Το DNS στην Επιχείρηση

Αυξάνοντας την Ασφάλεια και την Διαθεσιμότητα της Επιχείριση σας

Μαγκος Κωνσταντίνος
Εργαστήριο Δικτύων
Ινστιτούτο Πληροφορικής & Τηλεπικοινωνιών
ΕΚΕΦΕ Δημόκριτος

Θέματα Συζήτησης

1. Domain Name System
   - Ιστορία, Περιγραφή πρωτοκόλλου, Σημασία του στη λειτουργία του Διαδικτύου.
2. Θέματα Ασφάλειας του DNS
   - Κίνδυνοι, Απειλές, Περιγραφή επιθέσεων
3. Ενίσχυση Ασφάλειας DNS
   - Αντιμετώπιση απειλών
4. Berkeley Internet Name Daemon
   - Περιγραφή, Χρήση του BIND, Εφαρμογή του στην αντιμετώπιση του απειλών.

Domain Name System (DNS)

Ιστορική Αναδρομή

1969: Δημιουργείται το ARPANET, μεταξύ των UCLA & SRI. Οι διασυνδεόμενες μηχανές είναι λίγες (4 κόμβοι), δεν υπάρχει σύστημα αντιστοιχίας ονομάτων αντιστοιχίας.

1971: Καθώς το ARPANET μεγαλώνει παρουσιάζεται η ανάγκη καταγραφής των μηχανών και υπηρεσιών. Η Peggy Karp συντάσσει το RFC 226, τυποποιώντας τον 1ο μνημονικό κανόνα.

1972: Εκδίδεται η 1η έκδοση του "HOSTS.TXT", βασισμένο στο RFC 226. Το "HOSTS.TXT" τυποποιείται στο RFC 608. Κάθε διακομιστής διατηρεί αντίγραφό του και οι αλλαγές επικοινωνούνται μέσω e-mail στο SRI. Το αρχείο είναι διαθέσιμο μέσω FTP από το SRI. Για πολλά χρόνια, το αρχειο συντηρεί ο Jon Postel.

DNS: Ιστορική Αναδρομή

1981: Ο David Mills, προσπαθώντας να λύσει προβλήματα του ηλεκτρονικού ταχυδρομείου, γράφει το RFC 799 και ορίζει τα Internet Domain Names.

1982: Οι Jon Postel & Zaw-Sing Su γράφουν το RFC 819 και δίνουν μια γενική περιγραφή της δομής του DNS.

1983: Ο Paul Mockapetris δημοσιεύει τα RFC 882 “Domain Names – Concepts and Facilities” και RFC 883 “Domain Names – Implementation and Specification”. Περιγράφουν ένα τελείως νέο τρόπο επίλυσης ονομάτων. Σημαντικές έννοιες: Delegation και Authority.

1987: Τα RFC 1034 και 1035 του P. Mockapetris αντικαθιστούν τα 882 και 883.

Λειτουργία DNS

- Βασική λειτουργία: η αντιστοίχιση των ονομάτων χώρου (domain names) σε διευθύνσεις IP και το αντίστροφο. Τα ονόματα χώρου χρησιμοποιούνται από τους ανθρώπους, ενώ οι διευθύνσεις IP από τις μηχανές.
- Είναι μια ιεραρχική, παγκοσμίως κατανεμημένη, χαλαρής συνοχής, δυναμική και επεκτάσιμη βάση δεδομένων.
- Αποτελείται από τρία βασικά στοιχεία:
  - Το χώρο ονομάτων (namespace).
  - Τους διακομιστές που χειρίζονται το χώρο ονομάτων.
  - Τους πελάτες (resolvers) που ρωτάνε τους διακομιστές για το χώρο ονομάτων.
- Ο διακομιστής (“Nameserver” ή “DNS server") υλοποιεί την βάση δεδομένων και απαντά σε ερωτήσεις πελατών.

Λειτουργία DNS

- Οι πληροφορίες διατηρούνται τοπικά αλλά ανακτούνται από οπουδήποτε.
  - Δεν υπάρχει Μοναδικό Σημείο Αστοχίας (Single Point of Failure).
- Οι διαχειριστές έχουν έλεγχο ενός συγκεκριμένου τμήματος (ζώνη) του χώρου ονομάτων. Συντηρούν την βάση δεδομένων αυτού του τμήματος.
- Η πληροφορία μπορεί να αποθηκευτεί προσωρινά (cache) για βελτίωση της απόδοσης.
- Δυνατότητα διακομιστών εφεδρείας (slave servers) που μοιράζονται μέρος του φόρτου.
- Η βάση μπορεί να ενημερώνεται δυναμικά και η αντιγραφή της από τον master στον server γίνεται αυτόματα.

Τεχνικά Χαρακτηριστικά DNS

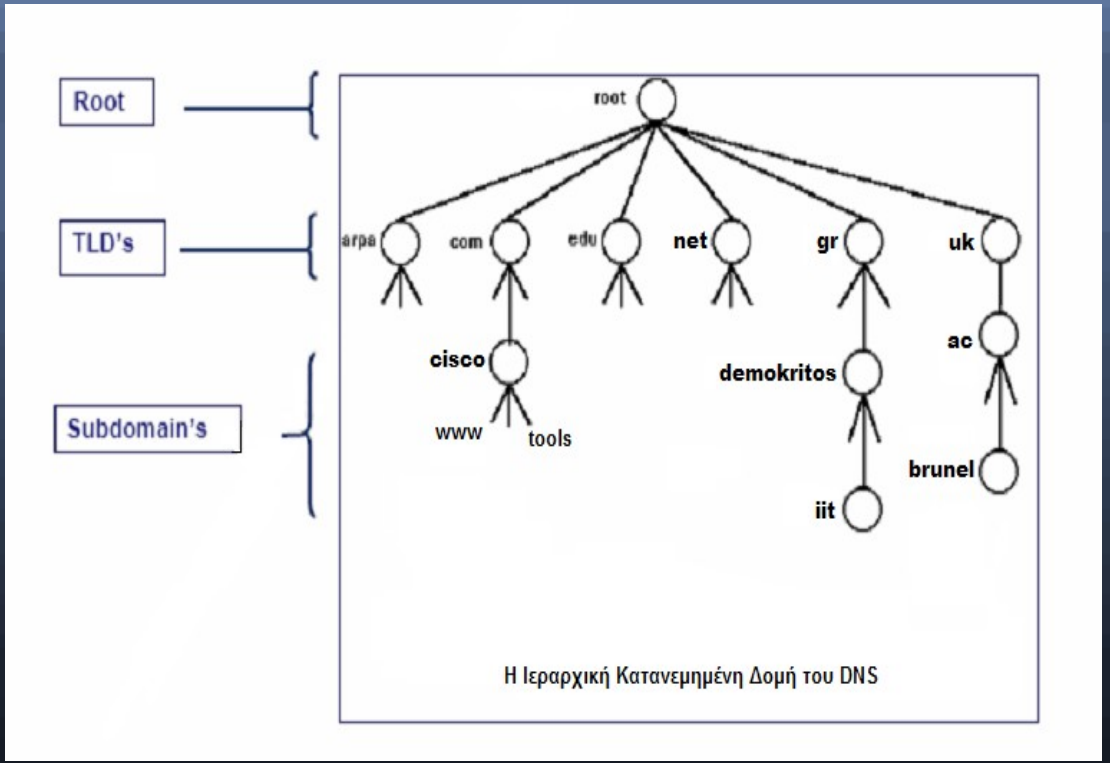
- Το DNS χρησιμοποιεί UDP και TCP στην πόρτα 53:
  - Στην περίπτωση UDP, το πρωτόκολλο ρυθμίζει θέματα αξιοπιστίας όπως, UDP retransmission, sequencing.
- Τυπικά, για τις ερωτήσεις χρησιμοποιείται udp/53. Τόσο ο διακομιστής όσο και ο resolver συνιστάται (SHOULD) να υποστηρίζουν tcp/53 (RFC 1123).
  - Οι απαντήσεις δεν πρέπει να ξεπερνούν τα 512 bytes (RFC 1035).
  - Για απαντήσεις μεγαλύτερες χρησιμοποιείται TCP.
  - EDNS0 (RFC 2671), UDP απαντήσεις μεγαλύτερες των 512 bytes.
- Η αντιγραφή της βάσης δεδομένων (μεταφορά ζώνης) γίνονται πάνω από TCP.

Τεχνικά Χαρακτηριστικά DNS

- Το DNS, εκτός από τις αντιστοιχίες ονομάτων χώρου – IP διευθύνσεων, περιέχει:
  - Πληροφορίες για την ανταλλαγή ηλεκτρονικού ταχυδρομείου.
  - Πληροφορίες για την λειτουργία της υπηρεσίας.
  - Γενικά πληροφορίες.
- Οι πληροφορίες αποθηκεύεται σε εγγραφές (Resource Records – RRs). Υπάρχουν διαφορετικά είδη, ανάλογα με το είδος της πληροφορίας. Πιο συνηθισμένες: SOA, NS, A, MX, PTR, TXT.
- Κάθε domain name αποτελείται από ένα ή περισσότερα ονόματα που χωρίζονται από τελείες “.”, κάθε όνομα έως 63 χαρακτήρες, σύνολο 255 μαζί με τις τελείες.

Domains

- Κάθε domain αντιστοιχεί σε αυτόνομο χώρο ονομάτων.
- Ο χώρος κάτω από το "gr" είναι το "gr" domain.
- Ο χώρος κάτω από το "demokritos.gr" είναι το "demokritos.gr" domain.



Zones

- Οι ζώνες (zones) αντιστοιχούν σε χώρους ευθύνης.
- Ο διαχειριστής μια ζώνης έχει την ευθύνη για ένα τμήμα του domain. Έχει την εξουσία (authority) του τμήματος αυτού.
- Είναι δυνατόν η εξουσία τμήματος του domain να μεταβιβαστεί.
  - Η μεταβίβαση (delegation) γίνεται από την γονική ζώνη (parent zone) στη θυγατρική ζώνη (child zone).

Τύποι DNS Διακομιστών

- **Authoritative** – Διακομιστής με την πιο έγκυρη, αυθεντική πληροφορία.
  - Master (primary): έχει αποθηκευμένες τοπικά τις ζώνες.
  - Slave (secondary): παίρνει περιοδικά αντίγραφο των ζωνών από τον master.
- **(Caching) Recursive** – Οι διακομιστές που ρωτούν τους authoritative nameservers εκ μέρους των DNS πελατών. Επιστρέφουν non-authoritative απαντήσεις. Προσωρινή αποθήκευση για μελλοντική χρήση (caching).
- **Forwarding** – Διακομιστής που προωθεί τις ερωτήσεις που δέχεται στον επόμενο recursive nameserver. Μπορούν να κάνουν και caching.

Stealth/Hidden Master

- Κρυφός authoritative nameserver
  - Δεν εμφανίζεται μέσα στη ζώνη (NS και SOA εγγραφές).
  - Δεν δέχεται ερωτήματα από εξωτερικούς διακομιστές.
- Διαχωρίζεται από τους υπόλοιπους nameservers μέσω firewall, αυξημένη πολιτική ασφαλείας.
- Οι διαχειριστές ενημερώνουν τις ζώνες αυτού και οι υπόλοιποι παίρνουν αντίγραφο από αυτόν.

Τύποι DNS Διακομιστών

- Ένας nameserver μπορεί να υλοποιεί ταυτόχρονα διαφορετικούς ρόλους.

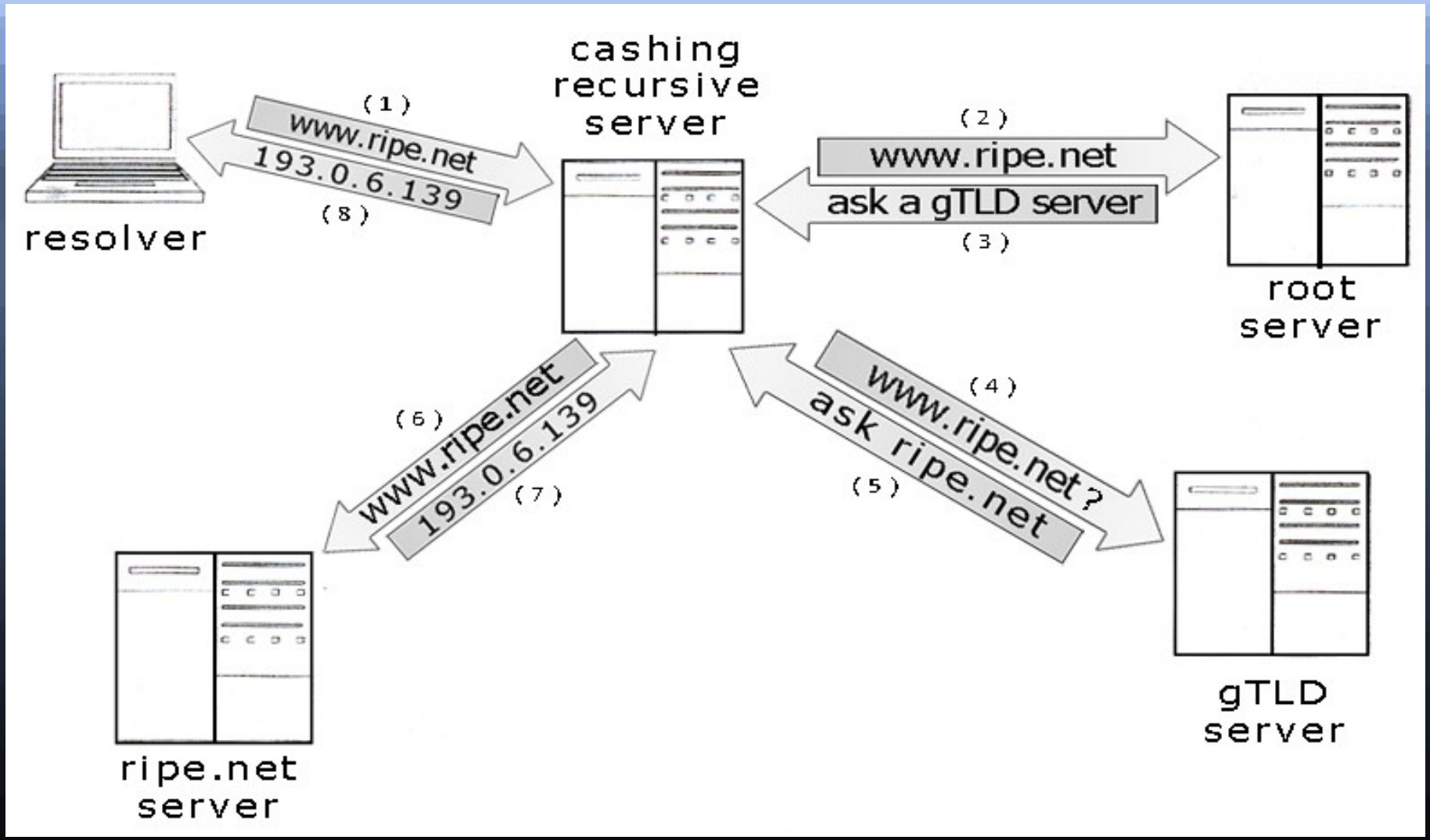
π.χ. Μπορεί να είναι master για κάποιες ζώνες, slave για κάποιες άλλες και να κάνει caching των πληροφοριών που μαθαίνει από άλλους nameservers.

Ερωτήσεις & Απαντήσεις

Όταν ένας nameserver δέχεται ερώτηση (query) τότε:

- Μπορεί να γνωρίζει την απάντηση, οπότε θα απαντήσει,
  - είναι authoritative για το όνομα χώρου ή
  - έχει την πληροφορία στην cache.
- Δεν γνωρίζει την απάντηση, οπότε
  - Προσπαθεί να βρει την απάντηση εκ μέρους του πελάτη (recursion available) ή
  - Εάν δεν επιτρέπεται η αναδρομική αναζήτηση, ανακατευθύνει σε πιο κοντινούς nameservers (referrals), που μπορεί να είναι οι authoritative.

Ερωτήσεις & Απαντήσεις

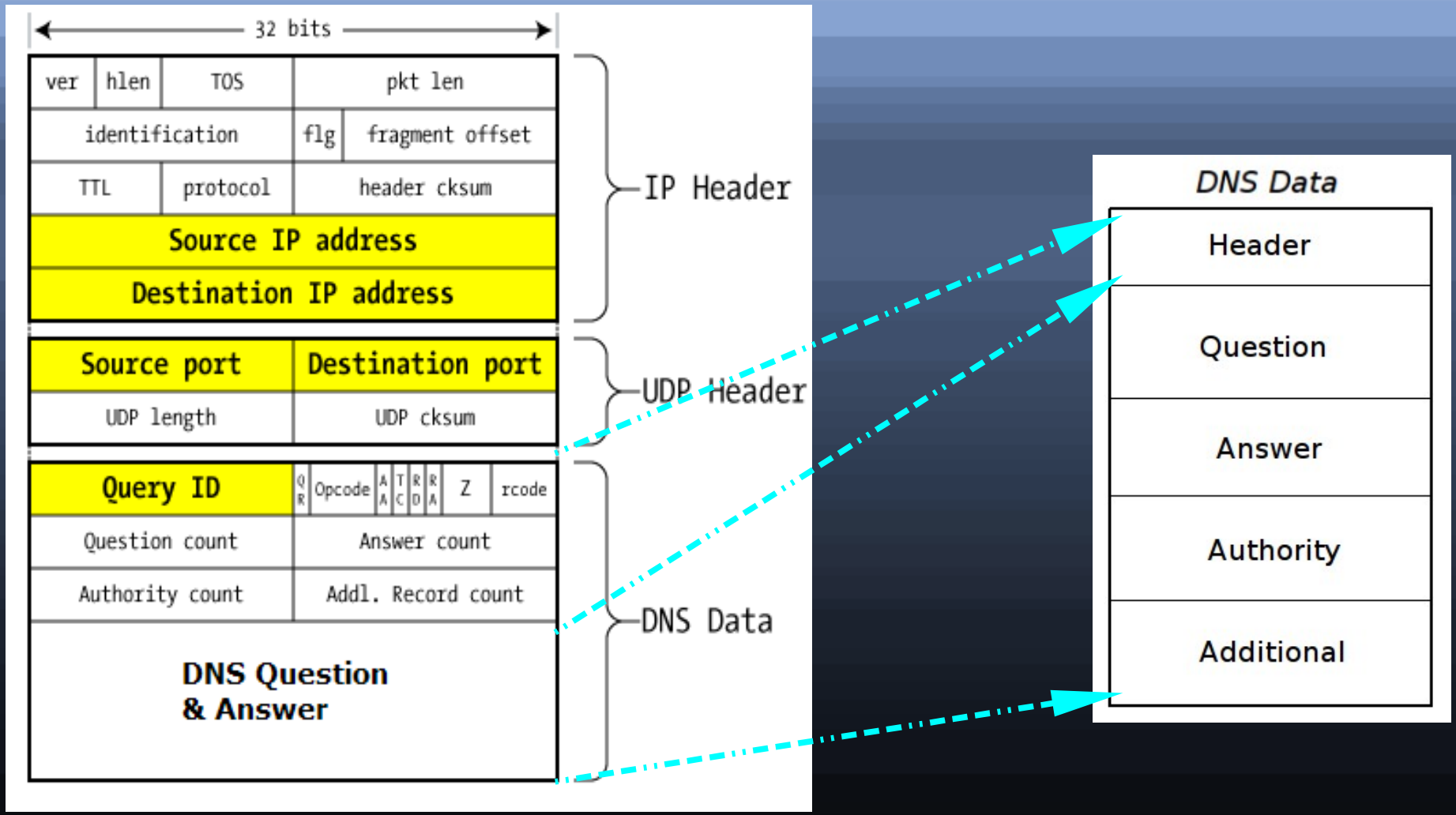


Η διαδικασία της επίλυσης (resolution)

Recursive queries

- Είναι οι ερωτήσεις που ζητούν από τον nameserver να πραγματοποίησει αναδρομική αναζήτηση, recursion.
  - Δηλαδή να βρει την απάντηση ξεκινώντας από τους root και καταλήγωντας στον authoritative.
- Οι πελάτες που διενεργούν μόνο recursive queries καλούνται stub resolvers.
- Πρέπει η παραμετροποίηση του nameserver να επιτρέπει την αναδρομική αναζήτηση, διαφορετικά τα recursive queries δεν γίνονται δεκτά (“WARNING: recursion requested but not available”).
- Τα non-recursive queries καλούνται iterative.

Μορφή DNS Πακέτου



Σημασία του DNS στο Διαδίκτυο

- Οι χρήστες απομνημονεύουν ονόματα και όχι νούμερα.
- Όλες οι ηλεκτρονικές υπηρεσίες (www, email, ftp etc) χρησιμοποιούν το DNS (MX records, URLs).
- Η ανάστροφη αντιστοίχιση (reverse mapping, IP σε όνομα) πολλές φορές εφαρμόζεται σαν ένας τρόπος πιστοποίησης ταυτότητας.
- Χρησιμοποιείται από υποστηρικτικές υπηρεσίες όπως DNSBL, SIP (VoIP) και αλλού. Πιο πρόσφατο παράδειγμα είναι το Sender Policy Framework (SPF).

Σημασία του DNS στο Διαδίκτυο

- Στο RFC 2915 ορίζεται το Naming Authority Pointer (NAPTR) που επιτρέπει την αντιστοίχιση ονομάτων χώρου σε οποιοδήποτε αναγνωριστικό (ID).
- Στα RFC 3401 και 3761 ορίζεται το ENUM (E.164 NUmber Mapping) που αντιστοιχεί τηλεφωνικά νούμερα σε URIs, IP και e-mail διευθύνσεις.
  - "It's really just a question of figuring out how to use the DNS - it's ready to carry arbitrary identifiers", Paul Mockapetris.

Τι θα γίνει αν ..... ;

" If the DNS doesn't work, the Internet doesn't work"

Alan Clegg, ISC

Web presentation, REN-ISAC

30-10-2008

Θέματα Ασφάλειας του DNS

Κίνδυνοι για το DNS της Επιχείρισης

Κινδυνεύουν:

- Η Διαθεσιμότητα της DNS υπηρεσίας: επηρεάζει την λειτουργία των υπηρεσιών Διαδικτύου (web, e-mail), την εργασία των χρηστών.
  - Κινδυνεύει η παρουσία της Επιχείρισης στο Διαδίκτυο.
- Οι Πληροφορίες που περιέχονται στο DNS: η εσκεμμένη αλλοίωση οδηγεί σε ανακατεύθυνση σε διακομιστές υπό τον έλεγχο κακόβουλων τρίτων
  - Κινδυνεύουν οι υπάλληλοι και συνεργάτες της Επιχείρισης.

Είδη Απειλών: Αλλοίωση DNS Πληροφορίας

- Αλλοίωση Authoritative Δεδομένων
  - Λάθη παραμετροποίησης (μείωση ασφάλειας διακομιστή)
  - Δυναμικές ενημερώσεις
  - Προβλήματα Λογισμικού/Εφαρμογής (ευπάθεια σε επιθέσεις)
- Αλλοίωση Προσωρινών Δεδομένων
  - DNS Cache Poisoning: "Μόλυνση" cache με δεδομένα που ανακατευθύνουν σε υπηρεσίες υπό τον έλεγχο των επιτιθεμένων.
  - DNS Spoofing: Εξαπάτηση χρησιμοποιώντας ψεύτικα στοιχεία ταυτοποίησης.

Είδη Απειλών: Διαθεσιμότητα DNS Πληροφορίας

- Προβλήματα Λογισμικού/Εφαρμογής: Προβλήματα του λογισμικού του διακομιστή (πχ BIND) προκαλούν αστοχία της DNS υπηρεσίας ή/και ευπάθεια σε επιθέσεις.
- Denial of Service επιθέσεις: στοχεύουν στην αδυναμία εξυπηρέτησης μέσω εξάντληση πόρων (υπολογιστικών, δικτύου)
  - DNS Amplification Attack (DNS Reflector Attack)

Αδυναμίες DNS Πρωτόκολλου

- Οι επιθέσεις αλλοίωσης των προσωρινών (cached) δεδομενων εκμεταλλεύονται αδυναμίες του DNS πρωτοκόλλου.
  - Δηλαδή στον τρόπο που λειτουργεί το DNS.
- Το DNS δημιουργήθηκε στα πρώτα χρόνια του Internet.
  - Τότε δεν υπήρχαν θέματα εμπιστοσύνης
- Έχουν ανακαλυφθεί αδυναμίες και ελλείψεις του αρχικού πρωτοκόλλου
  - Νέες πρακτικές, νέα RFC.
  - π.χ. Μετά από DNS Reflector Attack σε hosting εταιρεία το 2009, η επιστροφή referrals θεωρείται επικίνδυνη

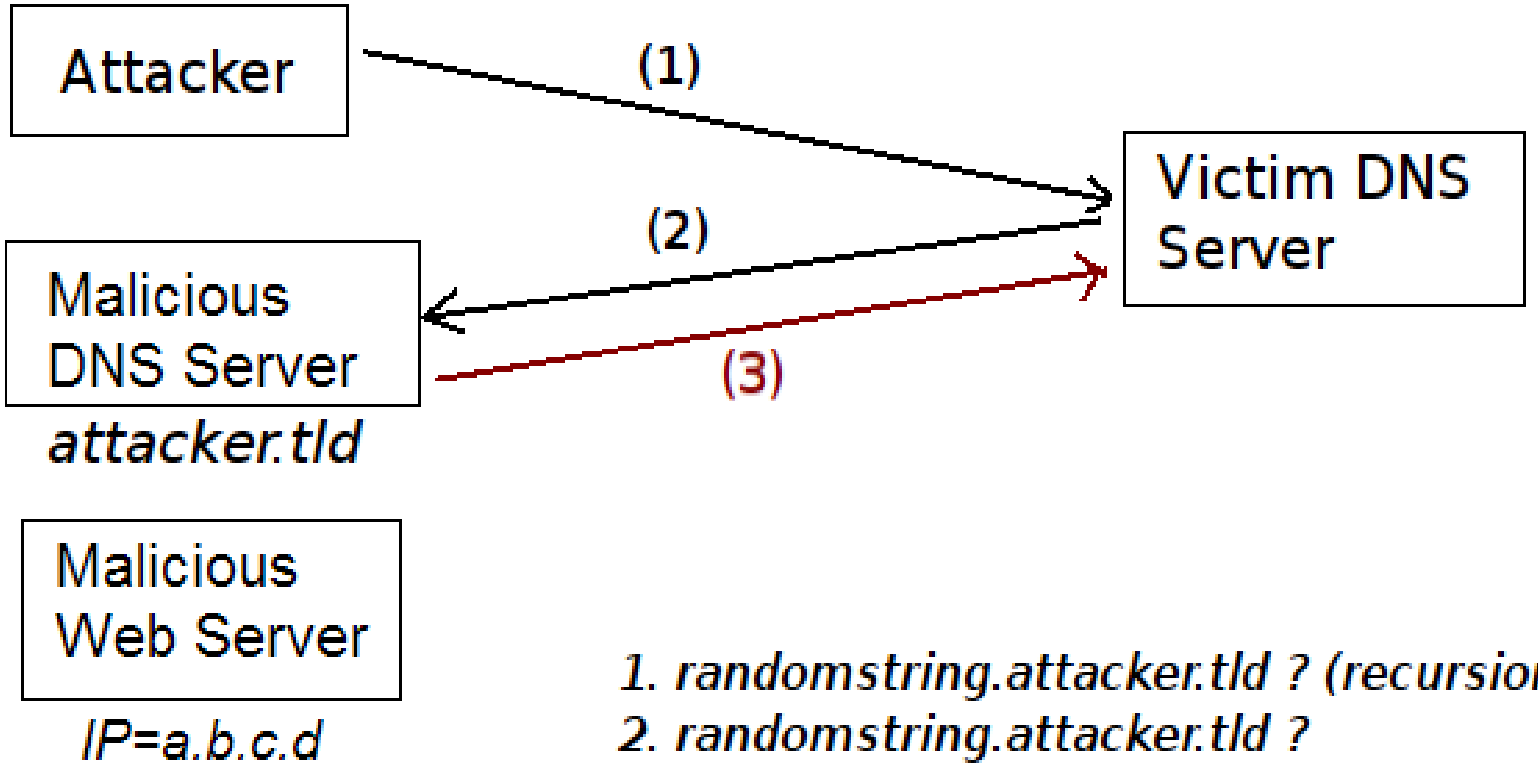
(https://www.dns-oarc.net/oarc/articles/upward-referrals-considered-harmful).

DNS Cache Poisoning

Unrelated data Attack: Η πρώτη που παρουσιάστηκε και η πιο απλή.

1. Ο επιτιθέμενος ρωτάει το DNS διακομιστή θύμα για ανύπαρκτο όνομα σε domain που ελέγχει ο επιτιθέμενος. Χρησιμοποιεί recursive query.
2. Ο διακομιστής θύμα αναγκάζεται να ρωτήσει τον DNS διακομιστή υπεύθυνο για το όνομα, δηλαδή τον DNS διακομιστή του επιτιθέμενου.
3. Στην απάντηση που θα δώσει ο απομακρυσμένος DNS διακομιστής, ο επιτιθέμενος θα προσθέσει (ADDITIONAL Section) την πληροφορία που θέλει να εισάγει στην cache του θύματος.

DNS Cache Poisoning



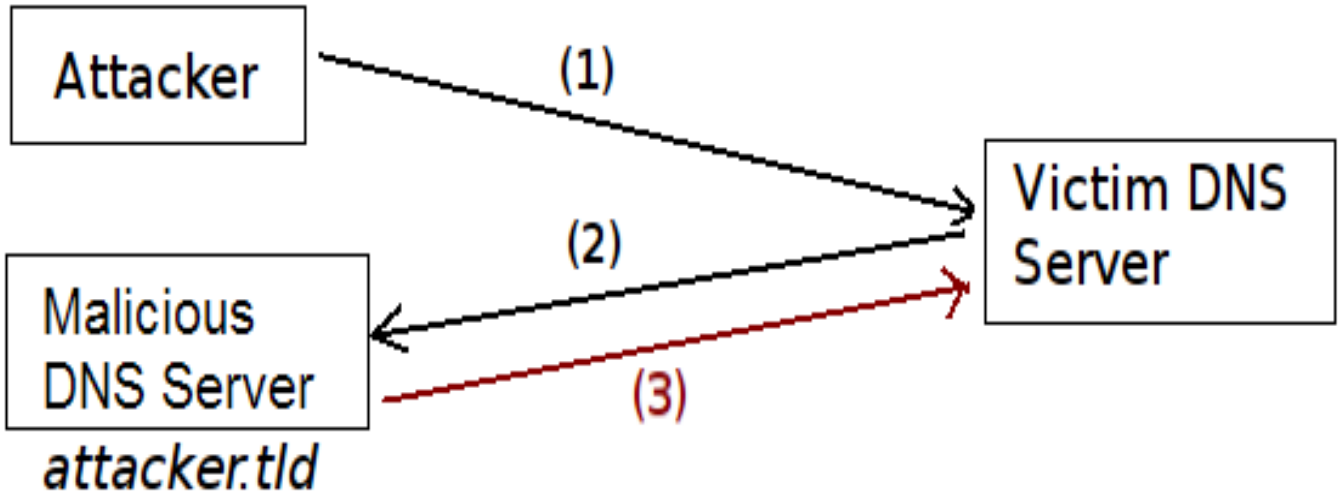
1. *randomstring.attacker.tld ? (recursion desired)*
2. *randomstring.attacker.tld ?*
3. *randomstring.attacker.tld -> x.y.w.z*
   + www.somebigbank.com -> a.b.c.d

DNS Cache Poisoning

Related data Attack: Παρόμοια με την πρώτη, αλλάζει η πληροφορία στο ADDITIONAL Section.

1. Ο επιτιθέμενος ρωτάει το DNS διακομιστή θύμα για ανύπαρκτο όνομα σε domain που ελέγχει ο επιτιθέμενος. Χρησιμοποιεί recursive query.
2. Ο διακομιστής θύμα αναγκάζεται να ρωτήσει τον DNS διακομιστή υπεύθυνο για το όνομα, δηλαδή τον DNS διακομιστή του επιτιθέμενου.
3. Η ψευδή πληροφορία είναι τύπου CNAME (alias), MX (mail exhanger), NS (nameserver) και άρα σχετίζεται με την ερώτηση.

DNS Cache Poisoning



1. *randomstring.attacker.tld ? (recursion desired)*
2. *randomstring.attacker.tld ?*
3. *randomstring.attacker.tld -> x.y.w.z*
   + www.somebigbank.com CNAME randomstring.attacker.tld

DNS Cache Poisoning

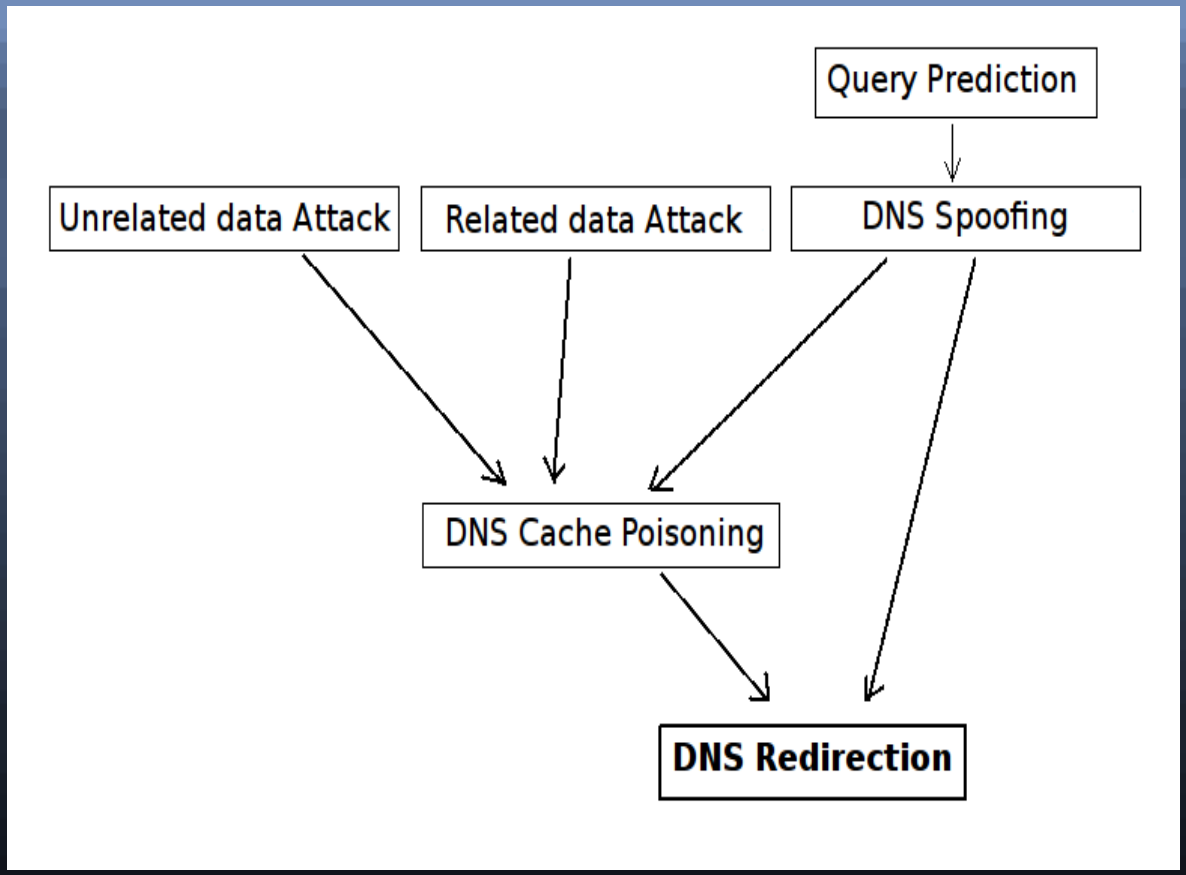
- **Αντιμετώπιση**
  - Unrelated data attack: Απαγορεύτηκε η παρουσία δεδομένων στο ADDITIONAL Section που δεν σχετίζονται με την ερώτηση.
  - Related data attack: Απαγορεύτηκαν τα “out-of-zone” δεδομένα στο ADDITIONAL Section.
- Αυτές οι επιθέσεις είναι παλιές και οι εν λόγω αδυναμίες έχουν καλυφθεί, αλλά.....
- Σε έρευνα που διεξαχθεί το 2005 (πριν το Kaminsky bug) από την εταιρεία “Measurement Factory”, το 84% των DNS servers παγκοσμίως πιθανολογείται ότι ευάλωτοι σε cache poisoning.

DNS Spoofing

Πρέπει ο επιτιθέμενος να μαντέψει α) το **Query ID** β) την **client UDP πόρτα** που χρησιμοποιεί το θύμα στις εξερχόμενες ερωτήσεις.

- Ο επιτιθέμενος στέλνει recursive queries στο διακομιστή θύμα,
- Ο διακομιστής θύμα πραγματοποιεί αναδρομική αναζήτηση,
- Όσο ο διακομιστής θύμα αναζητά την απάντηση, ο επιτιθέμενος προσπαθεί να μαντέψει το ID και την πόρτα στέλνοντας ψευδείς απαντήσεις.
- Παράλληλα, στέλνει χιλιάδες ερωτήσεις πλημμυρίζοντας το θύμα και αυξάνοντας τους χρόνους απόκρισης.

DNS Protocol Attacks



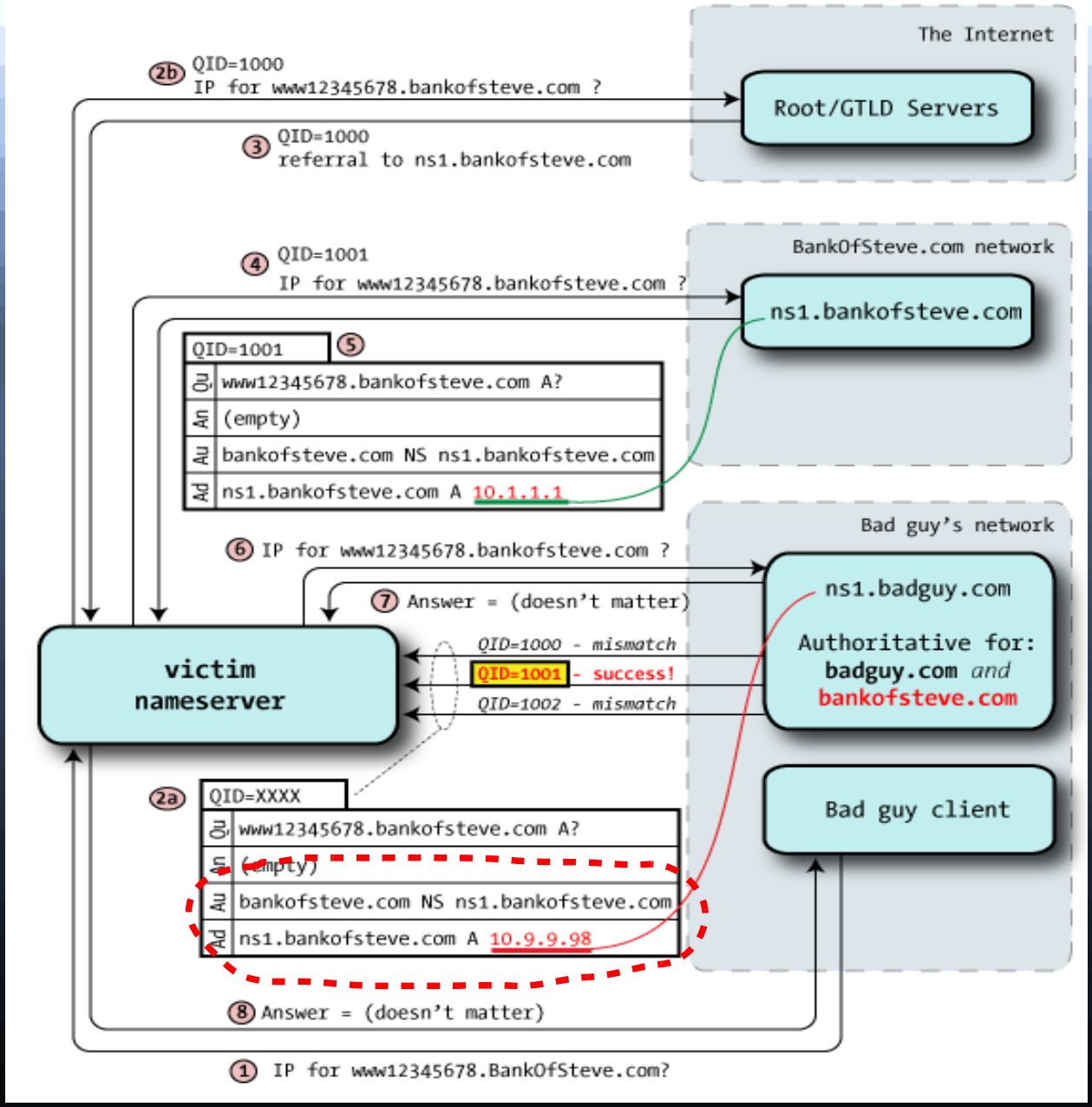
Οι επιθέσεις στο DNS Πρωτόκολλο βασίζονται στην εξυπηρέτηση recursive queries από τον DNS διακομιστή-στόχο.

Kaminsky bug (CVE-2008-1447)

- Τον Ιούλιο 2008, Ο Dan Kaminsky αποκάλυψε τεχνική DNS cache poisoning που επιτρέπει όχι απλά την ανακατεύθυνση μιας εγγραφή, αλλά ολόκληρης της ζώνης.
- Η τεχνική βασίζεται σε δύο γνωστές αδυναμίες του DNS:
  - Η UDP client πόρτα (χρησιμοποιείται στις εξερχόμενες ερωτήσεις) δεν αλλάζει.
  - Το 16-bit Query ID δεν είναι πάντα αρκετό.

Kaminsky bug (CVE-2008-1447)

- Η γενική αντίληψη ήταν ότι οι αδυναμίες αυτές δεν είναι τόσο σημαντικές γιατί:
  - Εάν ένα όνομα βρίσκεται ήδη στην cache, τότε δεν είναι δυνατό να μολυνθεί.
  - Εάν δεν είναι στην cache ή πλησιάζει το TTL, το παράθυρο επίθεσης είναι πολύ μικρό.
- Ο Dan Kaminsky έδειξε ότι ο επιτιθέμενος
  - ρωτώντας το θύμα ερωτήσεις για ανύπαρκτα ονόματα (άρα, όχι στην cache),
  - εξαναγκάζει το θύμα σε συνεχείς αναδρομικές αναζητήσεις,
  - όσο αυτός προσπαθεί να μαντέψει το Query ID.
  - Η επιτυχημένη προσπάθεια αλλάζει το IP του authoritative nameserver για το domain-στόχο.



http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

Denial of Service

- DNS Amplification/Reflector Attack
  - Ο επιτιθέμενος στέλνει recursive queries σε DNS διακομιστές (reflectors), αλλά με source IP αυτή του DNS θύματος.
  - Οι ερωτήσεις είναι ειδικά κατασκευασμένα ώστε προκαλούν απαντήσεις πολύ μεγαλύτερες από αυτές.
  - Το θύμα πλημμυρίζεται από μεγάλες απαντήσεις που ποτέ δεν ζήτησε.

Επικίνδυνες Ερωτήσεις

Είναι απαραίτητο να περιορίσουμε την έκθεση ενός nameserver σε recursive queries!

Ενίσχυση Ασφάλειας DNS

Αντιμετώπιση Απειλών

- **Split-Horizon DNS ή Split DNS**: Διαχωρισμός υπηρεσίας σε public DNS από private (internal) DNS.
- **DNS Functional Splitting ή Split-Service**: Διαχωρισμός nameservers βάσει ρόλου, advertising ή resolving.
- **Διασπορά Διακομιστών**: Διακομιστές σε διαφορετικά subnets, firewalls, διαφορετικό φυσικό χώρο.
- **Ποικιλία Σύνθεσης Διακομιστών**: Διαφορετικοί διακομιστές σε διαφορετικά λειτουργικά συστήματα, DNS λογισμικό.

Αντιμετώπιση Απειλών

- **Εφαρμογή DNSSEC**: πιστοποίηση ορθότητας δεδομένων μέσω κρυπτογραφίας.
- Διακομιστές **αφιερωμένοι** στην DNS υπηρεσία.
- Έγκαιρες **ενημερώσεις**, αναβαθμίσεις λογισμικού.
- **Θωράκιση** παραμετροποίησης:
  - Περιορισμός των zone transfers.
  - Περιορισμός των dymanic updates.
  - Απόκρυψη αριθμού έκδοσης λογισμικού.
  - Λειτουργία server από χρήστη με μειωμένα δικαιώματα.
  - Εφαρμογή chroot.

Αντιμετώπιση Απειλών

- Γενικότερα θέματα
  - Προστασία πίσω από firewall.
  - Λήψη αντιγράφων ασφαλείας.
  - Αδιάλειπτη τροφοδοσία.
  - Πλεονάζων υλισμικό.

Αντιμετώπιση Απειλών

- Για τον περιορισμό των Recursive Queries, εφαρμόζουμε:
  - **Split-Horizon**
  - **Functional Splitting**
- Χειρισμός recursive queries με μεγάλη ακρίβεια.

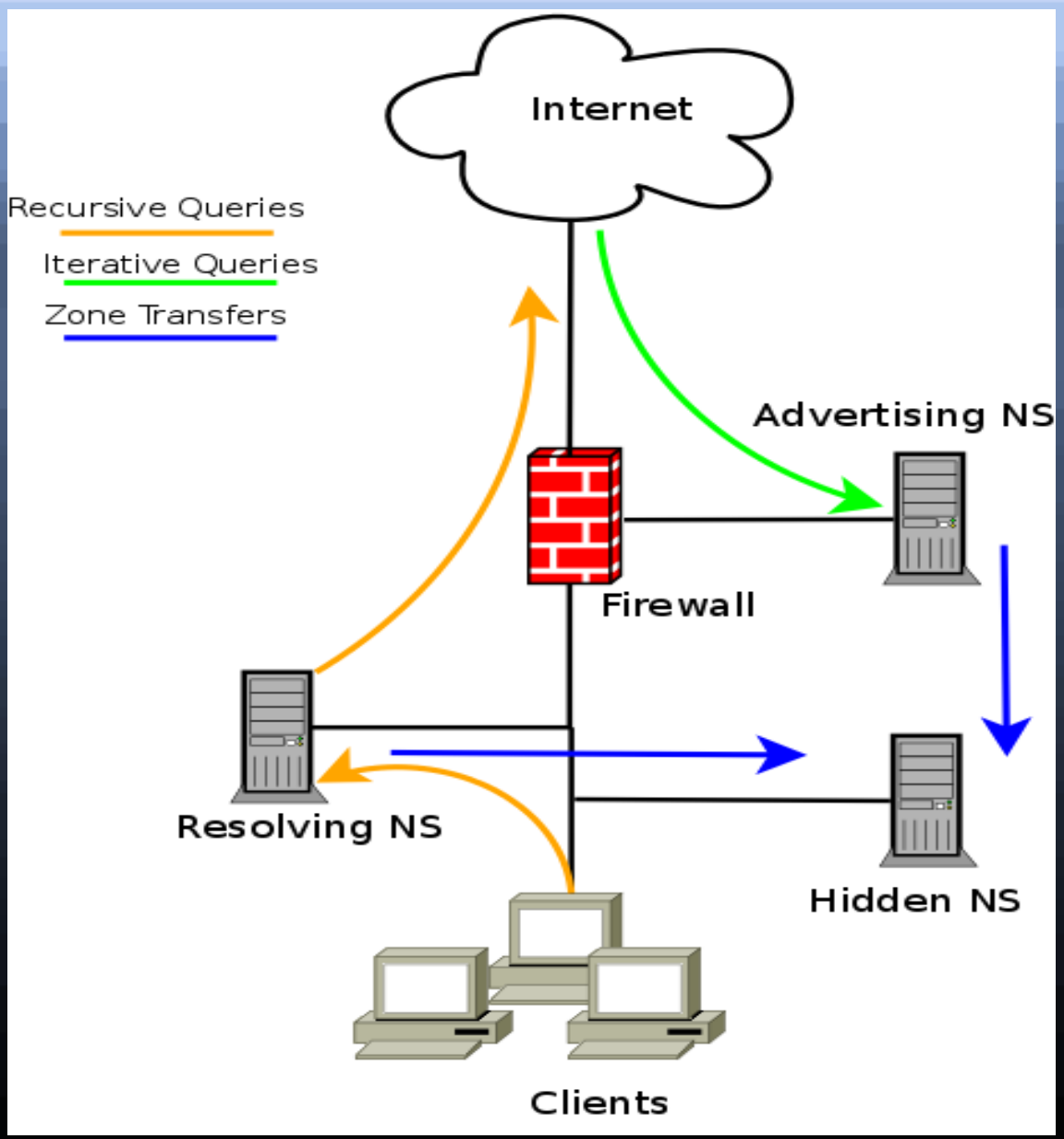
Split-Horizon DNS

- Τα εταιρικά δίκτυα που προστατεύονται από firewall χωρίζονται σε δύο μέρη:
  - Εσωτερικό δίκτυο: διακομιστές απομονωμένοι από το Διαδίκτυο - **private DNS**
  - Περιμετρικό δίκτυο: δημόσιες υπηρεσίες προσβάσιμες από το Διαδίκτυο - **public DNS**
- Στο private DNS περιέχονται:
  - Στοιχεία που δεν είναι επιθυμητό να εμφανίζονται εκτός εσωτερικού δικτύου.
  - Διακομιστές και υπηρεσίες που εμφανίζονται με διαφορετικό όνομα στο Διαδίκτυο.
- Η υλοποίηση μπορεί να γίνει α)Με διαφορετικές μηχανές, β) Με διαφορετικές ζώνες στην ίδια μηχανή γ) Μέσω παραμετροποίησης στην ίδια μηχανή (πχ BIND Views).

DNS Functional Splitting

- Ανάλογα με το ρόλο ενός DNS διακομιστή στο εταιρικό δίκτυο, διακρίνεται σε:
  - **Advertising Nameserver**: εξυπηρέτηση resolvers εκτός εταιρικού δικτύου.
  - **Resolving Nameserver**: εξυπηρέτηση resolvers εντός εταιρικού δικτύου.
- **Advertising Nameserver** – Authoritative για τις δημόσιες ζώνες, δεν εξυπηρετεί recursive queries, δεν κάνει caching, εξυπηρετεί queries μόνο από το Διαδίκτυο.
  - Hidden Authoritative: Master όλες τις ζώνες, slave σε αυτόν οι Advertising και Resolving servers.
- **Resolving Nameserver** – Authoritative για τις ιδιωτικές ζώνες, εξυπηρετεί (recursive) queries μόνο από το εσωτερικό δίκτυο, κάνει caching.

Splitting σε Δράση



DNSSEC

- Τα δεδομένα των απαντήσεων συνοδεύονται από ψηφιακές υπογραφές που πιστοποιούν την εγκυρότητα τους.
- Εφαρμόζεται μόνο στην διαδικασία επίλυσης ονομάτων (όχι σε dynamic updates, zone transfers).
- Στόχοι:
  - Η διαλειτουργία στην υπάρχουσα υποδομή
  - Σταδιακή μετάβαση.

DNSSEC

- Βασίζεται σε κρυπτογραφία δημόσιου κλειδιού (ασύμμετρη κρυπτογραφία).
  - Οι εγγραφές υπογράφονται μία προς μία με ιδιωτικό κλειδί.
  - Το δημόσιο κλειδί δημοσιεύεται στην ζώνη.
  - Το δημόσιο κλειδί χρησιμοποιείται στην επικύρωση της υπογραφής και συνεπώς τα DNS δεδομένα.
- Βασίζεται σε chains-of-trust: σε κάθε γονική ζώνη περιέχεται το δημόσιο κλειδί της θυγατρικής ζώνης, πιστοποιώντας έτσι το εν λόγω κλειδί σαν το σωστό κλειδί.
  - Στην κορυφή κάθε αλυσίδας βρίσκεται ο trust anchor.
  - Ιδανικά, αυτός θα είναι στην root ζώνη.

DNSSEC

- Στις 21 Ιουλίου 2008, το .ORG gTLD ανακοίνωσε την σταδιακή εφαρμογή του DNSSEC.
- Στις 28 Αυγούστου 2008, ανακοινώθηκε η εφαρμογή στο .GOV gTLD.
- Στην Ευρώπη, η Σουηδία ξεκίνησε πρώτη την υπογραφή του .SE στα τέλη 2005. Ακολούθησαν Τσεχία, Πούερτο Ρίκο και η Βουλγαρία. Εκτός Ευρώπης, η Βραζιλία έχει ολοκληρώσει την υπογραφή.
- Η ENISA προωθεί την χρήση του DNSSEC στα πλαίσια του θεματικού προγράμματος “Improving resilience in European e-Communication networks”.
- 1η Δεκεμβρίου 2009, ξεκίνησε η υπογραφή της root ζώνης από ICANN και VeriSign με την υποστήριξη του U.S. Department of Commerce.

Berkeley Internet Name Daemon (BIND)

BIND, η εφαρμογή

- Ξεκίνησε σαν μέρος του BSD-Unix project στο University of California, Berkeley το 1984 από 4 φοιτητές.
- Μέχρι την έκδοση BIND 4.8.3, αναπτυσσόταν από το UC.
- Οι εκδόσεις 4.9 και 4.9.1 αναπτύχθηκαν στην DEC. Τότε ανέλαβε ο Paul Vixie, ιδρυτής του Internet Software Consortium.
- Οι εκδόσεις 4.9.3 και έπειτα, αναπτύσσονται και συντηρούνται από το μη κερδοσκοπικό οργανισμό ISC.

BIND, η εφαρμογή

- Εκδόσεις
  - 1984: BIND 4, η πρώτη
  - 1997: BIND 8, κώδικας μερικώς ξαναγραμμένος
  - 2000: BIND 9, κώδικας γραμμένος από την αρχή
  - 2009: BIND 10 beta, κώδικας μερικώς ξαναγραμμένος, 5χρόνο project.
- Οι εκδόσεις 4 και 8 είναι επίσημα deprecated.
- BIND 9.7 είναι η πιο πρόσφατη έκδοση.

BIND, η εφαρμογή

Απαιτήσεις σε Υλισμικό

- CPU
  - Δεν ιδιαίτερα απαιτητικό σε υπολογιστική ισχύ.
  - Εξαρτάται και από τον αριθμό των ζωνών.
  - Η ενεργοποίηση DNSSEC προσθέτει φόρτο.
- Μνήμη
  - Είναι πιο σημαντική στους caching διακομιστές.
  - Πρέπει να είναι αρκετή για να χωράνε οι ζώνες και η cache.

Η Άδεια Χρήσης του ISC

- Το λογισμικό που αναπτύσει ο ISC εκδίδεται με την εξής άδεια χρήσης:
  - *Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.*
- Η άδεια χρήσης είναι εγκεκριμένη από το Open Source Initiative.

Παραμετροποίηση BIND

- Εξ' ορισμού, το αρχείο ρυθμίσεων είναι το “named.conf”.
  - Το που βρίσκεται στο σύστημα αρχείων εξαρτάται από το λειτουργικό σύστημα.
  - Μπορεί να αλλάξει όταν κτίζεται από τον πηγαίο κώδικα.
- Η σύνταξή του τεκμηριώνεται στο ARM (Administrator's Reference Manual)

  http://www.isc.org/software/bind/documentation

named.conf

- Χωρίζεται σε τμήματα (sections)
  - Κάθε τμήμα αφόρα συγκεκριμένο σύνολο ρυθμίσεων (π.χ. Logging)
- Στο αρχείο επιτρέπονται σχόλια σε οποιοδήποτε σημείο. Υποστηρίζεται σύνταξη C, C++ και perl/shell.

```
/* This is a BIND comment as in C */
// This is a BIND comment as in C++
# This is a BIND comment as in UNIX shells
# and perl
```

named.conf

acl	defines a named IP address matching list, for access control and other uses.
controls	declares control channels to be used by the rndc utility.
include	includes a file.
key	specifies key information for use in authentication and authorization using TSIG.
logging	specifies what the server logs, and where the log messages are sent.
lwres	configures named to also act as a light-weight resolver daemon (lwresd).
masters	defines a named masters list for inclusion in stub and slave zone masters clauses.
options	controls global server configuration options and sets defaults for other statements.
server	sets certain configuration options on a per-server basis.
trusted-keys	defines trusted DNSSEC keys.
view	defines a view.
zone	defines a zone.

named.conf

- Τα sections ολοκληρώνονται με ελληνικό ερωτηματικό (semicolon) και οι παράμετροι εσωκλείωνονται σε αγκυλωτες παρενθέσεις. Οι παράμετροι διαχωρίζονται με semicolon.
  - Για παράδειγμα:

```
options {
   directory “/etc/bind”;
   recursion yes;
   listen-on-v6 { any; };
};
```

- Οι περισσότεροι παράμετροι έχουν προκαθορισμένες τιμές, όποτε ορίζουμε μόνο αυτές που αλλάζουν.

named.conf - Options

- options { };
  - Παράμετροι που επηρεάζουν την λειτουργία του BIND.
  - Παράμετροι που επηρεάζουν όλες τις ζώνες.
- Μερικές χαρακτηριστικές:

```
directory “/etc/bind”;
port 53;
memstatistics-file “path/to/file”;
notify yes;
recursion no;
forward [first|only];
forwarders { 1.2.3.4; 4.3.2.1};
allow-query { any; };
allow-recursion { 1.2.3.0/24; };
listen-on { 5.6.7.8; };
```

named.conf - Logging

- logging { };
  - Τι καταγράφεται, πόσο και που.
- Η καταγραφή βοηθάει στην ανάδειξη προβλημάτων στην παραμετροποίηση και προβλημάτων άλλων διακομιστών.
- Η καταγραφή γινεται σε “channels”.
  - Υπάρχουν 4 προκαθορισμένα channels.
- Τα μηνύματα που καταγράφονται είναι ομαδοποιημένα σε προκαθορισμένες κατηγορίες
  - πχ default, config, security, update

named.conf - Logging

- Παράδειγμα νέου channel:

```
logging {
   channel config_log {
        file “/var/log/named/config.log”;
        versions 3;
        size 10m;
        print-time yes;
        print-category yes;
   };
   category config { config_log; };
};
```

named.conf - Zone

- zone { };
  - Δηλώσεις των ζωνών για τις οποίες είναι authoritative ο διακομιστής
  - Παράμετροι σχετικές με τις ζώνες αυτές, υπερισχύουν των αντίστοιχων στο options { };
- Ορίζεται ο τύπος της ζώνης, που βρίσκεται η ζώνη.
  - master
  - slave
  - hint, ζώνη που περιέχει τους root nameservers
  - forward, προώθηση ερωτήσεων

named.conf - Zone

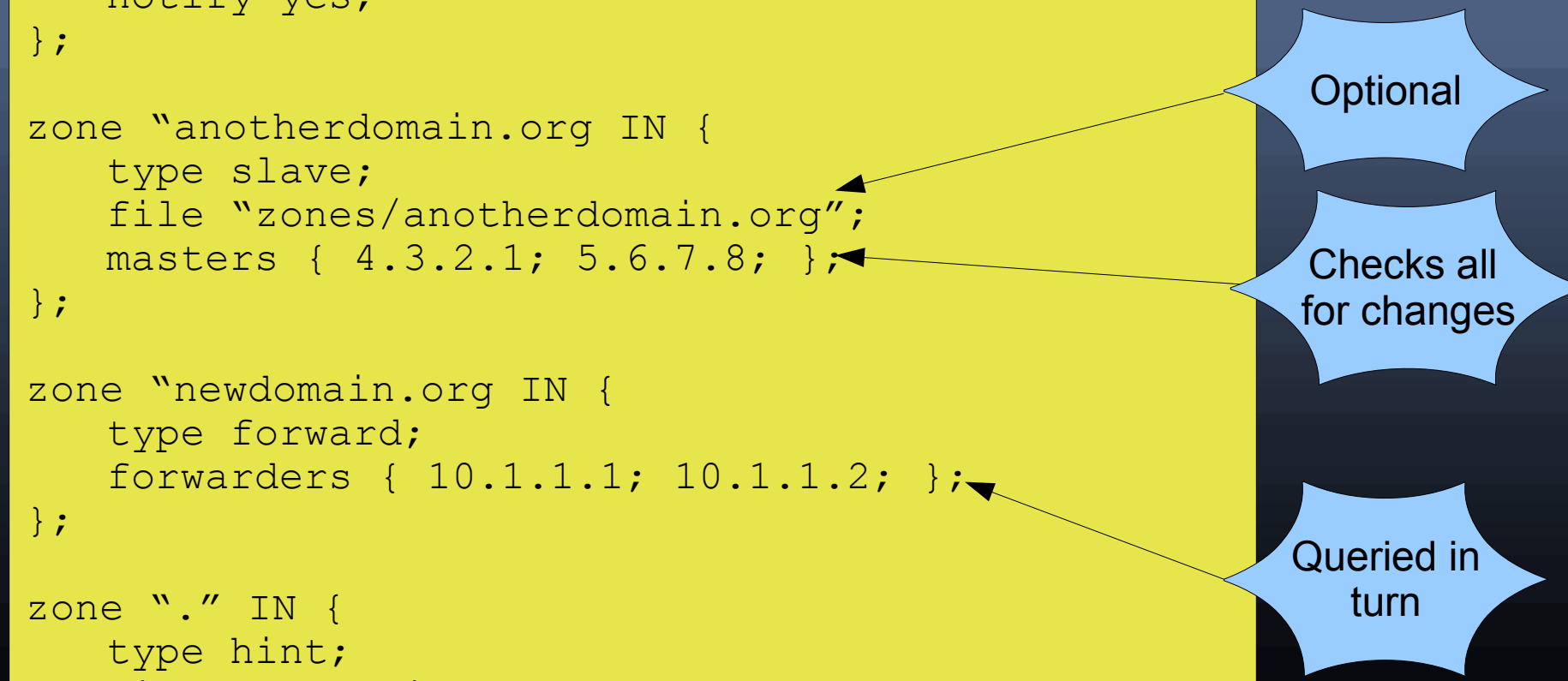
- Παραδείγματα:

```
zone "somedomain.org" IN {
    type master;
    file "zones/somedomain.org";
    allow-transfer { 1.2.3.4; };
    notify yes;
};

zone "anotherdomain.org IN {
    type slave;
    file "zones/anotherdomain.org";
    masters { 4.3.2.1; 5.6.7.8; };
};

zone "newdomain.org IN {
    type forward;
    forwarders { 10.1.1.1; 10.1.1.2; };
};

zone "." IN {
    type hint;
    file "root.hints";
};
```



named.conf - ACLs

- acls { };
  - Αποδίδει όνομα σε λίστα IP διευθύνσεων για χρήση σε έλεγχους πρόσβασης.
  - Προκαθορισμένα ονόματα: any, none, localhost, localnet.
- Παράδειγμα:

```
acl recursion_list {
   localhost;
   192.168.1.0/24;
};

acl transfer_list {;
   none;
};
options {
   allow-recursion { recursion_list; }; };
```

named.conf - INCLUDE

- include <filename>;
  - Συμπεριλαμβάνει τα περιεχόμενα ενός αρχείου στο τρέχων.
- Σε περίπτωση πολύπλοκης παραμετροποίησης με πολλές ζώνες, βοηθάει στην μείωση του συνολικού όγκου – διαχωρισμός ρυθμίσεων σε επιμέρους αρχεία.
  - Κάποιες διανομές GNU/Linux (πχ Debian) εφαρμόζουν αυτή τη λογική στο εγκατεστημένο BIND.

Εργαλεία Διαχείρισης και Αποσφαλμάτωσης BIND

- dig
  - Διαγνωστικό εργαλείο για το DNS.
- named-checkconf
  - Έλεγχει το συντακτικό της παραμετροποίησης του διακομιστή.
- named-checkzone
  - Έλεγχει το συντακτικό των ζωνών.
- named-compilezone (BIND 9.4)
  - Μετατρέπει τη ζώνη σε μορφή “raw” (binary) & πιο αυστηρούς ελέγχους από named-checkzone.

Εργαλεία Διαχείρισης και Αποσφαλμάτωσης BIND

- rndc
  - Εργαλείο ελέγχου και διαχείρισης του BIND.
  - Βρίσκεται στην διανομή του BIND9.
  - Δυνατότητα απομακρυσμένης διαχείρισης.
  - Επικοινωνεί με το BIND μέσω TCP στην πόρτα 953.
  - Πραγματοποίεται αυθεντικοποίηση μεταξύ rndc και BIND.

Εργαλεία - dig

- Μέρος της διανομής BIND9.
- Πολύ ισχυρό, αυτόνομο διαγνωστικό εργαλείο.
- Αντικαθιστά το “nslookup”.

```
kmag@lab:~$ dig @nic.grnet.gr www.ripe.net

; <<>> DiG 9.4.2-P2.1 <<>> @nic.grnet.gr www.ripe.net
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19419
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 8

;; QUESTION SECTION:
;www.ripe.net.                  IN      A

;; ANSWER SECTION:
www.ripe.net.           107697  IN      A       193.0.6.139
```

Εργαλεία – dig (συνέχεια)

```
;; AUTHORITY SECTION:
ripe.net.               105045  IN      NS      ns3.nic.fr.
ripe.net.               105045  IN      NS      sns-pb.isc.org.
ripe.net.               105045  IN      NS      sunic.sunet.se.
ripe.net.               105045  IN      NS      ns-pri.ripe.net.

;; ADDITIONAL SECTION:
sunic.sunet.se.         18650   IN      A       192.36.125.2
sunic.sunet.se.         18650   IN      AAAA    2001:6b0:7::2
sns-pb.isc.org.         18803   IN      A       192.5.4.1
sns-pb.isc.org.         28971   IN      AAAA    2001:500:2e::1
ns-pri.ripe.net.        105047  IN      A       193.0.0.195
ns-pri.ripe.net.        45635   IN      AAAA
2001:610:240:0:53::3
ns3.nic.fr.             105042  IN      A       192.134.0.49
ns3.nic.fr.             105042  IN      AAAA
2001:660:3006:1::1:1

;; Query time: 3 msec
;; SERVER: 194.177.210.210#53(194.177.210.210)
;; WHEN: Thu May 13 10:16:17 2010
;; MSG SIZE  rcvd: 323
```

Εργαλεία - rndc

- Η παραμετροποίηση του rndc γίνεται με το “rndc-confgen”
  - Παράγει συμμετρικό κλειδί για την αυθεντικοποίηση
- rndc-confgen
  - Δημιουργεί αρχείο rndc.key (παράμετρος “-a”)

    ή
  - Παράγει τη γραμμογράφηση του “rndc.conf” και του “named.conf” (περίπτωση απομακρυσμένης διαχείρισης).

Εργαλεία - rndc

```
kmag@mydns:/etc/bind$ sudo rndc-confgen
# Start of rndc.conf
key "rndc-key" {
        algorithm hmac-md5;
        secret "baCyLFl1/OBizyneNVvxMQ==";
};

options {
        default-key "rndc-key";
        default-server 127.0.0.1;
        default-port 953;
};
# End of rndc.conf

# Use with the following in named.conf, adjusting the allow list
# as needed:
# key "rndc-key" {
#       algorithm hmac-md5;
#       secret "baCyLFl1/OBizyneNVvxMQ==";
# };
#
# controls {
#       inet 127.0.0.1 port 953
#               allow { 127.0.0.1; } keys { "rndc-key"; };
# };
# End of named.conf
```

Εργαλεία - rndc

- Απομακρυσμένη χρήση

```
kmag@ns1:/etc/bind$ sudo more named.conf
key "ns1-key" {
        algorithm hmac-md5;
        secret "sfjljSAdfFJO/Jioaloi==”};
};

controls {
      inet 127.0.0.1 port 953
              allow { 127.0.0.1; } keys { "rndc-key"; };
      inet 192.168.1.1 port 953
              allow { 10.1.1.1; } keys { “ns1-key”; };
};
```

```
kmag@remotePC:/etc/bind$ sudo more rndc.conf
key "ns1-key" {
        algorithm hmac-md5;
        secret "sfjljSAdfFJO/Jioaloi==”};
};

server ns1.lab.org {
         keys { “ns1-key”; };
};
kmag@remotePC:/etc/bind$ sudo rndc -s ns1.lab.org reload
```

Εργαλεία - rndc

- Εντολές rndc
  - rndc stop: kill server
  - rndc status: show information
  - rndc stats: generate statistics file
  - rndc reconfig: re-read configuration
  - rndc reload: reload configuration file and zones
  - rndc reload <zone>: reload a zone
  - rndc trace: increase debug level
  - rndc flush: clear cache data

Θώρακιση Παραμετροποίησης BIND

- Διασφάλιση zone transfers
- Διασφάλιση dynamic updates
- Απόκρυψη έκδοσης
- Εφαρμογή chroot
- No root user

Διασφάλιση Zone Transfers

- Περιορισμός πρόσβασης

```
acl transfer_list {;
      1.2.3.4;
      1.3.3.5;
   };

options {
   allow-transfer { none; };
};

zone “somedomain.org” IN {
   type master;
   file “zones/somedomain.org”;
   allow-transfer { transfer-list; };
   notify yes;
};
```

Global, for all zones

Takes precedence

Διασφάλιση Zone Transfers

- Πιστοποίηση επικοινωνίας: TSIG
  - Χρησιμοποιείται στην υπογραφή των zone transfers, dynamic updates και queries.
- Ρύθμιση TSIG:
  - Παραγωγή συμμετρικού κλειδιού με την εντολή dnssec-keygen.
  - Προσθήκη του κλειδιού στην παραμετροποίηση των δύο authoritative.
  - Αντιστοίχιση διακομιστή-κλειδιού στην παραμετροποίηση.

Διασφάλιση Zone Transfers

- Παραγωγή κλειδιού

```
kmag@ns1:/etc/bind$ dnssec-keygen -a HMAC-MD5 -b 128 -n HOST \
                                  -r /dev/urandom test.tsig
kmag@ns1:/etc/bind$ ls
Ktest.tsig.+157+59573.key
Ktest.tsig.+157+59573.private
```

- Το dnssec-gen παράγει πάντα δύο αρχεία, στην περίπτωση TSIG τα αρχεία έχουν την ίδια πληροφορία με άλλη μορφή.

```
kmag@ns1:/etc/bind$ more Ktest.tsig.+157+59573.key
test.tsig    IN    KEY    512 3 157 hSic89aco7cGXSAS8bgogDF==
```

Διασφάλιση Zone Transfers

- Εισαγωγή κλειδιού στον named.conf και αντιστοίχιση με τον απομακρυσμένο authoritative.

```
key "test.tsig" {
        algorithm hmac-md5;
        secret "hSic89aco7cGXSAS8bgogDF==”};
};

server 1.2.3.4 {
         keys { “test.tsig”; };
};
```

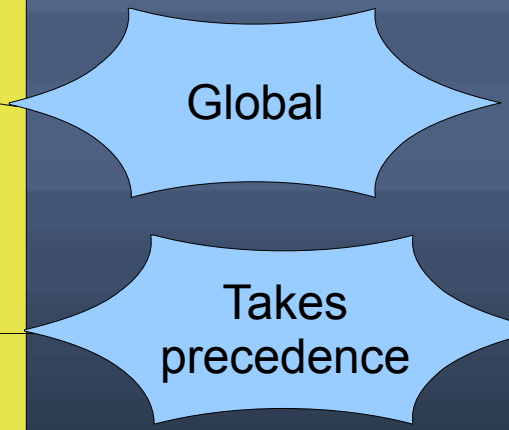
- Ρυθμίζουμε ομοίως στον απομακρυσμένο, το κλειδί πρέπει να έχει το ίδιο όνομα.
- Στο μέλλον, όλη η DNS κίνηση μεταξύ των δύο θα διακομιστών θα συνοδεύτεται από ψηφιακές υπογραφές.

Διασφάλιση Dynamic Updates

- Οι δυναμικές ενημερώσεις είναι εξ' ορισμού απενεργοποιημένες.

```
allow-update { none; };

zone "somedomain.org" IN {
   type master;
   file "zones/somedomain.org";
   allow-update { 1.2.3.0/24; };
   notify yes;
};
```



- Ο περιορισμός των ενημερώσεων βάσει IP δεν είναι καλή ιδέα, το UDP εύκολα πλαστογραφείται. TSIG!!

```
zone "somedomain.org" IN {
   type master;
   file "zones/somedomain.org";
   allow-update { key "test.tsig"; };
};
```

Θωράκιση, συνέχεια & τέλος

- Απόκρυψη έκδοσης λογισμικού.

```
options {
    ....
    version “Not Available”;
    ....
};
```

- Chroot & non-root user (παράδειγμα σε Debian)

```
kmag@ns1:/etc/default$ more bind9
OPTIONS="-u bind -t /var/lib/named"
```

- Ο χρήσης “bind” πρέπει να έχει δικαιώματα ανάγνωσης στα αρχεία ρυθμίσεων, master ζώνες και γραφής στα log, stats, slave ζώνες αρχεία.
- Στο jail - δομή αρχείων για την λειτουργία του BIND (null, random devices), ο syslogd να διαβάζει CHROOT/dev/log.

Παραμετροποίηση Split-DNS

view { };

- Δυνατότητα διαφορετικών απαντήσεων ανάλογα με το πηγή ή τον προορισμό της ερώτησης.
- Προσφέρει πολλαπλούς, παράλληλους, ανεξάρτητους χώρους ονομάτων (namespaces).

```
view "internal" {
    match-clients { 10.1.1.0/24; };
    zone "somedomain.org" IN {
        type master;
        file "somedomain.org.internal";
    };
...
};

view "external" {
    match-clients { !10.1.1.0/24; any; };
    zone "somedomain.org" IN {
        type master;
        file "somedomain.org.external";
    };
...
};
```

Παραμετροποίηση Split-DNS

- Το Split-DNS με τη χρήση Views είναι αρκετά πολύπλοκη διαδικασία.
  - Προσοχή στα zone transfers!
  - Κάθε ερώτηση πρέπει να ταιριάζει σε κάποιο View αλλίως απορρίπτεται.
  - Οι κοινές ζώνες πρέπει να δηλώνονται σε κάθε View.
- Πιο απλός τρόπος: διαφορετική ζώνη για κάθε περίπτωση, π.χ.
  - demokritos.gr, public zone
  - demokritos.local, private zone - περιορισμοί πρόσβασης μέσω παραμετροποίησης

Παραμετροποίηση Functional Splitting

- Advertising Nameserver
  - Όχι recursion
  - Όχι caching
  - Όχι transfers
  - Μόνο iterative queries.

```
options {
   recursion no;
   additional-from-cache no;
   allow-transfer { none; };
   allow-query { none; };
};

zone “somedomain.org” IN {
   type slave;
   masters { <Hidden NS IP>;};
   file “zones/somedomain.org”;
   allow-query { any; };
};
```

Παραμετροποίηση Functional Splitting

- Resolving Nameserver
  - Recursion μόνο εσωτερικά
  - Όχι transfers
  - Ενεργό Caching

```
options {
   recursion yes;
   allow-recursion { <priv_net>; };
   allow-query { <priv_net>; };
   allow-transfer { none; };
};

zone “somedomain.local” IN {
   type slave;
   masters { <Hidden NS IP>;};
   file “zones/somedomain.local”;
};
```

Παραμετροποίηση Functional Splitting

- Hidden Master Nameserver
  - Όχι recursion
  - Όχι caching
  - Transfers μόνο από Adv & Resolv NS
  - Queries μόνο από Adv & Resolv NS

```
options {
   recursion no;
   additional-from-cache no;
   notify yes;
   allow-transfer { <Adv_NS>;
                    <Resolv_NS>; };
   allow-query { <Adv_NS>;
                 <Resolv_NS>; };
};

zone "somedomain.org" IN {
   type master;
   file "zones/somedomain.org";
};

zone "somedomain.local" IN {
   type master;
   file "zones/somedomain.local";
};
```

Παραμετροποίηση Functional Splitting

- Hidden Master NS: Οι NS και SOA έγγραφες της δημόσιας ζώνης δείχνουν στον Advertising NS.

```
somedomain.org IN SOA adv-ns.somedomain.org.
                      hostmaster.somedomain.org.
                    ( 2009101002 86400 7200 604800 10800 }

somedomain.org IN NS adv-ns.somedomain.org
somedomain.org IN NS adv-ns.somedomain.org
```

BIND 9.7: “DNSSEC for Humans!”

- Πλήρως αυτοματοποιημένη υπογραφή ζωνών
  - Αν “dnssec-enable yes”, ο δαίμονας παράγει κλειδιά.
- Απλοποιημένα εργαλεία υπογραφής και συντήρησης εργαλείων (key-rollover).
- Πιο απλοποιημένη παραμετροποίηση των DNSSEC DLV.
- Αυτοματοποιημένη συντήρηση των trust anchors (RFC 5011).

Ευχαριστώ
για την υπομονή

http://islab.demokritos.gr/gr/html/parousiaseis/ellak2010-DNS_in_Business.pdf