

Security Development Lifecycle

Russ McMahon

Associate Professor of Information Technology,
School of Computing Sciences & Informatics
College of Engineering & Applied Science
University of Cincinnati

Are you ready for a
snipe hunt?



ASIS, InfraGard, ISACA, ISSA, OWASP, 2600
A Founder of TechLife Cincinnati

<http://www.meetup.com/TechLife-Cincinnati/>



ZARF Is With You Again

- What was Multics?
- What year was the 1st federal prosecution of computer fraud?
- For an expert bent on crime, cracking a computer system's defenses is about as difficult as _____.
- Human error accounts for _____ of all data losses
- List 6 security problems for today's companies:
- True/False
- Most detected frauds are never reported.
- Dishonest insider (>, <, or =) evil outsider
- Ideally, the first step in securing a system would be to shot the programmer.
- Ratio of undiscovered to discovered crime may be on the order of 10 to 1.
- Passwords often turn out to be laughably weak defense.



Where Do I Start?

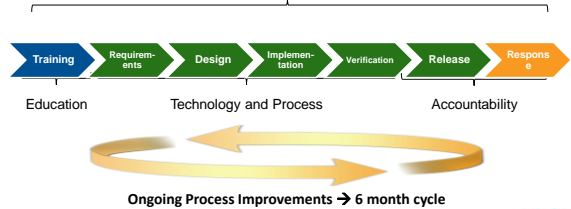
- Microsoft Security
 - msdn.microsoft.com/en-us/security/default.aspx
 - msdn.microsoft.com/en-us/security/cc448120.aspx (pubs +)
 - msdn.microsoft.com/en-us/library/ee790621.aspx (agile dev)
 - www.microsoft.com/security/msec.aspx (Security Eng Ctr)
- Security Development Lifecycle (v5.0)
 - <http://www.microsoft.com/security/sdl/default.aspx>
 - msdn.microsoft.com/en-us/library/84aed186-1d75-4366-8e61-8d258746b09a.aspx
 - 2004 – Microsoft mandatory policy
 - introduces security and privacy early and throughout the development process
 - is risk-based
 - msdn.microsoft.com/en-us/library/ms995349.aspx
 - NIST – The Economic Impacts of Inadequate Infrastructure for SW Testing
 - www.nist.gov/director/prog-ofc/report02-3.pdf
 - csrc.nist.gov/
- Digital Blackbelt Series
 - www.microsoft.com/events/series/digitalblackbelt.aspx?tab=overview



Microsoft Security Development Lifecycle (SDL)

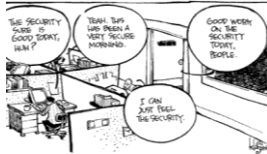
Delivering secure software requires:

Executive commitment → SDL a mandatory policy at Microsoft since 2004



Threat Modeling Overview

- 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



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
 - <http://msdn.microsoft.com/en-us/security/sdl-threat-modeling-tool.aspx>
 - 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 5
 - Creative Commons license
 - Includes a SDL for Agile Development section
 - <http://www.microsoft.com/security/sdl/default.aspx>
 - msdn.microsoft.com/en-us/library/84aed186-1d75-4366-8e61-8d258746b09a.aspx



STRIDE Threat Types

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

NR-CIA3



Identifying STRIDE Threats by DFD Element Type

Element	S	T	R	I	D	E
External entity	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Data Store		✓	✓	✓	✓	
Data Flow		✓		✓	✓	

Data stores are affected by reputation threats whenever the data stores themselves are a log



Examples of Standard Mitigations

Threat	Example Standard Mitigations
Spoofing	IPsec Digital signatures Message authentication codes Hashes
Tampering	ACLs Digital signatures Message Authentication Codes
Repudiation	Strong Authentication Secure logging and auditing
Information Disclosure	Encryption ACLs
Denial of Service	ACLs Quotas High availability designs
Elevation of Privilege	ACLs Group or role membership Input validation

- Refer to Chapter 9 of the Microsoft SDL for a more complete listing
 - <http://www.microsoft.com/learning/en/us/books/8753.aspx>



SDL Optimization Model

- A framework to gradually move development organizations towards the adoption of the Security Development Lifecycle (SDL)
 - <http://msdn.microsoft.com/en-us/security/sdl-model-optimization.aspx>
- 5 docs
 - Intro (14p)
 - 4 maturity levels
 - Basic to Standardized (lvs 1 - 2) (29p)
 - Security is reactive; customer risk is undefined
 - Security is proactive; customer risk is understood
 - Standardized to Advanced (lvs 2 - 3) (29p)
 - Security is integrated; customer risk is controlled
 - Advanced to Dynamic (lvs 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 of 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

- 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
 - blogs.msdn.com/securitytools/archive/2009/07/09/web-protection-library-wpl-a-brief-introduction.aspx
 - channel9.msdn.com/posts/Jossie/Using-the-Web-Protection-Library-WPL-CTP-Version/
 - msdn.microsoft.com/en-us/security/dd547422.aspx
- Connected Information Security Framework (CISF)
 - blogs.msdn.com/securitytools/archive/2009/07/28/an-introduction-to-the-connected-information-security-platform-or-cisf.aspx
- Risk Tracker
 - risktracker.codeplex.com/
- !exploitable -- crash analysis & security risk assessment
 - www.codeplex.com/msecdbg



Data Flow Diagrams (DFDs) Elements

Element	Represented By	Description
External Entity		Any entity not within the control of the application, such as people and external systems
Process		Code, such as native code executables and .NET assemblies
Data Store		Data at rest, such as registry keys and databases
Data Flow		How data flows between elements, such as function calls and network data
Trust Boundary		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



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
- 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/d8931975.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
 - <http://msdn.microsoft.com/en-us/security/aa570413.aspx>
 - http://blogs.msdn.com/ace_team/
 - Six Rules to Stop Bad Guys
 - InfoSec Assessment & Protection Suite
 - Dogfooding: How Microsoft IT InfoSec Dogfoods:

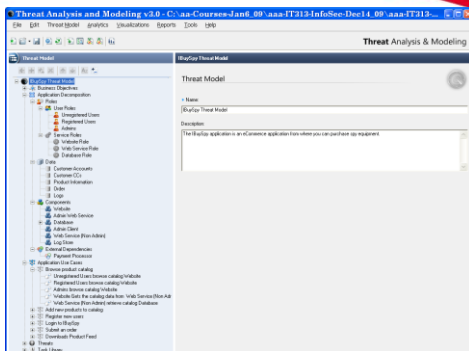


TAM Tool

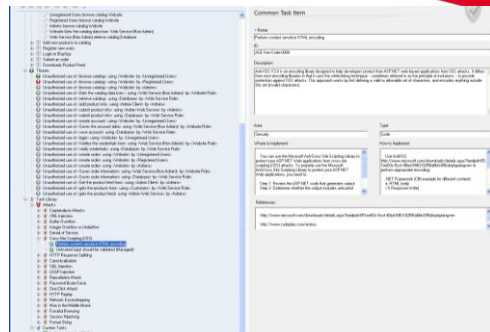
- 3 main areas of the tool
 - threat modeling methodology
 - gathering application architecture
 - security guidance
 - <http://ms.events.microsoft.com/cui/eventdetail.aspx?eventid=103225724&culture=en-us>
 - 3.0 beta (videos available)
 - <http://www.microsoft.com/downloads/details.aspx?familyid=AAD6DEC7-26CF-4053-9963-D5974631C070&displaylang=en>
 - <http://channel9.msdn.com/posts/Jossie/Thread-Analysis-Modeling-Tool-TAM-30/>
 - <http://blogs.msdn.com/threatmodeling/archive/2009/07/20/threat-analysis-and-modeling-tam-v3-0-learn-about-the-new-features.aspx>
- The Value of Microsoft TAM (2009)
 - www.ciozone.com/index.php/Security/The-Value-of-Microsoft-TAM.html
- North Carolina State – TAM Tutorial
 - <http://agile.csc.ncsu.edu/SEMaterials/tutorials/mstthreatmodeling/>



TAM Tool



TAM Tool



Other Threat Modeling Systems

- OWASP
 - http://www.owasp.org/index.php/Threat_Risk_Modeling
- Trike (Squeak)
 - www.octotrike.org/faq/
 - map.squeak.org/package/2b30afd8-a8f2-46ad-ba5e-3a72f2456d5a
 - seclists.org/webappsec/2005/q3/138
- AS/NZ 4360:2004 Risk Mgmt
 - superseded by AS/NZS ISO 31000:2009
 - infostore.saiiglobal.com/store/getpage.aspx?path=/publishing/shop/promotions/AS_NZS_ISO_31000_2009_Risk_Management_Principles_and_guidelines.htm&site=RM
- 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 Compatible Tools
 - SCAP Data Feeds (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
 - Impact Metrics (CVSS)
 - Product Dictionary (CPE)
 - Common Weakness Enumeration (CWE)



DHS CVSS

- 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/cvss/
 - Common Vulnerability Scoring System v2
 - nvd.nist.gov/cvss.cfm?version=2
 - 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



DHS CVSS

The page provides a calculator for creating CVSS vulnerability severity scores. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in accordance with the Base Score, the Temporal Score and the Environmental Score. The Temporal Score is used to calculate the Environmental Score. A copy of the page is available to CVSS experts.

[CVSS Scores](#) | [Base Score](#) | [Base Score](#) | [Base Score](#) | [Base Score](#)

CVSS Base Score	5.4	Environmental Score Metrics	
Impact Subscore	7.8	General Modifiers	
Exploitability Subscore	2.4	Organization specific potential for loss (CollateralDamagePotential)	<input type="text" value="1"/> (See right text)
CVSS Temporal Score	5.1	Percentage of vulnerable systems (TargetDistribution)	<input type="text" value="1"/> (See right text)
CVSS Environmental Score	1.4	Impact Subscore Modifiers	
Modified Impact Subscore	10	System confidentiality requirement (confReq)	<input type="text" value="Medium"/> (See right text)
Overall CVSS score	8.9	System integrity requirement (integrityReq)	<input type="text" value="Low"/> (See right text)
Base Score Metrics		System availability requirement (availReq)	<input type="text" value="High"/> (See right text)
These metrics describe inherent characteristics of the vulnerability. All of these metrics must be filled in to perform an CVSS scoring.			
Exploitability Metrics		Temporal Score Metrics	
Related exploit range (AccessVector)	<input type="text" value="Local"/>	System confidentiality requirement (confReq)	<input type="text" value="Medium"/>
Attack complexity (AccessComplexity)	<input type="text" value="Medium"/>	System integrity requirement (integrityReq)	<input type="text" value="Low"/>
Level of authentication needed (Authentications)	<input type="text" value="None"/>	System availability requirement (availReq)	<input type="text" value="High"/>
Impact Metrics		These metrics describe elements about the vulnerability that change over time. If all of these values are left as "Undefined", the environmental score will be based on the base score.	
Confidentiality impact (ConfImpact)	<input type="text" value="Partial"/>	Availability of exploit (Exploitability)	<input type="text" value="Unknown"/>
Integrity impact (IntegImpact)	<input type="text" value="None"/>	Availability of fix available (RemediationAvailable)	<input type="text" value="Workaround"/>
Availability impact (AvailImpact)	<input type="text" value="Complete"/>	Level of verification that vulnerability exists	<input type="text" value="Uncolaborated"/>



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

- 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/



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.riskworld.net/
 - www.27001.com/products/32
 - www.27005.net/
 - www.securitypark.co.uk/books-governance.asp
 - www.17799central.com/iso17799.htm
 - www.17799-toolkit.com/



Other Microsoft Resources

- Security Guidance for Applications (2005)
 - msdn.microsoft.com/en-us/library/ms998408.aspx
- Security Guidance Center
 - www.microsoft.com/security/default.aspx
- MSDN Security Center
 - msdn.microsoft.com/en-us/security/aa570411.aspx
- Channel9 Videos
 - channel9.msdn.com/tags/Security/
- MSDN Webcast: Writing Secure Code
 - msevents.microsoft.com/cui/eventdetail.aspx?eventid=1032253724&culture=en-us
- Patterns & Practices (2003)
 - msdn.microsoft.com/en-us/library/aa302419.aspx
- Threat Modeling for Web Applications Using STRIDE (2004)
 - www.securityworld.be/security/threat%20modeling%20for%20web%20applications%20using%20the%20STRIDE%20model.pdf
- IT Compliance Management Guide (GovncRskComp) (2009)
 - <http://technet.microsoft.com/en-us/library/dd206732.aspx>



Additional Resources

- DREAD (is dead)
 - weblogs.asp.net/hurbut/archive/2005/11/15/430662.aspx
- A Practical Approach to Threat Modeling (2008)
 - www.devx.com/Security/Article/37502/1763/page/1
- Software Security Assurance Report (2007)
 - 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 (iist.org)
- Secure World -- www.hellosecureworld.com
- "Beautiful Security" Chapter 9 download
 - securlib.budha.com/2009/06/22/free-pdf-download-of-beautiful-security-chapter-tomorrows-security-cogs-and-levers-here/
- DataLossDB -- datalossdb.org/



A Test

- What was Multics? OS developed by GE & MIT (Bell Labs) (ZARP)
- What year was the 1st federal prosecution of computer fraud? 1966
- For an expert bent on crime, cracking a computer system's defenses is about as difficult as solving a hard crossword puzzle.
- Most detected frauds are never reported. (T)
- Dishonest insider > evil outsider (2nd most reason for data lose in 1972)
- Human error accounts for 50% of all data losses
- Ratio of undiscovered to discovered crime may be on the order of 100 to 1.
- Passwords often turn out to be laughably weak defense. (T)
- List 6 security problems for today's companies:
 - Social engineering
 - Mother nature
 - Vanishing paper trail
 - The sheer complexity of today's systems
 - Security comes at a cost including inconvenience
 - There is still reluctance to spend money for computer security
- Donn Parker -- www.cbi.umn.edu/collections/inv/cbi00166.html

ZARP is with you again

Waiting for the Great Computer Rip-off, FORTUNE, July 1974



From the grandfather of the ENIAC to the grandfather of ET



In 1953 the first computer (IBM-701) arrived in the Cincinnati area at GE Aircraft Engines plant. In 1958 UC got its first computer an IBM-650.

