McAfee
Together is power.

Foundstone Application Threat Modeling

Recognize software security weakness well before implementation

Research shows that fixing security problems early in the development cycle is both more efficient and more cost effective than the traditional penetrate-and-patch model. Foundstone® Services provides threat modeling services that help identify detrimental software security problems, often before the software is even built. Software engineering studies have shown that about 80% of the security bugs and flaws are introduced during the early stages of software development, often before even a single line of code has been written. Using our threat modeling services, we typically identify more than 75% of issues, enabling development teams to build secure software.

Foundstone Experts at Your Fingertips

Our consultants are expert reviewers and have helped define the industry approach for application threat modeling. We have significant experience building models for a wide variety of software including portals, ecommerce sites, financial services, healthcare applications, and desktop and developer software.

Our capability in building threat models is built on the expertise of our software security consultants, who have performed threat models and source code audits on numerous client applications, as well as their own software. All of our software security consultants have worked as development practitioners on large enterprise software systems with software vendors or within corporate IT departments. Thus, they understand the software development process as well as why and how security bugs are introduced.[1]

Methodology

All sizeable code assessments start with a threat model. This helps us manage the size of the code base we need to examine down to a much smaller scope (typically between 40% and 60% of the original code size).

The Foundstone threat modeling methodology is based on OCTAVE, which stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation. One of the key aspects of threat modeling is that the team responsible for the modeling must always view the system as the attacker would see it.

Benefits

- Discover bugs earlier in the software development lifecycle. Early detection equals low-cost remediation.
- Identify design flaws that may not be identified through black-box testing.
- Obtain with more information for code reviews and penetration testing. This helps reduce the code review effort down to 60% and eliminates false positives.
- Our one-day or two-day onsite/ remote workshops are designed to accommodate your tight schedules.
- Prioritize usage of your security budget.

Conceptually, threat modeling is a systematic process that consists of several discrete steps with clearly defined entry and exit criteria, deliverables, and objectives. Based on our experience, we have seen that successful modeling activity usually follows a pattern. By ensuring that key steps take place, we ensure that our modeling activity is focused and effective.

Step 1: Planning Activity and Optimizing the Process

This includes activities such as:

- Identifying threat modeling team
- Defining the risk rating model to be used, if any
- Agreeing on terminology for the modeling activity

Next steps occur during a remote or onsite workshop that we conduct with the application team, including the lead architect, developers, testers, business analyst, database administrator, system administrator, and others. This step is designed to have the minimal impact on your staff.

Step 2: Modeling the Business View

The business environment in which the system operates needs to be analyzed to ensure that the system's functionality and business purpose is understood. Laws, guidelines, policies, and other relevant regulations have to be considered.

Step 3: Analyzing from a Technical Standpoint

A solid understanding of the system is important for the success of the whole process. As part of this step, Foundstone consultants perform a detailed architecture and design review for security that focuses on identifying the attack surface and potential attack vectors. Based on the information collected during this process, we can model threats and existing countermeasures. From there, we develop a model of your risk level. We have designed our methodology to be generic enough for different risk models. Often the entire process is iterative in nature.

To ensure quality and consistency of results, our consultants use a standard framework for identifying threats and vulnerabilities in an application.

The Foundstone Software Security Framework

- Configuration Management
- Data Protection in Storage and Transit
- Authentication
- Authorization
- User and Session Management
- Data Validation
- Error Handling and Exception Management
- Logging and Auditing

Deliverables

Our deliverables include:

- Workshop with presentation on Application Threat Modeling
- Application Threat Modeling Technical Report
- Executive Summary Report
- Visio Diagram
- Next Steps Recommendation
- Close-Out Presentation

Depending on the needs of your organization, there are several post-threat modeling activities that can be conducted, including source code reviews, application penetration testing, remediation roadmap development, and vulnerability remediation. We can work with your organization to determine the correct next steps and can provide assistance in achieving your goals.

Reporting and Deliverables

We produce both graphical and textual models that are used to drive pragmatic security decisions. Our deliverables typically include Microsoft Visio-based models of the application architecture, as well as the sorted and tabulated data and results. Our models can include testing plans on demand.

The Foundstone Difference

All Foundstone projects are managed using our proven Security Engagement Process (SEP) for project management. This process ensures continual communication with your organization to ensure the success of all Foundstone consulting engagements. Reports are communicated securely using agreed-upon methods, for example, PGP encryption.

Our staff are certified in their areas of expertise, including CISSP, CEH, CISM, PCI QSA, GIAC, and more. All Foundstone employees have full background investigations performed prior to offers being extended. They go through a rigorous interview and hiring process and are put on the internal training program until they are qualified to meet our standards.

Learn More about Foundstone Services

Fill the gaps in your information security program with trusted advice from Foundstone Services—part of the McAfee® global professional services organization that provides security consulting, customized product deployments, and training and advisory services. Let our consultants help your organization assess current policies, create new programs that meet compliance goals, and cost effectively prepare for security emergencies. Speak with your technology advisor about integrating our services. You can get more information at **www.foundstone.com**.

Related Foundstone Services

Foundstone offers many related services and training classes:

- Web Application Penetration Testing (WAPT)
- Web Services Security Assessment
- Thick Client Assessment
- Mobile Application Assessment
- Security Source Code Review
- Writing Secure Code Training (Java, .Net, C/C++)
- Secure Coding Policies and Standards
- Software Security Maturity Assurance (SSMA) Assessment/ S-SDLC Gap Analysis

1. http://www.mcafee.com/us/resources/white-papers/foundstone/wp-software-security-beyond-dev.pdf.

McAfee Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com