Ηλεκτρονική Διακυβέρνηση

Παπανικολάου Γεώργιος

Εισαγωγή στην ασφάλεια

- Ασφάλεια Υπολογιστών

Ασφάλεια Υπολογιστών είναι η διαδικασία ανίχνευσης και παρεμπόδιση από ανεπιθύμητη χρήση του υπολογιστή μας.

Μέτρα ασφαλείας λαμβάνονται για να μην μπορούν εισβολείς να έχουν πρόσβαση σε οποιοδήποτε σημείο του υπολογιστή μας.

Αποτροπή πρόσβασης στον υπολογιστή από ανεπιθύμητους επισκέπτες (intruders).

Εισαγωγή στην ασφάλεια

- Ασφάλεια Πληροφοριακών Συστημάτων

Ο όρος «Ασφάλεια Πληροφορίας αναφέρεται στην προστασία της πληροφορίας και των πληροφοριακών συστημάτων από την μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διατάραξη διαφοροποίηση και καταστροφή τους.

Στόχος μας είναι οι εμπιστευτικότητα, διαθεσιμότητα, ακεραιότητα της πληροφορίας.

Internet – Που βρισκόμαστε σήμερα

- Σήμερα έχουμε γρήγορο και φθηνό Internet παντού.
- Συνδέονται εκατομμύρια υπολογιστές στο Internet.
- Δυνατότητα προστασίας συνολικά του δικτύου ανάγεται στην ικανότητα και επιθυμία του κάθε υπολογιστή να προστατευτεί.

Έννοιες

- Μέσο προστασίας (safeguard) = ενέργειες για περιοριστεί ο κίνδυνος.
- Μειώνουμε την πιθανότητα να πετύχουν οι απειλές.
- Ελάττωση επιπτώσεων prevent, detect, handle, recover, mitigate (reduce, diminish).
- Γενική αρχή είναι το κόστος προστασίας των προστατευόμενων αγαθών να είναι λιγότερο από ότι η αξία των αγαθών.

Ζημιές σε Αγαθά

- Ανεξέλεγκτη φυσική πρόσβαση σε υπολογιστές.
- Αστοχία υλικού.
- Ελλιπείς υλοποιήσεις πρωτοκόλλων επικοινωνίας.
- Σφάλματα λειτουργικού
- Απλούς κωδικούς(passwords), μη συχνή αλλαγή κωδικών (passwords)

Είδος επιθέσεων

- Viruses
- Worms
- Trojans
- Spyware
- Malware
- Denial of service (DoS) attacks

Βασικές κατηγορίες Επιθέσεων

- Χαρακτηριστικά Παθητικών επιθέσεων
  - Λήψη & πρόσβαση στην πληροφορία
  - Χωρίς άλλες εμφανείς συνέπειες
  - Δύσκολες στην ανίχνευση

- Χαρακτηριστικά ενεργητικών επιθέσεων
  - Αλλοίωση πληροφορίας
  - Μείωση απόδοσης πληροφοριακού συστήματος
  - Τρόπος ενεργοποίησης εξαρτάται από το δίκτυο
  - Αν και πιο δύσκολα ενεργοποιείται έχει ως αποτέλεσμα μεγαλύτερες ζημιές

Στόχοι

- Στόχος της ασφάλειας ενός υπολογιστικού συστήματος
  Διαφύλαξη υπολογιστικών πόρων από κακόβουλες ενέργειες.

- Προστασία των μεταδεδομένων.

- Προστασία κατά την διάρκεια μετάδοσης των δεδομένων.

- Τήρηση της εμπιστευτικότητας, ακεραιότητας, και διαθεσιμότητας της πληροφορίας (δεδομένα) σύμφωνα με το διεθνή πρότυπο ISO/IEC 17799:2000 (Code of practice for information security management).

Πιστοποίηση Χρηστών

- Ανάγκη επιβεβαίωσης ότι ο χρήστης που επικοινωνεί είναι πράγματι αυτός που ισχυρίζεται ότι είναι.

- Η πιστοποίηση της ταυτότητας του χρήστη γίνεται σε πραγματικό (real time) χρόνο.

- Ας υποθέσουμε ότι έχουμε δυο χρήστες Α, Β που επικοινωνούν μεταξύ τους και ο Α πρέπει να αποδείξει την ταυτότητα του στον χρήστη Β.

- Ο Α θα πρέπει να μπορεί να αποδείξει την ταυτότητα του ενώ ο Β δεν θα πρέπει να μπορεί να χρησιμοποιήσει την πληροφορία του Α για να υποκλέψει την ταυτότητα του.

- Η πιστοποίηση θα πρέπει να εξασφαλίζει ότι αν στην συνομιλία του Α με Β εισβάλει ένας τρίτος (C) τότε αυτός να μην μπορεί να προσποιηθεί τον Α.

Πιστοποίηση Χρηστών

- Ο Β περιμένει από τον Α συγκεκριμένο κωδικό για να πειστεί ότι είναι αυτός.

- Οι κωδικοί των χρηστών κρατούνται κρυπτογραφημένοι σε κάποιο αρχείο. Το αρχείο αυτό δεν μπορεί να διαβαστεί από μη εξουσιοδοτημένους χρήστες.

- Χαρακτηριστικά κωδικών : να έχουν μεγάλο μήκος ώστε να μην μπορούν να αποκαλυφθούν. Να εφαρμόζονται διάφορες τεχνικές ώστε να είναι ανθεκτικοί σε «επιθέσεις λεξικού».

Υποδομή Δημοσίου Κλειδιού

- Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure – PKI) αποτελεί ένα συνδυασμό λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών, ο οποίος πιστοποιεί την εγκυρότητα του κάθε φυσικού προσώπου που εμπλέκεται σε μια συναλλαγή στο Διαδίκτυο, και παράλληλα προστατεύει την ασφάλεια της συναλλαγής.

- Το PKI ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα. Μια τυπική υλοποίηση του PKI περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες, εξυπηρετητές (servers) και λογισμικό χρηστών. Παράλληλα προσφέρει σειρά εργαλείων για τη διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών.

Βασικές λειτουργίες/υπηρεσίες του PKI

- Εμπιστευτικότητα (Confidentiality)
- Ακεραιότητα (Integrity)
- Μη Άρνηση Αποδοχής (Non repudiation)
- Πιστοποίηση (Authentication)

Βασικές λειτουργίες/υπηρεσίες του PKI

- Εμπιστευτικότητα (Confidentiality) Πρόκειται για προστασία δεδομένων ενάντια σε μια μη εξουσιοδοτημένη πρόσβαση. Χρησιμοποιείται μηχανισμός έλεγχου κατά την διαδικασία αποθήκευσης δεδομένων και διαδικασία κωδικοποίησης κατά την αποστολή τους.

- Η υποδομή δημοσίου κλειδιού παρέχει διαδικασίες κωδικοποίησης αφού η μηχανισμοί ελέγχου πρόσβασης υλοποιούνται από το συνδυασμό μεθόδων πιστοποίησης (authentication) και εξουσιοδότησης (authorization).

Βασικές λειτουργίες/υπηρεσίες του PKI

- Ακεραιότητα (integrity) Είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση η αντικατάστασης τους. Γι το σκοπό αυτό χρησιμοποιούνται ψηφιακές υπογραφές.

- Μη άρνηση αποδοχής, συνδυάζει τις υπηρεσίες πιστοποίησης και της ακεραιότητας. Ένας χρήστης δεν μπορεί να αποποιηθεί ότι δημιούργησε και έστειλε ένα μήνυμα αφού θα συνοδεύεται από την ψηφιακή υπογραφή του. Με αυτόν τον τρόπο ο οποιοσδήποτε μπορεί να επιβεβαιώσει την ηλεκτρονική υπογραφή του αποστολέα.

Βασικές λειτουργίες/υπηρεσίες του PKI

- Πιστοποίηση (Authentication) Είναι η επιβεβαίωση της ταυτότητας ενός χρήστη η μιας πηγής αποστολής πληροφοριών (όπως πχ μιας ιστοσελίδας η μιας βάσεις δεδομένων).

- Παραδοσιακές μέθοδοι πιστοποίησης είναι οι παρακάτω:
  - Με την χρήση ενός κωδικού (π.χ. PIN, password,…)
  - Με την χρήση κάποιου αντικειμένου όπως πχ κάρτα ATM
  - Με δακτυλικά αποτυπώματα, φωνή.

- Το πιστοποιητικό (certificate) είναι ένας έγκυρος για την Υποδομή Δημοσίου Κλειδιού να μεταδώσει τιμές των δημοσίων κλειδιών η πληροφορίες που σχετίζονται με αυτά.

Βασικές λειτουργίες/υπηρεσίες του PKI

- Αρχή Πιστοποίησης : Οι Αρχές Πιστοποίησης διασφαλίζουν τη δημοσίευση των δημοσίων κλειδιών και συγκεντρώνουν τα δημόσια κλειδί των χρηστών.

- Ο χρήστης υποχρεούται να παραχωρήσει όλα τα απαραίτητα στοιχεία που πιστοποιούν την ταυτότητα τους.

- Αν ο χρήστης ενεργεί εκ μέρους κάποιας επιχείρησης τότε υποχρεούται να παραχωρήσει όλες τις νομικές πληροφορίες που πιστοποιούν την ταυτότητα και την ορθή λειτουργιά τους.

Βασικές λειτουργίες/υπηρεσίες του PKI

- Η αρχή πιστοποίησης έχει τις εξής αρμοδιότητες:

είναι

- Προσδιορίζει την αρχή πιστοποίησης που την εξέδωσε
- Περιέχει το όνομα και κάποιες άλλες πληροφορίες του εγγεγραμμένου.
- Κρατάει το δημόσιο κλειδί του εγγεγραμμένου, το οποίο ψηφιακά υπογεγραμμένο από την αρχή πιστοποίησης που το εξέδωσε.

Βασικές λειτουργίες/υπηρεσίες του PKI

- Υπάρχουν δυο είδη πιστοποιητικά:
  - Τα προσωπικά πιστοποιητικά, τα οποία αποτελούν ένα είδος εγγύησης ότι ο χρήστης είναι αυτός που δηλώνει ότι είναι. Σε αυτά καταχωρούνται προσωπικές πληροφορίες, όπως όνομα χρήστη και κωδικός πρόσβασης. Στη συνέχεια, οι πληροφορίες αυτές αποθηκεύονται σε ένα πιστοποιητικό, το οποίο χρησιμοποιείται όταν στέλνονται προσωπικές πληροφορίες σε ένα διακομιστή ελέγχου ταυτότητας που απαιτεί πιστοποιητικό. Επίσης, ένα προσωπικό πιστοποιητικό επιτρέπει στο χρήστη να λαμβάνει κρυπτογραφημένα μηνύματα από τους υπόλοιπους χρήστες.

Βασικές λειτουργίες/υπηρεσίες του PKI

- Υπάρχουν δυο είδη πιστοποιητικά:
  - Τα πιστοποιητικά δικτυακών τόπων, τα οποία περιέχουν πληροφορίες που πιστοποιούν ότι η συγκεκριμένη ιστοσελίδα είναι γνήσια και ασφαλής. Αυτό διασφαλίζει ότι κανένα άλλο site δεν μπορεί να παρουσιαστεί με την ταυτότητα της γνήσιας, ασφαλούς τοποθεσίας. Επίσης, τα πιστοποιητικά δικτυακών τόπων χρονολογούνται κατά την έκδοσή τους. Όταν προσπαθείτε να συνδεθείτε με το website ενός οργανισμού, το πρόγραμμα ανάγνωσης επαληθεύει τη διεύθυνση Internet που είναι αποθηκευμένη στο πιστοποιητικό και ελέγχει την ημερομηνία λήξης του. Εάν οι πληροφορίες αυτές δεν είναι έγκυρες ή εάν έχει παρέλθει η ημερομηνία λήξης, εμφανίζεται προειδοποιητικό μήνυμα (Warning).

Βασικές λειτουργίες/υπηρεσίες του PKI

- Τα πρωτόκολλα ασφαλείας που έχουν αναπτυχθεί για την εγκυρότητα, γνησιότητα ενός site είναι το SSL της Netscape και το SET της VISA και της MASTERCARD.

- Τα αρχικά SSL σημαίνουν Secure Sockets Layer και χρησιμοποιείται ευρέως σήμερα.

- Τα αρχικά SET σημαίνουν Secure Electronic Transactions.

Βασικές λειτουργίες/υπηρεσίες του PKI

- SSL : Αρκετές ιστοσελίδες είναι εξοπλισμένες με προγράμματα που χρησιμοποιούν το πρωτόκολλο αυτό προκειμένου να διασφαλιστούν από μη εξουσιοδοτημένους χρήστες κατά την αποστολή δεδομένων από και προς τις ιστοσελίδες αυτές.

- Τέτοια site θεωρούνται ασφαλή γι αυτό και η ονομασία.

Βασικές λειτουργίες/υπηρεσίες του PKI

- Ο τρόπος λειτουργίας μιας “ασφαλούς” σύνδεσης σε ιστοσελίδα έχει ως εξής:

  – Ο φυλλομετρητής συνδέεται με τον ασφαλή διαδικτυακό τόπο.

  – Ο διαδικτυακός τόπος δηλώνει την ταυτότητα του με τη χρήση των πιστοποιητικών που εκδίδονται από τις υπηρεσίες πιστοποίησης.

  – Ο φυλλομετρητής και η ασφαλής ιστοσελίδα συμφωνούν να χρησιμοποιήσουν συγκεκριμένο κλειδί και αλγόριθμο για την περαιτέρω επικοινωνία τους.

  – Τα δεδομένα που διακινούνται είναι κρυπτογραφημένα με το κλειδί/ αλγόριθμο που έχουν συμφωνηθεί.

Βασικές λειτουργίες/υπηρεσίες του PKI

- Η κρυπτογράφηση γίνεται χρησιμοποιώντας αλγόριθμο 40bit η 128bit.

- Για να αποκρυπτογραφήσει κάποιος το 40 bit αλγόριθμο πρέπει να δοκιμάσει 240 κλειδιά ενώ για το 128 bit αλγόριθμο πρέπει να δοκιμάσει 2128 κλειδιά.

- Για να αποκρυπτογραφήσει κάποιος το 40 bit αλγόριθμο χρειάζεται μερικές μέρες ενώ για το 128 bit αλγόριθμο είναι πρακτικά αδύνατο.

Δείτε για SSL Ψηφιακά Πιστοποιητικά στο ΣΥΖΕΥΞΙΣ

http://pki.syzefxis.gov.gr/page0005.htm

Πρωτόκολλο SSL/TLS

- Η υπηρεσία SSL (Secure Sockets Layer) η οποία πλέον ονομάζεται TLS (Transport Layer Security), είναι το πρωτόκολλο κρυπτογράφησης που παρέχει ασφάλεια για τις επικοινωνίες μέσω δικτύων όπως το Internet.

- Αυτό το πρωτόκολλο είναι απαραίτητο σε ιστοσελίδες οι οποίες ανταλλάσουν σημαντικές πληροφορίες όπως προσωπικά δεδομένα ή κωδικούς πιστωτικών καρτών.

Πρωτόκολλο SSL/TLS

- Τι προσφέρει και τι κερδίζω

  - Ασφάλεια, αξιοπιστία στις αγορές.
  - Ικανότητα αποδοχής πληρωμών πιστωτικών καρτών σε πραγματικό χρόνο.
  - Αποφυγή κλοπής κωδικών αφού προστατεύει την ιστοσελίδα μας.
  - Επίσης ιστοσελίδες που αποθηκεύουν και ανταλλάσουν ευαίσθητα, προσωπικά δεδομένα πρέπει να προστατεύονται από τον αλγόριθμο αυτό.

Τρόπος Λειτουργίας πρωτοκόλλου SSL/TLS

- Ο φυλλομετρητής (browser) συνδέεται με μια σελίδα υψηλής ασφάλειας και ο απομακρυσμένος server στέλνει πίσω ένα μήνυμα καλωσορίσματος.

- Για να ξεκινήσει μια σύνδεση ασφαλείας πρέπει ο browser να απαντήσει με ένα μήνυμα “client hello” και ο server να απαντήσει με ένα “server hello”.

- Στην αρχική φάση αυτή ο server και ο browser διαπραγματεύονται τις παραμέτρους ασφαλείας χρησιμοποιώντας το πρωτόκολλο “handshake” που είναι το πρώτο τμήμα του SSL.

- Το μήνυμα “client hello” περιέχει έναν αριθμό, που ονομάζεται session id και χαρακτηρίζει τον τύπο της σύνδεσης.

Τρόπος Λειτουργίας πρωτοκόλλου SSL/TLS

- Το μήνυμα “client hello” περιέχει πληροφορίες σχετικά με τους αλγόριθμους κρυπτογράφησης, την έκδοση του SSL και της μεθόδους συμπίεσης δεδομένων που υποστηρίζει ο browser.

- Το μήνυμα “server hello” απαντά με το τη μέθοδο συμπίεσης και τον αλγόριθμο κρυπτογράφησης που επέλεξε με βάση τις προτάσεις του browser (client) την έκδοση του SSL, ένα νέο τυχαίο αριθμό και μια αποδεκτή ταυτότητα σύνδεσης.

- Στη συνέχεια client και server ανταλλάσουν ψηφιακά πιστοποιητικά, που επιβεβαιώνουν ότι τα δυο μέρη είναι στην πραγματικότητα αυτά που ισχυρίζονται.

Τρόπος Λειτουργίας πρωτοκόλλου SSL/TLS

- Το πιστοποιητικό του server μπορεί να περιέχει και ένα δημόσιο κλειδί για τον αλγόριθμο κρυπτογράφησης ιδιωτικού- δημοσίου κλειδιού που έχει επιλεγεί κατά το handshake. Το κλειδί αυτό θα χρησιμοποιηθεί για μικρό χρονικό διάστημα.

- Η συναλλαγή αυτή καθεαυτή (πχ αποστολή αριθμού πιστωτικής κάρτας) θα κωδικοποιηθεί με χρήση ενός συμβατικού αλγορίθμου κρυπτογράφησης (με ιδιωτικό μόνο κλειδί).