Security Development Lifecycle

Russ McMahon
Associate Professor of Information Technology
School of Computing & Informatics
College of Engineering & Applied Science
University of Cincinnati

Cincinnati Chapters ISSA, OWASP*, ISACA*, InfraGard*
A Founder of TechLife Cincinnati
http://www.meetup.com/TechLife-Cincinnati/

Microsoft Security Development Lifecycle (SDL)

Delivering secure software requires:
Executive commitment → SDL a mandatory policy at Microsoft since 2004

Ongoing Process Improvements → 6 month cycle

SDL Threat Modeling Tool

• is a tool designed for rich client/server app dev
  – requires Visio 2007
  – uses STRIDE methodology
    • Spoofing, Tampering, Repudiation, Info disclosure, DoS, Elevation of privilege
    • Based on Microsoft Security Response Center (MSRC) issues and Common Vulnerability and Exposures (CVE) (cve.mitre.org)
  – videos available
  – assumes the final deployment pattern is unknown
    • If it will be used to manage business-critical applications with customer credit cards or not
  – focus → to ensure security of the underlying code
  – Security Development Lifecycle Version 4.1a (127p)
    • Includes a SDL for Agile Development section

Where Do I Start?

• Microsoft Security
  – msdn.microsoft.com/en-us/library/cc448120.aspx (policies)
• Security Development Lifecycle
  – NIST – The Economic Impacts of Inadequate Infrastructure for SW Testing
• Digital Blackbelt Series
• Microsoft ForeFront (Business Ready Security)

Microsoft SDL Threat Modeling Overview

Microsoft SDL Threat Modeling: A process to understand security threats to a system, determine risks from those threats, and establish appropriate mitigations

• Microsoft SDL Threat Modeling
  1. Diagramming – Data Flow Diagrams (DFDs)
  2. Threat Enumeration
  3. Mitigation
  4. Validation
• Can be performed by both security and non-security experts
• 4 Steps
  – Diagram – Analyze – Describe – Report

STRIDE Threat Types

<table>
<thead>
<tr>
<th>Desired Property</th>
<th>Threat</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Spoofing</td>
<td>Impersonating something or someone else</td>
</tr>
<tr>
<td>Integrity</td>
<td>Tampering</td>
<td>Modifying code or data without authorization</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Repudiation</td>
<td>The ability to claim to have not performed some action against an application</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Information Disclosure</td>
<td>The exposure of information to unauthorized users</td>
</tr>
<tr>
<td>Availability</td>
<td>Denial of Service</td>
<td>The ability to deny or degrade a service to legitimate users</td>
</tr>
<tr>
<td>Authorization</td>
<td>Elevation of Privilege</td>
<td>The ability of a user to elevate their privileges with an application without authorization</td>
</tr>
</tbody>
</table>

NR-CIA3
### Examples of Standard Mitigations

<table>
<thead>
<tr>
<th>Threat</th>
<th>Example Standard Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>Digital signatures, message authentication codes</td>
</tr>
<tr>
<td>Tampering</td>
<td>Digital signatures, message authentication codes</td>
</tr>
<tr>
<td>Repudiation</td>
<td>Digital signatures, message authentication codes</td>
</tr>
<tr>
<td>Information Disclosure</td>
<td>Encryption, ACLs</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>ACLs, quotas</td>
</tr>
<tr>
<td>Elevation of Privilege</td>
<td>ACLs, group or role membership, input validation</td>
</tr>
</tbody>
</table>

- Refer to Chapter 9 of the Microsoft SDL for a more complete listing.

### SDL Optimization Model

- A framework to gradually move development organizations towards the adoption of the Security Development Lifecycle (SDL)
- 5 docs
  - Intro (14p)
  - 4 maturity levels
    - Security is reactive; customer risk is undefined
    - Security is proactive; customer risk is understood
    - Security is integrated; customer risk is controlled
  - Advanced to Dynamic (v1s 3 - 4) (18p)
    - Security is specialized; customer risk is minimized
  - Self-Assessment Guide (21p)

### Overview - SDL Developer Starter Kit

- Secure Design Principles
  - Attack surface
  - Threat modeling
  - SDL principles
- Secure Implementation Principles
  - covers some the more common types of attacks
  - basically reflects the tools that they currently have
- Threat Modeling Principles Overview
  - SDL
  - STRIDE
- Threat Modeling Tool Principles
  - 4 steps – SDL Threat Modeling tool

### Tools

- Many of these integrate with VS 2008
- MiniFuzz File Fuzzer
  - inputting malformed data into an application and analyzing the application’s reaction to the malformed data
- BinScope Binary Analyzer
  - reports on dangerous constructs of your binaries
- FxCop
  - an application that analyzes managed code assembles (code that targets the .NET Framework common language runtime) and reports information about the assemblies, such as possible design, localization, performance, and security improvements

- [Overview - SDL Developer Starter Kit](http://msdn.microsoft.com/en-us/library/bb288454.aspx)
- [MiniFuzz File Fuzzer](http://blogs.msdn.com/sdl/archive/2007/09/20/fuzz-testing-at-microsoft-and-the tríage process.aspx)
- [FxCop](http://msdn.microsoft.com/en-us/library/bb429476(VS.80).aspx)
• SiteLock
  – for ActiveX controls -- can be used in an Active Template Library (ATL) or C++ project to help you write a secure control that restricts the domains in which it can be scripted
  – Copy sitelock.h to your include directory or into your Visual C++/ATL project to use it.

• Anti-Cross Site Scripting v3 beta
  • www.codeplex.com/AntiXSS
  – How do I sanitize HTML using Anti-XSS
    • msdn.microsoft.com/en-us/library/dd68975(VS.80).aspx
  – Protecting Contoso
    • msdn.microsoft.com/en-us/library/aa73913.aspx

• Web Protection Library (WPL)
  – contains libraries to protect web applications from common vulnerabilities and attacks -- Security Runtime Engine (SRE)
  – goal - comprehensive web app protection with minimal configuration
  – protection for SQL Injection, Click Jacking, File Canonicalization
  – Connected Information Security Framework or CISF
    • blogs.msdn.com/securitytools
  – Risk Tracker
    • risktracker.codeplex.com/
    • sqlinjection.codeplex.com
  – is exploitable -- crash analysis & security risk assessment
    • www.codeplex.com/msedbg

Tools

[Image of SiteLock]

Tools

[Image of Web Protection Library]

Tools

[Logo for Contoso]

Tools

[Image of Web App Configuration Analyzer (WACA)]

Tools

[Image of SQL Injection Code Scanning Tools]

SQL Injection Code Scanning Tools

• Any code, developed in any language, that accesses any type of database using a dynamically built SQL statement is suspect for SQL injection

<table>
<thead>
<tr>
<th>Microsoft Tool</th>
<th>Applies To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft FxCop</td>
<td>.NET Framework languages</td>
</tr>
<tr>
<td>Microsoft Visual Studio Code</td>
<td>.NET Framework languages</td>
</tr>
<tr>
<td>Analysis Feature (Analyza)</td>
<td></td>
</tr>
<tr>
<td>Microsoft Source Code Scanner</td>
<td>Legacy ASP Code</td>
</tr>
<tr>
<td>Analyzer for SQL Injection</td>
<td></td>
</tr>
</tbody>
</table>

Tools

[Image of CAT.NET]

Tools

[Image of Code Analysis Tool (.NET)]

Tools

[Image of Web App Configuration Analyzer (WACA)]

Tools

[Image of Web Protection Library (WPL)]

Tools

[Image of SQL Injection Code Scanning Tools]
SDL Process Template for VSTS

• The SDL Process Template -- leverages the technology of Visual Studio Team System & Team Foundation Server to integrate the policy, process and tools of the SDL v4.1
• There are 5 short videos (downloadable)
  – A lot of features apply to C/C++

SDL Blog & War Stories

• How to open a parachute during free-fall: Introducing Quick Security References (QSRs)
• HeapSetInformation in Visual C++ 2010 beta 2
• Introducing the InfoSec Assessment & Protection Suite
• SDL War Story Videos
  • http://www.microsoft.com/security/bakingsecurityin/video.htm
  – Steve Lipner & Michael Howard
  – comic strip with a cast of characters
  > Agents of SDL (Kevlar) vs Legion of Malware

Data Flow Diagrams (DFDs) Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Represented By</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Entity</td>
<td></td>
<td>Any entity not within the control of the application, such as people and external systems</td>
</tr>
<tr>
<td>Process</td>
<td></td>
<td>Code, such as native code executables and .NET assemblies</td>
</tr>
<tr>
<td>Data Store</td>
<td></td>
<td>Data at rest, such as registry keys and databases</td>
</tr>
<tr>
<td>Data Flow</td>
<td></td>
<td>How data flows between elements, such as function calls and network data</td>
</tr>
<tr>
<td>Trust Boundary</td>
<td></td>
<td>A point within an application where data flows from one privilege level to another, such as network sockets, external entities and processes with different trust levels</td>
</tr>
</tbody>
</table>

SDL Book

• The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software
• By: Michael Howard; Steve Lipner
• Publisher: Microsoft Press
• Pub. Date: June 28, 2006
• Print ISBN-10: 0-7356-2214-0
• Pet Shop 4.0 risk analysis example (Chapter 9)
  – PetShop for .NET 3.5 on www.codeplex.com

TAM Tool

• Threat Analysis & Modeling Tool – SDL-LOB
  – an asset-focused tool designed for LOB applications for the non-security subject matter expert
  > msdn.microsoft.com/en-us/library/dd833775.aspx
  – based on the CIA model
  – where business objectives, deployment pattern, and data assets and access control are clearly defined
  – focus -- to understand the business risk in the application, help identify controls needed to manage that risk, and protect the assets
• App Consulting & Engineering (ACE) team
  • Six Rules to Stop Bad Guys
  • InfoSec Assessment & Protection Suite
  • Dogfooding: How Microsoft IT InfoSec Dogfoods:

TAM Tool

• 3 main areas of the tool
  – threat modeling methodology
  – gathering application architecture
  – security guidance
  > 3.0 beta (videos available)
• The Value of Microsoft TAM (2009)
Other Microsoft Resources

- Security Guidance Center
  - www.microsoft.com/security/default.aspx
- MSDN Security Center
- Channel9 Videos
  - channel9.msdn.com/TAGS/Safety
- MSDN Webcast: Writing Secure Code
- IT Compliance Management Guide (GovncRskComp) (2009)

Other Threat Modeling Systems

- OWASP
- Trike (Squeak)
  - www.octotrike.org/faq/
  - map.squeak.org/package/2b30a0d6-a812-46ad-ba5e-3a72045565b3
  - seclists.org/webappsec/2005q1/138
- AS/NZ 4360:2004 Risk Mgmt
  - superseded by AS/NZS ISO 31000:2009
  - info@cert.org/octave/methodintro.html
- OCTAVE (CERT)
  - CVSS – Common Vulnerability Scoring System(DHS)
- Open Source Risk Mgmt Tools

OCTAVE

- CERT
  - www.cert.org/octave/methodintro.html
  - Operationally Critical Threat, Asset, and Vulnerability Evaluation
  - CIA based
  - for smaller organizations
  - 3 Phases – 8 Processes
    - Build Asset Based Threat Profiles (P1-4)
    - Identify Infrastructure Vulnerabilities (P5-6)
    - Develop Security Strategy and Plans (P7-8)
  - presented at 2009 ISACA Information Security and Risk Management conference
  - OWASP does not anticipate that OCTAVE will be used at large
    by application designers/developers
    - it fails to take threat risk modeling into consideration by all participants, to
      reduce the overall risk of an application becoming vulnerable to attack

DHS CVSS

- National Vulnerability Database
  - http://nvd.nist.gov/
  - Vulnerability Search Engine (CVE software flaws and CCE misconfigurations)
  - National Checklist Program (automatable security configuration
guidance in XCCDF and OVAL)
  - SCAP (program and protocol that NVD supports)
  - SCAP Complitable Tools
  - SCAP Data Feeds (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
  - Impact Metrics (CVSS)
  - Product Dictionary (CPE)
  - Common Weakness Enumeration (CWE)
• Forum of Incident Response and Security Teams (FIRST)
  – an international confederation of trusted computer incident response
teams who cooperatively handle computer security incidents and
promote incident prevention programs
  • www.first.org
• Common Vulnerability Scoring System v2
  – open framework for communicating the characteristics and impacts
  of IT vulnerabilities
  – ensures repeatable accurate measurement while enabling users to
  see the underlying vulnerability characteristics that were used to
  generate the scores
  – Two uses are:
    • prioritization of vulnerability remediation activities
    • calculating the severity of vulnerabilities discovered on one's systems

Open Source Risk Mgmt Tools

• Information can be found at SourceForge.net (or not)
• CORAS Risk Assessment Platform*
• Open Source Requirements Mgmt Tool (OSRMT)*
• ISO 17799 Risk Assessment Toolkit (RAT)
• ThreatMind (2005) – based on FreeMind
• OSMR (2005) – based on ISO 17799
• MARCO -- MAximized Risk COntrol
• Easy Risk Assessment (2006)
• ARMS (2007) – based on ISO 17799 (27001)
• Minaccia (2005)

Open Source Risk Mgmt Tools

• Open Source Requirements Management Tool
  – requirements management tool designed to achieve full SDLC
  traceability for features, requirements, design, implementation and
testing (osrmt_01_50_mar28)
  – It is rated well (25/29 users)
• ISO 17799 (27000) Risk Assessment Toolkit
  – there was nothing on SourceForge
  – plenty of other organizations with their own 27k tools (~$1k)
  • www.27005.net
  • www.27001.com/products/32
  • www.27001central.com/iso17799.htm
  • www.17799-toolkit.com/

Open Source Risk Mgmt Tools

• CORAS Risk Assessment Platform
  – a European research and technological development project for
  model-based security risk assessment
    • www.ercim.eu/publication/Ercim_News/enw49/dimitrakos.html
  – platform for risk analysis of security critical IT systems using
  UML, based on the CORAS model-based risk assessment
    methodology
    • coras.sourceforge.net/
  – contains an XML and UML repository, facilitating management
  and reuse of analysis results (beta 2.1b1 Windows)
    • www2 nr no/ /coras/

Whatever Else

• DREAD (is dead)
  • writing.asp.net/hubby/archive/2005/11/15/43662.aspx
• A Practical Approach to Threat Modeling (2008)
  • www.devx.com/security/Article/37502/1763/page1
  – Information Assurance Technology Analysis Center (IATAC)
  – Data and Analysis Center for Software (DACS)
• Software security blog -- hackerco.de/
• SAFECode -- www.safecode.org/
• Improving Information Security Risk Analysis Practices …
  – Beachboard, Cole & others
    • Issues in Informing Science and Information Technology, vol 5, 2008 (iisit.org)
• Secure World -- www.hellosecureworld.com
• “Beautiful Security” Chapter 9 download
• DataLossDB -- datalossdb.org/