您的潜力，我们的动力

Microsoft
微软（中国）有限公司

Visual Studio Tools for Office 系列课程（4）-- 安全性与部署

付仲恺
微软特邀开发专家

msdn

MSDN Webcasts

议题

- VSTO安全性
  - 策略，许可和证据概述
  - 智能文档安全策略
- VSTO部署
  - 概述
  - 客户端要求
  - 部署模式
  - 离线问题考虑
  - 部署工具

安全性

- 策略，许可和证据概述
- VSTO安全系统

什么是策略

- 策略是通过确保决定被执行而实现良好效果的工具
  - 策略需要提前而不是临时制定
  - 往往通过策略专家制定，而不是最终用户

许可和证据

- 许可: 在银行兑换支票
- 证据: 照片，ID
- 证据策略:
  - ID必须由可信的权威机构发布
  - 照片必须与当事人相符
  - 等等；策略往往非常复杂
- 如果证据不充分，那么请求将被拒绝

.NET代码访问安全

- 四种策略级别: Enterprise, Machine, User, Application
- 策略级别由一组树结构构成
- 每个代码组与特定的一组权限集合证据相关联
- 只有当所有策略级别都允许授予权限时操作才能被许可

代码组成员条件的证据类型

- Zone: MyComputer, Intranet, etc.
- Url: http://customizations/*, file://c:\docs*
- Hash: 识别指定文件
- Publisher Certificate: 创建一组信任链
- Strong Name: 保证加载正确版本的正确代码
- OfficeDocument: VSTO新支持
  - 需要将MSOSEC.DLL加载到GAC中
  - MSOSEC.DLL 默认没有被加载到GAC中

强名称

- 设计用于安全加载，同时也可作为证据使用
- 不等同于证书：没有信任链
- Strong name/publisher code组应该位于location组之下
- 使用配制文件来管理版本不匹配问题

策略特点

- Enterprise: 所有代码完全被信任
- Machine: 所有代码均不被信任
  - 来自local machine的代码获得完全信任
    - Microsoft/ECMA强名称获得完全信任
  - 来自intranet的代码获得部分信任
  - 来自Internet的代码几乎不被信任
- User: 所有代码均被完全信任
- Application:所有代码均被完全信任
- 由于所有级别都必须要获得许可，因此任何一个级别的策略调整都能够影响整个策略

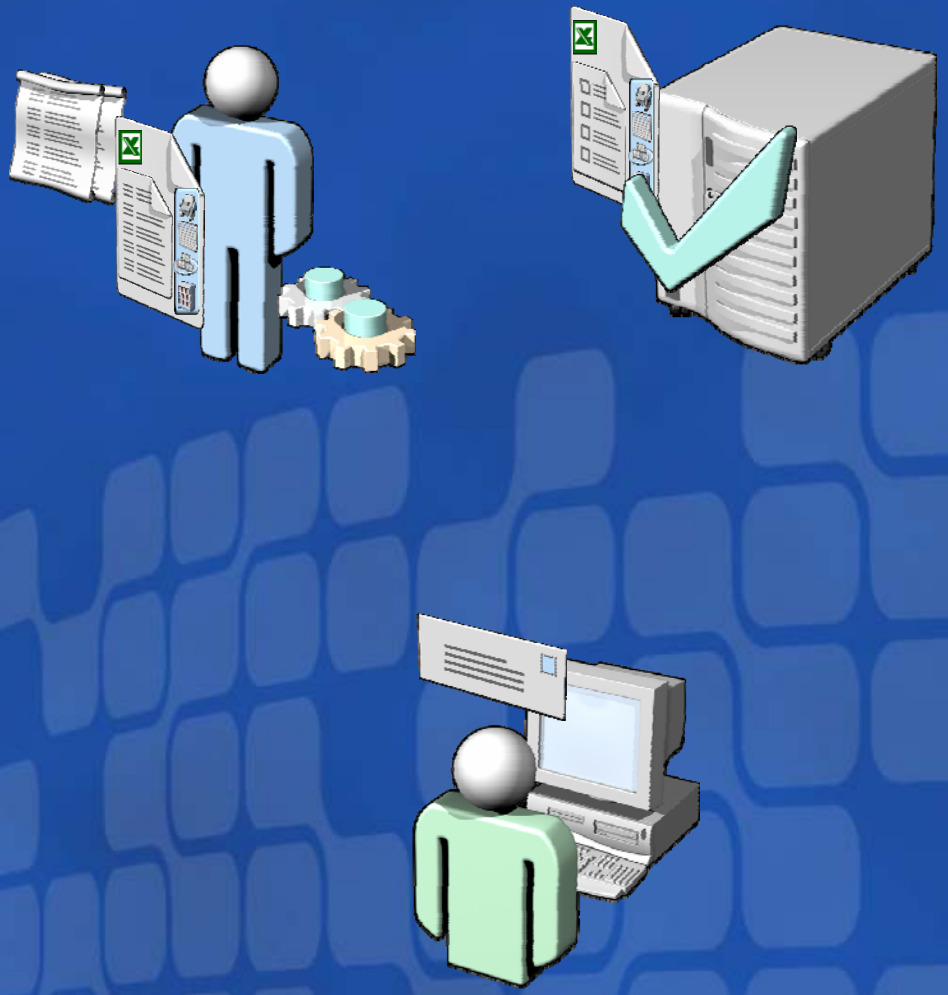
VSTO安全特点

- 文档具有高度的可移动性和可编辑性
- Office对象模型变得更加强大
- 基于OOB 策略，复制应用程序到您的本机后将获得完全信任权限
- 用户不需要将带有代码的文档考虑为应用程序
- 我们不希望成为下一代平台的宏病毒作者

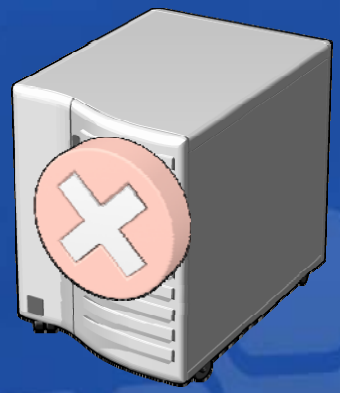
VSTO安全策略

- 保证缺省安全
- 文档和程序集必须同时获得完全信任才能被执行
  - 因为VSTO文档需要调用非托管代码的Office对象模型
  - 缺省情况下代码不会被执行
- 通过位置来获取文档证据
  - E-mail附件必须要复制到桌面(Outlook临时目录具有Internet Zone权限)
- 程序集证据通过：
  - 签名：认证代码或者强名称
  - 位置: URL
  - Local Machine Zone不够充分

正常模式



非法模式



DEMO

智能文档安全配置实例

部署

- 概述
- 客户端要求
- 部署模式
- 离线问题考虑
- 部署工具

概述

- 基于清单的部署方式
  - 应用程序清单
  - 部署清单
- 什么是清单?
  - 提供解决方案的丰富信息
  - 自升级处理

清单和ClickOnce

- 充分利用在线ClickOnce技术
  - 在.NET Framework 2.0和Visual Studio .NET 2005中发布
- 提供对于应用程序的完全描述
  - 描述DLL所使用的状态
  - 包含依赖程序集
  - 描述程序集位置
  - 不用于本地安装

相关文件

- 文档，代码以及程序集各自分开保存
  - 代码是Visual Studio项目的一部分
  - 程序集只与文档在一起部署
- 程序集与文档进行“链接”
  - VSTO 2003: 自定义属性
  - VSTO 2005: 嵌入在文档中的应用程序清单
  - 应用程序清单指向部署清单

应用程序清单样例

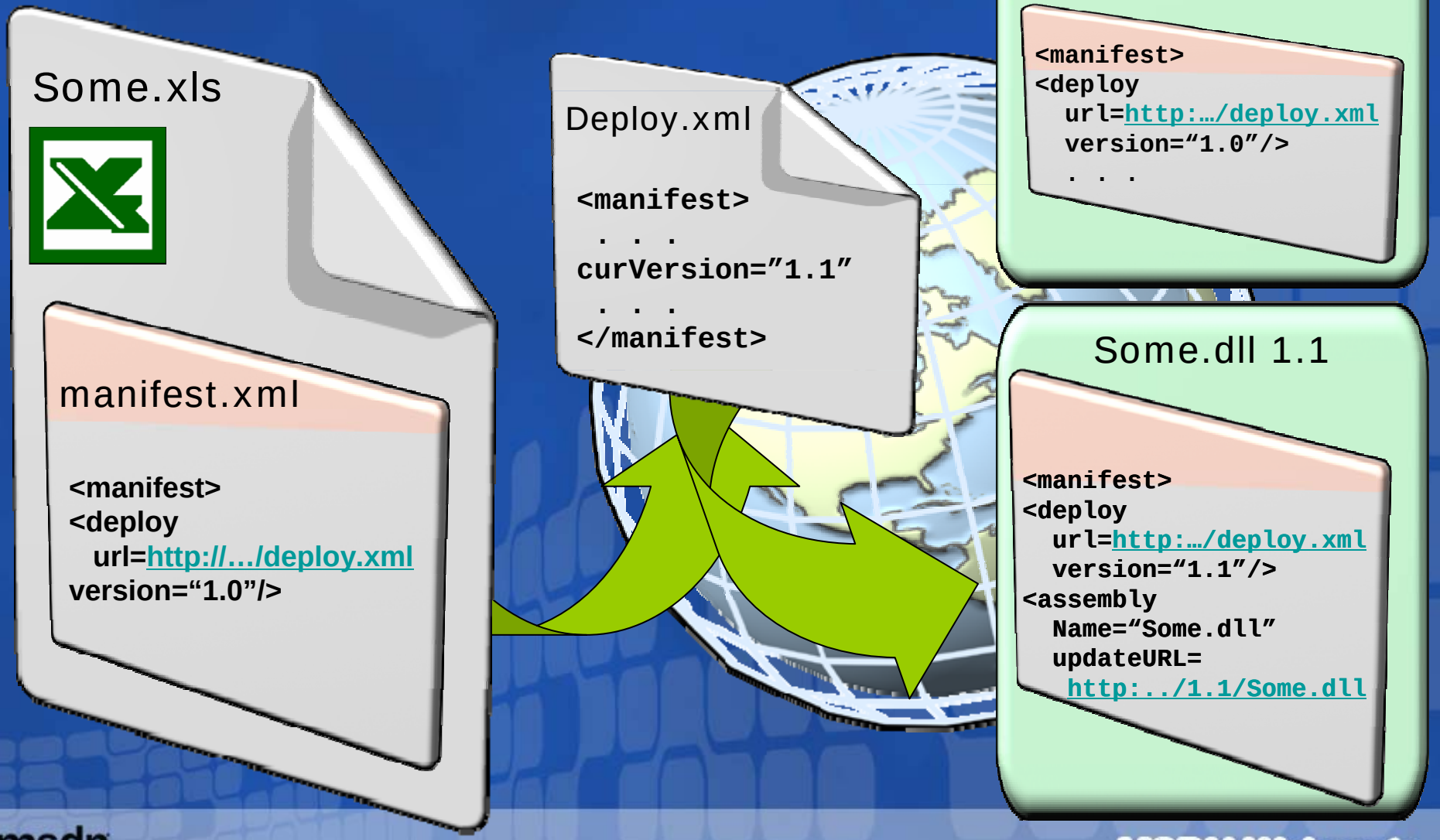

```
<assembly ...>
   <assemblyIdentity name="Excel4.manifest"
        version="1.0.22"/>
   <entryPoint name="Startup" dependencyName="Excel4">
        <clrClassInvocation class="Sheet1"/>
        </entryPoint>
   <dependency name="Excel4">
        <dependentAssembly>
          <assemblyIdentity name="Excel4" version="1.0.1"/>
        </dependentAssembly>
        <installFrom
           codebase="http://deployweb/excel4.dll" />
   </dependency>
   <installFrom
        codebase="http://deployweb/excel4.deploy"/>
</assembly>
```

部署清单样例

```
<assembly ...>
   <assemblyIdentity
        name="Excel4.deploy"
        version="1.0.1"/>

   <dependency>
        <dependentAssembly>
              <assemblyIdentity
                    name="Excel4.manifest"
                    version="1.0.22"/>
        </dependentAssembly>
        <installFrom
          codebase="http://deployweb/Excel4.manifest"/>
   </dependency>
</assembly>
```

自动更新处理过程



对客户端计算机的要求

- .NET Framework 2.0
- Office Professional Edition 2003
  - 或者单机版Excel 2003/Word 2003
  - 推荐使用完整安装以确保PIAs被安装
    - 在缺省安装条件下，PIAs没有被要求安装
- VSTO 2005运行时
- 适当的.NET安全策略

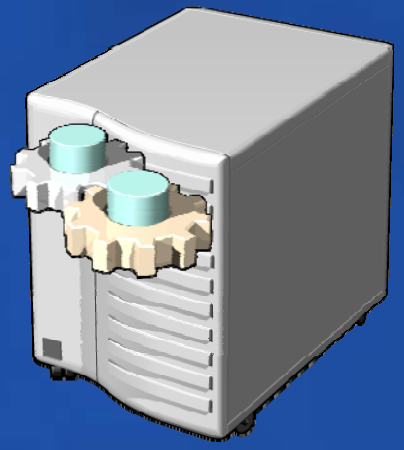
部署模型

- 本地/本地
- 本地/网络
- 网络/网络

本地/本地 模型

- 需要考虑:
  - 正在加载的文档没有网络权限
  - 用户必须要安装解决方案
  - 用户需要拥有个人的文档副本
  - 更新后需要重发布

本地/网络 模型



- 需要考虑:
  - 文档加载需要网络权限
  - 用户需要拥有个人的文档副本
  - 程序集在中心位置更新
  - 更新后需要重发布

网络/网络 模型

- 需要考虑：
  - 文档加载需要网络权限
  - 用户共享文档实例
  - 在中心服务器更新数据

对于离线状态

- 本地安装 (如: Program Files)
  - 需要用户交互操作
  - 首次安装需要运行
  - 服务MSI
- 离线文件夹
  - 需要用户交互操作
  - 版本更新无需用户交互
  - 在第一次离线访问前需要同步
- IE缓存
  - 版本更新无需用户交互
  - 在第一次离线访问前需要同步
  - 短时间缓存
  - 被引用程序集延时加载

部署工具

- Publishing Wizard
- ServerDocument class

ServerDocument

- 能够修改应用程序清单的任何一部分

```
ServerDocument doc = new
    ServerDocument("file.doc");
doc.AppManifest.DeployManifestPath =
    “http://...";
```

DEMO

智能文档部署实例

总结

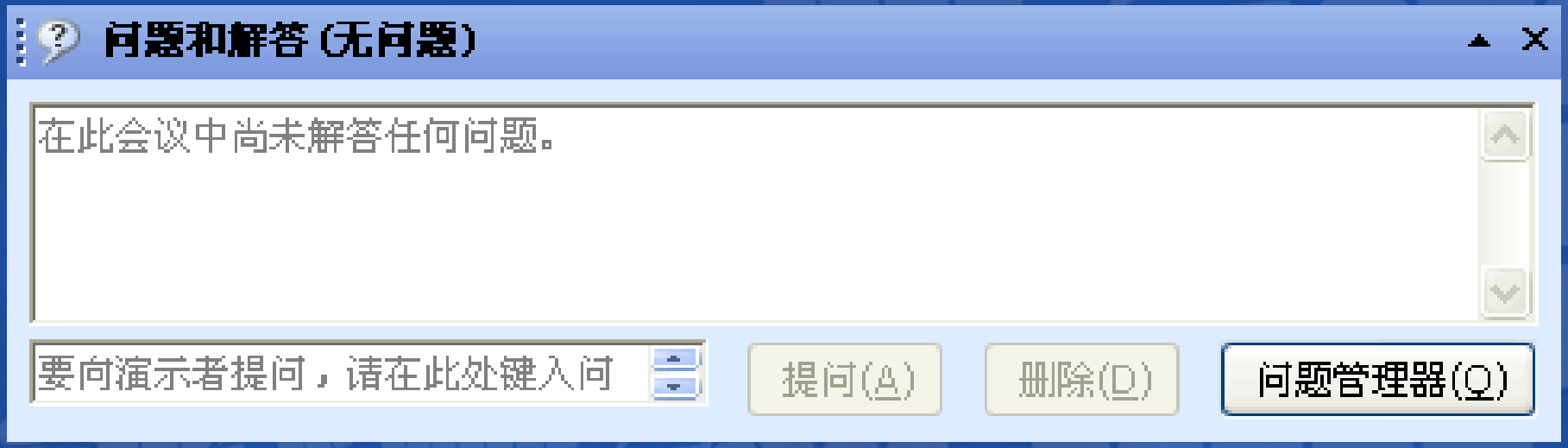
- 基于策略，证据和许可的安全系统
  - VSTO基于.NET代码访问安全策略
  - 智能文档安全性特点
- 基于清单的部署方式
  - 应用程序清单
  - 部署清单
  - 3种部署模式
  - 部署工具

您的潜力，我们的动力

Microsoft
微软（中国）有限公司

Q&A

如需提出问题，请单击“提问”按钮并在随后显示的浮动面板中输入问题内容。一旦完成问题输入后，请单击“提问”按钮。




您的潜力，我们的动力
Microsoft
微软（中国）有限公司
Microsoft
msdn
MSDN Webcasts