Создание безопасных приложений с использованием средств разработки Microsoft

Константин Юштин
Microsoft IT Academy Program
при Киевском Национальном университете имени Тараса Шевченко

канд. физ.-мат. наук

Типичные методы обеспечения безопасности

- Моделирование угроз
- Статические анализаторы кода
- Автоматическое тестирование кода
- Code review
- Ежедневная сборка с проверкой всех тестов
- Минимизация «поверхности атаки»

Статические анализаторы кода

Находят дополнительные ошибки во время компиляции

- Приведения типов
- Быстродействия
- Безопасности
- Операций с памятью

Утилиты:

PREfast, Viva64

Ключи студии **Visual Studio 2005 Team Edition for Software Developers**

/analyze

/GS

/Wp64

Моделирование угроз

1. Диаграммы потоков данных (data flow diagram, DFD).
2. Списки всех сценариев использования приложения, списки уровней привилегий пользователей, списки защищаемых ценностей (assets)
3. Возможные сценарии взлома
   - классификация по STRIDE
   - оценка по шкале опасности DREAD

Утилиты доступные с сайта www.microsoft.com:

- Microsoft Threat Analysis & Modeling tool
- Threat Modeling Tool

Stride: Категоризация Угроз

- Систематический обзор архитектуры с точки зрения атакующего
- Определение ресурсов, угроз, уязвимостей, механизмов защиты и рисков
- Имеет большое значение для тестирования безопасности

Угроза	Защита
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiaton
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Dread: оценка риска уязвимости

- **D**amage potential: Какова величина ущерба при использовании уязвимости?
- **R**eproducibility: Насколько легко повторить атаку?
- **E**xploitability: Насколько легко запустить атаку?
- **A**ffected users: Какой ориентировочный процент пользователей затрагивается?
- **D**iscoverability: Насколько легко найти эту уязвимость?

Расширенное тестирование

- Visual Studio 2005 Team Edition for Testers
- Visual Studio 2005 Team Edition for Database Professionals

Виды тестов

- Модульные (Unit) тесты
- Web тесты
- Нагрузочные (Load) тесты
- Ручные (Manual) тесты
- Внешние (Generic) тесты
- Упорядоченные (Ordered) тесты

Новые средства безопасности в Visual Studio 2005

- Улучшенная защита от переполнения буфера (/GS)
- Статический анализ исходного кода (/analyze)
- Динамический анализ (AppVerifier)
- Безопасные стандартные библиотеки (SafeCRT)
- Встроенный FxCop
- Отладка в зонах (Debug in Zones)
- Улучшенная работы с исключениями
- PermCalc – анализ требований безопасности

Встроенный FxCop

- FxCop - часть Visual Studio
- Статический анализ управляемого кода
- Можно выбрать желаемые проверки в свойствах проекта
- Находит проблемы
  - Безопасности
  - Быстродействия
  - Надежности

Категории возможных проблем с кодом

- Input validation
- Authentication
- Authorization
- Configuration management
- Sensitive data
- Session management
- Cryptography
- Parameter manipulation
- Exception management
- Auditing and logging

Input Validation: Безопасные строковые функции

Содержатся в

- Visual Studio 2005
- Windows SDK начиная с Microsoft Windows XP SP1
- Windows Driver Kit (WDK)
- Driver Development Kit (DDK)

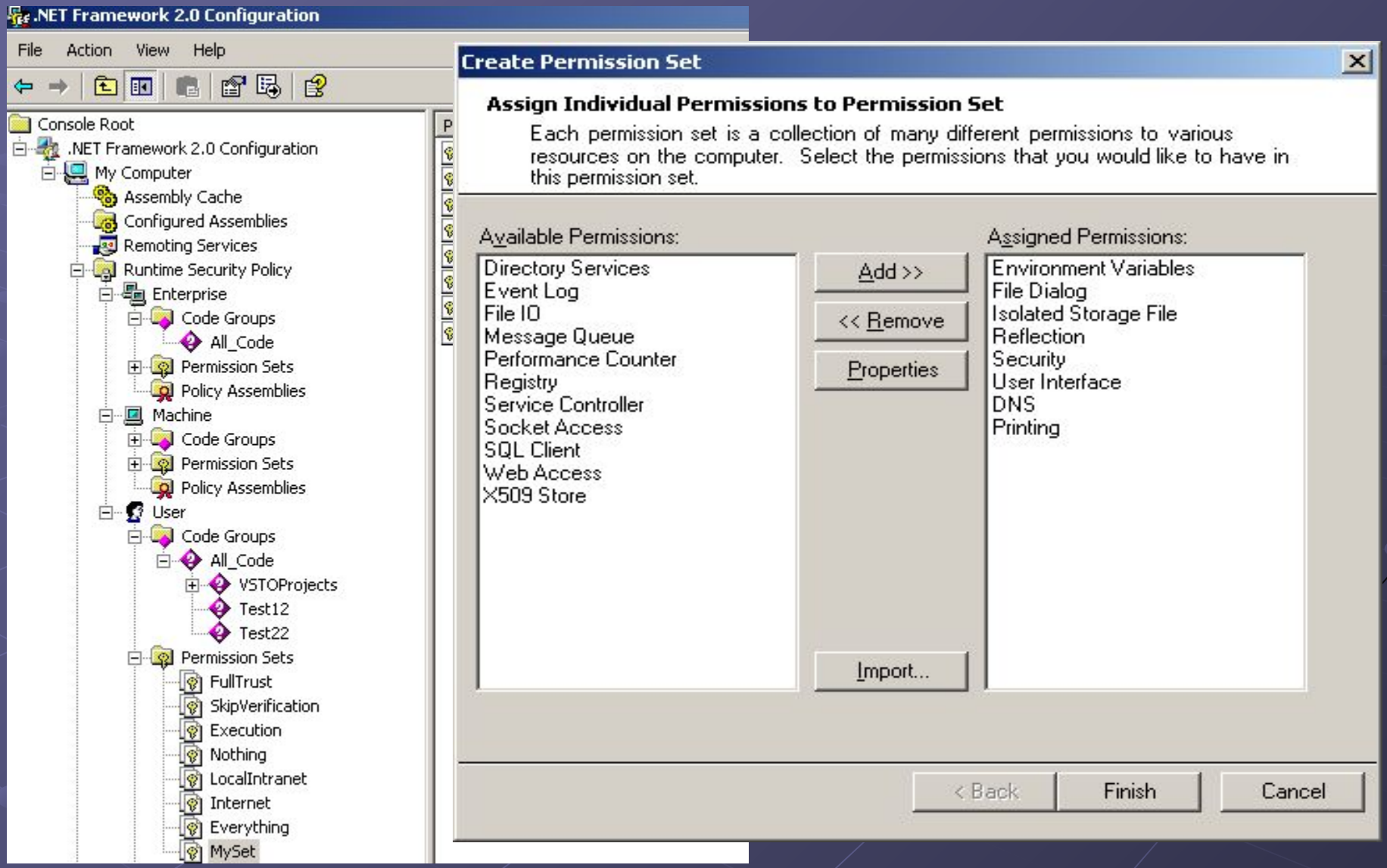
Функции	Цель	Заменяет
RtlStringCbCat и др.	Склейка двух строк	strcat wcscat
RtlStringCbCatN и др	Склейка 2-байтовых строк	strncat wcsncat
RtlStringCbCopy и др.	Копирование строки из буфера	strcpy wcscpy
RtlStringCbCopyN и др.	Копирование строки в буфер с ограничением длины	strncpy wcsncpy
RtlStringCbLength и др.	Определение длины строки	strlen wcslen
RtlStringCbPrintf и др.	Создание форматированной строки	sprintf swprintf _snprintf _snwprintf
RtlStringCbVPrintf и др.	Создание форматированной строки с 1 доп. параметром	vsprintf vswprintf _vsnprintf _vsnwprintf

Code access security .NET Framework

- Права доступа код к системе с фильтрацией:
  - **Simple assembly name**
  - **Code location (URL)**
  - **Zone of origin**
  - **Strong assembly name**
  - **Cryptographic hash**
  - **Authenticode signature**

Декларативный запроса приложения прав для своей сборки

```
assembly: FileIOPermission(SecurityAction.RequestMinimum,
    Unrestricted=true)]
```


.NET Framework 2.0 Configuration
File
Action
View
Help
Console Root
.NET Framework 2.0 Configuration
My Computer
Assembly Cache
Configured Assemblies
Remoting Services
Runtime Security Policy
Enterprise
Code Groups
All_Code
Permission Sets
Policy Assemblies
Machine
Code Groups
Permission Sets
Policy Assemblies
User
Code Groups
All_Code
VSTOProjects
Test12
Test22
Permission Sets
FullTrust
SkipVerification
Execution
Nothing
LocalIntranet
Internet
Everything
MySet
Create Permission Set
Assign Individual Permissions to Permission Set
Each permission set is a collection of many different permissions to various resources on the computer. Select the permissions that you would like to have in this permission set.
Available Permissions:
Directory Services
Event Log
File IO
Message Queue
Performance Counter
Registry
Service Controller
Socket Access
SQL Client
Web Access
X509 Store
Add >>
<< Remove
Properties
Import...
Assigned Permissions:
Environment Variables
File Dialog
Isolated Storage File
Reflection
Security
User Interface
DNS
Printing
< Back
Finish
Cancel

Аутентификация в .NET

Типы аутентификации в .NET Framework:

- **Windows**
- **Generic**
- **Custom**

Cryptography: криптографические функции

- SQL Server 2005 - первая версия SQL сервера, в которой появилась серьезная поддержка криптографии.

- .NET Framework использует цифровую подпись для сборок и специальные классы, реализующие симметричное и асимметричное шифрование в пространстве имен **System.Security.Cryptography**

Достижения

- Согласно внутренним исследованиям корпорации Microsoft, компьютеры с ОС Windows XP с пакетом обновления 2 (SP2) в 13—15 раз менее подвержены заражению вредоносным ПО, чем компьютеры под управлением предыдущих версий Windows XP.
- В Windows Server 2003 было обнаружено на 50 процентов меньше уязвимостей, чем в предыдущей версии, Windows Server 2000.
- С момента выпуска в 2003 г. последней версии веб-сервера корпорации Microsoft, Internet Information Services 6.0, в нем было обнаружено только два уязвимых места.
- В SQL Server 2005 не обнаружено ни одного дефекта с момента выпуска этого продукта в ноябре 2005 года.

(http://www.microsoft.com/rus/midsizebusiness/security/sdl.mspx)

Вопросы ?

Константин Юштин
Microsoft IT Academy Program
при Киевском Национальном университете имени Тараса Шевченко

Microsoft CERTIFIED Professional Developer
Web Developer
Windows Developer

Microsoft CERTIFIED Trainer
Windows Development
Web Development
Enterprise Application Development
Database Development