
Microsoft Office SharePoint Server, Threat Modeling, and 34a Labs Prevent Server

A Technical Brief

Robert B Yonaitis

Contents

Introduction 3

The Players..... 4

Defining the Basic Threat Vectors..... 5

 The Accessibility Perspective 5

 The Privacy Perspective 6

 The Operational Security Perspective..... 6

Resolution 6

 Preventing versus Monitoring..... 7

 Standards based solutions and reliable 7

Summary 7

Terms 8

Acronyms 8

Introduction

In today's business environment it would be challenging to find a company that does not have policies and procedures in place to address the way that they handle sensitive information, employee information, and confidential information (financial, customers, etc...). These procedures provide protection for the organization and helps prevent risk. However it is not surprising to learn that many organizations have not considered the additional threats and risk to this information as well as a paradigm shift that is caused through migration of some of this information to the Internet through their Web sites, Web based applications and the social networking tools which are common in Enterprise 2.0 (E2) and Government 2.0 (Gov 2.0) environments. Much like Human Resource Departments, Information Technology Departments must put policies and procedures in place to deal with a wide range of compliance issues from employee and customer data, to general security as well as role based security. These policies are generally put together through the use of a threat model.

There are many different definitions of Threat Modeling and there are several books are available on the topic. This document utilizes the software-centric threat model-and reviews some of the specific threat vectors related to information managed through Microsoft Office SharePoint Server. It introduces both considerations and preventative measures that can be taken to create a secure environment. It should be noted that this document will introduce basic topics and base threat vectors to initiate an informed dialogue and promote a deeper analysis, **but** this is not intended to be a **comprehensive** threat model. Instead, the reader should develop their own to match their implementation.

The Players

It is important to use as narrow a scope as you can when defining the central target that you are considering in your threat model. This paper will actually look at three similar and somewhat joined targets as they can all be used alone or together as a single unit.

The target set will be **Microsoft Windows SharePoint Services, SharePoint Server 2007, and SharePoint Server Publishing Sites** specifically.

The threat vectors for the purposes of this paper will be **general content compliance including but not limited to all content created or input into the system**. The attacks will be perpetrated by users of the system, (knowingly and unknowingly) and/or automated systems designed to attack the SharePoint Server. This document will not cover how to handle different extensions or html file types or simple word filtering. This can be handled easily by Microsoft ForeFront™ Server <http://www.microsoft.com/forefront/en/us/default.aspx>. Additionally, this document will not cover viruses and other platform specific threats. This document is concerned with interface and content.

The player tasked with dealing with the content that will be discussed is the 34a Labs Prevent Server. This solution provides compliance validation of: Accessibility, Privacy, Operational Security, Profanity Filtering, Accounting data test suite, Inappropriate Sites, Extended Keyword Filtering, and Custom Test Suites

Defining the Basic Threat Vectors

SharePoint has become a mission-critical part of businesses and government organizations and central to Enterprise 2.0 and Government 2.0. SharePoint can be used not only to manage Web content, but also can be used to provide a front end Web based interface to mission critical information managed within SharePoint or other applications behind it. With this in mind steps must be taken to both protect the integrity of the solution and to defend against malicious attacks. System Administrators of course need to protect against virus and malicious files, while HR and IT policy personal must protect the environment from compliance errors, threats and oversights. Each of the compliance items listed in the previous section has specific threat vectors to be considered. **This** paper will define potential target locations. A critical threat vector to consider is the "purpose" of the solution. As SharePoint is a collaboration tool it makes sense for an attacker to attack the collaboration points:

- Document Libraries
- Blogs
- Wikis
- Team Sites
- Publishing Sites
- **And** any other collaboration, meeting, enterprise or Publishing site you may implement

The Accessibility Perspective

Accessibility of the system and content is not a malicious attack but still a threat none the less.

First, non-accessible content may pose a legal risk to the organization. Next, if people needing to access information cannot do so because it is not accessible to them, they may seek to obtain that information in another way, introducing a new threat through accessing information through an unintended back door in the system. Some basic threat vectors to consider are:

1. Adding a document to the document library that is not accessible
2. Modifications to a Template that is not accessible
3. User Added Content that is not accessible

The Privacy Perspective

Privacy issues may represent either a Malicious or non malicious attack. Some basic threat vectors to consider are:

1. A user, in a Blog, enters personal data about one or many employees as a response to a post that can cause damage to the company by violating privacy policy
2. A user adds HR Documents like employment contracts or salaries into an unprotected document store
3. A Publishing Site Template is created without having proper privacy information

The Operational Security Perspective

This can be either a Malicious or non malicious attack. Some basic threat vectors to consider are:

1. A user, in a Blog, enters personal data about one or many officers' locations or non related personal data
2. A user adds Documents that include troop movements
3. A user posts weapon data in a wiki that they think is cool

Resolution

Implement a proactive solution that can prevent the malicious or non malicious data from being entered into your system. Once content with compliance issues is published in your environment, the threat already exists. 34a Labs Prevent is more than a monitoring solution, it is proactive. It takes an entirely different approach allowing you to stop compliance issues before they occur. As a high performance enterprise Web service, 34a Labs Prevent integrates with the content management system to provide immediate results back to the system. Results can have several parameters: Pass, Fail, Validate, Message, and Route. The messaging and routing is controlled by administrators to fully prevent the offending data from being published or imported into the document store, or it can clean the data and publish it.

Preventing versus Monitoring

In the past, monitoring content and repairing it "after the fact" made some sense because of the high percentage of static data on the Web. Today, the Web is a broad combination of content management scenarios, Micro Blogging, E2, Gov 2.0. There are almost endless forms of Social Media. By the time you find a problem with a post production monitoring solution, the threat has already released and has likely been reproduced on several servers as well. Static Monitoring does not work.

Standards based solutions and reliable

When working on security solutions it is important to understand one solution cannot do it all, with this in mind your solution should be standards based. 34a Labs Prevent is standards based. Every test is conducted via enterprise web services that have been load-tested for concurrent user hits emulating enterprise environments. The data is stored in a well-architected database for speed. It utilizes EARL for multiple layers of true decision making on testing results: <http://www.w3.org/WAI/intro/earl.php> . The solutions are developed and tested using best practices for structured engineering and extensive quality assurance. All of these items add up to reliability. We want the user to think of 34a Labs Prevent as "electricity." It's on all the time and flowing, but not something that you never have to touch.

Summary

This document provided an introductory analysis of SharePoint Server and the creation through it of a Threat Vector to your organization. The basics of threat modeling were reviewed for specific compliance groups under specific attacks. In order to effectively handle compliance in SharePoint you

need to think in the terms and practices of threat modeling as related to computer software. Monitoring the system for content that is already exposed, does not solve the threat. In fact, monitoring alone just enables you to know that you have already been compromised. 34a Labs Prevent Server can assist you in proactively preventing and defending against risk. You also may wish to consider a security assessment as related to compliance. More information is available at the 34a Labs web site <http://www.34alabs.com/>

Terms

Threat Model – While there are multiple definitions for the purpose of this paper, computer security where the software application designer cares about security or compliance issues related to risks to compliance or system.

Threat Vector – Is a path that a person or tool can use to attack the target specified in a threat model.

Acronyms

E2 – Enterprise 2.0, a new technology defined business operations

Gov 2.0 – Government 2.0, a New Technology defined government operations