

ΕΚΔΟΣΕΙΣ ΚΛΕΙΔΑΡΙΘΜΟΣ

# ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ

## ΑΡΧΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ

3η αμερικανική έκδοση



William Stallings • Lawrie Brown



# Κεφάλαιο 7

Επιθέσις άρνησης εξυπηρέτησης

# Επίθεση άρνησης εξυπηρέτησης (DoS)

Στον Οδηγό αντιμετώπισης περιστατικών σχετικών με την ασφάλεια υπολογιστών (Computer Security Incident Handling Guide) του NIST, η επίθεση άρνησης εξυπηρέτησης (denial-of-service, DoS) ορίζεται ως εξής:

«Μια ενέργεια που εμποδίζει ή δυσκολεύει την εξουσιοδοτημένη χρήση δικτύων, συστημάτων, ή εφαρμογών εξαντλώντας πόρους όπως κεντρικές μονάδες επεξεργασίας (CPU), μνήμη, εύρος ζώνης, και αποθηκευτικό χώρο δίσκου.»



# Άρνηση εξυπηρέτησης (DoS)

- Μια μορφή επίθεσης με στόχο τη διαθεσιμότητα κάποιας υπηρεσίας
- Κατηγορίες πόρων που μπορούν να δεχθούν επίθεση:

## Εύρος ζώνης δικτύου

Σχετίζεται με τη χωρητικότητα των δικτυακών συνδέσμων που συνδέουν έναν διακομιστή με το Διαδίκτυο

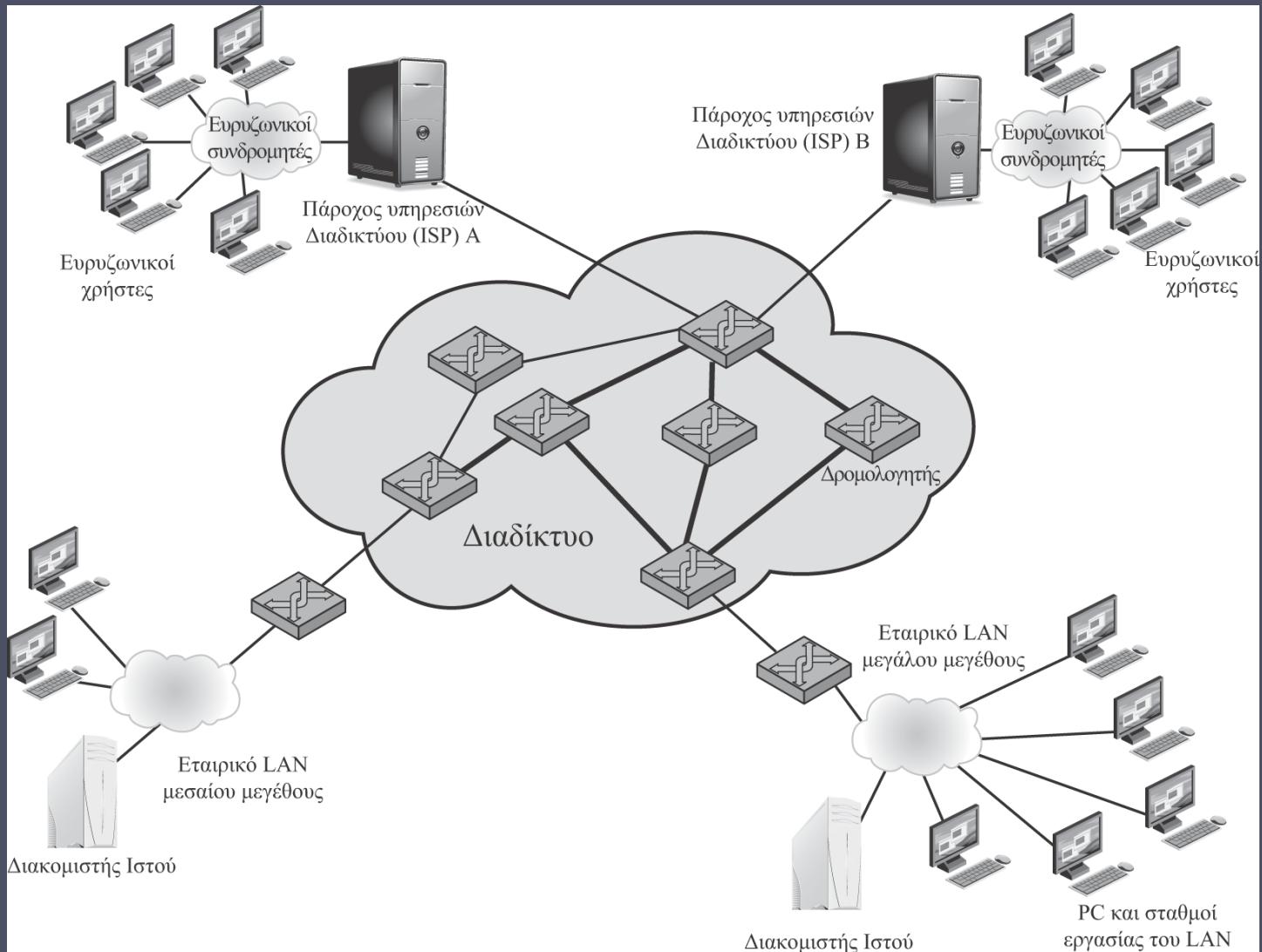
Για τους περισσότερους οργανισμών, πρόκειται για τη σύνδεσή τους με τον πάροχο υπηρεσιών Διαδικτύου (ISP)

## Πόροι συστήματος

Επιδιώκει να προκαλέσει υπερφόρτωση ή κατάρρευση του λογισμικού που χειρίζεται τις συνδέσεις δικτύου

## Πόροι εφαρμογών

Συνήθως περιλαμβάνει αρκετές έγκυρες αιτήσεις, καθεμία από τις οποίες καταναλώνει σημαντικούς πόρους, περιορίζοντας τη δυνατότητα του διακομιστή να εξυπηρετήσει αιτήσεις από άλλους χρήστες



# Κλασικές επιθέσεις DoS

- Κατακλυσμός με εντολές ηχοβολισμού (ping)
  - Ο σκοπός της είναι να υπερβεί τη χωρητικότητα της σύνδεσης δικτύου του οργανισμού-στόχου
  - Οι σύνδεσμοι υψηλότερης χωρητικότητας που βρίσκονται στο ενδιάμεσο της διαδρομής μπορούν να διαχειριστούν τον όγκο κυκλοφορίας, αλλά καθώς η χωρητικότητα μειώνεται, αρχίζουν να απορρίπτονται πακέτα
  - Η προέλευση της επίθεσης είναι εμφανής εκτός και αν χρησιμοποιείται παραπλανητική διεύθυνση
  - Η απόδοση του δικτύου επηρεάζεται αισθητά

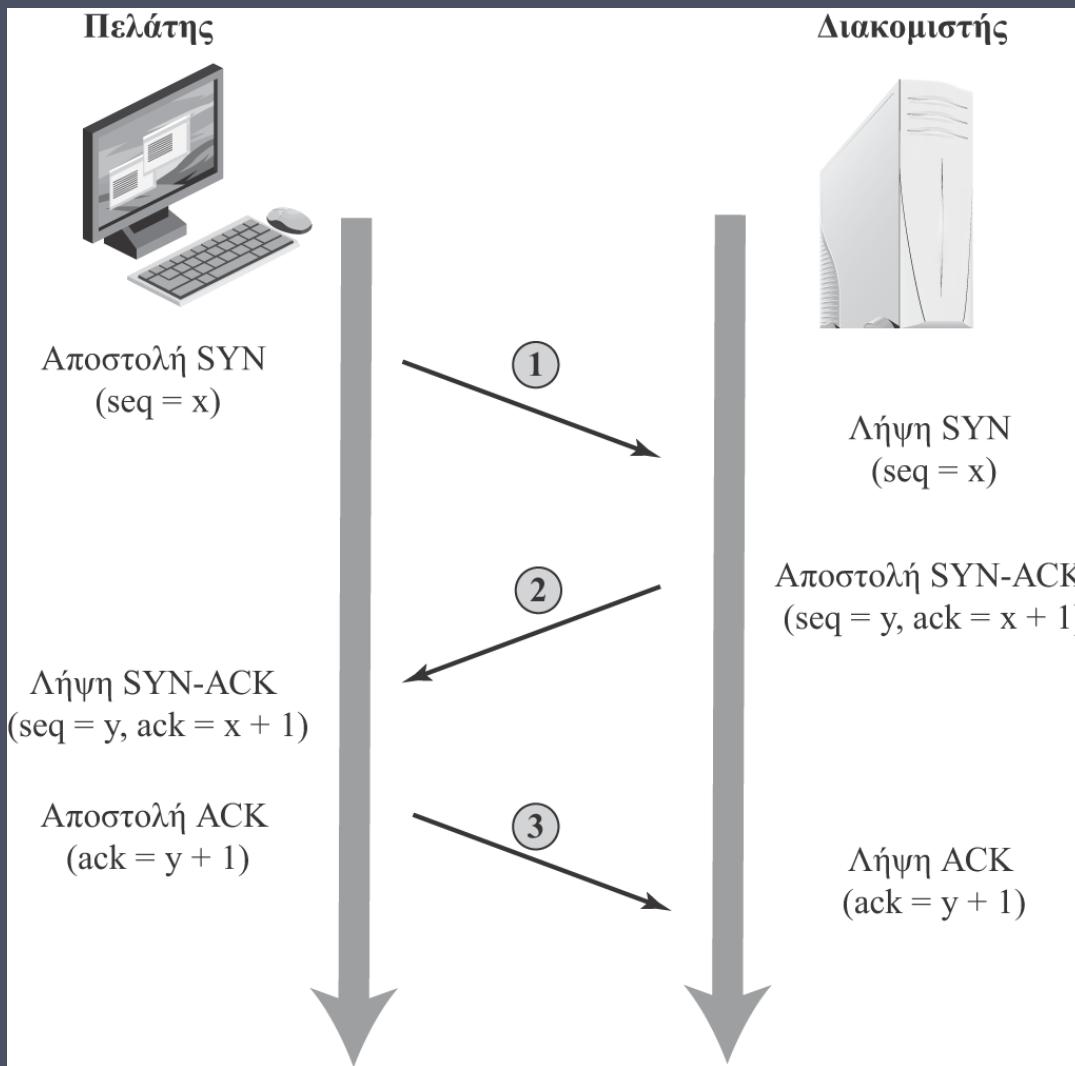


# Παραπλάνηση διεύθυνσης προέλευσης

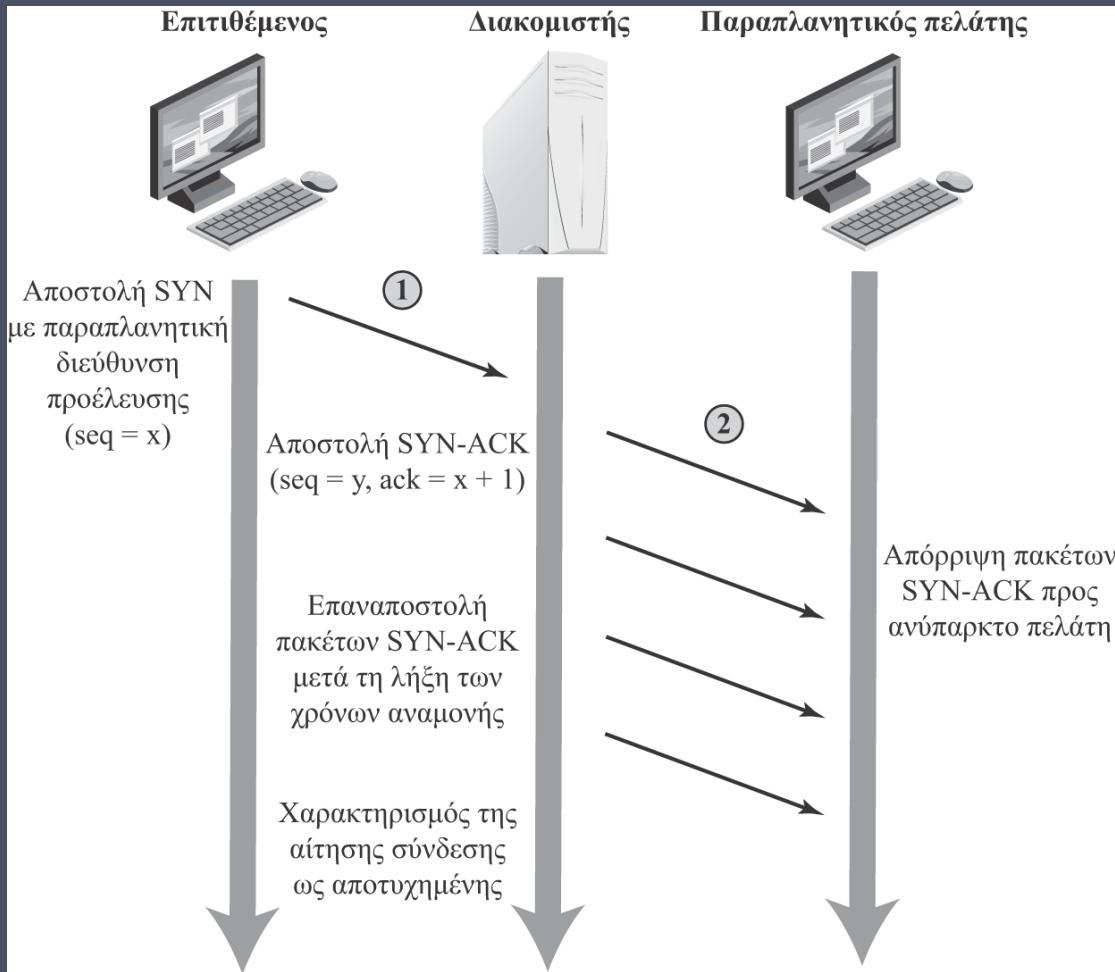
- Χρήση πλαστών διευθύνσεων προέλευσης
  - Επιτυγχάνεται συνήθως μέσω της διασύνδεσης υποδοχής γραμμής (raw socket interface) σε πολλά λειτουργικά συστήματα
  - Δυσκολεύει την ταυτοποίηση του συστήματος που χρησιμοποιείται για την επίθεση
- Ο επιπλέοντας παράγει μεγάλους όγκους πακέτων που έχουν ως διεύθυνση προορισμού το σύστημα-στόχο
- Αυτό θα είχε ως αποτέλεσμα να παρουσιαστεί συμφόρηση στον δρομολογητή που συνδέεται με τον τελικό σύνδεσμο χαμηλότερης χωρητικότητας
- Απαιτεί από τους μηχανικούς δικτύου να υποβάλλουν συγκεκριμένα ερωτήματα σχετικά τη ροή πληροφοριών από τους δρομολογητές τους
- Κυκλοφορία οπισθοσκέδασης
  - Γνωστοποίηση διαδρομών προς αχρησιμοποίητες διευθύνσεις IP για την παρακολούθηση της κυκλοφορίας που σχετίζεται με την επίθεση

# Παραπλάνηση SYN

- Διαδεδομένη επίθεση DoS
- Βάζει στο στόχαστρό της τη δυνατότητα ενός διακομιστή να αποκρίνεται σε μελλοντικές αιτήσεις σύνδεσης, υπερχειλίζοντας τους πίνακες που χρησιμοποιούνται για τη διαχείριση τέτοιων συνδέσεων
- Δεν επιτρέπεται σε έγκυρους χρήστες να αποκτήσουν πρόσβαση στον διακομιστή
- Επομένως, πρόκειται για μια επίθεση εναντίον των πόρων του συστήματος, και ειδικότερα του κώδικα του λειτουργικού συστήματος ο οποίος χειρίζεται τις συνδέσεις δικτύου



Εικόνα 7.2 Τριπλή χειραψία σύνδεσης του πρωτοκόλλου TCP



Εικόνα 7.3 Επίθεση παραπλάνησης TCP SYN

# Επιθέσεις κατακλυσμού

- Ταξινομούνται με βάση το χρησιμοποιούμενο πρωτόκολλο δικτύου
- Επιδίωξη είναι η υπερφόρτωση της δικτυακής χωρητικότητας κάποιου συνδέσμου με έναν διακομιστή
- Μπορούν να χρησιμοποιηθούν σχεδόν όλοι οι τύποι πακέτων δικτύου

## Κατακλυσμός ICMP

- Κατακλυσμός με ηχοβολισμό που χρησιμοποιεί πακέτα αίτησης αντήχησης ICMP
- Οι διαχειριστές συνήθως επιτρέπουν την ύπαρξη τέτοιων πακέτων στα δίκτυά τους επειδή ο ηχοβολισμός είναι χρήσιμο διαγνωστικό εργαλείο

## Κατακλυσμός UDP

- Χρησιμοποιεί πακέτα UDP τα οποία διοχετεύονται προς κάποιον αριθμό θύρας του συστήματος-στόχου

## Κατακλυσμός TCP SYN

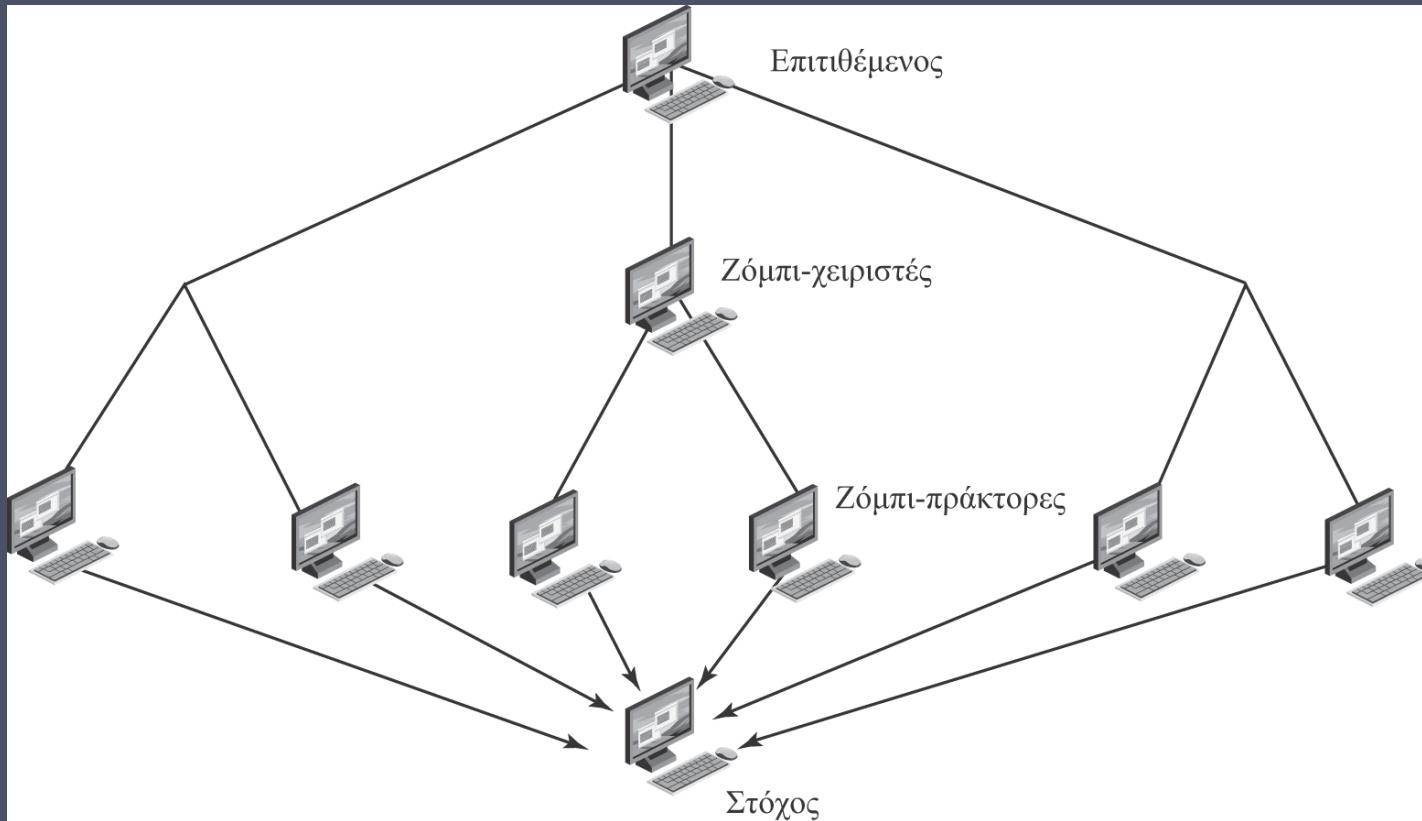
- Στέλνει πακέτα TCP στο σύστημα-στόχο
- Στόχος της επίθεσης δεν είναι ο κώδικας του συστήματος αλλά ο συνολικός όγκος πακέτων

# Επιθέσεις κατανεμημένης άρνησης εξυπηρέτησης (DDoS)

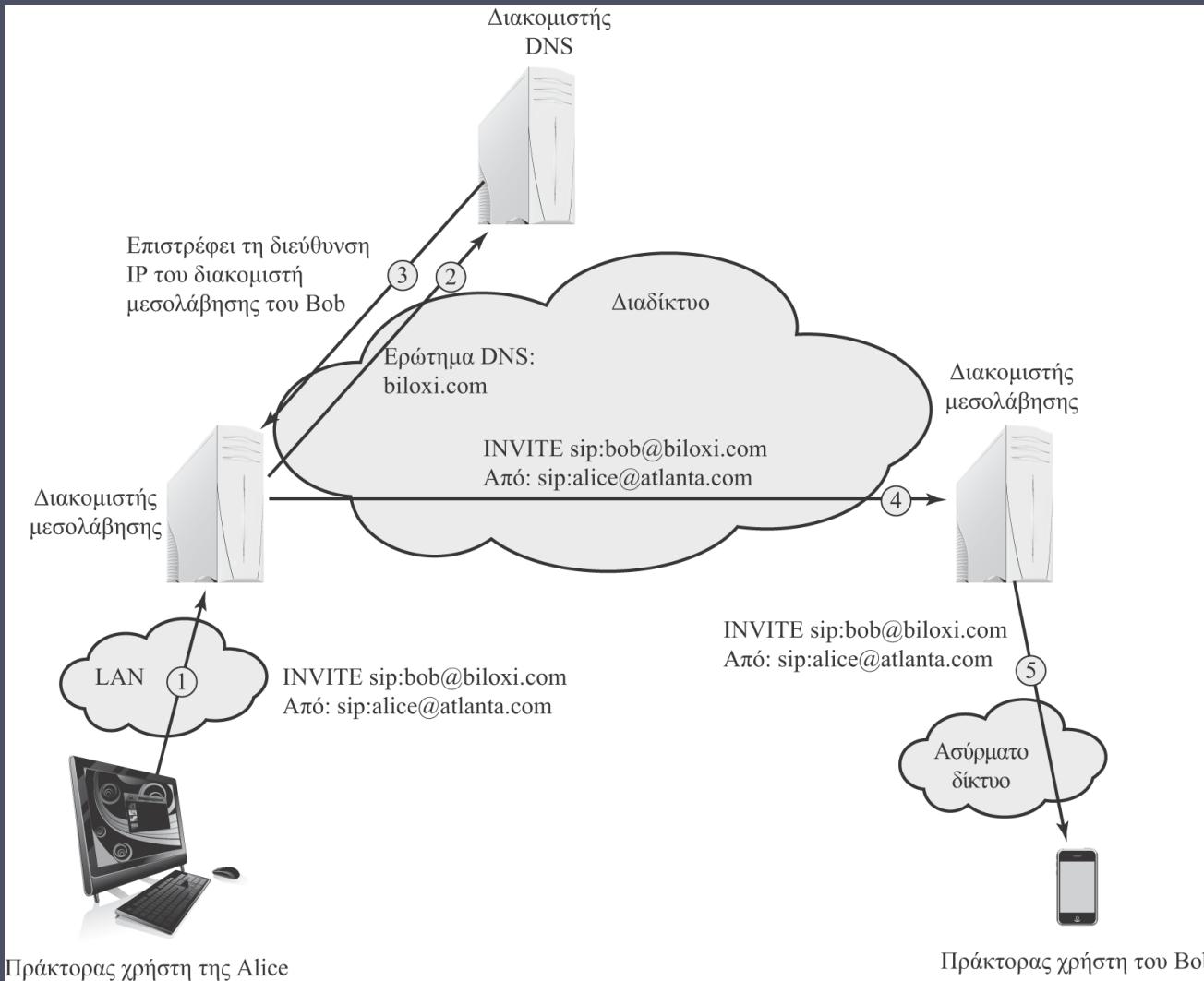
Χρήση πολλών  
συστημάτων  
για επιθέσεις

Ο επιτιθέμενος  
εκμεταλλεύεται  
μια αδυναμία  
του λειτουργικού  
συστήματος  
ή μιας δημοφιλούς  
εφαρμογής για να  
αποκτήσει πρόσβαση  
και να εγκαταστήσει  
το πρόγραμμά του  
στο σύστημα (ζόμπι)

Μπορούν να  
δημιουργηθούν  
μεγάλες ομάδες  
από τέτοια συστήματα  
που ελέγχονται  
από έναν επιτιθέμενο,  
οι οποίες συλλογικά  
σχηματίζουν ένα δίκτυο  
ρομπότ (botnet)



Εικόνα 7.4 Αρχιτεκτονική επίθεσης DDoS



Εικόνα 7.5 Σενάριο μηνύματος SIP INVITE

# Επιθέσεις βασισμένες στο Πρωτόκολλο Μεταφοράς Υπερ-κειμένου (HTTP)

## Κατακλυσμός HTTP

- Επίθεση που βομβαρδίζει διακομιστές Ιστού με αιτήσεις HTTP
- Καταναλώνει σημαντικούς πόρους
- Επίθεση αράχνης
  - Τα ρομπότ ξεκινούν από έναν δεδομένο σύνδεσμο HTTP και ακολουθούν όλους τους συνδέσμους που περιέχονται στον παρεχόμενο ιστότοπο με αναδρομικό τρόπο

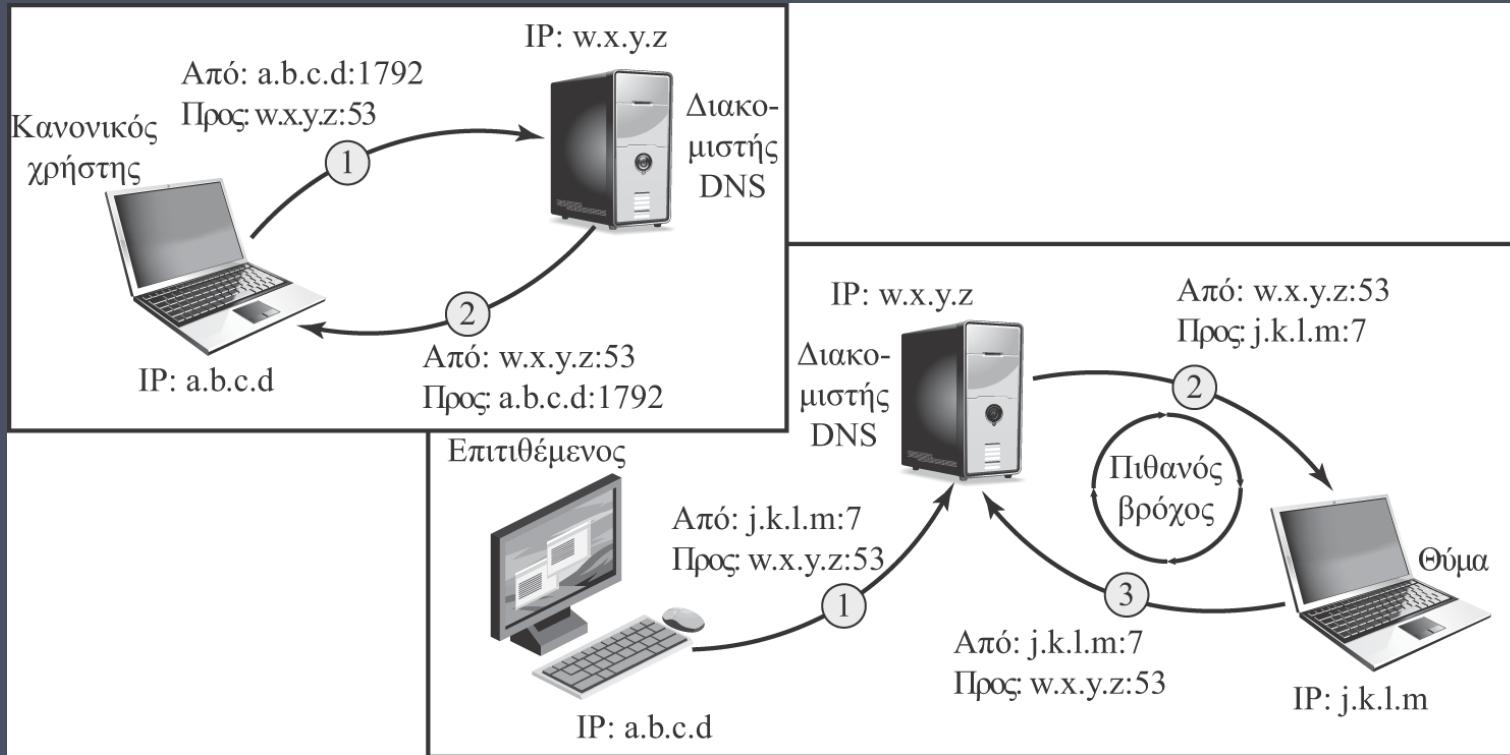
## Slowloris

- Προσπαθεί να μονοπωλήσει στέλνοντας αιτήσεις HTTP που δεν ολοκληρώνονται ποτέ
- Καταναλώνει τελικά όλη τη χωρητικότητα των συνδέσεων του διακομιστή Ιστού
- Κάνει χρήση της έγκυρης κυκλοφορίας HTTP
- Οι υπάρχουσες λύσεις ανίχνευσης και αποτροπής εισβολών (που στηρίζονται σε υπογραφές για την ανίχνευση επιθέσεων) δεν είναι γενικά σε θέση να αναγνωρίζουν μια επίθεση Slowloris

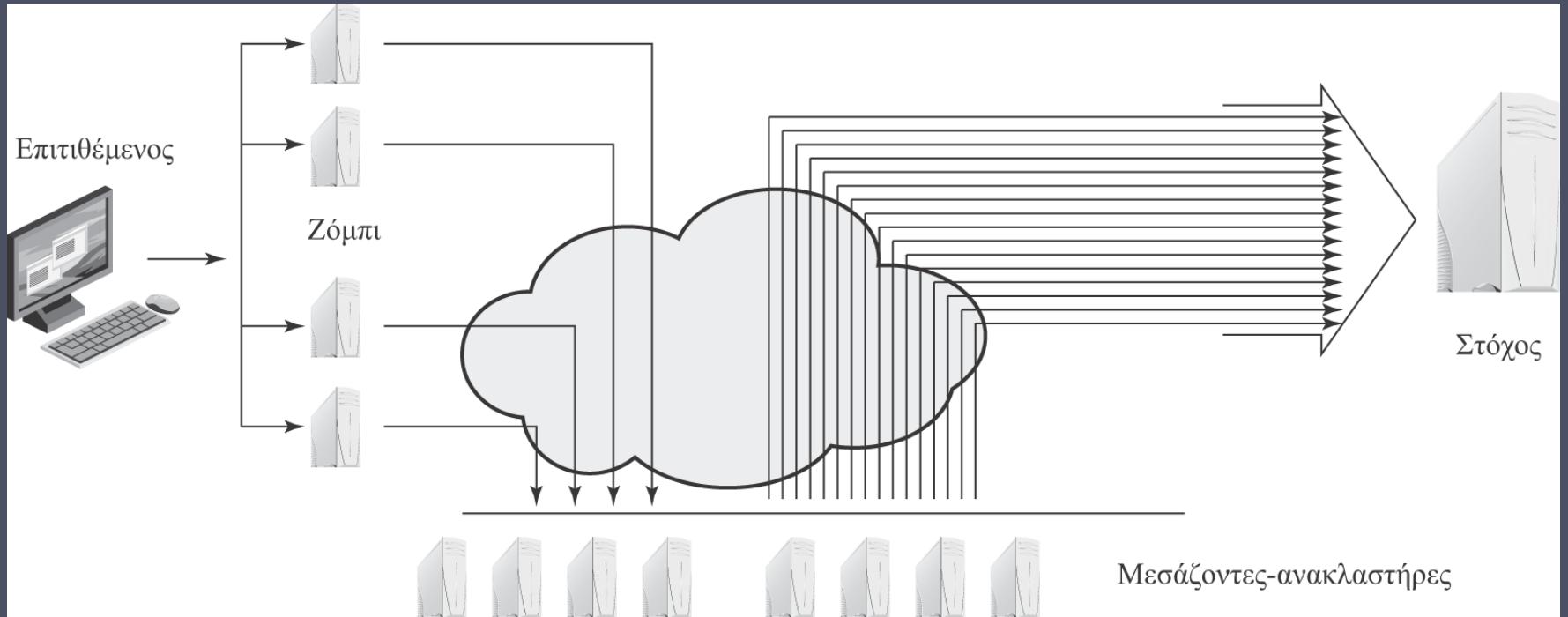
# Επιθέσεις ανάκλασης



- Στέλνει πακέτα σε μια γνωστή υπηρεσία του μεσάζοντα με παραπλανητική διεύθυνση προέλευσης του πραγματικού συστήματος-στόχου
- Όταν ο μεσάζοντας αποκριθεί, η απάντηση αποστέλλεται στον στόχο
- Προκαλείται ουσιαστικά μια «ανάκλαση» της επίθεσης στον μεσάζοντα (ανακλαστήρα)
- Ο σκοπός είναι να παραχθούν αρκετά μεγάλοι όγκοι πακέτων τα οποία θα κατακλύσουν τον σύνδεσμο με το σύστημα-στόχο χωρίς ο μεσάζοντας να αντιληφθεί τι συμβαίνει
- Η καλύτερη άμυνα κατά τέτοιων επιθέσεων είναι το μπλοκάρισμα πακέτων με παραπλανητικές διευθύνσεις προέλευσης



Εικόνα 7.6 Επίθεση ανάκλασης DNS



Εικόνα 7.7 Επίθεση ενίσχυσης

# Επιθέσεις ενίσχυσης DNS

- Χρησιμοποιούν πακέτα που έχουν ως προορισμό έναν έγκυρο διακομιστή DNS στο σύστημα-μεσάζοντα
- Ο επιπλέοντας δημιουργεί μια σειρά από αιτήσεις DNS που περιέχουν την παραπλανητική διεύθυνση προέλευσης του συστήματος-στόχου
- Εκμεταλλεύονται τη συμπεριφορά του πρωτοκόλλου DNS ώστε να μετατρέψουν μια μικρή αίτηση σε μια πολύ μεγαλύτερη απάντηση (ενίσχυση)
- Ο στόχος κατακλύζεται από τις απαντήσεις
- Η βασική άμυνα κατά τέτοιων επιθέσεων είναι η αποτροπή της χρήσης παραπλανητικών διευθύνσεων προέλευσης

# Άμυνες κατά επιθέσεων DoS

Τέσσερις γραμμές άμυνας κατά επιθέσεων DDoS

- Αυτές οι επιθέσεις δεν μπορούν να αποτραπούν εντελώς
- Ύψηλοί όγκοι ενδέχεται να αντιστοιχούν σε έγκυρη κυκλοφορία
  - Υψηλή δημοτικότητα ενός συγκεκριμένου ιστότοπου
  - Δραστηριότητα σε έναν πολύ δημοφιλή ιστότοπο
  - Για την περιγραφή τέτοιων συμβάντων χρησιμοποιούνται οι όροι *slashdotted*, *flash crowd*, ή *flash event*

## Αποτροπή και πρόληψη επιθέσεων

- Πριν από την εκδήλωση της επίθεσης

## Ανίχνευση και φίλτραρισμα επιθέσεων

- Κατά τη διάρκεια της επίθεσης

## Αντίστροφη παρακολούθηση και ταυτοποίηση της πηγής

- Κατά τη διάρκεια της επίθεσης και μετά από αυτήν

## Αντίδραση στην επίθεση

- Μετά από την επίθεση

# Αποτροπή επιθέσεων DoS

- Μπλοκάρισμα παραπλανητικών διευθύνσεων προέλευσης
  - Σε δρομολογητές όσο το δυνατόν πιο κοντά στην πηγή
- Μπορούν να χρησιμοποιηθούν φίλτρα ώστε να εξασφαλιστεί ότι η αντίστροφη διαδρομή προς την υποτιθέμενη διεύθυνση προέλευσης είναι εκείνη που χρησιμοποιείται από το τρέχον πακέτο
  - Πρέπει να εφαρμόζονται στην κυκλοφορία δεδομένων προτού αυτή εγκαταλείψει το δίκτυο του ISP, ή ακόμα και στο σημείο εισόδου του δικού τους δικτύου
- Χρήση μιας τροποποιημένου κώδικα χειρισμού των συνδέσεων TCP
  - Κρίσιμες πληροφορίες κωδικοποιούνται με κρυπτογράφηση σε ένα «μπισκότο» το οποίο αποστέλλεται στον ως αρχικός αριθμός ακολουθίας του διακομιστή
    - Ένας έγκυρος πελάτης αποκρίνεται στέλνοντας ένα πακέτο ACK που περιέχει το μπισκότο με τον προσαυξημένο αριθμό ακολουθίας
  - Απόρριψη μιας καταχώρισης για μια ατελή σύνδεση από τον πίνακα συνδέσεων TCP όταν παρατηρείται υπερχείλιση

# Αποτροπή επιθέσεων DoS

- Μπλοκάρισμα της χρήσης κατευθυνόμενων εκπομπών IP
- Μπλοκάρισμα κυκλοφορίας προς ύποπτες υπηρεσίες, ή συνδυασμούς θυρών
- Αποτροπή επιθέσεων εναντίον εφαρμογών με μια μορφή γραφικού παζλ που ονομάζεται (captcha) για τη διάκριση έγκυρων αιτήσεων από ανθρώπους
- Πρέπει να υιοθετούνται συνολικά καλές πρακτικές σχετικές με την ασφάλεια των συστημάτων
- Χρήση ειδώλων και αντιγράφων διακομιστών όταν απαιτούνται υψηλή απόδοση και αξιοπιστία

# Αντιμετώπιση επιθέσεων DoS

## Καλό σχέδιο αντιμετώπισης περιστατικών

- Λεπτομερείς οδηγίες για τον τρόπο επικοινωνίας με το τεχνικό προσωπικό του ISP
- Απαιτείται για την επιβολή φίλτραρισμάτος στην άνοδο (upstream)
- Λεπτομέρειες σχετικά με τον τρόπο αντιμετώπισης της επίθεσης

- Πρέπει να εφαρμόζονται φίλτρα αντιπαραπλάνησης (antispoofing), κατευθυνόμενης εκπομπής, και περιορισμού ρυθμού
- Ιδανικά, πρέπει να υπάρχουν συστήματα παρακολούθησης δικτύου και IDS που θα ειδοποιούν το προσωπικό όταν ανιχνεύεται μη φυσιολογική κυκλοφορία δεδομένων

# Αντιμετώπιση επιθέσεων DoS

- Αναγνώριση του τύπου της επίθεσης
  - «Σύλληψη» και ανάλυση πακέτων
  - Σχεδιασμός φίλτρων που θα μπλοκάρουν τη ροή πακέτων της επίθεσης στην άνοδο
  - Εναλλακτικά, εντοπισμός και διόρθωση σφάλματος συστήματος/εφαρμογής
- Μπορεί να ζητηθεί από τον ISP να παρακολουθεί την αντίστροφη πορεία των πακέτων για να εντοπίσει την πηγή
  - Ενδέχεται να αποδειχθεί δύσκολο και χρονοβόρο
  - Υποχρεωτικό αν θα κινηθούν νομικές διαδικασίες
- Εφαρμογή σχεδίου έκτακτης ανάγκης
  - Χρήση εναλλακτικών εφεδρικών διακομιστών
  - Έναρξη λειτουργίας νέων διακομιστών σε νέα τοποθεσία με νέες διευθύνσεις
- Ενημέρωση του σχεδίου αντιμετώπισης περιστατικών
  - Ανάλυση της επίθεσης και του τρόπου αντιμετώπισης για μελλοντικούς χειρισμούς



# Σύνοψη

- **Επιθέσεις άρνησης εξυπηρέτησης**

- Η φύση των επιθέσεων άρνησης εξυπηρέτησης
- Κλασικές επιθέσεις άρνησης εξυπηρέτησης
- Παραπλάνηση διεύθυνσης προέλευσης
- Παραπλάνηση SYN

- **Επιθέσεις κατακλυσμού**

- Κατακλυσμός ICMP
- Κατακλυσμός UDP
- Κατακλυσμός TCP SYN

- **Άμυνες κατά επιθέσεων άρνησης εξυπηρέτησης**

- **Αντιμετώπιση επίθεσης άρνησης εξυπηρέτησης**



- **Επιθέσεις κατανεμημένης άρνησης εξυπηρέτησης**

- **Επιθέσεις εύρους ζώνης βασισμένες σε εφαρμογές**

- Κατακλυσμός SIP
- Επιθέσεις βασισμένες στο HTTP

- **Επιθέσεις με ανακλαστήρες και ενισχυτές**

- Επιθέσεις ανάκλασης
- Επιθέσεις ενίσχυσης
- Επιθέσεις ενίσχυσης DNS