您的潜力，我们的动力

Microsoft
微软（中国）有限公司

基于Internet 和Extranet 企业应用解决方案的安全开发实践

钟卫
开发平台合作部
微软公司

msdn

MSDN Webcasts

Session Prerequisites

- Experience designing, developing, or testing in a Windows environment
- Development experience with Microsoft Visual Basic, Microsoft Visual C++, or C#

Level 200-300

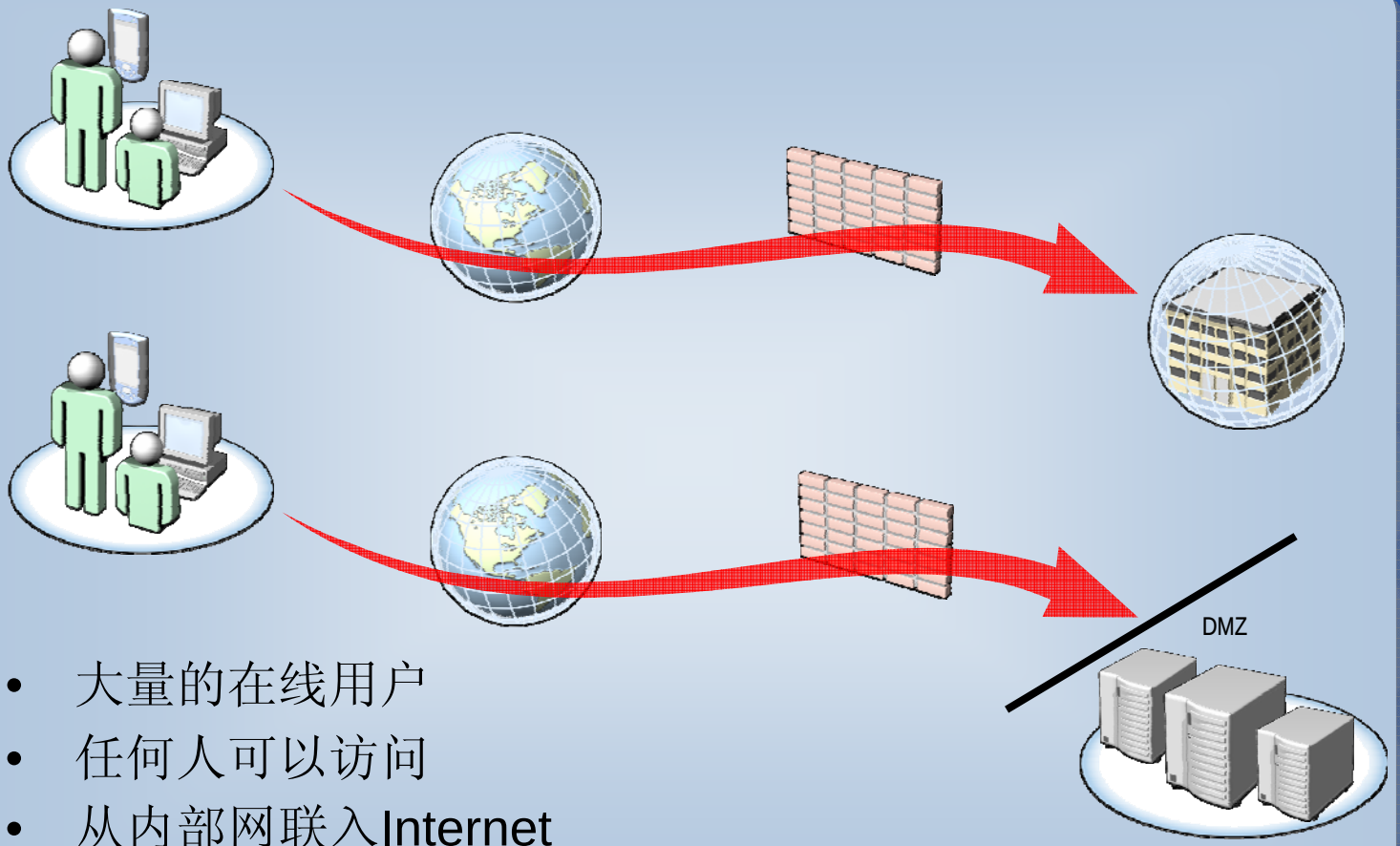
课程概述

- 基于Internet 的应用安全简介
- 数据传输安全实践
- 身份管理实践
- 基于Forms的认证
- Web Services 的安全实践

基于Internet的应用安全简介

- 基于Internet 的应用安全简介
- 数据通讯安全实践
- 身份管理实践
- 基于Forms的认证
- Web Services 的安全实践

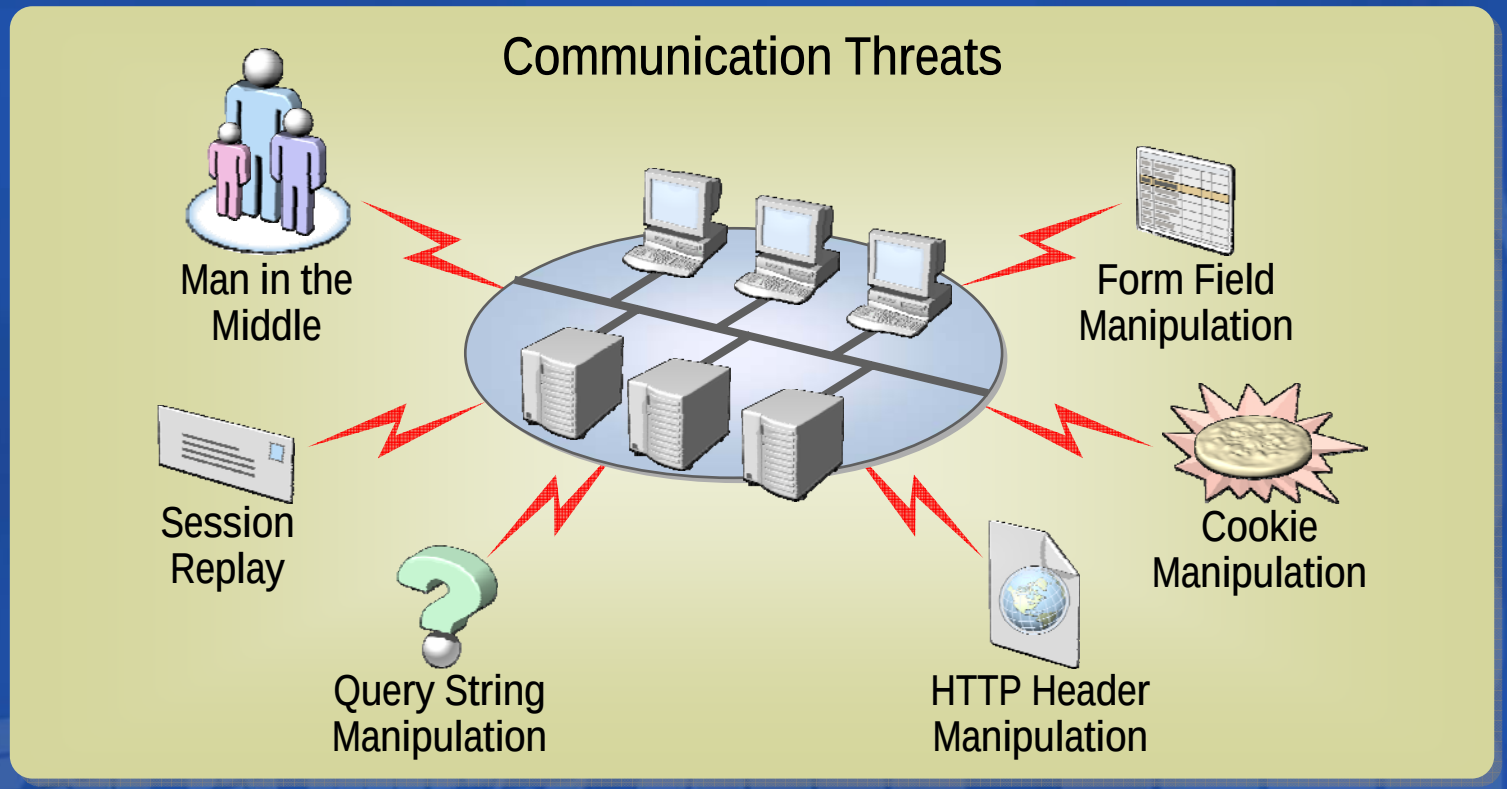
Internet应用的环境特征



- 大量的在线用户
- 任何人可以访问
- 从内部网联入Internet

数据通讯安全

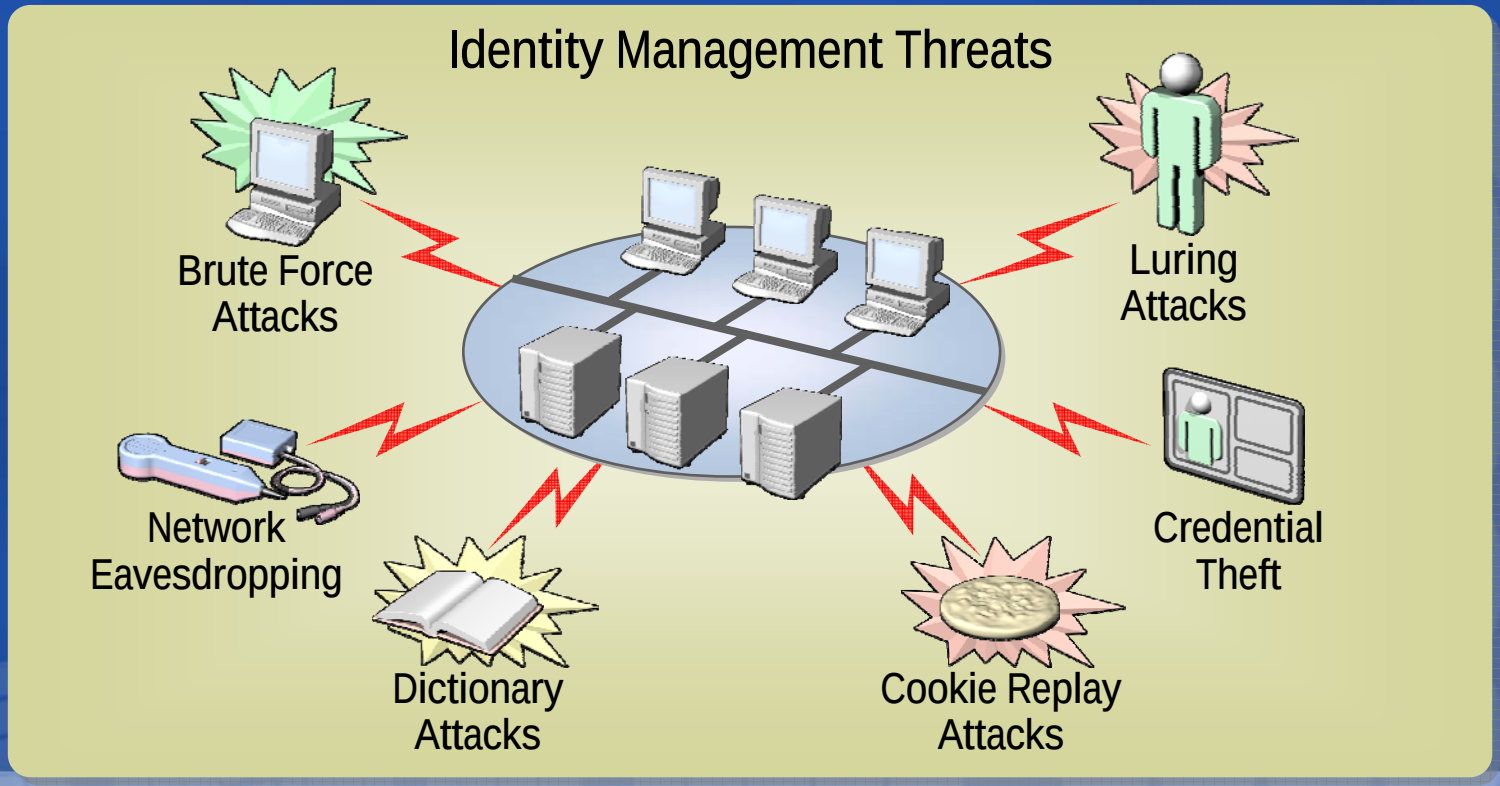
- 通过Internet的数据传输过程会被监听
- 敏感数据的传输确保安全



身份管理

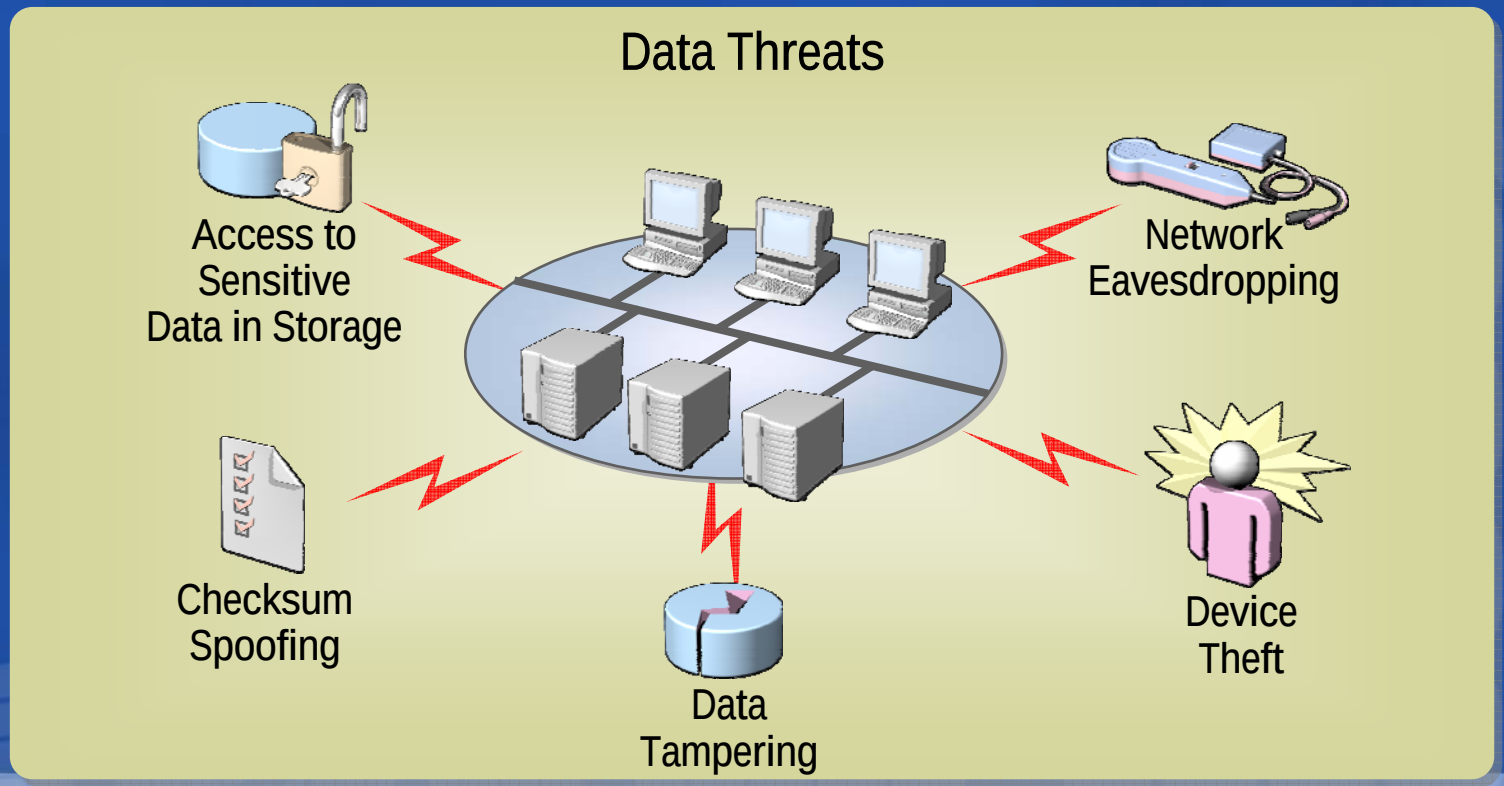
身份管理可以通过：

- 认证
- 授权



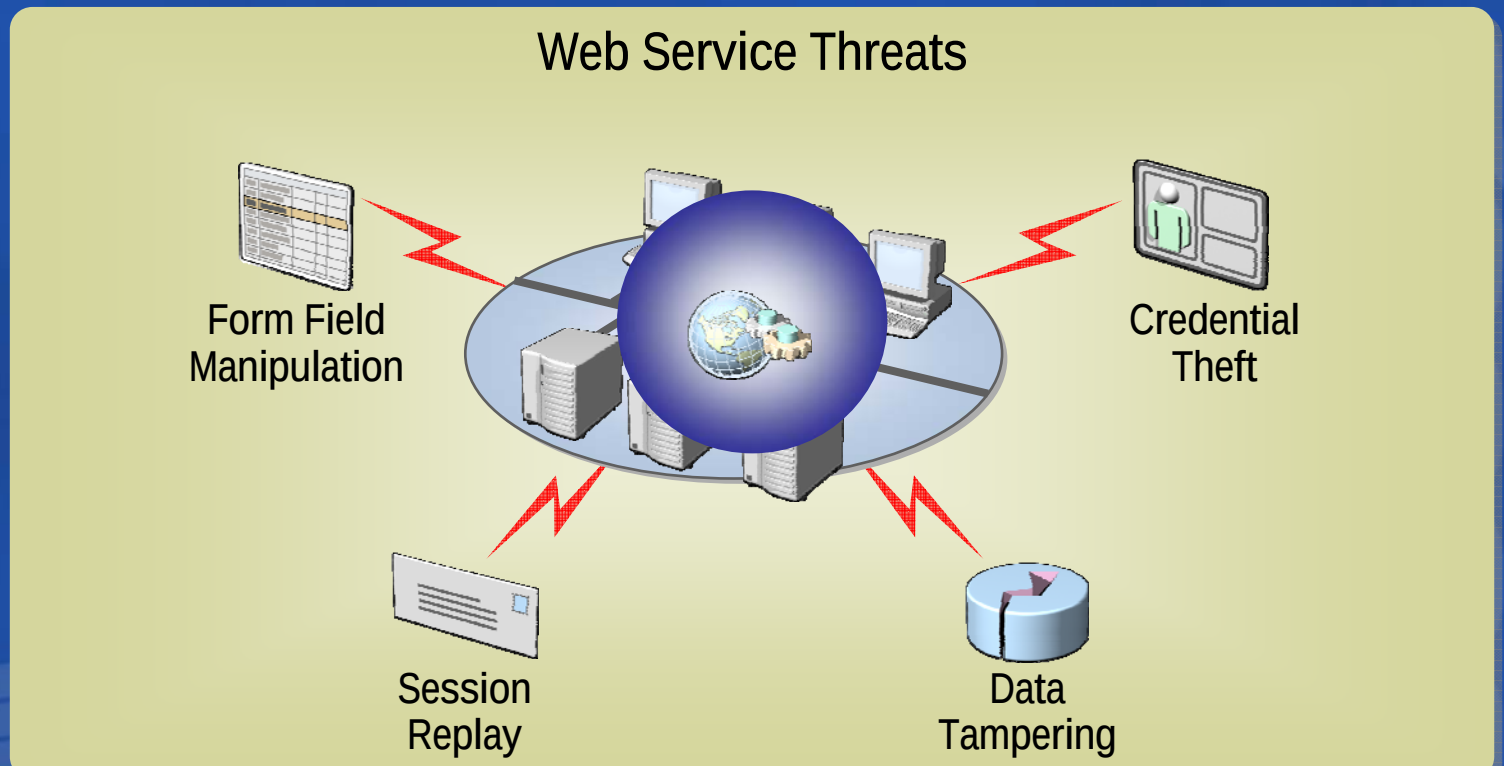
数据安全

- 能够通过身份管理和通讯策略来保护数据的安全
- 敏感数据还可以通过其他方式（比如加密，哈希）确保安全



Web Services的安全

Web service	应用程序的部分功能定义成公用接口放于网络上供调用，接口的定义和实现通过标准的XML实现



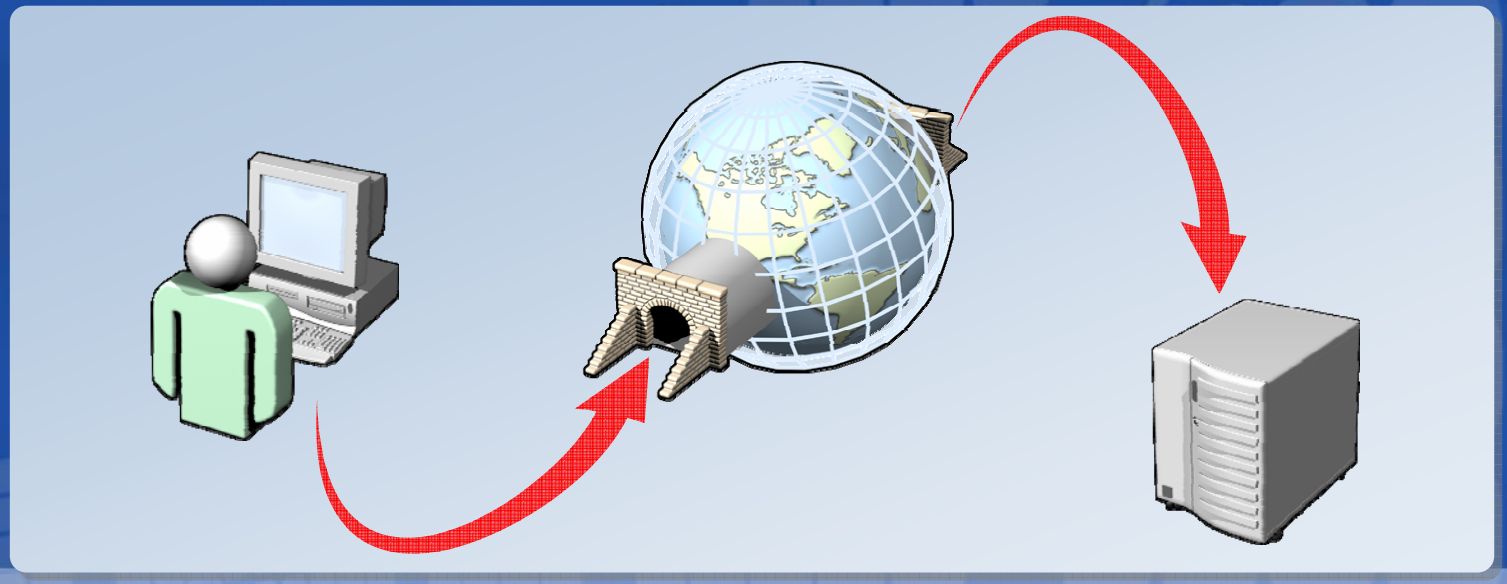
数据通讯安全实践

- 基于Internet 的应用安全简介
- 数据通讯安全实践
- 身份管理实践
- 基于Forms的认证
- Web Services 的安全实践

Virtual Private Network Tunnels

VPN Tunnel	在client computer和host computer之间提供加密信道，使得之间能够相互访问

- 允许外部用户访问内部的网络和资源
- 通过VPN连接拨入，通过硬件实现加密

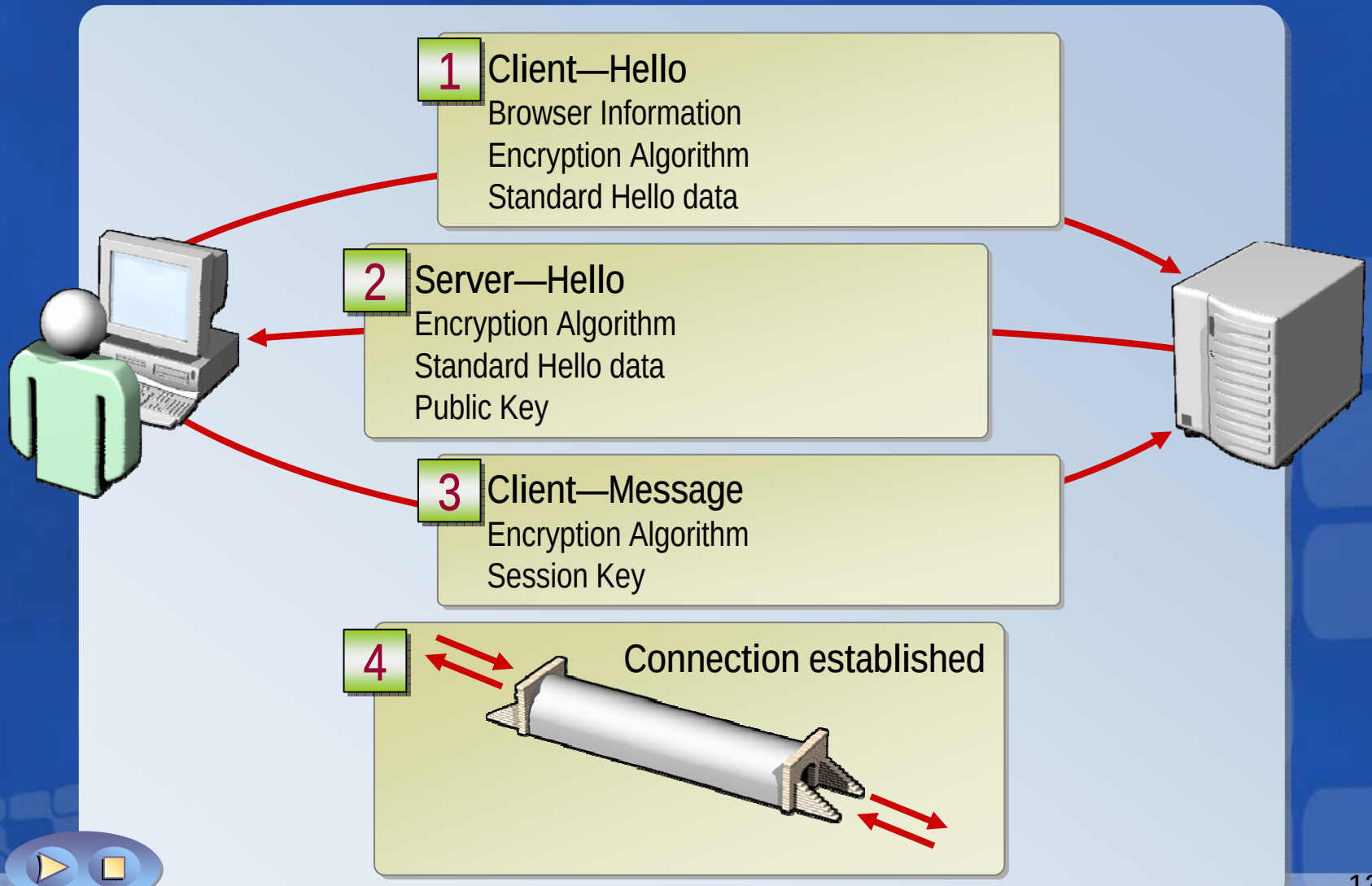


加密套接字协议层SSL

SSL	基于网络层的数据加密通讯协议

- 最常用的client-server加密通讯方式
- SSL is a layered approach
  - 工作与网络层与会话层之间的协议
  - 适用于大部分的应用程序
  - 使用asymmetric encryption 交换session keys， 当session建立后使用symmetric encryption数据通讯

SSL连接如何被建立


1
Client—Hello
Browser Information
Encryption Algorithm
Standard Hello data
2
Server—Hello
Encryption Algorithm
Standard Hello data
Public Key
3
Client—Message
Encryption Algorithm
Session Key
4
Connection established

Comparing Communication Strategies

	Advantages	Disadvantages
VPN	• Secure access • Additional application security not necessary	• VPN Client • Known user base • Not application specific
SSL	• Widely supported • Secure transmission	• Additional overhead • Certificate Authority

身份管理实践

- 基于Internet 的应用安全简介
- 数据通讯安全实践
- 身份管理实践
- 基于Forms的认证
- Web Services 的安全实践

Managing Identities in Internet Applications

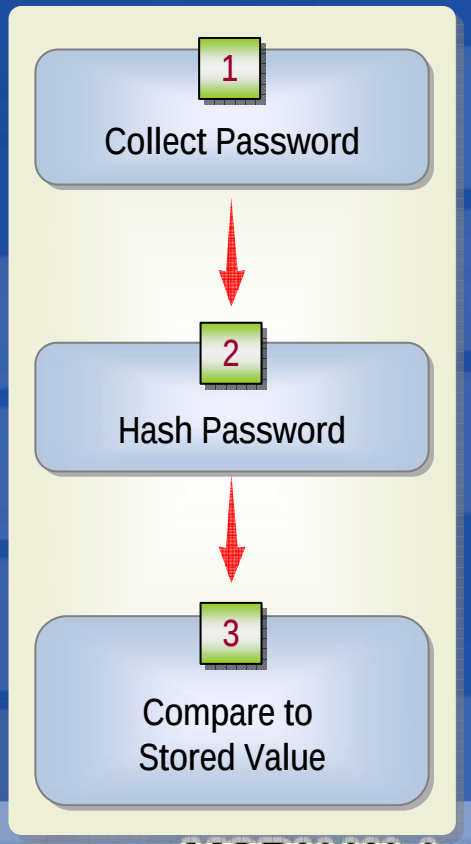
- Custom Databases require extra effort
- Platform directory and security services are preferred
- Use Active Directory rather than ADAM:
  - Richer authentication features
  - Richer authorization features
  - Support for cross-forest trusts
  - Additional connectivity

Do not invent identity stores within your application

Hashing and Password Storage

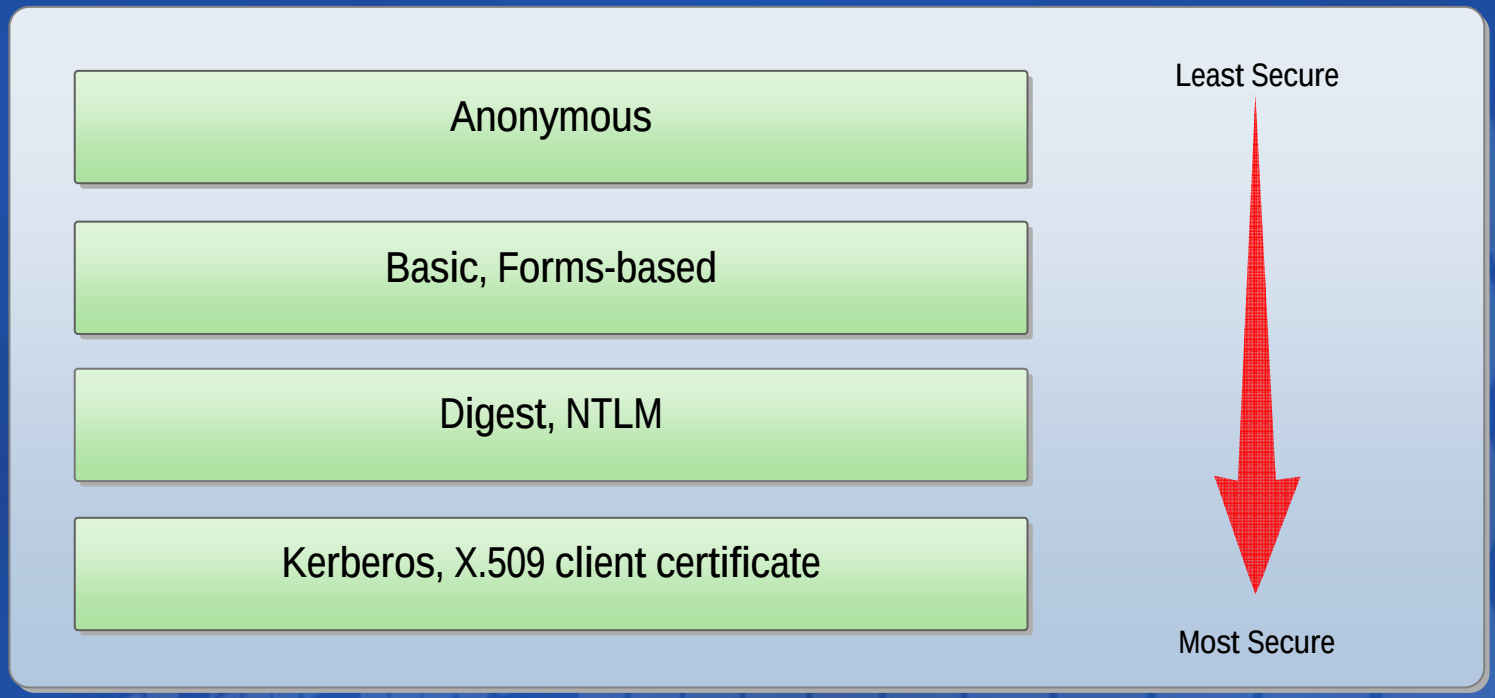
Hashing	一种数据转换算法，经过**Hashing**之后会产生一个特殊数值，原数据无法还原

- 经过hashing过数据的不可还原
- Hashing的常见用法:
  - Storing passwords
  - Ensuring transmitted data integrity

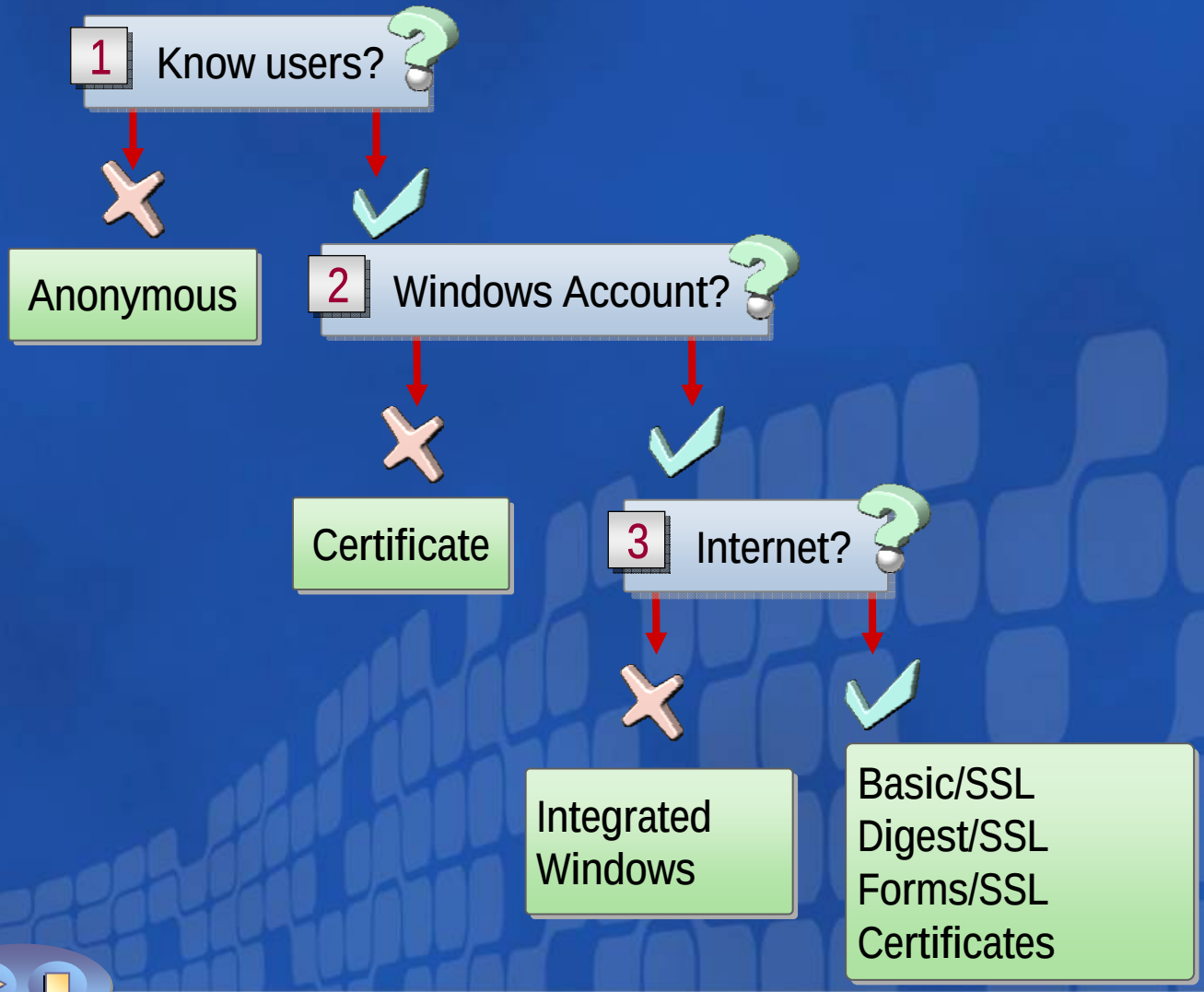


Authentication Options for Internet Applications

The following are common authentication methods for Internet applications:



Choosing an Authentication Method



Authorization Options for Internet Applications

Two options for authorization in Internet applications:

Access Control List - A list of security identities and actions—access control entries—that apply to an object

Role-based access control through Windows Authorization Manager

Best Practices for Identity Management

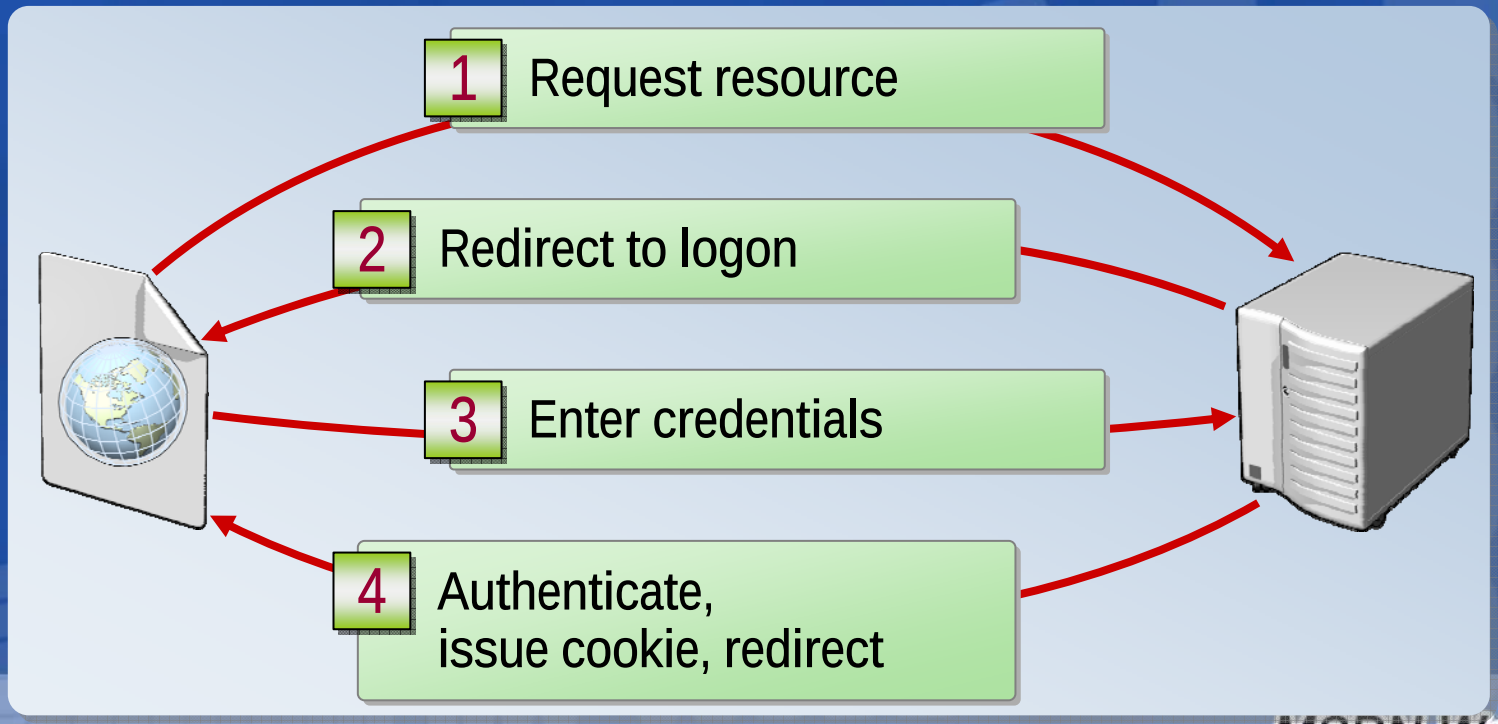
- Use Active Directory for your identity store
- Do not disclose sensitive information without authentication
- Only use security groups for authorization

基于Forms的认证

- 基于Internet 的应用安全简介
- 数据通讯安全实践
- 身份管理实践
- 基于Forms的认证
- Web Services 的安全实践

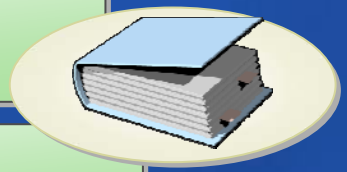
What Is Forms-Based Authentication?

- An ASP.NET authentication service providing custom authentication
- Uses cookies to store authentication token
- Client must support cookies or authentication will fail



Forms-Based Authentication with Active Directory

1. User submits credentials



2. Server looks up user in Active Directory
3. Server looks up user's group membership
4. Server authenticates user and creates a Forms Authentication ticket
5. Server encrypts authentication ticket
6. Server adds ticket to cookie and returns to client

Securing Forms-Based Authentication

- Use SSL when authenticating
- Use cookie expiration timers
- Do not trust browser to expire cookies
- Do not trust user input
  - Secure authentication cookies
  - Prevent SQL Injection

Securing Authentication Cookies

- Restrict authentication cookies to HTTPS connections
- Encrypt the cookie contents
- Limit cookie lifetime
- Do not persist authentication cookies
- Keep authentication and personalization cookies separate

```
<forms
    loginUrl="\Secure\Login.aspx"
    requireSSL="true"
    protection="all"
    timeout="10"
    slidingExpiration="false" … />
```

Preventing SQL Injection

- Never trust user input
- Never use dynamic SQL
- Never connect to a database using administrator-level account
- Divulge minimal information in exceptions
- Use parameterized queries or stored procedures

Validating Input

Look for valid data and reject everything else

Check length of string

```
bool CheckDomain(string name) {
if (8 != name.Length )
      { return false ; }
```

Validate first character is alphabetic

```
if (char.IsLetter(name,0))
      { return false; }
```

Check that the string does not contain any symbols

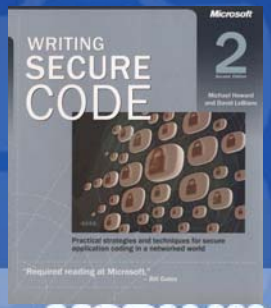
```
foreach(char foo in name)
      { if(char.IsSymbol(foo))
            {return false;} }
return true; }
```

Best Practices for Forms-Based Authentication

- Use SSL when authenticating
- Secure authentication cookies
- Prevent SQL injections

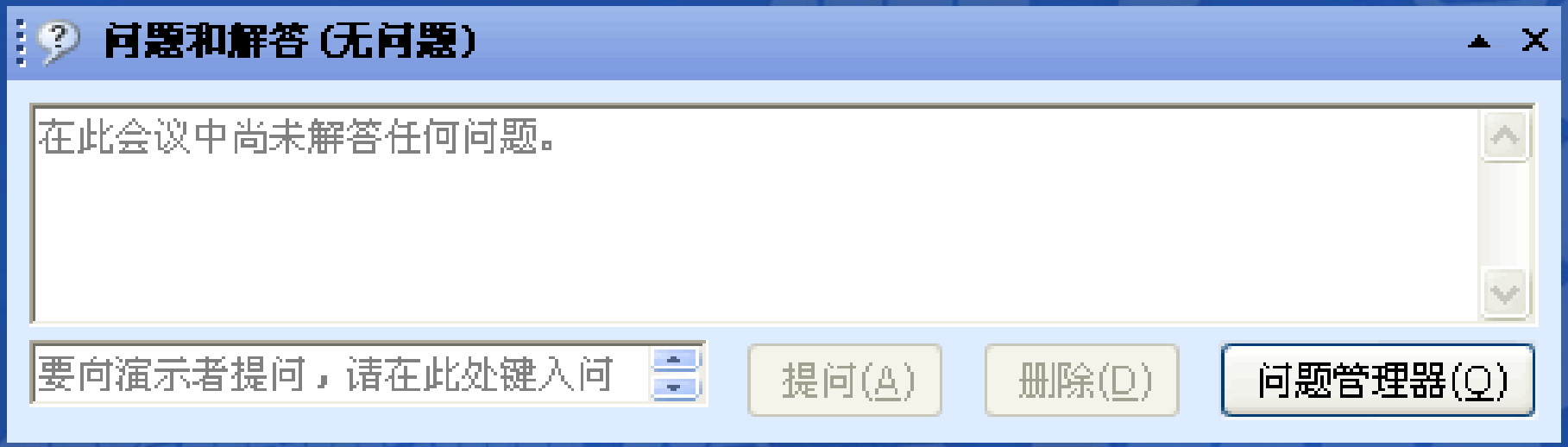
Next Steps

- “Active Directory® Services in Windows Server™ 2003”, available online at http://www.microsoft.com/technet/community/columns/profwin/pw0503.mspx
- “Introduction to Windows Server 2003 Active Directory Application Mode”, available online at http://www.microsoft.com/windowsserver2003/techinfo/overview/adam.mspx
- “Security briefs: Hashing Passwords, The AllowPartiallyTrustedCallers Attribute”, available online at http://msdn.microsoft.com/msdnmag/issues/03/08/SecurityBriefs
- The OASIS Web Services Security: SOAP Message Security 1.0 (WS-Security 2004) specification available online at http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf
- WS-SecurityPolicy, available online at http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnglobspec/html/ws-securitypolicy.asp
- WS-Trust, available online at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnglobspec/html/ws-trust.asp
- WS-SecureConversation, available online at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnglobspec/html/ws-secureconversation.asp



Question & Answer

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

msdn

MSDN Webcasts