- User machine does not have user prompting turned off (default)
- User is prompted at app launch

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

Agenda

- Quick Intro to ClickOnce
- Code Access Security at a Glance
- ClickOnce Security Protections
- User Prompting Privilege Elevation
- Configuring Trusted Publishers

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

Trusted Publisher Permissions

- Prevent user prompting
- Enterprise environment
 - Admins can configure desktop one time on all client machines
- Install trusted publisher certificate
 - Certmgr management console or command line
 - Trusted Publishers store
 - Signing authority must be in Trusted Root
- ClickOnce application manifests signed by trusted publisher get requested permissions

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

Agenda

- Quick Intro to ClickOnce
- Code Access Security at a Glance
- ClickOnce Security Protections
- User Prompting Privilege Elevation
- Configuring Trusted Publishers

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

Application Trust

- User CAS Policies
- One trust per app per version
- Created when app launches
 - User prompt accepted
 - Trusted publisher match
- Elevates app privilege to requested permissions in manifest
 - Applies to all assemblies that are part of manifest

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

User Prompting

- Registry Key
 - HKLM\Software\Microsoft\NETFramework\Security\TrustManager\PromptingLevel
 - String values:
 - Internet
 - LocalIntranet
 - MyComputer
 - TrustedSites
 - UntrustedSites
 - Values:
 - Enabled
 - Disabled
 - AuthenticodeRequired

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

User Prompting Reg Keys

- **Meaning:**
 - Enabled – Can prompt regardless of who signed the manifest
 - Disabled – If it needs to prompt, can't run
 - AuthenticodeRequired – Can only prompt if signed by a trusted root certificate
- **Defaults:**
 - "Internet" – "AuthenticodeRequired"
 - "LocalIntranet" – "Enabled"
 - "MyComputer" – "Enabled"
 - "TrustedSites" – "Enabled"
 - "UntrustedSites" – "Disabled"

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

Administrative ClickOnce Security Management - MAGE

- **MANifest GENerator**
- **Admin editing of manifests through GUI**
- **Signing of manifests**

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

What about securing the server?

- **Intranet**
 - Secure files based on ACLs
 - Optionally add a custom module/handler for HTTP requests for ClickOnce files
- **Intranet**
 - No good solution at this time

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!

Resources

- Smart Client Deployment with ClickOnce, Brian Noyes, Addison-Wesley, expect release Summer 2006
- Configuring ClickOnce Trusted Publishers, Brian Noyes, MSDN Online, April 2005
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwinforms/html/clickonctrustpub.asp>
- Deploy and Update Your Smart Client Projects from a Single Server, Brian Noyes, MSDN Magazine, May 2004
<http://www.msdn.microsoft.com/msdnmag/issues/04/05/ClickOnce/default.aspx>
- Automated Smart Client Deployment, Today and Tomorrow, Brian Noyes, The Server Side .NET, April 2005
<http://www.theserverside.net/articles/showarticle.tss?id=AutomatedSmartClient>
- Email: brian.noyes@idesign.net
- Blog: <http://www.softinsight.com/bnoyes>

Visual Studio
CONNECTIONS
Celebrating
its Four Year Anniversary!