Τίτλος Διατριβής: «Ασφάλεια Συστημάτων Ηλεκτρονικού Ταχυδρομείου»

ΖΑΛΜΑ ΚΩΝΣΤΑΝΤΙΝΑ ΜΠΠΛ/09066
Επιβλέπων: Παναγιώτης Κοτζανικολάου

Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών «Πληροφορική»

Δομή Πτυχιακής

- Βασικές Έννοιες Ηλεκτρονικού Ταχυδρομείου
- Πρωτόκολλα Ηλεκτρονικού Ταχυδρομείου
- Απειλές
- Μηχανισμοί Ασφάλειας
- Υλοποίηση Ασφάλειας

Βασικές Έννοιες Ηλεκτρονικού Ταχυδρομείου

- Πρωτόκολλα Ηλεκτρονικού Ταχυδρομείου
- Απειλές
- Μηχανισμοί Ασφάλειας
- Υλοποίηση Ασφάλειας

Ορισμός Ηλεκτρονικού Ταχυδρομείου

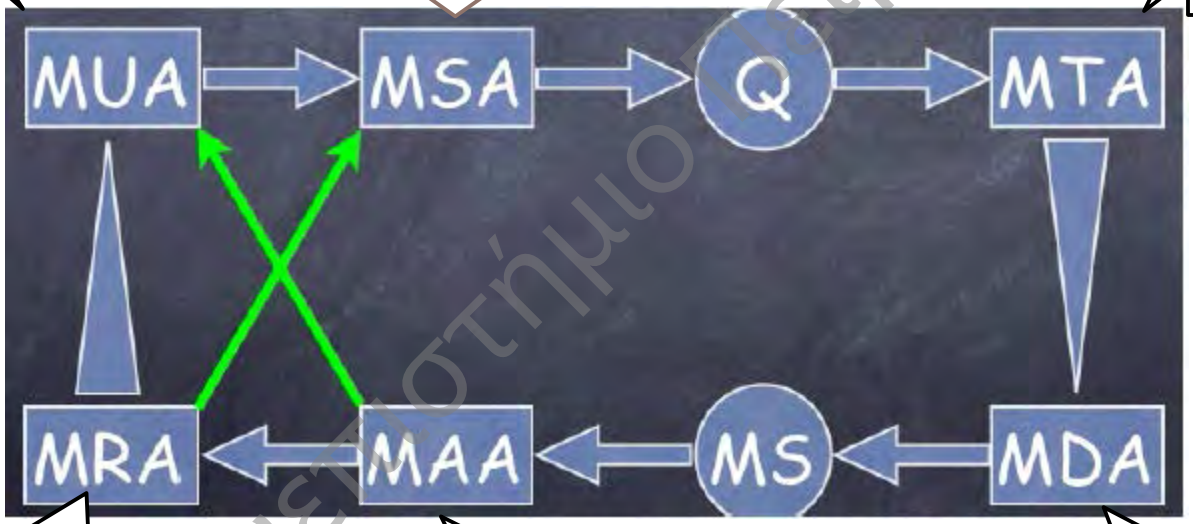
- Ηλεκτρονικό ταχυδρομείο ή ηλεκτρονική αλληλογραφία- **Electronic mail** ή αλλιώς **e-mail**
- Πανίσχυρος μηχανισμός του Διαδικτύου.
- Έρευνα **Pew Internet & American Life** ανέδειξε το e-mail ως την πιο δημοφιλής δραστηριότητα με ποσοστό 93%.
- **Ανταλλαγή ψηφιακών μηνυμάτων** ή και σύνθετης πληροφορίας (εικόνα ,βίντεο) από ένα αποστολέα σε ένα ή περισσότερους παραλήπτες με **ανέξοδο** , **ασφαλή** τρόπο και ενιαία μορφή.
- Βασίζεται στην τεχνική **store and forward** (αποθήκευση και προώθηση) που είναι βασικό χαρακτηριστικό των Δικτύων Μεταγωγής Μηνυμάτων (Message Switching).

Αρχιτεκτονική Ηλεκτρονικού Ταχυδρομείου

Mail User Agent(MUA)
αναγνώστης email, διαχειρίζεται το mailbox του χρήστη

Mail submission agent (MSA)
πράκτορας υποβολής ταχυδρομείου / πρόγραμμα που λαμβάνει μηνύματα από έναν MUA και συνεργάζεται με έναν MTA για την παράδοση mail.

Message Transfer Agent (MTA)
Λογισμικό μεταφοράς μηνυμάτων (πρότυπο πελάτη/διακομιστή)



Mail retrieval agent (MRA)
πράκτορας ανάκτησης μηνύματος / εφαρμογή που ανακτά μηνύματα από απομακρυσμένο mail server συνεργάζεται άμεσα με ένα MDA

Mail Access agent (MAA)
πράκτορας πρόσβασης μηνύματος / πρόγραμμα εξαγωγής (pull) μηνυμάτων

Mail delivery agent (MDA)
Λογισμικό για την παράδοση των μηνυμάτων στο mailbox του παραλήπτη. (π.χ. Procmail, MailDrop)

- Βασικές Έννοιες Ηλεκτρονικού Ταχυδρομείου
- **Πρωτόκολλα Ηλεκτρονικού Ταχυδρομείου**
- Απειλές
- Μηχανισμοί Ασφάλειας
- Υλοποίηση Ασφάλειας

Πρότυπα TCP/IP για Email

- Στόχος των πρωτοκόλλων του TCP/IP είναι να προσφέρει διαλειτουργικότητα σε όλο το εύρος υπολογιστικών συστημάτων και δικτύων. Το TCP/IP χωρίζει τα πρότυπα ταχυδρομείου σε δύο σύνολα:

1. Το ένα πρότυπο καθορίζει **τη μορφή** για τα μηνύματα αλληλογραφίας (πρότυπο RFC 822).
2. Και το άλλο **τις λεπτομέρειες για την ανταλλαγή** ηλεκτρονικής αλληλογραφίας μεταξύ δύο υπολογιστών.

1. Μορφή Email

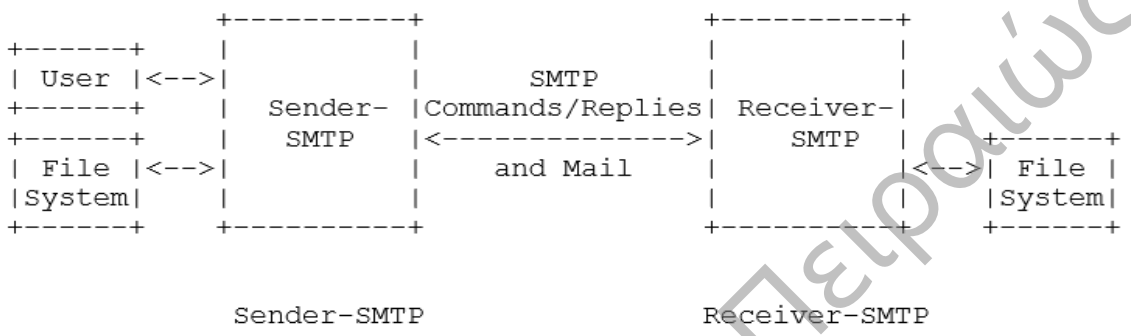
- Το πρότυπο TCP/IP καθορίζει τα μηνύματα ηλεκτρονικού ταχυδρομείου να αποτελείται από 3 συστατικά:
- **Το φάκελο του μηνύματος (envelope)**- που ενθυλακώνει το μήνυμα. Περιέχει πληροφορίες όπως τη διεύθυνση προορισμού, την προτεραιότητα, το επίπεδο ασφάλειας.
- **Την επικεφαλίδα του μηνύματος και (header)-** αποτελείται από μία σειρά από λέξεις κλειδιά (From, To, Cc, Subject κ.ο.κ)
- **Το σώμα του μηνύματος (body)-** το κείμενο του μηνύματος.

- Η **επικεφαλίδα** περιέχει πληροφορίες ελέγχου για τους πράκτορες χρήστη ενώ το **σώμα** του μηνύματος προορίζεται καθαρά για τον ανθρώπινο αποδέκτη.

Email Address/DNS/MX Records

- **Διεύθυνση ηλεκτρονικού ταχυδρομείου** (**Email address**) μοναδική, εντοπίζει τη θυρίδα του χρήστη, αποτελείται από 2 μέρη:
  1. Το μέρος πριν το σύμβολο **@** το **local-τοπικό μέρος**
  2. Το τμήμα μετά το σύμβολο @ το **όνομα τομέα-domain.**
- Η αντιστοίχιση ASCII χαρακτήρων σε διευθύνσεις δικτύου γίνεται με τη χρήση του **Συστήματος Ονομασίας Περιοχών DNS (Domain Name System). Ψευδώνυμα εξυπηρετητή ταχυδρομείου** είναι πληροφορία του DNS **(**hotmail.com το κανονικοποιημένο όνομα = relay1.west-coast.hotmail.com)
- Η εγγραφή πόρου είναι μια τετράδα, που περιέχει τα παρακάτω πεδία: **(Όνομα, Τιμή, Τύπος, TTL)**
  - **Αν τύπος = MX** , τότε η τιμή είναι το κανονικοποιημένο όνομα ενός εξυπηρετητή ταχυδρομείου που έχει ψευδώνυμο υπολογιστή υπηρεσίας πρόκειται για μια εγγραφή MX.

2. Ανταλλαγή Email



- **Simple Mail Transfer Protocol – SMTP**: απλό πρωτόκολλο μεταφοράς αλληλογραφίας. (TCP port 25)
- Βασική Ιδέα:
  - ο χρήστης κάνει ένα αίτημα για mail,
  - ο αποστολέας δημιουργεί ένα αμφίδρομο κανάλι μετάδοσης με το δέκτη (τελικός προορισμός-user account ή ενδιάμεσος - mail server).
  - Ο αποστολέας παράγει SMTP-εντολές που αποστέλλονται στον παραλήπτη.
  - Ο παραλήπτης απαντά.

Ανάκτηση Αλληλογραφίας

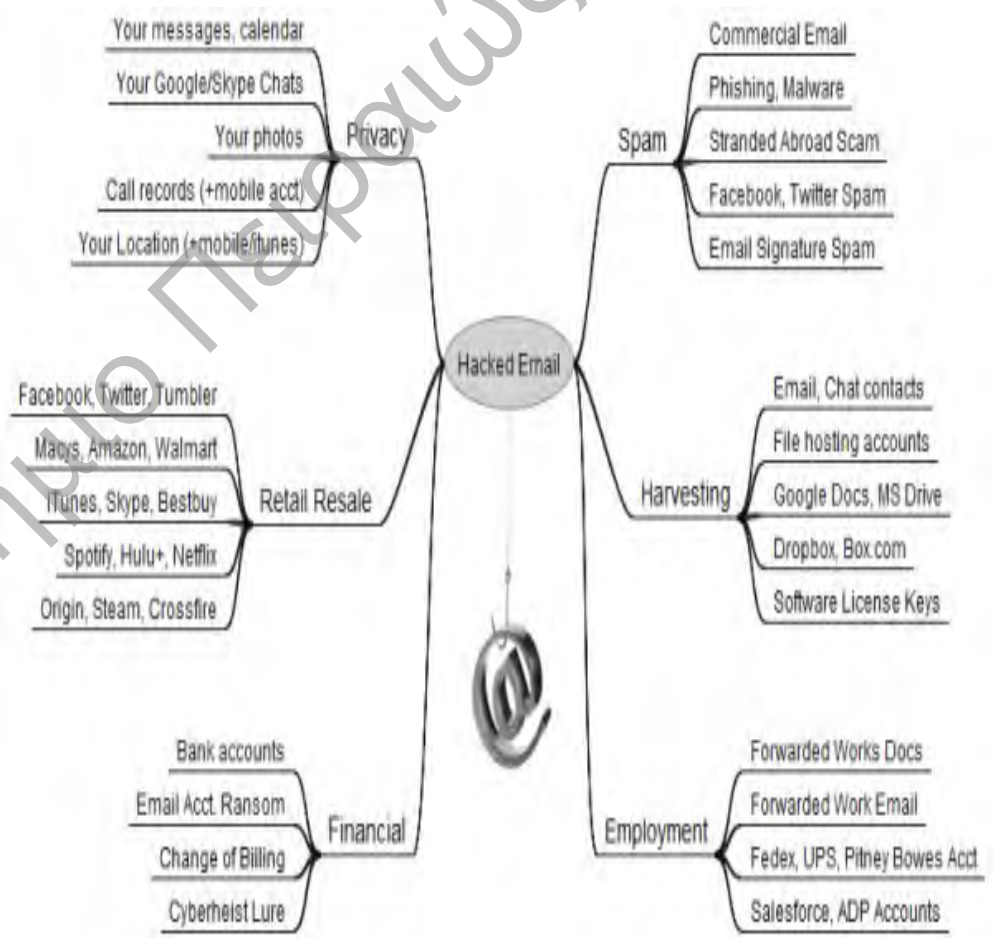
- **Έκδοση 3** του **Πρωτοκόλλου Ταχυδρομείου (Post Office Protocol, POP3)** TCP port 110 -επιτρέπει σε έναν χρήστη να εξάγει και να διαγράφει μηνύματα από το γραμματοκιβώτιο χωρίς να χρειάζεται να παραμένουν συνδεδεμένοι στο διαδίκτυο. (εξουσιοδότηση, συναλλαγή και ενημέρωση).
- **Internet Message Access Protocol** ή **IMAP -** TCP port 143, Διαδικτυακό πρωτόκολλο για ανάκτηση των e-mail, συνδυάζει δυνατότητες POP3 και SMTP (webmail), λειτουργεί και με σύνδεση και χωρίς, παραμένουν τα μηνύματα στον διακομιστή, λαμβάνει πληροφορίες μηνυμάτων,

- Βασικές Έννοιες Ηλεκτρονικού Ταχυδρομείου
- Πρωτόκολλα Ηλεκτρονικού Ταχυδρομείου
- **Απειλές**
- Μηχανισμοί Ασφάλειας
- Υλοποίηση Ασφάλειας

Email hacking

- Λόγω της απλότητας και των ισχυρών δυνατοτήτων του μηχανισμού της ηλεκτρονικής αλληλογραφίας αποτελεί ταυτόχρονα και μία από **τις πιο αποτελεσματικές μορφές επίθεσης.**
- **Email hacking** είναι παράνομη πρόσβαση σε λογαριασμό email ή αλληλογραφία.
- 3 γνωστές κατηγορίες επιθέσεων:

  Spam, Virus και Phishing



Spam- Ανεπιθύμητη Ηλεκτρονική Αλληλογραφία

- Μήνυμα ανεξαρτήτως περιεχομένου που αποστέλλεται από spammers σε πολλούς παραλήπτες χωρίς την συγκατάθεση τους.
- Χαρακτηριστικά spam: Απρόσκλητο, Εμπορικό, Μαζικό (90% επικράτηση)

  - Είδη Spam:
    - Adult
    - Health and Medicine
    - Personal finance
    - Fraud
    - Leisure
    - Political
    - Scams
    - Spiritual
    - Education
    - Προϊόντα υπολογιστών και Internet

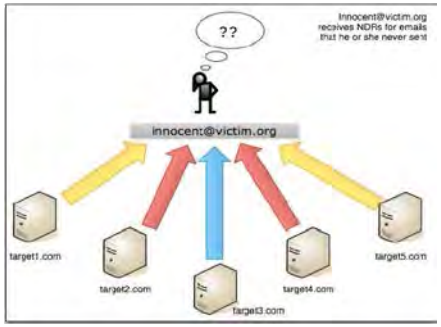
Τεχνικές Spam

I. **Email appending –** πρακτική σύνδεσης στοιχείων χρηστών με διευθύνσεις αλληλογραφίας

II. **Image spam-** μέθοδος παραπλάνησης με σκοπό την αποφυγή των spam φίλτρων

III. **Blank spam** – κενό μήνυμα (σκοπός μαζική επίθεση -**directory harvest attack**)

IV. **Backscatter spam -** «μεταμφίεση» ενός νόμιμου μηνύματος π.χ. μήνυμα αποτυχίας παράδοσης.



Phishing

- Προσπάθεια απόκτησης ευαίσθητων πληροφοριών όπως ονόματα χρηστών , κωδικούς πρόσβασης και στοιχεία πιστωτικών καρτών.
- **Τεχνικές Phishing:**

I. **Clone phishing -** μεταμφίεση νόμιμου email που περιέχει ένα συνημμένο ή ένα σύνδεσμο όπου περιέχει κακόβουλο λογισμικό.
II. **Link manipulation** -ανορθόγραφα URLs που οδηγούν σε μία σελίδα phishing.
III. **IDN spoofing** - οπτικά πανομοιότυπες διευθύνσεις ιστοσελίδων να οδηγήσουν σε διαφορετικές, ενδεχομένως κακόβουλες, ιστοσελίδες.
IV. **Filter evasion** - εικόνες αντί για κείμενο για να μην εντοπίζεται εύκολα από τα anti-phishing φίλτρα των emails.

Virus

- Λογισμικό μικρό σε χωρητικότητα, αποτελεσματικό σε δράση, μεταδίδεται μεταξύ υπολογιστών και δικτύων και να δημιουργηθεί αντίγραφα του εαυτού του χωρίς φυσικά να το γνωρίζει ή να το εγκρίνει ο τελικός χρήστης.
- Μορφές ιών:
  - **Ιός (virus) Κακόβουλο λογισμικό,**
  - **Ιοί των e-mail,**
  - **Σκουλήκι (Worm),**
  - **Δούρειοι Ίπποι (Trojan Horses),**
  - **Spyware – Adware,**
  - **Rootkits,**
  - **Bots – zombies.**

- Βασικές Έννοιες Ηλεκτρονικού Ταχυδρομείου
- Πρωτόκολλα Ηλεκτρονικού Ταχυδρομείου
- Απειλές
- **Μηχανισμοί Ασφάλειας**
- Υλοποίηση Ασφάλειας

Κρυπτογραφία

- Με μεγάλη διαφορά το μόνο αυτοματοποιημένο εργαλείο που μπορεί να παρέχει ασφάλεια στην ηλεκτρονική αλληλογραφία είναι η **κρυπτογράφηση**.
- **Στόχοι**:
  - Εμπιστευτικότητα ή μυστικότητα
  - Ακεραιότητα των δεδομένων
  - Πιστοποίηση ταυτότητας
  - Πιστοποίηση μηνύματος
  - Υπογραφή
  - Εξουσιοδότηση
  - Επικύρωση
  - Μη αποκύρηξη ευθύνης

Κρυπτογραφικά Συστήματα

- **Συμμετρική κρυπτογραφία:** χρησιμοποιείται ένα κλειδί για τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης.
- **Ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημοσίου κλειδιού:** χρησιμοποιούνται δυο διαφορετικά κλειδιά για τις διαδικασίες της κρυπτογράφησης (δημόσιο κλειδί) και αποκρυπτογράφησης (ιδιωτικό κλειδί).
- **Ψηφιακή Υπογραφή:** Πιστοποίηση του αποστολέα.
- **Σύνοψη μηνύματος (message digest):** αποτέλεσμα συνάρτησης κατακερματισμού (hash function) , μαθηματική συνάρτηση που υπολογίζεται στο αρχικό μήνυμα δίνοντας μία τιμή που στην αποκρυπτογράφηση εάν είναι ίδια πιστοποιεί την ακεραιότητα του μηνύματος.

PGP

- Εργαλείο κρυπτογραφίας είναι το σχήμα κρυπτογράφησης e-mail **Pretty Good Privacy (PGP)** που δημιουργήθηκε από τον Phil Zimmermann το 1991.
- Χρησιμοποιείται για την ασφάλεια, πιστοποίηση και αυθεντικότητα ενός μηνύματος από την πλευρά του χρήστη.
- Λογισμικό στον υπολογιστή που:
  - δημιουργεί ιδιωτικό κλειδί
  - δημοσιεύσει το δημόσιο κλειδί
  - Εισάγει δημόσια κλειδιά
  - Κρυπτογραφεί/ Αποκρυπτογραφεί
  - Δημιουργεί Ψηφιακά Πιστοποιητικά και Υπογραφές

SSL

- Επίπεδο Ασφαλούς Υποδοχής- **SSL (Secure Sockets Layer)** και το μεταγενέστερο **TLS (Transport Layer Security)**
- Ευρύτατα χρησιμοποιούμενες υπηρεσίες ασφάλειας.
- Πρωτόκολλα που εγγυώνται την ασφαλή επικοινωνία εξυπηρετητή - πελάτη μέσω Διαδικτύου χωρίς παρέμβαση τρίτων.
- Ενδιάμεσα πρωτόκολλα μεταξύ του επιπέδου εφαρμογών και του επιπέδου μεταφοράς.
- Χρησιμοποιεί το TCP/IP για να παρέχει αξιόπιστη υπηρεσία ασφάλειας από άκρο σε άκρο.
- **Λειτουργία**:
  - Φάση χειραψίας : διαπραγμάτευση αλγόριθμου κρυπτογράφησης (π.χ. DES ή IDEA) και κλειδιά - πιστοποίηση εξυπηρετητή στον πελάτη.
  - μετάδοση των δεδομένων της εφαρμογής, όλα τα δεδομένα κρυπτογραφούνται.

- Βασικές Έννοιες Ηλεκτρονικού Ταχυδρομείου
- Πρωτόκολλα Ηλεκτρονικού Ταχυδρομείου
- Απειλές
- Μηχανισμοί Ασφάλειας
- **Υλοποίηση Ασφάλειας**

Ασφάλεια από πλευράς Διακομιστή

Λογισμικό

- Διακομιστής Email: **hMailServer 5.4**
- Βάση Δεδομένων: **Microsoft SQL Compact**
- Προγράμματα Πελάτη: **Outlook 2007** και **Opera Mail**
- Σαρωτής Ιών: **Windows Defender**
- Εξωτερικό σύστημα ανίχνευσής spam: **SpamAssassin**
- Πρόγραμμα ασφαλούς επικοινωνίας εξυπηρετητή – πελάτη: **OpenSSL**

Κρυπτογράφηση Επικοινωνίας

- **SSL πιστοποιητικό** – για να κρυπτογραφήσετε τα email ανάμεσα στον διακομιστή και τους χρήστες.
  - **αγορά ενός πιστοποιητικού SSL**
  - **Δημιουργία αυτό-υπογεγραμμένου πιστοποιητικού.**
    - Δημιουργία ιδιωτικού κλειδιού, με OpenSSL.
    - Δημιουργία αιτήματος υπογραφής πιστοποιητικού, με OpenSSL.
    - Αφαίρεση κωδικού πρόσβασης από το ιδιωτικό.
    - Δημιουργία αυτό-υπογεγραμμένου πιστοποιητικού με OpenSSL.
    - Ενσωμάτωση στο Διακομιστή.

Τεχνικές ANTI-SPAM

- η προστασία απέναντι στα spam ενεργοποιείται σε τρεις άξονες: **σκορ**, **χρόνο** και **είδος** των μηνυμάτων.
- **Mark όριο** - αν ξεπεραστεί το θέμα τροποποιείται ως spam.
- **Όριο Διαγραφής**.- αν ξεπεραστεί, το μήνυμα διαγράφεται.
- **Μέγιστο όριο σάρωσης (σε KB)-** συνήθως τα spam είναι μικρά σε μέγεθος μηνύματα.
- **SPF** -Sender Policy Framework -Πλαίσιο Πολιτικής Αποστολέα. Έλεγχος IP αποστολέα ταιριάζει με IP εγγραφή DNS.
- **Έλεγχος ονόματος κεντρικού υπολογιστή στην εντολή HELO** - DNS lookup και να επιβεβαιωθεί ότι ο αποστολέας διακομιστής έχει δώσει το σωστό όνομα κεντρικού υπολογιστή.

- **Έλεγχος ότι αποστολέας έχει DNS MX εγγραφές .**
- **SpamAssassin** - δημοφιλές, εξωτερικό σύστημα, ανίχνευσής spam.
- **Tarpitting** –επιβράδυνση επικοινωνίας του hMailServer με τους spammers.
- **DNS blacklists.**
- **SURBL -** εντοπίζουν τα spam sites που περιέχονται στο σώμα ενός μηνύματος.
- **Grey listing** – προσωρινή απόρριψη μηνύματος αν είναι νόμιμος αποστολέας θα κάνει επανεκπομπή.
- **DKIM-επαλήθευση-** ψάχνει για μια DKIM-υπογραφή σε κάθε μήνυμα.

Τεχνικές ANTI-VIRUS

- **ClamWin -** ενσωματωμένη υποστήριξη απέναντι στην ανίχνευση ιών.
- **External virus scanner -** επιλογής εξωτερικού scanner.
- **Block attachments -** μπλοκάρονται συνημμένα αρχεία με βάση την επέκταση.
- **Μέγιστο όριο σάρωσης (σε KB)-** συνήθως τα μηνύματα που περιλαμβάνουν ιούς είναι μικρά σε μέγεθος μηνύματα.

Ασφάλεια από πλευράς Πελάτη

Εγκατάσταση Λογισμικού OpenPGP

- **Gpg4win** επιτρέπει στους χρήστες να μεταφέρουν με ασφάλεια μηνύματα και αρχεία με τη βοήθεια της κρυπτογράφησης και ψηφιακών υπογραφών.
- Προσφέρει ασφάλεια και ακεραιότητα περιεχομένου και ταυτοποίηση αποστολέα.

- Demo Εφαρμογής

Ευχαριστώ Πολύ