DEV380
用VS2005轻轻松松开发安全应用

蔺华
ISV开发合作经理
DPE
Microsoft Corporation

您最担心的安全问题是什么?

#1 回答

“提高代码安全性的软件工具”

关于开发人员安全性的一些数据

- “75 percent of hacks happen at the application” - ***Gartner “Security at the Application Level”***
- “The conclusion is unavoidable: any notion that security is a matter of simply protecting the network perimeter is hopelessly out of date” - ***IDC and Symantec, 2004***
- “11 of CERT’s 13 major security advisories for 2003 are bugs arising from programming errors in applications [not the OS]” - ***Carnegie Mellon University***
- “If only 50 percent of software vulnerabilities were removed prior to production … costs would be reduced by 75 percent” - ***Gartner “Security at the Application Level”***
- “The battle between hackers and security professionals has moved from the network layer to the Web applications themselves” - ***Network World***
- “64 percent of developers are not confident in their ability to write secure applications” - ***Microsoft Developer Research***

```
// Example #1
#define MAX (50)
char szDest[MAX];
strncpy(szDest,pszSrc,strlen(pszSrc));
```

Wrong buffer size!

```
// Example #2
#define MAX (50)
char szDest[MAX];
strncpy(szDest,pszSrc,MAX);
pszDest[MAX] = '\0';
```

Wrote NULL to element 51, not 50!

```
// Example #3
string strQry = "SELECT
Count(*) FROM Users
WHERE UserName='" +
txtUser.Text + "' AND
Password='" +
txtPassword.Text + "'";
```

SQL Injection!

Or 1=1 --

➔SELECT Count(*) FROM Users WHERE UserName='' Or 1=1 -- ' AND Password=''
➔SELECT Count(*) FROM Users WHERE UserName='' Or 1=1
➔True

```
string Status = "No";
string sqlstring ="";
try {
    SqlConnection sqlc= new SqlConnection(
          @"data source=localhost;" +
          "user id=sa;password=password;");
    sql.Open();
    sqlstring="SELECT HasShipped" +
          " FROM Shipment WHERE ID='" + Id + "'";
    SqlCommand cmd = new SqlCommand(sqlstring,sql);
    if ((int)cmd.ExecuteScalar() != 0)
        Status = "Yes";
} catch (SqlException se) {
    Status = sqlstring + " failed\n\r";
    foreach (SqlError e in se.Errors) {
        Status += e.Message + "\n\r";
    }
} catch (Exception e) {
    Status = e.ToString();
}
```

Connecting as sysadmin

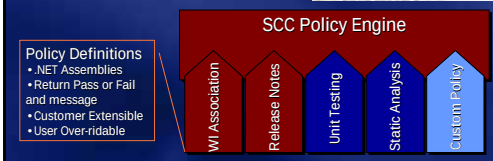
Hard to guess password!

String concat for dynamic SQL

Telling the bad guy too much on failure

Create Project Policies

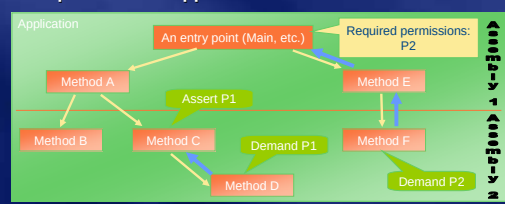
- Create Policies around testing using VSTS



demo

Permission Calculator

- Checks the security requirements of an application
- Statically checks for called APIs
  - For each library API a permission set is returned
- Outputs estimate of minimum set of permissions required to run application

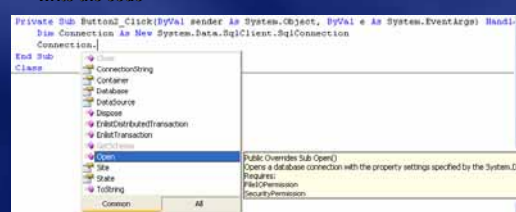


Writing Partial Trust Applications

- Develop and Debug logged in as Least Privilege
  - If a developer wants to write a least privilege application, she can log in as a least privilege user herself
- Code Access Security
  - Enables developers writing managed code to run the code in a sandbox using custom privileges

IntelliSense in Zone

- Set a zone
- Grays out items in the IntelliSense list that would cause an app to violate the security settings
- Allows developers to catch security issues before they actually write the code



demo

VB.NET My Classes

- Exposes easy to use methods for many tasks
  - My.User.IsAuthenticated
  - My.User.CurrentPrincipal.Identity
  - My.User.IsInRole
  - My.User.Name

Data Protection API

- Built into .NET Framework 2.0
- Makes it easy to secure data
- Uses underlying features of Windows 2000 and up

ASP.NET Membership Service

- Service for managing users and credentials
  - Declarative access via Web Site Admin Tool
  - Programmatic access via Membership and MembershipUser classes
- Membership class provides base services
- MembershipUser class represents users and provides additional services
- Provider-based for flexible data storage

ASP.NET Role Management Service

- Role-based security in a box
  - Declarative access via Web Site Admin Tool
  - Programmatic access via Roles class
- Roles class contains static methods for creating roles, adding users to roles, etc.
- Maps users to roles on each request
  - Replaces Application_AuthenticateRequest
- Provider-based for flexible data storage

demo

ASP.NET Configuration Class

- Gateway to the configuration API
- Provides merged view of configuration settings for machine or application
- ConfigurationManager implementation for combination Winform/Webform apps
- ConfigurationManagerpart of System.Configuration
- Can be used to automatically encrypt/decrypt sections

Static Analysis Tools

- PREfast
  - Scans applications built in C/C++ for security vulnerabilities
    - Examples:
      - Buffer overruns
      - Un-initialized memory
      - Memory leaks
- FxCop
  - Scans managed code for 200 total defects
    - Examples
      - SQL injection
      - Permissions
      - Pointers

Integrated Bug Tracking

- Easy, Integrated into development process
- Design your own process – Fields, Forms, States, Rules
- Extensive linking – bugs, reports, artifacts
- Notifications

C++ SafeCRT Libraries

- Changes in C/C++ Libraries where specific functions were found to have unsafe design
- Example: ***char** * strcpy **(char * dest, const char * src)***
- Microsoft has deprecated these functions
- Compiler warnings when inherently unsafe functions are used

demo

Code Coverage and Stress Testing

- Code Coverage
  - Code coverage analysis
  - Enables development teams to know with confidence how much and what parts of their code is exercised by their testing, thus allowing them to focus on the weak spots.
- Load/Stress Testing
  - Some defects only manifest themselves when the server is put under load or stress.
  - Includes load/stress testing for your web applications.

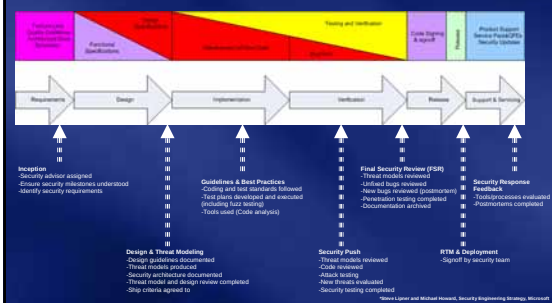
/GS Switch

- /GS Switch
  - Used to mitigate buffer overrun exploits
  - Used to recompile Windows XPSP2 and Windows Server 2003
  - Considerable enhancements
  - On by default

Application Verifier

- Application Verifier
  - Focuses on detecting the common issues that deal with application security and quality such as:
    - heap corruption
    - handle
    - locks
  - Results in:
    - Better quality
    - Increased security
    - Reduced debugging time
  - Native code

Security Development Lifecycle



http://msdn.microsoft.com/security/sdl

Conclusion

- Security is a challenge
- People, Process, and Tools
- Visual Studio 2005 will help you write more secure code with innovative tools and features

http://msdn.microsoft.com/security

Questions?

Microsoft®

您的潜力，我们的动力