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 （之二）
编写安全代码的最佳实践

钟卫

Msdn讲师

微软公司

msdn

MSDN Webcasts

课程概述

- Secure Development Process
  安全的开发过程
- Threat Modeling
  威胁建模
- Security Best Practices
  安全的最佳实践

您的潜力，我们的动力
Microsoft
微软（中国）有限公司

Session Prerequisites

- Development experience with Microsoft Visual Basic®, Microsoft Visual C++®, or C#
- Internet user experience

Level 200

您的潜力，我们的动力
Microsoft
微软（中国）有限公司

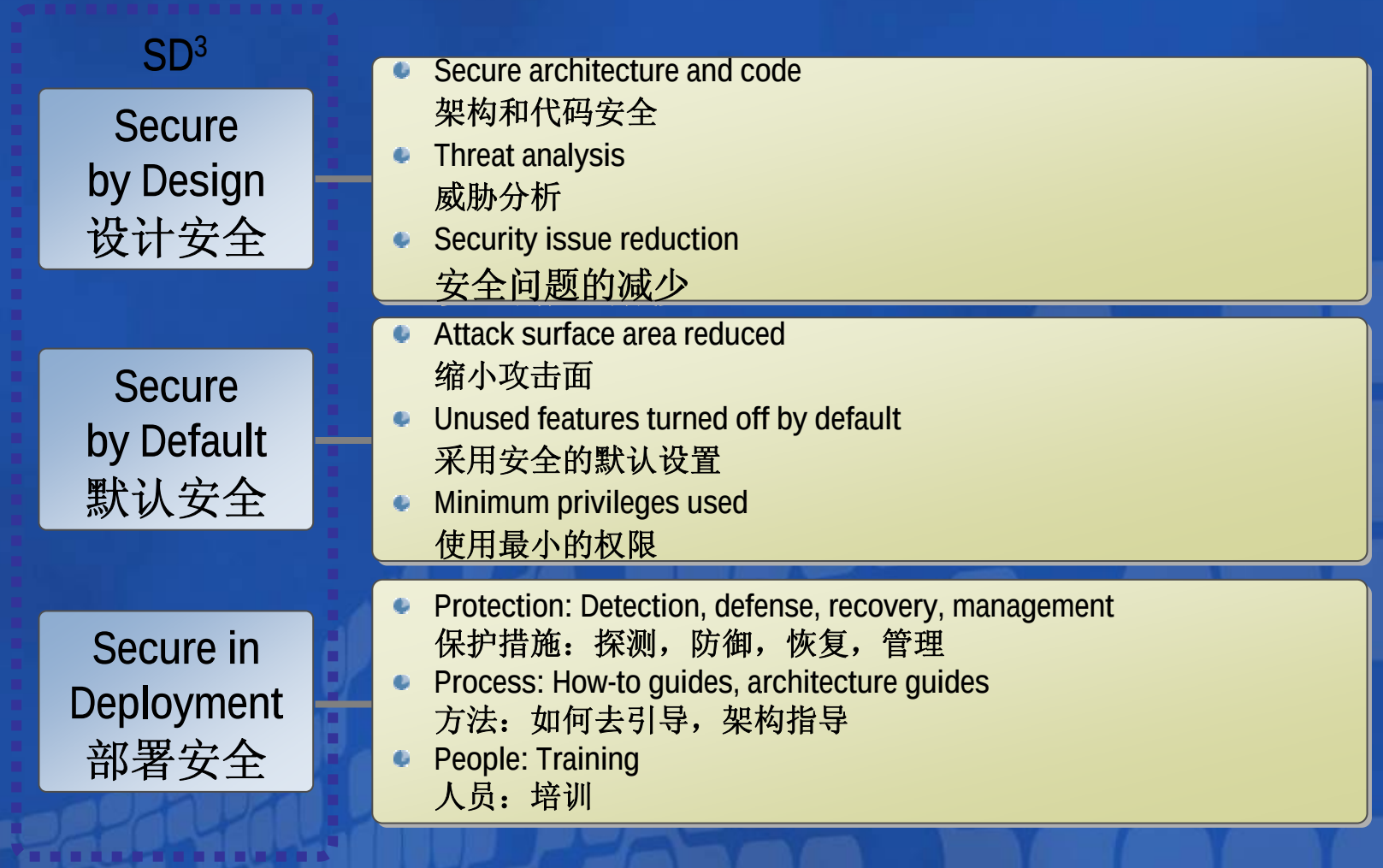
安全的开发过程

- 安全的开发过程
- 威胁建模
- 安全的最佳实践

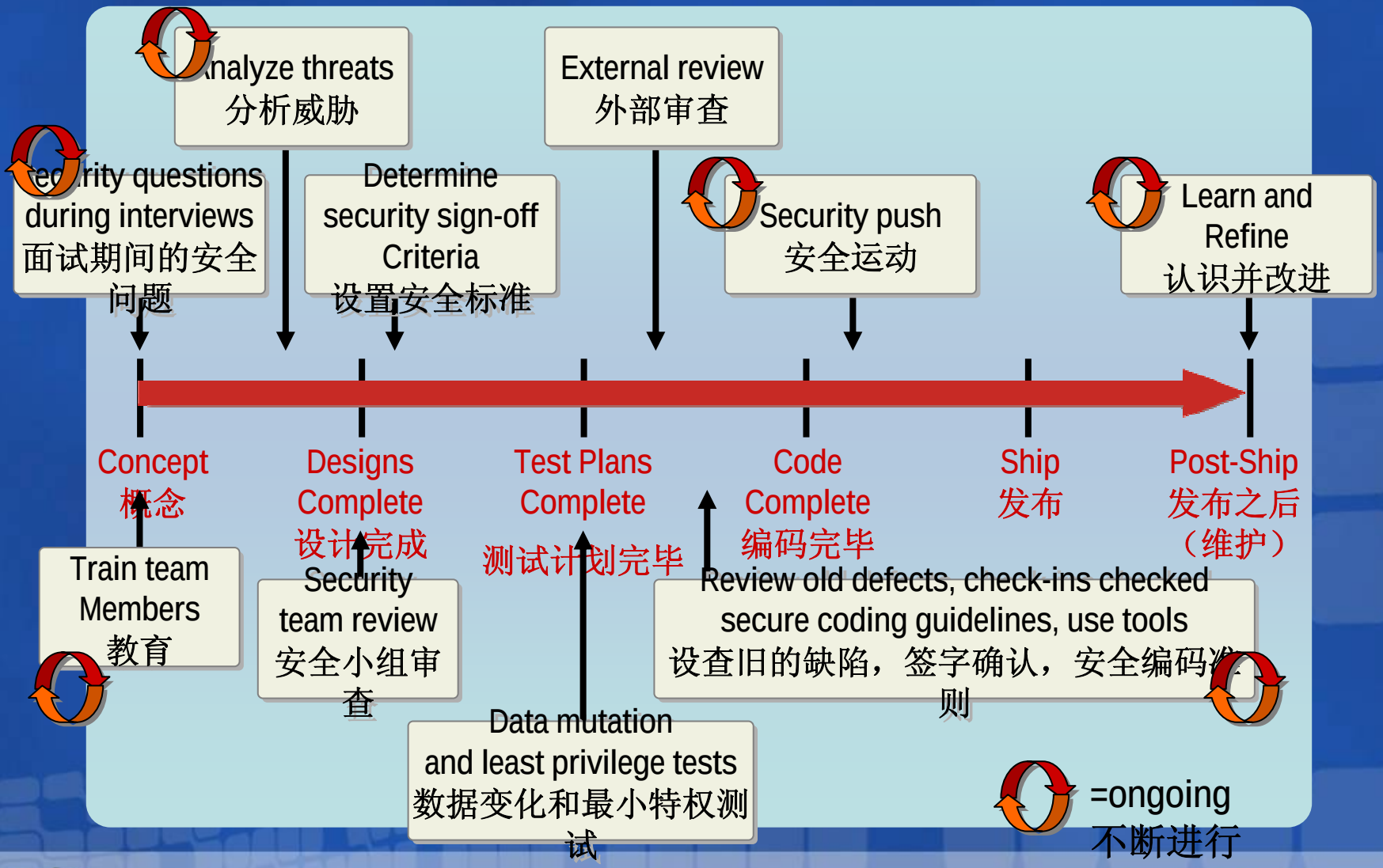
开发过程中安全的改进

- 对于安全，需要考虑的开发过程
  - 需要贯穿整个开发过程
  - 需要在每一个里程碑结束时进行检验
- 在开发的整个过程中，始终不停寻找安全漏洞

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

项目生命周期各个环节的安全问题



设计安全

不断提供设计团队的安全意识

- 不断的培训与学习
- 错误的做事态度，“What I don’t know won’t hurt me” does not apply!

- 设计阶段的安全问题
  - 定义产品的安全目标
  - 安全是产品的一种特性
  - 安全的设计来自威胁建模

您的潜力，我们的动力
Microsoft
微软（中国）有限公司

威胁建模

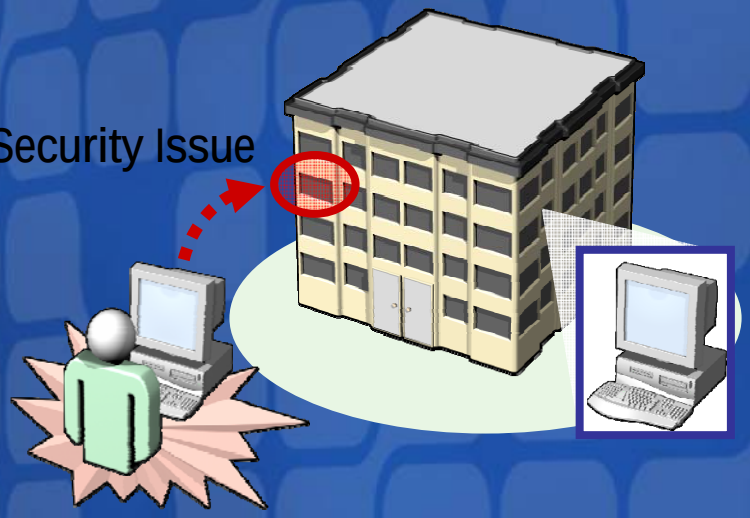
- 安全的开发过程
- 威胁建模
- 安全的最佳实践

什么是威胁建模

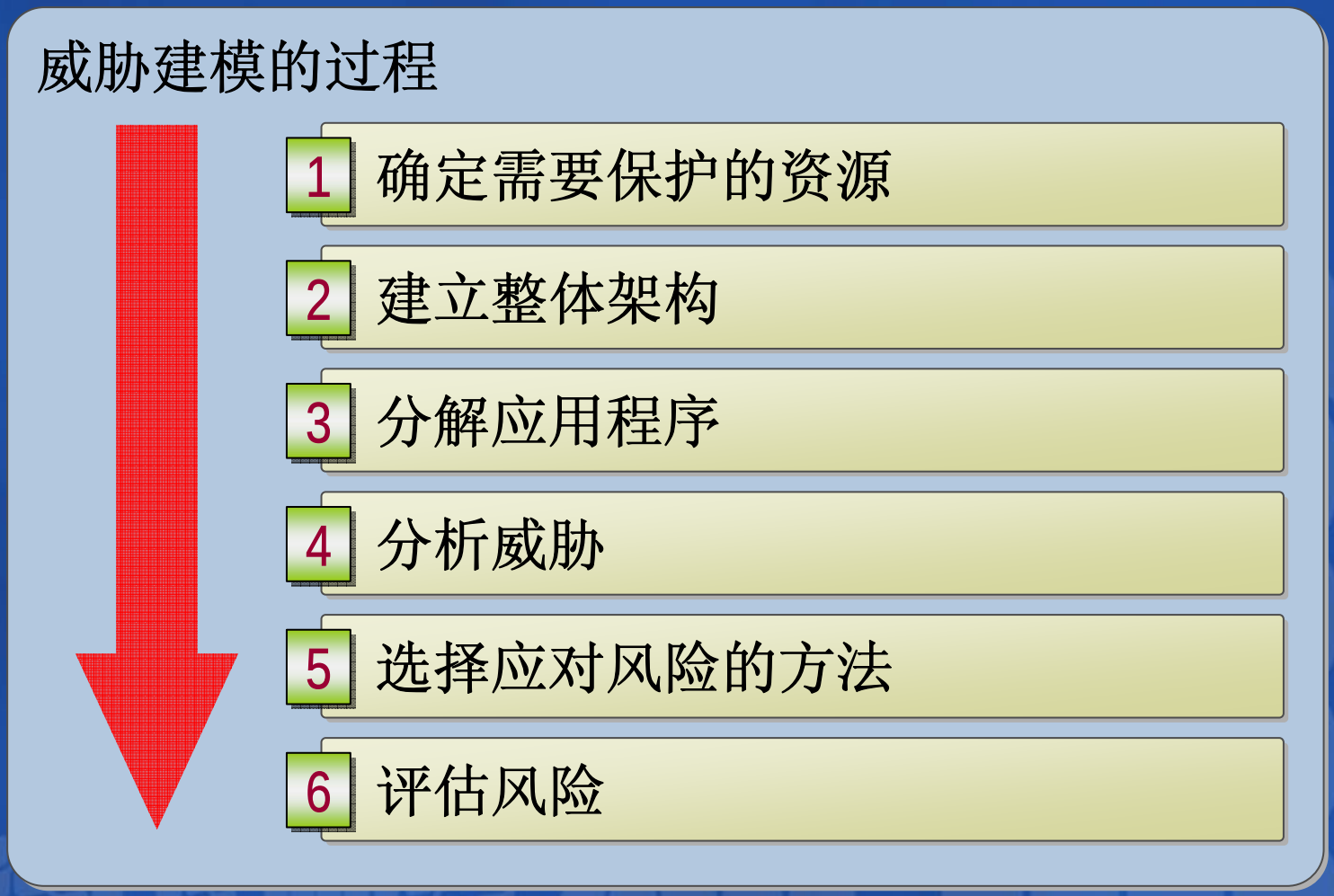
- 威胁建模是一种基于安全的分析
  - 帮助开发团队发现哪里是产品最易受攻击的环节
  - 评估风险
  - 降低整体的外在威胁
  - 分析需要保护的资源
  - 揭示系统弱点
  - 识别威胁类型
  - 有助于形成安全设计规范

威胁建模的好处

- 有助于更好的理解你的应用程序
- 帮助你查找**bug**
- 发现以其他方式都不太可能发现的复杂的设计**bug**
- 威胁模型应该让基于产品的其他开发小组读到
- 威胁建模对测试人员也非常有用



威胁建模的过程

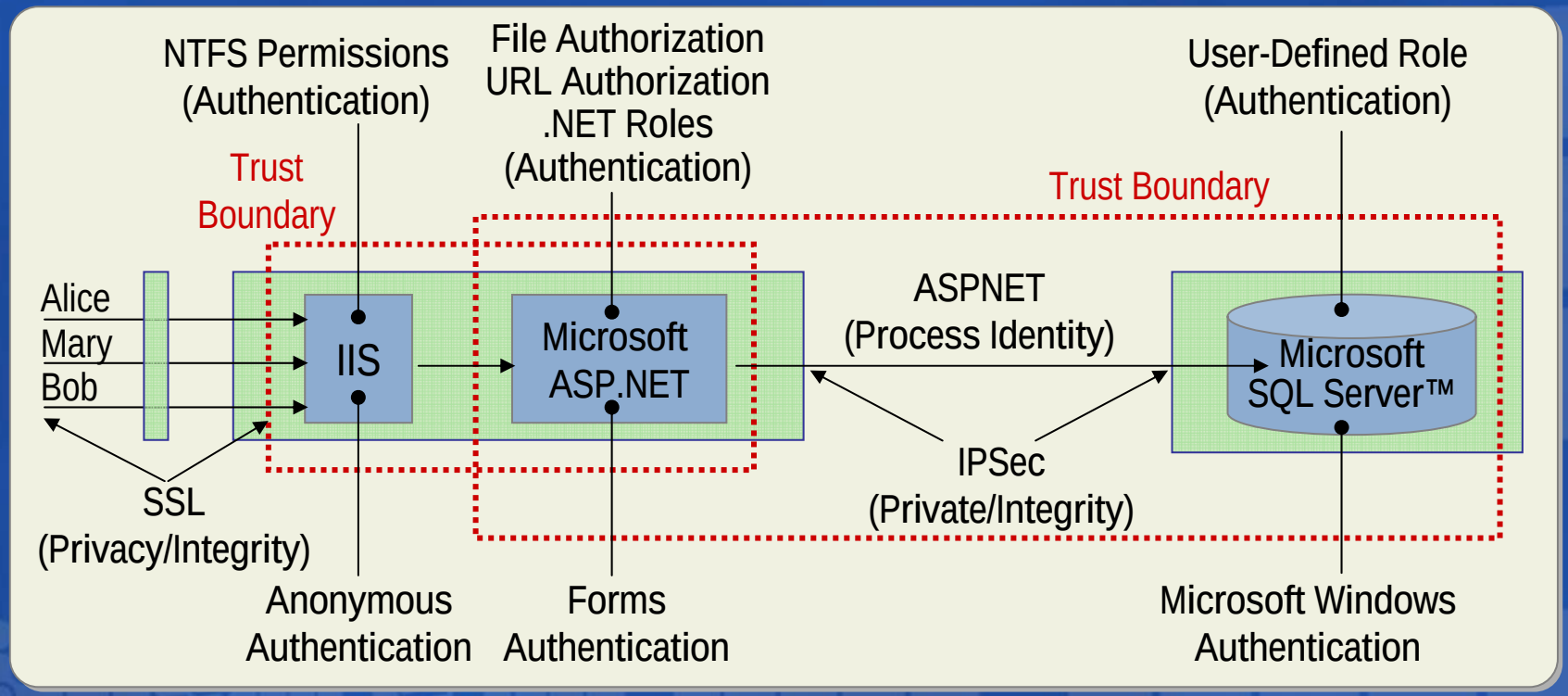

威胁建模的过程
1 确定需要保护的资源
2 建立整体架构
3 分解应用程序
4 分析威胁
5 选择应对风险的方法
6 评估风险

威胁建模 Step 1:确定需要保护的资源

- 建立一个列表，列出需要保护各种资源
  - 机密数据，例如客户信息数据库
  - Web 页面
  - 系统的可用性
  - 其他
  - 注意折衷的态度会危及的应用程序的安全

威胁建模 Step 2: 建立整体架构

- 确定应用的具体功能
- 创建应用的整体架构设计
- 确定适用的技术



威胁建模 – Step 3: 分解应用程序

- 中止系统运行
- 基于现有的系统建立安全分析档案
- 检查不同子系统之间的交互
- 使用数据流图或者uml活动图

威胁建模– Step 4: 确定威胁

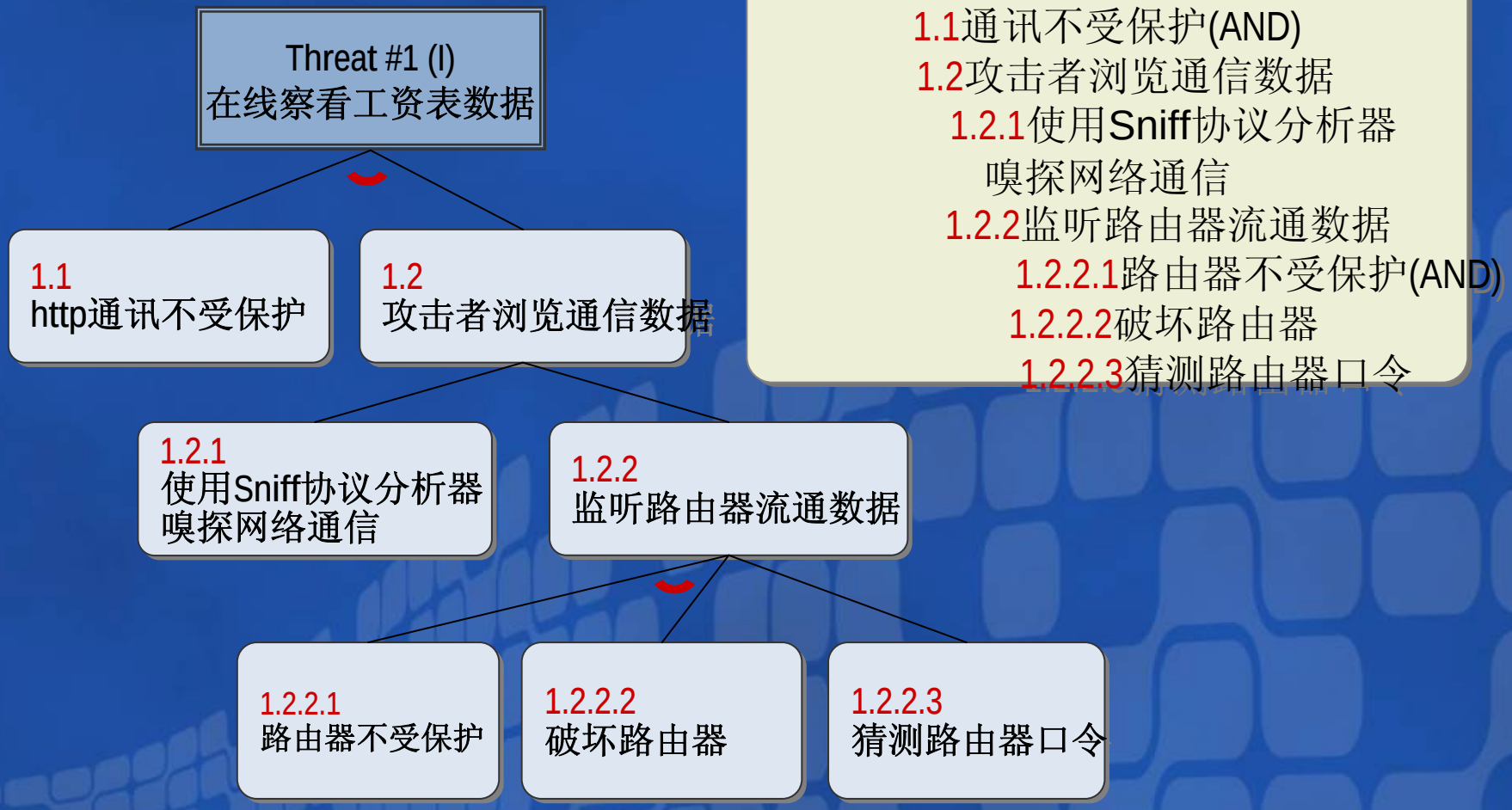
- 分析威胁
  - 网络威胁
  - 服务器威胁
  - 应用程序威胁

威胁建模 – 使用 STRIDE给威胁分类

Types of threats	Examples
Spoofing 身份欺骗	伪造**email**发送信息 截获并重发认证数据包
Tampering 篡改数据	传输时更改数据 修改文件数据
Repudiation 否认	在系统中作了非法操作，同时系统缺少跟踪被禁止操作的能力 买了一件商品后否认购买
Information disclosure 信息泄漏	信息暴露于执行错误中 **Web**站点暴露了执行代码
Denial of service 拒绝服务	**SYN packets**造成的网络瘫痪 伪造 **ICMP packets**造成的网络瘫痪
Elevation of privilege 特权提升	通过缓冲区溢出获得特权 获得了 **administrator** 的特权

威胁建模 – 使用威胁树分析攻击

您的潜力，我们的动力
Microsoft
微软（中国）有限公司



威胁建模 – Step 5: 建模需要纪录的项目

- 使用模板记录威胁

Threat description	Injection of SQL commands
攻击目标	**Data Access Component**
风险	
攻击方式	**Attacker appends SQL commands to user name, which is used to form a SQL query**
对策	**Use a regular expression to validate the user name, and use a stored procedure with parameters to access the database**

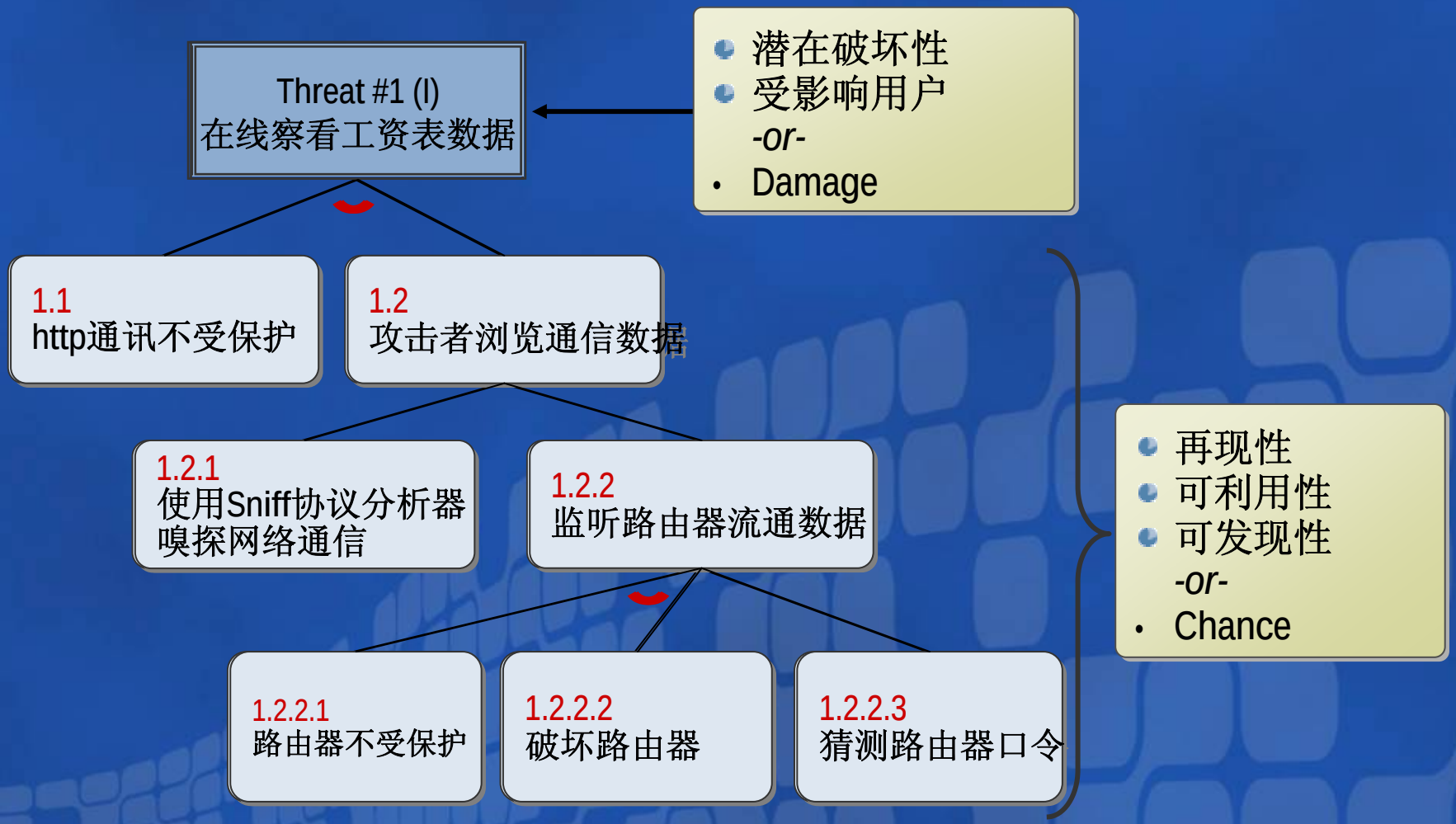
威胁建模 – Step 6: 评估威胁

- 应用公式

  风险= 危急程度 * 发生可能性

- 使用 DREAD 计算风险
  - Damage potential 潜在的破坏性
  - Reproducibility 再现性
  - Exploitability 可利用性
  - Affected users 受影响的用户
  - Discoverability 可发现性

威胁建模 – Example: 评估威胁



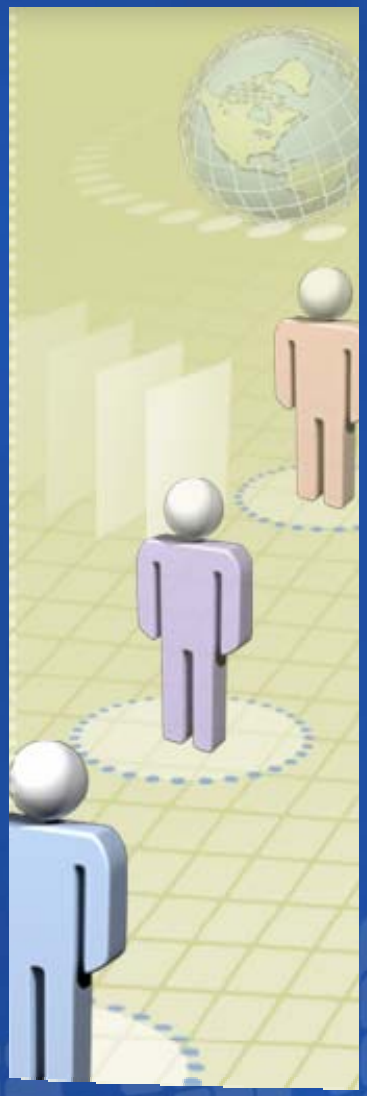
您的潜力，我们的动力
Microsoft
微软（中国）有限公司

安全的最佳实践

- 安全的开发过程
- 威胁建模
- 安全的最佳实践

以最小权限运行

- 众所周知的安全准则
  “使用完成任务所需的最小特权集来执行任务
- 特权的提升，将导致安全问题的出现
  - 恶意代码在用户提高了权限的情况下运行
  - 很多病毒的传播环境是具有特权的管理员账户



Demonstration 1: ASP.NET Applications Security

- Investigating ASP.NET Application Privileges
- Restricting ASP.NET Applications Trust Levels
- Sandboxing Privileged Code
- Using Sandboxed Assemblies

缩小攻击面

- 只将有限的，没问题的程序界面对外公布
- 只运行应用程序所必需的服务
  - 如果不将默认关闭的服务开启， Slammer and CodeRed 病毒不会发作
  - 只有在 scripting 被起用，ILoveYou 病毒才会发作

不要相信用户的输入

- 验证所有的输入
  - 在被证明之前，所有的输入都是有害的
  - 数据在通过不可信环境进入可信环境的边界时，必须经过验证
- 约束，拒绝，整理用户的输入：
  - 类型验证
  - 长度检查
  - 范围检查
  - 格式检查

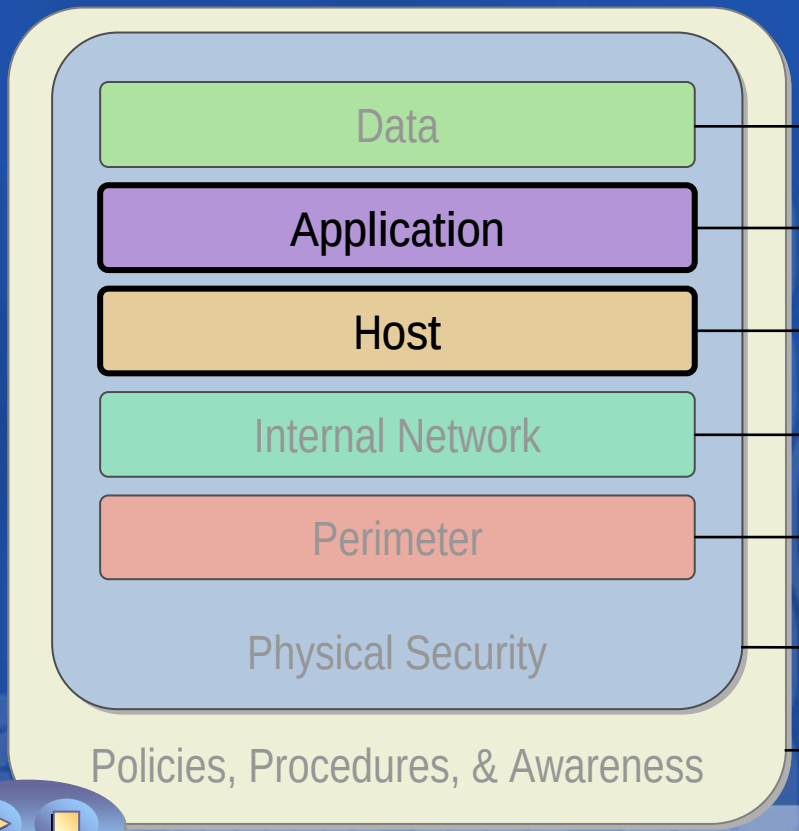
```
Validator.ValidationExpression =
"\w+([-+.]\w+)*@\w+([-.]\w+)*\.\w+([-.]\w+)*";
```

您的潜力，我们的动力
Microsoft
微软（中国）有限公司

纵深防御

使用层次防御

- 加大了攻击难度
- 减少了攻击的数量



ACLs, encryption, EFS

Application hardening, antivirus

OS hardening, authentication, patch management,

Network segments, IPSec, NIDS

Firewalls, Network Access Quarantine Control

Guards, locks, tracking devices

Security documents, user education

您的潜力，我们的动力
Microsoft
微软（中国）有限公司

Fail Intelligently (1 of 2)

```
DWORD dwRet = IsAccessAllowed(…);
if (dwRet == ERROR_ACCESS_DENIED) {
    // Security check failed.
       // Inform user that access is denied
} else {
    // Security check OK.
       // Perform task…
}
```

What if IsAccessAllowed() returns ERROR_NOT_ENOUGH_MEMORY?

- If your code does fail, make sure it fails securely

Fail Intelligently (2 of 2)

您的潜力，我们的动力
Microsoft
微软（中国）有限公司

- Do not:
  - –不要暴露执行错误

```
<customErrors mode="On"/>
```

  - –错误发生不要浪费过多的资源消耗
- Do:
  - –使用异常处理模块以防止错误影响程序的运行
  - –将可疑的错误写进日志

安全测试

- 项目开始就需要定下测试小组的人员
- 根据威胁建模制定安全性测试计划
- 像一个haker一样去思考，去测试
  - 自动脚本攻击
  - 提交各种无效数据
  - 删除文件和探测应用入口
  - 以非管理员角色进行测试
- 了解我们的敌人和我们自己
  - Hackers的技能和技巧?
  - 测试组的技能和技巧?

从错误中吸取教训

- 当发生安全问题，我们应该吸取教训
  - 安全问题如何发生
  - 项目中是否存在相同问题
  - 如何阻止此类问题再次发生
  - 是否需要更新教育和分析工具
  - 约定时间交互问题

Next Steps

您的潜力，我们的动力
Microsoft
微软（中国）有限公司

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

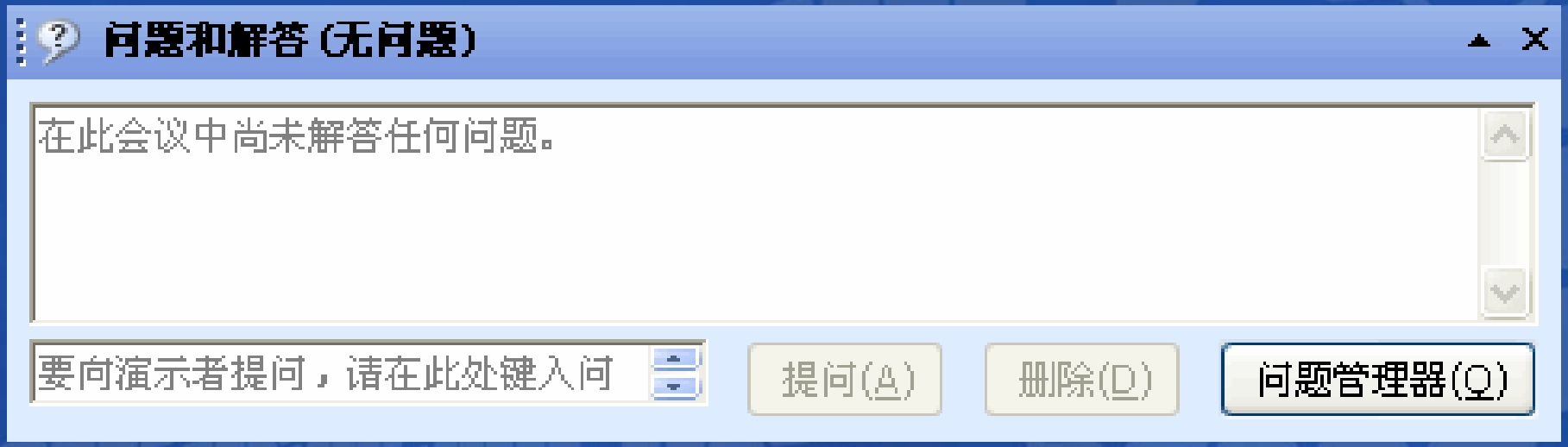
您的潜力，我们的动力
Microsoft
微软（中国）有限公司

- 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

Q&A

您的潜力，我们的动力
Microsoft
微软（中国）有限公司

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