

# LIST OF FIGURES

Figure 1: Email Delivery Process .....	4
Figure 2: Basic structure of an email message .....	11
<i>Figure 3: How SMTP Works? .....</i>	<i>12</i>
<i>Figure 4: How POP3 works? .....</i>	<i>16</i>
<i>Figure 5: How IMAP works? .....</i>	<i>16</i>
<i>Figure 6: Usage of various ports at different stages of email delivery .....</i>	<i>17</i>
Figure 7: Email Spoofing Process .....	23
<i>Figure 8: Gmail Settings for changing the display name .....</i>	<i>24</i>
<i>Figure 9: Inbox view having received an email with the fake display name .....</i>	<i>24</i>
<i>Figure 10: Email details view of an email having a fake display name .....</i>	<i>24</i>
<i>Figure 11: Email message header showing spoofing via lookalike domains .....</i>	<i>25</i>
<i>Figure 12: Email message showing spoofing via legitimate domains .....</i>	<i>26</i>
Figure 13: Example of a Spoofed Email .....	30
Figure 14: spoofed email showing via in-sender email .....	32
Figure 15: spoofed email showing warning message to user .....	33
Figure 16: Message header of a spoofed email.....	33
Figure 17: Sender Policy Framework (SPF) Process Flow .....	35
Figure 18: DomainKeys Identified Mail (DKIM) Process Flow .....	37
Figure 19: DMARC Process Flow .....	39
Figure 20: Email Message Details showing ARC Headers .....	42
Figure 21: Reverse DNS process flow .....	55
Figure 22: Result of reverse DNS lookup .....	56
Figure 23: mail-server.in email server home page .....	57
Figure 24: DKIM key setup in Modoboa .....	57

Figure 25: Preview of OpenDKIM configuration file .....	59
Figure 26: Preview of OpenDKIM Key Table .....	59
Figure 27: Preview of OpenDKIM Signing Table .....	59
Figure 28: DNS entry of SPF for domain mail-server.in .....	60
Figure 29: DNS entry of DKIM for domain mail-server.in .....	60
Figure 30: DNS entry of DMARC for domain mail-server.in .....	61
Figure 31: Regular email delivery in inbox for domain “mail-server.in” without having any anti-spoofing protocols .....	61
Figure 32: Raw email summary for domain “mail-server.in” without having any anti-spoofing protocols .....	62
Figure 33: Raw email details for domain “mail-server.in” without having any anti-spoofing protocols .....	62
Figure 34: Regular email delivery in inbox for domain “mail-server.in” with all 3 anti-spoofing protocols .....	63
Figure 35: Raw email summary for domain “mail-server.in” with all 3 anti-spoofing protocols .....	63
Figure 36: Raw email details for domain “mail-server.in” with all 3 anti-spoofing protocols .....	63
Figure 37: Spoofed email delivery in inbox for domain “msubaroda.ac.in” without having any anti-spoofing protocols .....	64
Figure 38: Spoofed email summary for domain “msubaroda.ac.in” without having any anti-spoofing protocols .....	64
Figure 39: Spoofed email details for domain “msubaroda.ac.in” without having any anti-spoofing protocols .....	65
Figure 40: Spoofed email delivery in inbox for domain “gmail.com” with all 3 anti-spoofing protocols .....	65

Figure 41: Raw email summary for domain “gmail.com” with all 3 anti-spoofing protocols .....	66
Figure 42: Raw email details for domain “gmail.com” with all 3 anti-spoofing protocols .....	66
Figure 43: Part of python script used to send spoofed email .....	67
Figure 44: Spoofed email delivery in inbox after bypassing SPF .....	67
Figure 45: Raw email summary for spoofed email after bypassing SPF.....	67
Figure 46: Spoofed email delivery in inbox after bypassing SPF and DKIM .....	68
Figure 47: Raw email summary for spoofed email after bypassing SPF and DKIM.....	68
Figure 48: Raw email details for spoofed email after bypassing SPF and DKIM .....	69
Figure 49: Part of python script used to send spoofed email with multiple email ids...69	
Figure 50: Spoofed email delivered in inbox of “yahoo.co.in” after bypassing SPF, DKIM and DMARC.....	69
Figure 51: Spoofed email delivered in inbox of “gmail.com” after bypassing SPF, DKIM and DMARC.....	70
Figure 52: Raw email summary for spoofed email after bypassing SPF, DKIM and DMARC .....	70
Figure 53: Raw email details for spoofed email after bypassing SPF, DKIM and DMARC .....	70
Figure 54: Raw email summary for genuine email sent from domain “msubaroda.ac.in” .....	71
Figure 55: Raw email details for genuine email sent from domain “msubaroda.ac.in”	71
Figure 56: Email delivery report for spoofed email from domain “gmail.com” .....	72
Figure 57: Email delivery report for genuine email from domain “msubaroda.ac.in” ...	72
Figure 58: Email delivery information for genuine email from domain “msubaroda.ac.in” .....	72
Figure 59: Raw email summary for spoofed email from domain “msubaroda.ac.in” ....	73

Figure 60: Raw email summary for spoofed email from domain "gmail.com" .....	74
Figure 61: Email delivery report for spoofed email from domain "msubaroda.ac.in" ..	74
Figure 62: Email delivery report for spoofed email from domain "gmail.com" .....	74
Figure 63: Email delivery information for spoofed email from domain "msubaroda.ac.in" .....	75
Figure 64: Basic flow chart of various components involved in email process .....	79
Figure 65: Process of calculation of EAIC.....	80
Figure 66: Process of calculation of EAIC in case EAIC gets more than 16 digits .....	80
Figure 67: Flowchart for calculation of EAIS score .....	82
Figure 68: Email header details showing EAIC code received by RMS.....	84
Figure 69: Flowchart for Adaptive Authentication Framework for Email (AAFE) .....	85
Figure 70: Application server representing domain "yahoo.com" .....	86
Figure 71: Application server representing domain "gmail.com" .....	86
Figure 72: Application server representing domain "msubaroda.ac.in" .....	87
Figure 73: Sending email using our application server.....	88
Figure 74: Email successfully authenticated at RMS using our proposed AAFE.....	90
Figure 75: Email not authenticated at RMS using our proposed AAFE .....	90
Figure 76: Spoofed email successfully delivered in inbox of recipient.....	94
Figure 77: Raw email message for spoofed email for domain msubaroda.ac.in .....	94
Figure 78: Raw email message for spoofed email for domain gmail.com .....	94
Figure 79: Test results for spoofed email for domain gmail.com having multiple senders .....	95
Figure 80: Spoofed email message header displaying EAIC code .....	95