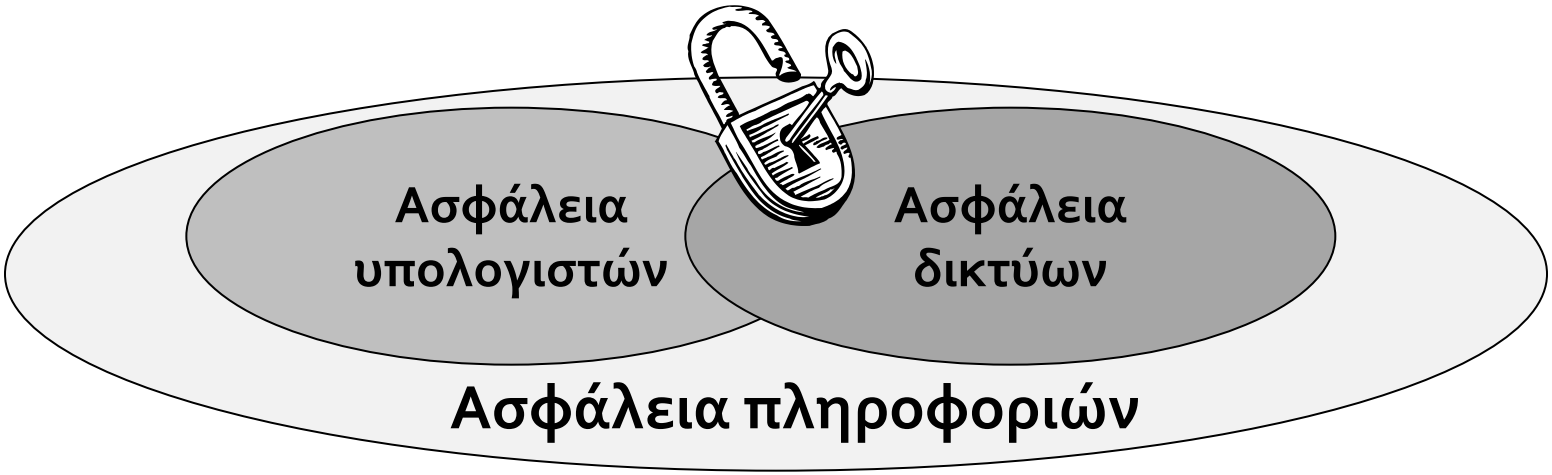
Πανεπιστήμιο Πελοποννήσου
Τμήμα Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών

Διαχείριση και Ασφάλεια Δικτύων

Εισαγωγή στην Ασφάλεια Δικτύων

Κάποιες έννοιες…



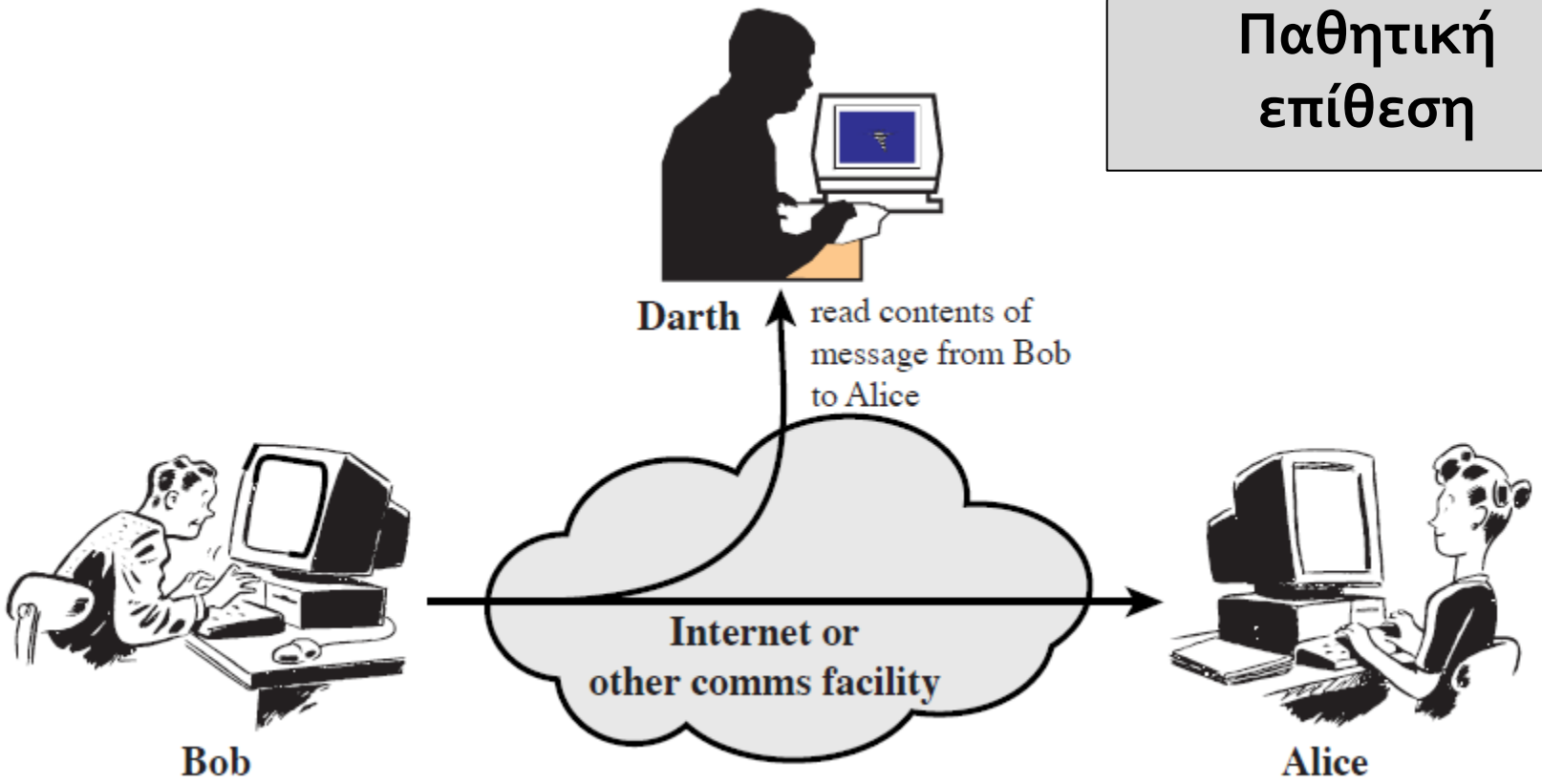
- Στόχοι ασφάλειας:
  - Εμπιστευτικότητα
  - Ακεραιότητα
  - Διαθεσιμότητα
  - Αυθεντικότητα, πιστοποίηση ταυτότητας
- Βασικές έννοιες:
  - Επίθεση ασφάλειας
  - Μηχανισμός ασφάλειας
  - Υπηρεσία ασφάλειας

Απειλές και επιθέσεις

- Απειλή: η δυνατότητα πραγματοποίησης κάποιας επίθεσης, λόγω π.χ. κάποιας εγγενούς ευπάθειας του υποκείμενου συστήματος
- Επίθεση: η διεξαγωγή κακόβουλης ενέργειας η οποία προσβάλει την ασφάλεια του συστήματος
  - Παθητικές
  - Ενεργητικές
- Παθητικές επιθέσεις:
  - Υποκλοπή περιεχομένου (μη εξουσιοδοτημένη πρόσβαση)
  - Ανάλυση κίνησης
- Ενεργητικές επιθέσεις:
  - Μεταμφίεση
  - Επανεκπομπή
  - Τροποποίηση
  - Διακοπή παροχής υπηρεσίας

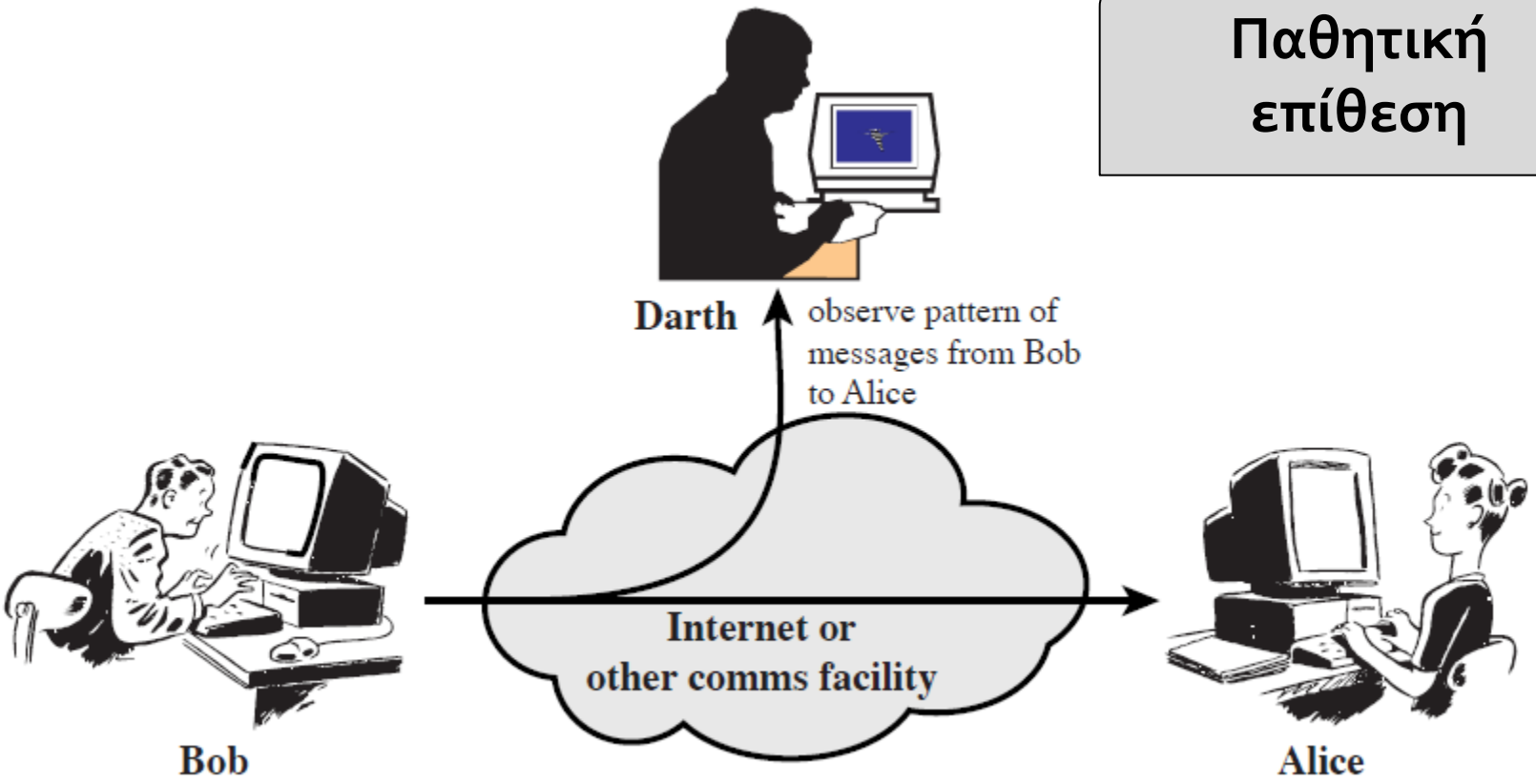
Υποκλοπή περιεχομένου μηνύματος

Παθητική επίθεση



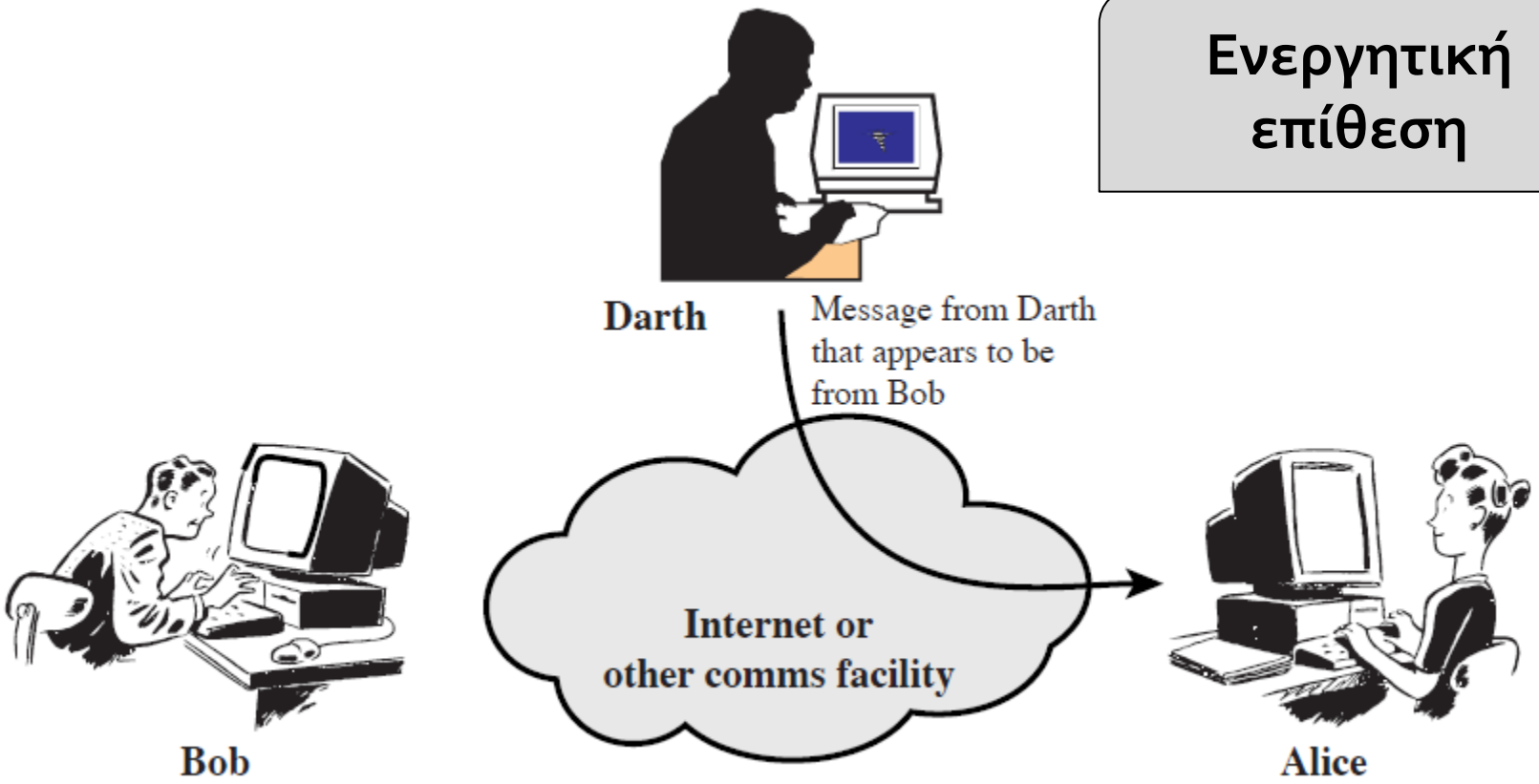
Ανάλυση κίνησης

Παθητική επίθεση



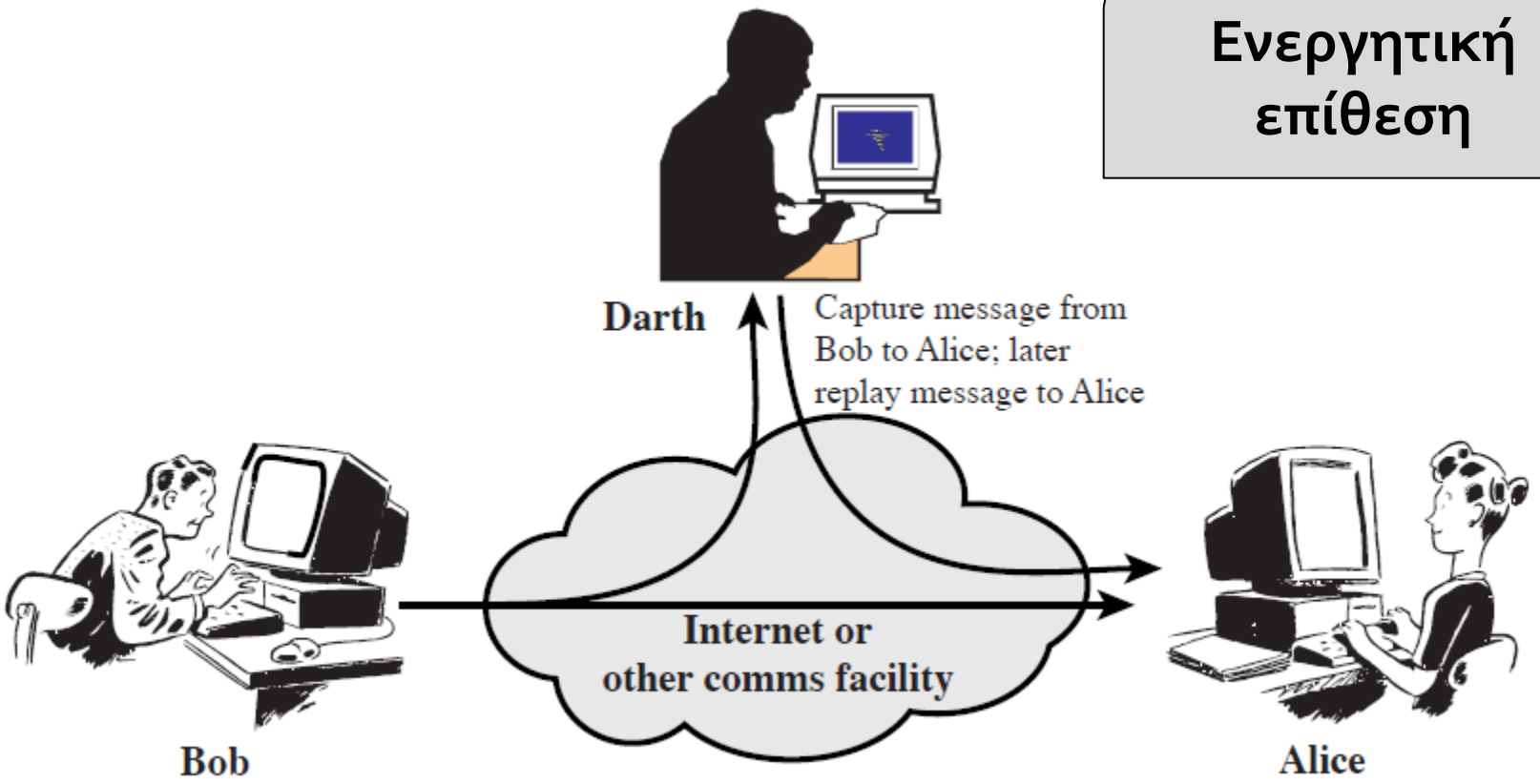
Μεταμφίεση

Ενεργητική επίθεση



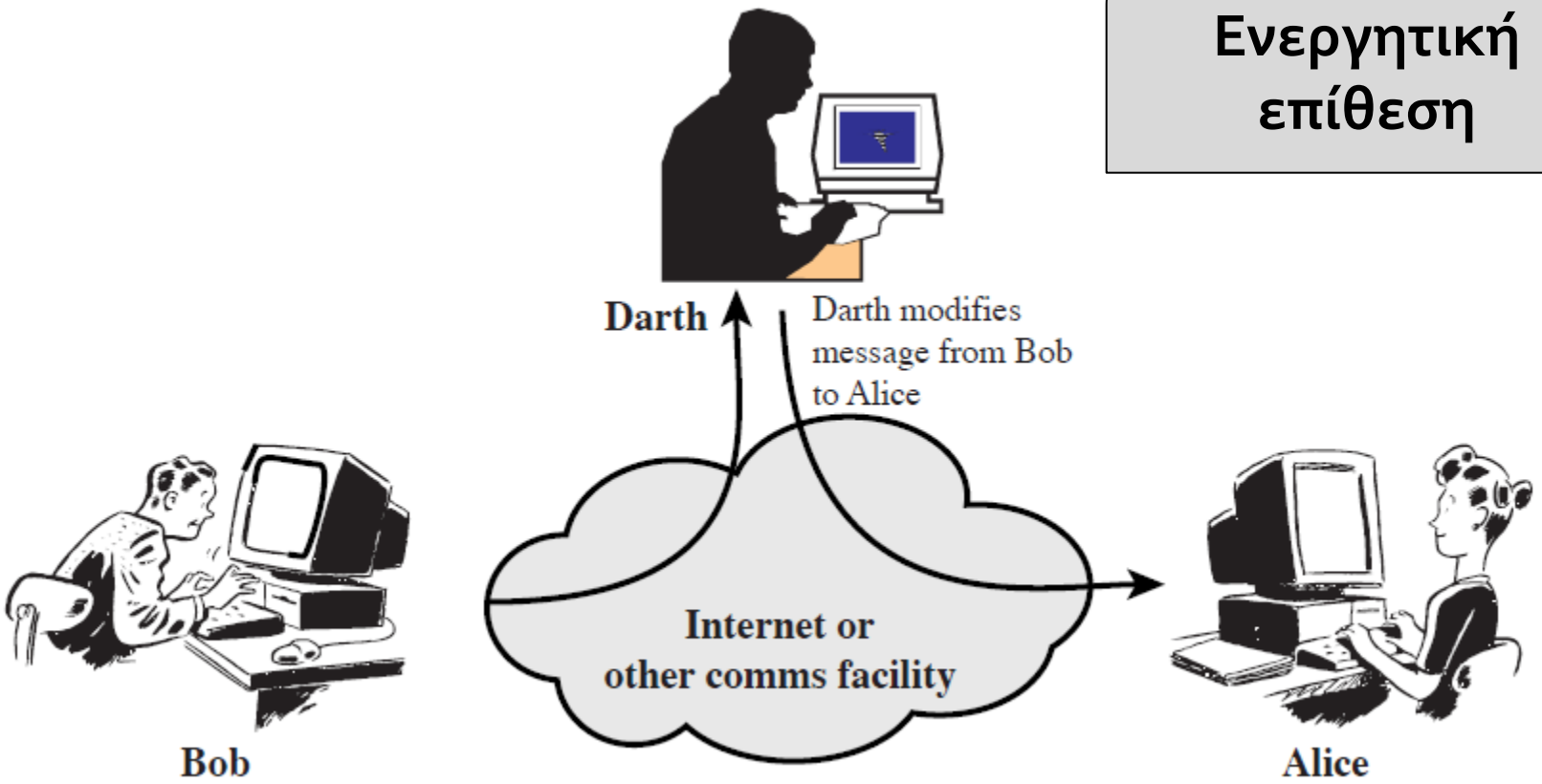
Επανεκπομπή

Ενεργητική επίθεση



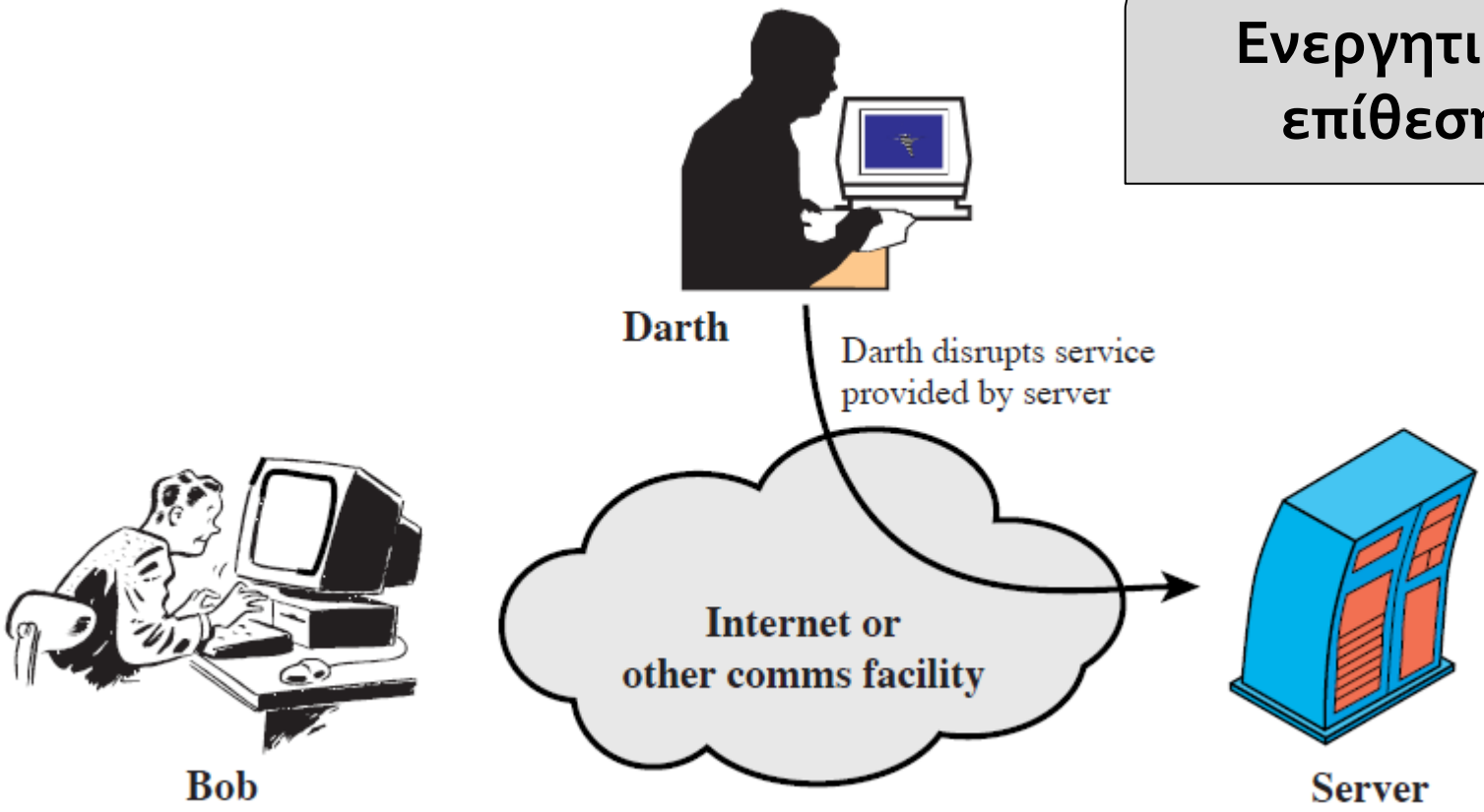
Τροποποίηση μηνυμάτων

Ενεργητική επίθεση



Διακοπή εξυπηρέτησης

Ενεργητική επίθεση



Υπηρεσίες ασφάλειας (κατά Χ.800)

- Πιστοποίηση ταυτότητας
  - Ομότιμης οντότητας
  - Προέλευσης δεδομένων
- Έλεγχος πρόσβασης
- Απόρρητο δεδομένων – εμπιστευτικότητα
  - Εμπιστευτικότητα σύνδεσης
  - Ασυνδεσμική εμπιστευτικότητα
  - Εμπιστευτικότητα επιλεγμένου πεδίου
  - Εμπιστευτικότητα ροής κίνησης

Υπηρεσίες ασφάλειας (κατά Χ.800)

- Ακεραιότητα δεδομένων
  - Ακεραιότητα σύνδεσης με αποκατάσταση
  - Ακεραιότητα σύνδεσης χωρίς αποκατάσταση
  - Ακεραιότητα σύνδεσης επιλεγμένου πεδίου
  - Ασυνδεσμική ακεραιότητα
  - Ασυνδεσμική ακεραιότητα επιλεγμένου πεδίου
- Μη αποποίηση
  - Μη αποποίηση, προέλευση
  - Μη αποποίηση, προορισμός

Μερικοί μηχανισμοί ασφάλειας (κατά Χ.800)

- Κρυπτογράφηση
- Ψηφιακή υπογραφή
- Μηχανισμοί ελέγχου πρόσβασης
- Μηχανισμοί ακεραιότητας
- Μηχανισμοί πιστοποίησης ταυτότητας
- Προσαύξηση κίνησης
- Έλεγχος δρομολόγησης
- Μηχανισμοί επικύρωσης
- Έμπιστη λειτουργικότητα
- Ετικέτα ασφάλειας
- Ανίχνευση συμβάντων
- Αρχείο καταγραφής συμβάντων
- Ανάκαμψη ασφάλειας

Συγκεκριμένοι μηχανισμοί ασφάλειας

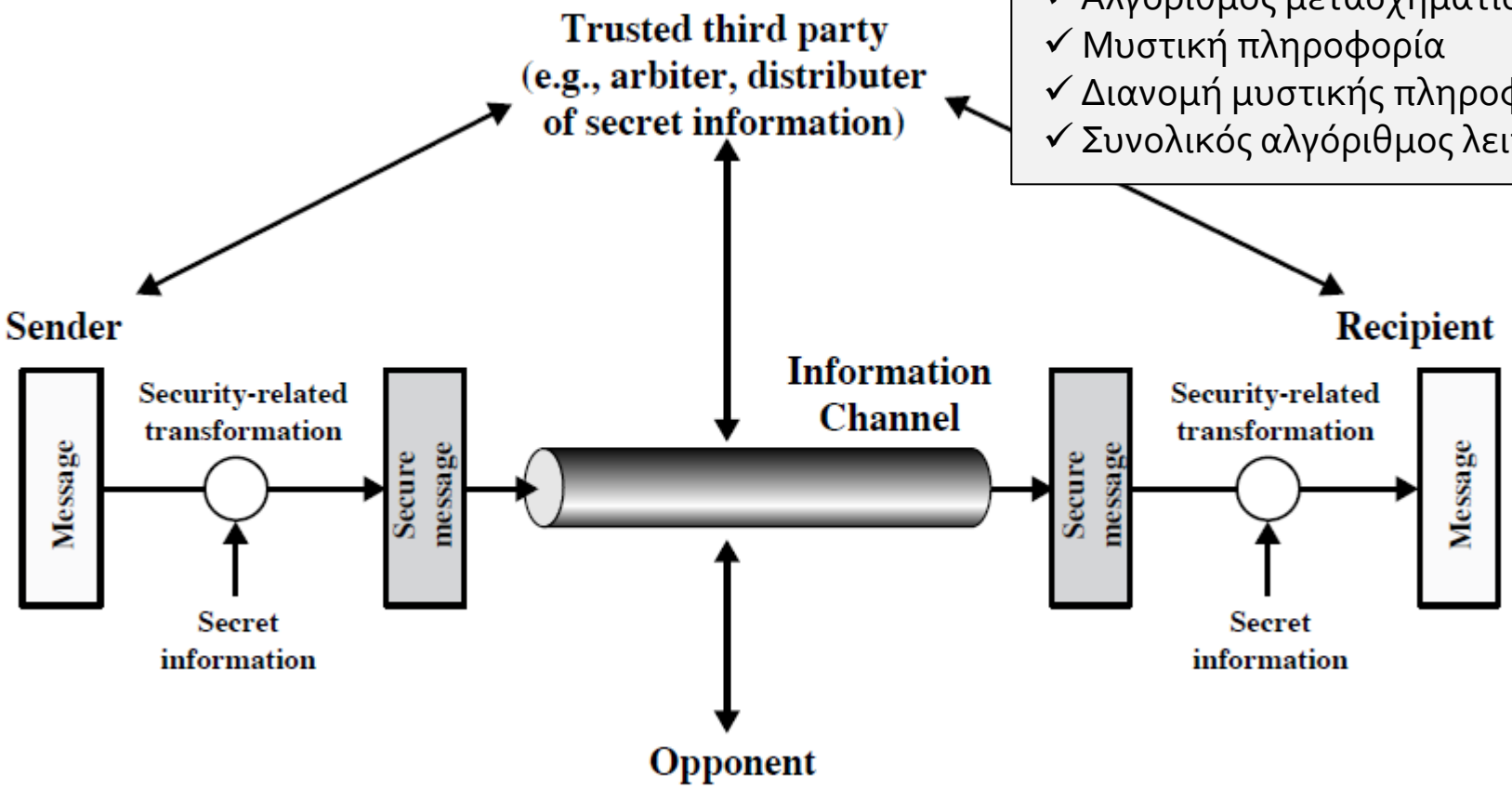
Γενικοί μηχανισμοί ασφάλειας

Σχέση μεταξύ υπηρεσιών και μηχανισμών

	Mechanism							
Service	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Μοντέλο ασφάλειας δικτύου

Κρίσιμα θέματα:
- ✓ Αλγόριθμος μετασχηματισμού
- ✓ Μυστική πληροφορία
- ✓ Διανομή μυστικής πληροφορίας
- ✓ Συνολικός αλγόριθμος λειτουργίας



Μοντέλο ασφάλειας δικτυακής πρόσβασης

Κρίσιμα θέματα:
- ✓ Η προστασία από εξωτερικούς εχθρούς
- ✓ Η προστασία από εσωτερικούς εχθρούς
- ✓ Η ανίχνευση των επιθέσεων
- ✓ Η σωστή σχεδίαση σε συνδυασμό με τις υποκείμενες υπηρεσίες