



ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΙΡΑΙΑ  
ΤΟΜΕΑΣ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ Η/Υ, ΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΚΤΥΩΝ  
ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ  
*Εργ. Τεχνολογίας Λογισμικού & Υπηρεσιών*  
S<sup>2</sup>E Lab

# ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Σπουδαστές:

Ριζόπουλος Αντώνιος

Τσιουτσιουρήγας Δημήτριος

Θέμα:

**“Αποτίμηση Ασφάλειας Πληροφοριακού Συστήματος  
Διακομιδής Ηλεκτρονικού Ταχυδρομείου”**



**Εισηγητές:**

Δρ. Γ. Ν.Πρεζεράκος  
Καθηγητής

Δ. Ν. Καλλέργης  
Εργ. Συνεργάτης

# ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΛΗΨΗ.....	8
ΚΕΦΑΛΑΙΟ 1: Επεξήγηση και παρουσίαση τεχνολογιών, πρωτοκόλλων και διαδικασιών που χρησιμοποιούνται στις υπηρεσίες Ηλεκτρονικού Ταχυδρομείου.....	9
1.1 Ιστορική αναδρομή.....	9
1.2 Η έννοια του Ηλεκτρονικού Ταχυδρομείου.....	11
1.3 Τα οφέλη του Ηλεκτρονικού Ταχυδρομείου.....	12
1.4 Διαχειριστής Αλληλογραφίας Ηλεκτρονικού Ταχυδρομείου (Mail Client) ....	13
1.5 Διακομιστής Ηλεκτρονικού Ταχυδρομείου (Mail Server).....	14
1.6 Βασικά Ηλεκτρονικού Ταχυδρομείου – Επισκόπηση των υπηρεσιών αποστολής ηλεκτρονικών μηνυμάτων.....	15
1.6.1 Απλό σύστημα Ηλεκτρονικού Ταχυδρομείου ενός Οργανισμού.....	16
1.6.2 Απομακρυσμένος χρήστης με πρόσβαση στο δίκτυο Ηλεκτρονικού Ταχυδρομείου του Οργανισμού.....	17
1.6.3 Απλό σύστημα Ηλεκτρονικού Ταχυδρομείου μεταξύ δύο παραρτημάτων του Οργανισμού.....	19
1.6.4 Επικοινωνία μεμονωμένου χρήστη με Παροχέα Υπηρεσιών Διαδικτύου (ISP).....	21
1.6.5 Επικοινωνία χρηστών Οργανισμού με Παροχέα Υπηρεσιών Διαδικτύου (ISP).....	23
1.6.6 Δίκτυο Οργανισμού συνδεδεμένο με Παροχέα Υπηρεσιών Διαδικτύου (ISP).....	24
1.6.7 Δίκτυο Οργανισμού συνδεδεμένο με το Διαδίκτυο.....	26
1.7 Παρουσίαση της διεύθυνσης Ηλεκτρονικού Ταχυδρομείου.....	27
1.8 Μεταφορά ηλεκτρονικού μηνύματος (email) μεταξύ Διαχειριστών Αλληλογραφίας Ηλεκτρονικού Ταχυδρομείου (Mail Client).....	28
1.8.1 Μεταφορά ηλεκτρονικού μηνύματος στο ίδιο δίκτυο.....	28
1.8.2 Μεταφορά ηλεκτρονικού μηνύματος σε διαφορετικά δίκτυα.....	29

1.9	Διαδικασία εσφαλμένης αναγνώρισης μεταξύ των Διακομιστών Ηλεκτρονικού Ταχυδρομείου (Mail Server) του αποστολέα και του παραλήπτη.....	31
1.10	Διαδικασία μεταφοράς των e-mails από τον Διαχειριστή Αλληλογραφίας Ηλεκτρονικού Ταχυδρομείου (Mail Client) στον Διακομιστή Ηλεκτρονικού Ταχυδρομείου (Mail Server) και αντίστροφα .....	32
1.11	Περιγραφή του πρωτοκόλλου SMTP (Simple Mail Transfer Protocol).....	33
1.12	Περιγραφή του πρωτοκόλλου POP3 (Post Office Protocol - version 3).....	36
1.13	Σύνδεση μεταξύ πρωτοκόλλων SMTP και POP3 .....	39
1.14	Περιγραφή πρωτοκόλλου IMAP (Internet Message Access Protocol) .....	40
1.15	Περιγραφή πρωτοκόλλου SSL (Secure Sockets Layer) .....	43
1.15.1	Γενική περιγραφή .....	43
1.15.2	Τρόπος λειτουργίας .....	44
1.15.3	Επιβάρυνση σε υπολογιστική ισχύ από τη χρήση του πρωτοκόλλου SSL .	47
1.15.4	Διαφορά μεταξύ SSL και TLS .....	47
1.16	Περιγραφή πρωτοκόλλου UUCP (Unix-to-Unix Copy Protocol).....	49
1.17	Η έννοια της Υπηρεσίας Ονομάτων Τομέων (Domain Name System) .....	50
1.17.1	Συσχέτιση Εξυπηρετητή Ονομάτων Τομέων (DNS Server) με Mail Server	50

## ΚΕΦΑΛΑΙΟ 2: Αναλυτική περιγραφή των καταγραφέντων θεμάτων ασφαλείας από οικονομοτεχνική σκοπιά.....

2.1	Κατηγορίες λογισμικών βασιζόμενες στην άδεια χρήσης τους.....	52
2.1.1	Λογισμικό Ανοικτού Κώδικα (open source) .....	52
2.1.2	Ελεύθερο Λογισμικό .....	53
2.1.3	Εμπορικό Λογισμικό .....	54
2.2	Κόστος πληροφοριακού συστήματος ηλεκτρονικού ταχυδρομείου .....	55
2.2.1	Σύγκριση κόστους ελεύθερων/εμπορικών εφαρμογών.....	55
2.3	Το κόστος της ανεπιθύμητης αλληλογραφίας.....	57
2.3.1	Γενικές δαπάνες των ανεπιθύμητων μηνυμάτων.....	59
2.4	Πολιτική Αποδεκτής Χρήσης (acceptable ή appropriate use policy) .....	62

ΚΕΦΑΛΑΙΟ 3: Αναλυτική περιγραφή των καταγραφέντων θεμάτων ασφαλείας από τη σκοπιά του μηχανικού Η/Υ συστημάτων .....	66
3.1 Ασφάλεια πληροφοριακών συστημάτων .....	66
3.2 Ανάλυση θεμάτων ασφαλείας .....	67
3.2.1 Ανεπιθύμητη αλληλογραφία (spam).....	67
3.2.1.1 Τρόποι αντιμετώπισης από την πλευρά του χρήστη .....	68
3.2.1.2 Τρόποι αντιμετώπισης από την πλευρά του διαχειριστή. ....	69
3.2.2 Phising .....	70
3.2.3 Κακόβουλα λογισμικά (ιοί) .....	71
3.2.3.1 Κριτήρια επιλογής κατάλληλου λογισμικού ανίχνευσης και καταπολέμησης κακόβουλου λογισμικού .....	74
3.2.4 Λειτουργία open relay και επικοινωνία του Διακομιστή με απομακρυσμένους Η/Υ χρησιμοποιώντας το πρωτόκολλο telnet. ....	74
3.2.5 Διασφάλιση των διαπιστευτηρίων εισόδου των χρηστών στις παρεχόμενες υπηρεσίες.....	75
3.2.6 Απομακρυσμένη σύνδεση χρησιμοποιώντας το πρωτόκολλο SSH (Secure Shell authentication protocol).....	76
ΚΕΦΑΛΑΙΟ 4: Αντιπαράθεση των επικρατέστερων M.T.A. (Mail Transfer Agent) εφαρμογών σε συστήματα Linux.....	77
4.1 Γενικά περί M.T.A. εφαρμογών .....	77
4.2 Περιγραφή των Sendmail και Postfix.....	78
4.2.1 Έλεγχος περιεχομένου των ηλεκτρονικών μηνυμάτων .....	78
4.2.2 Τρόπος εκτέλεσης .....	79
4.2.3 Διαχείριση ουράς μηνυμάτων (mail queues) .....	79
4.2.4 Ασφάλεια .....	82
4.2.5 Αποθήκευση ηλεκτρονικών μηνυμάτων .....	82
4.2.6 Συμπεράσματα .....	84
ΚΕΦΑΛΑΙΟ 5: Συνεργαζόμενα λογισμικά με την M.T.A. (Mail Transfer Agent) εφαρμογή Postfix.....	85

5.1	Σύντομη περιγραφή συνεργαζόμενων λογισμικών .....	86
5.1.1	SpamAssassin.....	86
5.1.2	ClamAV .....	86
5.1.3	Amavisd-New .....	87
5.1.4	Courier-IMAP.....	88
5.1.4.1	Διαδικασία ανάκτησης μηνυμάτων .....	89
5.1.5	Cyrus-SASL.....	89
5.2	Παρουσίαση συνεργασίας της εφαρμογής Postfix με τα λογισμικά Amavis, SpamAssassin και ClamAV .....	90
5.2.1	Διαδικασία παράδοσης εισερχόμενου μηνύματος .....	90
5.2.2	Διαδικασία αποστολής μηνύματος με χρήση M.U.A. εφαρμογής.....	91
5.2.3	Διαδικασία αποστολής μηνύματος με χρήση διαδικτυακής εφαρμογής διαχείρισης ηλεκτρονικής αλληλογραφίας (Web Mail Client) .....	92
ΚΕΦΑΛΑΙΟ 6: Πιστοποίηση ταυτότητας χρηστών - μέθοδοι και τεχνικές που χρησιμοποιούνται .....		94
6.1	Διαχείριση και αποθήκευση χρηστών.....	94
6.2	Περιγραφή υποστηριζόμενων βάσεων δεδομένων .....	94
6.2.1	CDB (Constant Database) .....	94
6.2.2	Berkley DB (DataBase).....	95
6.2.3	MySQL (My Structured Query Language).....	95
6.2.4	LDAP (Lightweight Directory Access Protocol) .....	96
6.3	Εργαστηριακή Υλοποίηση .....	96
6.4	Περιπτώσεις ταυτοποίησης χρηστών.....	97
6.4.1	Ταυτοποίηση χρήστη για αποστολή μηνυμάτων χρησιμοποιώντας M.U.A. εφαρμογή .....	98
6.4.2	Ταυτοποίηση χρήστη για ανάκτηση μηνυμάτων χρησιμοποιώντας M.U.A. εφαρμογή .....	99
6.4.3	Ταυτοποίηση χρήστη για αποστολή μηνυμάτων χρησιμοποιώντας τις διαδικτυακές εφαρμογές Horde ή RoundCube Mail.....	100

6.4.4	Ταυτοποίηση χρήστη για ανάκτηση μηνυμάτων χρησιμοποιώντας τις διαδικτυακές εφαρμογές Horde ή RoundCube Mail.....	101
ΚΕΦΑΛΑΙΟ 7: Πολιτικές ασφάλειας πληροφοριακών συστημάτων.....		102
7.1	Γενικά .....	102
7.2	Ανάλυση ζητημάτων ασφάλειας.....	104
7.2.1	Αυτόκλητη/ανεπιθύμητη αλληλογραφία (spam) σε συνδυασμό με τις ευπάθειες του SMTP πρωτοκόλλου.....	104
7.2.2	Η τεχνική email spoofing ως απόρροια των αδυναμιών του SMTP πρωτοκόλλου .....	104
7.2.2.1	Αναλυτική παρουσίαση τεχνικής email-spoofing .....	106
7.2.2.2	Ευπαθή συστήματα σε επιθέσεις με μεθόδους e-mail spoofing σε Α.Ε.Ι. της χώρας.....	109
7.2.2.3	Επίλυση της επίθεσης (χρησιμοποιώντας την τεχνική e-mail spoofing) στον Mail Server που υλοποιήσαμε .....	114
7.2.2.4	Πολιτικές ασφάλειας που ισχύουν στον Mail Server.....	118
7.2.3	Μέτρα και πολιτικές για την αντιμετώπισης των κακόβουλων λογισμικών (ιών) .....	119
7.2.4	Απομακρυσμένη πρόσβαση .....	120
7.2.5	Πολιτικές ασφάλειας για την εφαρμογή Postfix.....	122
7.2.6	Πολιτικές ασφάλειας MySQL Εξυπηρετητή στο πληροφοριακό σύστημα με domain name: isovitis.teipir.gr .....	123
ΚΕΦΑΛΑΙΟ 8: Ενδελεχής ανάλυση της M.T.A. (Mail Transfer Agent) εφαρμογής Postfix .....		125
8.1	Ανάλυση Postfix : Αλληλεπιδρούσες Διεργασίες .....	130
8.2	Ανάλυση Postfix : Ουρές μηνυμάτων (mail queues).....	139
8.3	Ανάλυση Postfix : Πίνακες αντιστοίχισης (table maps).....	145
8.4	Περιγραφή υπηρεσίας RBL (Real-time Block List) .....	147
8.5	Περιγραφή πινάκων αντιστοίχισης.....	148

ΚΕΦΑΛΑΙΟ 9: Δικτυακές πλατφόρμες διαχείρισης ηλεκτρονικής αλληλογραφίας Horde και Roundcube Mail .....	154
9.1 Δικτυακή πλατφόρμα Horde.....	154
9.1.1 Σύντομη περιγραφή λειτουργιών.....	155
9.2 Διαδικτυακή πλατφόρμα RoundCube Mail .....	161
ΚΕΦΑΛΑΙΟ 10: Μέθοδοι και τεχνικές διαχείρισης και εποπτείας του υλοποιηθέντος συστήματος Διακομιδής Ηλεκτρονικού Ταχυδρομείου.....	165
10.1 Διαχωρισμός αρχείων καταγραφής.....	166
10.2 Ανάλυση αρχείων καταγραφής .....	166
10.3 Δημιουργία και κοινοποίηση γραφημάτων παρουσίασης κίνησης των ηλεκτρονικών μηνυμάτων (e-mails) .....	169
10.4 Παρουσίαση AWStats.....	170
10.5 Διαδικτυακή πλατφόρμα Webmin .....	171
ΚΕΦΑΛΑΙΟ 11: Συντήρηση συστήματος .....	173
11.1 Εγκατάσταση UPS.....	173
11.1.1 Λογισμικό διαχείρισης και συνδεσμολογία .....	174
11.1.2 Δυνατότητες λογισμικού nut 2.2.2.....	175
11.2 Διαδικασία δημιουργίας αντιγράφων ασφαλείας (Backup) .....	176
11.2.1 Τύποι αντιγράφων ασφαλείας.....	176
11.2.2 Εγκατάσταση λογισμικού dar v2.3.8 .....	176
ΠΑΡΑΡΤΗΜΑ: Shell scripts.....	178
ΑΝΑΦΟΡΕΣ .....	180
ΒΙΒΛΙΟΓΡΑΦΙΑ .....	181
ΔΙΑΔΙΚΤΥΑΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ .....	181

## ΠΕΡΙΛΗΨΗ

Σκοπός του συγκεκριμένου κειμένου είναι μια αναλυτική και εμπειριστατωμένη αποτίμηση αναφορικά στην ασφάλεια ενός πληροφοριακού συστήματος Διακομιδής Ηλεκτρονικού Ταχυδρομείου. Στα πρώτα στάδια της ανάλυσης προσεγγίζονται τα ζητήματα που εξετάσαμε από τη θεωρητική τους σκοπιά. Πιο συγκεκριμένα, αναφέρονται τα πρωτόκολλα και οι συνηθέστερες περιπτώσεις χρήσεις που χρησιμοποιούνται σε συστήματα Ηλεκτρονικού Ταχυδρομείου. Ακολούθως αποτυπώνεται η μελέτη μας για την αποτίμηση ασφάλειας των συστημάτων Διακομιδής Ηλεκτρονικού Ταχυδρομείου η οποία διαχωρίζεται σε δύο τομείς. Ο πρώτος είναι ο οικονομοτεχνικός και ο δεύτερος ο τομέας από την οπτική του μηχανικού Η/Υ. Εν συνεχεία, και μετά από ενδελεχή σύγκριση των δύο από τις πολυχρησιμοποιούμενες M.T.A (*Mail Transfer Agent*) εφαρμογές, καταλήξαμε σε αυτή που πληρούσε τις ανάγκες μας για την υλοποίηση του πληροφοριακού συστήματος για το πρακτικό μέρος της εν λόγω Πτυχιακής Εργασίας. Κατόπιν, αναφέρονται τα συνεργαζόμενα λογισμικά με την M.T.A. εφαρμογή τα οποία και παρέχουν επιπρόσθετες υπηρεσίες προς τους χρήστες. Ακολούθως παρουσιάζονται οι πολιτικές ασφάλειας σε γενικό επίπεδο καθώς και του υλοποιηθέντος συστήματος. Σημαντικό τμήμα του κειμένου είναι η καταγραφή και η παρουσίαση των ευπαθειών που βρήκαμε στο σύστημα που υλοποιήσαμε. Στα ζητήματα ασφάλειας που καταγράψαμε παρέχουμε και την επίλυση αυτών με τον τρόπο που την πραγματοποιήσαμε. Στη συνέχεια, περιγράφονται δύο διαδικτυακές εφαρμογές διαχείρισης ηλεκτρονικής αλληλογραφίας που εγκαταστήσαμε όπως επίσης αναφέρονται και αναλύονται τα διάφορα λογισμικά διαχείρισης και συντήρησης που ενσωματώθηκαν στον Διακομιστή Ηλεκτρονικού Ταχυδρομείου.