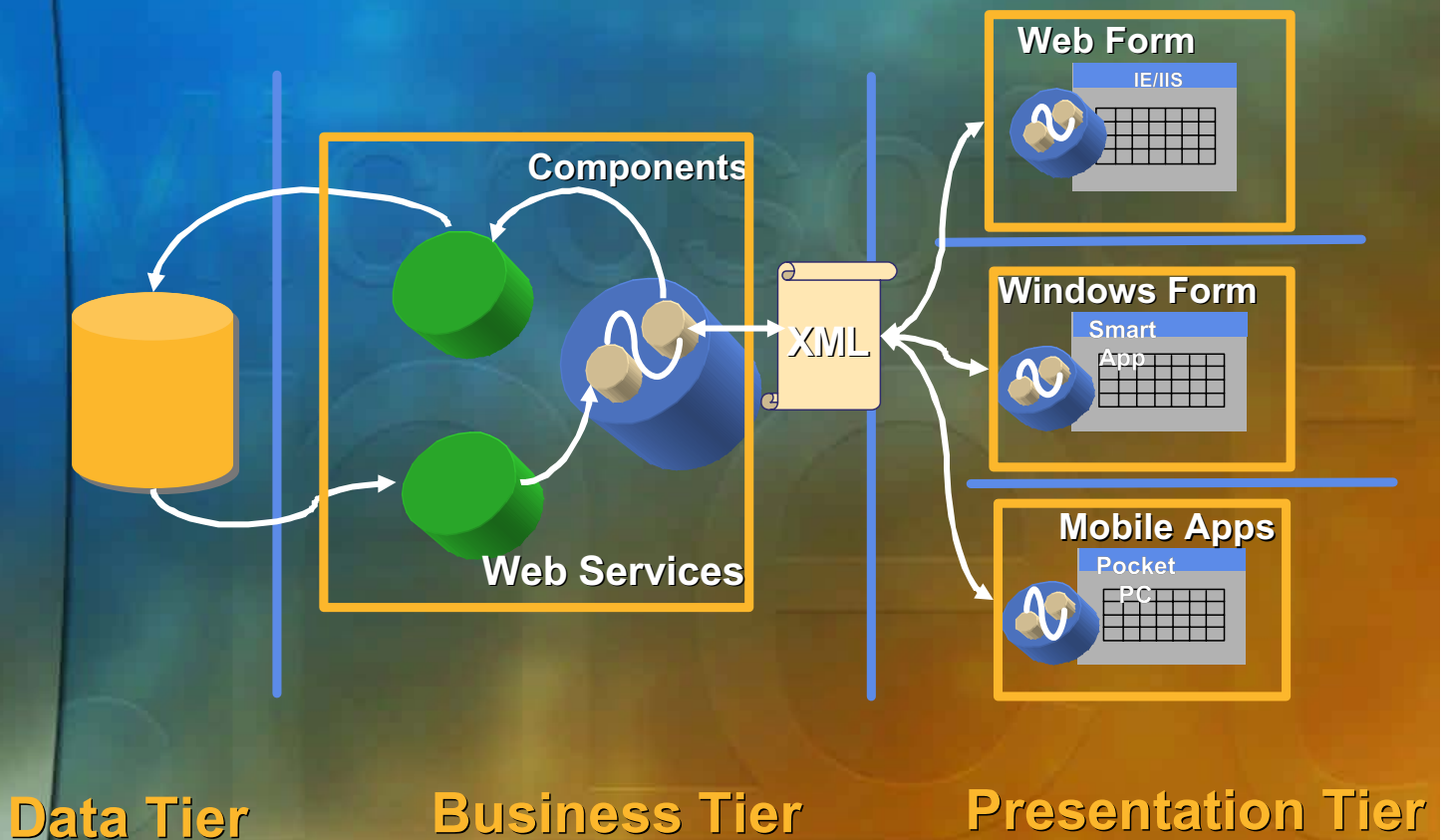


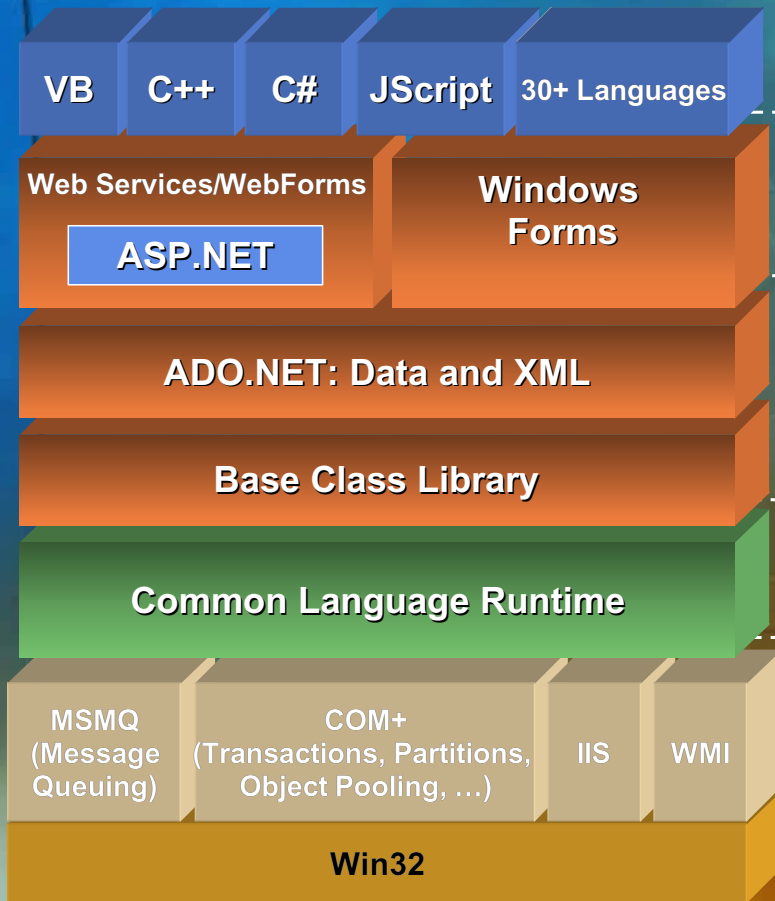
Introduction to .NET Framework and Security Features

Peter Ty
Developer Evangelist
Developer and Platform Group
Microsoft Hong Kong

.NET System Architecture

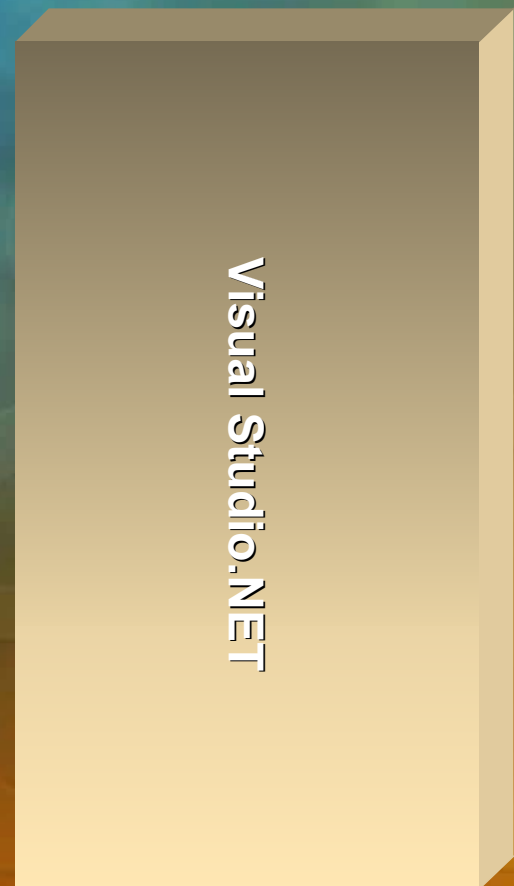
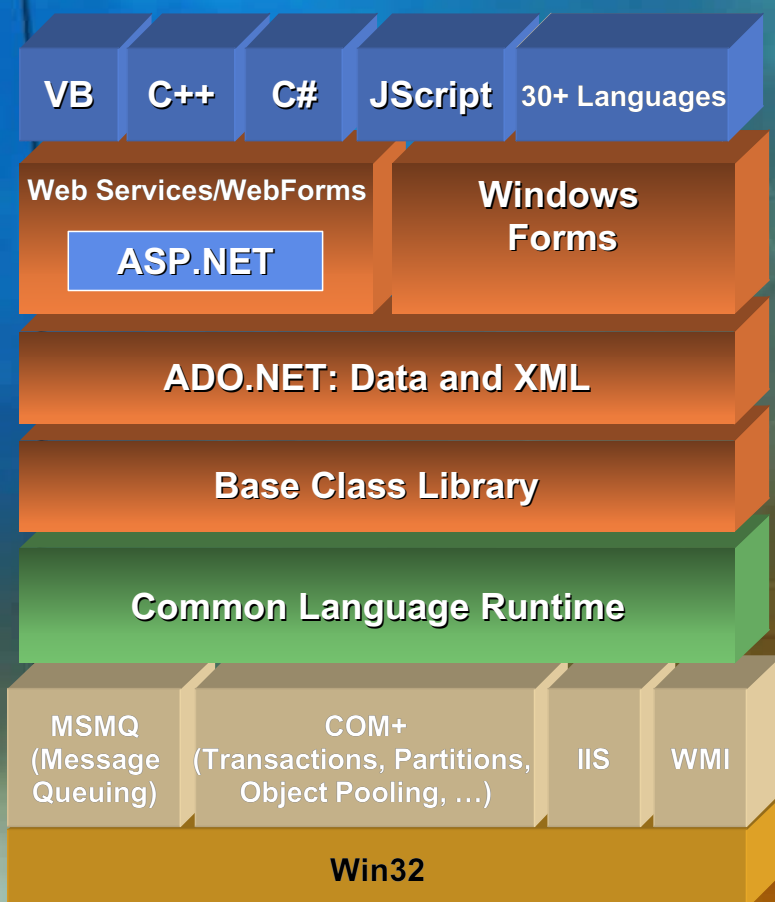


The .NET Framework



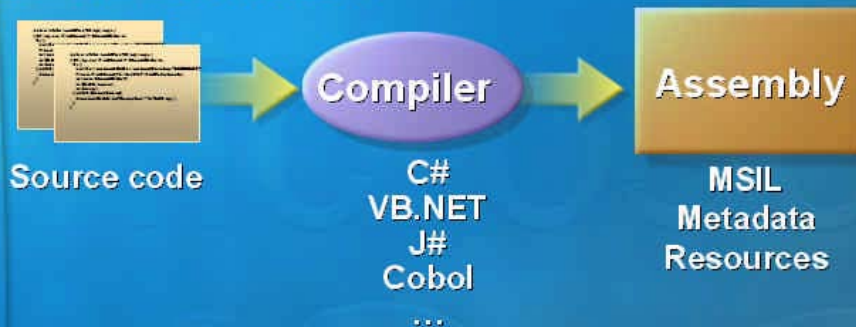
- Supports Many Languages
- Delivers Rich/Thin Clients/XML Web Services
- Unified programming models across Rich/Thin Client
- Cross-language integration
- One single set of API
- Managed execution environment
- Windows Application Services

The .NET Framework



Common Language Runtime

DEVELOPMENT



MSIL Security Implications

- ◆ .NET Framework programs compile to intermediate language
- ◆ Under native compilation, symbols are left out
- ◆ Not so with .NET Framework Apps
 - ❖ Decompilers already exist to recreate source code from compiled programs
 - ❖ Anakrino
<http://www.saurik.com/net/exemplar/>
 - ❖ Salamander
<http://www.remotesoft.com/salamander/>

What is Obfuscation?

- ◆ Technology of shrouding the facts
- ◆ Hide what's required, remove the rest
- ◆ Confuse observers, but give Runtime Environment the same delivery

General Obfuscation Transforms

- ◆ Symbol renaming
- ◆ Removal of unnecessary metadata
- ◆ Modification of control flow
- ◆ String encryption

Dotfuscator Community Edition

A lite version that performs overload induction renaming and Integrated in Visual Studio.NET 2003

Obfuscation

demo

Common Language Runtime

- ◆ **Manages running code**
 - ❖ Threading, Memory management
 - ❖ Eliminates memory management drudgery
 - ❖ Kills entire classes of bugs (e.g., memory corruption, ref counting)
 - ❖ Auto-versioning, no more DLL Hell
- ◆ **Fine-grained evidence-based security**
 - ❖ Code access + Role-based
 - ❖ Integrated with underlying OS
- ◆ **No-touch deployment**
 - ❖ XCOPY, no registry required

CLR Security Infrastructure

- ◆ **Components and Security needs**
 - ❖ Security flexibility for distributed applications
 - ❖ Enforcement on all callers – direct and indirect
- ◆ **Code Access Security**
 - ❖ Evidence
 - ❖ Policy
 - ❖ Permissions

Evidence

Determines what permissions to grant to code

- ◆ **Evidence**
 - ❖ Known information about .NET assembly
 - ❖ As input to the Security policy mechanism
- ◆ **Types of Evidences**
 - ❖ Where the code is loaded from: Site, Url, Zone and Application Directory
 - ❖ Who wrote the code: Strong Name and Publisher
 - ❖ Hash

Policy

Determines the permissions granted to assemblies

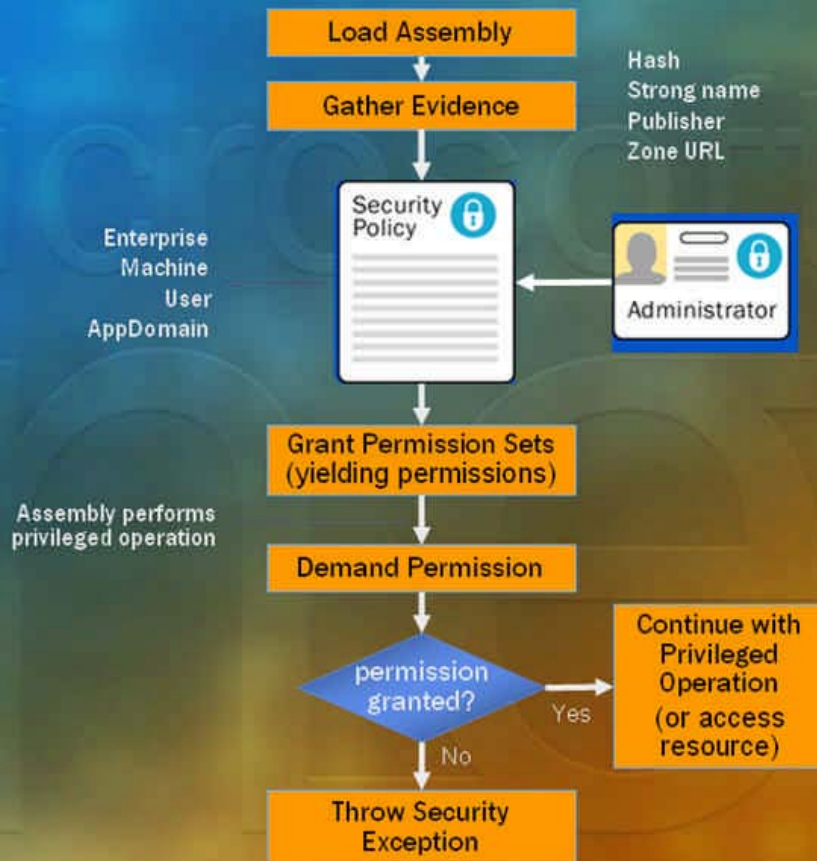
- ◆ **Configurable by System admin and users**
- ◆ **4 Levels**
 - ❖ User
 - ❖ Machine
 - ❖ Enterprise
 - ❖ AppDomain
- ◆ **Code Group hierarchy**
 - ❖ Membership conditions
 - ❖ Permission Sets

Permissions

Rights for code

- ◆ **Granted by code access security policy**
- ◆ **Enforcing security**
 - ❖ Demands
 - ◆ Walk through stack frames
 - ❖ Link Demands
 - ◆ Only checks the immediate caller

Evidence + Policy = Permissions

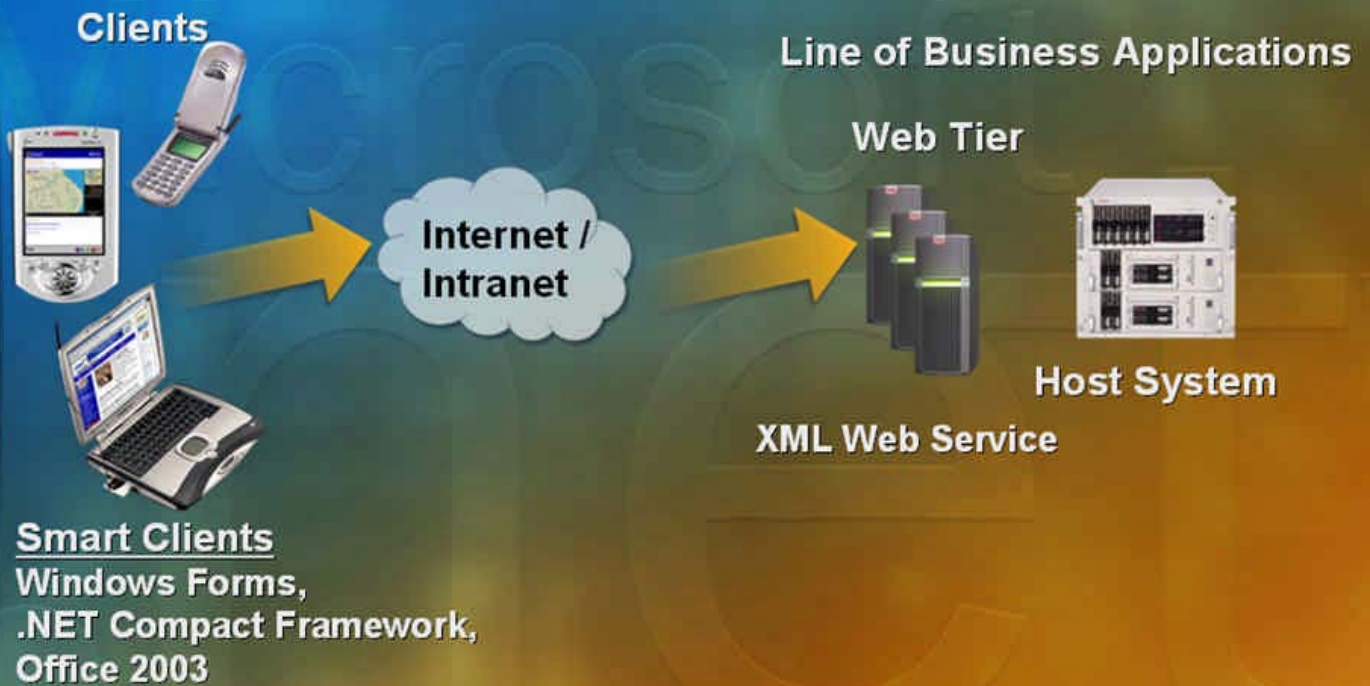


Code Access Security

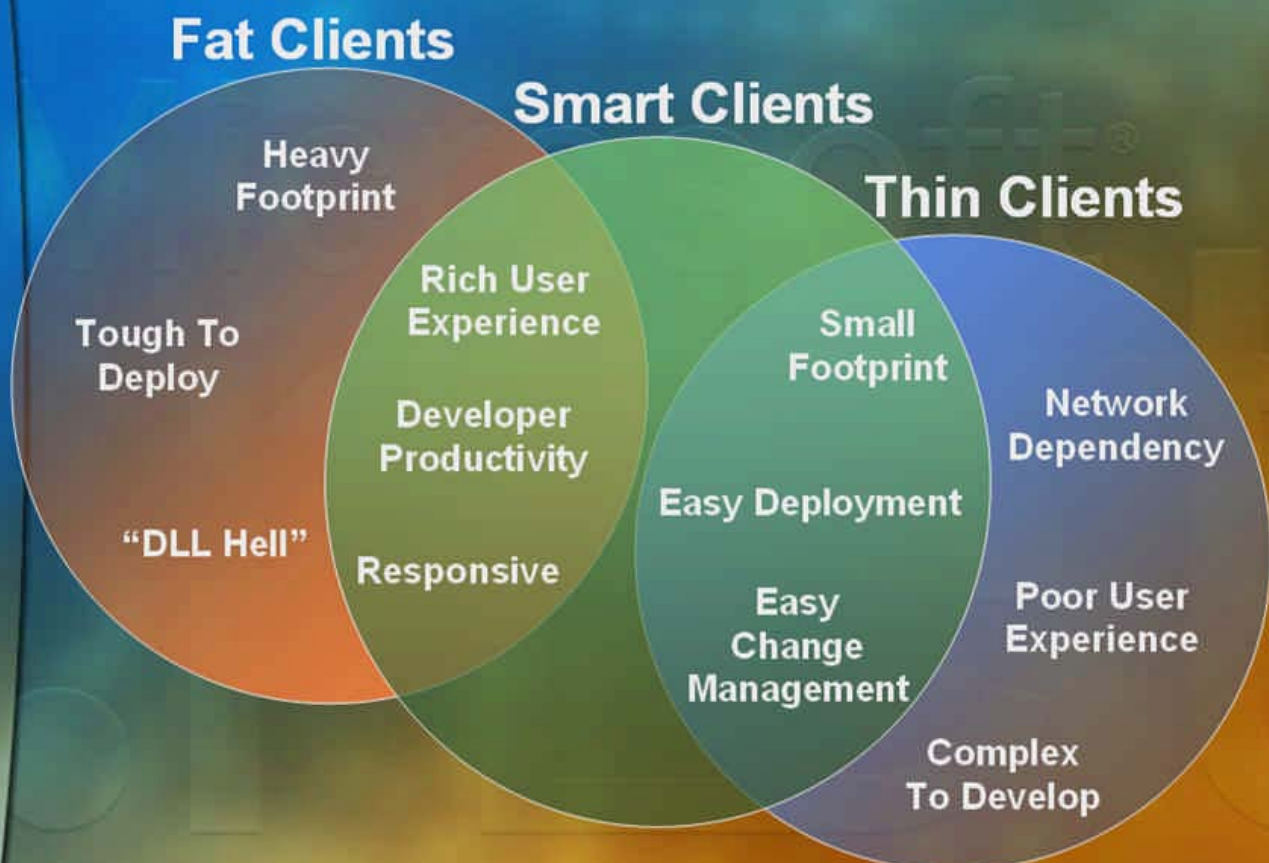
demo

Smart Client Applications

XML Web Services



What are Smart Client Apps?



Deployment Options

- ◆ **.NET offers several options for deploying and installing smart clients**
 - ❖ **Run From Web**
 - ❖ **Code download**
 - ❖ **MSI-deployed**

Run From Web - Security

- ◆ **Entire app is downloaded to Assembly Download Cache**
 - ❖ **IEExec process launches the app with restricted security settings**
- ◆ **Advantages**
 - ❖ **Very easy to deploy / update**
- ◆ **Limitations**
 - ❖ **Runs only inside Internet Explorer 5.01+**
 - ❖ **Semi-trusted**
 - ❖ **Can be difficult for users to discover**

Smart Client Demo

demo

ASP.NET Page Development

- ◆ Rich server controls
 - ❖ Provides VB-Like Model
- ◆ Compiled languages
 - ❖ VB, C#, JScript, COBOL, etc.
- ◆ Separation of code and content
 - ❖ Developers and designers can work independently
- ◆ Automatic multiple client support
 - ❖ DHTML, HTML 3.2, WML, small devices

ASP.NET Security



ASP.NET Authentication

- ◆ **Windows authentication**
 - ❖ Uses existing Windows user accounts
 - ❖ Ideal for intranet applications
- ◆ **Passport authentication**
 - ❖ Convenient for users (single sign-in)
 - ❖ Puts credential storage in hands of others
- ◆ **Forms authentication**
 - ❖ Typically uses eBay-style login pages
 - ❖ Ideal for Internet applications

Web Services Authentication

- ◆ Windows auth (NTLM)
 - ❖ Easy choice for intranet applications
- ◆ Roll-your-own
 - ❖ Recommended for interop with non-WS-Security platforms
 - ❖ Common path before WSE 2.0
- ◆ Web Services Enhancements (WSE) 2.0
 - ❖ Cross-platform, evolving standard
 - ❖ Uses standard SOAP header to transmit caller's credentials

Technical Resources

- ◆ MSDN
 - ❖ Online resources
<http://msdn.microsoft.com/>
- ◆ www.gotdotnet.com
- ◆ Windows Forms development
www.windowsforms.net/
- ◆ ASP.NET redefines web development!
www.asp.net

Local Developer Community

- ◆ Hong Kong .NET User Group

<http://www.HKNetUG.com>

- ◆ IT4All forum: Share and learn from peers

<http://www.it4all.com.hk/>