Μηχανή Αίνιγμα – η επιρροή της στις σύγχρονες επικοινωνίες στο Internet

Μαθητής: Ρούσσος Νικόλαος
Υπεύθυνος εκπαιδευτικός: Βακάλης Γεώργιος

Περιεχόμενα

Ιστορική εξέλιξη της κρυπτογράφησης

- Δίσκος της Φαιστού.
- Το τετράγωνο του Πολύβιου.
- Σπαρτιατική σκυτάλη.
- Κρυπτογραφικός δίσκος.

Μηχανή αίνιγμα
Ανάγκη κατασκευής της μηχανής Enigma

- Το μεγάλο πρόβλημα των εκάστοτε επικοινωνιών ήταν πως ο δέκτης δεν επέλεγε ποιος θα λάμβανε το μήνυμά του.
- Ή υπάρχουσα τεχνολογία καθιστούσε σχεδόν αδύνατη την ασφαλή επικοινωνία.
- Η μηχανή Αινίγμα, έκανε σχεδόν αδύνατη την αποκρυπτογράφηση των μηνυμάτων.

Λειτουργία της μηχανής Enigma

- Ο χρήστης πατούσε ένα από τα 26 πλήκτρα που αντιστοιχούσαν στα γράμματα του λατινικού αλφαβήτου από το πληκτρολόγιο της μηχανής.
- Ένα ηλεκτρικό σήμα ξεκινούσε από αυτό το πλήκτρο, περνούσε μέσα από τους 3 ρότορες και κατέληγε σε ένα λαμπτήρα, ο οποίος υποδείκνυε ένα "τυχαίο" γράμμα στον πίνακα λυχνιών, ακριβώς από πάνω από το πληκτρολόγιο.
- Το σήμα αυτό αναμεταδίδοταν μέσω ασυρμάτου σε κώδικα Mors, σε ένα κρυπτογραφημένο μήνυμα.
- Ο δεύτερος χρήστης της μηχανής θα σημείωνε κατά σειρά ποιο γράμμα άναβε στον πίνακα με τους λαμπτήρες, και θα έκανε αντίστροφη διαδικασία για να το αποδικοποιήσει.

Τροποποίηση Της Μηχανής Enigma από Τον Γερμανικό Στρατό

- Ο γερμανικός στρατός πρόσθεσε έναν πίνακα ηλεκτρικών υποδοχών.
- Αργότερα ένα σετ με 5 ρότορες από τους οποίους θα έπρεπε να μπουν οι 3 στην μηχανή, ή ακόμα σε κάποιες μηχανές μέχρι και 4 ρότορες την φορά.
- Σε συνδυασμό με τις ρυθμίσεις του πίνακα ηλεκτρικών υποδοχών οι συνολικοί συνδυασμοί έφταναν τους 158.962.555.217.826.360.000.

Ασφάλεια στο internet
Ασφαλή παρουσία στο διαδίκτυο

- Τα προσωπικά μας στοιχεία, δεν θα πρέπει να τα αποκαλύπτουμε σε άλλους χρήστες του Διαδικτύου.
- Θα πρέπει να είμαστε επιφυλακτικοί σε όσα διαβάζουμε στο Διαδίκτυο και σε αυτά που μας λένε οι άλλοι χρήστες του.
- Οι συναλλαγές μέσω του Διαδικτύου για την αγορά προϊόντων και θα πρέπει να γίνονται με μεγάλη προσοχή και μόνο από site που τα εμπιστευόμαστε.

Δωμάτια επικοινωνίας - chat

- Το chat στο Διαδίκτυο είναι ένας τρόπος άμεσης επικοινωνίας ενός συνόλου ανθρώπων, οι οποίοι βρίσκονται συγκεντρωμένοι σε έναν συγκεκριμένο δικτυακό χώρο.
- Ο καθένας, χρησιμοποιώντας απλά ένα ψευδώνυμο, μπορεί να παρακολουθεί ή να συμμετέχει σε συζητήσεις.
- Τα ψευδώνυμα βοηθούν στην απόκρυψη της ταυτότητας μας.
- Πολλές φορές όμως επειδή νιώθουμε ασφαλής τότε βρισκόμαστε και στον μεγαλύτερο κίνδυνο.

Κρυπτογράφηση δεδομένων στο internet

- Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτήν μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος.
- Η κρυπτογραφία αναφέρεται στην τροποποίηση των μηνυμάτων που στέλνουμε, ώστε να γίνονται κατανοητά μόνο στον παραλήπτη που επιλέγουμε εμείς.
- Είναι μια διαδικασία που μπορεί να εκτελεστεί τόσο με hardware όσο και σε software.

Αξιοπιστία στο Internet
Σκοπός της πηγής

- Τα χαρακτηριστικά μιας ηλεκτρονικής διεύθυνσης, δηλώνουν τις περισσότερες φορές, το σκοπό της πηγής:
  - Εκπαιδευτικός
  - Εμπορικός
  - Πληροφοριακός
  - Προσωπικός

Αξιοπιστία Υπευθυνότητας

- Η αναφορά του ονόματος.
- Ιδιότητα του συγγραφέα.
- Πόσο σχετικός είναι ο συγγραφέας με το θέμα.
- Εάν μπορούμε να επικοινωνήσουμε με το συγγραφέα
- Εάν η πηγή έχει δημιουργηθεί ή δημοσιευθεί από κάποιον έγκυρο οργανισμό.

Τεκμηρίωση πληροφοριών

- Κριτήρια που μπορούν να επιβεβαιώσουν την εγκυρότητα των πληροφοριών είναι οι βιβλιογραφικές αναφορές.
- Η βιβλιογραφία αποδεικνύει ότι ο συγγραφέας έχει συμβουλευτεί άλλες αξιόπιστες πηγές για να τεκμηριώσει τις πληροφορίες που παρουσιάζει.

Αντικειμενικότητα πληροφοριών

- Οι πληροφορίες και απόψεις που διατυπώνονται θα πρέπει να είναι αντικειμενικές και αμερόληπτες, να μην είναι επηρεασμένες από ιδεολογικά ή οικονομικά οφέλη.
- Η ταυτότητα του συγγραφέα ή του οργανισμού να μην προτείνει μια προκατάληψη.

Επικαιρότητα πληροφοριών

- Για την επικαιρότητα των πληροφοριών της πηγής θα πρέπει να ελέγχετε η ημερομηνία που δημιουργήθηκε η πληροφορία καθώς και το πότε ενημερώθηκε για τελευταία φορά η πηγή.
- Η επικαιρότητα των πληροφοριών είναι ιδιαίτερα σημαντική στις επιστήμες, δεδομένου ότι τα συμπεράσματα. μπορούν να αλλάξουν δραστικά σε μικρό χρονικό διάστημα.

Προσβασιμότητα της πηγής

- Η προσβασιμότητας της πηγής καθορίζεται από την εύκολη και γρήγορη πρόσβασής της.
- Η σελίδα θα πρέπει να εμφανίζεται εύκολα στην οθόνη και να μην υπάρχουν ανενεργοί σύνδεσμοι που δεν οδηγούν πουθενά.
- Καλό θα είναι να μην υπάρχουν διαφημίσεις, που παρεμβαίνουν και εμποδίζουν την εύκολη χρήση της πηγής.

Σαφήνεια περιεχομένου της πηγής

- Τα κριτήρια που καθορίζουν την σαφήνεια της πηγής είναι το καλό οργανωμένο κείμενο, οι σαφείς πληροφορίες που περιέχονται και η έλλειψη ορθογραφικών και συντακτικών λαθών.

Διαμοιρασμός αρχείων από το διαδίκτυο Ασφάλεια

- Είναι η δυνατότητα, που προσφέρει το Διαδίκτυο στους χρήστες του, να ανταλλάσουν αρχεία κάθε είδους.
- Μπορεί να πραγματοποιηθεί μέσω διαφόρων προγραμμάτων (που διατίθενται στο διαδίκτυο ελεύθερα ή με πληρωμή).
- Καθένα από τα προγράμματα αυτά λειτουργεί έτσι ώστε να κάνει κοινόχρηστο ένα μέρος του σκληρού δίσκου του τοπικού υπολογιστή του χρήστη, σε όλους χρήστες, οι οποίοι είναι συνδεδεμένοι στο Διαδίκτυο και χρησιμοποιούν το ίδιο πρόγραμμα.
- Με αυτό τον τρόπο κάθε μέλος αυτής της κοινότητας μπορεί να αναζητεί αρχεία στους υπολογιστές των μελών της και να δημιουργεί ένα αντίγραφο οποιουδήποτε από αυτά τα αρχεία, στον δικό του υπολογιστή.

Ασφάλεια

- Όταν χρησιμοποιούμε αυτά τα προγράμματα, μοιραζόμαστε αρχεία με χρήστες που δεν τους γνωρίζουμε και δεν θα πρέπει να τους εμπιστευόμαστε.
- Η ασφάλεια του υπολογιστή μας μπορεί να κινδυνεύει από ιούς και άλλα κακόβουλα προγράμματα που διαχέονται στον υπολογιστή μας και τον μολύνουν.

Πρόσβαση των παιδιών σε πορνογραφικό υλικό

- Οι ανήλικοι ενδέχεται να έχουν πρόσβαση μέσω των προγραμμάτων διαμοιρασμού αρχείων στο Διαδίκτυο, σε ακατάλληλα βίντεο ή εικόνες.
- Για παράδειγμα μπορεί να αναζητούν την αγαπημένη τους μουσική μπορεί αθέλητα να γίνουν παραλήπτες πορνογραφικού υλικού, απλά επειδή αυτό περιέχει τις ίδιες λέξεις-κλειδιά με τις οποίες γίνεται η αναζήτηση.
- Πολλά από τα προγράμματα ελέγχου της πλοήγησης, δεν είναι καθόλου αποτελεσματικά όταν η διακίνηση του ακατάλληλου υλικού γίνεται μέσα από προγράμματα διαμοιρασμού.

Νομικά προβλήματα

- Ο νόμος περί της πνευματικής ιδιοκτησίας, προστατεύει τους δημιουργούς των αντίστοιχων έργων πχ βίντεο, μουσική, τραγούδια, βιντεοπαιχνίδια και επιβάλει περιορισμούς στην αντιγραφή και την διακίνηση του προϊόντος.
- Υπάρχουν περιπτώσεις όπου τρίτα άτομα αποκτούν πρόσβαση σε αυτά τα αρχεία και τα οικειοποιούνται.
- Σε αυτή την περίπτωση τα άτομα αυτά μπορεί να εκμεταλλεύονται οικονομικά αυτά τα αρχεία, εκμεταλλευόμενοι την ανωνυμία τους.

Προσωπικά δεδομένα

- Από λάθος στις ρυθμίσεις του προγράμματος διαμοιρασμού αρχείων, μπορεί να γίνει κοινόχρηστος ολόκληρος ο σκληρός δίσκος του τοπικού υπολογιστή.
- Τότε προσωπικά δεδομένα, που πιθανόν έχετε στον υπολογιστή σας όπως αριθμοί πιστωτικών καρτών ή φορολογικά δεδομένα, θα εκτεθούν σε όλους τους χρήστες που χρησιμοποιούν το πρόγραμμα αυτό.

Τεχνικές επίθεσης
Phishing

- Η πρώτη περιγραφή της τεχνικής Phishing έγινε το 1987.
- Στην διαδικτυακή του μορφή πρωτοεμφανίστηκε το 1995 μέσω της υπηρεσίας e-mail, και στη συνέχεια με άμεσο μήνυμα.
- Άλλες τεχνικές Phishing χρησιμοποιούν αναδυόμενα παράθυρα, πολλαπλές καρτέλες ή ακόμα και τη δημιουργία ψεύτικων δημοσίων δικτύων σε αεροδρόμια, ξενοδοχεία και καφετέριες.

Πώς ξεκίνησε το Phishing: Μία 'κόλαση' για το AOL

- Οι phishers, δημιουργώντας ψεύτικους λογαριασμούς, επικοινωνούσαν με τους χρήστες της υπηρεσίας υποδυόμενοι υπαλλήλους της ίδιας της εταιρίας.
- Ο hacker στέλνει ένα e-mail ή άμεσο μήνυμα στο 'θύμα', στο οποίο συστήνεται ως αξιόπιστο πρόσωπο που ανήκει σε κάποια εταιρία ή οργανισμό, πολλές φορές και την ίδια την υπηρεσία του e-mail, και ζητά από το θύμα κάποια προσωπικά στοιχεία. Βασικό εργαλείο του phishing είναι οι αποπλανητικοί σύνδεσμοι.

Πού στηρίζεται η επιτυχία του Phishing

- Στηρίζεται σε τρεις βασικούς παράγοντες:

1. την έλλειψη γνώσεων του θύματος,
2. την έλλειψη προσοχής του θύματος,
3. την οπτική εξαπάτηση.

Επιθέσεις Drown

- Ερευνητές ανακάλυψαν πρόσφατα ένα νέο τρόπο ο οποίος απενεργοποιεί την προστασία κρυπτογράφησης των ιστοσελίδων.
- Οι επιθέσεις αυτές στοχοποιούν τους κωδικούς πρόσβασης, τους αριθμούς πιστωτικών καρτών, μηνύματα ηλεκτρονικού ταχυδρομείου καθώς και ευαίσθητα δεδομένα.
- Αν και έχει αναπτυχθεί ένα antivirus για την αποφυγή τέτοιου είδους επιθέσεων, η διαδικασία προστασίας των συστημάτων αναμένεται να είναι χρονοβόρα για τους διαχειριστές των ιστοσελίδων

Τέλος Εργασίας