

Ασφάλεια Δικτύων

Ασφάλεια δικτύων

- Στα χαμηλά επίπεδα: να φτάσουν τα πακέτα στον παραλήπτη χωρίς σφάλματα
- Σε ανώτερο επίπεδο: να προστατευθεί η διακινούμενη πληροφορία έτσι ώστε:
 - Να μην μπορεί να διαβαστεί από μη εξουσιοδοτημένα πρόσωπα ή συσκευές
 - Να μην μπορεί να τροποποιηθεί από μη εξουσιοδοτημένα άτομα
 - Να μην επιτρέπεται η πρόσβαση σε υπολογιστικούς και δικτυακούς πόρους από μη εξουσιοδοτημένα άτομα
 - Να ταυτοποιείται το πρόσωπο που στέλνει το μήνυμα
 - Να ταυτοποιείται ένα μήνυμα και ο αποστολέας του

Οι παραβιάσεις ασφάλειας γίνονται από άτομα που προσπαθούν ...

- Να προσποριστούν κέρδος
- Να προκαλέσουν την προσοχή
- Να εκδικηθούν ή να βλάψουν κάποιον
- Να διασκεδάσουν
- Να κερδίσουν στρατηγικό πλεονέκτημα
- Ένα μεγάλο ποσοστό προβλημάτων ασφαλείας προκαλούνται από εσωτερικούς χρήστες, υπαλλήλους, κ.λ.π.

Τέσσερις κύριες Έννοιες

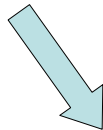
- **Εμπιστευτικότητα** (Confidentiality ή secrecy): η πληροφορία να πηγαίνει μόνο στα χέρια του ενδιαφερομένου
 - Ιδιωτικότητα (privacy)
 - Μυστικότητα (secrecy)
- **Ακεραιότητα** (Integrity): ότι το μήνυμα δεν έχει αλλοιωθεί. Προστασία από μετατροπή, διαγραφή ή/ και δημιουργία.
- **Αυθεντικοποίηση** (Authentication): Να ξέρεις σίγουρα ότι αυτός με τον οποίον μιλάς είναι αυτός που ισχυρίζεται. → επέκταση στα μηνύματα που ανταλλάσσεις μαζί του
- **Μη απάρνηση** (non-repudiation): η δυνατότητα να αποδείξουμε ότι κάποιος έλαβε ένα μήνυμα ή ότι πραγματικά έστειλε αυτός ένα μήνυμα και όχι κάποιος άλλος.

Διαθεσιμότητα

- **Διαθεσιμότητα** (availability): κρίσιμη έννοια που δεν συνδέεται όμως στενά με την έννοια της ασφάλειας. Με αυτήν ασχολείται ο κλάδος που ονομάζεται **fault tolerant computing**. Οι ενέργειες κατά της διαθεσιμότητας εντάσσουν τους κακόβουλους χρήστες στην κατηγορία των επιτιθέμενων στην ασφάλεια του συστήματος επειδή παρακωλύουν την απρόσκοπτη πρόσβαση των νομίμων χρηστών στο σύστημα.

Συνεπαγόμενες έννοιες

Αυθεντικοποίηση + μη-απάρνηση



Απόδοση ευθυνών (accountability) + **χρέωση** (billing)

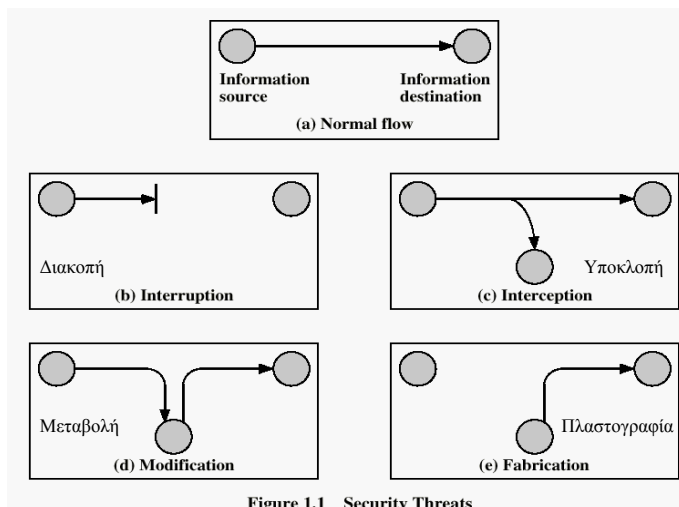
Άλλες έννοιες

- Έκθεση σε κίνδυνο (exposure): μια μορφή πιθανής απώλειας (loss) ή ζημιάς (harm).
- Ευπάθεια (vulnerability): αδυναμία ή ευάλωτο σημείο
- Επίθεση (attack)
- Απειλή (threat): καταστάσεις όπου υπάρχει το ενδεχόμενο απωλειών ή ζημιών. Ανθρώπινες, φυσικές καταστροφές, ακούσια λάθη, ατέλειες
- Έλεγχος (control): προστατευτικό μέσο: πράξη, συσκευή, διαδικασία, τεχνική που μειώνει την ευπάθεια

Ευπάθειες

- Φυσικές (αφορούν το χώρο εγκατάστασης)
- Εκ φύσεως (πλημμύρες, πυρκαγιές, ...)
- Υλικού και λογισμικού
- Μέσων (π.χ. μαγνητικά μέσα)
- Εκπομπών
- Επικοινωνιών
- Ανθρώπινες

Είδη απειλών



Μέτρα Προστασίας Πληροφοριακών Συστημάτων

- Φυσική ασφάλεια
- Ασφάλεια υπολογιστικού συστήματος (computer security): ποιος δικαιούται προσπέλαση
- Ασφάλεια βάσεων δεδομένων
- Ασφάλεια Δικτύων

Τρόποι άμυνας

- Έλεγχος προσπέλασης στο σύστημα
- Έλεγχος προσπέλασης στα δεδομένα
- Διαχείριση συστήματος και ασφάλειας
- Σχεδιασμός συστήματος (αξιοποίηση δυνατοτήτων ασφάλειας)

Τύποι μέτρων προστασίας

- Κρυπτογράφηση: Η κύρια μέθοδος προστασίας των δεδομένων κατά τη μετάδοσή τους
- Μέτρα λογισμικού:
 - χρήση προτύπων, λειτουργικό σύστημα, μέτρα στα προγράμματα (π.χ. passwd στις ΒΔ)
- Μέτρα υλικού
 - συσκευές κρυπτογράφησης ή βιομετρικής αναγνώρισης χρηστών (ίριδα, δακτυλικά απ., hasp, κάρτες πρόσβασης κ.α.)
- Φυσικά μέτρα υλικού
 - κλειδαριές, back up, UPS, κλιματισμός, ...
- Πολιτικές ασφάλειας.
 - Συχνή αλλαγή συνθηματικών
 - Απαραίτητες σε μεγάλους οργανισμούς

Προβλήματα κατά ή για την εισαγωγή ασφάλειας

- Δεν σχεδιάζεται / περιλαμβάνεται από την αρχή αλλά προστίθεται μετά
- Κοστίζει, συνήθως, αρκετά.
- Μεγάλη πολυπλοκότητα (κυρίως στα λογισμικά)
- Το κύριο πρόβλημα ασφάλειας είναι οι χρήστες

Παθητικές επιθέσεις

- Παρακολούθηση επικοινωνιών
- Για την απόκτηση πληροφορίας
- Ανίχνευση περιεχομένου μηνυμάτων
- Ανάλυση κίνησης
 - Υπάρχει δυνατότητα εύρεσης του τύπου της επικοινωνίας από τη συχνότητα και το μέγεθος των μηνυμάτων.
- Δύσκολη ανίχνευση
- Μπορεί να αποφευχθεί

Ενεργητικές επιθέσεις

- Μασκάρωμα
 - Ο επιτιθέμενος προσποιείται ότι είναι διαφορετική οντότητα
- Επανάληψη (Replay)
- Παραποίηση μηνυμάτων
- Άρνηση υπηρεσίας (Denial of service)
- Εύκολη ανίχνευση
 - Η ανίχνευση μπορεί να οδηγήσει σε τιμωρία
- Δύσκολη αντιμετώπιση

Ασφάλεια και Δίκτυα

Ασφάλεια και Δίκτυα

- Σε ποιο σημείο της στοίβας πρωτοκόλλων ανήκει η ασφάλεια; Απάντηση: Σε όλα!
 - Φυσικό: κλείδωμα κατανομών, σωλήνες αερίου,...
 - Ζεύξης: κρυπτογράφηση: εφαρμόζεται εύκολα
 - Πρόβλημα κατά τη διέλευση από δρομολογητές
 - Δικτύου: έλεγχος πρόσβασης με firewalls
 - Μεταφοράς: κρυπτογράφηση από άκρο σε άκρο
 - Εφαρμογής: ο κύριος χώρος εφαρμογής της αυθεντικοποίησης και της μη-απάρνησης
- Η κύρια μέθοδος για τη βελτίωση της ασφάλειας στα δίκτυα: **ΚΡΥΠΤΟΓΡΑΦΗΣΗ**

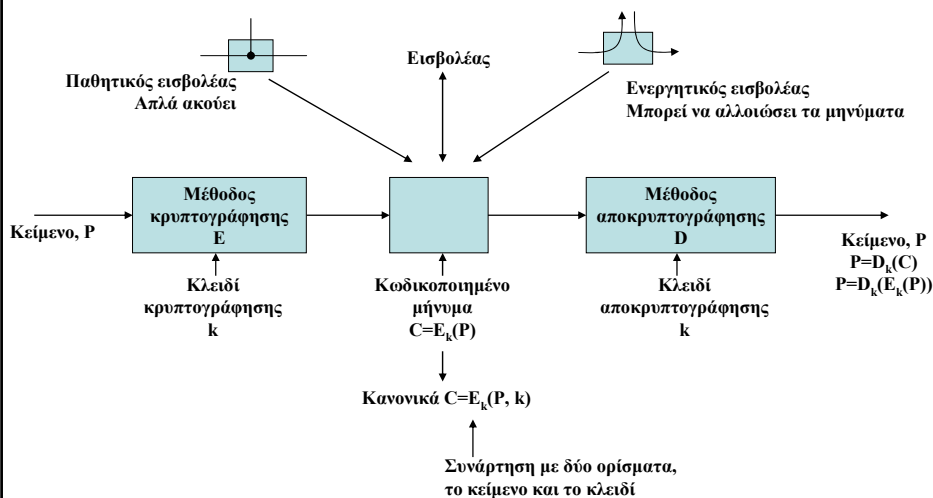
Κρυπτολογία (cryptology)

- Κρυπτογραφία (cryptography) : η τέχνη να κατασκευάζεις κώδικες
- Κρυπτανάλυση (cryptanalysis): η τέχνη να σπας κώδικες
- Κρυπτογραφικοί κώδικες (ciphers): byte προς byte ή bit προς bit μετασχηματισμός ενός μηνύματος ανεξάρτητα από το νόημά του.
- Κώδικες (codes): αντικατάσταση μιας λέξης με κάποια άλλη ή με κάποιο σύμβολο
 - δεν βρίσκονται πλέον σε χρήση
 - WWII: Navajo
- Παραδοσιακοί χρήστες της κρυπτογραφίας
 - Οι στρατιωτικοί
 - Οι διπλωμάτες
 - Οι συγγραφείς ημερολογίων, και
 - Οι εραστές

Απαιτήσεις κωδίκων

- Να εφαρμόζονται εύκολα
- Να αλλάζουν εύκολα
- Να είναι απόρρητοι από τους μη-γνώστες
- Να είναι εύκολα αναγνωρίσιμοι από τους χρήστες

Μοντέλο κρυπτογράφησης



Η αρχή του Kerckhoff

- Φλαμανδός κρυπτογράφος Auguste Kerckhoff (1883)
- «Όλοι οι αλγόριθμοι πρέπει να είναι δημόσιοι· μόνο τα κλειδιά πρέπει να μένουν μυστικά.»
- Η προσπάθεια να κρατήσω μυστικό τον κώδικα είναι μάταιη.
- Επίσης, η κοινοποίηση του κώδικα βοηθά στον έλεγχο της ικανότητάς του από πολλούς ειδικούς.
- Τα κλειδιά πρέπει να αλλάζουν συχνά και να είναι τέτοια ώστε η εύρεσή τους να αποτελεί τη μεγάλη δυσκολία του κώδικα.

Κώδικες αντικατάστασης

- Κάθε γράμμα ή ομάδα γραμμάτων αντικαθίσταται από ένα άλλο γράμμα ή ομάδα γραμμάτων για να τα κρύψουμε
- Ο κώδικας του Καίσαρα
 - Αποδίδεται στον Ιούλιο Καίσαρα
 - Το αλφάβητο μετατοπίζεται κατά k χαρακτήρες. Το k είναι το κλειδί του κώδικα.

Βελτίωση του κώδικα του Καίσαρα

- Μονοαλφαβητική αντικατάσταση (monoalphabetic substitution).

Plaintext: α β γ δ ε ζ η θ ι κ λ μ ν ξ ο π ρ σ τ υ φ χ ψ ω

Cyphertext: Ε Ρ Τ Υ Θ Ι Ο Π Α Σ Δ Φ Γ Η Ξ Κ Λ Ζ Χ Ψ Ω Β Ν Μ

$24!$ Συνδυασμοί = 6×10^{23} πιθανά κλειδιά.

- Με διάρκεια δοκιμής 1nsec χρειάζονται 10^8 έτη για να δοκιμαστούν όλα τα πιθανά κλειδιά.

Το εύκολο σπάσιμο ενός κώδικα

- Στατιστικές ιδιότητες των φυσικών γλωσσών
- Συχνότητα εμφάνισης γραμμάτων: e, t, o, a, n, i, ...
- Διγράμματα (digrams): th, in, er, re, an, ...
- Τριγράμματα (trigrams): the, ing, and, ion, ...
- Τακτική σπασίματος κώδικα:
 - Βρίσκω τη συχνότητα εμφάνισης των κωδικών γραμμάτων, διγράμμάτων, τριγραμμάτων, κ.α.
 - Τα πιο συχνά κωδικά γράμματα αντιστοιχούν μάλλον στο e και το t.
 - Το πιο συχνό τρίγραμμα είναι μάλλον το tXe, οπότε βρίσκουμε την κωδικοποίηση του h(X).
 - Αν πάλι συναντήσουμε συχνά μια λέξη thYt τότε το Y=a.
- Μια άλλη τακτική είναι να εντοπιστεί μια πολύ πιθανή λέξη ή φράση

Κώδικες αντιμετάθεσης (transposition ciphers)

- Οι κώδικες αντικατάστασης διατηρούν τη θέση των γραμμάτων αλλά τα αλλοιώνουν (μασκαρεύουν).
- Οι κώδικες αντιμετάθεσης δεν αλλοιώνουν τα γράμματα αλλά αλλάζουν τη θέση τους.
- Το κλειδί πρέπει να είναι μια λέξη στην οποία κάθε γράμμα υπάρχει μια μόνο φορά.

Ένας κώδικας αντιμετάθεσης

M E G A B U C K
7 4 5 1 2 8 3 6
p l e a s e t r
a n s f e r o n
e m i l l i o n
d o l l a r s t
o m y s w i s s
b a n k a c c o
u n t s i x t w
o t w o a b c d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUEIRICXB

Σπάσιμο κώδικα αντιμετάθεσης

- Καταρχήν πρέπει να ξέρω ότι πρόκειται για κώδικα αντιμετάθεσης.
- Μπορώ να ελέγξω τη συχνότητα εμφάνισης των γραμμάτων που θα ταίριαζε με εκείνη ενός απλού κειμένου.
 - Πρέπει να μαντέψω τον αριθμό των στηλών
 - Βοηθάει αν έχω κάποια εικόνα ή γνώση μιας λέξης μέσα στο κείμενο, π.χ. milliondollars.
 - Βρίσκω διγράμματα και ψάχνω την αλληλουχία. Αν βρω το κλειδί, π.χ. 8, μένει να βρω τη σωστή διάταξη των στηλών.
 - Μπορεί κανείς να δοκιμάσει $k(k-1)$ συνδυασμούς μέχρι να βρει κάποιον του οποίου οι συχνότητες εμφάνισης διγραμμάτων και τριγραμμάτων να ταιριάζουν με εκείνες μιας φυσικής γλώσσας.

One-time pads

«ένας άσπαστος κώδικας»

- Επέλεξε ως κλειδί μια τυχαία ακολουθία από bits με μήκος ίσο με το μήνυμα.
- Μετέτρεψε το μήνυμα σε ακολουθία από bits και εκτέλεσε XOR με το κλειδί.
- Το αποτέλεσμα δεν μπορεί να αποκρυπτογραφηθεί από κανέναν χωρίς το κλειδί.
- Ο λόγος προκύπτει άμεσα από τη θεωρία της πληροφορίας.
 - Επειδή το κλειδί είναι τυχαίο, οποιοδήποτε απλό κείμενο με το ίδιο μήκος είναι το ίδιο πιθανό να είναι το αρχικό. Με άλλα λόγια, σε ένα αρκετά μεγάλο κρυπτογραφημένο κείμενο η πιθανότητα εμφάνισης όλων των γραμμάτων, διγραμμάτων, τριγραμμάτων, κλπ, θα είναι εξίσου πιθανή, δίνοντας μηδενική πληροφορία για το σπάσιμο του κώδικα.

One-time pad

Message 1: 1001001 0100000 1101100 1101111 1110110 1100101 0100000 1111001 1101111 1110101 0101110
Pad 1: 1010010 1001011 1110010 1010101 1010010 1100011 0001011 0101010 1010111 1100110 0101011
Ciphertext: 0011011 1101011 0011110 0111010 0100100 0000110 0101011 1010011 0111000 0010011 0000101

Pad 2: 1011110 0000111 1101000 1010011 1010111 0100110 1000111 0111010 1001110 1110110 1110110
Plaintext 2: 1000101 1101100 1110110 1101001 1110011 0100000 1101100 1101001 1110110 1100101 1110011

Μειονεκτήματα

- Το κλειδί δεν μπορεί να απομνημονευθεί
- Το μήκος του κειμένου που μπορεί να κρυπτογραφηθεί εξαρτάται από το μήκος του κλειδιού.
- Είναι μέθοδος ευαίσθητη στην απώλεια ή εισαγωγή δεδομένων
- Αν ο αποστολέας και ο δέκτης χάσουν το συγχρονισμό τους τα δεδομένα θα γίνουν ακατάληπτα.

Κβαντική κρυπτογραφία

- Το πρωτόκολλο BB84 (Bennet and Brassard 1984)
- Η Alice και ο Bob ονομάζονται principals
- Trudy: intruder
- Φωτόνια $\rightarrow$ πόλωση
 - rectilinear basis
 - diagonal basis
- qubits $\rightarrow$ bits που αποστέλλονται με φωτόνια
- Αρχή της απροσδιοριστίας –Werner Heisenberg 1927
 - Pockels cell – polarizer
 - κρύσταλλος CaCO_3
- privacy amplification

Κβαντική κρυπτογραφία

Bit number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Data	1	0	0	1	1	1	0	0	1	0	1	0	0	1	1	0	What Alice sends
(a)																	
(b)																	Bob's bases
(c)																	What Bob gets
(d)	No	Yes	No	Yes	No	No	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No	Correct basis?
(e)		0		1				0	1		1	0	0		1		One-time pad
(f)																	Trudy's bases
(g)	x	0	x	1	x	x	x	?	1	x	?	?	0	x	?	x	Trudy's pad

Βασικές αρχές κρυπτογραφίας

- Πλεονασμός (redundancy)
 - Χρειάζεται και για την κρυπτογράφηση αλλά και για τη διόρθωση σφαλμάτων
- Φρεσκάδα (freshness)
 - Πρέπει να υπάρχει μια μέθοδος που να εντοπίζει τις επανεκπομπές παλαιότερων μηνυμάτων που έχουν σα σκοπό τους να προκαλέσουν σύγχυση στο δέκτη.