Security Considerations for Client and Cloud Applications

November 6, 2009

For the latest information, please see <http://www.microsoft.com/sdl>.

Abstract

The increasing adoption of "client and cloud" computing raises several important concerns about security. This paper discusses security issues that are associated with “client and cloud” and their impact on organizations that host applications “in the cloud.” The paper then describes how Microsoft minimizes the security vulnerabilities in these, possibly mission-critical, platforms and applications by following two, complementary approaches: developing the policies, practices, and technologies to make their “client and cloud” applications as secure as possible, and managing the security of the platform environment through clearly defined operational security policies.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form, by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft is a trademark of the Microsoft group of companies.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

“Client and Cloud” Computing

“Client and cloud” is a term that describes a paradigm of computing that is currently seeing a great deal of interest in the IT industry. Enterprises can rent computing resources as a utility and use those resources to make services available to client applications over the Internet. Some characteristics of this paradigm are significant from a security perspective:

* A third party manages the computing resources that host the cloud-based applications.
* Cloud services often store data on behalf of the client application.
* The client application is not necessarily a Web browser, but could be a rich client or business system.

An enterprise that is planning to use “client and cloud” computing must concern itself with the security of two major elements of the cloud environment. The first is the security of the third-party cloud platform. The other is the security of the business applications that the enterprise is hosting “in the cloud.” The security of the cloud platform depends on the security of the software that is used to implement the cloud platform and on the operational security that is applied by the third party that is providing the cloud platform.

This paper describes how Microsoft has addressed security for its “client and cloud” platform and offers some guidance to other organizations who want to host their applications “in the cloud.” The paper begins by explaining how Microsoft applied the Security Development Lifecycle (SDL) to the development of its “client and cloud” applications, and how the SDL has evolved to meet the demands of this environment. The paper then moves on to discuss the operational security policies that Microsoft applies to its cloud platform, and to explain the level of security that users can expect from Microsoft’s cloud platform.

Secure Design and Coding

In terms of technologies and processes, the development of “client and cloud” platforms and applications does not differ significantly from the development of other types of software. Microsoft has long recognized that the software development life cycle must address security threats at all stages. For example, threat modeling during the Design phase is one of the most effective ways to build security into the software development process. It makes software less vulnerable to potential threats by identifying them before building the software. This proactive process reduces the reliance on reactive measures that depend either on penetration testing performed before releasing the software, or worse, on user discovery of security vulnerabilities after releasing the software. During the implementation phase, development teams should enforce the use of coding standards because one of the benefits of applying coding standards is to ensure that developers follow security best practices in a consistent manner. The testing phase should include security and privacy testing alongside other test types to verify that the team has securely implemented the secure design.

Development groups within Microsoft use the SDL to address systematically the security threats that may be inherent in their software products. The SDL is a set of processes and tools designed to reduce the number and severity of vulnerabilities in software products. It encompasses education of development personnel, secure development processes, and accountability of individuals and product teams for building consistently more secure software. An executive commitment to sustaining the drive for more secure products underpins these pillars of the SDL. The SDL is constantly evolving (it is currently at version 5.0) as it responds to newly discovered security threats and adopts advances in security science at Microsoft. Software is subject to the SDL if it exhibits one or more of the following characteristics:

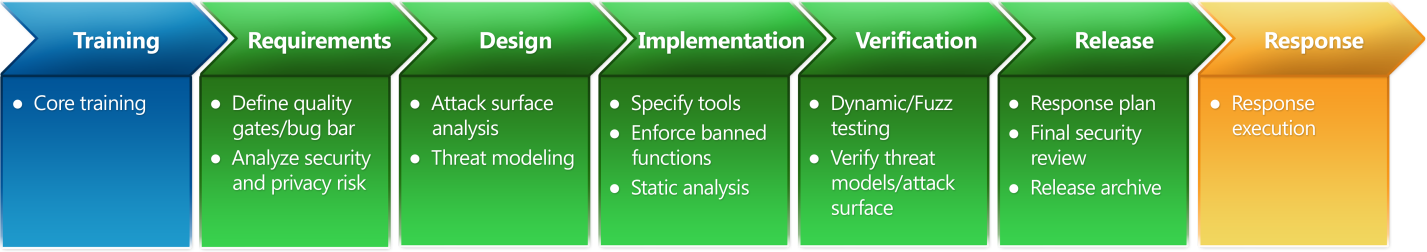
* It will be used in a business environment.
* It processes sensitive or personally identifiable information.
* It is Web based or Internet based.

The SDL is therefore mandatory for any “client and cloud” software that Microsoft develops[[1]](#footnote-1).

## The Security Development Lifecycle

The SDL is a rigorous set of security practices that development teams at Microsoft employ. The SDL process can be adapted to work with various development methodologies from spiral to agile. In a spiral development project, various phases of the SDL process emphasize education and training, and mandate that development teams apply specific activities and processes to each phase of software development. Senior leadership within Microsoft continues to support the mandate that teams apply the SDL during the development of Microsoft products, including the delivery of online services.

The following diagram outlines the SDL process.



The SDL process identifies specific activities that development teams must complete during each phase. The following list describes each phase, starting with the Requirements phase:

* **Requirements**. The primary objective in this phase is to identify key security objectives and otherwise maximize software security while minimizing disruption to customer usability, plans, and schedules.
* **Design**. Critical security steps in this phase include documenting the potential attack surface and conducting threat modeling.
* **Implementation**. During this phase, the development team must take steps to ensure that there are no known security vulnerabilities in the code by adhering to specific coding standards, and by applying analysis tools to the evolving software.
* **Verification**. During this phase, the team must ensure that the code meets the security and privacy tenets that were established in the previous phases. The team must also complete a public release privacy review.
* **Release**. The Final Security Review (FSR) happens during this phase. The FSR helps to determine whether the product is secure enough to ship by ensuring that the software complies with all SDL requirements and with any additional security requirements that are specific to the project.
* **Response**. After software has been released the Microsoft Security Response Center (MSRC) identifies, monitors, resolves, and responds to security incidents and Microsoft software security vulnerabilities. The MSRC also manages a company-wide security update release process and serves as the single point of coordination and communications.

## Applying the SDL to Microsoft’s Online Services

The SDL incorporates comprehensive security and privacy protections for online services and Web applications[[2]](#footnote-2). It includes requirements that address widely exploited classes of Web vulnerabilities, including cross-site scripting (XSS), SQL injection, and cross-site request forgery (XSRF) among others. These types of issues are of concern for developers of both traditional Web applications and of emerging cloud services.

Microsoft has continued to evolve its practices to address emerging threats on the Internet. For example, the latest version of the SDL includes guidance to help developers protect their applications against “clickjacking,” a new type of attack first demonstrated in October 2008.

## Extending the SDL to Emerging Development Models or SDL for Agile

Developing cloud-based applications introduces some additional challenges due to the rapidly evolving environments into which organizations will deploy these applications, and the aggressive and frequent product and service release schedules that the market demands. Agile, a dominant methodology for managing Web projects, is frequently used to manage cloud-based projects. Microsoft has recently announced “SDL for Agile” as an approach to embedding security into the agile development methodology.

For further details of SDL for Agile, see “[Security Development Lifecycle for Agile Development](http://go.microsoft.com/?linkid=9694872).”

## Sharing with the Ecosystem

Microsoft shares the SDL and related tools publicly[[3]](#footnote-3), and offers consulting assistance in applying the SDL. In this way, any organization wanting to develop more secure software can benefit from the lessons that Microsoft has learned since the SDL was mandated at Microsoft. If an organization is hosting an application that has its own “in the cloud” security requirements, using the SDL as a part of its development methodology is an excellent way to ensure that its application meets those security requirements.

The Importance of Operational Security to Cloud Services

To reduce the number and severity of security threats, Microsoft develops client and cloud applications by using the SDL. After the application has been deployed to the cloud, Microsoft applies a clearly defined set of security policies that continue to protect the application from security threats.

Parts of the SDL also address the operational security of “in the cloud” applications. During the Requirements phase the analysis of security and privacy risks in a cloud-hosted application must take into account the target operational environment. The Release phase includes an Operational Security Review (OSR) alongside the FSR. The OSR reviews the application’s network communications, platform requirements, system configuration, and monitoring capabilities against established security standards and baselines. This process ensures that appropriate security controls are part of the operational plans for the application before granting permission to deploy the software to the cloud infrastructure.

## Policy Compliance

Online service environments must meet numerous government-mandated and industry-specific security requirements in addition to their own business-driven specifications. Within Microsoft, the Operational Services Security and Compliance (OSSC) team works across the operation, product, and service delivery teams and with internal and external auditors to ensure compliance with the relevant standards and regulatory obligations. The following list presents an overview of some of the audits and assessments that the Microsoft cloud environment must undergo on a regular basis:

* **Payment Card Industry Data Security Standard (PCI-DSS)**. This standard requires an annual review and validation of the security controls related to credit card transactions.
* **Media Ratings Council**. This relates to the integrity of advertising system data generation and processing.
* **Sarbanes-Oxley (SOX)**. This legislation requires that selected systems are audited annually to validate compliance with key processes related to financial reporting integrity.
* **Health Insurance Portability and Accountability Act (HIPAA)**. This act specifies privacy, security, and disaster recovery guidelines for the electronic storage of health records.
* **Internal audit and privacy assessments**. Assessments occur throughout a given year.

After analyzing all of these requirements, Microsoft determined that many of the audits and assessments required an evaluation of the same operational controls and processes. Recognizing the significant opportunity to eliminate redundant efforts, streamline processes, and proactively manage compliance expectations in a more comprehensive manner, the OSSC team developed a comprehensive compliance framework. This framework and associated processes follow the five-step methodology represented in the following illustration.

**OSSC Compliance Framework**

* **Identify and integrate requirements**. Define the scope and applicable controls. Standard operating procedures (SOPs) and process documents are gathered and reviewed.
* **Assess and remediate gaps**. Identify and remediate gaps in process or technology controls.
* **Test effectiveness and assess risk**. Measure and report on the effectiveness of controls.
* **Attain certifications and attestations**. Engage with third-party certification authorities and auditors.
* **Improve and optimize**. Assess and document the root cause of any noncompliance, and then track the remediation process. This phase also involves continuing to optimize controls across security domains to generate efficiencies in passing future audit and certification reviews.

As a result of implementing this framework, Microsoft’s cloud infrastructure has gained both the SAS 70 type I and Type II [[4]](#footnote-4)attestations, and the ISO/IEC 27001:2005 [[5]](#footnote-5)certification:

* The ISO/IEC 27001:2005 certificate validates that Microsoft has implemented the internationally recognized information security controls defined in this standard.
* The SAS 70 attestations illustrate Microsoft’s willingness to open up its internal security programs to outside scrutiny.

The physical security of all of Microsoft's data centers is an example of the operational security that the OSSC manages. Policies define the access controls applied to inner and outer perimeters, the levels of automated monitoring applied at the data centers, and the security incident notification procedures in force. Microsoft specifies the security requirements upon which data center employees and contractors are reviewed. In addition to contractual stipulations about site staff, OSSC policies define a further layer of security within the data center for the personnel who operate the facility. Access is restricted by applying a least privilege policy so that only essential personnel are authorized to manage users’ applications and services[[6]](#footnote-6).

Understanding the Security that Cloud Services provide

As described above, the initial phase of the SDL encompasses the identification of the security requirements that the product or service under development must meet. The security required will vary, depending on the type of system. For example, a government system dealing with millions of social security numbers will have much stronger requirements than a standard business application. Microsoft classifies systems as low, moderate, or high business impact to help determine security requirements and the strength of security features that they must provide. The categories take into account the relative potential for financial and reputational damage if the asset was involved in a security incident. For example, data assets falling into the moderate impact category are subject to encryption requirements when they reside on removable media or when they are involved in external network transfers. Data in the high impact category, in addition to moderate impact requirements, is subject to encryption requirements for storage and for internal system and network transfers.

For all cloud services that Microsoft offers, the documentation provided to users will always state what is protected and how it is protected. For example, users who choose to host their applications “in the cloud” may want to have their applications and processing protected from those of other users. For these users, Microsoft is committed to providing this level of protection. Additional security feature and protection requirements will vary from user to user, and from application to application, depending on data sensitivity and on applicable laws and regulations. Microsoft will be transparent about the strength and applicability of the security protections that its cloud services offer so that users will know what security features and processes are available, and will be able to determine how Microsoft will protect their data and processing. The information provided will enable users to evaluate the suitability of Microsoft’s cloud platform for their security requirements and to make informed decisions about their use of cloud services.

Summary

Microsoft addresses potential security vulnerabilities during the development of “client and cloud” applications by using the SDL. Where necessary, Microsoft has updated the SDL to ensure its relevance to developing “in the cloud” applications, and to reflect the changing security landscape. Microsoft manages the security of deployed cloud applications through clearly defined operational policies that are appropriate to the nature of the application and to its specific security requirements.

An enterprise that is planning to use “client and cloud” computing must concern itself with the security of two major elements of the cloud environment. The first is the security of the third-party cloud platform. The other is the security of the business applications that the enterprise is hosting “in the cloud.” The security of the cloud platform depends on the security of the software that is used to implement the cloud platform and on the operational security that is applied by the third party that is providing the cloud platform.

When an enterprise chooses to host some, or all, of its applications in the cloud, the enterprise faces many of the same security challenges as any other organization that builds an online application. These challenges are secure development, operational security, and selection of appropriate security features and data protection mechanisms. Part of this selection process will depend on the security features that the cloud provider commits to support. If those features are well considered and engineered, the decision to host applications “in the cloud” may simplify or reduce some of the security challenges that the enterprise faces.

You can use the SDL and related tools to help develop your own secure “client and cloud” applications by using the information and resources found at http://www.microsoft.com/sdl.

1. For some recent case studies highlighting the effectiveness of the SDL, see these white papers:

   [Preventing Security Development Errors: Lessons Learned at Windows Live Using ASP.NET MVC](http://go.microsoft.com/?linkid=9695423)

   [Microsoft Silverlight 1.0: An SDL Implementation Story](http://go.microsoft.com/?linkid=9695422) [↑](#footnote-ref-1)
2. See “The Microsoft Security Development Lifecycle (SDL): Process Guidance” at http://msdn.microsoft.com  
   /en-us/security/cc420639.aspx. [↑](#footnote-ref-2)
3. See “The Microsoft Security Development Lifecycle (SDL): Process Guidance” at http://msdn.microsoft.com  
   /en-us/security/cc420639.aspx. [↑](#footnote-ref-3)
4. Statement on Auditing Standards No. 70: Service Organizations issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (http://www.aicpa.org). [↑](#footnote-ref-4)
5. ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties (see http://www.iso.org/iso/iso\_catalogue/catalogue\_tc/catalogue\_detail.htm?csnumber=42103). [↑](#footnote-ref-5)
6. <http://www.globalfoundationservices.com/security/index.html>.  [↑](#footnote-ref-6)