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 （十三）
系列课程总结

钟卫

Msdn讲师

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 300-400

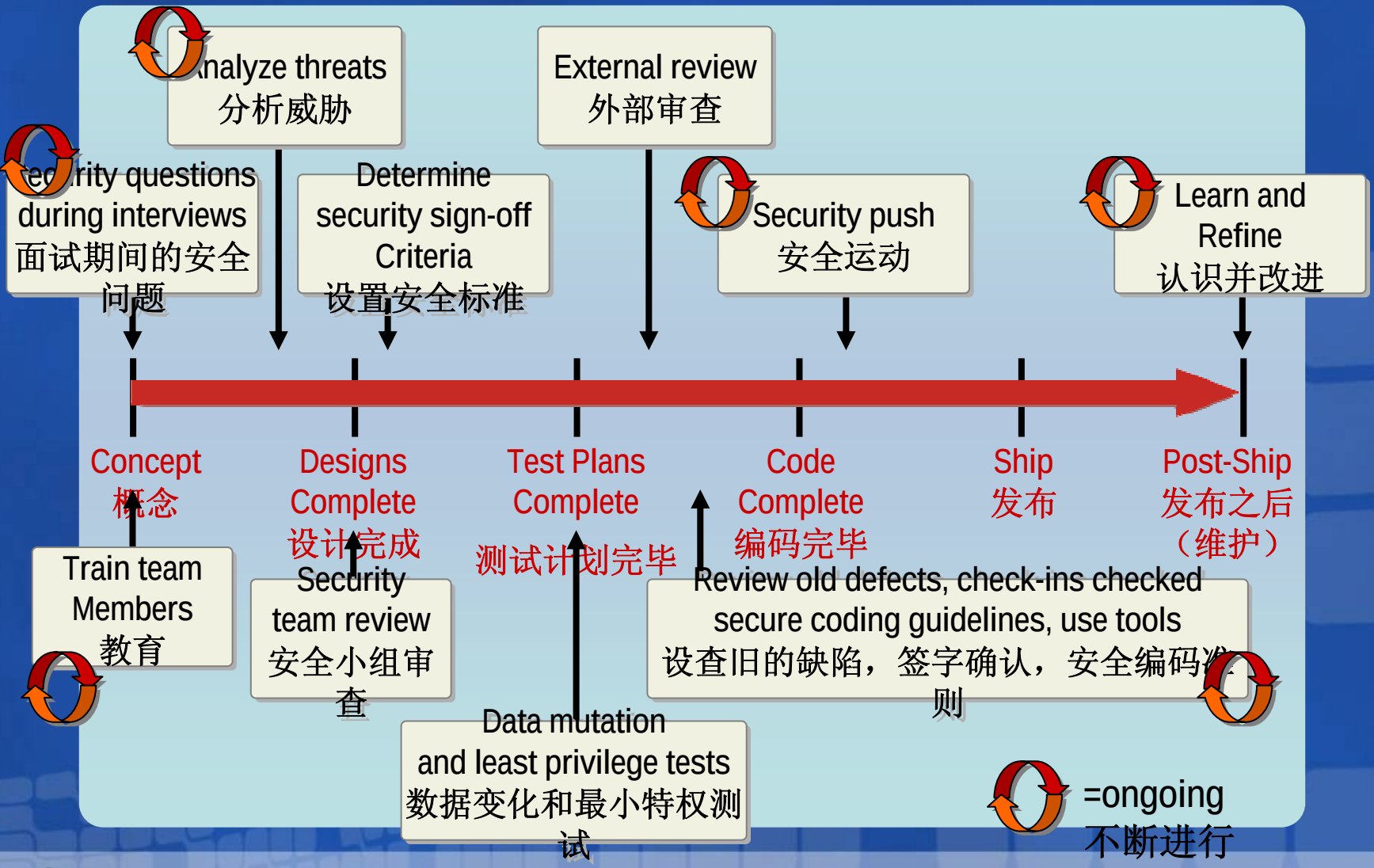
课程概述

- 安全开发生命周期
- .NET Framework 安全特性及代码访问安全
- 常见攻击手段
- 常见安全策略
- WSE

安全开发生命周期

- 安全开发生命周期
- .NET Framework 安全特性及代码访问安全
- 常见攻击手段
- 常见安全策略
- WSE

Security Throughout Project Lifecycle
项目生命周期各个环节的安全问题



安全教育

安全教育是整个生命周期的核心内容

- 团队培训
- 不断更新的培训

为什么？

- 意识和行动的转变
- 经过培训会对错误更敏感

威胁建模

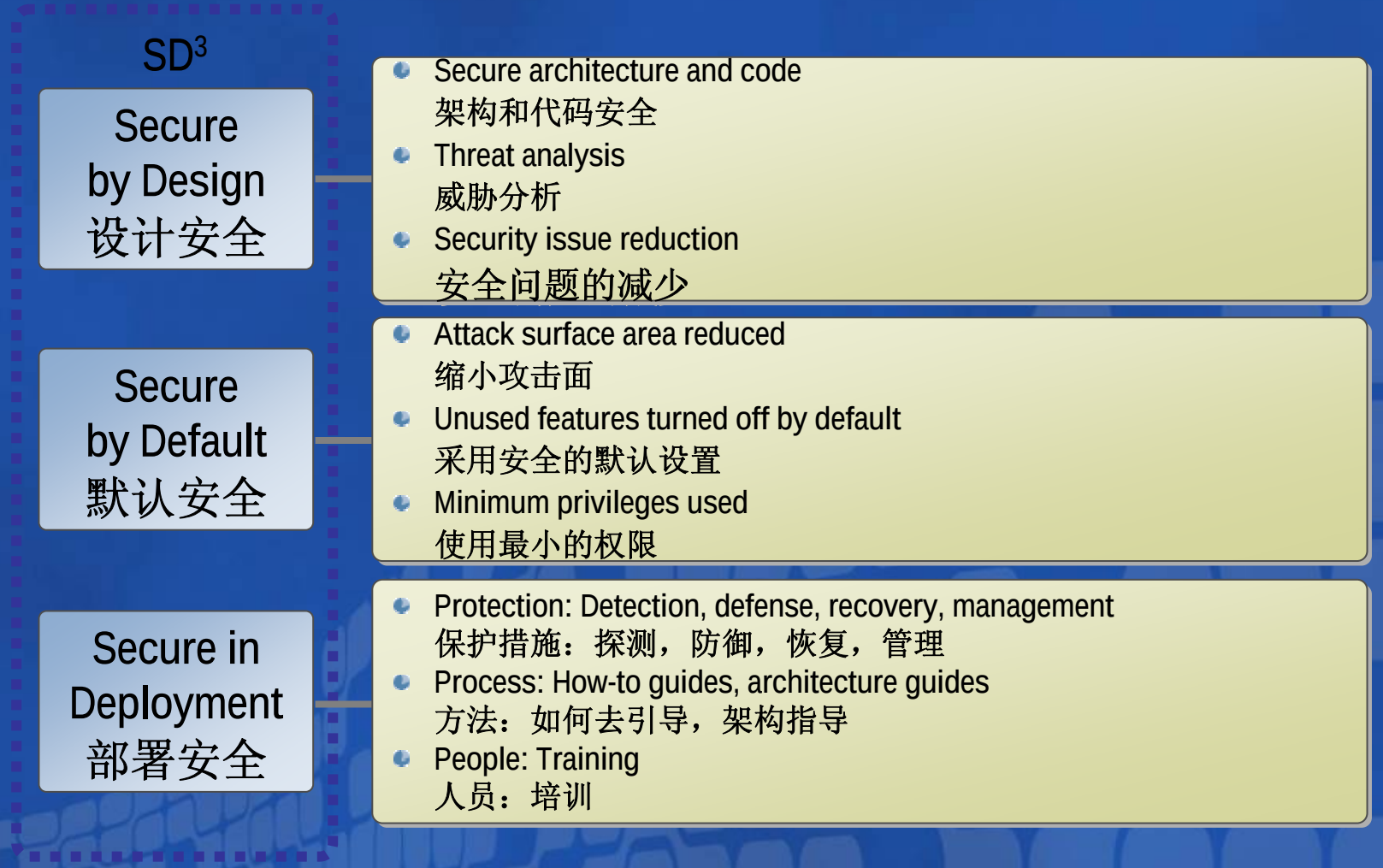
威胁建模是基于安全角度对程序的分析:

- 确定和评估威胁
- 找到保护资源
- 确定产品的弱点
- 基于安全规范进行开发

S	spoofing identity
T	tampering with data
R	repudiation
I	information disclosure
D	denial of service
E	elevation of privilege

D	damage potential
R	reproducibility
E	exploitability
A	affected users
D	discoverability

SD3安全框架


SD3
Secure by Design 设计安全
Secure by Default 默认安全
Secure in Deployment 部署安全
Secure architecture and code
架构和代码安全
Threat analysis
威胁分析
Security issue reduction
安全问题的减少
Attack surface area reduced
缩小攻击面
Unused features turned off by default
采用安全的默认设置
Minimum privileges used
使用最小的权限
Protection: Detection, defense, recovery, management
保护措施：探测，防御，恢复，管理
Process: How-to guides, architecture guides
方法：如何去引导，架构指导
People: Training
人员：培训

Practices for Improving Security
提高应用程序安全的各种实践

您的潜力，我们的动力
Microsoft
微软（中国）有限公司

Practice	Benefit
Adopt threat modeling 采用威胁建模	• **Identifies security issues** **确定安全问题** • **Increases awareness of application architecture** **提高应用程序架构的安全意识**
Train development team 培训开发团队	• **Avoids common security defects** **避免常见的安全问题** • **Correct application of security technologies** **如果使用安全技术纠正程序**
Code review 代码复审	• **Secures code that** –Accesses the network 网络访问 –Runs by default 默认环境运行 –Uses unauthenticated protocols 使用不安全的协议 –Runs with elevated privileges 最小权限运行
Use tools 工具的使用	• **More consistent testing for security issues** **对于安全问题持续的测试**
Use infrastructure solutions 使用基础的解决办法	• **More secure with SSL/TLS and IPSec** **使用SSL/TLS and IPSec进行加密**
Use component solutions 使用组件的解决方案	• **More robust with CAPICOM and .NET Cryptography namespace** **多使用CAPICOM 和引用.net里的Cryptography 名字空间**
Migrate managed code 移植托管代码	• **Avoids common security issues** • **避免常见的安全问题**

msdn
MSDN Webcasts

安全审查

- 内部审核
  - 找一个安全专家作审核
  - 代码应该被多个开发者审核
  - 只有通过审核的代码能做迁入
- 外部审核
  - 找到一个第三方机构审核代码
  - 确保外面审核不会做官样文章，造成安全上的假相

常见代码错误

- 不使用最小权限
- 依赖客户端验证
- 使用低的安全策略

安全运动

- 约定一个时间
- 确保Team全部人员的参加
- 设置目标
  - 提高安全意识
  - 改正坏的习惯
  - 寻找和修补问题
- 相对于项目时间更动关注开发驱动

安全代码规范

- 安全规范体现在代码的编写和审核阶段：
- 代码规范的种类
  - 通用的
  - 和数据库
  - 加密和私密数据管理
  - 托管代码
- 代码规范需要经常更新

.NET Framework 安全特性及代码访问安全

- 安全开发生命周期
- .NET Framework 安全特性及代码访问安全
- 常见攻击手段
- 常见安全策略
- WSE

.NET 托管代码的执行安全

- .NET Framework 安全特性
  帮助您开发更加安全的应用
  - 内置很多的安全组件
    - 类型察看
    - 异常管理
    - 安全引擎
  - 与Windows 的安全性相互补充
  - 具备很高的灵活性和扩展性

A Type-Safe System
类型安全的系统

- Type-safe code:
  类型安全代码
  - Prevents buffer overruns
    防范缓冲区溢出
  - Restricts access to authorized memory locations
    授权方式限制访问内存
  - Allows multiple assemblies to run in the same process
    允许相同进程运行多程序集
- App Domains provide:
  应用程序域提供：
  - Increased performance
    性能增强
  - Increased code security
    代码安全性的增强

基于证据的安全机制

- 证据:
  - 当程序集被访问时评估证据
  - 被用于确定程序集所具有的权限
  - 包含了程序集的:
    - 强命名信息
    - URL（可信，非可信）
    - Zone（安全区域）
    - 可信的代码签名
    - 用户自定义信息

安全策略

Security entity	Description
Policy	• **Is set by administrators** • **Is enforced at runtime** • **Simplifies administration** • **Contains permissions** • **Contains code groups**
Code group	• **Associates similar components** • **Is evidence based** • **Is linked to permission set(s)**
Permission set	• **Is a set of granted permissions**

常见攻击手段

- 安全开发生命周期
- .NET Framework 安全特性及代码访问安全
- 常见攻击手段
- 常见安全策略
- WSE

常见攻击手段

- Defending Against Memory Issues
- Defending Against Cross-Site Scripting
- Defending Against SQL Injection
- Defending Against Cryptography Weaknesses
- Defending Against Unicode Issues

Cross-Site Scripting常见的攻击方式

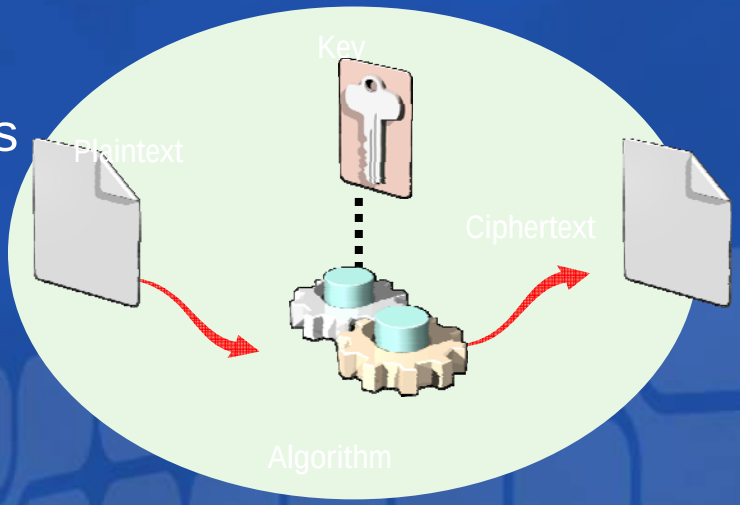
- Attacking Web-based e-mail platforms and discussion boards
- Using HTML <form> tags to redirect private information

什么是 SQL Injection?

- SQL injection is:
  - The process of adding SQL statements in user input
  - Used by hackers to:
    - Probe databases
    - Bypass authorization
    - Execute multiple SQL statements
    - Call built-in stored procedures

Cryptography Weaknesses

- Inappropriate use of algorithms
  - Creating your own
  - Using weak ones
  - Incorrect application
- Failure to keep keys secure
  - Insecure storage
  - Extensive duration of use
- The human factor



Unicode Issues

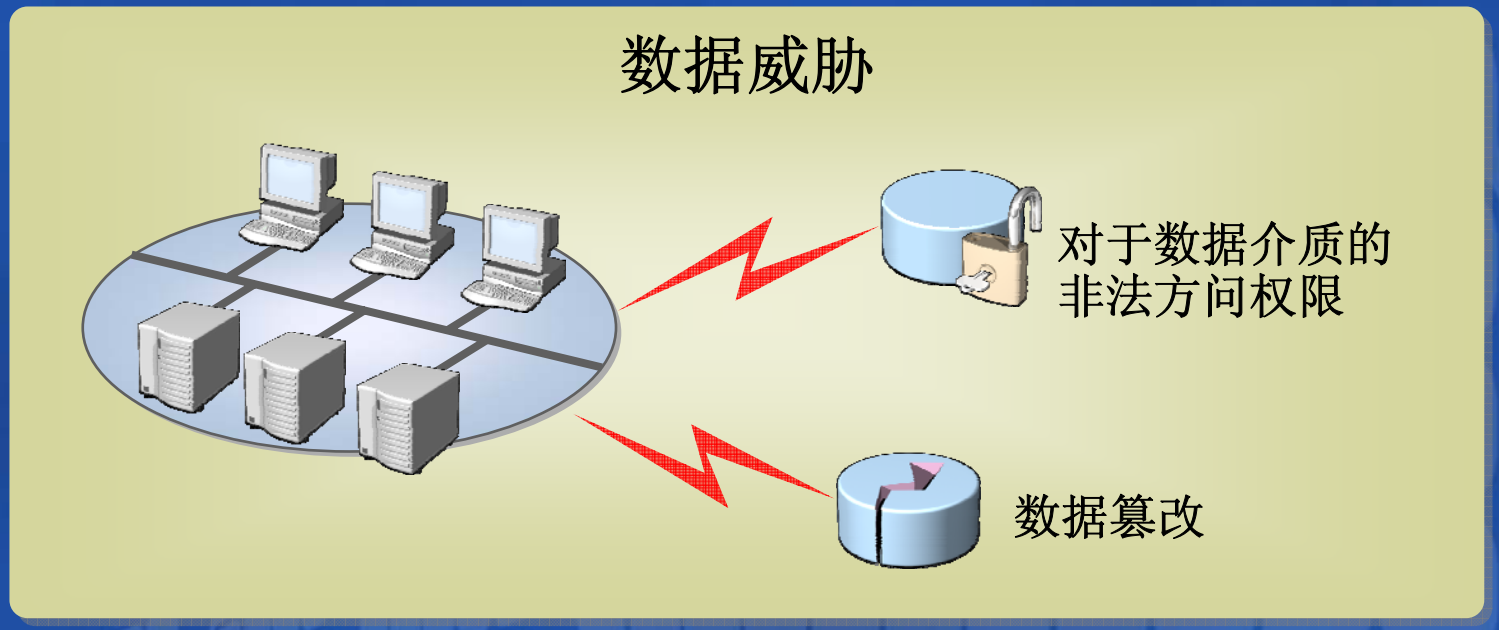
- Common mistakes
  - Treating a Unicode character as a single byte
  - Miscalculating required buffer size
  - Misusing **MultiByteToWideChar**
  - Validating data before conversion, but not afterward
- Results
  - Buffer overruns
  - Potentially dangerous character sequences slipping through your validation routines

常见安全策略

- 安全开发生命周期
- .NET Framework 安全特性及代码访问安全
- 常见攻击手段
- 常见安全策略
- WSE

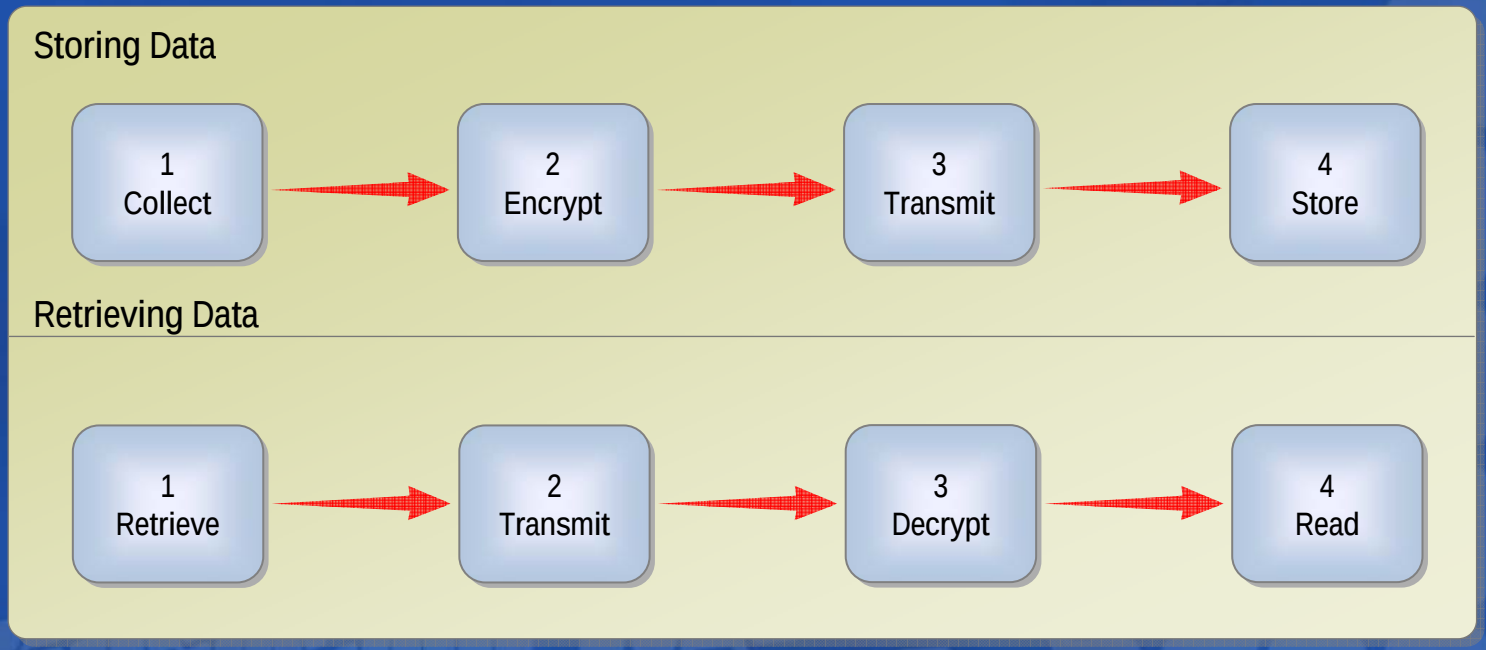
数据安全

- 私密数据的安全存储
- 数据存储介质需要应对威胁



数据的加密和解密

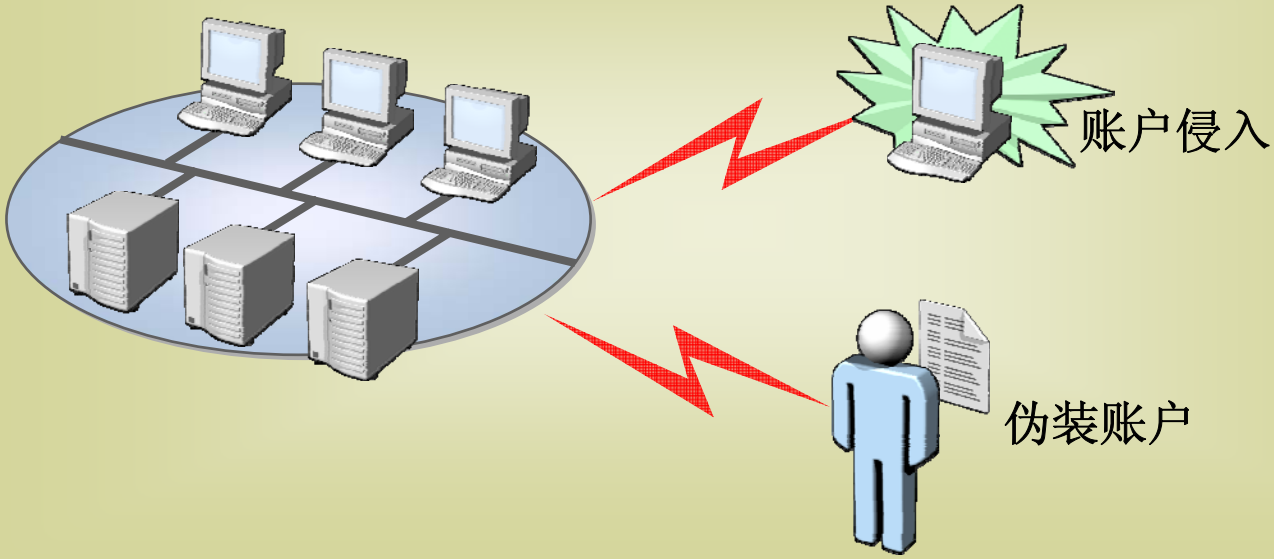
- 存储和传输私密数据时，使用加密手段
- Longer encryption key = Stronger encryption



身份认证

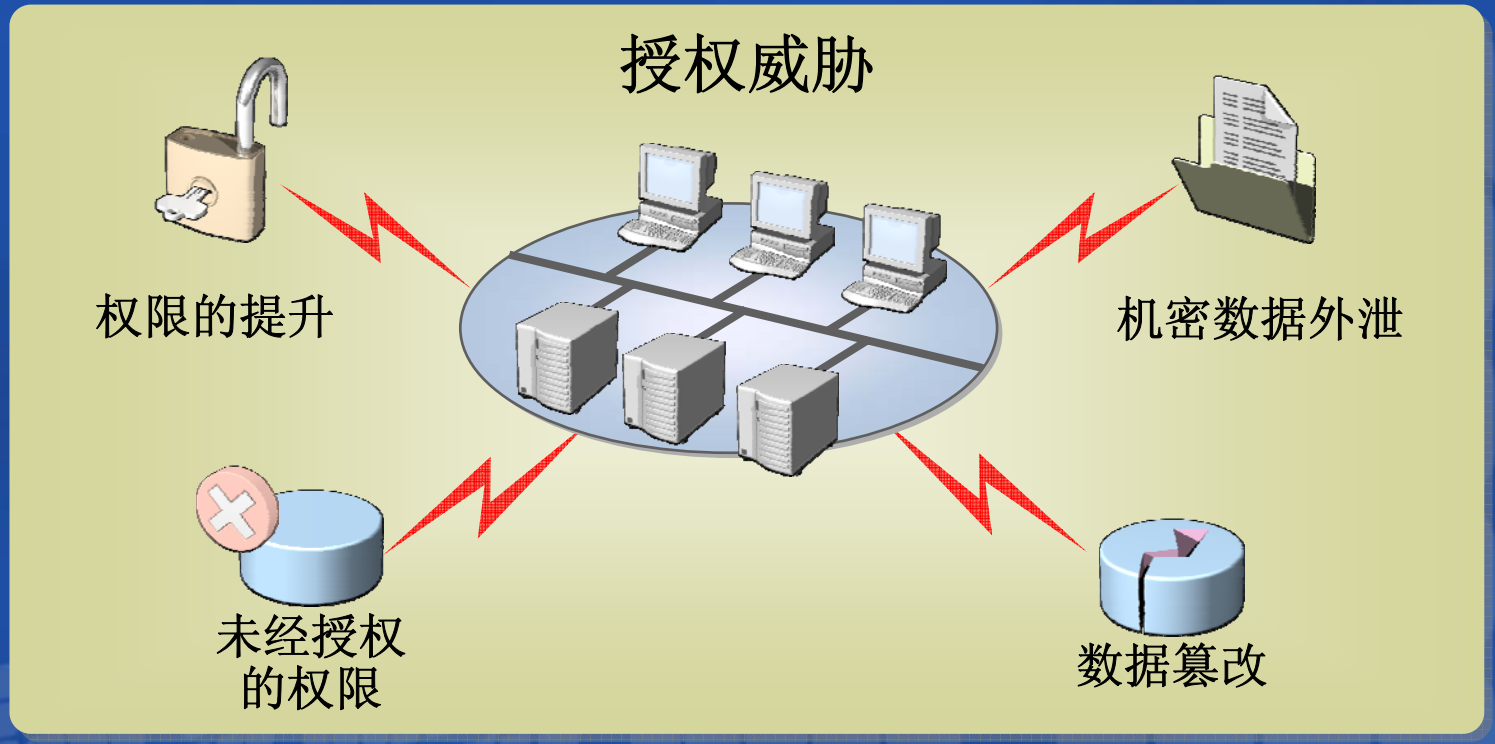
身份认证	A process that checks the credentials of a security principal against values in an identity store

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

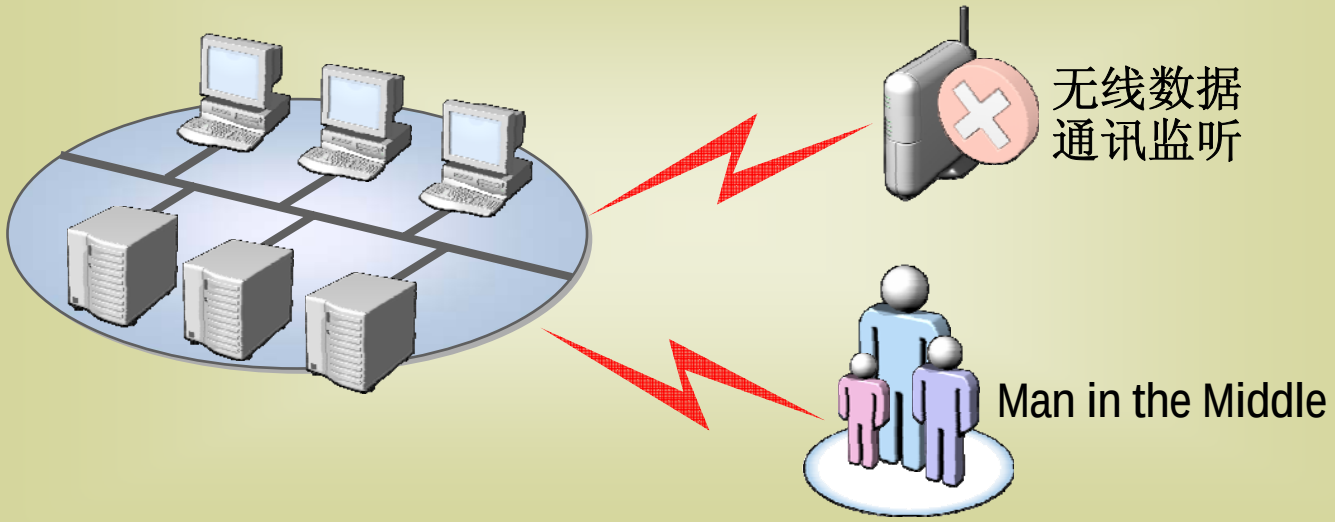


通讯安全

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



WSE

- 安全开发生命周期
- .NET Framework 安全特性及代码访问安全
- 常见攻击手段
- 常见安全策略
- WSE

Secure Communication
Protocol-level security

- SSL is a great example
- Sender must trust intermediaries.
  - Include Soap Routers, Dispatchers, etc…
- Message decrypted at intermediaries
- Encrypts the entire message
- Restricts protocols that can be used

Secure Communication
Message-level security

- End-to-end message security independent of transport
- Supports multiple protocols and multiple encryption technologies
- Can encrypt parts of the message
  - For the intermediary and/or ultimate receiver independently
- Sender needs to only trust the ultimate receiver
- The signature is stored with the data
  - The message content on the wire includes integrity

WSE 3.0 Pilla

Indigo

WSE 3.0 combined with .NET Framework 2.0 puts you on the path to Indigo

Simplified development of Service-Oriented systems using the WS-* protocols and the .NET Framework v2.0

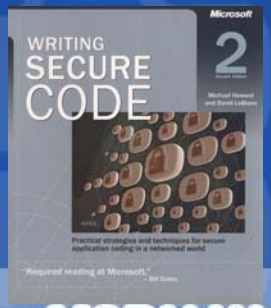
Build secure Web services more easily

Next Steps

您的潜力，我们的动力

Microsoft
微软（中国）有限公司

- 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, 2nd Edition
  - Michael Howard and David LeBlanc
  - ISBN: 0-7356-1722-8



msdn

MSDN Webcasts

Next Steps

Blogs

- http://blogs.msdn.com/clrsecurity/
- http://blogs.msdn.com/shawnfa/

Next Steps

1. Stay informed about security
   - **Sign up for security bulletins:**
     http://www.microsoft.com/security/security_bulletins/alerts2.asp
   - **Get the latest Microsoft security guidance:**
     http://www.microsoft.com/security/guidance/
2. Get additional security training
   - **Find online and in-person training seminars:**
     http://www.microsoft.com/seminar/events/security.mspx
   - **Find a local CTEC for hands-on training:**
     http://www.microsoft.com/learning/

For More Information

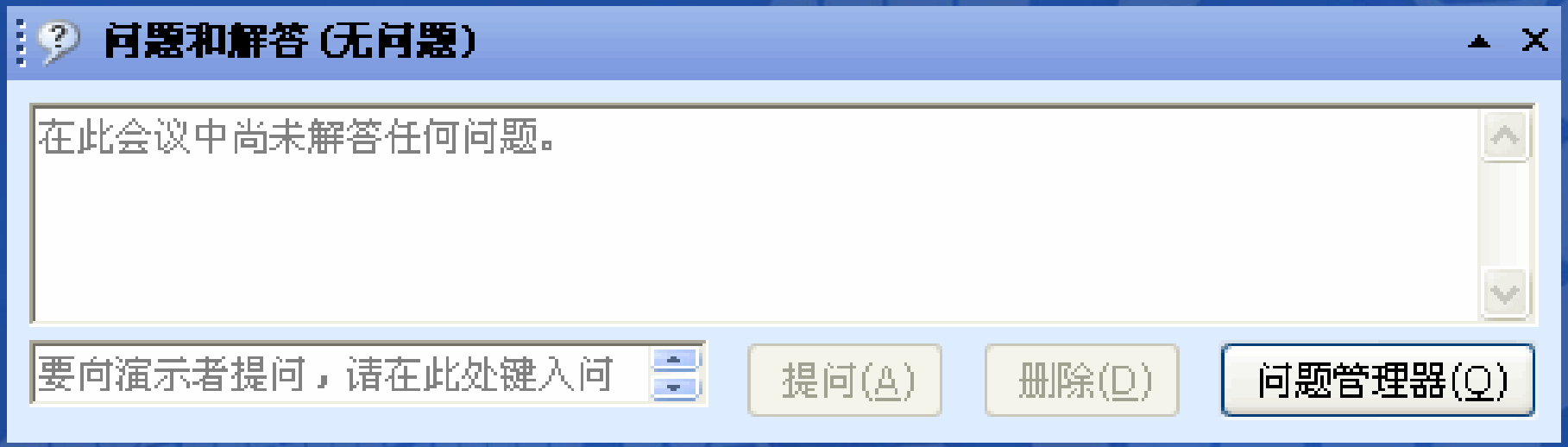
您的潜力，我们的动力

Microsoft
微软（中国）有限公司

- Microsoft Security Site (all audiences)
  http://www.microsoft.com/security
- MSDN Security Site (developers)
  http://msdn.microsoft.com/security
- TechNet Security Site (IT professionals)
  http://www.microsoft.com/technet/security

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

Microsoft®

您的潜力，我们的动力

msdn

MSDN Webcasts