您的潜力，我们的动力

Microsoft®
微软（中国）有限公司

智能设备解决方案上的安全开发实践

钟卫

微软（中国）开发与平台技术部

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

- 移动设备解决方案的安全简介
- Device Security设备安全
- Windows Mobile 安全模型
- 通讯安全
- 数据安全

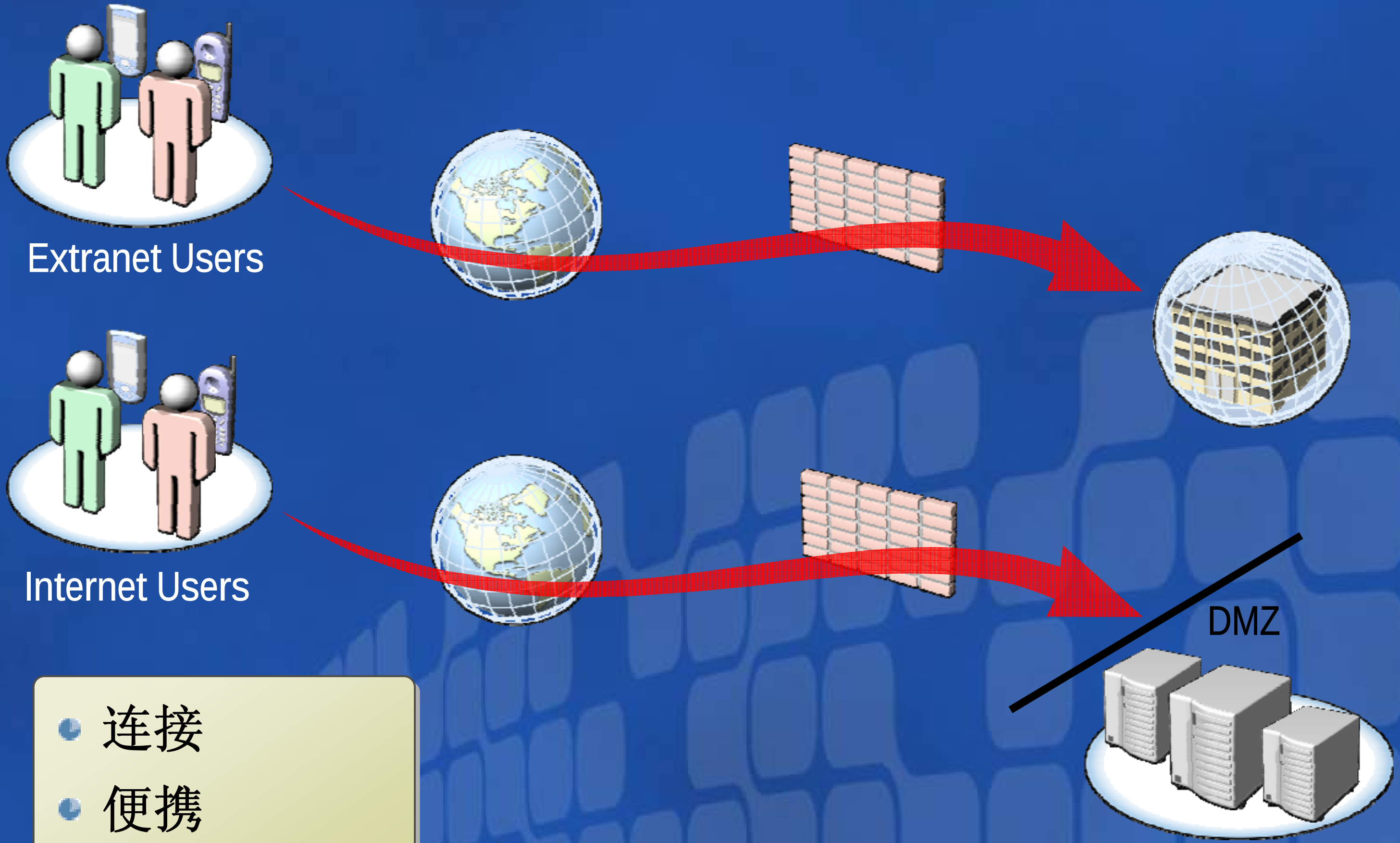
移动设备解决方案的安全简介

- 移动设备解决方案的安全简介
- Device Security设备安全
- Windows Mobile 安全模型
- 通讯安全
- 数据安全

Windows Mobile的市场增长

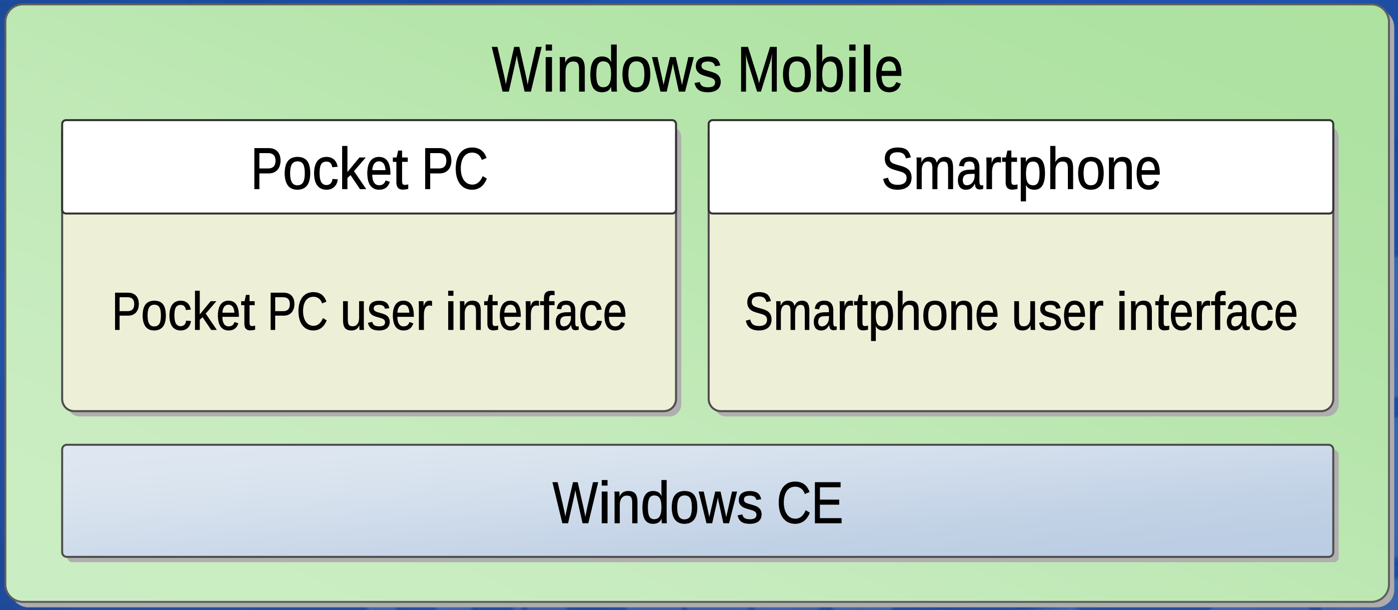
- 61 mobile operators in 28 countries
- 37 Windows Mobile device maker partners
- 380,000+ active Windows Mobile developers
- 2.5 million Visual Studio developers targeting mobile
- In 2004, 31% increase in Mobile2Market certified applications
- In 2004, 35% growth in new developers

Mobile开发的环境特征



- 连接
- 便携
- 安全

Windows Mobile的开发环境



Windows Mobile

Pocket PC

Pocket PC user interface

Smartphone

Smartphone user interface

Windows CE

Windows Mobile offers a consistent user experience and familiar developer APIs and tools

.NET Compact Framework的特征

- 是.NET Framework 内容的一个子集，类层次结构与之兼容
- 不包含那些不适合mobile devices功能的函数和类
- 类似桌面应用开发的环境

The .NET Compact Framework assumes full trust

Windows Mobile Releases

Windows Mobile 2003 and Windows Mobile 2003 Second Edition 都是基于Windows CE 4.2 操作平台的

Windows Mobile 2003 software

- **ROM**内置.NET Compact Framework
- 配置管理
- 支持蓝牙编成
- 短消息服务支持

Windows Mobile 2003 Second Edition software

- 横向显示，支持高分辨分辨率
- QVGA screens for Smartphone

代码

本地代码	应用程序直接运行于操作系统之上
托管代码	应用程序运行于common-language runtime 环境中
服务器端	运行于服务器端的应用

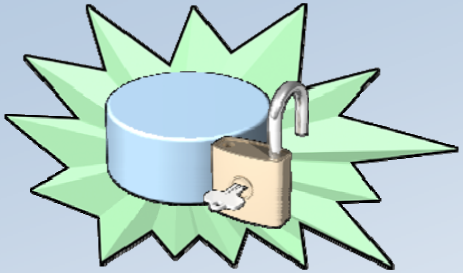
Mobile 开发工具

- Visual Studio .NET 2003
  - Managed code
  - Web services
  - Visual Basic or Visual C#
  - Rapid development
- eMbedded Visual C++
  - Native code
- Mobile emulators
  - Available from MSDN Mobile and Embedded Application Developer Center

推荐使用 Windows Mobile 2003 Second Edition编写应用

常见的攻击方式

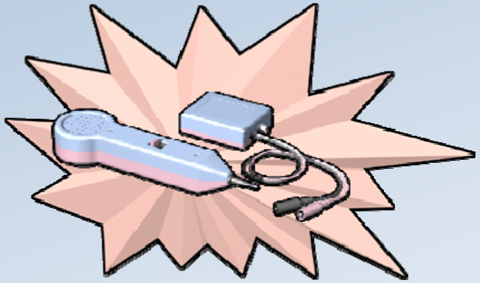
设备遗失或被盗



访问私密数据

对于内部资源未授权访问

通讯攻击



网络监听

Device Security设备安全

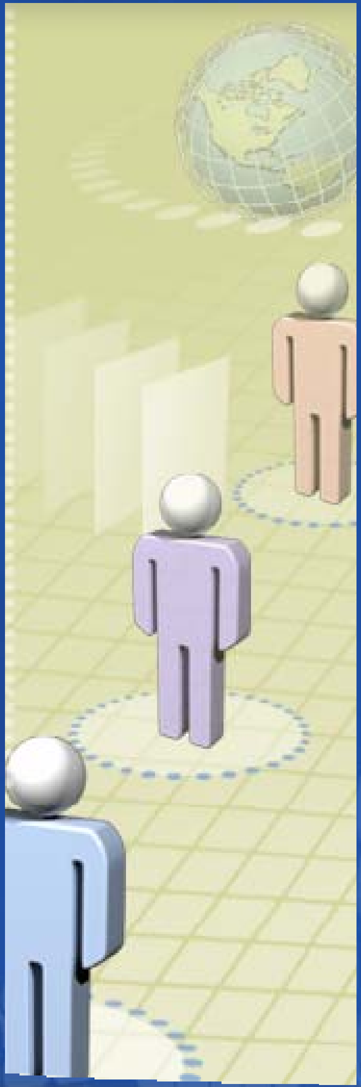
- 移动设备解决方案的安全简介
- Device Security设备安全
- Windows Mobile 安全模型
- 通讯安全
- 数据安全

设备安全和数据存储

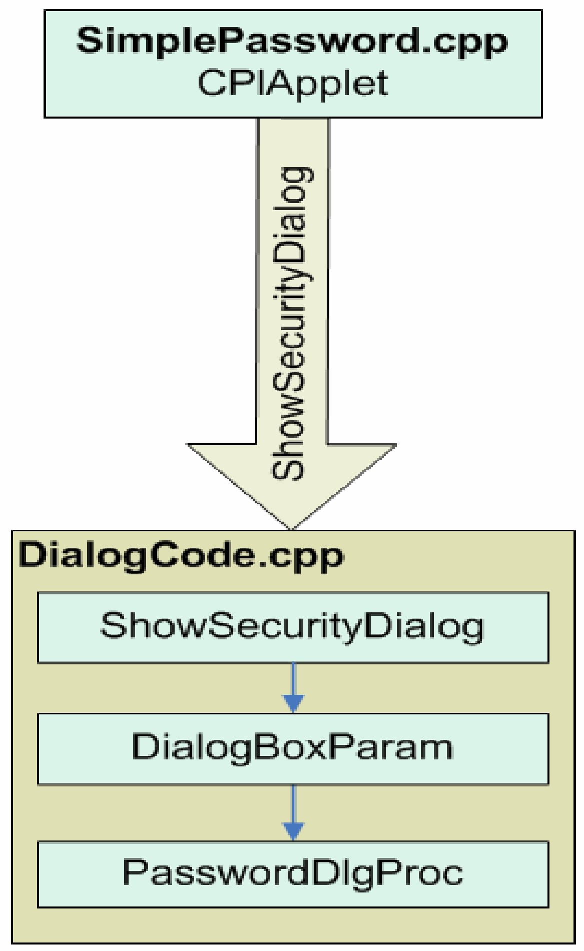
- 通过设备安全防止直接物理访问
- 主要的机制是通过密码保护
- Windows Mobile 2003 支持用户设备密码，也可以使用StartUI登陆组件进行编程

✓ 当多次登陆失败后，自动删除敏感数据

可以使用**StartUI**登陆组件进行编程



Demonstration 1: A Custom Power-on Password



Windows Mobile 安全模型

- 移动设备解决方案的安全简介
- Device Security设备安全
- Windows Mobile 安全模型
- 通讯安全
- 数据安全

应用程序代码签名

Digital Code Signing	Method of authenticating the origin of applications
Application Code Signing	Feature in Windows Mobile software for Smartphones using digital code signing

- The requirement for application code signing is set by the mobile operator
- Developers must be aware of signing requirements

Code Groups and Code Identity

Code Group	Defines what the application is allowed to access once it starts running

Code Groups

- Trusted
- Normal

Code Identity	The identity of the publisher that is responsible for the application

Code Identity classes

- Privileged
- Unprivileged

When Do Applications Need to Run Trusted?为什么应用程序需要

Privileged is necessary when:

- 修改注册表
- 访问短消息子系统
- 访问SIM卡管理模块
- 访问电话通讯管理
- Using low-level system APIs
- Writing a component that plugs into a system-level process or privileged process

证书存储

Certificate Store	Contains the public portion of the digital certificates installed on the phone

Smartphone 包含3种证书存储:

- Unprivileged execution trust authorities certificate store
- Privileged execution trust authorities certificate store
- Installation certificate store安装证书存储

Mobile Code-Signing Development Tools

Code signing development tools for Windows Mobile 2003 software for Smartphone software are located in:

```
C:\Program Files\Windows CE Tools\wce420\
SMARTPHONE 2003\Tools
```

Tool	Description
spdps	Creates privileged developer certificate
signcode	Attaches certificate to .dll or .exe file

通讯安全

- 移动设备解决方案的安全简介
- Device Security设备安全
- Windows Mobile 安全模型
- 通讯安全
- 数据安全

Client/Server 通讯方式

Media	Examples	Characteristics
Mobile	•GSM •CDMA	•Uses air as medium •Supports always on
Wireless	•802.11 •Bluetooth •IrDA	•Uses air as medium •Can be always on or connection-oriented
Wired	•Serial •USB •Ethernet	•Physical medium •Typically connection-oriented

ActiveSync	在mobile 和 桌面computer之间同步数据的软件

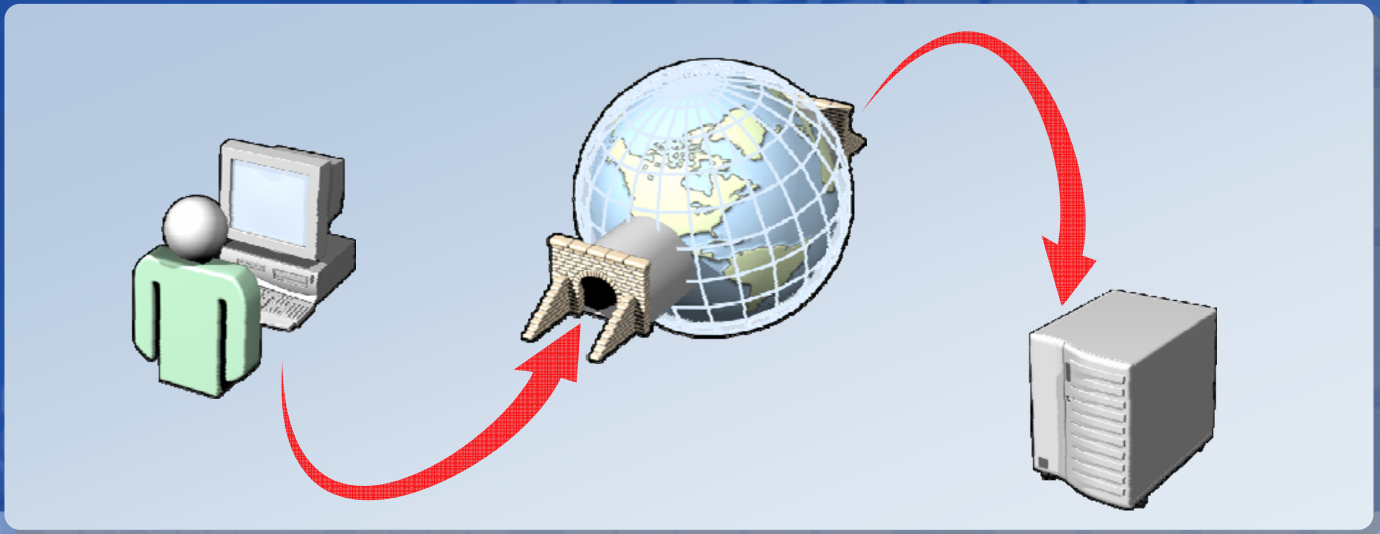
Strategies for Securing Communication Media

- Mitigate security risk associated with wireless connectivity
- Use one of the following to secure wireless data transmission:
  - VPN
  - SSL
  - WEP
  - WPA

Virtual Private Network Tunnels

VPN Tunnel	Provides an encrypted communication path between the client computer and the host computer

- Permits extranet users to connect to an intranet and access resources
- Enterprise-wide decision requiring hardware or software
- Windows Mobile 2003 supports PPTP and L2TP/IPSec



Secure Sockets Layer Sessions

SSL	Secure Sockets Layer A protocol for transmitting encrypted communication over networks

- Most common client-server encryption schema
- SSL is a layered approach
  - Resides on top of the TCP/IP stack
  - Can be used by most applications
- Uses asymmetric encryption to exchange session keys and symmetric encryption for communication once the session is established

WEP and WPA

- WEP
  - – IEEE 802.11 standard
  - – Provides weak encryption

When using WEP also use SSL or VPN for sensitive data

- WPA
  - – Intended as replacement for WEP
  - – Uses TKIP to increase encryption key

数据安全

- 移动设备解决方案的安全简介
- Device Security设备安全
- Windows Mobile 安全模型
- 通讯安全
- 数据安全

Data Storage Media

- Devices are small, light weight, low-power, so fixed storage not viable
- Device format and capacity vary
- Four types of storage:
  - ROM
  - RAM
  - Internal persistent memory
  - External persistent memory

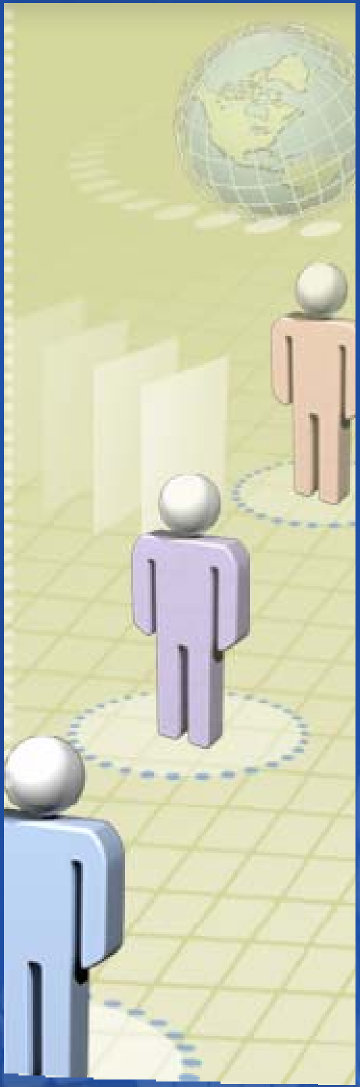
Data Security and SQL Server CE

SQL Server CE is a compact database for mobile devices

SQL Server CE provides data security by:

- ✓ Securing data on the mobile device
- ✓ Supporting secure data transmission

Demonstration 2: Creating an Encrypted SQL Server CE Database

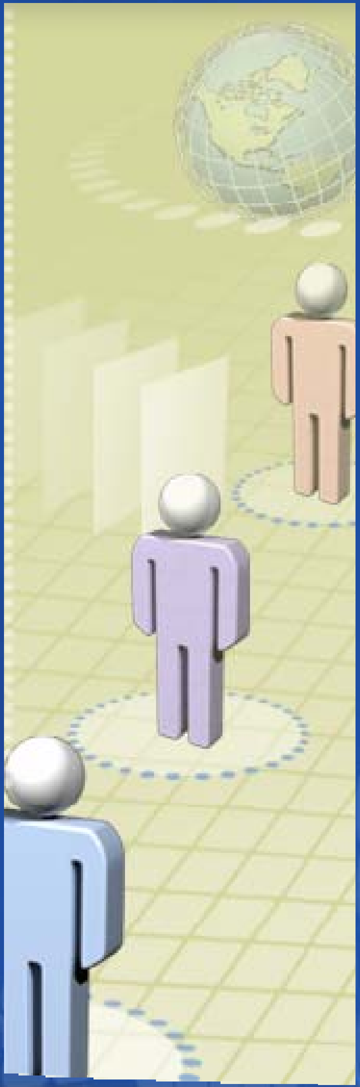


CreateDBButton_Click

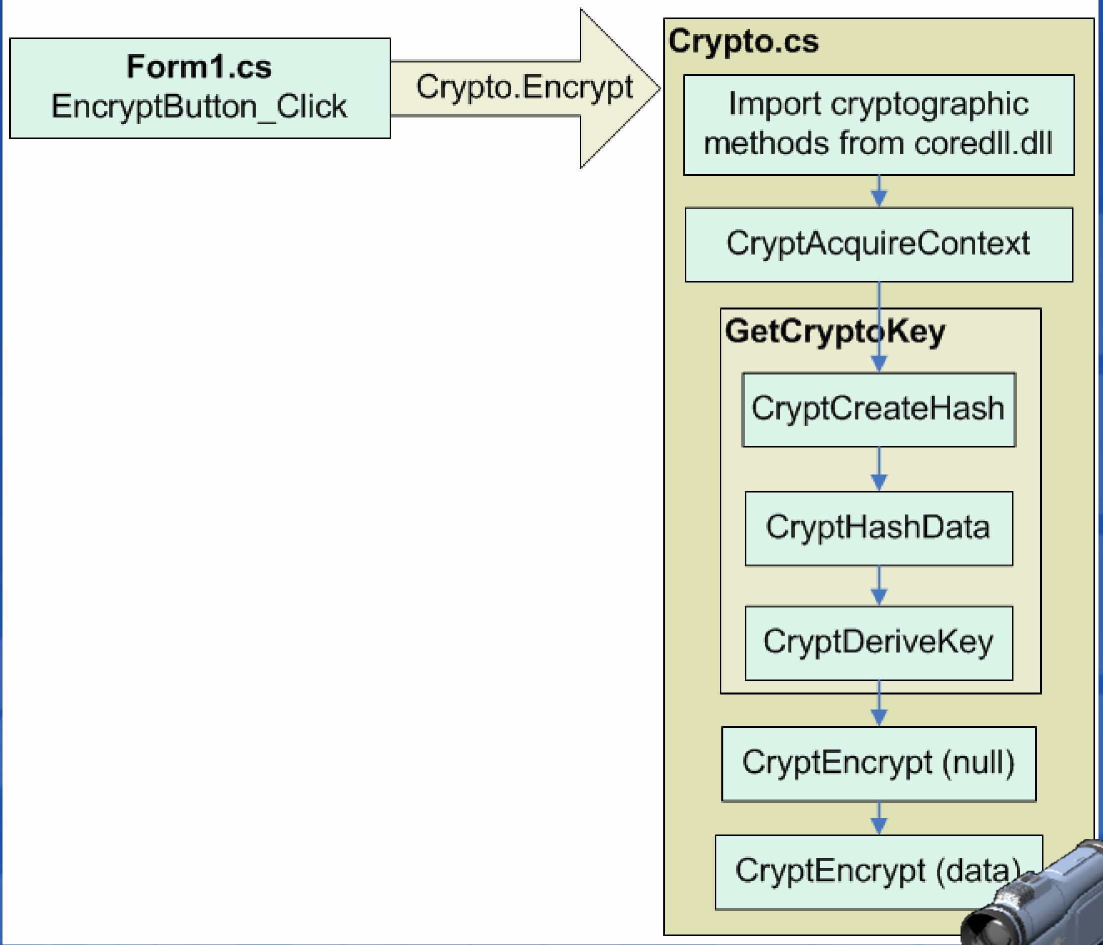
```
SqlCeEngine eng = new SqlCeEngine("Data
    Source = \\my
    documents\\pda.sdf;password=" +
    passwordBox.Text +";encrypt
    database=TRUE");
```

OpenDBButton_Click

```
conn = new SqlCeConnection("Data Source =
    \\my documents\\pda.sdf;password=" +
    passwordBox.Text +";encrypt
    database=TRUE");
```



Demonstration 3: Data Encryption in Windows Mobile



Form1.cs
EncryptButton_Click

Crypto.Encrypt

Crypto.cs

Import cryptographic methods from coredll.dll

CryptAcquireContext

GetCryptoKey

CryptCreateHash

CryptHashData

CryptDeriveKey

CryptEncrypt (null)

CryptEncrypt (data)

Best Practices for Mobile Data Security

Mobile devices can be stolen, therefore data security is essential

- ✓ Password-protect the hardware
- ✓ Avoid storing sensitive data
- ✓ Encrypt your data
- ✓ Backup your sensitive data

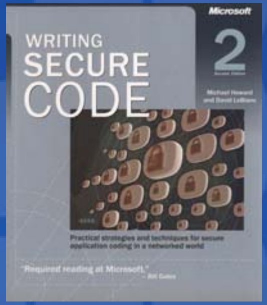
Session Summary

Mobile devices are small and therefore easily stolen

- ✓ Use eMbedded Visual C++ for native applications
- ✓ Use Visual Studio .NET 2003 for managed and server-side applications
- ✓ Write unprivileged normal Smartphone applications
- ✓ Use device password
- ✓ Encrypt sensitive data
- ✓ Consider SQL Server CE when transferring data

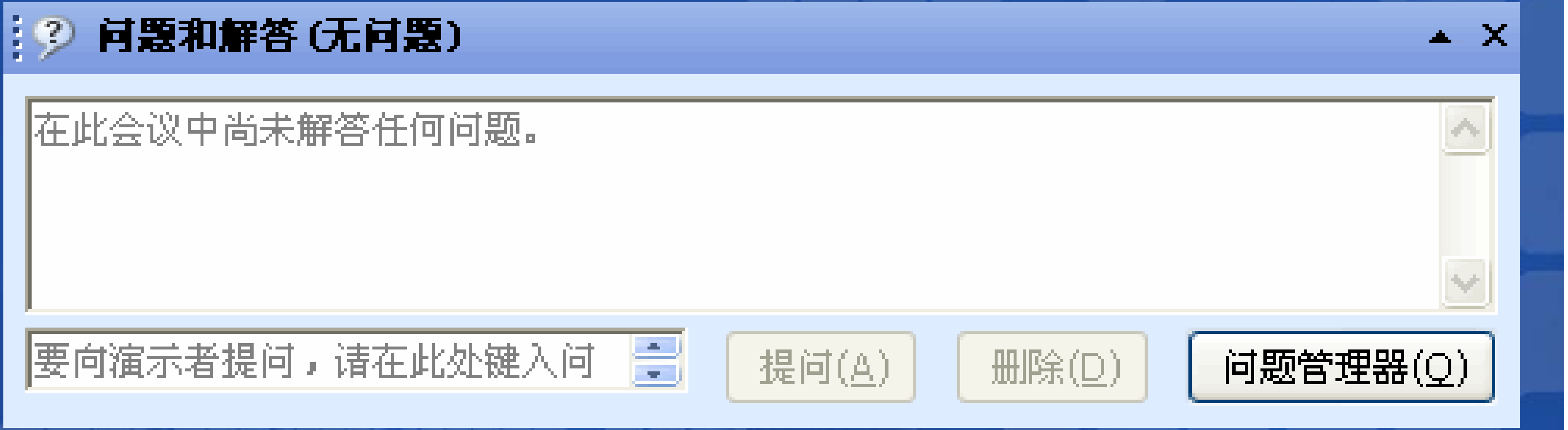
Next Steps

- 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



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。



问题和解答 (无问题)

在此会议中尚未解答任何问题。

您的潜力，我们的动力

Microsoft®
微软（中国）有限公司

Microsoft®

msdn

MSDN Webcasts