您的潜力，我们的动力

Microsoft
微软（中国）有限公司

开发高安全级别的企业应用系列课程（之六）
WEB项目的的安全开发实践

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

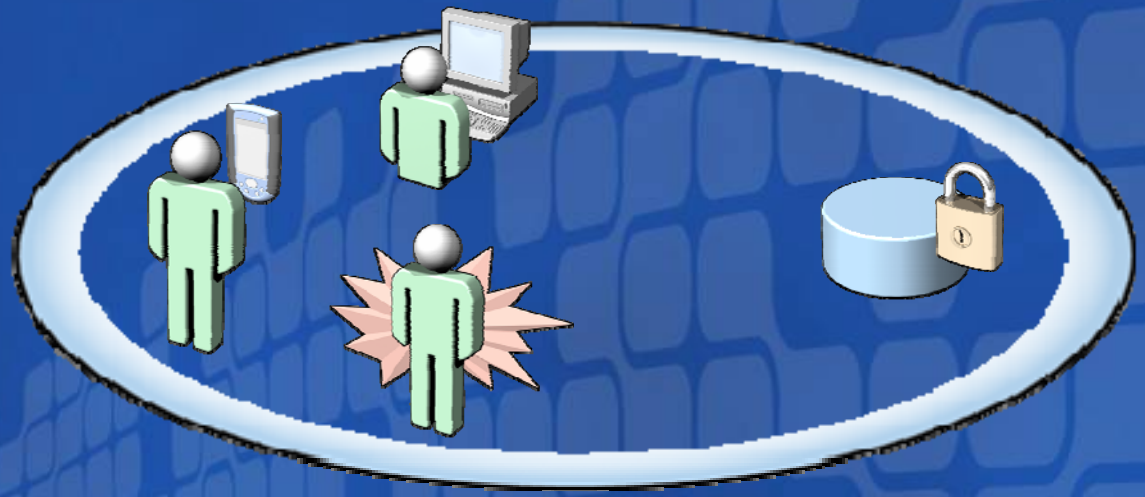
- 构建安全的Intranet 应用程序简介
- 保证数据安全的基本原则
- 身份管理
- Intranet应用程序的身份认证
- Intranet应用程序的授权访问

构建安全的Intranet 应用程序简介

- 构建安全的Intranet 应用程序简介
- 保证数据安全的基本原则
- 身份管理
- Intranet应用程序的身份认证
- Intranet应用程序的授权访问

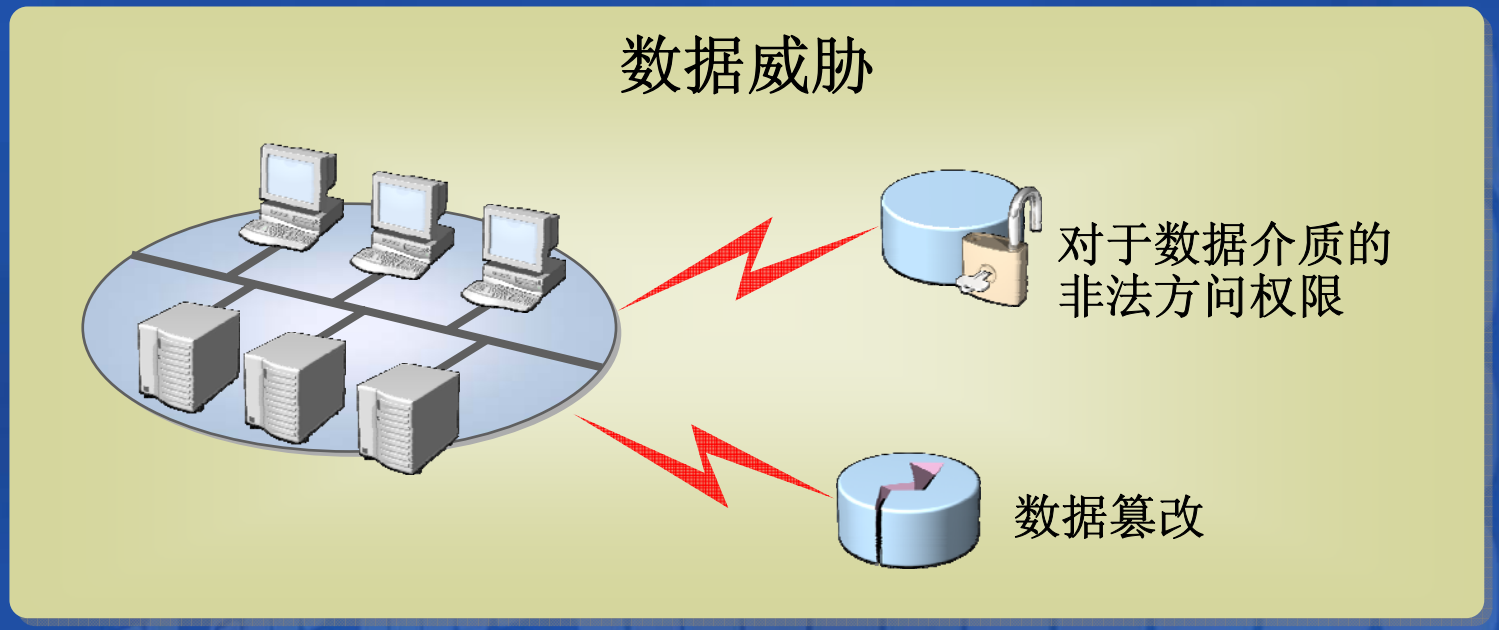
企业Intranet环境的几个特征

- 用户是已知的
- 数据私密程度高
- 最大的安全威胁来自于内部用户



数据安全

- 私密数据的安全存储
- 数据存储介质需要应对威胁



身份信息的存储

Identity Store	A repository that contains digital identities

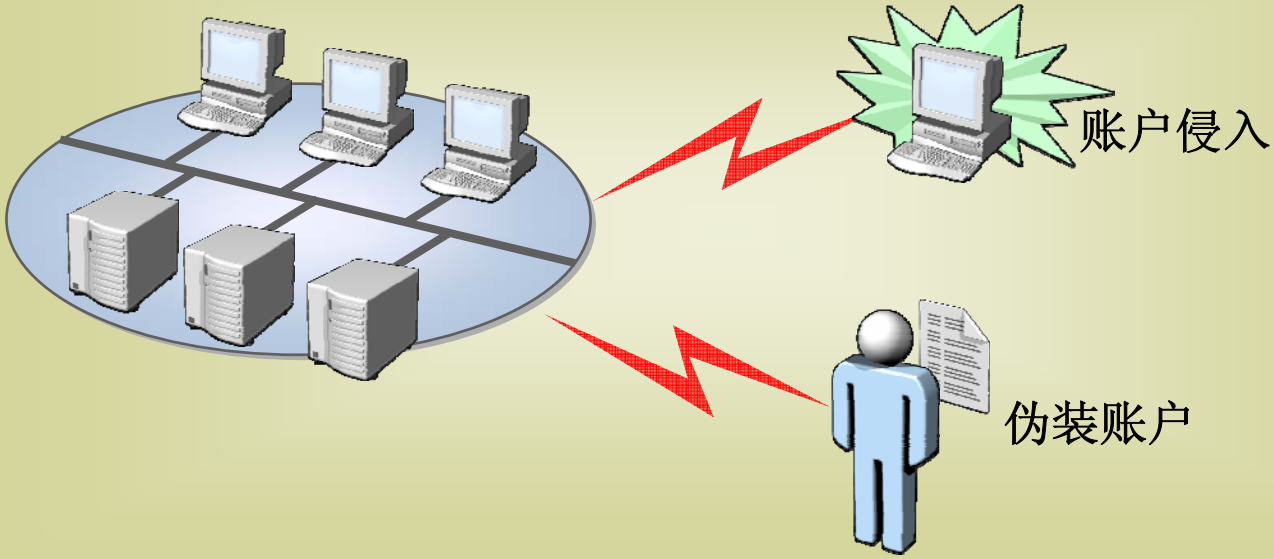
- Directory or database目录和数据库
- Centralized or distributed
- Well-defined schema
- Encryption or hashing加密或哈西

Directory目录	Database数据库
Active Directory ADAM Generic LDAP	SQL

身份认证

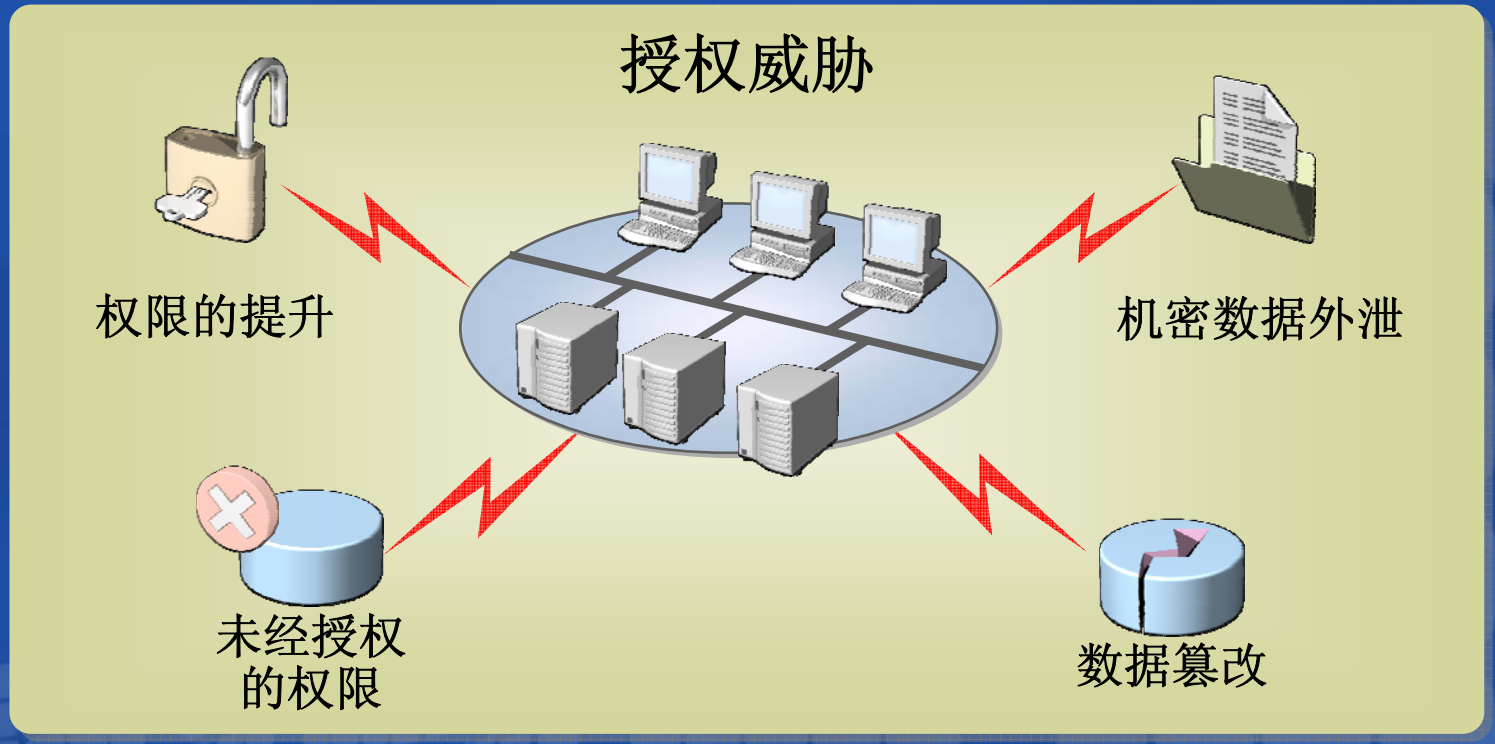
身份认证	A process that checks the credentials of a security principal against values in an identity store

身份认证威胁



授权

授权	通过授权可以配置用户对于资源访问权限

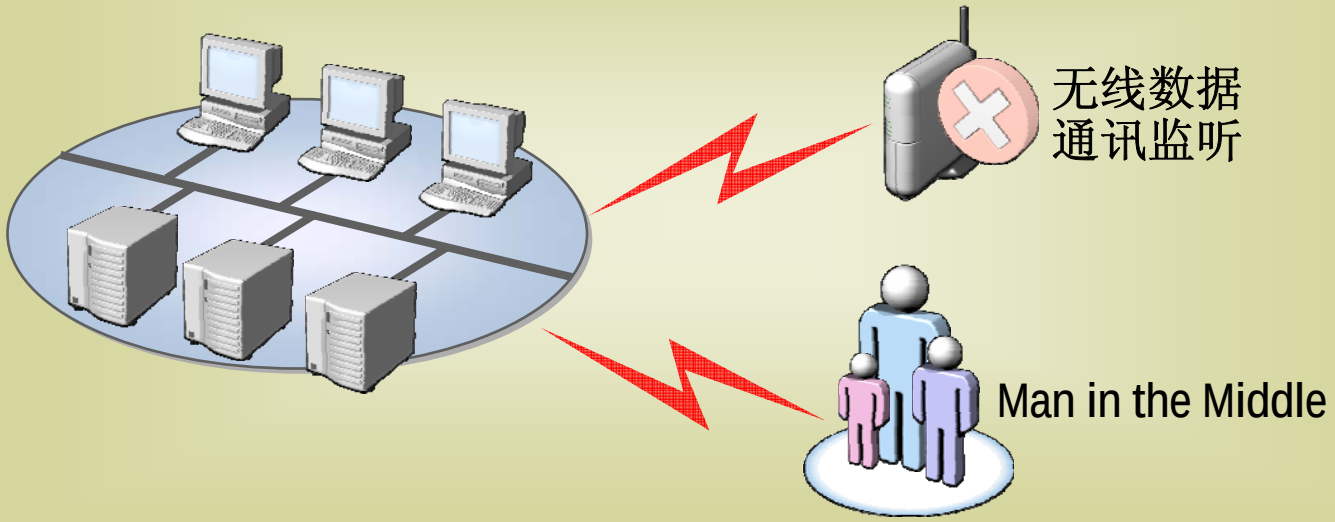


通讯安全

Securing Communication	确保服务器端和客户端的数据流传递安全

- 像应对Internet威胁一样处理Intranet应用威胁
- 使用SSL

通讯威胁



保证数据安全的基本原则

- 构建安全的Intranet 应用程序简介
- 保证数据安全的基本原则
- 身份管理
- Intranet应用程序的身份认证
- Intranet应用程序的授权访问

Data Security in Applications

- 数据安全需要达到如下要求:
  - 重视数据对于用户的私密性
  - 重要数据不被篡改或删除
  - 授权用户才有数据访问权
- 确保数据安全可通过:
  - 许可
  - 加密

数据安全和权限

Permissions	文件数据安全策略，是通过用户授权等级来限制访问

- 一般的，数据文件权限依托于以下:
  - Full control
  - Modify
  - Read & Execute
  - Read
  - Write

什么是加密

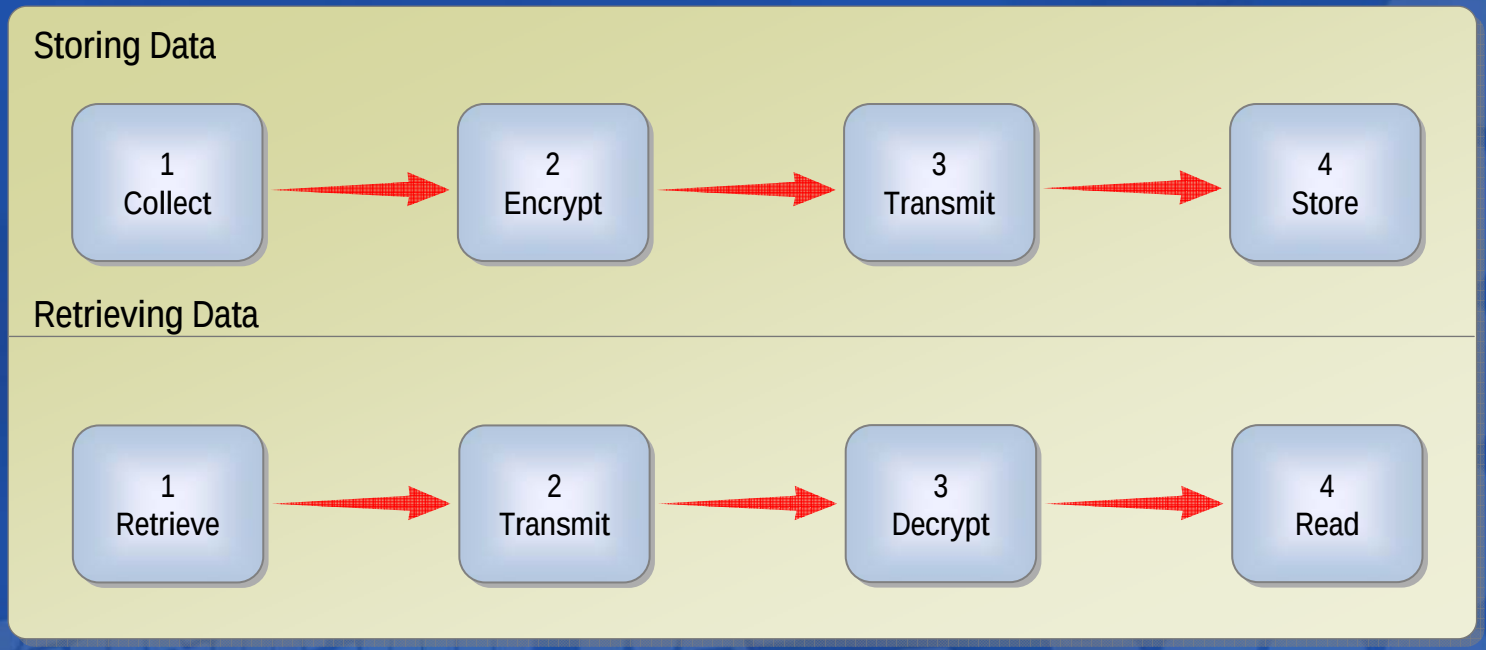
Encryption	A method of transforming data by passing it through a cryptographic function to generate data in a format that can read only by an entity that knows the specific decryption key and algorithm

- 2种主要的加密方式:
  - 对称加密
  - 不对称加密
- 相同的session中，2种方式可同时使用

不要自己创建加密方法，使用成熟的算法

数据的加密和解密

- 存储和传输私密数据时，使用加密手段
- Longer encryption key = Stronger encryption

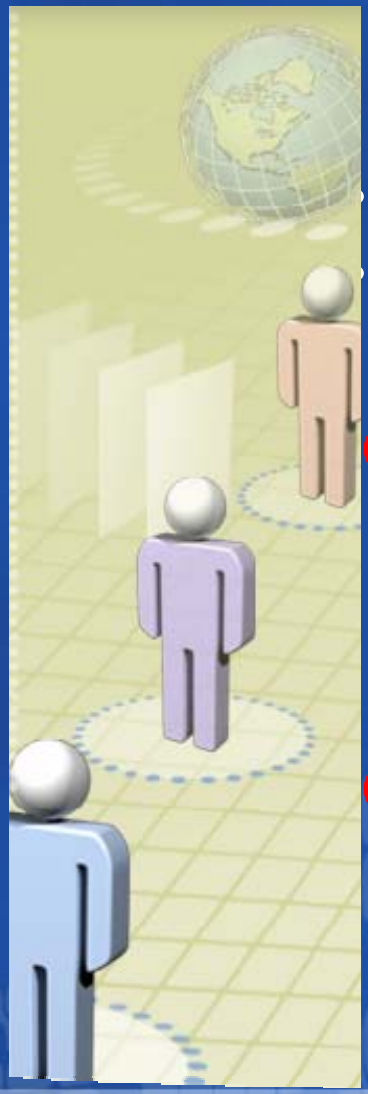


.NET Framework中提供的数据加密方式

电子签名	电子签名可被用来验证电子文档的证实性和完整性

对称算法	非对称算法
DES	DSA
TripleDES	RSA
Rijndael	
RC2	

Demonstration 1: Using .NET Framework Encryption



- Viewing and storing prices
- .NET Framework Encryption and Decryption API

`decryptPrice` function

`RijndaelManaged` Object
`CreateDecryptor().TransformFinalBlock` API

`encryptPrice` function

`RijndaelManaged` Object
`CreateEncryptor().TransformFinalBlock` API

数据安全的最佳实践

- 如果存储介质受到攻击，首先要确保私密数据的安全
- 经常更换密钥
- 使用现有的加密方式

身份管理

- 构建安全的Intranet 应用程序简介
- 保证数据安全的基本原则
- 身份管理
- Intranet应用程序的身份认证
- Intranet应用程序的授权访问

应用和身份信息的存储

应用

- 数字信息认证
- 访问权限评估

常见的企业内部身份信息存储在

- Active Directory
- ADAM
- SQL
- Generic LDAP

不要创建自己的身份信息存储

Access Management

控制用户的访问权限可通过：

- 身份认证
- Credential mapping
- 授权访问

Trust	A state that describes the agreements between different parties and systems for sharing identity information

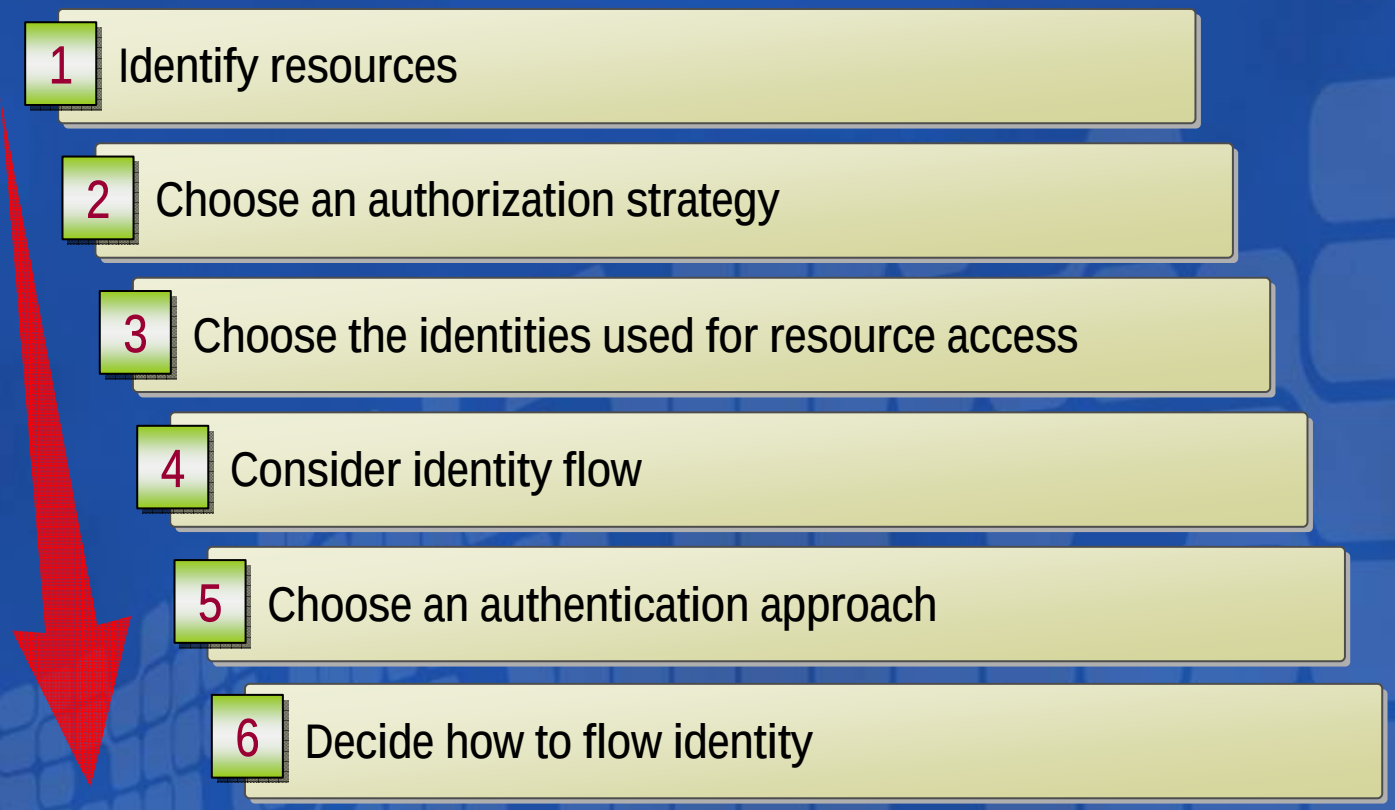
身份认证流程

Identity Flow	The action of passing identity information between resources

- 分布式环境下有3种用户认证模型:
  - Impersonation/delegation
  - Trusted subsystem
  - Credential mapping

权限管理策略的设置

以下展示一个认证流程，能帮助你如何为您的应用开发认证和授权策略:



身份管理的最佳实践

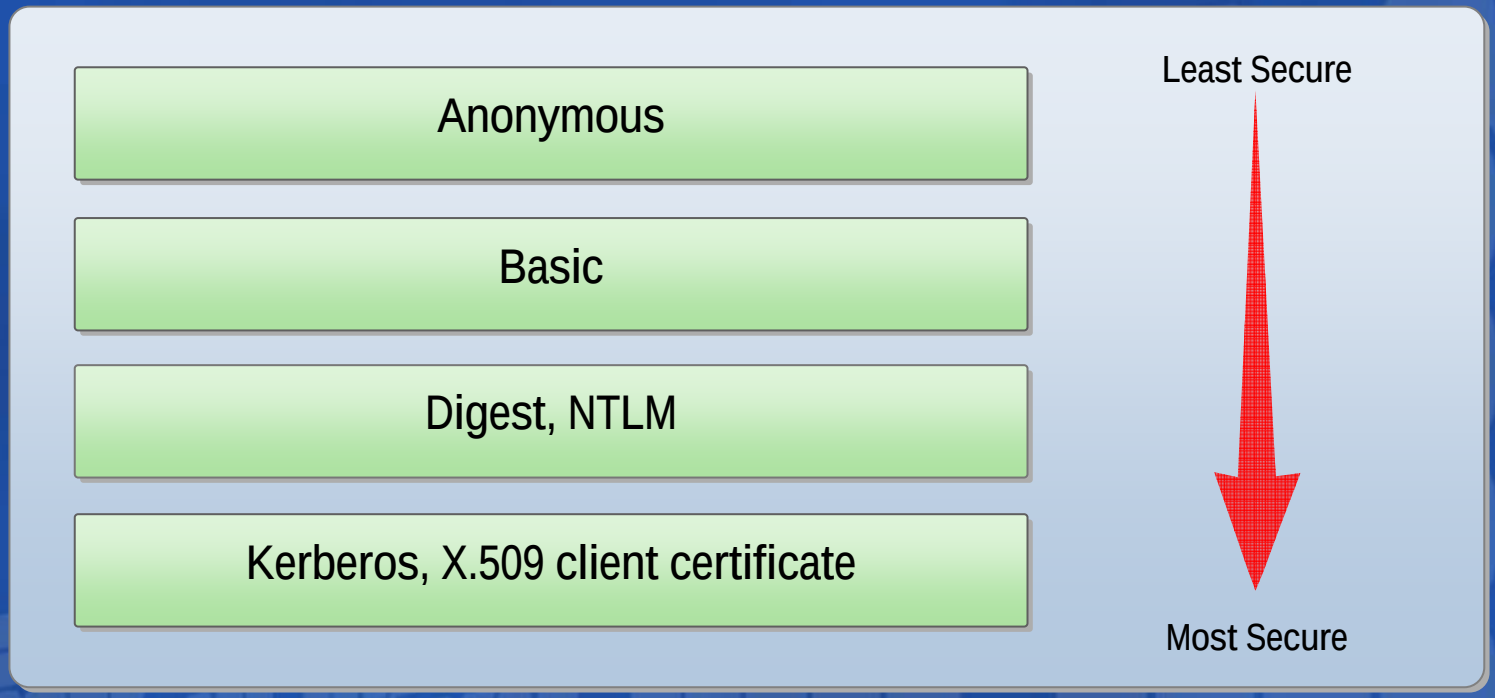
- Minimize the number of identity stores within your organization
- 使用**Active Directory**
- Use an identity store that exists rather than creating your own

Intranet应用程序的身份认证

- 构建安全的Intranet 应用程序简介
- 保证数据安全的基本原则
- 身份管理
- Intranet应用程序的身份认证
- Intranet应用程序的授权访问

Intranet 应用的身分认证选项

如下是常见的Intranet 应用的身分认证选项:

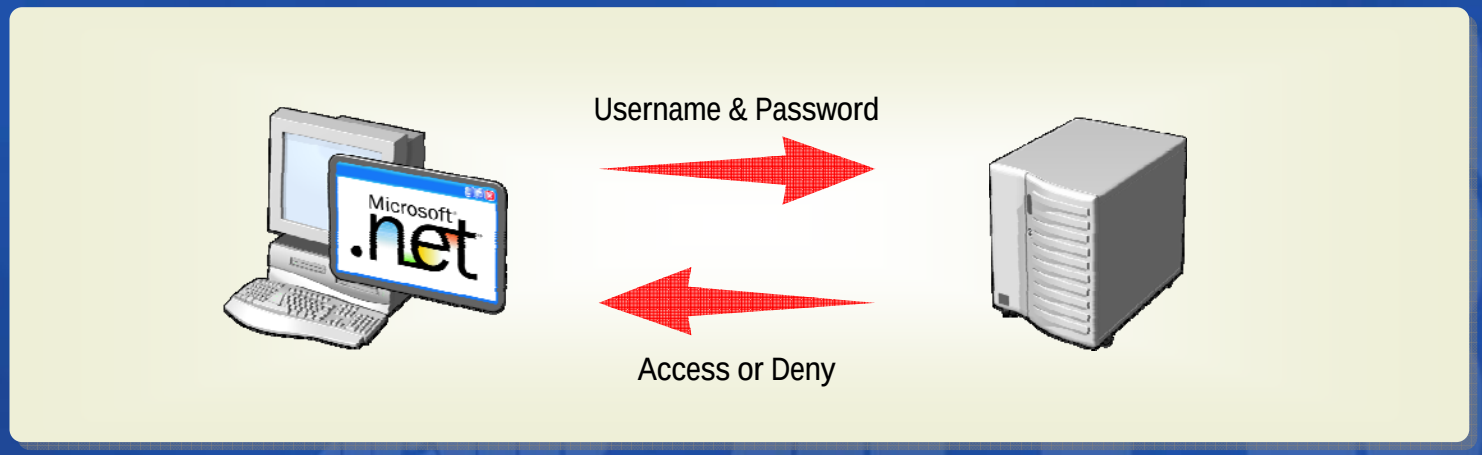


Anonymous 认证

- No authentication = Anonymous access
- Anonymous 方式不提供认证信息
- Anonymous 不存在安全性
- Anonymous给 用户只读权限

Basic 认证

- Specified in HTTP 1.0
- 不安全—密码给予 Base64 方式发送



Secure the authentication stream by using an SSL connection

Windows 集成认证方式

- 适用于intranet应用
- Kerberos 替代了 NTLM

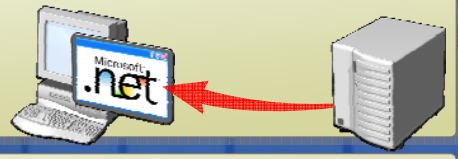
Kerberos	NTLM
Windows 2000 Server	Windows NT Server
Windows Server 2003	Windows 2000 Server
	Windows Server 2003

Digest 认证和 NTLM

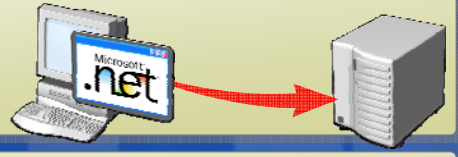
- Digest credentials: user name & hashed password
- NTLM credentials: domain name, user name, & hashed password

Does not secure the data stream

1. Challenge with code

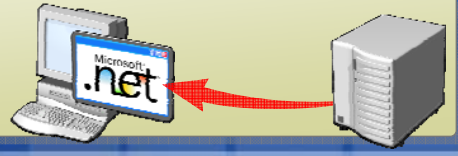


2. User name and hashed password



3. Compares hashed password

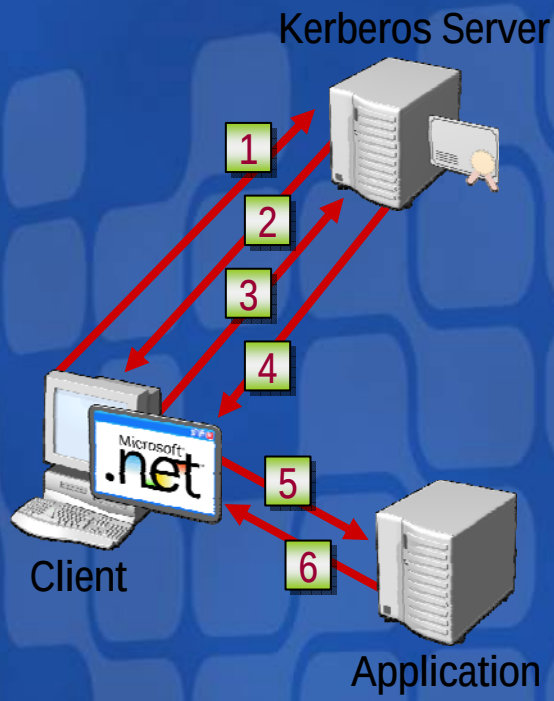
4. Access or deny access

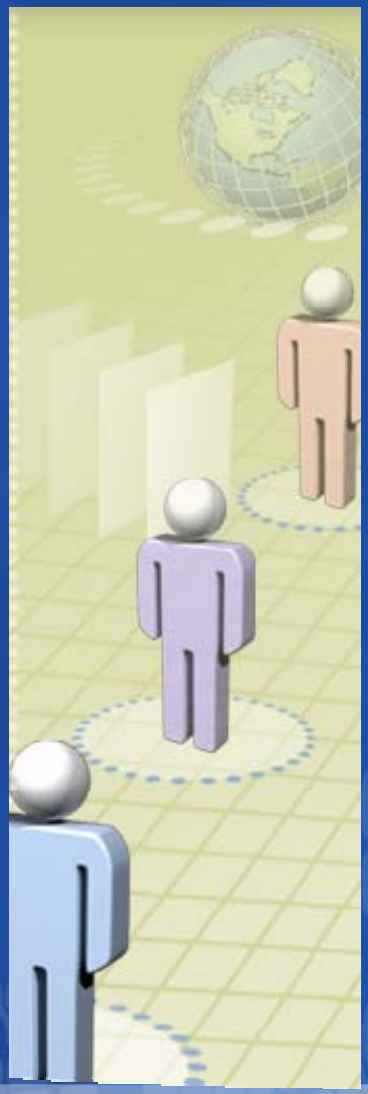


Kerberos 认证

- 基于公钥和数字证书
- Windows 提供身份验证服务

1. Client requests a client ticket
2. Kerberos server replies with ticket
3. Client requests session ticket to application
4. Kerberos server replies with ticket
5. Client sends tickets to application
6. Application sends validation (optional)





Demonstration 2: Using Windows Integrated Authentication

Using Windows Integrated Authentication

Open
`web.config`

```
<authentication mode = "Windows" />
```

IIS Manager

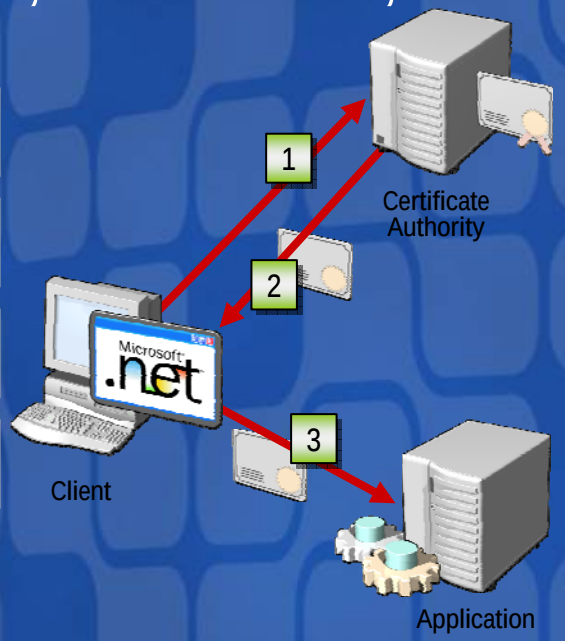
Properties

Directory Security

X.509 Client Authentication

- Requires the exchange of digital certificates
  - Level of security is related to contents of certificate
- Trusted certificate authority issues certificate
- Commonly used in extranet access, not intranet, access

1. Client requests certificate from authority
2. Certificate authority replies with certificate
3. Client sends certificate to application
4. Application decodes certificate



关于认证的最佳实践

- ✓ 使用SSL确保认证信息安全
- ✓ 确保数据流安全
- ✓ 在 intranet applications中使用**Windows** 集成认证方式

Intranet应用程序的授权访问

- 构建安全的Intranet 应用程序简介
- 保证数据安全的基本原则
- 身份管理
- Intranet应用程序的身份认证
- Intranet应用程序的授权访问

Intranet 应用的授权选项

提供2种授权选项:

- **Access control list -** A list of security identities and actions—access control entries—that apply to an object
- Role-based access control

Access Control Lists

- Discretionary ACL (DACL) **- identifies the trustees that are allowed or denied access to a securable object**
- System ACL (SACL) **- enables administrators to log attempts to access a secured object**
- Use APIs to write ACLs; do not try to manipulate them directly

Impersonation

- Authentication package authenticates and builds security context

Impersonation	Taking on the identity of another entity in order to access resources with that entity's security context

- Application or service uses the security context to impersonate the user

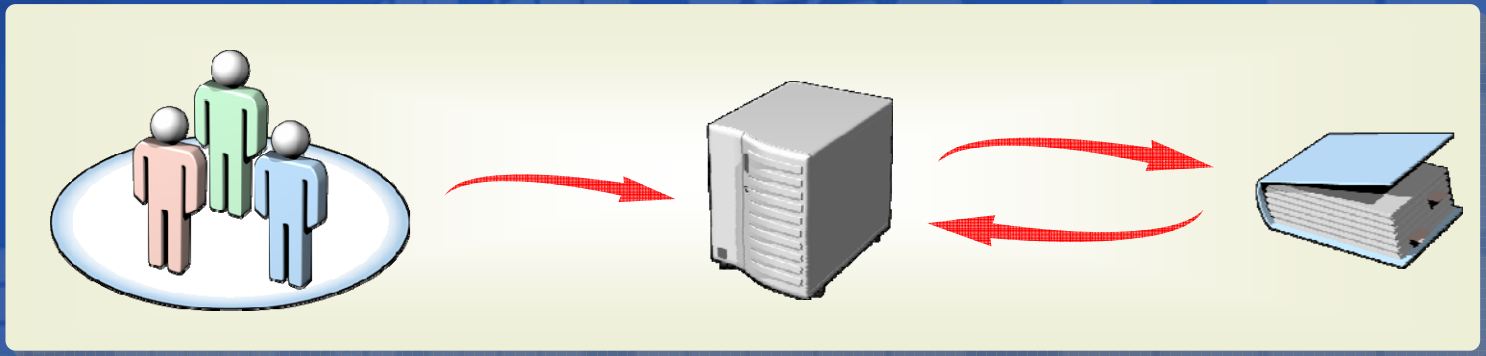
Role-Based Authorization Control

- A user-centric authorization model that controls access in terms of the organizational structure of a company
- Permissions are granted based on high-level abstractions
- Role-based access control groups are similar to groups in Active Directory

Role	Set of tasks or operations to which a category of users requires access Or Set of users and groups that fit into that category

Authorization Manager

- Provides role-based security which is scalable, flexible, and easy to implement
- Stores authorization policy in Active Directory or XML files
- Applies authorization policy at run time



Using Role-Based Access in Applications

At application development time:

- Identify roles, implement operations, roll the operations into tasks

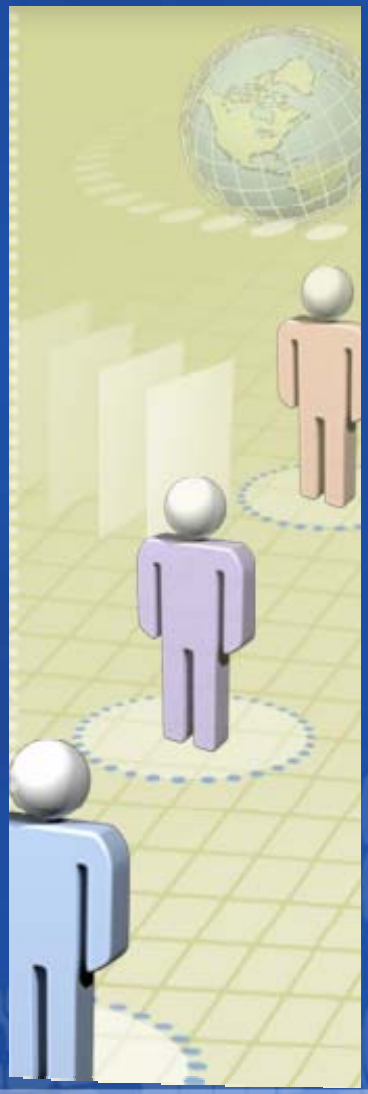
At installation time:

- Call appropriate APIs to create Authorization Store

At run time:

- Initialize Authorization Manager to connect to the Authorization Store
- When client connects, execute custom behavior based on roles

Demonstration 3: Authorizing Users with AzMan



Viewing Content Restricted by AzMan

Configuring AzMan

AzMan Code

Import
`Microsoft.Interop.Security.AzRoles`

Collect user identity

Determine users rights

Set display visibility

关于授权的最佳实践

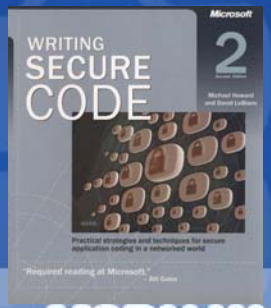
- Use .NET Framework APIs to write ACL information
- 贯彻最小特权的原则
- 是基于角色的授权

课程总结

- 使用现有成熟的加密方式确保数据安全
- 使用**Active Directory**
- 使用**Windows**集成认证方式
- 使用给予角色的授权方式

Next Steps

- Stay informed about security
  - Microsoft Developers Network Security Center
    http://msdn.microsoft.com/security/
  - Microsoft Security Guidance
    http://www.microsoft.com/security/guidance/
- Get additional security training
  - Find online and in-person training seminars:
    http://www.microsoft.com/seminar/events/security/
- Read the book: Writing Secure Code
  - Michael Howard and David LeBlanc
  - ISBN: 0-7356-1722-8



获取更多MSDN资源

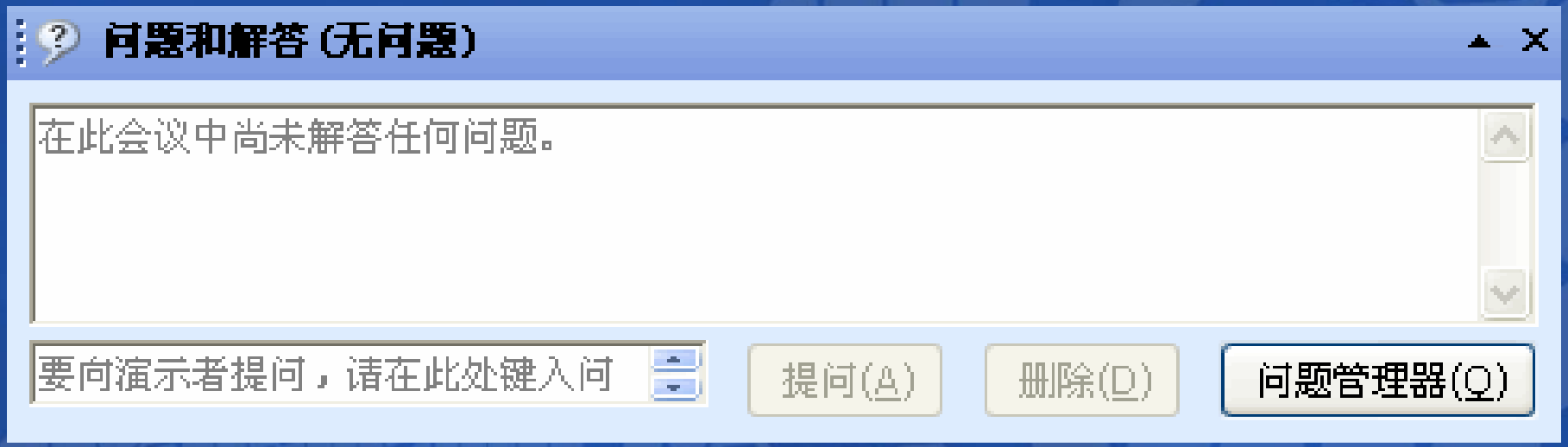
您的潜力，我们的动力

Microsoft
微软（中国）有限公司

- **MSDN中文网站**
  http://www.microsoft.com/china/msdn
- **MSDN中文网络广播**
  http://www.msdnwebcast.com.cn
- **MSDN Flash**
  http://www.microsoft.com/china/newsletter/case/msdn.aspx
- **MSDN开发中心**
  http://www.microsoft.com/china/msdn/DeveloperCenter/default.mspx

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。



Microsoft®

您的潜力，我们的动力