Microsoft Tech·Ed 2005中国

创新 · 远见 · 分享 · 协作

# Session: Essentials of Application Security
# 应用系统安全内幕

钟卫

微软公司

## Session Overview 概述

- The Importance of Application Security
  应用系统安全的重要性
- Secure Application Development Practices
  开发安全的系统的实践
- Security Technologies
  可用的安全技术
- Secure Development Guidelines
  开发安全应用的指导

## Session Prerequisites 课程的要求

- Development experience with Microsoft Visual Basic®, Microsoft Visual C++®, or C#
  在Visual Basic®, Microsoft Visual C++®, or C#有实际的开发经验
- Internet user experience
  Internet 用户

**Level 200**

## The Importance of Application Security
## 应用程序安全的重要性

- The Importance of Application Security
  应用系统安全的重要性
- Secure Application Development Practices
  开发安全的系统的实践
- Security Technologies
  可用的安全技术
- Secure Development Guidelines
  开发安全应用的指导

## Trustworthy Computing 可信计算

"Trustworthy Computing has four pillars:

Reliability **means a computer system is dependable, is available when needed, and performs as expected and at appropriate levels.**

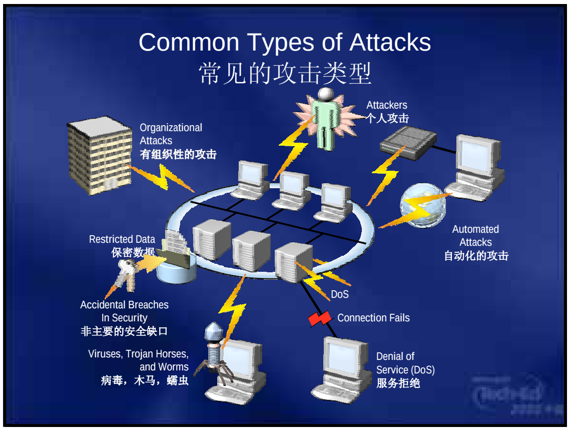
Security **means a system is resilient to attack, and the confidentiality, integrity, and availability of both the system and its data are protected.**

Privacy **means that people can control their personal information and organizations that use the information faithfully protect it.**

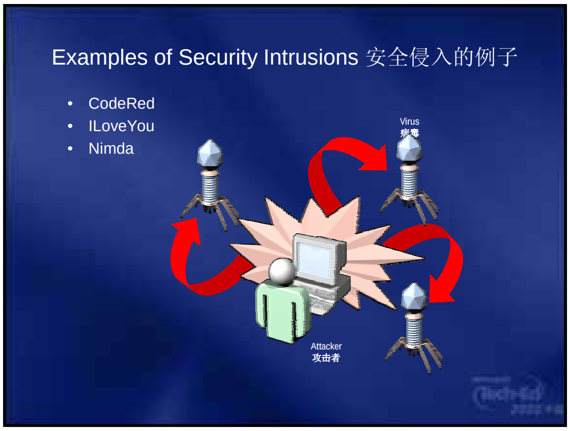
Business **integrity is about companies in our industry being responsible to customers and helping them find appropriate solutions for their business issues, addressing problems with products or services, and being open in interactions with customers."**

Bill Gates
July 18, 2002

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

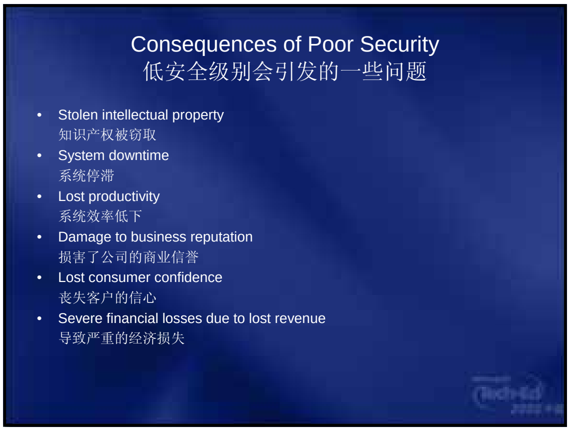


## Common Types of Attacks
## 常见的攻击类型



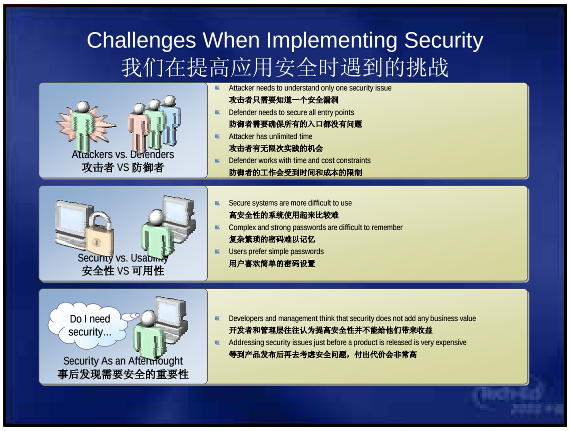
## Examples of Security Intrusions 安全侵入的例子

- CodeRed
- ILoveYou
- Nimda



## Consequences of Poor Security
## 低安全级别会引发的一些问题

- Stolen intellectual property
  知识产权被窃取
- System downtime
  系统停滞
- Lost productivity
  系统效率低下
- Damage to business reputation
  损害了公司的商业信誉
- Lost consumer confidence
  丧失客户的信心
- Severe financial losses due to lost revenue
  导致严重的经济损失



## Challenges When Implementing Security
## 我们在提高应用安全时遇到的挑战

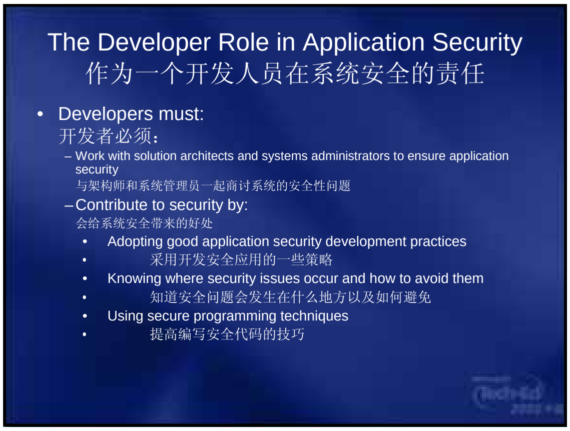
Attackers vs. Defenders
攻击者 VS 防御者

- Attacker needs to understand only one security issue
  攻击者只需要知道一个安全漏洞
- Defender needs to secure all entry points
  防御者需要确保所有的入口都没有问题
- Attacker has unlimited time
  攻击者有无限次实践的机会
- Defender works with time and cost constraints
  防御者的工作会受到时间和成本的限制

Security vs. Usability
安全性 VS 可用性

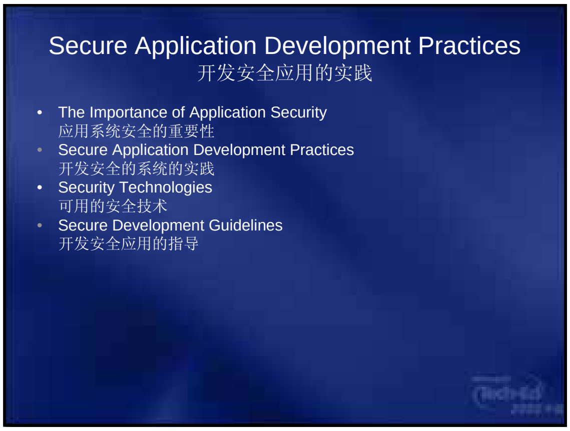
- Secure systems are more difficult to use
  高安全性的系统使用起来比较难
- Complex and strong passwords are difficult to remember
  复杂繁琐的密码难以记忆
- Users prefer simple passwords
  用户喜欢简单的密码设置

- Developers and management think that security does not add any business value
  开发者和管理层往往认为提高安全性并不能给他们带来收益
- Addressing security issues just before a product is released is very expensive
  等到产品发布后再去考虑安全问题，付出代价会非常高



## The Developer Role in Application Security
## 作为一个开发人员在系统安全的责任

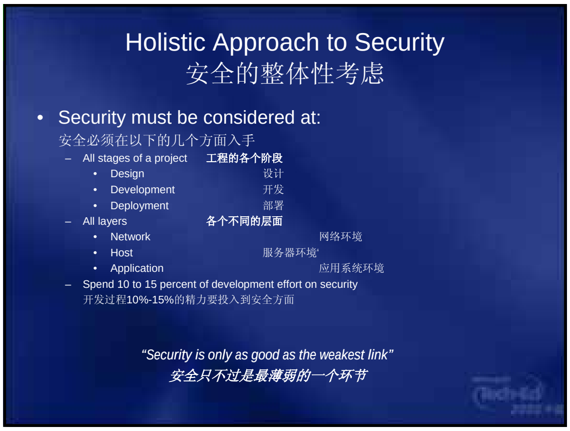
- Developers must:
  开发者必须：
  - Work with solution architects and systems administrators to ensure application security
    与架构师和系统管理员一起商讨们系统的安全性问题
  - Contribute to security by:
    会给系统安全带来的好处
    - Adopting good application security development practices
    - 采用开发安全应用的一些策略
    - Knowing where security issues occur and how to avoid them
    - 知道安全问题会发生在什么地方以及如何避免
    - Using secure programming techniques
    - 提高编写安全代码的技巧



## Secure Application Development Practices
## 开发安全应用的实践

- The Importance of Application Security
  应用系统安全的重要性
- Secure Application Development Practices
  开发安全的系统的实践
- Security Technologies
  可用的安全技术
- Secure Development Guidelines
  开发安全应用的指导

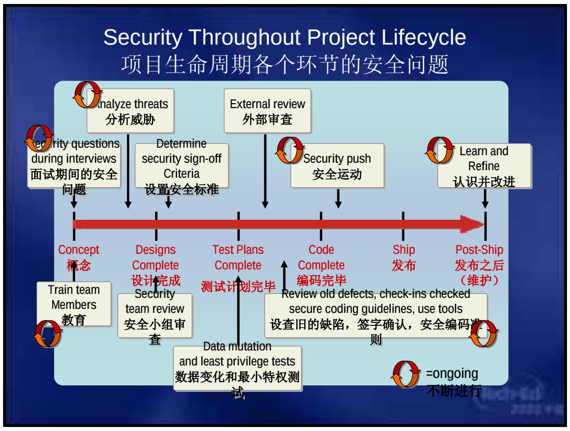
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.



## Holistic Approach to Security
## 安全的整体性考虑

- Security must be considered at:
  安全必须在以下的几个方面入手
  - All stages of a project **工程的各个阶段**
    - Design 设计
    - Development 开发
    - Deployment 部署
  - All layers **各个不同的层面**
    - Network 网络环境
    - Host 服务器环境‘
    - Application 应用系统环境
  - Spend 10 to 15 percent of development effort on security
    开发过程10%-15%的精力要投入到安全方面

*"Security is only as good as the weakest link"*
*安全只不过是最薄弱的一个环节*



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

Analyze threats
分析威胁

External review
外部审查

Security questions during interviews
面试期间的安全问题

Determine security sign-off Criteria
设置安全标准

Security push
安全运动

Learn and Refine
认识并改进

Concept
概念

Designs Complete
设计完成

Test Plans Complete
测试计划完毕

Code Complete
编码完毕

Ship
发布

Post-Ship
发布之后
（维护）

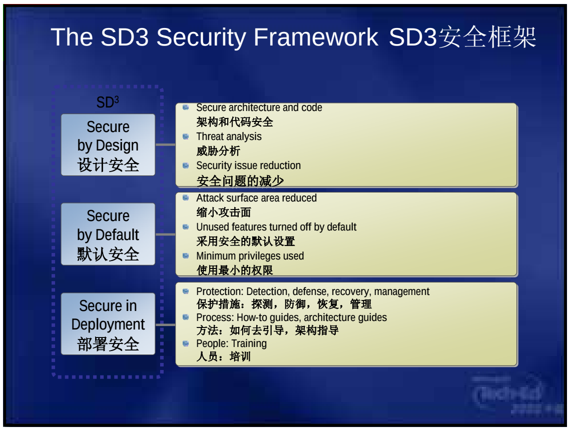
Train team Members
教育

Security team review
安全小组审查

Data mutation and least privilege tests
数据变化和最小特权测试

Review old defects, check-ins checked secure coding guidelines, use tools
设查旧的缺陷，签字确认，安全编码准则

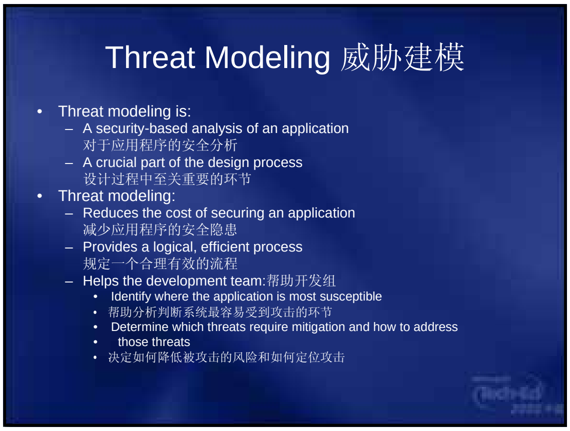
=ongoing
不断进行



## The SD3 Security Framework SD3安全框架

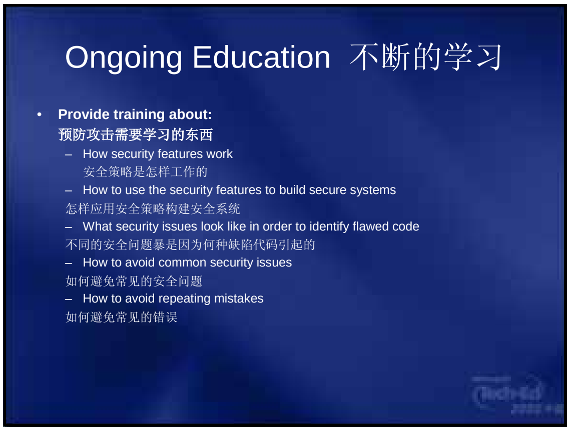
SD$^3$

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



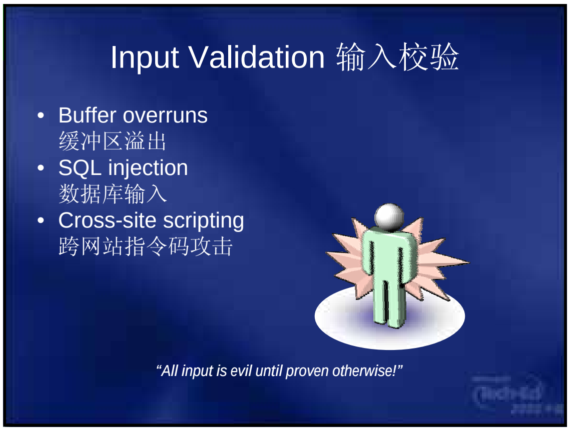
## Threat Modeling 威胁建模

- Threat modeling is:
  - A security-based analysis of an application
    对于应用程序的安全分析
  - A crucial part of the design process
    设计过程中至关重要的环节
- Threat modeling:
  - Reduces the cost of securing an application
    减少应用程序的安全隐患
  - Provides a logical, efficient process
    规定一个合理有效的流程
  - Helps the development team:帮助开发组
    - Identify where the application is most susceptible
    - 帮助分析判断系统最容易受到攻击的环节
    - Determine which threats require mitigation and how to address
    - those threats
    - 决定如何降低被攻击的风险和如何定位攻击



## Ongoing Education 不断的学习

- **Provide training about:**
  **预防攻击需要学习的东西**
  - How security features work
    安全策略是怎样工作的
  - How to use the security features to build secure systems
  怎样应用安全策略构建安全系统
  - What security issues look like in order to identify flawed code
  不同的安全问题暴是因为何种缺陷代码引起的
  - How to avoid common security issues
  如何避免常见的安全问题
  - How to avoid repeating mistakes
  如何避免常见的错误



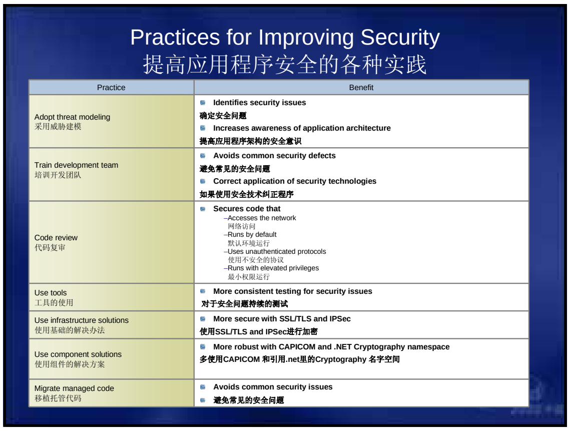
## Input Validation 输入校验

- Buffer overruns
  缓冲区溢出
- SQL injection
  数据库输入
- Cross-site scripting
  跨网站指令码攻击

*"All input is evil until proven otherwise!"*

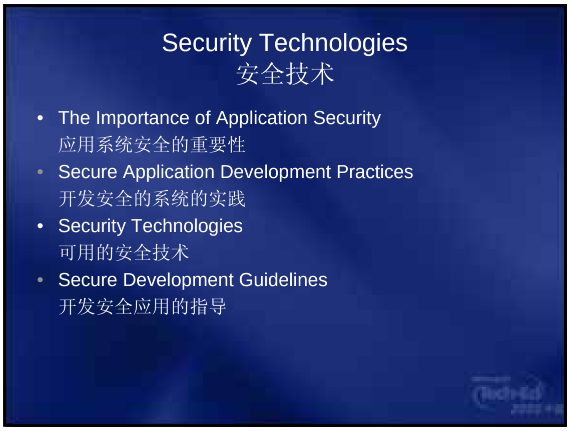
# demo

Buffer Overruns 缓冲区溢出



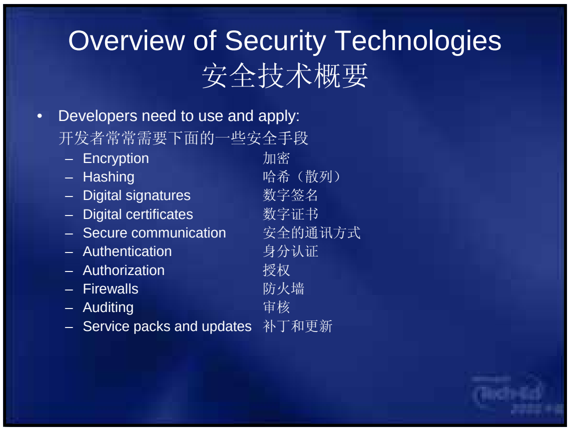
## Practices for Improving Security
## 提高应用程序安全的各种实践

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



## Security Technologies
## 安全技术

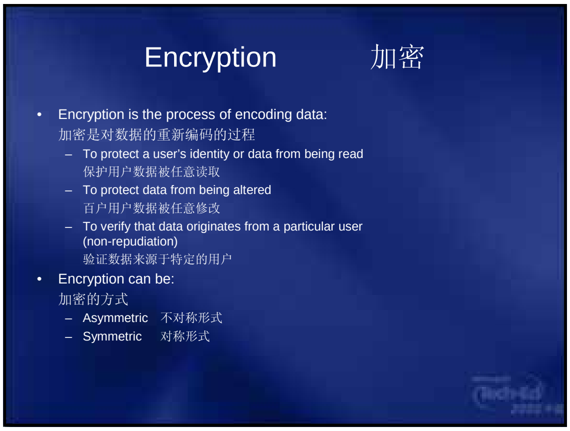
- The Importance of Application Security
  应用系统安全的重要性
- Secure Application Development Practices
  开发安全的系统的实践
- Security Technologies
  可用的安全技术
- Secure Development Guidelines
  开发安全应用的指导



## Overview of Security Technologies
## 安全技术概要

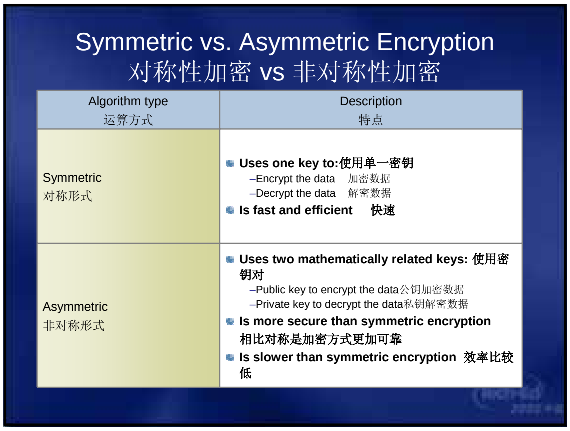
- Developers need to use and apply:
  开发者常常需要下面的一些安全手段

| | |
|---|---|
| – Encryption | 加密 |
| – Hashing | 哈希（散列） |
| – Digital signatures | 数字签名 |
| – Digital certificates | 数字证书 |
| – Secure communication | 安全的通讯方式 |
| – Authentication | 身分认证 |
| – Authorization | 授权 |
| – Firewalls | 防火墙 |
| – Auditing | 审核 |
| – Service packs and updates | 补丁和更新 |



## Encryption 加密

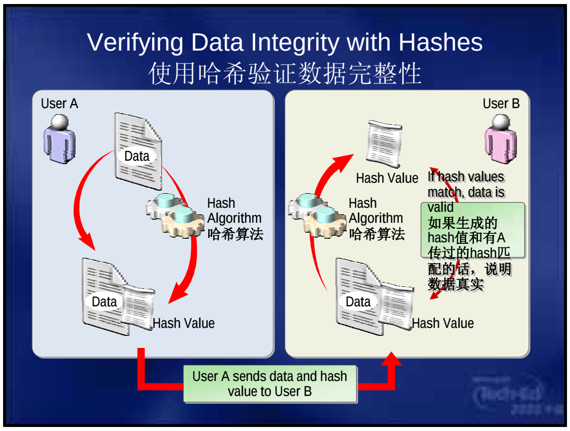
- Encryption is the process of encoding data:
  加密是对数据的重新编码的过程
  - To protect a user's identity or data from being read
    保护用户数据被任意读取
  - To protect data from being altered
    百户用户数据被任意修改
  - To verify that data originates from a particular user (non-repudiation)
    验证数据来源于特定的用户
- Encryption can be:
  加密的方式
  - Asymmetric 不对称形式
  - Symmetric 对称形式



## Symmetric vs. Asymmetric Encryption
## 对称性加密 vs 非对称性加密

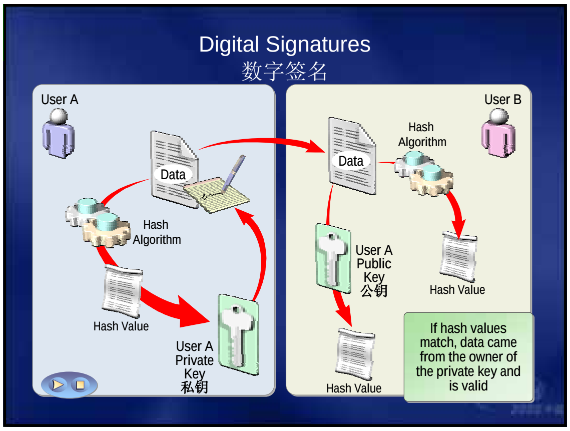
| Algorithm type<br>运算方式 | Description<br>特点 |
|---|---|
| Symmetric<br>对称形式 | **Uses one key to:使用单一密钥**<br>–Encrypt the data 加密数据<br>–Decrypt the data 解密数据<br>**Is fast and efficient 快速** |
| Asymmetric<br>非对称形式 | **Uses two mathematically related keys: 使用密钥对**<br>–Public key to encrypt the data公钥加密数据<br>–Private key to decrypt the data私钥解密数据<br>**Is more secure than symmetric encryption 相比对称是加密方式更加可靠**<br>**Is slower than symmetric encryption 效率比较低** |

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.



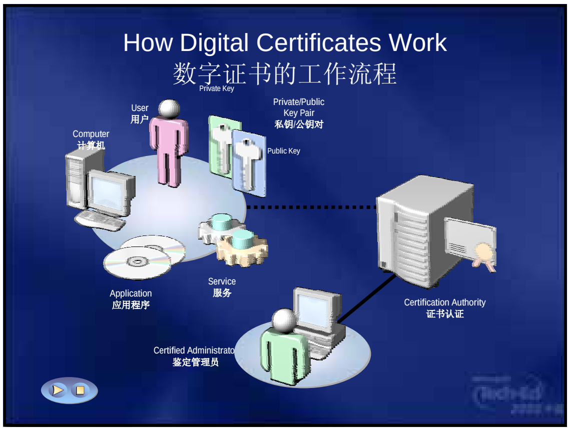
## Verifying Data Integrity with Hashes
## 使用哈希验证数据完整性

If hash values match, data is valid
如果生成的hash值和有A传过的hash匹配的话，说明数据真实

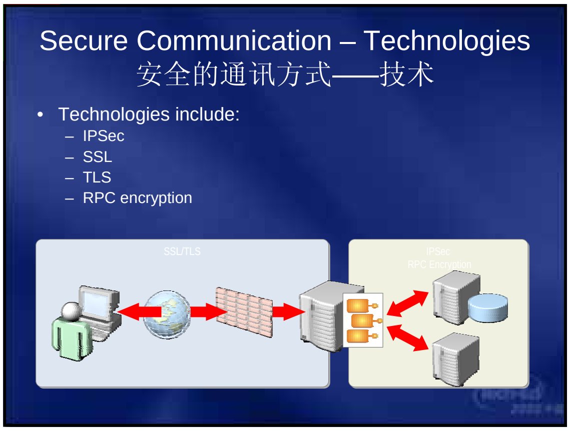


## Digital Signatures
## 数字签名

If hash values match, data came from the owner of the private key and is valid

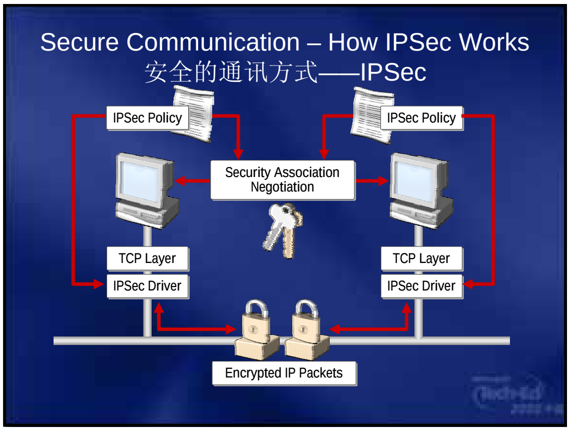


## How Digital Certificates Work
## 数字证书的工作流程

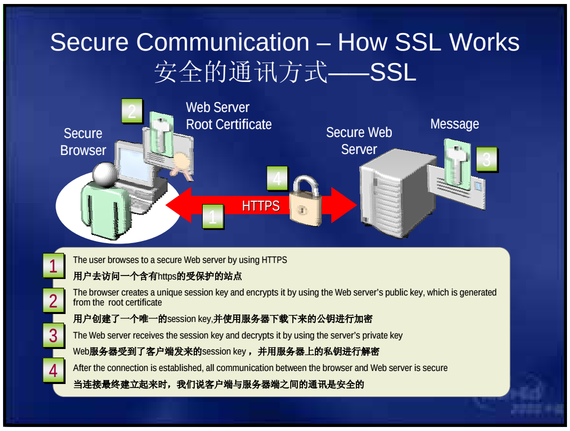


## Secure Communication – Technologies
## 安全的通讯方式——技术

- Technologies include:
  - IPSec
  - SSL
  - TLS
  - RPC encryption



## Secure Communication – How IPSec Works
## 安全的通讯方式——IPSec



## Secure Communication – How SSL Works
## 安全的通讯方式——SSL

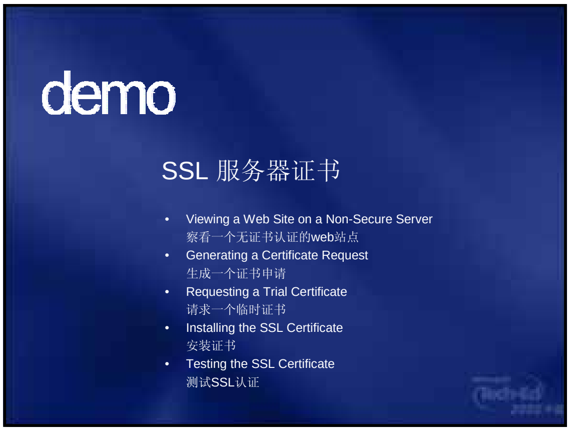
1 The user browses to a secure Web server by using HTTPS
用户去访问一个含有https的受保护的站点

2 The browser creates a unique session key and encrypts it by using the Web server's public key, which is generated from the root certificate
用户创建了一个唯一的session key,并使用服务器下载下来的公钥进行加密

3 The Web server receives the session key and decrypts it by using the server's private key
Web服务器受到了客户端发来的session key，并用服务器上的私钥进行解密

4 After the connection is established, all communication between the browser and Web server is secure
当连接最终建立起来时，我们说客户端与服务器端之间的通讯是安全的

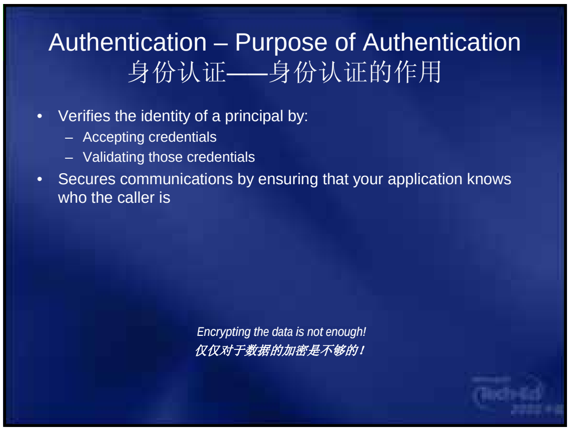
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.



# demo

## SSL 服务器证书

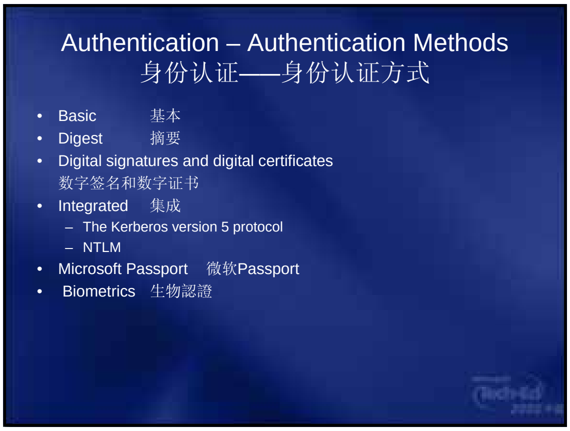
- Viewing a Web Site on a Non-Secure Server
  察看一个无证书认证的web站点
- Generating a Certificate Request
  生成一个证书申请
- Requesting a Trial Certificate
  请求一个临时证书
- Installing the SSL Certificate
  安装证书
- Testing the SSL Certificate
  测试SSL认证



## Authentication – Purpose of Authentication
## 身份认证——身份认证的作用

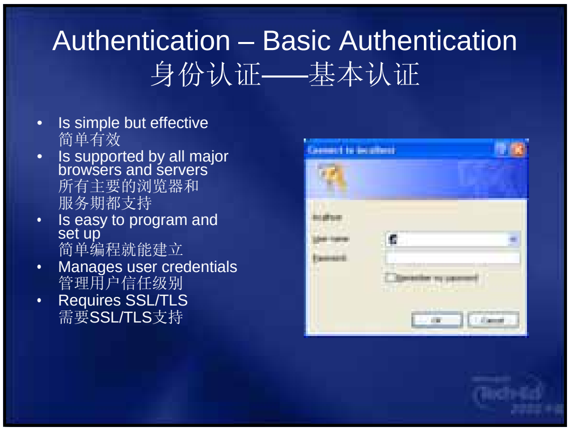
- Verifies the identity of a principal by:
  - Accepting credentials
  - Validating those credentials
- Secures communications by ensuring that your application knows who the caller is

*Encrypting the data is not enough!*
*仅仅对于数据的加密是不够的！*



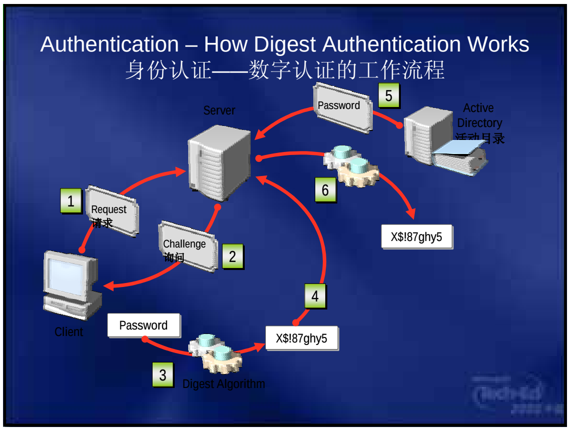
## Authentication – Authentication Methods
## 身份认证——身份认证方式

- Basic 基本
- Digest 摘要
- Digital signatures and digital certificates
  数字签名和数字证书
- Integrated 集成
  - The Kerberos version 5 protocol
  - NTLM
- Microsoft Passport 微软Passport
- Biometrics 生物認證

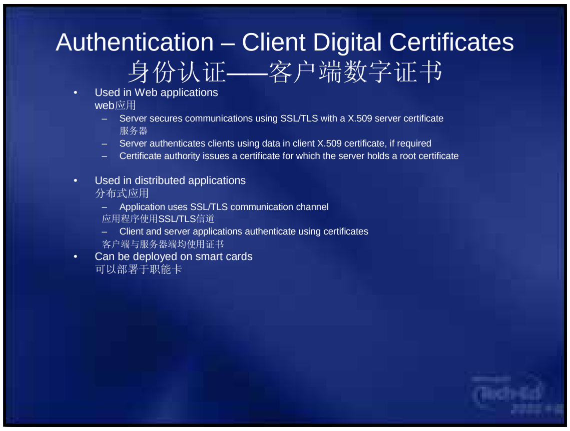


## Authentication – Basic Authentication
## 身份认证——基本认证

- Is simple but effective
  简单有效
- Is supported by all major browsers and servers
  所有主要的浏览器和服务期都支持
- Is easy to program and set up
  简单编程就能建立
- Manages user credentials
  管理用户信任级别
- Requires SSL/TLS
  需要SSL/TLS支持

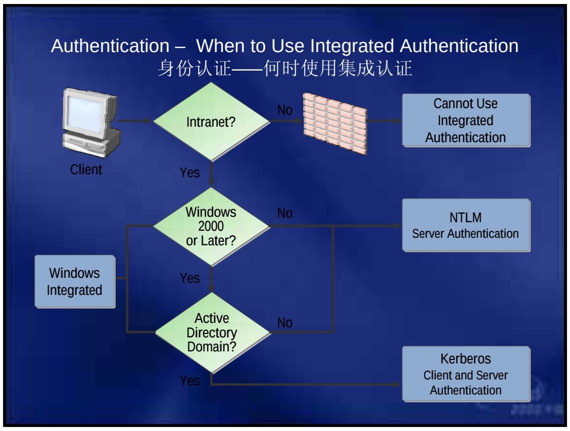


## Authentication – How Digest Authentication Works
## 身份认证——数字认证的工作流程



## Authentication – Client Digital Certificates
## 身份认证——客户端数字证书

- Used in Web applications
  web应用
  - Server secures communications using SSL/TLS with a X.509 server certificate
    服务器
  - Server authenticates clients using data in client X.509 certificate, if required
  - Certificate authority issues a certificate for which the server holds a root certificate
- Used in distributed applications
  分布式应用
  - Application uses SSL/TLS communication channel
    应用程序使用SSL/TLS信道
  - Client and server applications authenticate using certificates
    客户端与服务器端均使用证书
- Can be deployed on smart cards
  可以部署于职能卡



## Authentication – When to Use Integrated Authentication
## 身份认证——何时使用集成认证

Client

Intranet?

No

Cannot Use Integrated Authentication

Yes

Windows 2000 or Later?

No

NTLM Server Authentication

Windows Integrated

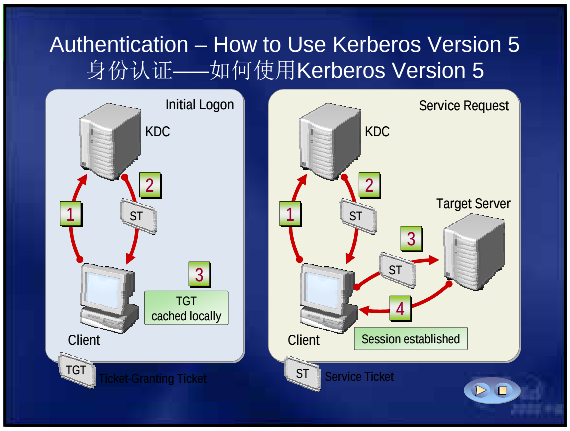
Yes

Active Directory Domain?

No

Yes

Kerberos Client and Server Authentication



## Authentication – How to Use Kerberos Version 5
## 身份认证——如何使用Kerberos Version 5

Initial Logon

KDC

1

2

ST

3

TGT cached locally

Client

Service Request

KDC

Target Server

1

2

ST

3

ST

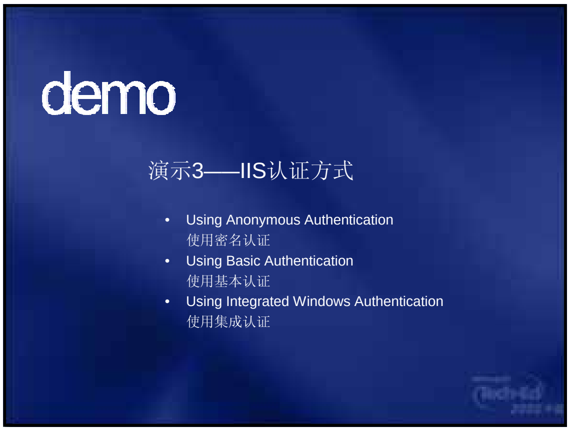
4

Client

Session established

TGT Ticket-Granting Ticket

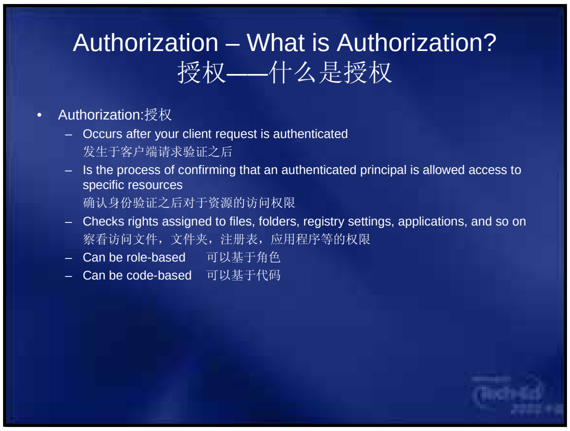
ST Service Ticket



# demo

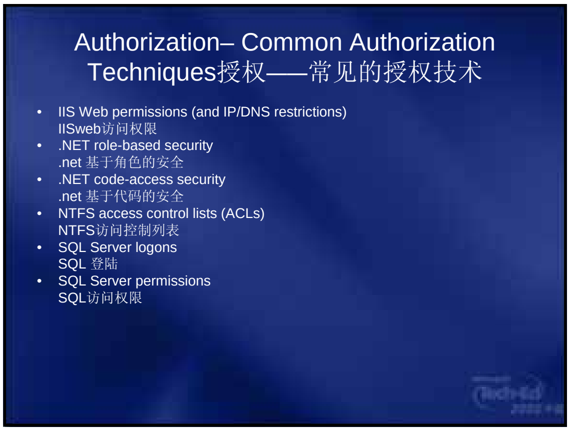
## 演示3——IIS认证方式

- Using Anonymous Authentication
  使用密名认证
- Using Basic Authentication
  使用基本认证
- Using Integrated Windows Authentication
  使用集成认证



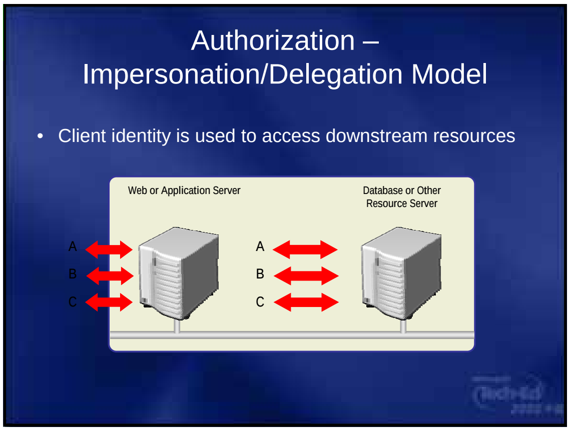
## Authorization – What is Authorization?
## 授权——什么是授权

- Authorization:授权
  - Occurs after your client request is authenticated
    发生于客户端请求验证之后
  - Is the process of confirming that an authenticated principal is allowed access to specific resources
    确认身份验证之后对于资源的访问权限
  - Checks rights assigned to files, folders, registry settings, applications, and so on
    察看访问文件，文件夹，注册表，应用程序等的权限
  - Can be role-based　可以基于角色
  - Can be code-based　可以基于代码



## Authorization– Common Authorization Techniques授权——常见的授权技术

- IIS Web permissions (and IP/DNS restrictions)
  IISweb访问权限
- .NET role-based security
  .net 基于角色的安全
- .NET code-access security
  .net 基于代码的安全
- NTFS access control lists (ACLs)
  NTFS访问控制列表
- SQL Server logons
  SQL 登陆
- SQL Server permissions
  SQL访问权限



## Authorization – Impersonation/Delegation Model

- Client identity is used to access downstream resources

Web or Application Server

Database or Other Resource Server

A

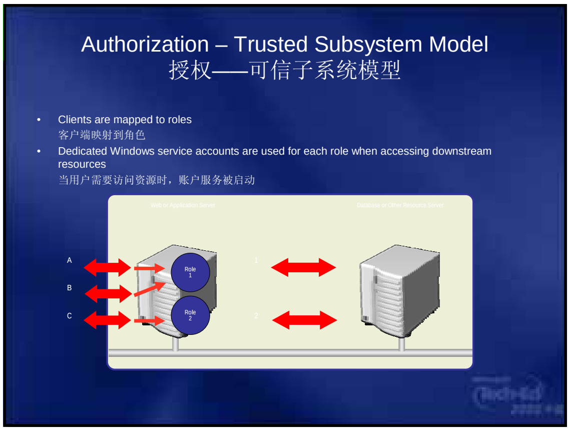
B

C

A

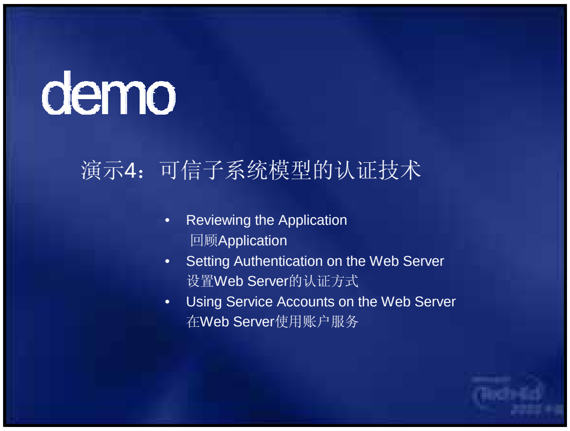
B

C



## Authorization – Trusted Subsystem Model
## 授权——可信子系统模型

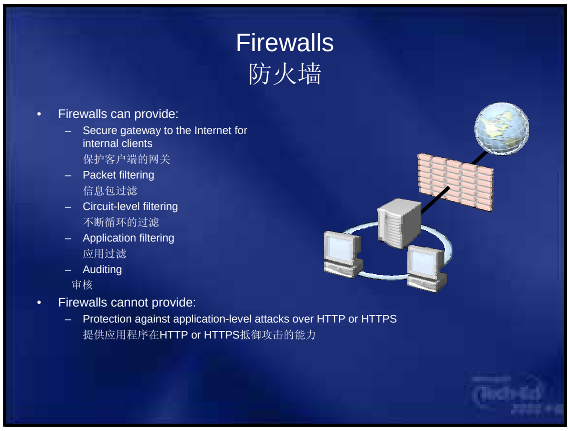
- Clients are mapped to roles
  客户端映射到角色
- Dedicated Windows service accounts are used for each role when accessing downstream resources
  当用户需要访问资源时，账户服务被启动



## demo

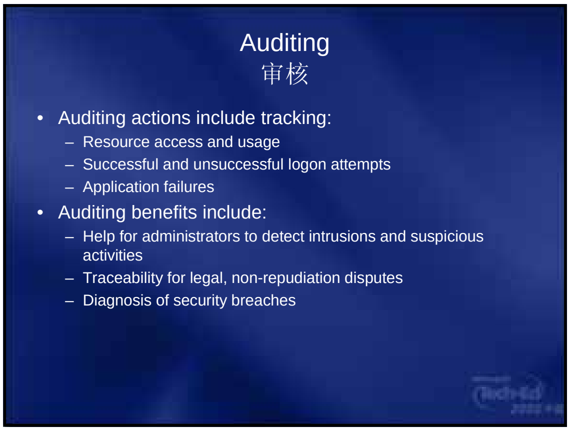
演示4：可信子系统模型的认证技术

- Reviewing the Application
  回顾Application
- Setting Authentication on the Web Server
  设置Web Server的认证方式
- Using Service Accounts on the Web Server
  在Web Server使用账户服务



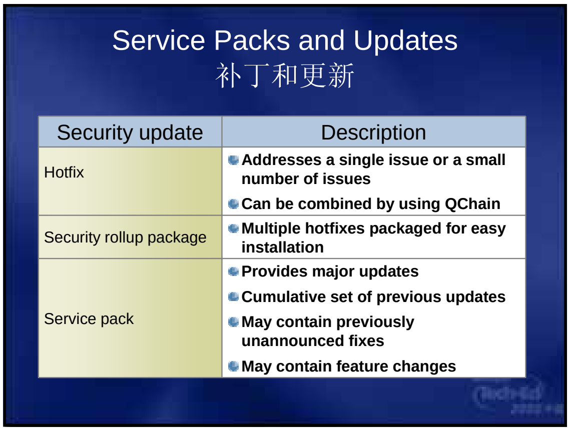
## Firewalls
## 防火墙

- Firewalls can provide:
  - Secure gateway to the Internet for internal clients
    保护客户端的网关
  - Packet filtering
    信息包过滤
  - Circuit-level filtering
    不断循环的过滤
  - Application filtering
    应用过滤
  - Auditing
    审核
- Firewalls cannot provide:
  - Protection against application-level attacks over HTTP or HTTPS
    提供应用程序在HTTP or HTTPS抵御攻击的能力



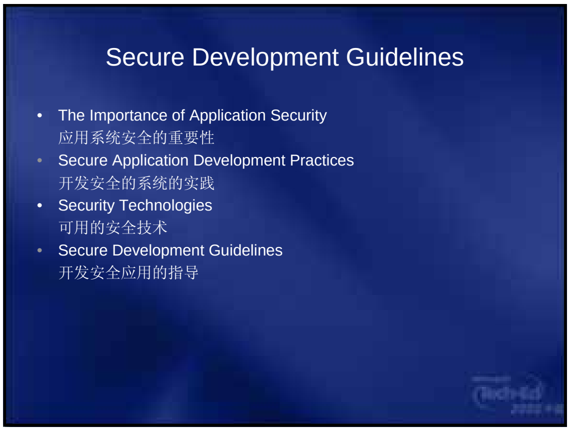
## Auditing
## 审核

- Auditing actions include tracking:
  - Resource access and usage
  - Successful and unsuccessful logon attempts
  - Application failures
- Auditing benefits include:
  - Help for administrators to detect intrusions and suspicious activities
  - Traceability for legal, non-repudiation disputes
  - Diagnosis of security breaches



## Service Packs and Updates
## 补丁和更新

| Security update | Description |
|---|---|
| Hotfix | Addresses a single issue or a small number of issues<br>Can be combined by using QChain |
| Security rollup package | Multiple hotfixes packaged for easy installation |
| Service pack | Provides major updates<br>Cumulative set of previous updates<br>May contain previously unannounced fixes<br>May contain feature changes |



## Secure Development Guidelines

- The Importance of Application Security
  应用系统安全的重要性
- Secure Application Development Practices
  开发安全的系统的实践
- Security Technologies
  可用的安全技术
- Secure Development Guidelines
  开发安全应用的指导

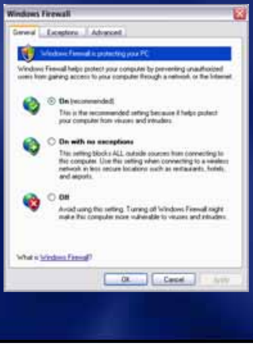
## Proactive Security Development

- Integrate security improvements throughout the development process
  讲安全整合到开发的过程中去
- Focus on security and ensure that your code can withstand new attacks
  关注安全问题，确保您的代码抵御攻击的能力
- Promote the key role of education
  加强关键人员的学习
  - Raise awareness within your team
    提高各团队的安全意识'
  - Learn from your mistakes and from the mistakes of others
    从自己或他人的错误中吸取教训

## Windows XP SP2 Advanced Security Technologies

- Network protection
  网络的保护
- Memory protection
  内存的保护
- Safer e-mail handling
  更加安全处理邮件
- More secure browsing
  更加安全的访问
- Improved computer maintenance
- Protection from internal threats
  提高了应对攻击的手段
- Get more information on Windows XP Service Pack 2
  at http://www.microsoft.com/sp2preview

## Client Firewall turned on by default
## 客户端windows防火墙



Windows Firewall is protecting your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through a network or the Internet.

● On (recommended)
This is the recommended setting because it helps protect your computer from viruses and intruders.

○ On with no exceptions
This setting blocks ALL outside sources from connecting to this computer. Use this setting when connecting to a wireless network in less secure locations such as restaurants, hotels, and airports.

○ Off
Avoid using this setting. Turning off Windows Firewall might make this computer more vulnerable to viruses and intruders.

What is Windows Firewall?

- Closes ports that are not in use
- Reduces RPC attack surface
- Reduces chance of virus spreading from notebooks and VPN clients
- On by default to protect the user by default
- Configurable

## Windows XP SP2 Security enhancements

- DCOM launch permissions
- RPC restrictions
- WebDAV redirector

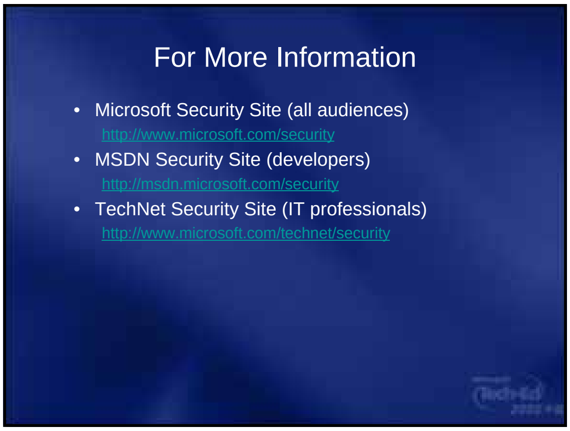
## Session Summary

- The Importance of Application Security
  应用系统安全的重要性
- Secure Application Development Practices
  开发安全的系统的实践
- Security Technologies
  可用的安全技术
- Secure Development Guidelines
  开发安全应用的指导

## 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/

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.



## For More Information

- 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

## Questions and Answers

Microsoft®

您的潜力，我们的动力