ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΣΠΟΥΔΑΣΤΕΣ:
ΜΑΝΤΖΙΟΣ ΙΩΑΝΝΗΣ
ΜΠΑΝΤΙΑΣ ΣΠΥΡΙΔΩΝ

ΕΙΣΑΓΩΓΗ

Ορισμός Διαδικτύου: διασύνδεση όλων των επιμέρους δικτύων σε ένα ευρύτερο σύνολο, διευκολύνοντας και επιταχύνοντας την επικοινωνία.

Ασφάλεια

- Στο σημερινό κόσμο της διαδικτύωσης και του ηλεκτρονικού εμπορίου κάθε υπολογιστικό σύστημα είναι ένας πιθανός στόχος.
- Πολλοί διαφορετικοί τύποι ανθρώπων μπαίνουν σε υπολογιστικά συστήματα τρυπώντας την ασφάλειά τους.
- Ασφάλεια υπολογιστικού συστήματος έχουμε όταν μπορούμε να βασιστούμε σε αυτό και στο λογισμικό του να συμπεριφερθεί όπως περιμένουμε από αυτό.

Κρυπτογράφηση

Ορισμός:

Κρυπτογράφηση είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να διαβαστεί χωρίς την γνώση της σωστής ακολουθίας bit.

- Συμμετρική
- Ασύμμετρη

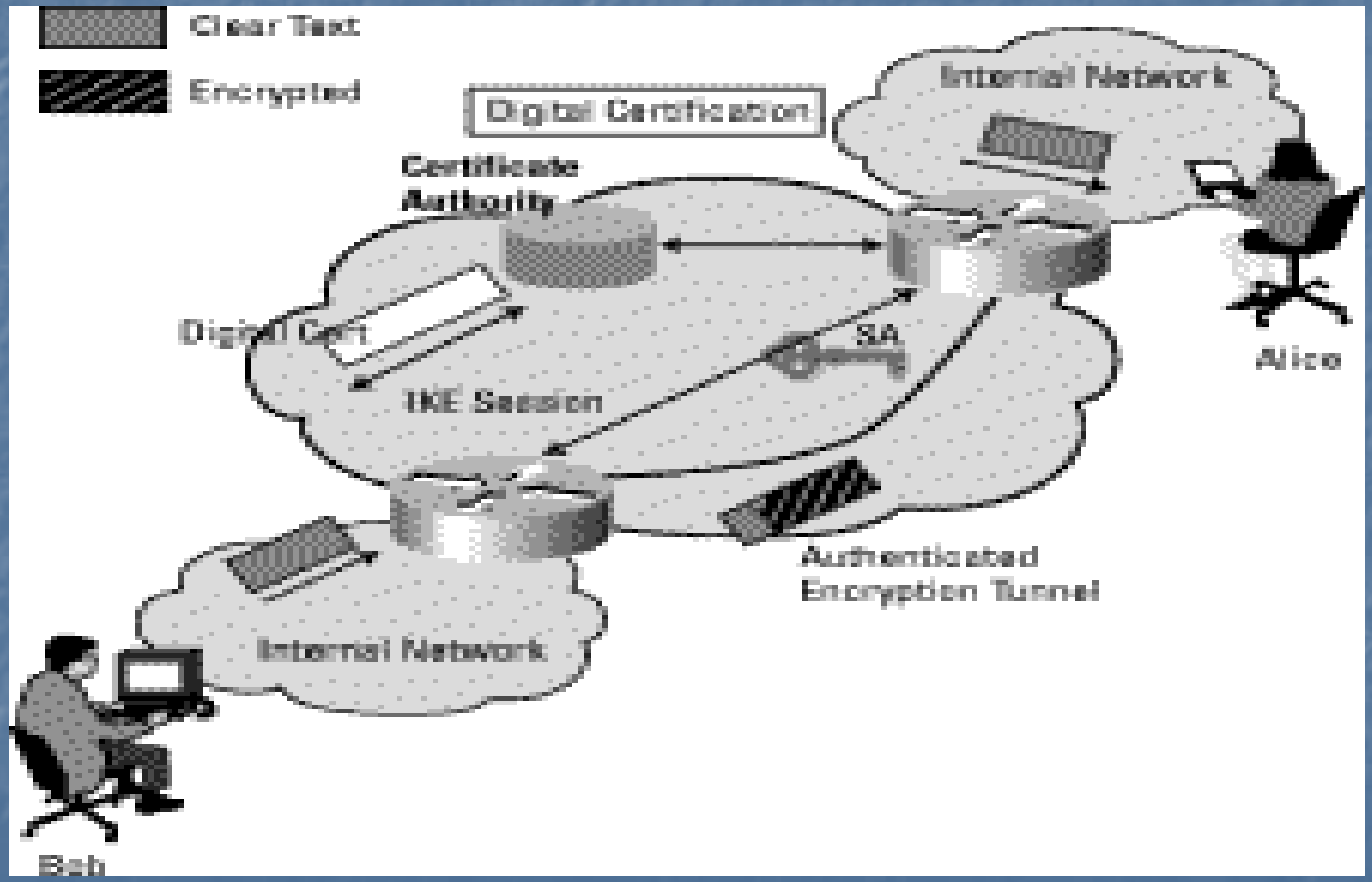
Το Μοντέλο

5.	*APPLICATIONS*
4.	*INTERNET SERVICES*
3.	*HIGHER INTERNET PROTOCOLS*
2.	*TCP/IP*
1.	*NETWOR K ACCESS*

IPSec (IP Security)

Η IPSec είναι ένα πρωτόκολλο ανοικτών προδιαγραφών για τη διασφάλιση του απορρήτου των επικοινωνιών.

παράδειγμα


Clear Text
Encrypted
Digital Certification
Certificate Authority
Internal Network
Alice
SA
IKE Session
Authenticated Encryption Tunnel
Internal Network
Bob

Secure Socket Layer (SSL)

Το πρωτόκολλο SSL έχει σχεδιαστεί για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν client και το άλλο σαν server.

Secure Socket Layer (SSL)

- **SSL Handshake Protocol**
- **SSL Record Protocol**

S/MIME (Secure MIME)

Το S/MIME είναι ένα πρωτόκολλο που χρησιμοποιείται από προγράμματα ηλεκτρονικού ταχυδρομείου για την εφαρμογή κρυπτογραφικών υπηρεσιών σε αποστέλλοντα μηνύματα και για την επεξεργασία προστατευμένων παραληφθέντων.

PGP (Pretty Good Privacy)

Το λογισμικό Pretty Good Privacy (PGP), το οποίο σχεδιάστηκε από τον Phill Zimmerman, είναι ένα λογισμικό κρυπτογράφησης υψηλής ασφάλειας για λειτουργικά συστήματα όπως τα MS DOS, Unix και για άλλες πλατφόρμες.

SSH (Secure Shell)

Το SSH είναι ένα πρωτόκολλο που παρέχει ασφαλή απομακρυσμένη σύνδεση σε υπολογιστές πάνω από μη ασφαλές δίκτυο.

Αποτελείται από τρία βασικά στοιχεία:

- Το Transport layer protocol
- Το User Authentication protocol
- Το Connection protocol

S/HTTP (Secure Hyper-Text Transfer Protocol)

Το πρωτόκολλο Secure HTTP παρέχει ασφαλής μηχανισμούς επικοινωνίας μεταξύ ένα ζευγάρι HTTP server – client

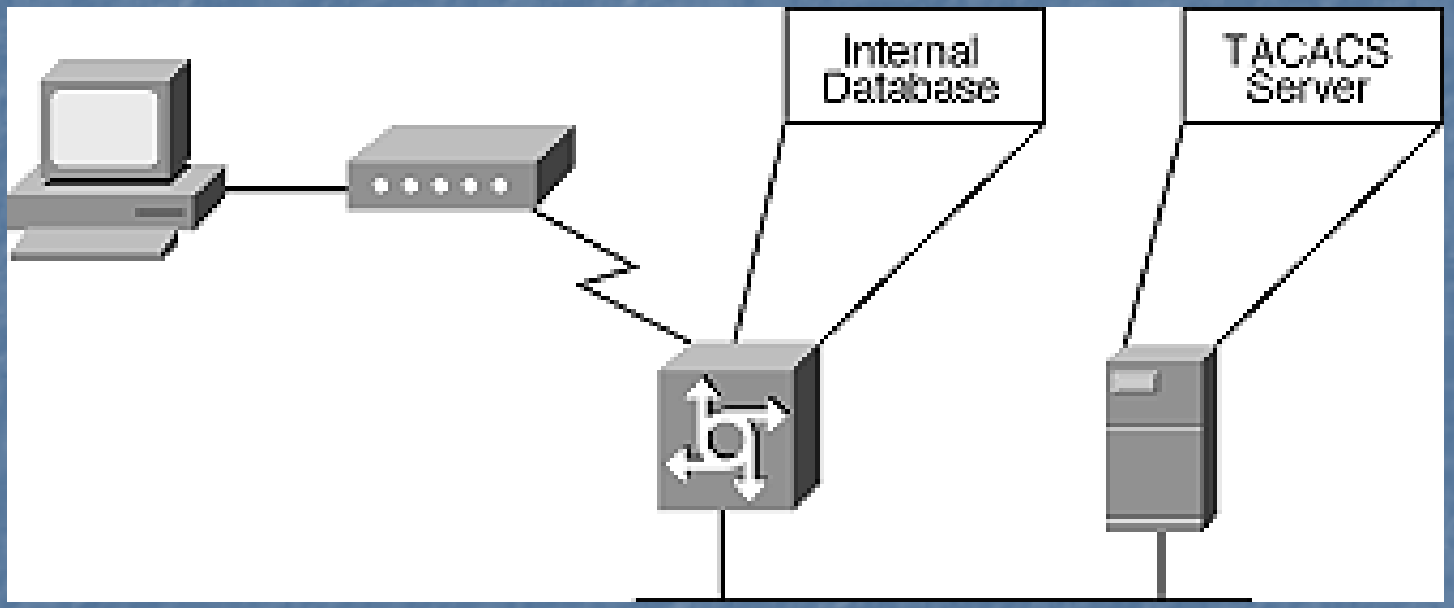
Είδη Προστασίας:

- Υπογραφές
- Κρυπτογράφηση
- Παραγωγή Message Authentication Codes (MACs)

Το Πρωτόκολλο RADIUS

Το πρωτόκολλο RADIUS αναπτύχθηκε από την Livingston Enterprises ως ένας server πρόσβασης, πιστοποίησης και παρακολούθησης.

Το πρωτόκολλο TACACS+



Σύγκριση RADIUS & TACACS+

- Μηχανισμός Μεταφοράς
- Εμπιστευτικότητα
- Διανομή Λειτουργιών
- Υποστήριξη Πολλαπλών Πρωτοκόλλων

Cisco NetSonar

Το Cisco NetSonar είναι ένα προϊόν Ανίχνευσης Αδυναμιών Ασφάλειας και Χαρτογράφησης Δικτύου.

Cisco NetRanger

Το σύστημα NetRanger είναι μια διαδικασία η οποία ανιχνεύει και αντιδρά σε κάθε παραβίαση ή κατάχρηση που γίνεται στην πολιτική ασφάλειας ενός δικτύου.

ΤΕΛΟΣ