

TABLE OF CONTENTS

Chapter No.	Title	Page No.
I	NEED OF SOFTWARE SECURITY AND LOW-LEVEL ATTACKS	01-35
	1.1 Software Assurance and Software Security	
	1.2 Threats to Software Security	
	1.3 Sources of Software Insecurity	
	1.4 Benefits of Detecting Software Security	
	1.5 Properties of Secure Software	
	1.6 Memory-Based Attacks:	
	1.7 Defense against Memory-Based Attacks	
II	SECURE SOFTWARE DESIGN	36-82
	2.1 Requirements Engineering for Secure Software	
	2.2 SQUARE Process Model	
	2.3 Requirements Elicitation and Prioritization	
	2.4 Isolating the Effects of Untrusted Executable Content	
	2.5 Stack Inspection	
	2.6 Policy Specification Languages	
	2.7 Vulnerability Trends	
	2.8 Buffer Overflow	
	2.9 Code Injection	
	2.10 Session Hijacking	
	2.11 Secure Design: Threat Modeling, Security Design Principles	
III	SECURITY RISK MANAGEMENT	83-106
	3.1 Risk Management Life Cycle	
	3.2 Risk Profiling	
	3.3 Risk Exposure Factors	
	3.4 Risk Evaluation and Mitigation	
	3.5 Risk Assessment Techniques	
	3.6 Threat and Vulnerability Management	

IV	SECURITY TESTING	107-160
	4.1 Traditional Software Testing Comparison	
	4.2 Secure Software Development Life Cycle (SSDLC)	
	4.3 Risk-Based Security Testing	
	4.4 Prioritizing Security Testing with Threat Modeling	
	4.5 Penetration Testing	
V	SECURE PROJECT MANAGEMENT	161-177
	5.1 Governance and Security	
	5.2 Adopting an Enterprise Software Security Framework	
	5.3 Security and Project Management	
	5.4 Maturity of Practice	