

Advanced ClickOnce Taking it to the Next Level

Brian Noyes
IDesign, Inc. (www.idesign.net)
brian.noyes@idesign.net



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>



Agenda

- Quick Intro to ClickOnce
- Code Access Security at a Glance
- ClickOnce Security Protections
- Configuring Trusted Publishers
- Securing ClickOnce Application File Access
- What's Next in WinFX

DEVTEACH

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

DEVTEACH

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

DEVTEACH

Agenda

- Quick Intro to ClickOnce
- Code Access Security at a Glance
- ClickOnce Security Protections
- Configuring Trusted Publishers
- Securing ClickOnce Application File Access
- What's Next in WinFX

DEVTEACH

Code Access Security

- Component oriented security
- Based on identity or origin of code, not user
- Complex permissions schema
- Managed programmatically and administratively
- Restricts operations or access to resources based on code evidence

DEVTEACH

Agenda

- Quick Intro to ClickOnce
- Code Access Security at a Glance
- ClickOnce Security Protections
- Configuring Trusted Publishers
- Securing ClickOnce Application File Access
- What's Next in WinFX

DEVTEACH

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

DEVTEACH

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

DEVTEACH

ClickOnce Execution

- 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

DEVTEACH

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

DEVTEACH

Agenda

- Quick Intro to ClickOnce
- Code Access Security at a Glance
- ClickOnce Security Protections
- Configuring Trusted Publishers
- Securing ClickOnce Application File Access
- What's Next in WinFX



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



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

DEVTEACH

User Prompting

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

DEVTEACH

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"

DEVTEACH

Administrative ClickOnce Security Management - MAGE

- MANifest GEnerator
- Admin editing of manifests through GUI
- Signing of manifests

DEVTEACH

Agenda

- Quick Intro to ClickOnce
- Code Access Security at a Glance
- ClickOnce Security Protections
- Configuring Trusted Publishers
- Securing ClickOnce Application File Access
- What's Next in WinFX

DEVTEACH

Securing ClickOnce Application File Access

- How do I restrict access to my application files on the deployment server?
- Challenge: A ClickOnce launch or update is a set of separate and uncorrelated file requests
- Need to determine user identity on each file request
- Windows authentication only tractable way
 - Intranet user launches ClickOnce app
 - Each file request includes authenticated Windows identity of user
 - Secure file access through ACLs and/or custom authentication handler
- Other options:
 - Custom authentication / authorization in app code
 - Username / password in querystring parameters
 - Custom proxy on the client

DEVTEACH

What's next in WinFX?

- WPF Applications can be deployed through ClickOnce as well
- Installed mode same as today with Windows Forms
- Online mode goes away
- Replaced by browser hosting (Express applications)
 - WPF app hosted in the browser
 - Restricted security context
 - No user prompting for permission elevation



Resources

- Smart Client Deployment with ClickOnce, Brian Noyes, Addison-Wesley, expect release Summer 2006
- Programming Windows Presentation Foundation, Chris Sells and Ian Griffiths, O'Reilly & Associates, 2005.
- Configuring ClickOnce Trusted Publishers, Brian Noyes, MSDN Online, April 2005
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwinforms/html/clickonceitrustpub.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>

