

CONTENTS

ACKNOWLEDGMENTS.....	I
DEDICATION.....	II
LIST OF FIGURES.....	III
ABBREVIATIONS.....	IV
ABSTRACT.....	V
ملخص البحث.....	VI
TABLE OF CONTENTS.....	VII
<u>CHAPTER-1: INTRODUCTIOMN.....</u>	1
1.1 Background.....	1
1.2 VOIP Components.....	2
1.2.1 The IP network.....	2
1.2.2 Call Processor/Controllers.....	3
1.2.3 Media/Signaling Gateways.....	4
1.2.4 Subscriber Terminal.....	5
1.3 VOIP Standards and Protocols.....	5
1.4 Problem statements.....	9
1.5 Objectives of the research.....	10
1.6 Methodologies.....	11
1.7 Thesis outlines.....	11
<u>CHAPTER-2:H.323 SIGNALING PROTOCOL.....</u>	13
2.1 Background.....	13
2.2 H.323 Components.....	15
2.2.1 The gateway.....	15
2.2.2 The gatekeeper.....	16
2.2.3 Multipoint control unit (MCU).....	17
2.2.4 Terminals.....	18
2.3 Basic architecture of H.323.....	20
2.3.1 Audio CODECs.....	20
2.3.2 Video CODECs.....	20
2.3.3 Data conferencing.....	21
2.4 Call establishment.....	23
2.4.1 Registration.....	23
2.4.2 Negotiation channel usage and capabilities (H.245).....	24
2.4.3 Q.931.....	24
2.5 VOIP Quality of service (QoS).....	29
2.5.1 Packet Loss.....	30
2.5.2 Latency (delay).....	31
2.5.3 Jitter.....	32
2.5.4 Bandwidth.....	33
2.6 Media Gateway Control Protocol (MGCP) and H.248.....	35

CHAPTER-3: SESSION INITIATION PROTOCOL (SIP).....37

3.1 Backgrounds.....	37
3.2 Basic components.....	38
3.2.1 User agent (UA).....	38
3.2.2 SIP Proxy.....	38
3.2.3 Registrar.....	39
3.2.4 SIP redirect server.....	39
3.3 SIP basic Architecture.....	39
3.3.1 Transmission Control Protocol (TCP).....	45
3.3.1.1 Protocol operation.....	46
3.3.1.2 Connection establishment.....	48
3.3.1.3 Data transfer.....	49
3.3.1.4 Congestion throttling.....	51
3.3.1.5 Connection termination.....	52
3.3.1.6 TCP ports.....	52
3.3.1.7 TCP packet.....	53
3.3.2 User Datagram Protocol (UDP).....	56
3.3.2.1 UDP Packet structure.....	57
3.3.3 Real Time Streaming Protocol (RTSP).....	60
3.3.3.1 RTSP commands	61
3.3.4 Session Description Protocol (SDP).....	62
3.4 Call establishment	63

CHAPTER-4: VOIP VULNERABILITIES ANDTHREATS.....65

4.1 Viruses, Worms and Trojan Horses.....	68
4.2 Denial of Service (DoS)	68
4.2.1 Implementation Flaw DoS.....	70
4.2.2 Flood DoS.....	70
4.2.3 Application-level DoS.....	70
4.2.4 Platform DoS.....	70
4.2.5 Signaling and Media DoS.....	71
4.3 Traffic Flow Redirection.....	71
4.4 Authentication Weakness.....	72
4.5 MAC Spoofing.....	72
4.6 Information Sniffing.....	73
4.7 Man-In-The-Loop (MITL) Attacks.....	73
4.8 Protocol vulnerabilities.....	74
4.9 Eavesdropping.....	75

4.10 Voice SPAM or SPAM over Internet Telephony (SPIT).....	75
4.11 Platform Vulnerabilities.....	75
4.12 IP Phones Vulnerabilities.....	76
4.13 Registration Hijacking.....	76
4.14 Proxy Impersonation.....	77
4.15 Message Tampering.....	78
4.16 Session Tear-Down.....	78
4.17 Instant Messaging Security Threats.....	78
4.18 Lack of The network security policies.....	79
4.18.1 Acceptable use of corporate assets policy.....	80
4.18.2 Server and workstation configuration policy.....	80
4.18.3 Patch management policy.....	80
4.18.4 Network infrastructure policy.....	81
4.18.5 User account policy.....	81
4.18.6 Other policies.....	81
4.18.7 Designing, implementing and evaluating the network security policies.....	82
4.18.7.1 Preparation.....	82
4.18.7.2 Prevention.....	82
4.18.7.3 Response.....	82
4.18.8 The benefit of the network security policies.....	83
4.18.8.1 Savings by ensuring security of data.....	83
4.18.8.2 Savings by preventing a denial-of-service (DoS) attack.....	83
4.18.8.3 Savings by preventing data manipulation.....	84
4.18.8.4 Savings by increasing efficiency.....	84
4.18.8.5 Savings by reducing "unknown" problems on the network.....	84
4.18.9 General goals of the network security Policies.....	84

CHAPTER-5: VOIP SECURITY STRATEGIES AND RECOMMENDED SOLUTIONS.....86

1. Planning.....	87
2. Security analysis.....	87
3. Network components.....	88
4. Standard-based authentication and encryption signaling and media.....	90
5. Physical security.....	91
6. Redundancy power and data backup systems.....	91
7. Patches updating.....	92
8. Network segmentation	92
8.1 Logical Address Segregation.....	93
8.2 VLANs.....	94
9. Access control.....	95

9.1 Dynamic port mapping.....	96
9.2 Static mapping	96
10. Protect against switch-directed attacks.....	99
11. Network traffic monitoring.....	102
12. Perfect security policies.....	103

CHAPTER-6: DESIGNING, IMPLEMENTING AND EVALUATING

THE VOIP SYSTEM104

6.1 The system designing implementation and testing steps.....	104
6.2 Preparation of Equipments.....	104
6.3 System Design	105
6.4 Design Steps.....	106
6.3.1 Downloading Asterisk Source Code.....	106
6.3.2 Installing Linux for Asterisk.....	106
6.3.3 Asterisk Compilation, installation and configuration steps.....	128
6.3.4 Asterisk Basic Configurations	128
6.4 Results and evaluation.....	133

CHAPTER-7: CONCLUTION.....134

REFERENCES.....137

APPENDICIES.....137

8.1 APPENDIX-A (Ports and Services).....	140
8.2 APPENDIX-B (DPH-120S Specifications).....	141
8.3 APPENDIX-C (NETASQ-F5000 Specifications).....	143
8.4 APPENDIX -D (Alpine3804 Switch Specifications).....	144
8.5 APPENDIX -E (Asterisk Specifications).....	150