THE ART OF SOFTWARE SECURITY ASSESSMENT

Identifying and Avoiding Software Vulnerabilities

MARK DOWD
JOHN McDONALD

THE ART OF

SOFTWARE SECURITY ASSESSMENT

Art of Software Security Assessment, The: Identifying and Preventing Software Vulnerabilities

Table of Contents

TABLE OF CONTENTS
ABOUT THE AUTHORS
PREFACE
ACKNOWLEDGMENTS
I: Introduction to Software Security Assessment
- 1 SOFTWARE VULNERABILITY FUNDAMENTALS
  - Introduction
  - Vulnerabilities
  - The Necessity of Auditing
  - Classifying Vulnerabilities
  - Common Threads
  - Summary
- 2 DESIGN REVIEW
  - Introduction
  - Software Design Fundamentals
  - Enforcing Security Policy
  - Threat Modeling
  - Summary
- 3 OPERATIONAL REVIEW
  - Introduction

Table of Contents

Exposure

Web-Specific Considerations

Protective Measures

Summary

4 APPLICATION REVIEW PROCESS

Introduction

Overview of the Application Review Process

Preassessment

Application Review

Documentation and Analysis

Reporting and Remediation Support

Code Navigation

Code-Auditing Strategies

Code-Auditing Techniques

Code Auditors Toolbox

Case Study: OpenSSH

Summary

II: Software Vulnerabilities

5 MEMORY CORRUPTION

Introduction

Buffer Overflows

Shellcode

Protection Mechanisms

Assessing Memory Corruption Impact

Summary

6 C LANGUAGE ISSUES

Introduction

C Language Background

Table of Contents

Data Storage Overview
Arithmetic Boundary Conditions
Type Conversions
Type Conversion Vulnerabilities
Operators
Pointer Arithmetic
Other C Nuances
Summary

7 PROGRAM BUILDING BLOCKS
Introduction
Auditing Variable Use
Auditing Control Flow
Auditing Functions
Auditing Memory Management
Summary

8 STRINGS AND METACHARACTERS
Introduction
C String Handling
Metacharacters
Common Metacharacter Formats
Metacharacter Filtering
Character Sets and Unicode
Summary

9 UNIX I: PRIVILEGES AND FILES
Introduction
UNIX 101
Privilege Model
Privilege Vulnerabilities

Table of Contents

File Security
File Internals
Links
Race Conditions
Temporary Files
The Stdio File Interface
Summary

10 UNIX II: PROCESSES
Introduction
Processes
Program Invocation
Process Attributes
Interprocess Communication
Remote Procedure Calls
Summary

11 WINDOWS I: OBJECTS AND THE FILE SYSTEM
Introduction
Background
Objects
Sessions
Security Descriptors
Processes and Threads
File Access
The Registry
Summary

12 WINDOWS II: INTERPROCESS COMMUNICATION
Introduction
Windows IPC Security

Table of Contents

Window Messaging

Pipes

Mailslots

Remote Procedure Calls

COM

Summary

13 SYNCHRONIZATION AND STATE

Introduction

Synchronization Problems

Process Synchronization

Signals

Threads

Summary

III: Software Vulnerabilities in Practice

14 NETWORK PROTOCOLS

Introduction

Internet Protocol

User Datagram Protocol

Transmission Control Protocol

Summary

15 FIREWALLS

Introduction

Overview of Firewalls

Stateless Firewalls

Simple Stateful Firewalls

Stateful Inspection Firewalls

Spoofing Attacks

Summary

Table of Contents

16 NETWORK APPLICATION PROTOCOLS

- Introduction
- Auditing Application Protocols
- Hypertext Transfer Protocol
- Internet Security Association and Key Management Protocol
- Abstract Syntax Notation (ASN.1)
- Domain Name System
- Summary

17 WEB APPLICATIONS

- Introduction
- Web Technology Overview
- HTTP
- State and HTTP Authentication
- Architecture
- Web Tier: Model-View-Controller
- Problem Areas
- Common Vulnerabilities
- Harsh Realities of the Web
- Auditing Strategy
- Summary

18 WEB TECHNOLOGIES

- Introduction
- Web Services and Service-Oriented Architecture
- Web Application Platforms
- CGI
- Perl
- PHP
- Java

Table of Contents

ASP
ASP.NET
Summary
BIBLIOGRAPHY
INDEX