DISTRIBUTED SYSTEMS SECURITY
Issues, Processes and Solutions

Abhijit Belapurkar, Yahoo! Software Development India Pvt. Ltd., India
Anirban Chakrabarti, Infosys Technologies Ltd., India
Harigopal Ponnapalli, Infosys Technologies Ltd., India
Niranjan Varadarajan, Infosys Technologies Ltd., India
Srinivas Padmanabhuni, Infosys Technologies Ltd., India
Srikanth Sundarraj, Infosys Technologies Ltd., India

WILEY
A John Wiley and Sons, Ltd., Publication
# Contents

List of Figures                                                                                          xv
List of Tables                                                                                           xvii
Foreword                                                                                                 xix
Preface                                                                                                  xxi

## Chapter 1  Introduction

1.1 Background                                                                                         1
1.2 Distributed Systems
   1.2.1 Characteristics of Distributed Systems
   1.2.2 Types of Distributed System
   1.2.3 Different Distributed Architectures
   1.2.4 Challenges in Designing Distributed Systems
1.3 Distributed Systems Security
   1.3.1 Enterprise IT – A Layered View
   1.3.2 Trends in IT Security
1.4 About the Book
   1.4.1 Target Audience
References                                                                                               19

## Chapter 2  Security Engineering

2.1 Introduction                                                                                         21
2.2 Secure Development Lifecycle Processes – An Overview
   2.2.1 Systems Security Engineering Capability Maturity Model (SSE-CMM)
   2.2.2 Microsoft’s Security Development Lifecycle (SDL)
   2.2.3 Comprehensive Lightweight Application Security Process (CLASP)
   2.2.4 Build Security In
2.3 A Typical Security Engineering Process
   2.3.1 Requirements Phase
   2.3.2 Architecture and Design Phase
Chapter 3  Common Security Issues and Technologies  
3.1 Security Issues  
3.1.1 Authentication  
3.1.2 Authorization  
3.1.3 Data Integrity  
3.1.4 Confidentiality  
3.1.5 Availability  
3.1.6 Trust  
3.1.7 Privacy  
3.1.8 Identity Management  
3.2 Common Security Techniques  
3.2.1 Encryption  
3.2.2 Digital Signatures and Message Authentication Codes  
3.2.3 Authentication Mechanisms  
3.2.4 Public Key Infrastructure (PKI)  
3.2.5 Models of Trust  
3.2.6 Firewalls  
3.3 Conclusion  
References  
Chapter 4  Host-Level Threats and Vulnerabilities  
4.1 Background  
4.1.1 Transient Code Vulnerabilities  
4.1.2 Resident Code Vulnerabilities  
4.2 Malware  
4.2.1 Trojan Horse  
4.2.2 Spyware  
4.2.3 Worms/Viruses  
4.3 Eavesdropping  
4.3.1 Unauthorized Access to Confidential Data – by Users  
4.3.2 Unauthorized Access to Protected or Privileged Binaries – by Users  
4.3.3 Unauthorized Tampering with Computational Results  
4.3.4 Unauthorized Access to Private Data – by Jobs  
4.4 Job Faults  
References
Chapter 5  Infrastructure-Level Threats and Vulnerabilities  

5.1 Introduction 71
5.2 Network-Level Threats and Vulnerabilities 71
  5.2.1 Denial-of-Service Attacks 72
  5.2.2 DNS Attacks 76
  5.2.3 Routing Attacks 77
  5.2.4 Wireless Security Vulnerabilities 79
5.3 Grid Computing Threats and Vulnerabilities 82
  5.3.1 Architecture-Related Issues 82
  5.3.2 Infrastructure-Related Issues 86
  5.3.3 Management-Related Issues 88
5.4 Storage Threats and Vulnerabilities 92
  5.4.1 Security in Storage Area Networks 92
  5.4.2 Security in Distributed File Systems 95
5.5 Overview of Infrastructure Threats and Vulnerabilities 96
References 98

Chapter 6  Application-Level Threats and Vulnerabilities 101

6.1 Introduction 101
6.2 Application-Layer Vulnerabilities 102
  6.2.1 Injection Vulnerabilities 102
  6.2.2 Cross-Site Scripting (XSS) 105
  6.2.3 Improper Session Management 106
  6.2.4 Improper Error Handling 108
  6.2.5 Improper Use of Cryptography 109
  6.2.6 Insecure Configuration Issues 110
  6.2.7 Denial of Service 111
  6.2.8 Canonical Representation Flaws 112
  6.2.9 Overflow Issues 113
6.3 Conclusion 114
References 114
Further Reading 114
Chapter 10  Application-Level Solutions  
10.1 Introduction  
10.2 Application-Level Security Solutions  
  10.2.1 Input Validation Techniques  
  10.2.2 Secure Session Management  
  10.2.3 Cryptography Use  
  10.2.4 Preventing Cross-Site Scripting  
  10.2.5 Error-Handling Best Practices  
10.3 Conclusion  
References  

Chapter 11  Service-Level Solutions  
11.1 Introduction  
11.2 Services Security Policy  
  11.2.1 Threat Classification  
11.3 SOA Security Standards Stack  
  11.3.1 Inadequacy of SSL for Web Services  
11.4 Standards in Depth  
  11.4.1 XML Signature  
  11.4.2 XML Encryption  
  11.4.3 Web-Services Security (WS Security)  
  11.4.4 Security Assertions Mark-Up Language (SAML)  
  11.4.5 WS Policy  
  11.4.6 WS Trust  
  11.4.7 WS Security Policy  
  11.4.8 WS Secure Conversation  
  11.4.9 XKMS (XML Key Management Specification)  
  11.4.10 WS Privacy and P3P  
  11.4.11 Federated Identity Standards – Liberty Alliance Project and WS Federation  
  11.4.12 WS-I Basic Security Profile  
  11.4.13 Status of Standards  
11.5 Deployment Architectures for SOA Security  
  11.5.1 Message-Level Security and Policy Infrastructure  
  11.5.2 XML Firewalls  
11.6 Managing Service-Level Threats  
  11.6.1 Combating SQL and XPath Injection Attacks  
  11.6.2 Combating Cross-Site Scripting Attacks  
  11.6.3 Combating Phishing and Routing Attacks  
  11.6.4 Handling Authentication Attacks  
  11.6.5 Handling Man-in-the-Middle Attacks  
  11.6.6 Handling SOAP Attachment Virus Attacks  
  11.6.7 Handling Parameter-Tampering Attacks  
  11.6.8 XML Attacks  
  11.6.9 Known-Bug Attacks  

References  
