Important Note Regarding This Microsoft PowerPoint Presentation

*** Do not include this slide in your presentation ***

- This slide deck has been intentionally provided with very limited graphics and formatting to simplify content integration into your own preferred PowerPoint themes and styles.

Security Development Lifecycle (SDL) Training

Secure Design Principles (Level 100)

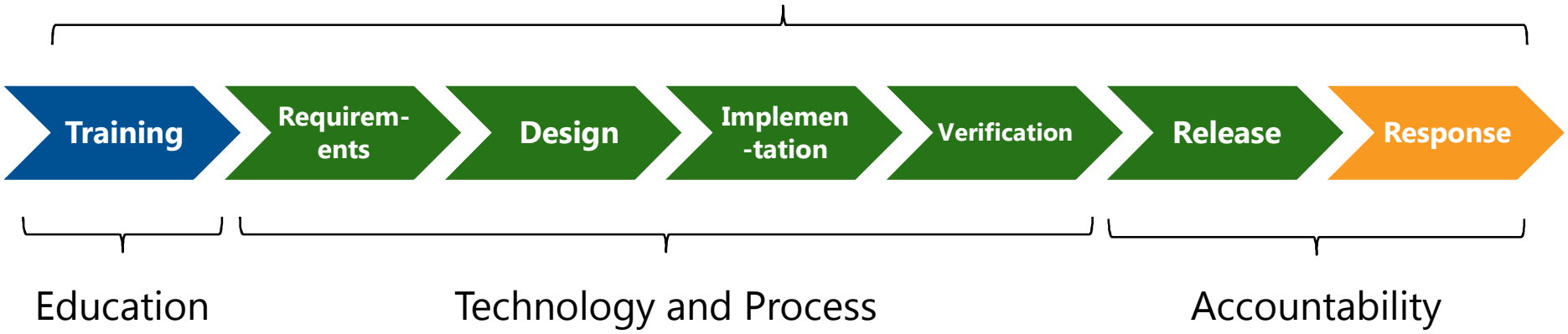
Agenda

- Microsoft SDL and Secure Design
- Secure Design Principles

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 Secure Design Principles

- Safer applications begin with secure design
- Core SDL secure design principles:
  - Attack Surface Reduction
  - Basic Privacy
  - Threat Modeling
  - Defense in Depth
  - Least Privilege
  - Secure Defaults

SDL Core Principle: Attack Surface Reduction

- **Attack Surface:** Any part of an application that is accessible by a human or another program
  - Each one of these can be potentially exploited by a malicious user
- **Attack Surface Reduction:** Minimize the number of exposed attack surface points a malicious user can discover and attempt to exploit

Attack Surface Example

Attack Surface Analysis

Step 1: Look at Your Entry Points

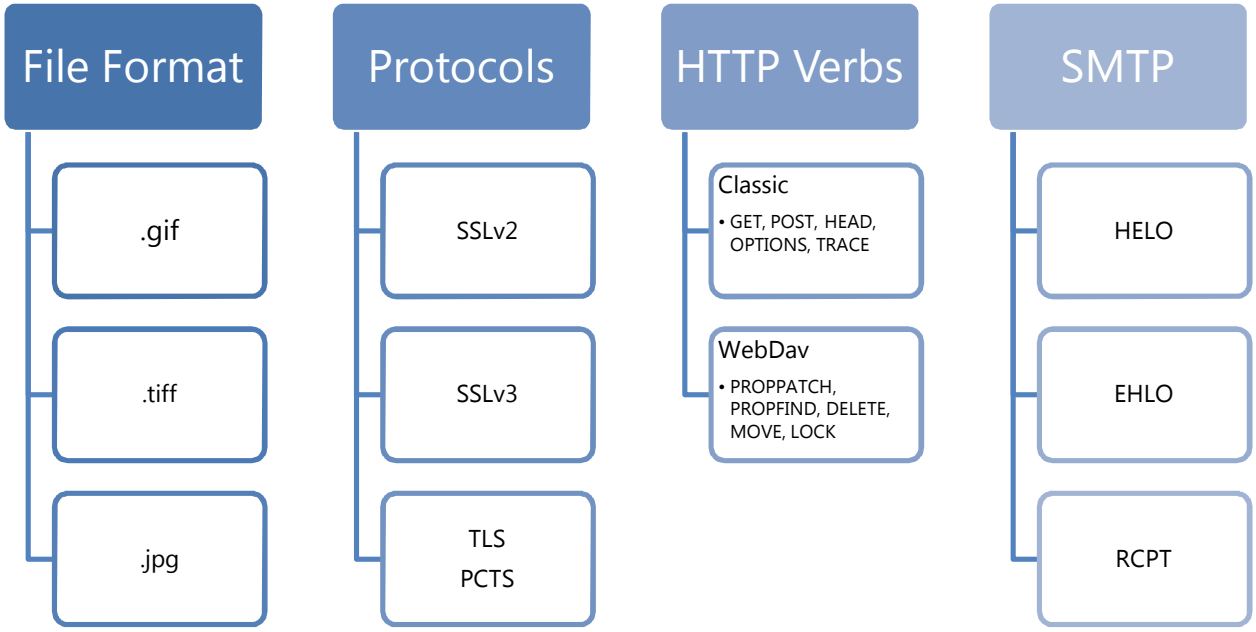
- Network inputs/outputs
- File inputs/ outputs
- Etc.

Step 2: Rank Your Entry Points

- Authenticated or non-authenticated
- Administrative or user-level access
- Network or local
- UDP or TCP
- Etc.

Attack Surface Analysis Tips

- Iterative process, for all features you need to also analyze their sub-features
- Restrict access to features as much as possible



It's Not Just About Turning Things Off

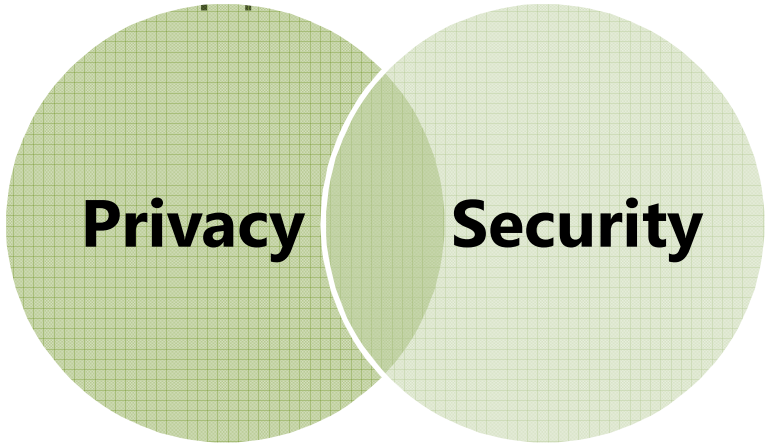
Higher Attack Surface	Lower Attack Surface
On by default	Off by default
Open socket	Closed socket
UDP	TCP
Anonymous access	Authenticated user access
Constantly on	On as needed
Administrative access	User access
Internet accessible	Local subnet accessible
Running as SYSTEM	Running as user, network service or local service account
Uniform defaults	User defined settings
Large code	Small code
Weak access controls	Strong access controls

Attack Surface Reduction Examples

Microsoft Product	Attack Surface Reduction
Windows	• Authenticated Remote Procedure Call (RPC) • Firewall on by default
Internet Information Services 6.0 and 7.0	• Off by default • Running as network service by default • Static files by default
SQL Server 2005 and 2008	• xp_cmdshell stored procedure off by default • CLR and COM off by default • Remote connections off by default
Visual Studio 2005 and 2008	• Web server localhost only • SQL Server Express localhost only

SDL Core Principle: Basic Privacy

- Privacy versus Security
  - **Privacy:** Empowering users to control the use, collection and distribution of their personal information
  - **Security:** Establishing protective measures that defend against hostile acts or influences and protects the confidentiality of personal information
- Privacy AND Security together are key factors for building trusted applications



Important Note: Security Does Not Always Guarantee Privacy

It is possible to have a secure system that does not preserve users' privacy.

Primary Objectives When Developing Privacy-Aware Applications

- Three primary objectives:
  1. Fulfill legal obligations;
  2. Increase customer trust; and
  3. Prevent blocked deployments.

Understanding Application Behaviors and Concerns

Application Behavior	Privacy Concern
Target children	Children Online Privacy Protection Act (COPPA)
Transfer sensitive PII	Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA)
Transfer non-sensitive PII	European Union (EU) or Federal Trade Commission (FTC)
Modify system	Computer Fraud and Abuse Act (CFAA)
Continuous monitoring	Anti-Spyware Legislation, Deployment Blocker
Anonymous transfer	Deployment Blocker

Microsoft Privacy Guidelines for Developing Products and Services

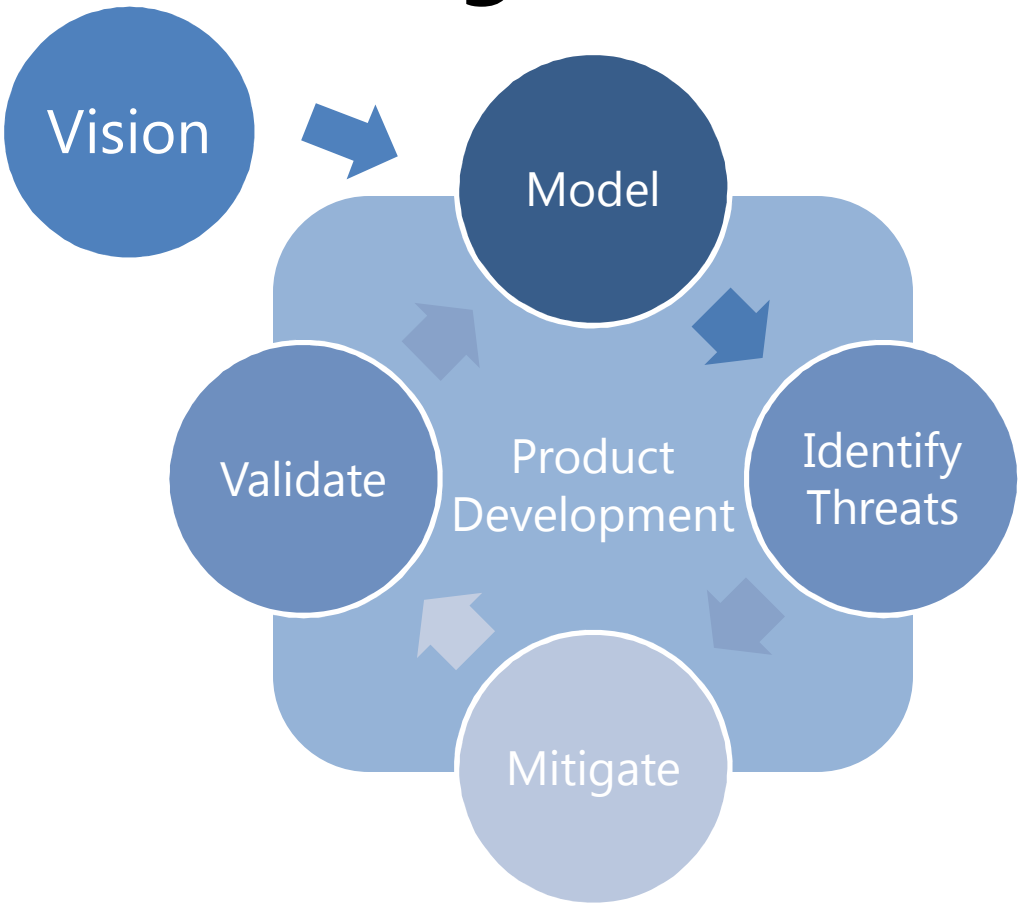
- Documented requirements and recommendations for privacy-compliant products and services
- Available online for download

Microsoft customers will be empowered to control the collection, use, and distribution of their personal information

SDL Core Principle: Threat Modeling

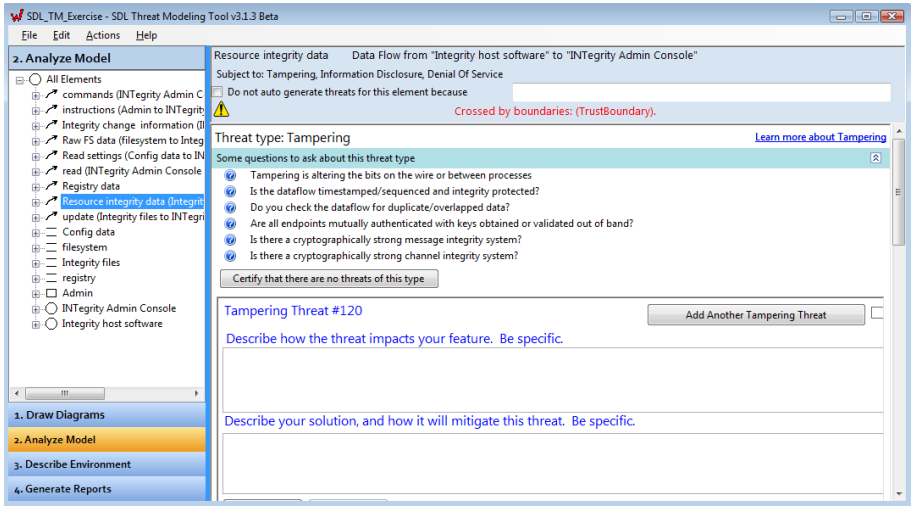
- **Threat Modeling:** A process to understand threats to an application
- Threats and vulnerabilities are not the same thing:
  - **Threats:** What a malicious user may attempt in order to compromise a system
  - **Vulnerabilities:** A specific way a threat is exploitable, such as a coding error

Threat Modeling In a Nutshell



Microsoft SDL Threat Modeling Tool

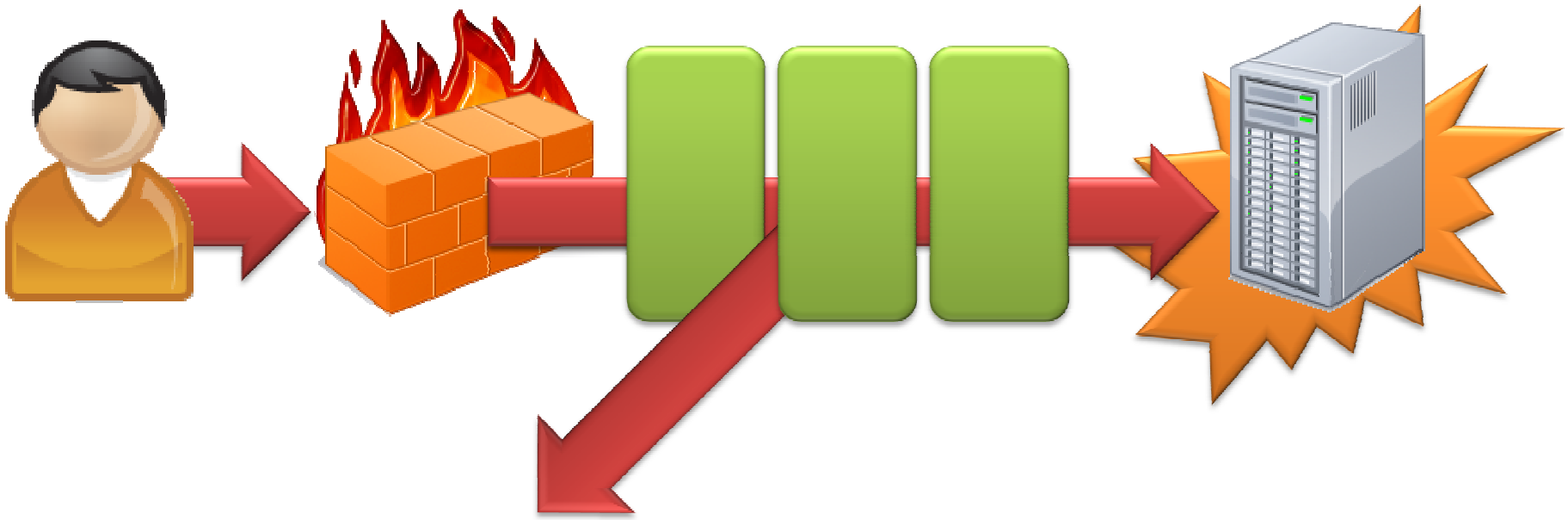
- Microsoft has published the threat modeling tool it uses internally to assess threats against products and services
- Freely available online for download at http://msdn.microsoft.com/en-us/security/dd206731.aspx



SDL Core Principle: Defense In Depth

- Assume that software and hardware will fail at some point
  - Trusted applications: security and privacy features and mechanisms
- Most applications today can be compromised when single, and often only, layer of defense is breached (firewall)
- **Defense in Depth:** If one defense layer is breached, what other defense layers (if any) provide additional protection to the application?

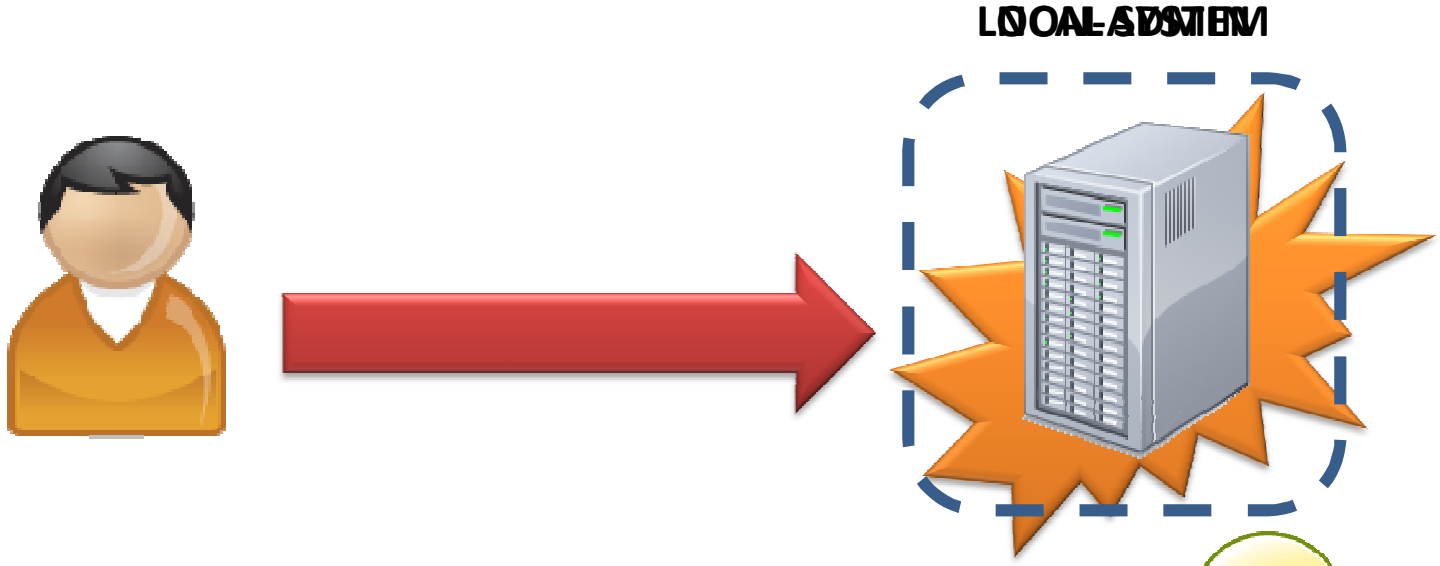
Defense in Depth Example



SDL Core Principle: Least Privilege

- Assume that all applications can and will be compromised
- **Least Privilege:** If an application is compromised, then the potential damage that the malicious person can inflict is contained and minimized accordingly

Least Privilege Example



ADMIN / SYSTEM LEVEL

- Read user files
- Change system passwords
- Download malicious files
- Anything

NON-ADMIN

- ~~Read user files~~
- ~~Change system passwords~~
- ~~Download malicious files~~
- Limited capabilities

Least Privilege Tips

- Evaluate your application and think minimally!
- What is the minimum access level your application requires to perform its functions?
- Elevate privileges only when needed, and then release those elevated privileges when their purposes have been satisfied

SDL Core Principle: Secure Defaults

- **Secure Defaults:** Deploy applications in more secure configurations by default.
- Helps to better ensure that customers get safer experience with your application out of the box, not after extensive configuration
- It is up to the user to reduce security and privacy levels

Secure Defaults Examples

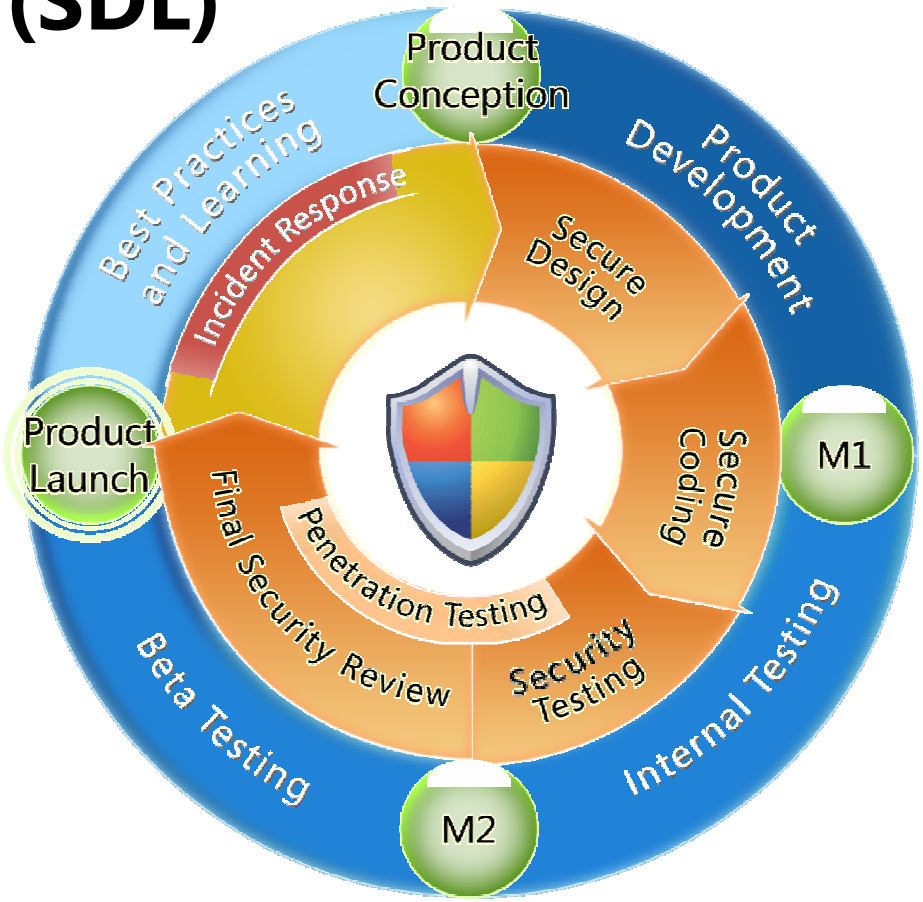
Application Component	Secure Defaults Principle
Firewall	Firewall ON by default
SSL Socket	Requires last latest SSL version (v3, TLS, etc.) by default
User can access application anonymous or authenticated	Application requires authenticated user sessions by default
Password complexity can be enforced	Password complexity is required by default
Store user passwords as hashes or clear text	Store user passwords as hashes by default

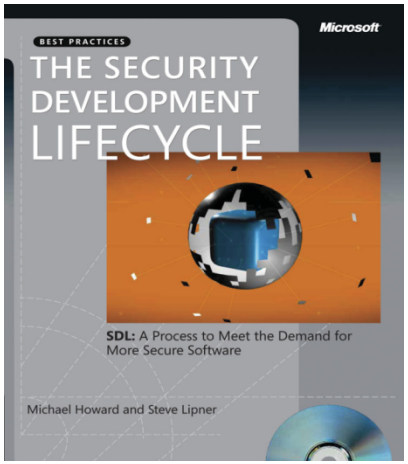
Conclusion

- Microsoft SDL and Secure Design
- SDL Core principles:
  - Attack Surface Reduction
  - Basic Privacy
  - Threat Modeling
  - Defense in Depth
  - Least Privilege
  - Secure Defaults

Appendix

Microsoft Security Development Lifecycle (SDL)

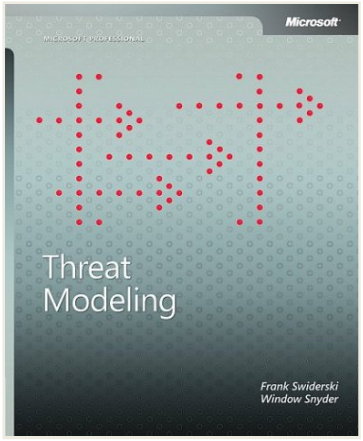




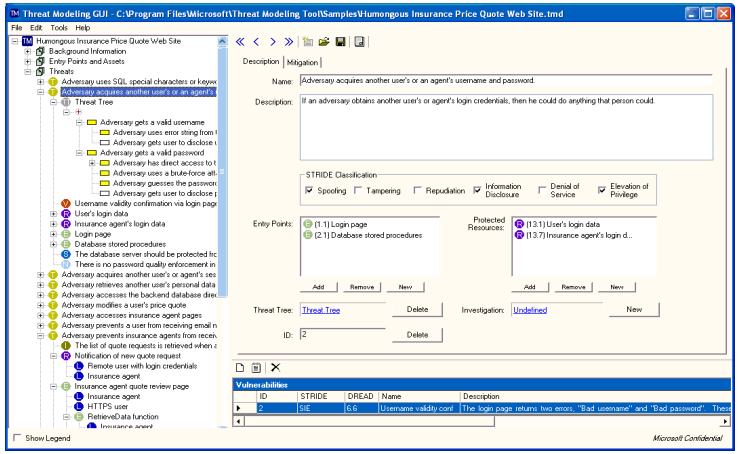
SDL Book:
http://www.microsoft.com/mspress/books/8753.aspx

Official SDL Web Site: http://www.microsoft.com/sdl

Threat Modeling Resources



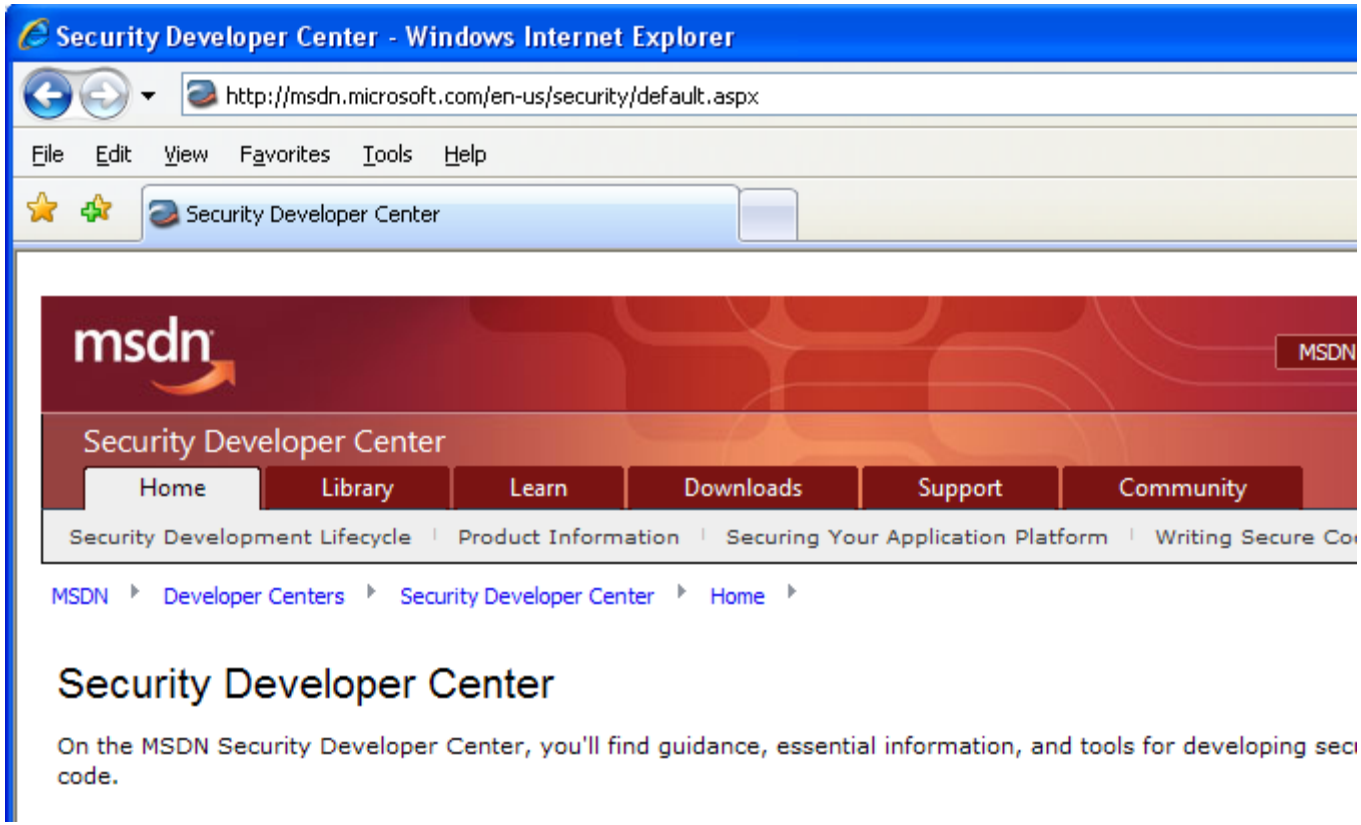
Threat Modeling Book:
http://www.microsoft.com/mspress/books/6892.aspx



Threat Modeling Tool:
http://www.microsoft.com/downloads/details.aspx?FamilyID=62830f95-0e61-4f87-88a6-e7c663444ac1&displaylang=en

Microsoft Developer Network (MSDN) Security Developer Center

- Official Web site: http://msdn.microsoft.com/security



Secure Development Blogs

- The Microsoft Security Development Lifecycle (SDL) Blog: http://blogs.msdn.com/sdl
- Michael Howard's Blog: http://blogs.msdn.com/michael_howard