What we will cover:

- Why is security so important?
  - Security fundamentals
  - Hacking overview
  - Computer crime metrics
  - Computer crime and the law
  - Reducing your security risk and product demonstrations
  - Recovering from a security breach

Level 100

What we will cover:
Security Fundamentals
The Security Stack
Security Fundamentals
A Comprehensive Security Plan

- Process & Policies - Security processes and policies must be achievable, concise and well-defined to obtain your security objectives.
- Infrastructure – Typically includes firewalls, intrusion detection and prevention.
- Product Security – Each product will usually have Security Best Practices.
- OS Security – Applying security best practices to your OS and keeping current on patches and updates is critical.
Security Fundamentals
A Comprehensive Security Plan

- Application Security – Incorporating development best practices is paramount to a secure solution. Failure to do so can leave an opening which will allow hackers to bypass all other layers of security.

- Database Security – Securing your database can be accomplished by following the security best practices.

- Physical Security – Restrict access to your business assets.
Security Fundamentals
Microsoft Developers and Security “The Last Mile”

Threats
- Hackers
- Competitors
- Foreign Governments
- Disgruntled Employees

Security Index
- 100
- 80
- Adequate Security

Assets
- Customers and Employees
- Microsoft Reputation
- IP
- Money

Security Fundamentals Microsoft Developers and Security “The Last Mile”
Hacking Overview
Most Pervasive Hacking Techniques

- Cross-site scripting
- Buffer overflow
- Backdoor and debug options
- Forceful browsing
- Stealth commanding
- SQL injection
- Hidden field manipulation
- Cookie poisoning
- Cryptographic hacking
Hacking Overview Definitions

- Cross-Site Scripting – Scripting, usually JavaScript, that attacks the browser, not the web server.
- Buffer Overflow – Dumping as much data as possible into an input field.
- Backdoor and Debug Options - Programmers will sometimes forget to remove backdoor or debugging options from code before deploying into production. This may allow malicious users to gain access to the site.
Hacking Overview Definitions (continued)

- Forceful Browsing – Hackers try to gain access to files and directories by guessing what they are and typing them into the URL.
- Stealth Commanding – Hackers can embed script into a e-greeting form for example, which would then be mailed out and could run on the receiving user’s computer.
- SQL Injection - A form of attack on a database driven Web site in which the attacker executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet.
Hacking Overview Definitions (continued)

- Hidden Field Manipulation - Hidden fields are embedded within HTML forms to maintain values that will be sent back to the server. These fields can be manipulated and potentially damage the application.
- Cookie Poisoning - Modification of a cookie (personal information in a Web user's computer) by an attacker to gain unauthorized information about the user, potentially allowing the hacker to impersonate the user.
- Cryptographic Hacking – Homegrown weak cryptographic algorithms used to encrypt data. Hackers break them to gain control of important information.
Computer Crime Metrics Unauthorized Use of Computer Systems Within the Last 12 Months

[Bar chart showing percentage of respondents for different years]

Source: Computer Security Institute

Computer Crime Metrics Unauthorized Use of Computer Systems Within the Last 12 Months
Computer Crime Metrics

Internet Connection is Increasingly Cited as a Frequent Point of Attack

![Bar chart showing increased percentage of Internet as point of attack from 1999 to 2003.]

Source: Computer Security Institute

- 2003: 445 Respondents/84%
- 2002: 481 Respondents/66%
- 2001: 314 Respondents/72%
- 2000: 443 Respondents/60%
- 1999: 314 Respondents/60%

Computer Crime Metrics Internet Connection is Increasingly Cited as a Frequent Point of Attack
Computer Crime Metrics Likely Sources of Attack

Source: Computer Security Institute

2003: 488 Respondents/92%
2002: 414 Respondents/82%
2001: 484 Respondents/91%
2000: 583 Respondents/90%
1999: 460 Respondents/88%
Computer Crime Metrics
Dollar Amount of Losses By Type

CSIS/IBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute
Computer Crime and the law
Applicable Laws

- Computer Fraud and Abuse Act of 1986
- Electronic Communications Privacy Act of 1986
- Computer Security Act of 1987
- National Information Infrastructure Protection Act of 1996
- Gramm-Leach-Bliley Financial Services Modernization Act
- Health Insurance Portability and Accountability Act (HIPAA)
- The Sarbanes-Oxley Act of 2002
Computer Crime and the law
Legal Liability

- Laws generally take aim at hackers and other individuals who abuse computer networks for illegal purposes
- Collection amount from a hacker may be small
- Companies that maintain the computer applications and networks, on the other hand, tend to have deeper pockets, and it appears likely that victims of security breaches will seek redress from them
Reducing Your Security Risk
Security Assessments

- Remote scan (application)
- Remote scan (network)
- Threat assessment
- Risk assessment
- Technical assessment
  - Application
  - Database
  - Infrastructure
- Process and policies assessment
- Physical assessment
Reducing Your Security Risk
Getting Started

- Envisioning - Identify your potential threats and electronic assets
- Envisioning - Determine the appropriate amount of security for your needs
- Envisioning - Perform a security inventory
- Planning - Perform a security assessment (all areas)
- Planning – Create the Security and Disaster Recovery Plans
- Developing – Implement (non production) your security plan
- Stabilizing – Test your security via security assessment
- Deploying – Deploy your security solution
Recovering from a Security Breach
Disaster Recovery Plan

- Disaster Recovery should not be limited to natural disasters and technical failures
- Disaster Recovery Plan should be prepared, tested and updated regularly
- Recovering from a disaster without a Disaster Recovery Plan can be time consuming, costly and prevent business continuity
- Plan should be understood by all personnel involved in the recovery process

Recovering from a Security Breach Disaster Recovery Plan
Recovering from a Security Breach
Disaster Recovery Considerations

- Secure offline storage
- Computer Forensics capability
- Co-location
- Mirror Site
- Customer & Partner notification procedures
Principals of Secure Design
Implement Application Security Best Practices

- Use platform based Authentication and Authorization
- No input is trusted
- Avoid storing sensitive data in cookies and hidden fields
- Secure sensitive data
- Use managed code
- Do not build SQL statements on the fly
- Avoid use of weak cryptography
- Run with least privilege account
- Fail intelligently
- Enable logging
- Perform code reviews
- Defense in depth
- Security test plan (assessments, etc.)
Secure Design Implementation
Security Best Practices

Authenticate (Internet focus)
- Partition website
- ASP.NET Forms Authentication (SSL)
- Use SALT and Hash for user passwords
- Protect authentication cookie

Authorize (Internet focus)
- IIS NTFS Permission
- URL Authorization for page and directory access
- .NET Roles at class, method or code level

Validate input
- Centralize validation
- Validate input on the server side
- Use ASP.NET Validators and regular expressions
- Validate data for type, length, format, and range
- Sanitize your input - HtmlEncode
Secure Design Implementation  
Security Best Practices... Continued

- Sensitive data handling
  - Sensitive data is not passed across pages; it is maintained using server side state management
  - Avoid plain text passwords in configuration files
  - Use .NET Cryptography for encrypting sensitive data
  - Do not cache sensitive data

- Further secure assemblies with .NET code access security
  - Restrict which code can call you (authorize code)
  - Restrict what your code can do (constrain code)
Secure design Implementation
Security Best Practices... Continued

- Secure data access
  - Use Integrated Windows® Authentication for SQL Server™
  - Use stored procedures and use parameters collections when building SQL statements
- Secure communication via SSL and IPSec
- Defense in depth
  - IIS – Apply security patches, IISLockown, URLScan
  - Web application security
  - OS security, network security

Secure design Implementation  Security Best Practices... Continued
Demonstration 1

demo

Secure Coding Techniques
A Sharing Slide

[ Share C ]
Demonstration 2
demo
Code Access Security

Demonstration 2
A Sharing Slide

[ Share B ]
Demonstration 3

demo

Sanctum AppScan DE
A Sharing Slide

[ Share F ]
Reducing Your Security Risk Assessment Tools

- Microsoft Baseline Security Analyzer

- Sanctum http://www.sanctuminc.com/

- eEye http://www.eeye.com/html/

- FxCop www.godotnet.com/team/fxcop - Code analysis tool that checks .NET managed code assemblies for conformance to the Microsoft .NET Framework Design Guidelines

- IIS Lockdown
Reducing Your Security Risk
Product Security Best Practices

- Windows Server 2003 -

- Application Center -


- Commerce Server -
Reducing your security risk
Product Security Best Practices (continued)

- Content Management Server -

- Exchange Server -
  http://www.microsoft.com/exchange/techinfo/security/

- Operations Manager -

SQL Server -
Additional Resources


- [download.microsoft.com/download/4/f/8/4f89f896-f020-46d1-ada0-08a18e8432d5/aspnet_security.ppt](download.microsoft.com/download/4/f/8/4f89f896-f020-46d1-ada0-08a18e8432d5/aspnet_security.ppt) - ASP.NET: Security Best Practices To Protect Against Hacker Attacks

- [www.securityfocus.com](http://www.securityfocus.com) - BugTraq, SecurityFocus Vulnerability Database

- [www.sans.org](http://www.sans.org) - Top 20 Internet Security Vulnerabilities and remediation measures, Security Policy samples, GIAC Certification

- [www.gocsi.com](http://www.gocsi.com) - Annual CSI/FBI Computer Crime Study, alerts, newsletters and publications

- [www.cert.org](http://www.cert.org) - Studies Internet security vulnerabilities, provides incident response services to sites
Get Up to Speed on .NET

Get Trained on Microsoft Developer Technologies

Register for an upcoming webcasts at http://www.microsoft.com/usa/webcasts/

All times are Pacific Standard Time

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Webcast Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuesday, February 17, 2004</td>
<td>11:00AM-12:00PM</td>
<td>MSDN Architecture Webcast: Advanced Architecture Issues</td>
</tr>
<tr>
<td>Tuesday, February 17, 2004</td>
<td>1:00PM-2:30PM</td>
<td>MSDN Webcast: Working with Classes and Class Libraries</td>
</tr>
<tr>
<td>Tuesday, February 17, 2004</td>
<td>1:00PM-2:30PM</td>
<td>MSDN Webcast: Creating a Single Sign-On Enterprise Security Portal</td>
</tr>
<tr>
<td>Wednesday, February 18, 2004</td>
<td>9:00AM-10:30AM</td>
<td>MSDN Webcast: Dave's Secure Remoting Chat Application</td>
</tr>
<tr>
<td>Wednesday, February 18, 2004</td>
<td>1:00PM-2:30PM</td>
<td>MSDN Webcast: Protecting Your System From SQL Injection Attacks</td>
</tr>
<tr>
<td>Thursday, February 19, 2004</td>
<td>9:00AM-10:30AM</td>
<td>MSDN Webcast: Application Hacking Techniques and How to Stop Them</td>
</tr>
</tbody>
</table>
Where Can I Get MSDN?

- Purchase, renew or upgrade an MSDN subscription at http://msdnbuynow.one.microsoft.com
- Free online developer resources at msdn.microsoft.com
- Free MSDN Flash Newsletter at msdn.microsoft.com/flash
- Free MSDN local events in your area at www.msdnevents.com
DevDays is coming to a city near you

Register now for just US$99 AND get a FREE Developer Welcome Kit.
http://www.microsoft.com/devdays2004

Each DevDays attendee will receive:

- DevDays DVD featuring presentations and sample code for all sessions
- “Whidbey” pre-release software
- ASP.NET Resource CD – NEW!
- Smart Client Resource DVD
- SQL Server 2000 Evaluation Edition
Questions?

- Submit text questions using the “Ask a Question” button
- For recordings of past MSDN Webcasts: www.microsoft.com/usa/webcasts/ondemand
- Don’t forget to fill out the survey.
- Got webcast content ideas? Email us at: webcasts@microsoft.com

Survey Slide