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（之五）
软件开发生命周期的安全问题

钟卫

DPE

微软公司

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

- 软件开发周期的安全构建
- 设计阶段的安全构建
- 开发阶段的安全构建
- 测试阶段的安全构建
- 部署和维护阶段的安全构建

软件开发周期的安全构建

- 软件开发周期的安全构建
- 设计阶段的安全构建
- 开发阶段的安全构建
- 测试阶段的安全构建
- 部署和维护阶段的安全构建

什么能确保应用的安全性？

Secure applications are built with secure code

安全应用的源于安全代码

Identify Users

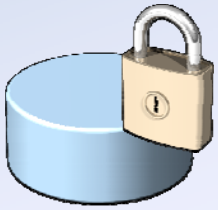
用户身份确认

Restrict Access

策略约束

Communicate Discreetly

通讯安全



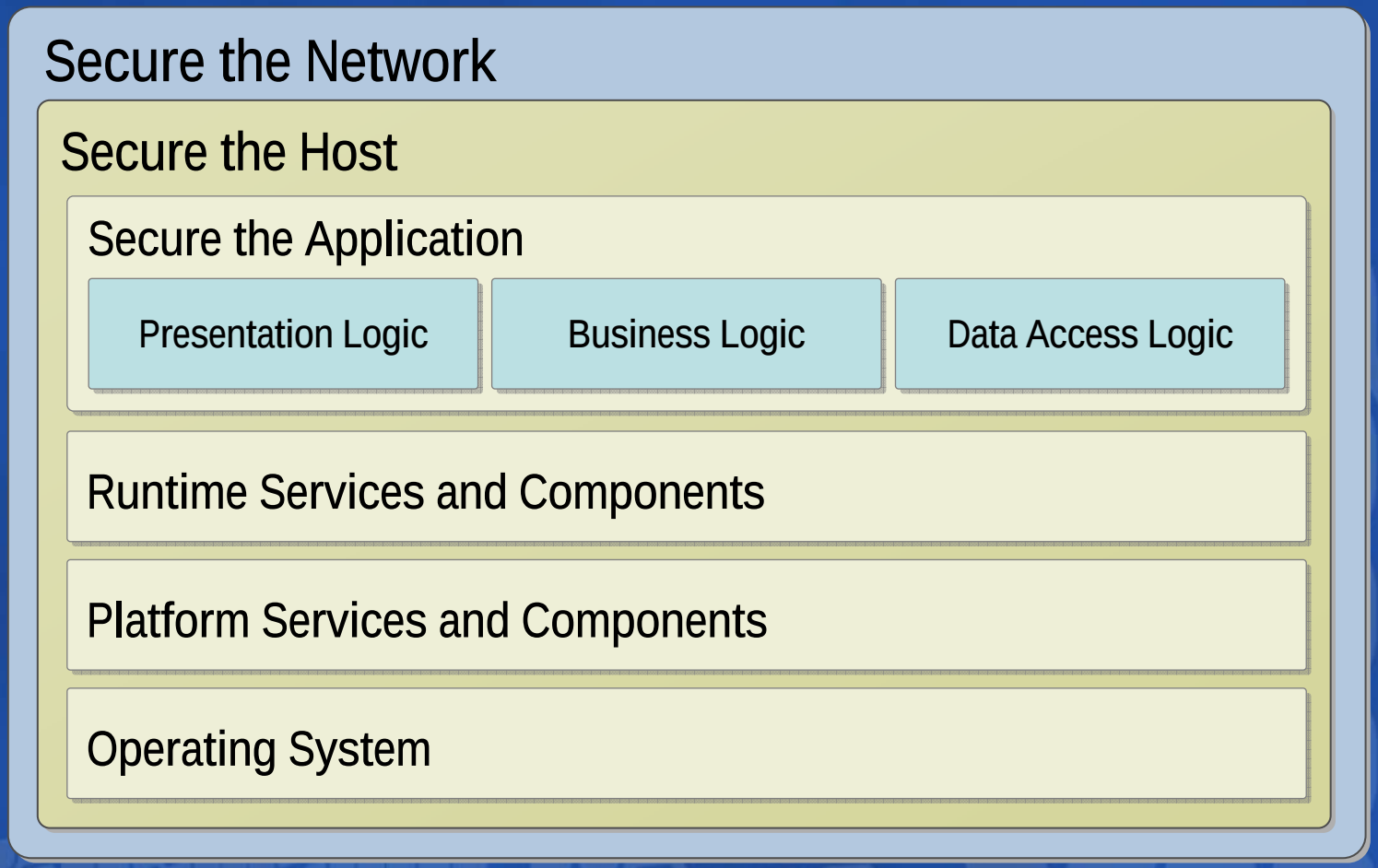
Store Data Securely

数据存储安全

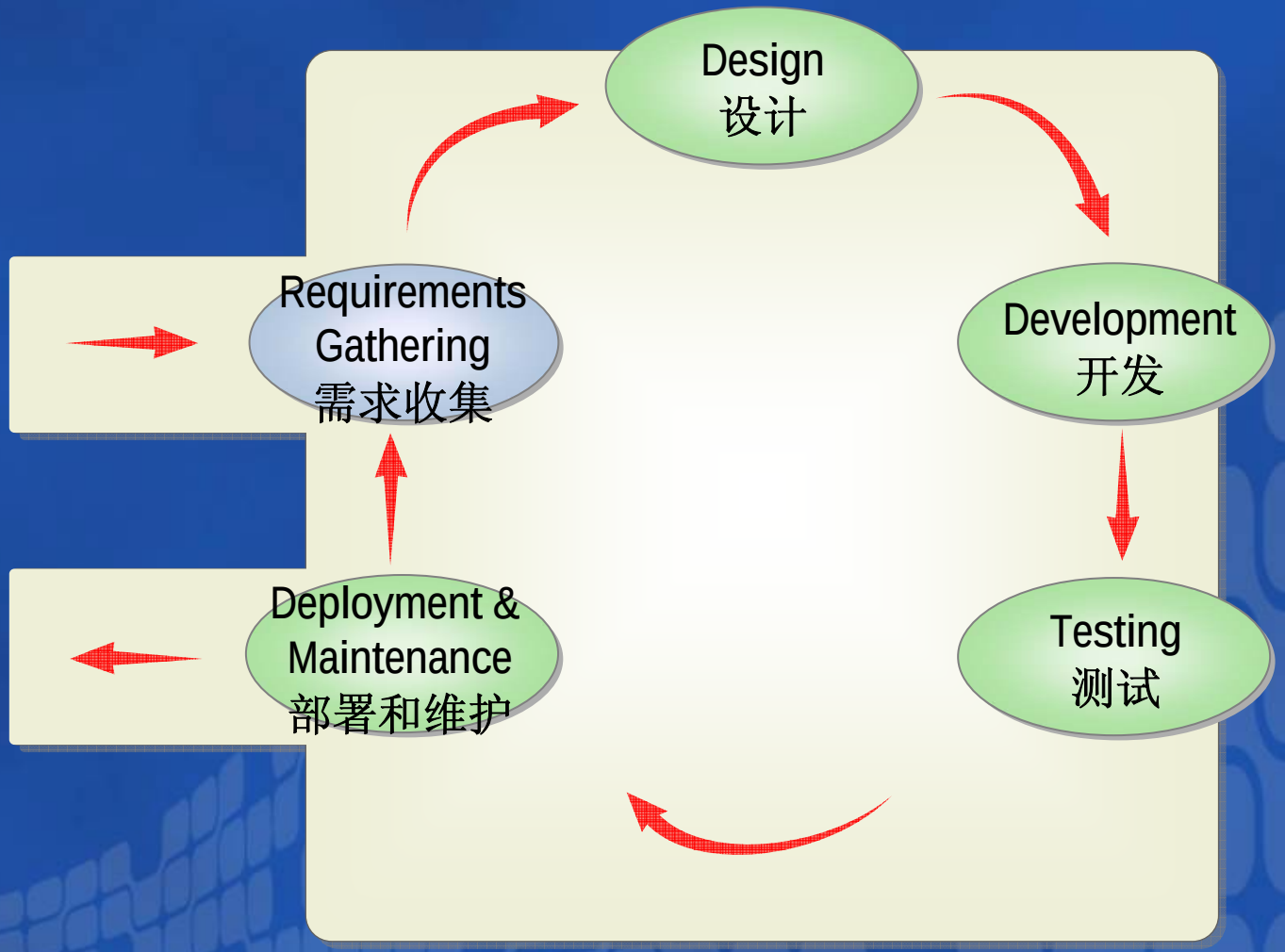
安全词汇定义

Asset 资源	有用的资源
Threat 威胁	对于资源潜在的破坏力
Vulnerability 弱点	使攻击成为可能的漏洞
Attack 攻击	对资源会造成破坏的手段
Countermeasure 策略	能够定位攻击或降低危险的手段

安全体系的整体分析


Secure the Network
Secure the Host
Secure the Application
Presentation Logic
Business Logic
Data Access Logic
Runtime Services and Components
Platform Services and Components
Operating System

软件开发周期的一个例子



Trustworthy Computing

"Trustworthy Computing is computing that is as available, reliable and secure as electricity, water services or telephony. And it is Microsoft's primary, long-term, companywide focus."

- Craig Mundie, CTO

Elements of trustworthy computing:

- Availability
- Security
- Privacy

"Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve."

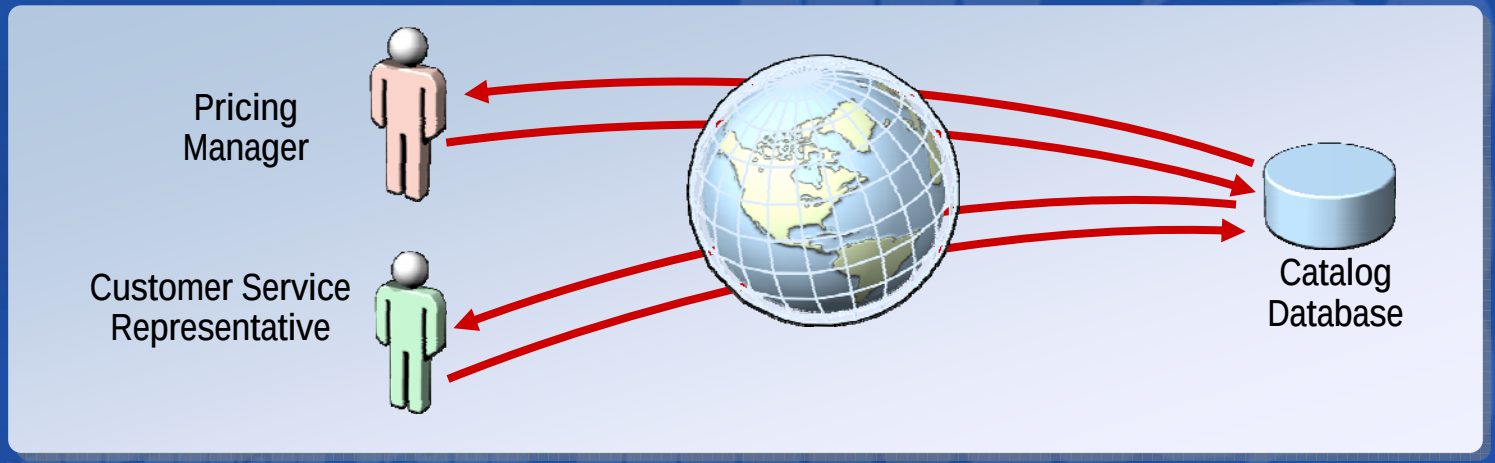
- Bill Gates

安全损失的一些真实数字

Case Study: Introduction to Adventure Works

Adventure Works	Sporting goods catalog and retail outlet

Extranet application requiring identity management and secure communication



软件开发周期的安全构建

- 软件开发周期的安全构建
- 设计阶段的安全构建
- 开发阶段的安全构建
- 测试阶段的安全构建
- 部署和维护阶段的安全构建

为什么在设计阶段就要考虑安全?

- ✓ 会节省更多的开发成本
- ✓ 防止应用被重新设计

跟质量是一样的，安全不是附加的，需要内建其中。

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

威胁建模的流程

1. 确认威胁
2. 建立一个概要架构
3. 分解应用
4. 确定攻击
5. 纪录攻击
6. 评估威胁

设计阶段的安全考虑

对于应用在设计阶段应该考虑如下:

- 用户身份管理
- 输入验证
- 配置和session 管理
- 私密数据和加密
- 审核和登陆

用户身份管理

- 可信用户能够在可信区域内访问资源
- 通过身份管理机制保护用户信息
- 需要强密码格式
- 身份认证失败，返回最少的信息

输入验证

- 所有的用户数据都是有害的、
- 检查数据的格式，长度，范围的有效性
- 不要依赖客户端验证

配置和Session管理

配置

- 保证管理员入口的安全
- 配置文件不能放置未处理过的私密数据
- 使用最小权限服务账户

Session

- 使用SSL保证**authentication cookies**的安全
- 加密 authentication cookies
- 限制session lifetime

私密数据和加密

私密数据

- 不要存储非必要数据
- 不要在代码中存储数据
- 不要在配置文件中存储私密数据

加密

- 确定加密方式
- 尽量使用现有加密方式
- 定期的更换密钥

Demonstration 1: Threat Modeling

1. Identify assets
2. Create an architecture overview
3. Decompose the application graphically
4. Identify the threats
5. Document the threats
6. Rate the threats

开发阶段的安全构建

- 软件开发周期的安全构建
- 设计阶段的安全构建
- 开发阶段的安全构建
- 测试阶段的安全构建
- 部署和维护阶段的安全构建

为什么要在开发阶段引入安全问题?

Insecure code is not reliable

Insecure code is not private

Insecure code cannot be trusted

- 使开发者意识到各种安全隐患
- Informed developers = reduced security vulnerabilities

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

通用代码规范

- 检查所有输入
- 确保无缓冲区溢出错误
- 不要给攻击者太多的错误信息
- 检查调用时的异常处理情况
- 不要在代码中给操作分配GENERIC_ALL 权限

Web 和 数据处理规范

- Do not use string concatenation for SQL statements
- Do not connect to SQL servers as sa or dbo
- Perform access and validity checks on the server

加密和私密保护规范

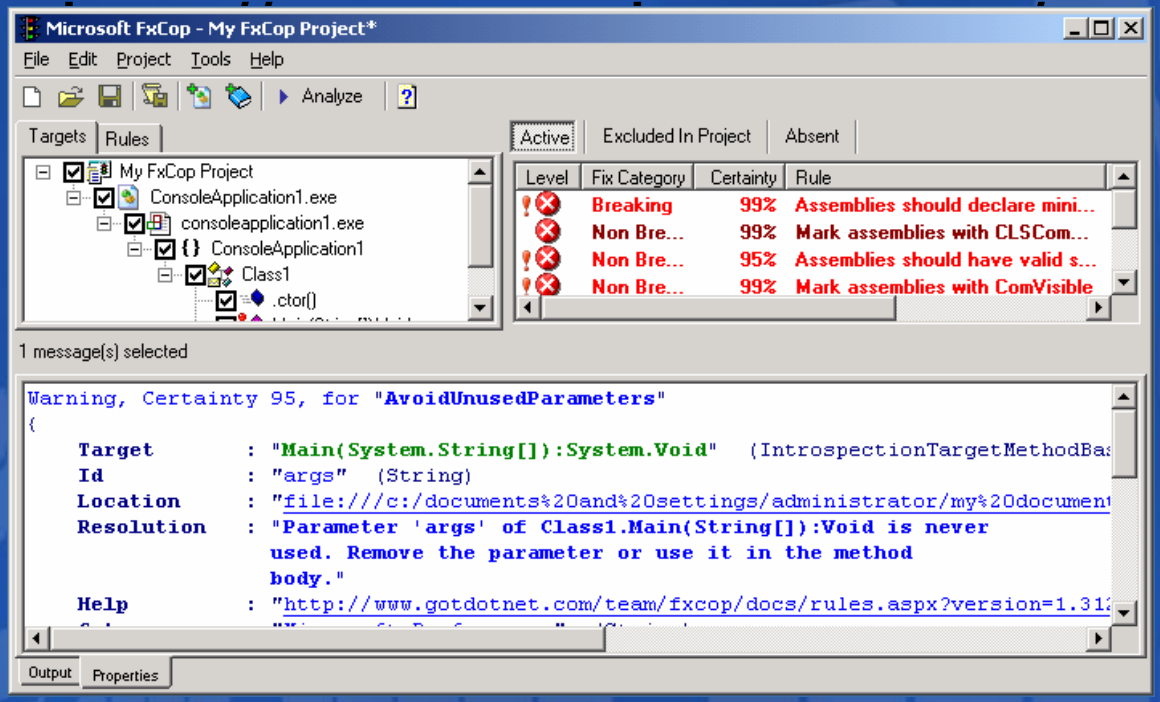
- 不要随意嵌入私密数据
- 选择适当的方法保护私密
- 不要创建自己的加密代码
- 检查随机数生成
- 检查密码生成结果是随机的
- 不要使用弱的加密手段

托管代码规范

- 不要将未加米的私密数据暴露在XML或配置文件中
- 对于程序集使用强命名
- 检查程序集的信任策略
- 不要为不信任用户提供堆栈追踪
- 检查所有非托管代码的正确性
- 确认需要的权限操作

Demonstration 2: FxCop

FxCop	A software tool that validates coding guidelines for .NET Managed code assemblies



测试阶段的安全构建

- 软件开发周期的安全构建
- 设计阶段的安全构建
- 开发阶段的安全构建
- 测试阶段的安全构建
- 部署和维护阶段的安全构建

为何要在测试阶段引入安全?

Developers think their code works

Testers know better

- 测试能使安全的缺失问题更加暴露
- 软件的质量就是安全和可靠
- 测试人员应该:
  - 了解系统的运行
  - 从威胁的角度思考攻击手段

测试计划应该考虑的安全问题

- 攻击威胁建模分析的系统弱点
- SQL injection and cross-site scripting
- 典型的攻击
- 过去的攻击
- 各种的用户权限
- 确保默认安装尽可能的安全
- 测试样例代码

High-Priority Entry Points

High-risk application entry points:

- Listen sockets
- Pipes
- Files that open automatically
- Protocol handlers
- ActiveX controls
- RPC
- HTTP requests
- E-mail
- .NET remoting

测试工具

- 使用工具产生有效/无效输入数据
- 使用工具发布代码缺陷
- 确保 test code 的高质量

Bad test code leads to overconfidence in the product

测试 End-to-End 解决方案

- 组件之间的通讯会有安全问题
- 整个解决方案的安全依赖于它最弱的部分（木桶原理）

Testing is complete when all KNOWN vulnerabilities have been mitigated

部署和维护阶段的安全构建

- 软件开发周期的安全构建
- 设计阶段的安全构建
- 开发阶段的安全构建
- 测试阶段的安全构建
- 部署和维护阶段的安全构建

为何要在部署和维护阶段引入安全?

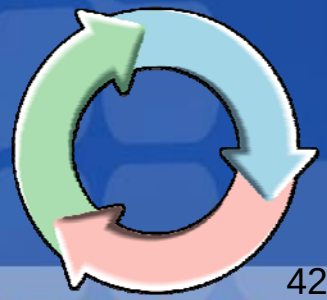
- 测试能够定位已知的威胁。攻击变化，防御手段就的更新
- 对于安全问题的相应也是产品服务的一部分

Create a process before you need one

创建问题相应机制

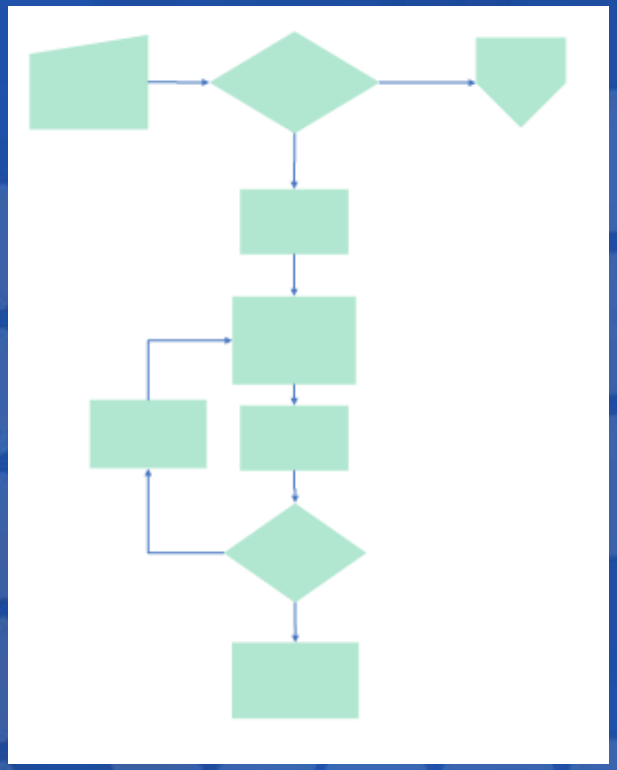
- After a product ships, security flaws are inevitable
- Create a post-deployment process to address new threats and vulnerabilities
- Look for related issues before deploying fixes

If developers who write the product code do not provide the code support, they will not learn about their mistakes



Demonstration 3: Security Response Process

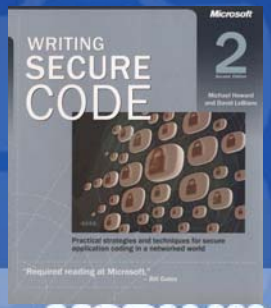
- Security Response Process



- Security News Flash

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



获取更多MSDN资源

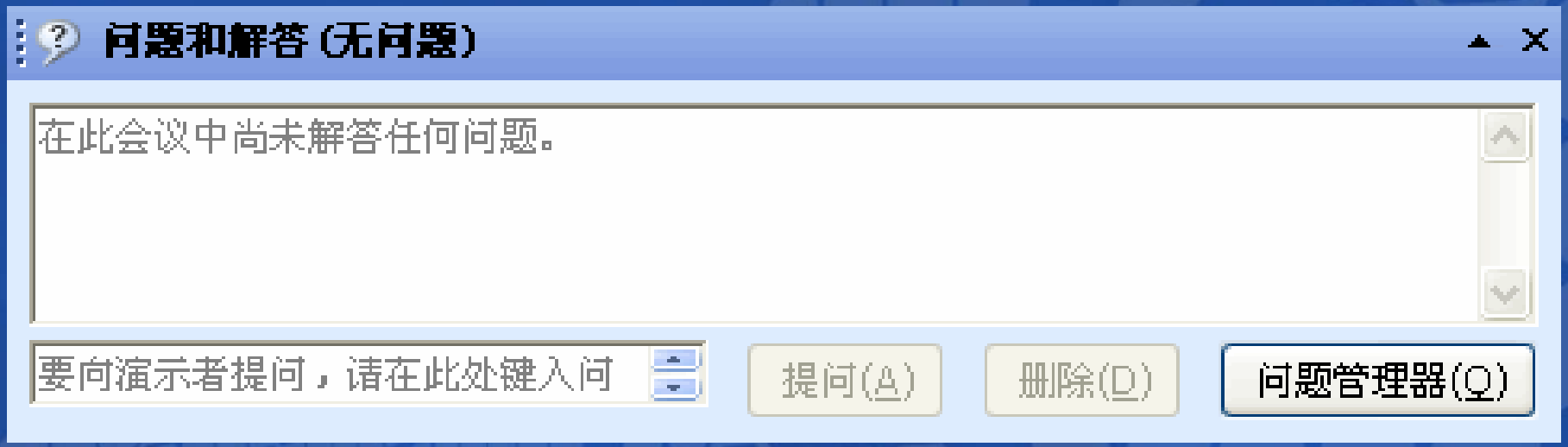
您的潜力，我们的动力

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。



您的潜力，我们的动力