NETWORK
AND
WEB SECURITY

Dr. PRATIK GITE
Assistant Professor
Department of Computer Science & Engineering
IPS ACADEMY : INSTITUTE OF ENGINEERING & SCIENCE
Indore, Madhya Pradesh, INDIA

NETWORK AND WEB SECURITY

Copyright © : Dr. Pratik Gite
Publishing Right ℗ : VSRD Academic Publishing
A Division of Visual Soft India Private Limited

ISBN-13: 978-93-87610-16-3
FIRST EDITION, AUGUST 2018, INDIA

Printed & Published by:
VSRD Academic Publishing
A Division of Visual Soft India Private Limited

Disclaimer: The author(s) are solely responsible for the contents of the papers compiled in this book. The publishers or its staff do not take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are requested to communicate such errors to the Editors or Publishers to avoid discrepancies in future.

Printed & Bound in India

VSRD ACADEMIC PUBLISHING
A Division of Visual Soft (India) Pvt. Ltd.

REGISTERED OFFICE
154, Tezabmill Campus, Anwarganj, KANPUR – 208 003 (UP) (INDIA)
Mob.: +91 9899936803 ||Web.: www.vsrdpublishing.com || Email: vsrdpublishing@gmail.com

MARKETING OFFICE
340, First Floor, Adarsh Nagar, Oshiwara, Andheri(W), MUMBAI – 400 053 (MH) (INDIA)
Mob.: +91 9956127040 || Web.: www.vsrdpublishing.com || Email: vsrdpublishing@gmail.com

FOREWORD

This reference book meets the requirement of students of engineering, professional and other courses. This book is useful to refer the syllabus of Indian Universities.

“Network and Web Security” takes a thorough approach to introduce the basic concepts of the network and security issues. It covers the key features of network and web security and advanced topics such as security issues and various attacks etc.

The book is organized in a systematic way to cover various topics with numerous examples. The goal of this book is to make the students to understand the concepts of network and web security.

This book will help the students to understand the concepts of network and web security in a simple and easy way. This book is for beginners who wish to know about introductory part of network and web security. This book is written by assuming that the reader need not be an expert of Mobile Ad-hoc Network.

The book has been provided summary and review questions which will be useful to the reader of the book. While writing this reference book, I have worked actively with the matter of the book to ensure that the book is technically correct, although it is hoped all material in this book is accurate, the possibility exists that some omissions or errors may present. It will be grateful if I receive suggestions from the users of this book and if they communicate to me for any errors they discover. It will help me to improve the future editions of this book. Suggested improvements should be mail at pratikgite135@gmail.com.

✍ *Dr. Pratik Gite*

ACKNOWLEDGEMENT

I am grateful to Dr. Sanjay Thakur, Principal, L.K.C.T. Indore, for his encouragement and suggestions in carrying out this book.

I am very much thankful to Dr. Archana Keerti Chowdhary, Principal, IES-IPS Academy Indore, for her continuous motivation and advice for this book. I would like to express my gratitude to Dr. Namrata Tapaswi, H.O.D., Computer Science and Engineering, IES-IPS Academy Indore, for her valuable comments and support. I express my sincere thanks to Dr. Ashish Moyade for their help throughout completion of this book.

I am very much thankful to my parents Mr. Rajendra Gite and Mrs. Sunita Gite for their personal attention and care. I am grateful to my Elder Brothers Mr. Sandeep Gite and Mr. Kapil Gite for inspiring me for this book. I want to thank my wife Mrs. Rajeshwari Gite for her patience and motivation.

I like to remember the motivation initiated by my respected Father in Law Mr. Rameshwar Tare and Mother in Law Anusuiya Tare.

I wish to thank faculty members of CSE department of IES-IPS Academy, Indore for their constant co-operation, directly inspiration and encouragement.

I deeply express my heartful thanks to the VSRD Academic Publishing (A Division of Visual Soft India Private Limited) for publishing this book in such a beautiful getup and well in time.

✍ *Dr. Pratik Gite*

KEY FEATURES

- *Easy language used for better understanding.*
- *Key concepts are mentioned at the beginning of each chapter.*
- *Each chapter contains summary and review questions.*
- *Reader friendly presentation for easy grasp.*
- *Thoroughly discussed the important topics of Information Technology.*
- *List of definitions for better understanding of technical terms.*
- *Topics are covered with real life examples.*
- *Technical terms are explained with pictorial presentation and screen shots.*
- *Includes notes and remarks for quick review.*
- *Some important points to be remembered are mentioned separately.*

Dedicated to

My Parents,
Wife, Brothers,
Son (Shivay)
&
All Students, Research
Scholars
and
Teachers

ABBREVIATION

ACRONYM	MEANING
ACK	Acknowledgement
ACL	Access control list
ADSL	Asymmetric digital subscriber line
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol (routing protocol)
BSS	Basic service set (Wi-Fi)
CAT	Category (e.g. CAT-5 cable)
CCITT (obs.)	Standards organization that has been replaced by ITU-T
CHAP	Challenge-Handshake Authentication Protocol (PPP)
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate (Frame Relay)
CLI	Command line interpreter
CPE	Customer premises equipment
CPU	Central processing Unit
CRC	Cyclical redundancy check
CRC-1 6-CCITT	Cyclical redundancy check (X.25, HDLC)
CRT	Cathode Ray Tube
CSMA/CA	Carrier sense multiple access / collision avoidance
CSMA/CD	Carrier sense multiple access / collision detection
CSU/DSU	Channel service unit / data service unit
CMOS	Comp metal-oxide semiconductor
DCE	Data communications equipment
DEC (obs.)	Digital Equipment Corporation
DES	Data Encryption Standard (obs. See AES)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRAM	Dynamic random-access memory
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexor
DTE	Data Terminal Equipment
DMI	Desktop Management Interface
EHA	Ethernet Hardware Address (MAC address)
EIA	Electronics Industry Alliance
EIGRP	Enhanced Interior Gateway Routing Protocol
EOF	End Of Frame (HDLC, etc.)
ESS	Extended service set (Wi-Fi group)
FCC	Federal Communications Commission (US)
FCS	Frame check sequence (Ethernet)
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
GBIC	Gigabit interface converter
gbps	Gigabit per second

ACRONYM	**MEANING**
GEPOF	Gigabit Ethernet (over) Plastic Optical Fiber
HDLC	High-level Data Link Control
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IANA	Internet Assigned Number Authority
ICMP	Internet Control Message Protocol
IDF	Intermediate distribution frame
IDS	Intrusion Detection
IEEE	Institute for Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion prevention system
IS-IS	Intermediate System to Intermediate System (routing protocol)
ISDN	Integrated Services Digital Network
ISP	Internet service provider
ITU-T	International Telecommunications Union
kbps	Kilobit per second
LACP	Link Aggregation Control Protocol
LAN	Local area network
LAPB	Link Access Procedure, Balanced (x.25)
LAPF	Link-access procedure for frame relay
LLC	Logical link control
MAC	Media access control
MAN	Metropolitan area network
Mbps	Megabits per second
MC	Multiple choice
MDF	Main distribution frame
MIB	Management information base (SNMP)
MoCA	Multimedia over Coax Alliance
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmission Unit
NAC	Network access control
NAT	Network Address Translation
NBMA	Non-Broadcast Multiple Access (e.g. Frame Relay ATM)
NIC	Network Interface Card
NRZ	Non-return-to-zero
NRZI	Non-return to zero inverted
NVRAM	Non-volatile RAM
OSI	Open System Interconnect (joint ISO and ITU standard)
OSPF	Open Shortest Path First (routing protocol)
OUI	Organization Unique Identifier
PAP	Password authentication protocol
PAT	Port address translation
PC	Personal computer (host)
PIM	Personal information manager
PIM	Privileged Identity Management
PCM	Pulse-code modulation
PDU	Protocol data unit (such as segment, packet, frame, etc.)

ACRONYM	MEANING
POP3	Post Office Protocol, version 3
POP	Point of presence
POST	Power-on self test
POTS	Plain old telephone service
PPP	Point-to-point Protocol
PPTP	Point-to-Point Tunneling Protocol
PTT	Public Telephone and Telegraph
PVST	Per-VLAN Spanning Tree
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RARP	Reverse ARP
RFC	Request for Comments
RIP	Routing Information Protocol
RLL	Run-Length Limited
ROM	Read-Only Memory
RSTP	Rapid Spanning Tree Protocol
RTP	Real-time Transport Protocol
RCP	Royal College of Physicians
SDLC	Synchronous Data Link Control
SDN	Software Defined Networking
SFD	Start-of-frame delimiter (Ethernet, HDLC, etc.)
SFP	Small form-factor pluggable
S-HTTP	Secure HTTP (rarely used)
SLARP	Serial Line ARP (Address Resolution Protocol)
SLIP	Serial Line Internet Protocol (obs.)
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture (IBM)
SNAP	SubNet Access Protocol
SNMP	Simple Network Management Protocol
SOF	Start of frame
SRAM	Static random access memory
SSH	Secure shell
SSID	Service set identifier (Wi-Fi)
STP	Spanning Tree Protocol
SYN (TCP)	Synchronization
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time-division multiplexing
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Alliance
TOFU	Trust On First Use
UDP	User Datagram Protocol
USB	Universal Serial Bus
UTP	Unshielded twisted pair
VC	Virtual circuit
VLAN	Virtual local area network
VLSM	Variable-length subnet masking
VPN	Virtual private network
W3C	World Wide Web Consortium
WAN	Wide-area network

ACRONYM	**MEANING**
WEP	Wired Equivalent Privacy
Wi-Fi	IEEE 802.11 (Wi-Fi Alliance)
WPA	Wi-Fi Protected Access
www	World Wide Web

DEFINITIONS

Public Key Infrastructure: Public Key Infrastructure is a technology used in modern security mechanisms on the internet. It covers a cryptographic system including encryption, asymmetric key cryptography, message digest and digital signature.

Cryptography: Art and science of achieving security by encoding messages to make them non-readable is known as cryptography.

Cryptanalysis: The technique of decoding messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.

Cryptology: A combination of cryptography and cryptanalysis is known as cryptology.

Plain Text: Any communication in the language that we speak- that is the human language, takes the form of plain text or clear text.

Cipher text: When a plain text message is codified using any suitable scheme, the resulting message is called as cipher text.

Encryption Algorithm: Step by step procedure to convert plaintext into cipher text and vice versa is known as encryption algorithm.

Key: Stream of bit used in cryptographic algorithm for encryption and decryption is called as a key.

Encryption: The process of encoding plain text message into cipher text message is called as encryption.

Decryption: The process of decoding cipher text message into plain text message is called decryption.

Brute force attack: Brute force attack is a method of defeating a cryptographic scheme by trying a large or all possible number of possibilities.

Symmetric Key Cryptography: In Symmetric Key Cryptography, only one key (same key) is used for both encryption and decryption. Both the parties (sender and receiver) agree upon the key before any transmission begins.

Asymmetric Key Cryptography: It Asymmetric Key Cryptography, a key pair (Two different Keys), is used i.e. one key is used for encryption and only the other corresponding key is used for decryption.

Threat: Any potential event or act that could cause injury to employee or assets.

Risk: The chance of a vulnerability being exploited.

Vulnerability: A cause to security that could permit a threat to make injury.

Digital Signature: A digital signature is used to authenticate the sender of the message and to check the integrity of the message, i.e. that it has not been altered in transit.

Digital Certificate: Digital certificate is a document such as our passport or driving license. It is basically a computer file such as ABC.cer and is certified by a trusted agency called certification Authority (CA).

Secure Socket Layer (SSL): It is an internet protocol used for exchange of information between browser & server developed by Netscape Corporation.

Secure Electronic Transaction (SET): The Secure Electronic Transaction (SET) is an open encryption and security specification that is designed for protecting credit card transactions on the Internet.

Cyber Law: Cyber Law is the law governing computers and the Internet.

Cyber stalking: Cyber stalking is a criminal offense with use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization.

Defamation: The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person.

Hacking: Hacking is the practice of modifying the features of a computer system, in order to accomplish a goal outside of the creator's original purpose.

Hacker: A hacker is a person who tries to gain un-authorized access to your computer.

Cracker: A hacker expert at accessing password-protected computers, files, and networks is known as "crackers."

Spam: Spam is any kind of unwanted email sent in bulk by companies

Information theft: Information theft or identity theft is a crime of obtaining the personal or financial information of another person for the sole purpose of assuming that person's name or identity in order to make transactions or purchases.

Denial of Service (DoS): An attack, in which an attacker attempts to prevent legitimate users from accessing information or services, is known as Denial of Service attack.

Logic Bomb: Logic bomb is a malware that is triggered by a response to an event, such as launching an application or when a specific date/time is reached.

Passive Attack: A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it.

Active Attack: An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks.

External Attack: External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls.

Internal Attacks: Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult

CONTENTS

CHAPTER 1 : NETWORK SECURITY

1.1. INTRODUCTION 1
1.2. CLASSIFICATION OF ATTACKS 2
1.3. PASSIVE ATTACK 2
1.4. ACTIVE ATTACK 2
1.6. INTRUSION DETECTION SYSTEM 3
1.7. TYPES OF IDS 3
1.8. SYSTEM INTEGRITY VERIFIER 3
1.9. SOME POPULAR IDS TOOLS 4
1.10. INTRUDERS 4
1.11. PANETRATION TESTING 4
1.12. TYPES OF PANETRATION TESTING 4
1.13. CATEGORIES OF SECURITY ASSESMENT 5
1.14. RISK ASSESMENT 5
1.15. THREAT MODELLING 5
1.16. THREAT ASSESMENT 5
1.17. BUG COUNTY 5
1.18. WHAT YOU LEARNED IN THIS CHAPTER? 6

CHAPTER 2 : CRYPTOGRAPHY

2.1. CRYPTOSYSTEM 9
2.2. CRYPTANYSIS 10
2.3. OBJECTIVE OF CRYPTOGRAPHY 10
2.4. BASIC MODEL OF CRYPTOSYSTEM 10
2.5. DIFFERENT COMPONENTS OF CRYPTOSYSTEM 11
2.6. TYPES OF CRYPTOSYSTEM 11
2.7. SYMMETRIC KEY ENCRYPTION 12
2.8. CHALLENGES IN SYMMTRIC KEY CRYPTOSYSTEM 12
2.9. ASYMMTRIC KEY ENCRYPTION 12
2.10. RELATION BETWEEN SYMMTRIC AND ASYMMTRIC 13
2.11. DEFINE ALL CRYPTOGRAPHIC ATTACK 13
2.12. CROSS SITE SCRIPTING 14
2.13. SQL INJECTION 14
2.14. WEB APPLICATION SECURITY 14
2.15. DIGITAL SIGNATURE 15
2.16. HOW DIGITAL SIGNATURE WORKS 15
2.17. DIGITAL CERTIFICATE 15
2.18. CLASSIFICATION OF COMPUTER MEMORY 16
2.19. REASON FOR USING DIGITAL CERTIFICATE 16
2.20. COMPONENTS OF DIGITAL SIGNATURE 16
2.21. COMPUTER VIRUS 16
2.22. FIVE MAJOR TYPES OF VIRUS 17
2.23. WORMS 17
2.24. WHAT YOU LEARNED IN THIS CHAPTER? 18

CHAPTER 3 : SECURITY ISSUES

3.1. NEED OF NETWORK SECURITY 20
3.2. NETWORK SECURITY REQUIREMENTS 20
3.3. SECURITY ATTACKS 20
3.4. NETWORK LAYER ATTACK 22
3.5. ROUTING ATTACK 24
3.6. RUSHING ATTACK 25
3.7. TRANSPORT LAYER ATTACK 25
3.8. APPLICATION LAYER ATTACK 25
3.9. REQUIREMENTS FOR THE SECURE ROUTING PROTOCOLS 27
3.10. WHAT YOU LEARNED IN THIS CHAPTER? 28

CHAPTER 4 : IP AND WEB SECURITY

4.1. HACKER AND HACKING 30
4.2. TYPES OF HACKING 30
4.3. OVERVIEW OF SYSTEM HACKING LIFECYCLE 31
4.4. OVERVIEW OF SYSTEM HACKING LIFECYCLE 31
4.5. IP SECURITY 32
4.6. WEB APPLICATION SECURITY 32
4.7. NEED OF SECURE AUTHENTICATION MECHANISM 32
4.8. EMAIL SPIDER 32
4.9. FIREWALL 32
4.10. COMPUTER FORENSICS 34

CHAPTER 5 : COMPUTER NETWORK AND IT APPLICATION IN COMMUNICATION

5.1. NETWORK SERVICES 37
5.2. TELEPHONE SERVICES 38
5.3. CELLULAR TELEPHONE SERVICES 38
5.4. RADIO AND TV BROADCASTING 39
5.5. AUDIO-VISUAL CONFERENCING 39
5.6. VIDEO-ON-DEMAND 40
5.7. INTRODUCTION TO NETWORK PROTOCOL AND TOPOLOGIES 41
5.8. TYPES OF NETWORK: LAN, WAN 47
5.9. WEB BROWSER 49
5.10. WHAT YOU LEARNED IN THIS CHAPTER? 52
5.11. WHAT YOU LEARNED IN THIS CHAPTER? 53

CHAPTER 6 : EVOLUTION OF CRYPTOGRAPHIC TECHNIQUES

6.1. INTRODUCTION 55
6.2. EVOLUTION OF CRYPTOGRAPHY 57
6.3. CHARACTERISTICS OF MODERN CRYPTOGRAPHY 57
6.4. KERCKHOFF’S PRINCIPLE FOR CRYPTOSYSTEM 58
6.6. ASSUMPTIONS OF ATTACKER 59
6.7. DETAILS OF THE ENCRYPTION SCHEME 60
6.8. CRYPTOGRAPHIC ATTACKS 60
6.9. PRACTICALITY OF ATTACKS 62

6.10. EARLIER CRYPTOGRAPHIC SYSTEMS 62
6.11. DATA ENCRYPTION STANDARD 71
6.12. ADVANCED ENCRYPTION STANDARD 77
6.13. PUBLIC KEY CRYPTOGRAPHY 84
6.14. PUBLIC KEY ENCRYPTION SCHEME 85
6.15. DATA INTEGRITY IN CRYPTOGRAPHY 89
6.16. CRYPTOGRAPHY HASH FUNCTIONS 90
6.17. DESIGN OF HASHING ALGORITHMS 91
6.18. APPLICATIONS OF HASH FUNCTIONS 93
6.19. DATA INTEGRITY CHECK 94
6.20. MESSAGE AUTHENTICATION 94
6.21. CRYPTOGRAPHY DIGITAL SIGNATURES 96
6.22. MODEL OF DIGITAL SIGNATURE 96
6.23. ENCRYPTION WITH DIGITAL SIGNATURE 98
6.24. CRYPTOGRAPHY – BENEFITS 103
6.25. FUTURE OF CRYPTOGRAPHY 104