Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Πρωτόκολλα Ασφάλειας για DNS Εξυπηρετητές**
Ονοματεπώνυμο Φοιτητή	**Μαρία Ιωάννου**
Πατρώνυμο	**Παύλος**
Αριθμός Μητρώου	**ΜΠΣΠ/08046**
Επιβλέπων	**Κωνσταντίνος Πατσάκης, Βαθμίδα**

Ημερομηνία Παράδοσης **Μήνας Έτος**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον Δόκτορα κύριο Κωνσταντίνο Πατσάκη, για την εμπιστοσύνη που μου έδειξε και τη βοήθεια και την καθοδήγηση που μου παρείχε.

Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου για τη συνεχή στήριξη τους στις σπουδές μου.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Το Σύστημα Ονοματοδοσίας Διευθύνσεων είναι ζωτικής σημασίας για το Διαδίκτυο, επειδή παρέχει έναν μηχανισμό για την ανάλυση των ονομάτων των κεντρικών υπολογιστών σε διευθύνσεις του πρωτόκολλου του Διαδικτύου. Η σωστή λειτουργία του συστήματος απειλήθηκε από μη ασφαλή πρωτόκολλα και από την έλλειψη του ελέγχου της ταυτότητας και της ακεραιότητας των πληροφοριών. Έχουν προταθεί κάποιες επεκτάσεις καθώς και πρωτόκολλα ασφάλειας που βελτιώνουν τα τρωτά σημεία του Συστήματος Ονοματοδοσίας των Διευθύνσεων. Αυτά τα θέματα ασφάλειας καθώς και τα πρωτόκολλα που έχουν προταθεί για την αντιμετώπισή τους παρουσιάζονται στην παρούσα διπλωματική εργασία.

The Domain Name System is vital for the Internet, because it provides a mechanism for resolving the host names into Internet Protocol (IP) addresses. The proper functionality of this system was threatened by insecure protocols and lack of authentication and information's integrity checking. Several security extensions and protocols which improve the Domain Name System (DNS) have been proposed. These security issues and the protocols that have been proposed are presented in this thesis.

ΚΕΦΑΛΑΙΟ 1. ΕΙΣΑΓΩΓΗ

Το Διαδίκτυο είναι μία ευρέως διαδεδομένη συσσώρευση εκατοντάδων χιλιάδων διασυνδεδεμένων ετερογενών δικτύων και υπολογιστών. Ο σχεδιασμός του βασίζεται σε μία ιεραρχία πρωτοκόλλων. Υπάρχουν πολλαπλές εφαρμογές αυτών των πρωτοκόλλων.

Οι υπολογιστές επικοινωνούν μεταξύ τους με διαφορετικούς τύπους διευθύνσεων: στο φυσικό επίπεδο χρησιμοποιώντας φυσικές διευθύνσεις χαμηλού επιπέδου όπως η διευθύνσεις της κάρτας Ethernet, στα επίπεδα σύνδεσης δεδομένων μέχρι και εφαρμογής χρησιμοποιώντας διευθύνσεις IP και στο επίπεδο εφαρμογής χρησιμοποιώντας υψηλού-επιπέδου, μνημονικά ονόματα κεντρικών υπολογιστών.

Ένα από τα καθήκοντα διαχείρισης στο Internet είναι η χαρτογράφηση των διευθύνσεων χαμηλότερου-επιπέδου σε ονόματα κεντρικών υπολογιστών. Το έργο της ονομασίας των διευθύνσεων των υπολογιστών και των δικτύων αντιμετωπίζεται με τη δημιουργία μιας ιεραρχικής σχέσης μεταξύ των ονομάτων διευθύνσεων, με τους κεντρικούς υπολογιστές να είναι οι απώτατοι απόγονοι μιας τεχνητής ρίζας ονόματος διεύθυνσης. Με την προσάρτηση των ετικετών των domain της μιας μετά της άλλης για τις κεντρικές ετικέτες στην πορεία μέχρι τη ρίζα του δένδρου ιεραρχίας, ένα μοναδικό, μνημονικό, και συνήθως εύκολο αναγνωριστικό δημιουργείται: το όνομα του κεντρικού υπολογιστή.

Η χαρτογράφηση, των διευθύνσεων IP σε ονόματα υπολογιστών έγινε ένα σημαντικό πρόβλημα στο ταχέως αναπτυσσόμενο Internet. Αυτό το υψηλό επίπεδο χαρτογράφησης δεσμευτικές πέρασε διαφορετικά στάδια ανάπτυξης μέχρι το σημερινό χρησιμοποιούμενο σύστημα, το Σύστημα Ονοματοδοσίας των Διευθύνσεων (Domain Name System – DNS). Το DNS είναι ένα κατανεμημένο σύστημα ανάλυσης της ονοματοδοσίας που χρησιμοποιείται από τις περισσότερες υπηρεσίες δικτύου σε όλο το Διαδίκτυο. Λειτουργεί με διαφάνεια για το χρήστη που στέλνει e-mail, που έχει πρόσβαση σε άλλο υπολογιστή μέσω του «telnet» ή του «rlogin»" ή μεταφέρει κάποια αρχεία μέσω του «ftp» από άλλον ιστοχώρο στο δικό του μηχάνημα. Το DNS παρέχει χαρτογράφηση ονόματος και προς δύο κατευθύνσεις: Δίνεται ένα όνομα διεύθυνσης υπολογιστή και επιστρέφει την κατάλληλη διεύθυνση IP, και αντιστρόφως.

Η παρούσα εργασία ασχολείται με την δομή του Domain Name System, με τα τρωτά σημεία που παρουσιάζει και με κάποιες βελτιώσεις – πρωτόκολλα που έχουν προταθεί για την ασφαλή του λειτουργία. Το κύριο μέρος της εργασίας αυτής αποτελείται από πέντε κεφάλαια.

Το πρώτο από αυτά τα πέντε κεφάλαια, το κεφάλαιο 2, περιγράφει το σύστημα ονοματοδοσίας των διευθύνσεων (DNS) εντός του πλαισίου του, του Internet, αναφέροντας τους σχεδιαστικούς του στόχους, τις οντότητες που το απαρτίζουν και τον τρόπο με τον οποίο λειτουργεί.

Το κεφάλαιο 3 ορίζει τα τρωτά σημεία του συστήματος DNS με την αναφορά των διαφόρων επιθέσεων που μπορεί να δεχτεί, ενώ το κεφάλαιο 4 αναφέρεται στη DNSSEC, η οποία αποτελεί έναν μηχανισμό ασφαλείας που παρέχει προστασία στην έγχυση λανθασμένων πληροφοριών στο σύστημα και είναι ζωτικής σημασίας για τις απαιτήσεις ασφάλειας του Διαδικτύου.

Το κεφάλαιο 5 αναφέρεται εξηγεί τους τρόπους με τους οποίους μπορούν να συνδυαστούν τα πιστοποιητικά ασφαλείας με τα ονόματα διευθύνσεων για την παροχή μεγαλύτερης ασφάλειας και τέλος, στο κεφάλαιο 6 εξηγείται η DNSCurve, η οποία αποτελεί μια εναλλακτική λύση για το DNS και τη DNSSEC.

ΚΕΦΑΛΑΙΟ 2. ΤΟ ΣΥΣΤΗΜΑ ΟΝΟΜΑΤΟΔΟΣΙΑΣ ΤΩΝ ΔΙΕΥΘΥΝΣΕΩΝ

2.1 ΕΙΣΑΓΩΓΗ

Ο κύριος τρόπος αναγνώρισης ενός υπολογιστή στο διαδίκτυο είναι η IP διεύθυνσή του. Η διεύθυνση αυτή έχει μέγεθος τριάντα δύο bit και τυπικά καταγράφεται με τη μορφή τεσσάρων δεκαδικών αριθμών (bytes) οι οποίοι διαχωρίζονται μεταξύ τους με τελείες. Επειδή δεν είναι εύκολο και λειτουργικό για τους χρήστες να θυμούνται τις διευθύνσεις IP, δίνουν στους υπολογιστές και στα δίκτυα συμβολικά ονόματα.

Η διεύθυνση IP προσδιορίζει μία συγκεκριμένη σύνδεση, δηλαδή ένα σημείο επαφής στο δίκτυο. Έτσι εάν ένας υπολογιστής μετακινηθεί σε άλλη θέση (στο ίδιο ή σε διαφορετικό δίκτυο), τότε η διεύθυνση του πρέπει να αλλάξει. Αντίθετα ένα όνομα προσδιορίζει τον ίδιο τον υπολογιστή, προσφέροντας ένα αναγνωριστικό στοιχείο που τον ξεχωρίζει από άλλους υπολογιστές του δικτύου. Έτσι εάν ένας υπολογιστής μετακινηθεί σε άλλη θέση (στο ίδιο ή σε διαφορετικό δίκτυο), τότε το όνομά του μπορεί να παραμείνει ίδιο.

Καθώς ένας υπολογιστής μπορεί να έχει περισσότερες από μια IP διευθύνσεις (αν είναι συνδεδεμένος σε πολλαπλά δίκτυα για παράδειγμα), με τον ίδιο τρόπο μπορεί να έχει και περισσότερα από ένα ονόματα, το καθένα εκ των οποίων να αντιστοιχεί και σε μια IP. Οι χρήστες μπορούν επίσης να αναφέρονται με ονόματα όχι μόνο σε συγκεκριμένες συσκευές (υπολογιστές) αλλά και σε ολόκληρα δίκτυα. Τα ονόματα των υπολογιστών είναι συνήθως περιγραφικά ώστε να μπορεί ο υπολογιστής να αναγνωρίζεται εύκολα μέσα στο δίκτυο, αλλά τα ονόματα των δικτύων αντικατοπτρίζουν συνήθως το όνομα του οργανισμού ή της εταιρίας στην οποία ανήκουν. Σε μεγάλα δίκτυα, τα ονόματα των ατομικών υπολογιστών είναι συνήθως συμβολικά και προκύπτουν κωδικοποιώντας δεδομένα όπως τον τύπο της συσκευής, τη θέση της και το σκοπό που εξυπηρετεί.

Τα ονόματα που χρησιμοποιούνται σε αυτές τις περιπτώσεις μπορεί να είναι εύκολα κατανοητά από τους ανθρώπους που χρησιμοποιούν το δίκτυο καθημερινά στην εργασία τους, αλλά πιθανόν να μην σημαίνουν κάτι το ιδιαίτερο για κάποιον τρίτο. Σε κάθε περίπτωση, για να πραγματοποιηθεί η επικοινωνία με κάποια απομακρυσμένη συσκευή είναι απαραίτητο να χρησιμοποιηθεί η IP διεύθυνση της. Όταν χρησιμοποιείται το όνομά της, το οποίο είναι πιο εύκολο για τον χρήστη, πρέπει με κάποιο τρόπο να γίνει η μετατροπή του στην αντίστοιχη IP διεύθυνση.

Ένας απλός τρόπος για να γίνει η μετατροπή αυτή είναι κάθε υπολογιστής να διαθέτει ένα αρχείο το οποίο να περιέχει την αντιστοιχία των συμβολικών ονομάτων με τις διευθύνσεις IP. Για να λειτουργήσει αυτό το σύστημα, θα πρέπει αυτό το αρχείο να περιέχει τα ονόματα και τις διευθύνσεις όλων των υπολογιστών του δικτύου, να υπάρχει σε όλους τους υπολογιστές και να διατηρείται ενημερωμένο όταν γίνονται αλλαγές. Με τη χρήση ενός τέτοιου αρχείου θα δημιουργούνταν βασικά προβλήματα, όπως το τεράστιο μέγεθός του και οι συνεχείς αλλαγές που θα έπρεπε να υφίσταται εξ αιτίας των αλλαγών που γίνονται στα δίκτυα.

Για το λόγο αυτό δημιουργήθηκε το σύστημα ονοματοδοσίας διευθύνσεων του Διαδικτύου, το οποίο αποτελεί έναν μηχανισμό που αντιστοιχίζει τις διευθύνσεις σε ονόματα και τα ονόματα σε διευθύνσεις.

2.2 DOMAIN NAME SYSTEM

Το σύστημα ονοματοδοσίας διευθύνσεων του Διαδικτύου (Domain Name System - DNS) [11] αποτελεί μία τυποποιημένη τεχνολογία με βάση την οποία πραγματοποιείται η διαχείριση των ονομάτων των ιστοχώρων στο διαδίκτυο. Η τεχνολογία αυτή επιτρέπει την αυτόματη εύρεση μιας διεύθυνσης στον διαδίκτυο, με την πληκτρολόγηση ενός ονόματος στον φυλλομετρητή. Ο ρόλος του δηλαδή είναι η μετατροπή των διευθύνσεων του διαδικτύου σε ονόματα κατανοητά από τους ανθρώπους. Το DNS διαθέτει μία παγκόσμια

συλλογή από DNS εξυπηρετητές, δηλαδή υπολογιστές που δημιουργήθηκαν για τη σύνδεση του Domain Name System.

Ένας εξυπηρετητής DNS εκτελεί ένα λογισμικό ειδικής χρήσης δικτύωσης, χαρακτηρίζει μία δημόσια διεύθυνση IP και διαθέτει μία βάση δεδομένων των ονομάτων και των διευθύνσεων. Οι DNS εξυπηρετητές επικοινωνούν μεταξύ τους με τη χρήση ιδιωτικών πρωτοκόλλων δικτύων και οργανώνονται σε μία ιεραρχία. Στο ανώτερο επίπεδο της ιεραρχίας τοποθετούνται οι αποκαλούμενοι κεντρικοί υπολογιστές ρίζας (root servers), οι οποίοι είναι συνολικά δεκατρείς σε όλο το διαδίκτυο και αποθηκεύουν την πλήρη βάση δεδομένων των ονομάτων περιοχών του διαδικτύου και των αντίστοιχων διευθύνσεων IP τους. Οι κυρίαρχοι αυτοί υπολογιστές διατηρούνται από διάφορους οργανισμούς και για την ονομασία τους χρησιμοποιούνται τα λατινικά κεφαλαία γράμματα A,B,... έως M.

Εκτός από τους δεκατρείς ανώτατους στην ιεραρχία υπολογιστές, υπάρχουν και άλλοι dns εξυπηρετητές σε χαμηλότερα επίπεδα της ιεραρχίας οι οποίοι διατηρούν μόνο ορισμένα τμήματα της γενικής βάσης δεδομένων. Οι περισσότεροι από αυτούς ανήκουν σε επιχειρήσεις ή σε φορείς παροχής υπηρεσιών του διαδικτύου(ISPs).

Το δίκτυο του DNS βασίζεται στην αρχιτεκτονική πελάτη/εξυπηρετητή. Ο φυλλομετρητής ενός χρήστη λειτουργεί ως dns πελάτης και εκδίδει αιτήματα στον DNS εξυπηρετητή του προμηθευτή Ίντερνετ του χρήστη κατά την πλοήγηση μεταξύ των ιστοχώρων. Όταν ένας dns εξυπηρετητής λαμβάνει ένα αίτημα (όχι στη βάση δεδομένων του όπως ένας γεωγραφικά μακριά ή ένας σπάνια επισκεπτόμενος ιστοχώρος), μετασχηματίζεται προσωρινά από έναν DNS εξυπηρετητή σε έναν dns πελάτη. Ο εξυπηρετητής αυτόματα περνά το αίτημα σε έναν άλλο dns εξυπηρετητή ή μέχρι το επόμενο πιό υψηλό επίπεδο στη dns ιεραρχία όπως χρειάζεται. Τελικά το αίτημα φθάνει σε έναν εξυπηρετητή που έχει το όνομα και τη διεύθυνση IP στη βάση δεδομένων του (ακόμα και μέχρι το επίπεδο των κεντρικών υπολογιστών ρίζας εάν είναι απαραίτητο), και η απάντηση κυλάει (flows) πίσω διαμέσω της αλυσίδας των DNS εξυπηρετητών στον πελάτη.

Ο σκοπός ενός dns εξυπηρετητή είναι να επιτρέπει στους ανθρώπους και στις εφαρμογές να κοιτάζουν τις εγγραφές στους πίνακες DNS. Οι περισσότεροι dns εξυπηρετητές είναι ιδιωτικοί, δηλαδή είναι έτσι διαμορφωμένοι ώστε να παρέχουν υπηρεσίες μόνο στους ανθρώπους και τους οργανισμούς που τους κατέχουν και τους διατηρούν. Ελάχιστοι dns εξυπηρετητές του Διαδικτύου παρέχουν dns λύσεις για τον κάθε ένα που τις ζητάει. Αυτοί είναι γνωστοί ως δημόσιοι dns εξυπηρετητές (Public Dns servers).Οι περισσότεροι δημόσιοι dns εξυπηρετητές είναι σκόπιμα δημόσιοι. Ελάχιστοι δημόσιοι dns εξυπηρετητές είναι δημόσιοι μόνο επειδή έχουν διαμορφωθεί με λάθος τρόπο από τους διαχειριστές του συστήματος. Αυτοί οι dns εξυπηρετητές τείνουν τελικά να διορθώνονται.

2.2.1 ΣΧΕΔΙΑΣΤΙΚΟΙ ΣΤΟΧΟΙ

Η προσπάθεια για τον σχεδιασμό του συστήματος ονοματοδοσίας διευθύνσεων του Διαδικτύου κατευθύνθηκε μεταξύ διάφορων στόχων, οι οποίοι αποτέλεσαν πρωταρχικό ρόλο στη σημερινή του μορφή [11]. Ο βασικός στόχος ήταν η δημιουργία ενός συστήματος το οποίο θα καλύπτει τα ακόλουθα κριτήρια:

2.2.1.1 ΣΥΝΕΠΕΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Ο πρωταρχικός στόχος ήταν να παρασχεθεί ένα συνεπές διάστημα ονόματος για να χρησιμοποιηθεί για να αναφερθεί στους πόρους. Εν μέρει, το διάστημα αυτό δεν θα έπρεπε να βασιστεί σε κανένα αναγνωριστικό δικτύου, και έτσι να είναι εντελώς ανεξάρτητο από τις πληροφορίες δρομολόγησης ή από την τοπολογία του δικτύου.

2.2.1.2 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ

Η ανάπτυξη του Διαδικτύου σε αριθμό μηχανών και υποδικτύων απαιτούσε την εισαγωγή ενός συστήματος ανάλυσης της ονοματοδοσίας, το οποίο θα μπορούσε και να χειριστεί τον τεράστιο όγκο των μηχανών και των αιτημάτων ανάλυσης αλλά και να ανταποκρίνεται αποδοτικά. Για να αποκομιστούν οι επιθυμητές αυτές επιδράσεις το σύστημα δημιουργήθηκε με έναν ιεραρχικό, κατανεμημένο τρόπο χρησιμοποιώντας την τεχνολογία της προσωρινής αποθήκευσης.

Στο διαδίκτυο, η πρόσβαση στα μηχανήματα των τοπικών δικτύων είναι πιο πιθανή από την απομονωμένη πρόσβαση μέσω πολλών συνδέσμων. Επομένως, λαμβάνονται τοπικά πολλά περισσότερα αιτήματα ανάλυσης ονόματος. Η γνώση για τις απαιτούμενες συνδέσεις στα τοπικά δίκτυα είναι διαθέσιμη με τη μορφή μιας τοπικής βάσης δεδομένων. Αυτά τα γεγονότα προτείνουν τη χρήση ενός ιεραρχικού και οργανωτικού σχήματος με το οποίο τα τοπικά αιτήματα ανάλυσης επιλύονται αποδοτικά από μία τοπική οντότητα, και τα σπάνια αιτήματα ανάλυσης για μακρινές χαρτογραφήσεις εξετάζονται μέσω μιας αλληλεπίδρασης τοπικών και απομακρυσμένων οντοτήτων. Η σαφής και καθαρή δομή έχει ως αποτέλεσμα να δούμε την κατανομή του διαστήματος του ονόματος ως δέντρο.

Η δημιουργία των ονομάτων των κεντρικών υπολογιστών προσαρτώντας κόμβους ετικετών από τα φύλλα του δένδρου προς την κορυφή εξυπηρέτησε την ανάγκη για εύκολα ονόματα για τα μηχανήματα. Η κατανεμημένη ρύθμιση του συστήματος συμβάλλει στη μείωση του τεράστιου χώρου ονόματος σε κομμάτια που μπορούν να αντιμετωπιστούν επαρκώς. Η προσωρινή αποθήκευση των πληροφοριών που ελήφθησαν από απομακρυσμένα σημεία τοπικά είναι άλλος ένας μηχανισμός για την απόκτηση της αποτελεσματικότητας. Εξαιτίας της δυναμικής του συστήματος, οι προσωρινά αποθηκευμένες πληροφορίες χαρακτηρίζονται με μία επιπλέον παράμετρο χρόνου ισχύος (Time to Live - TTL) για την εξασφάλιση του στόχου της συνέπειας των δεδομένων.

2.2.1.3 ΚΑΤΑΝΟΜΗ ΧΑΡΑΚΤΗΡΩΝ

Η επιλογή της εφαρμογής ενός παραδείγματος πελάτη-εξυπηρετητή μεγάλης κλίμακας σε μία γεωγραφική κατανομή του συνόλου των μηχανημάτων υποστηρίχθηκε από την ανάγκη για αυξημένη αξιοπιστία μέσω της ύπαρξης πλεοναζόντων βάσεων δεδομένων σε δευτερεύοντες εξυπηρετητές ονόματος. Σε περίπτωση οποιουδήποτε είδους αποτυχίας σε κάποιον από τους εξυπηρετητές για μία ζώνη, ο πλεονάζον αριθμός των εξυπηρετητών θα είναι ακόμη σε θέση να παράσχει την υπηρεσία χαρτογράφησης. Γι' αυτό μια αποτυχία σε έναν μόνο ιστοχώρο δε μπορεί να οδηγήσει σε άρνηση της υπηρεσίας ανάλυσης.

Οι τοπικές αρχές μπορούν να διαχειριστούν τις δικές τους ζώνες και διευθύνσεις δικτύου, διατηρώντας συνεπή τη βάση δεδομένων, παρέχοντας αυτόνομο έλεγχο και εκχώρηση ονόματος και αφαιρώντας το φόρτο από τις κεντρικές αρχές. Η αρχή περνάει κάτω από τις άκρες του δέντρου, ενώ οι πληροφορίες ρέουν κατά μήκος της ιεραρχίας από τον έναν εξυπηρετητή στον άλλο. Η εννοιολογική διάταξη των εξυπηρετητών διεύθυνσης ονομάτων σε ένα δέντρο που μοιάζει με τη δομή ονόματος είναι στην πραγματικότητα μια πιο ρεαλιστική ρύθμιση.

2.2.1.4 ΓΕΝΙΚΟΤΗΤΑ

Το κόστος εφαρμογής και το μέγεθος της διαχειριστικής προσπάθειας για την υποστήριξη του συστήματος υπαγορεύει μια γενική χρησιμότητα. Γι' αυτό το λόγο το σύστημα δεν περιέχει περιττές απαγορεύσεις όσο αναφορά το σκοπό του ή τις εφαρμογές. Αυτός ο στόχος μπορεί να αναδιατυπωθεί ως η επιθυμία να επιτραπεί η αύξηση της βάσης δεδομένων από τις νέες δομές δεδομένων.

2.2.1.5 ΑΝΕΞΑΡΤΗΣΙΑ

Το σύστημα σχεδιάστηκε έτσι ώστε να είναι ανεξάρτητο του υποκείμενου λογισμικού, είτε πρόκειται για κεντρικό υπολογιστή είτε για την διεπαφή του δικτύου. Επιπλέον, η διεξαγωγές πρέπει να είναι ανεξάρτητες του συστήματος επικοινωνίας που τις φέρει. Επομένως, όλα τα πιθανά είδη μεταγωγής πακέτων είναι κατάλληλα, όπως η μεταγωγή αποθήκευσης και διαβιβασμού, τα κυκλικά διαγράμματα ή πιθανόν οι υβριδικές προσεγγίσεις.

2.2.2 DNS ΟΝΤΟΤΗΤΕΣ

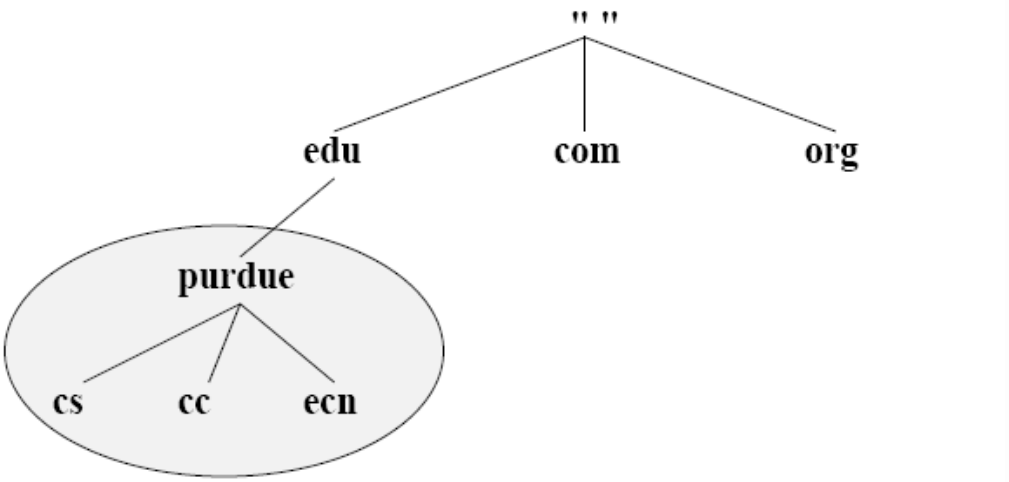
Το σύστημα ονοματοδοσίας των διευθύνσεων του διαδικτύου αποτελείται από μερικές οντότητες: αναλυτές, εξυπηρετητές ονομάτων και εγγραφές πόρων(Resource Records - RR). Αρχικά θα περιγραφεί το διάστημα διεύθυνσης ονόματος και οι εγγραφές πόρων τα οποία αποτελούν τμήματα των DNS μηνυμάτων. Εξυπηρετούν στην ανταλλαγή των

δεδομένων μεταξύ των εξυπηρετητών ονόματος και των αναλυτών. Κατόπιν θα περιγραφούν τα χαρακτηριστικά και οι σκοποί των εξυπηρετητών ονόματος και των αναλυτών.

2.2.2.1 ΔΙΑΣΤΗΜΑ ΔΙΕΥΘΥΝΣΗΣ ΟΝΟΜΑΤΟΣ

Το διάστημα διεύθυνσης ονόματος [11] είναι η προδιαγραφή για ένα δένδρο-δομημένο διάστημα ονόματος. Η ρίζα αυτού του δένδρου είναι η ρίζα-διεύθυνση διαδικτύου ακολουθούμενη από τα παιδιά της, τις διευθύνσεις ανώτερου επιπέδου, τα οποία μπορούν να περιλαμβάνουν διάφορα επίπεδα υποδιευθύνσεων.

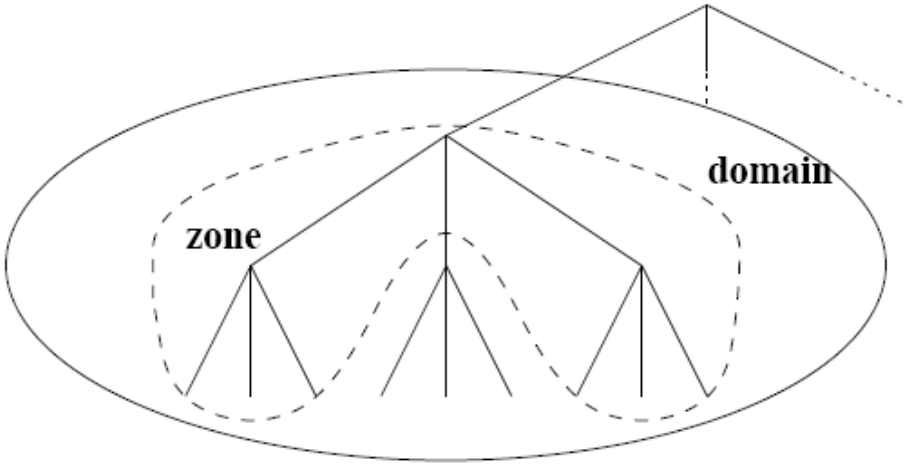
Η επόμενη εικόνα δείχνει τη δομή ενός τέτοιου δένδρου. Τα ονόματα των κεντρικών υπολογιστών αποτελούνται από μία αλληλουχία των ετικετών του κάθε κόμβου στο μονοπάτι από το φύλλο που αντιπροσωπεύει τον πραγματικό εξυπηρετητή μέχρι τη ρίζα. Οι γειτονικές ετικέτες χωρίζονται με μία τελεία. Οι διευθύνσεις του διαδικτύου είναι απλώς υποδένδρα του διαστήματος διεύθυνσης ονόματος. Στο ακόλουθο παράδειγμα το «purdue.edu» είναι ένα όνομα διεύθυνσης διαδικτύου:



Εικόνα 1. Όνομα διεύθυνσης pursue.edu

Ένα τμήμα του διαστήματος διεύθυνσης ονόματος το οποίο ελέγχεται απόλυτα από έναν κεντρικό εξυπηρετητή ονόματος ονομάζεται ζώνη. Η λεπτή διαφορά ανάμεσα σε μία διεύθυνση ονόματος και σε μία ζώνη είναι ότι η ζώνη περιέχει όλα τα ονόματα διευθύνσεων διαδικτύου και τα δεδομένα που περιλαμβάνει μία διεύθυνση, εκτός από τις διευθύνσεις και τα ονόματα που αντιπροσωπεύονται αλλού. Βλέποντας τις διευθύνσεις (κόμβους) και τους εξυπηρετητές (φύλλα) ως μία εννοιολογική διάταξη παράγεται ένα δένδρο με μεγαλύτερο ύψος απ' ότι βλέποντας τις ζώνες ως κόμβους. Το τελευταίο αποτελεί μία πιο ρεαλιστική απεικόνιση του δένδρου όσο αναφορά την αποδοτικότητα.

Ένα παράδειγμα για να γίνει κατανοητή η διαφορά ανάμεσα στη διεύθυνση και στη ζώνη είναι το ακόλουθο σενάριο. Μία τοπική αρχή διαχειρίζεται τη διεύθυνση «άλφα.dom". Η «άλφα.dom» έχει τρεις υποδιευθύνσεις την «φι», την «χι» και την «ψι» οι οποίες περιέχουν μερικούς εξυπηρετητές, αλλά όχι επιπλέον υποδιευθύνσεις. Εάν η αρχή για την υποδιεύθυνση «ψι» μεταφερθεί στο «ψι. άλφα.dom», έχουμε ως αποτέλεσμα δύο ζώνες. Η αρχή για την «άλφα.dom» μπορεί επιπρόσθετα να μεταφέρει την αρχή για το «χι» στην ίδια αρχή που χειρίζεται το «ψι». Αυτό το σενάριο δείχνει ότι οι ζώνες δεν χρειάζεται να συνδέονται από τις άκρες στη δομή δένδρου της διεύθυνσης διαδικτύου. Η διαφορά μεταξύ ζώνης και διεύθυνσης διαδικτύου γίνεται αισθητή με την παρακάτω εικόνα:



Εικόνα 2. Διαφορά μεταξύ της ζώνης και της διεύθυνσης

2.2.2.2 DNS ΜΗΝΥΜΑΤΑ

Τα μηνύματα dns αποτελούν μονάδες δεδομένων που μεταφέρονται μεταξύ των εξυπηρετητών ονομάτων και των αναλυτών. Ένα μήνυμα διεύθυνσης ονόματος αποτελείται από την επικεφαλίδα και μέχρι τέσσερα τμήματα και φαίνεται στην Εικόνα 3. Η επικεφαλίδα περιέχει τα ακόλουθα πεδία [11]:

- Ένα αναγνωριστικό των 16 bit το οποίο έχει τεθεί από το πρόγραμμα και παράγει κάθε είδους ερώτηση
- Το bit «QR» το οποίο καθορίζει πότε το μήνυμα είναι ερώτηση (τιμή 0) ή απάντηση (τιμή 1)
- Το «OPCODE» το οποίο είναι ένα πεδίο των 4 bit το οποίο καθορίζει το είδος της ερώτησης στο μήνυμα και μπορεί να περιέχει τις ακόλουθες τιμές:
  - 0 για μία κανονική ερώτηση (QUERY)
  - 1 για μία αντίστροφη ερώτηση (IQUERY)
  - 2 για ένα αίτημα κατάστασης του εξυπηρετητή (STATUS)
  - 3-15 κρατημένα για μελλοντική χρήση
- Το επόμενο bit «AA» είναι έγκυρο μόνο σε απάντηση και καθορίζει ότι ο ανταποκρινόμενος εξυπηρετητής είναι μία αρχή για τη διεύθυνση ονόματος στον τομέα της ερώτησης.
- Το bit «TC» καθορίζει εάν ένα μήνυμα έχει περικοπεί
- Το bit «RD» καθορίζει εάν είναι επιθυμητή η αναδρομή από μία ερώτηση
- Το bit «RA» καθορίζει εάν η αναδρομή είναι διαθέσιμη
- Τα επόμενα τρία bits στο πεδίο «Z» είναι κρατημένα για μελλοντική χρήση
- Τα τέσσερα τελευταία bits αποφασίζουν τον κωδικό απάντησης «RCODE». Πιθανές τιμές για τον κωδικό αυτό είναι:
  - 0 για κατάσταση μη λανθασμένη
  - 1 για να υποδείξει ένα σφάλμα διάταξης
  - 2 για να υποδείξει μία αποτυχία του εξυπηρετητή
  - 3 για να υποδείξει ένα σφάλμα ονόματος
  - 4 για να υποδείξει ότι το ζητούμενο χαρακτηριστικό δεν τέθηκε σε εφαρμογή

- 5 για να υποδείξει ότι ο εξυπηρετητής αρνήθηκε να πραγματοποιήσει τη συγκεκριμένη λειτουργία
- 6-15 κρατημένες για μελλοντική χρήση

- Οι ακόλουθες τέσσερεις απρόσημες τιμές ακέραιων των 16 bit καθορίζουν τον αριθμό των εισόδων στις ακόλουθες ερωτήσεις, απαντήσεις, αρχές και επιπρόσθετα τμήματα.

Τα περιεχόμενα των τεσσάρων αυτών τμημάτων εξυπηρετούν διαφορετικούς σκοπούς. Η σειρά αυτών των τμημάτων είναι πάντα η ίδια και μερικά από αυτά μπορεί να είναι κενά σε ένα dns μήνυμα. Η διάταξη της απάντησης, της αρχής και του επιπρόσθετου τμήματος είναι η ίδια.

Το τμήμα της ερώτησης φέρει το όνομα του ερωτήματος, τον τύπο του ερωτήματος και την κατηγορία αυτού. Έγκυροι τύποι ερωτημάτων αποτελούν όλοι οι κωδικοί για τους τύπους εγγραφής πόρων, και μερικοί πιο γενικοί για την μεταφορά ζώνης και το χειρισμό του ταχυδρομείου. Στη συνέχεια ορίζονται τα μνημονικά και οι τιμές της κατηγορίας:

- 1 για “IN” - Internet
- 2 για “CS”- CSNET
- 3 για “CH” – CHAOS
- 4 για “HS” – Hesiod
- 255 για wild-carding

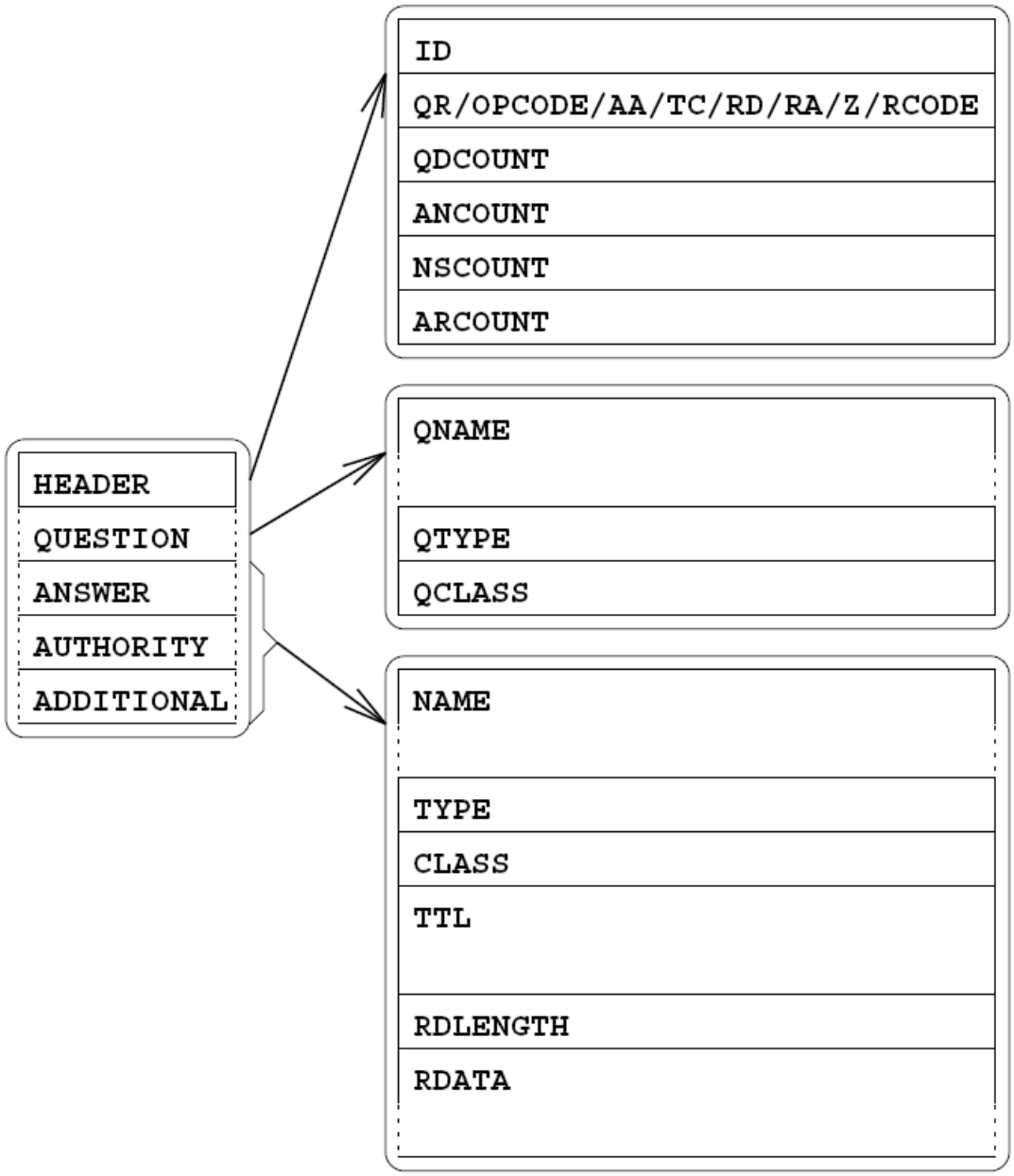
Το τμήμα απάντησης φέρει τις εγγραφές πόρων που απαντούν άμεσα το ερώτημα, το τμήμα αρχής φέρει τις εγγραφές πόρων που περιγράφουν άλλους επιτακτικούς εξυπηρετητές και το επιπρόσθετο τμήμα φέρει εγγραφές πόρων οι οποίες δεν απαιτούνται ρητά αλλά μπορεί να είναι χρήσιμες στη χρήση των εγγραφών πόρων άλλων τμημάτων.

Ο επιτακτικός τομέας περιλαμβάνει τα στοιχεία του εξυπηρετητή ονόματος στην ακόλουθη περίπτωση: Εάν ένας εξυπηρετητής ονόματος προσπαθεί να αναλύσει ένα όνομα και γνωρίζει από έναν επίσημο εξυπηρετητή για τη διεύθυνση του διαδικτύου στην οποία βρίσκεται το όνομα ότι πρέπει να αναλυθεί, βάζει το όνομα του εξυπηρετητή στο τμήμα αρχής της απάντησης. Αυτή είναι η προσέγγιση του DNS συστήματος για να αναφέρει τους πελάτες που δεν είναι σε αναδρομική λειτουργία στους άλλους εξυπηρετητές.

Το επιπρόσθετο τμήμα παίζει σημαντικό ρόλο στην ίδια περίπτωση. Εάν ένας εξυπηρετητής αναφέρει έναν αναλυτή σε έναν άλλον εξυπηρετητή ονόματος, καλύτερο είναι να παράσχει τη διεύθυνση του άλλου εξυπηρετητή, επειδή αυτή είναι η επόμενη πληροφορία που χρειάζεται ο αναλυτής για να προχωρήσει με τα ερωτήματά του. Ακόμα ένας λόγος για την ύπαρξη των επιπρόσθετων τμημάτων είναι να υπάρχει χώρος για παραπάνω, μη απαιτούμενες πληροφορίες. Αν ένας αναλυτής λάβει επιπλέον εγγραφές και τις αποθηκεύσει προσωρινά, μπορεί να τις χρησιμοποιήσει αργότερα.

Αυτό θα έχει ως αποτέλεσμα αυξημένη επίδοση του συστήματος, επειδή η ανάλυση των δεδομένων που είναι ήδη στην τοπική προσωρινή μνήμη είναι λογικά πιο αποδοτική από μία απομακρυσμένη ανάλυση η οποία απαιτεί κίνηση δικτύου. Αυτοί οι τρεις τύποι ενός dns μηνύματος έχουν την ίδια διάταξη:

- Ένα όνομα
- Ένα τύπο όπως σε ένα ερώτημα
- Μία κατηγορία όπως σε ένα ερώτημα
- Ένα χρόνο των 32 bit ζωής στο πεδίο ο οποίος δίνεται σε δευτερόλεπτα (TTL)
- Έναν απρόσημο ακέραιο των 16 bit ο οποίος καθορίζει το μήκος του πεδίου RDATA σε bytes
- Μία σειρά από bytes μεταβλητού μήκους που περιγράφουν τον πόρο



Εικόνα 3. DNS Μήνυμα

2.2.2.3 ΕΓΓΡΑΦΕΣ ΠΟΡΩΝ

Τα δεδομένα που συνδέονται με τους κόμβους και τα φύλλα αυτού το δένδρου ανταλλάσσονται στο κομμάτι RDATA των τριών τελευταίων τμημάτων σε ένα μήνυμα dns. Σε αυτές τις εγγραφές πόρων προστίθεται ετικέτα σύμφωνα με τον τύπο των δεδομένων που περιέχουν. Οι τύποι αυτοί είναι οι ακόλουθοι [11]:

- Μία «A» εγγραφή περιέχει μία διεύθυνση κεντρικού υπολογιστή: μία διεύθυνση των 32 bit όπου η κατηγορία είναι «IN»
- Μία «SOA» εγγραφή είναι η πρώτη εγγραφή σε κάθε αρχείο της βάσης δεδομένων και καθορίζει έναν εξυπηρετητή να είναι η επίσημη πηγή πληροφορίας μέσα στη διεύθυνση διαδικτύου
- Μία «NS» εγγραφή δηλώνει έναν εξυπηρετητή ονομάτων για μία ζώνη
- Μία «PTR» εγγραφή παρέχει ένα δείκτη σε μία άλλη περιοχή στο διάστημα του ονόματος διεύθυνσης

- Μία «HINFO» εγγραφή ορίζει τον τύπο της CPU και του λειτουργικού συστήματος που χρησιμοποιείται από τον κεντρικό υπολογιστή
- Μία «CNAME» εγγραφή καθορίζει το κανονικό ή το πρωτεύον όνομα του κατόχου- ο κάτοχος είναι ένα ψευδώνυμο
- Μία «MX» εγγραφή καθορίζει έναν κεντρικό υπολογιστή πρόθυμο να λειτουργήσει ως εναλλάκτης μηνυμάτων ηλεκτρονικού ταχυδρομείου για το όνομα του κατόχου και μία προτίμηση ανάμεσα στις άλλες καταγραφές πόρων του ίδιου κατόχου
- Μία «X25» εγγραφή περιέχει μία σειρά χαρακτήρων που ορίζει μια δημόσια διεύθυνση δικτύου μεταγωγής δεδομένων
- Μία «ISDN» εγγραφή περιέχει μία σειρά χαρακτήρων η οποία ορίζει τον ISDN αριθμό του κατόχου και το DDI, αν υπάρχει.

Οι εγγραφές πόρων ομαδοποιούνται σε σύνολα εγγραφών πόρων (RRSets). Τα σύνολα αυτά μπορεί να περιέχουν μηδέν ή περισσότερες εγγραφές πόρων, που έχουν ίδιο όνομα DNS, ίδια κατηγορία και τύπο, αλλά τα δεδομένα (δηλαδή, τα RDATA) είναι διαφορετικά. Εάν το όνομα, η κατηγορία, ο τύπος και τα δεδομένα είναι τα ίδια για δύο ή περισσότερες εγγραφές τότε υπάρχουν διπλοεγγραφές για το ίδιο όνομα DNS. Οι εξυπηρετητές ονομάτων θα πρέπει να καταστέλλουν τις διπλές εγγραφές. Στο ακόλουθο σχήμα φαίνεται ένα παράδειγμα ενός συνόλου εγγραφών πόρων.

example.com.	IN	NS	ns1.example.com.
example.com.	IN	NS	ns2.example.com.
example.com.	IN	NS	ns.plain.org.

Εικόνα 4. Σύνολο εγγραφών πόρων

2.2.2.4 ΕΞΥΠΗΡΕΤΗΤΕΣ ΟΝΟΜΑΤΟΣ

Ολόκληρη η βάση δεδομένων χωρίζεται σε ζώνες οι οποίες διανέμονται ανάμεσα στους εξυπηρετητές ονόματος. Η βασική λειτουργία ενός εξυπηρετητή ονόματος είναι να απαντά ερωτήματα χρησιμοποιώντας τα δεδομένα στη ζώνη του. Για να επιτευχθεί μεγαλύτερος βαθμός αξιοπιστίας του συστήματος, ο ορισμός του συστήματος ονοματοδοσίας διεύθυνσης απαιτεί ότι τουλάχιστον δύο εξυπηρετητές ονομάτων περιέχουν επίσημα δεδομένα για μία δοσμένη ζώνη. Μερικοί ιστοχώροι χρησιμοποιούν περισσότερους από δύο εξυπηρετητές ονομάτων: Ένας από αυτούς βρίσκεται συνήθως έξω από το επηρεασμένο δίκτυο για να εγγυηθεί την υπηρεσία ονόματος σε περίπτωση που το δίκτυο είναι απρόσιτο για κάποιο λόγο.

Ο κύριος εξυπηρετητής ονόματος ονομάζεται πρωταρχικός εξυπηρετητής ονόματος και οι εφεδρικοί εξυπηρετητές ονομάζονται δευτερεύοντες εξυπηρετητές ονόματος. Οι δευτερεύοντες επίσημοι εξυπηρετητές ονόματος ενημερώνουν τη βάση δεδομένων για τη ζώνη τους περιοδικά με δεδομένα καταγεγραμμένα από τους πρωταρχικούς εξυπηρετητές. Οι πρωταρχικοί εξυπηρετητές ονόματος φορτώνουν τα αρχεία της βάσης δεδομένων που προμηθεύονται από τον διαχειριστή ζώνης και διατηρούν μία προσωρινή μνήμη δεδομένων η οποία αποκτήθηκε μέσω της καταγραφής πόρων.

Οι εξυπηρετητές θέλουν να προσαρμόζονται δυναμικά στις αλλαγές της οργάνωσης του διαστήματος ονόματος των άλλων αρχών. Επομένως κάθε εγγραφή πόρου περιέχει ένα πεδίο χρόνου ισχύος το οποίο βεβαιώνει ότι οι εξυπηρετητές ονόματος δεν αποθηκεύουν δεδομένα προσωρινά χωρίς όριο χρόνου. Ο πραγματικός αλγόριθμος που χρησιμοποιούν οι εξυπηρετητές ονόματος εξαρτάται από το λειτουργικό σύστημα και τις δομές δεδομένων που χρησιμοποιούν για να αποθηκεύσουν τις καταγραφές πόρων.

2.2.2.5 ΑΝΑΛΥΤΕΣ

Η διεπαφή μεταξύ του συστήματος ονόματος διεύθυνσης και του προγράμματος του χρήστη είναι ο αναλυτής ονόματος. Στην πιο απλή περίπτωση, ένας αναλυτής λαμβάνει ένα αίτημα από ένα πρόγραμμα χρήστη με τη μορφή μιας κλήσης συστήματος ή υπορουτίνας και επιστρέφει την επιθυμητή πληροφορία. Ο αναλυτής βρίσκεται στο ίδιο μηχάνημα με το πρόγραμμα του χρήστη μα έρχεται σε επαφή με έναν ή περισσότερους εξυπηρετητές ονόματος σε (συνήθως) απομονωμένα μηχανήματα αν τα ζητηθέντα δεδομένα δεν είναι ανακτήσιμα από την τοπική προσωρινή μνήμη.

Η τυπική διεπαφή πελάτη-αναλυτή έχει τριπλή λειτουργικότητα: μετάφραση του ονόματος του κεντρικού υπολογιστή σε διεύθυνση IP, μετάφραση της διεύθυνσης IP σε όνομα κεντρικού υπολογιστή και αναζήτηση για γενικές πληροφορίες που καθορίζουν το όνομα του ερωτήματος, τον τύπο και την κατηγορία. Τα ακόλουθα αποτελέσματα μπορούν να ληφθούν μόλις ο αναλυτής εκτελέσει την υποδεικνυόμενη λειτουργία: τα δεδομένα που απαιτούνται, ένα σφάλμα ονόματος σε περίπτωση που το αναφερόμενο όνομα δεν υπάρχει, ή ένα σφάλμα που δηλώνει ότι τα δεδομένα δε βρέθηκαν. Για να αποκτηθεί μεγαλύτερη αποδοτικότητα είναι λογικό οι αναλυτές σε ένα μηχάνημα να μοιράζονται την προσωρινή μνήμη.

Ο πελάτης ενός DNS περιέχει συνήθως ρουτίνες λογισμικού, γνωστές ως λειτουργίες, που είναι αρμόδιες να ζητούν πληροφορίες από το διάστημα διεύθυνσης ονόματος εκ μέρους της εφαρμογής. Οι λειτουργίες αυτές ομαδοποιούνται σε μια βιβλιοθήκη λογισμικού που συνήθως αναφέρεται ως βιβλιοθήκη αναλυτής. Για το λόγο αυτό, οι πελάτες αποκαλούνται συχνά ως αναλυτές. Οι λειτουργίες της βιβλιοθήκης αναλυτή είναι υπεύθυνες για την αποστολή ενός ερωτήματος σε έναν εξυπηρετητή ονομάτων ζητώντας πληροφορίες σχετικά με ένα όνομα DNS και επιστρέφοντας την απάντηση στο ερώτημα πίσω στον αιτούντα.

2.2.3 DNS ΔΙΕΞΑΓΩΓΕΣ

Οι διεξαγωγές DNS εμφανίζονται συνεχώς σε ολόκληρο το Διαδίκτυο. Οι δύο πιο κοινές διεξαγωγές είναι οι DNS μεταφορές ζώνης και τα DNS ερωτήματα / απαντήσεις. Μια DNS μεταφοράς ζώνη συμβαίνει όταν ο δευτερεύων εξυπηρετητής ενημερώνει το αντίγραφο του για μια ζώνη για την οποία είναι επίσημος. Ο δευτερεύων εξυπηρετητής κάνει χρήση των πληροφοριών που διαθέτει στη ζώνη, δηλαδή το σειριακό αριθμό, και ελέγχει αν ο πρωταρχικός εξυπηρετητής έχει μια πιο πρόσφατη έκδοση. Αν συμβεί αυτό, ο δευτερεύων εξυπηρετητής ανακτά ένα νέο αντίγραφο της ζώνης.

Ένα ερώτημα DNS απαντάται από μια απάντηση DNS. Οι αναλυτές χρησιμοποιούν έναν ολοκληρωμένο κατάλογο των εξυπηρετητών ονομάτων, συνήθως όχι περισσότερων από τρεις, για να προσδιοριστεί ο τόπος όπου θα σταλούν τα ερωτήματα. Αν ο πρώτος εξυπηρετητής ονομάτων στη λίστα είναι διαθέσιμος να απαντήσει το ερώτημα, τότε οι άλλοι στη λίστα δεν λαμβάνονται υπόψη. Εάν δεν είναι διαθέσιμος, κάθε εξυπηρετητής ονομάτων στη λίστα λαμβάνεται υπόψη ώσπου να διαπιστωθεί ότι μπορεί να επιστρέψει μια απάντηση στο ερώτημα.

Ο εξυπηρετητής ονομάτων που λαμβάνει ένα ερώτημα από έναν πελάτη μπορεί να ενεργεί για λογαριασμό του πελάτη για την επίλυση του ερωτήματος. Στη συνέχεια, ο εξυπηρετητής ονομάτων μπορεί να υποβάλει το ερώτημα σε άλλους εξυπηρετητές, σε έναν κάθε φορά, με κάθε εξυπηρετητή να λαμβάνεται υπόψη που είναι πιθανώς πιο κοντά στην απάντηση. Ο εξυπηρετητής ονομάτων που έχει την απάντηση στέλνει μια απόκριση πίσω στον αρχικό εξυπηρετητή ονομάτων, ο οποίος στη συνέχεια μπορεί να αποθηκεύσει προσωρινά την απόκριση και να στείλει την απάντηση πίσω στον πελάτη. Μόλις μια απάντηση είναι προσωρινά αποθηκευμένη, ένας εξυπηρετητής DNS μπορεί να χρησιμοποιήσει τις προσωρινά αποθηκευμένες πληροφορίες, όταν ανταποκρίνονται σε επόμενα ερωτήματα για τις ίδιες πληροφορίες DNS. Η προσωρινή αποθήκευση κάνει το DNS πιο αποδοτικό, ειδικά όταν το σύστημα είναι υπερφορτωμένο.

Η Berkeley Internet Name Daemon (BIND) είναι η πιο δημοφιλής εφαρμογή του DNS στο Internet. Η κατανομή του BIND του DNS έχει λογισμικό πελάτη, λογισμικό εξυπηρετητή, και εργαλεία λογισμικού για την υποβολή ερωτημάτων στο DNS και για την αντιμετώπιση προβλημάτων.

ΚΕΦΑΛΑΙΟ 3. ΑΠΕΙΛΕΣ ΓΙΑ ΤΟ ΣΥΣΤΗΜΑ DNS

3.1 ΕΙΣΑΓΩΓΗ

Οι αρχικές προδιαγραφές του DNS δεν περιλαμβάνουν την ασφάλεια βασισμένες στο γεγονός ότι οι πληροφορίες που περιέχει, δηλαδή ότι φιλοξενεί τα ονόματα και τις διευθύνσεις IP, χρησιμοποιούνται ως μέσο για την επικοινωνία των δεδομένων. Καθώς όλο και περισσότερες εφαρμογές που βασίζονται στην IP έχουν αναπτυχθεί, αυξήθηκε η τάση για τη χρήση των διευθύνσεων IP και τα ονόματα υποδοχής ως βάση για τη χορήγηση ή την απαγόρευση της πρόσβασης (δηλαδή αυθεντικοποίηση βασισμένη στο σύστημα).

Ένας άλλος παράγοντας που συμβάλλει στα τρωτά σημεία του DNS είναι ότι το σύστημα έχει σχεδιαστεί για να αποτελεί μια δημόσια βάση δεδομένων στην οποία η έννοια της περιορισμένης πρόσβασης σε πληροφορίες στο διάστημα ονόματος DNS δεν είναι εσκεμμένα μέρος του πρωτοκόλλου. Νεότερες εκδόσεις της εφαρμογής BIND επιτρέπουν ελέγχους πρόσβασης για τέτοια πράγματα όπως οι μεταφορές ζώνης, αλλά σε γενικές γραμμές, το να περιοριστούν αυτοί που μπορούν να υποβάλουν ερωτήματα στο DNS για τις εγγραφές πόρων θεωρείται εκτός του πεδίου εφαρμογής του πρωτοκόλλου.

Η ύπαρξη και η διαδεδομένη χρήση των εν λόγω πρωτοκόλλων θέτει απαιτήσεις για την ακρίβεια των πληροφοριών που περιέχονται στο DNS. Ψευδείς πληροφορίες εντός του συστήματος μπορεί να οδηγήσουν σε απρόβλεπτα και ενδεχομένως επικίνδυνα ανοίγματα. Η πλειοψηφία των αδυναμιών στο πλαίσιο του συστήματος DNS εμπίπτουν σε μία από τις ακόλουθες κατηγορίες: παραποίηση της κρυφής μνήμης, υπερχείλιση πελατών, δυναμική ενημέρωση ευπάθειας, διαρροή πληροφοριών, και έκθεση της έγκυρης βάσης δεδομένων του DNS εξυπηρετητή.

3.2 ΔΗΛΗΤΗΡΙΑΣΗ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Όπως αναφέρθηκε προηγουμένως, το DNS αποτελεί έναν μηχανισμό ανάλυσης των ονομάτων των διευθύνσεων σε διευθύνσεις IP. Τα συστήματα των πελατών επιθυμώντας να γνωρίσουν την διεύθυνση IP ενός μηχανήματος θα ήθελαν να έρθουν σε επαφή με έναν αναλυτή για να υποβάλλει ερωτήματα σε έναν εξυπηρετητή DNS. Ο εξυπηρετητής στέλνει πίσω στον πελάτη μία απάντηση η οποία περιέχει την διεύθυνση IP.

Το πρωτόκολλο DNS δε διαθέτει κατ' ουσία ενσωματωμένη μία μέθοδο αυθεντικοποίησης. Δηλαδή δεν υπάρχει στο πρωτόκολλο κάποιο μέσο το οποίο να διαβεβαιώνει ότι ο αιτούμενος πελάτης ή ο εξυπηρετητής είναι πραγματικοί. Η επικεφαλίδα του μηνύματος ενός DNS ερωτήματος περιέχει ένα πεδίο αναγνώρισης των 16 bit αλλά χρησιμοποιείται κυρίως για την αντιστοίχηση ερωτημάτων και απαντήσεων. Εάν κάποιος επιτιθέμενος μπορεί να προβλέψει επιτυχώς τις μελλοντικές τιμές για το αναγνωριστικό, θα μπορούσε να εξαπατήσει τον πελάτη κάνοντας τον να δεχτεί μία ψεύτικη απάντηση ως σωστή. Ο πελάτης θα μπορούσε να είναι ένας αναλυτής, αλλά υπάρχει μεγαλύτερη πιθανότητα να προκαλέσει ζημιά αν ο πελάτης είναι άλλος ένας εξυπηρετητής ονόματος ο οποίος εκτελεί αναδρομική ανάλυση.

Η ακρίβεια του αναγνωριστικού είναι ασήμαντη, διότι άλλα λογισμικά πελατών χρησιμοποιούσαν διαδοχικά αυξανόμενα νούμερα για το πεδίο αναγνώρισης. Εάν κάποιος εισβολέας είναι ικανός να αποφασίσει το αναγνωριστικό ενός ερωτήματος, θα μπορούσε εύκολα να μαντέψει τα αναγνωριστικά για τα επακόλουθα ερωτήματα. Όταν σταλεί το επόμενο ερώτημα ο επιτιθέμενος στέλνει μία προσωποποιημένη απάντηση με την ψεύτικη πληροφορία χρησιμοποιώντας τον προβλεπόμενο αριθμό. Καθώς το λανθασμένο πακέτο φτάνει πριν από την απάντηση του πραγματικού εξυπηρετητή, ο αναλυτής θα αντιστοιχήσει το αναγνωριστικό της απάντησης με εκείνο του ερωτήματος και θα το δεχτεί ως επίσημη απάντηση.

Ένας εξελιγμένος εισβολέας δεν θα εξαπατήσει απλώς το αναγνωριστικό του ερωτήματος: θα εξαπατήσει και το πεδίο διεύθυνσης του στο IP πακέτο για να το κάνει να εμφανιστεί ως η απάντηση από τον αληθινό εξυπηρετητή. Κάνοντας το αυτό γίνεται πιο δύσκολο για τον πελάτη να αναγνωρίσει την πηγή της ψεύτικης απάντησης. Αυτό είναι πιθανό καθώς το μηχάνημα από το οποίο πραγματοποιείται η επίθεση είναι κάτω από τον πλήρη έλεγχο του εισβολέα και θα μπορούσε πιθανών να δημιουργήσει τα πακέτα με όποιο τρόπο επιθυμούσε. Επομένως ο εισβολέας θα μεταβάλλει το IP διάγραμμα έτσι ώστε η

διεύθυνση να είναι εκείνη του πραγματικού εξυπηρετητή και θα τροποποιήσει το αναγνωριστικό του ερωτήματος στο DNS μήνυμα έτσι ώστε να εμφανίζεται ως η αληθινή απάντηση. Όταν φτάσει το πακέτο από τον πραγματικό εξυπηρετητή, το λογισμικό του πελάτη θα υποθέσει ότι έχει ήδη ολοκληρωθεί η διαδικασία για αυτό το ερώτημα και ότι απλώς το απόθεσε.

Με την παροχή των ψεύτικων πληροφοριών στον αιτούμενο ο επιτιθέμενος έχει κρατήσει τον αιτούντα από την πρόσβαση στις πληροφορίες που επιθυμεί, δημιουργώντας κατά συνέπεια άρνηση της υπηρεσίας. Ακόμα χειρότερα, ο επιτιθέμενος θα μπορούσε να αναδιευθύνει το θύμα σε οποιοδήποτε εξυπηρετητή επιθυμεί.

Το πεδίο της άρνησης της υπηρεσίας εξαρτάται από την ιδιότητα του πελάτη που έκανε την ερώτηση. Εάν το ερώτημα προήλθε από έναν αναλυτή σε ένα μηχάνημα κεντρικού υπολογιστή, είναι πιθανότερο να επηρεαστεί μόνο ένα πρόσωπο. Εάν το ερώτημα είχε σταλεί σε έναν DNS εξυπηρετητή που λειτουργεί αναδρομικά, η ψεύτικη απάντηση θα αποθηκευόταν στην προσωρινή μνήμη του κεντρικού υπολογιστή μέχρι να λήξει ο χρόνος εισόδου.

Οι επιτιθέμενοι συχνά θέτουν στο πεδίο του χρόνου μεγάλες τιμές έτσι ώστε να παραμείνουν στην προσωρινή μνήμη περισσότερο. Η διαδικασία αυτή συνήθως αναφέρεται ως DNS δηλητηρίαση (poisoning) [8]. Κάθε επόμενο ερώτημα για αυτή την εγγραφή στο κεντρικό υπολογιστή που έχει δεχτεί επίθεση θα παράγει τις ψευδείς πληροφορίες και η έκταση της άρνησης της υπηρεσίας θα αυξηθεί σημαντικά. Κάθε πελάτης, όχι μόνο ο χρήστης, εκείνου του εξυπηρετητή ονομάτων θα επηρεαζόταν από τις ψεύτικες πληροφορίες.

Ένα ερώτημα που μπορεί να σκεφτεί κάποιος είναι με ποιον τρόπο βρίσκει ο επιτιθέμενος τη σειρά του αναγνωριστικού καθώς και πως θα το χρησιμοποιήσει για να επιτεθεί στην προσωρινή μνήμη. Πρώτα ο επιτιθέμενος διαμορφώνει έναν αναλυτή έτσι ώστε να δείχνει τον εξυπηρετητή ονομάτων του θύματος. Στη συνέχεια χρησιμοποιεί τον αναλυτή για να ρωτήσει τον εξυπηρετητή του θύματος πληροφορίες για έναν κεντρικό υπολογιστή στη δική του διεύθυνση ονόματος, ή οποιαδήποτε ονόματος όπου μπορεί να επηρεάσει την κίνηση στο δίκτυο που προορίζεται για τον εξυπηρετητή ονόματος. Ο επιτιθέμενος μπορεί να χρειαστεί να το κάνει αυτό αρκετές φορές ανάλογα με πόσο δύσκολο είναι να καθορίσει την ακολουθία που χρησιμοποιείται για να παραγάγει το αναγνωριστικό του ερωτήματος. Ακόμη και στην απλούστερη περίπτωση, όπου το αναγνωριστικό αυξάνεται διαδοχικά, ο επιτιθέμενος θα έπρεπε να το κάνει αυτό δύο φορές.

Μόλις προβλέψει το αναγνωριστικό του ερωτήματος, ο επιτιθέμενος θα ρωτήσει τον εξυπηρετητή ονόματος του θύματος για πληροφορίες για τους κεντρικούς υπολογιστές σε άλλες διευθύνσεις ονόματος. Μόλις ο εξυπηρετητής ονόματος του θύματος πραγματοποιήσει μια αναδρομική αναζήτηση για να ανακαλύψει τις σωστές πληροφορίες, ο επιτιθέμενος χρησιμοποιεί το προβλεπόμενο αναγνωριστικό του ερωτήματος για να δώσει μια ψεύτικη απάντηση. Για να εξασφαλίσει ότι πλαστογραφημένη απάντηση θα ληφθεί πριν από την απάντηση από τον πραγματικό εξυπηρετητή ονόματος, ο επιτιθέμενος μπορεί ταυτόχρονα να πραγματοποιήσει άρνηση της υπηρεσίας.

Νεότερες εκδόσεις και λογισμικά έχουν αλλάξει την εφαρμογή τους για να πραγματοποιήσουν τυχαία επιλογή του αναγνωριστικού σε μία προσπάθεια να καταπολεμήσουν αυτήν την επίθεση. Ωστόσο, αυτό δε λύνει εντελώς το πρόβλημα. Αν ο επιτιθέμενος ήταν ικανός να επηρεάσει τα πακέτα που περιέχουν τα ερωτήματα, η προηγούμενη γνώση του αναγνωριστικού δεν είναι αναγκαία. Όλες οι πληροφορίες που χρειάζεται θα βρίσκονται στο πακέτο, και η μόνη απαίτηση του επιτιθέμενου είναι η ικανότητα να κάνει το πακέτο να φτάσει πριν από την απάντηση του πραγματικού εξυπηρετητή. Ξανά, ένας αποφασισμένος επιτιθέμενος θα πραγματοποιούσε άρνηση της υπηρεσίας έναντι στον πραγματικό DNS εξυπηρετητή έτσι ώστε να μην ήταν ικανός να απαντήσει, ή τουλάχιστον να μη μπορούσε να απαντήσει γρήγορα. Αυτό το σενάριο πάντως είναι λιγότερο πιθανό και αν ένας επιτιθέμενος επηρεάσει τα πακέτα σε ένα δίκτυο, ο πελάτης θα πρέπει να ανησυχεί περισσότερο για τις «δηλητηριασμένες» DNS πληροφορίες.

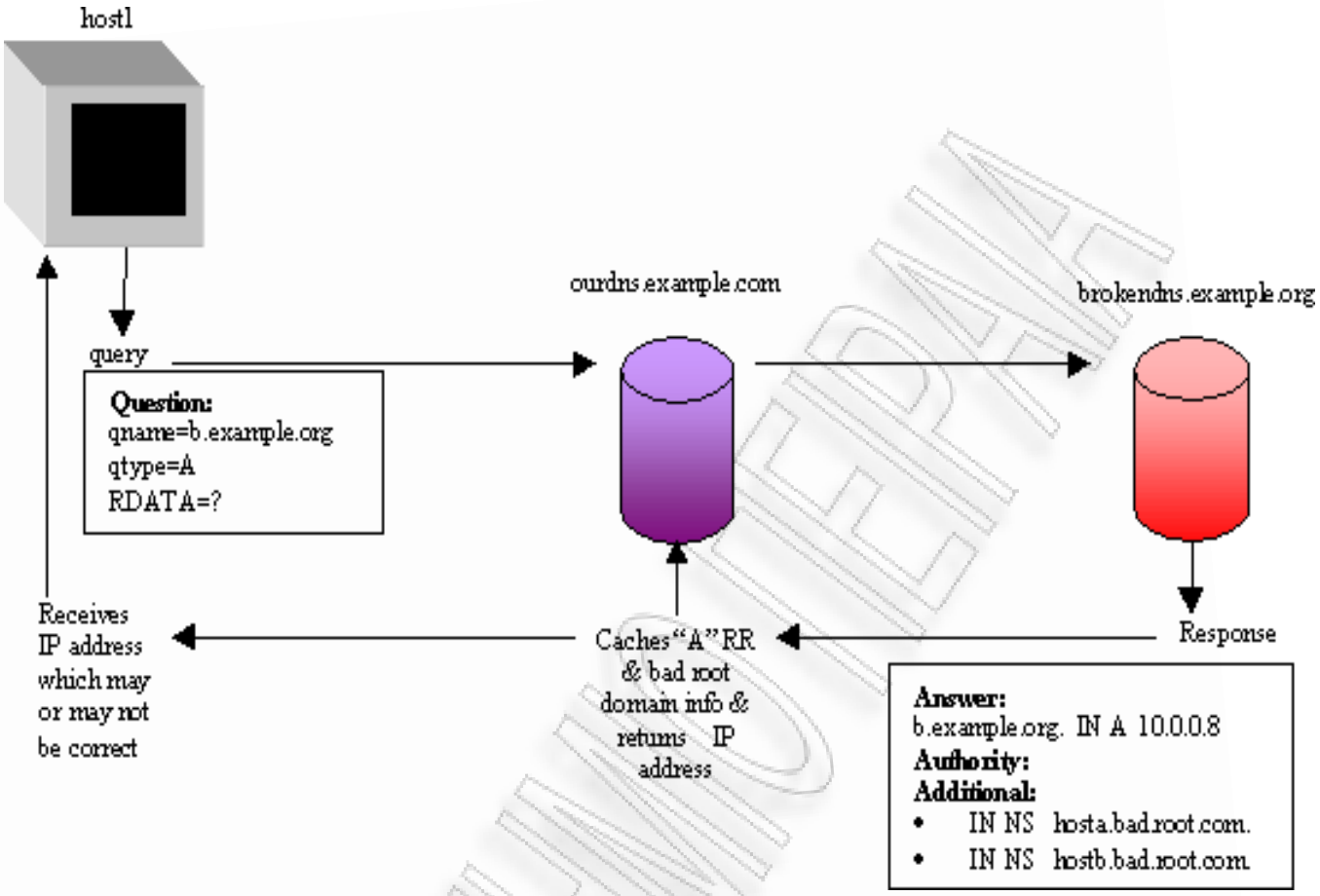
3.2.1 ΜΕΘΟΔΟΙ ΔΗΛΗΤΗΡΙΑΣΗΣ ΤΗΣ ΠΡΟΣΩΡΙΝΗΣ ΜΝΗΜΗΣ

Παλαιότερες εκδόσεις της εφαρμογής BIND του DNS ήταν ιδιαίτερα ευαίσθητες στη «δηλητηρίαση» της προσωρινής μνήμης. Ως μέσο για να δώσει μια χρήσιμη υπόδειξη, ένας

εξυπηρετητής ανταποκρίνεται σε ένα ερώτημα, αλλά όχι απαραίτητα με μια απάντηση, συμπληρώνοντας το πρόσθετο τμήμα των εγγραφών του μηνύματος απόκρισης με πληροφορίες που δεν αφορούν κατ 'ανάγκη την απάντηση. Ένας εξυπηρετητής με την αποδοχή αυτής της απόκρισης δεν έχει εκτελέσει τους αναγκαίους ελέγχους για να εξασφαλιστεί ότι οι συμπληρωματικές πληροφορίες ήταν σωστές ή ακόμα ότι σχετίζονται κατά κάποιο τρόπο με την απάντηση (δηλαδή, ότι ο εν λόγω εξυπηρετητής είναι αρμόδια αρχή για τις εγγραφές). Ο εξυπηρετητής δέχεται αυτές τις πληροφορίες και προσθέτει στην προσωρινή μνήμη το πρόβλημα της αλλοίωσης.

Άλλο ένα πρόβλημα με τις προηγούμενες εκδόσεις του BIND είναι ότι δεν υπάρχει μηχανισμός που να διαβεβαιώνει ότι η απάντηση που ελήφθη σχετίζεται με την αρχική ερώτηση. Ο εξυπηρετητής DNS που λαμβάνει την απόκριση αποθηκεύει προσωρινά την απάντηση και πάλι συμβάλλοντας στο πρόβλημα της της αλλοίωσης της προσωρινής μνήμης. Να σημειωθεί ότι αν και είναι καλά τεκμηριωμένο ότι η εφαρμογή BIND έχει βιώσει τέτοια θέματα, άλλες εφαρμογές μπορεί να είχαν, και ίσως εξακολουθούν να έχουν παρόμοια προβλήματα.

Για παράδειγμα, ας υποθέσουμε ότι υπάρχει ένα εξυπηρετητής ονόματος, γνωστός ως «ourdns.example.com», ο οποίος εξυπηρετεί ένα δίκτυο υπολογιστών (Εικόνα 5). Αυτοί οι υπολογιστές είναι στην ουσία οι DNS πελάτες. Μία εφαρμογή σε ένα σύστημα-πελάτη, η host1, δημιουργεί ένα ερώτημα DNS που αποστέλλεται στον «ourdns.example.com». Στη συνέχεια, ο «ourdns.example.com» εξετάζει την προσωρινή του μνήμη για να δει αν έχει ήδη την απάντηση στο ερώτημα. Για τους σκοπούς του παραδείγματος, ο «ourdns.example.com» δεν είναι επίσημος για το όνομα DNS στο ερώτημα ούτε έχει την απάντηση ήδη στη προσωρινή του μνήμη. Θα πρέπει να στείλει το ερώτημα σε άλλον εξυπηρετητή, ο οποίος ονομάζεται «brokendns.example.org». Οι πληροφορίες στον «brokendns.example.org» τυχαίνει να είναι λανθασμένες, συνήθως λόγω κακής ρύθμισης, και η απάντηση που στέλνεται πίσω στον «ourdns.example.com» περιέχει παραπλανητικές πληροφορίες. Εφόσον ο «ourdns.example.com» αποθηκεύει προσωρινά τις απαντήσεις, αποθηκεύει προσωρινά και αυτή την παραπλανητική πληροφορία και στέλνει την απάντηση πίσω στη host1. Όσο αυτή η πληροφορία υπάρχει στη μνήμη του «ourdns.example.com», όλοι οι πελάτες, όχι μόνο η host1, είναι πλέον ευπαθείς στη λήψη αυτής της ψεύτικης πληροφορίας.



Εικόνα 5. «Δηλητηρίαση της προσωρινής μνήμης

3.2.2 ΚΑΚΟΒΟΥΛΟΙ ΕΞΥΠΗΡΕΤΗΤΕΣ

Οι κακόβουλοι DNS εξυπηρετητές αποτελούν απειλή για την κοινότητα του Διαδικτύου, διότι οι πληροφορίες που περιέχουν μπορεί να μην είναι αξιόπιστες. Διευκολύνουν τεχνικές επίθεσης όπως η πλαστογράφηση του ονόματος του κεντρικού υπολογιστή και η πλαστογράφηση του συστήματος.

Η πλαστογράφηση του ονόματος [9] του κεντρικού υπολογιστή είναι μια ειδική τεχνική που χρησιμοποιείται με τις εγγραφές PTR. Διαφέρει ελαφρώς από τις περισσότερες τεχνικές πλαστογράφησης στο γεγονός ότι όλες οι διεξαγωγές που συμβαίνουν είναι νόμιμες, σύμφωνα με το πρωτόκολλο DNS, ενώ αυτό δεν συμβαίνει απαραιτήτως σε άλλα είδη πλαστογράφησης.

Με την πλαστογράφηση του ονόματος του κεντρικού υπολογιστή, ο εξυπηρετητής DNS προσπαθεί θεμιτά να επιλύσει ένα ερώτημα PTR χρησιμοποιώντας έναν νόμιμο εξυπηρετητή DNS για τη ζώνη που ανήκει σε αυτή τη PTR. Η εγγραφή PTR στο αρχείο δεδομένων της ζώνης για το πρωταρχικό εξυπηρετητή που έχει σκόπιμα ρυθμιστεί να δείχνει κάπου αλλού είναι συνήθως μια αξιόπιστη υποδοχή για έναν άλλο ιστοχώρο. Η πλαστογράφηση του ονόματος του κεντρικού υπολογιστή μπορεί να έχει χρόνο ισχύος μηδέν με αποτέλεσμα να μην γίνεται προσωρινή αποθήκευση των παραπλανητικών πληροφοριών, ακόμη και αν το όνομα του κεντρικού υπολογιστή πλαστογραφείται. Ένα πιο λεπτομερές παράδειγμα ακολουθεί αργότερα και αποδεικνύει την απειλή που αποτελούν τέτοιοι εξυπηρετητές για την κοινότητα του Διαδικτύου.

3.2.3 ΕΠΙΘΕΣΕΙΣ ΔΗΛΗΤΗΡΙΑΣΗΣ ΤΗΣ ΠΡΟΣΩΡΙΝΗΣ ΜΝΗΜΗΣ

Ένας επιτιθέμενος μπορεί να εκμεταλλευτεί την αδυναμία της «δηλητηρίασης» της προσωρινής μνήμης με τη χρήση πλαστογραφημένου εξυπηρετητή ονόματος και εκ

προθέσεως να διατυπώσει παραπλανητικές πληροφορίες. Αυτές οι ψευδείς πληροφορίες αποστέλλονται είτε ως απάντηση ή απλώς ως μια χρήσιμη υπόδειξη και αποθηκεύονται προσωρινά από το ανυποψίαστο DNS εξυπηρετητή.

Ένας τρόπος να εξαναγκάσει ο εισβολέας έναν ευπαθή εξυπηρετητή στην απόκτηση των ψευδών πληροφοριών είναι να στείλει ένα ερώτημα σε έναν απομακρυσμένο εξυπηρετητή, ζητώντας πληροφορίες που αναφέρονται σε μια ζώνη για την οποία ο DNS εξυπηρετητής του εισβολέα είναι επίσημος. Έχοντας προσωρινά αποθηκευμένες τις πληροφορίες, ο απομακρυσμένος εξυπηρετητής είναι πιθανό να κατευθύνει λανθασμένα τους νόμιμους πελάτες που εξυπηρετεί.

Με παλαιότερες εκδόσεις της εφαρμογής BIND, ένας επιτιθέμενος μπορεί να εισάγει ψευδείς πληροφορίες σε μία προσωρινή μνήμη, χωρίς να χρειάζεται να ανησυχεί για το αν ή όχι ένα ερώτημα δημιουργήθηκε για να επικαλεστεί μια τέτοια απόκριση. Αυτή η προθυμία να αποδέχεται και να αποθηκεύει προσωρινά κάθε μήνυμα απόκρισης επιτρέπει σε έναν εισβολέα να χειριστούν τέτοια πράγματα όπως το όνομα του υπολογιστή για τις αντιστοιχίσεις των διευθύνσεων IP, τις αντιστοιχίσεις των εγγραφών NS, κα.

3.2.4 ΣΤΟΧΟΙ ΤΩΝ ΕΠΙΘΕΣΕΩΝ

Ένας επιτιθέμενος κάνει χρήση «δηλητηρίασης» της προσωρινής μνήμης για έναν από δύο λόγους. Ο ένας είναι η άρνηση της υπηρεσίας (Denial of Service - DoS) και ο άλλος να μετασχηματιστεί σε μία έμπιστη οντότητα.

3.2.4.1 ΑΡΝΗΣΗ ΤΗΣ ΥΠΗΡΕΣΙΑΣ

Η άρνηση της υπηρεσίας επιτυγχάνεται με διάφορους τρόπους. Ένας από αυτούς είναι η εκμετάλλευση των αρνητικών αποκρίσεων (δηλαδή, οι αποκρίσεις που δείχνουν το όνομα DNS στο ερώτημα και δεν μπορούν να αναλυθούν).

Στέλνοντας πίσω την αρνητική απόκριση για το όνομα DNS που θα μπορούσε να επιλυθεί με άλλο τρόπο, οδηγεί σε μια άρνηση της υπηρεσίας για τον πελάτη που επιθυμεί να επικοινωνήσει με κάποιο τρόπο με το όνομα DNS στο ερώτημα. Ο άλλος τρόπος με τον οποίο επιτυγχάνεται η άρνησης της υπηρεσίας είναι να στείλει ένας κακόβουλος εξυπηρετητής μια απάντηση που ανακατευθύνει τον πελάτη σε ένα διαφορετικό σύστημα που δεν περιλαμβάνει την υπηρεσία που επιθυμεί.

Μια άλλη άρνηση της υπηρεσίας που συνδέεται με «δηλητηρίαση» της προσωρινής μνήμης περιλαμβάνει την εισαγωγή μιας εγγραφής CNAME σε ένα χώρο προσωρινής αποθήκευσης που αναφέρεται στον εαυτό της, όπως το κανονικό όνομα:

foobar.example.org. IN CNAME foobar.example.org.

Σε αυτό το παράδειγμα, ένας αναδρομικός εξυπηρετητής ονομάτων μπορεί να καταλήξει με αυτήν την εγγραφή πόρου στην προσωρινή του μνήμη. Αυτός ο τύπος εγγραφής CNAME συνήθως αναφέρεται ως μια αυτοαναφορική εγγραφή πόρου. Ένας εισβολέας, μετά την εισαγωγή αυτής της καταγραφής πόρου στην προσωρινή μνήμη ενός εξυπηρετητή μπορεί να προκαλέσει το όνομα του εξυπηρετητή να συντριβεί από την απλή υποβολή αιτήματος μεταβίβασης ζώνη για το foobar.example.org.

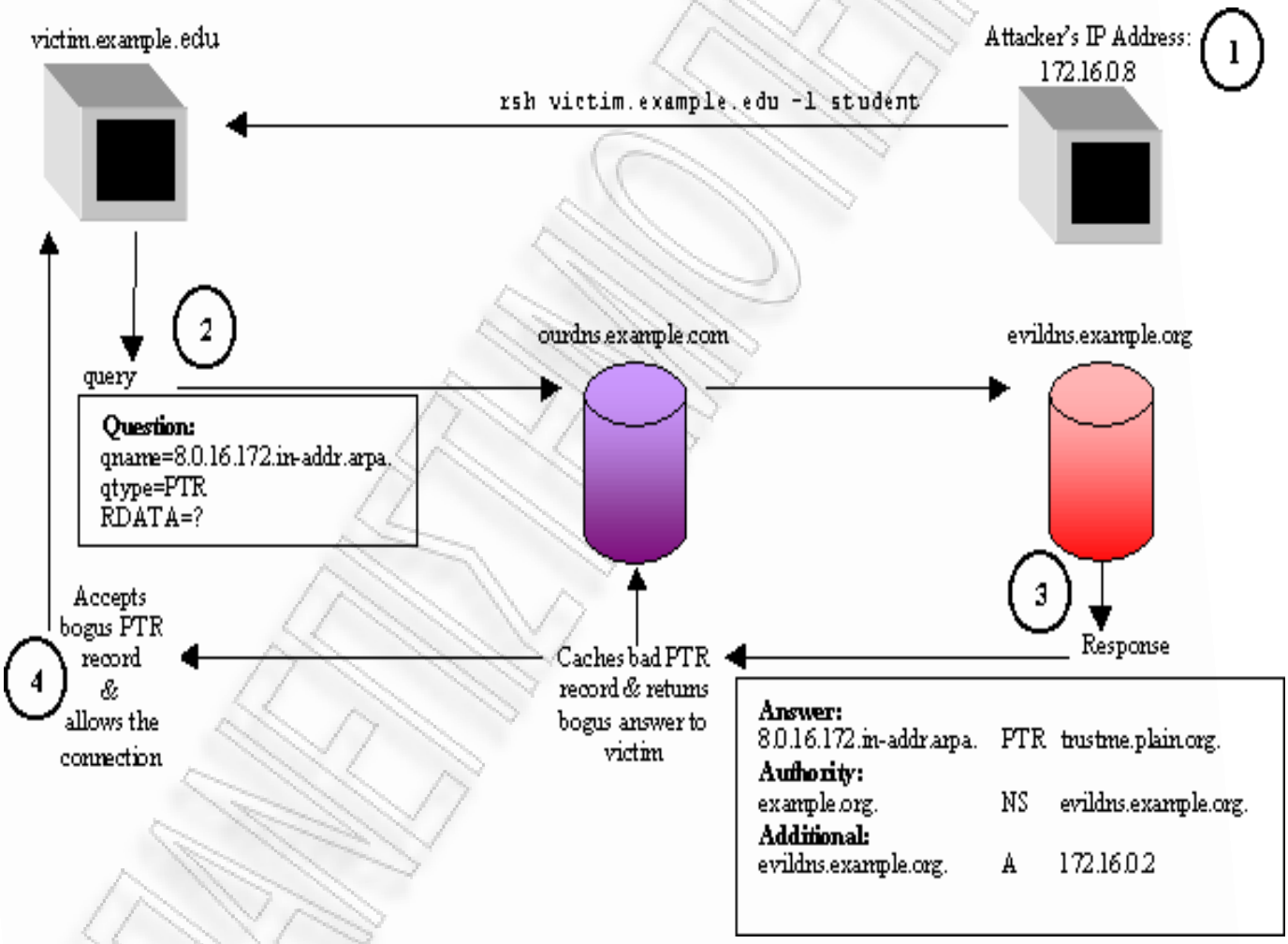
3.2.4.2 ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ ΣΕ ΜΙΑ ΑΞΙΟΠΙΣΤΗ ΟΝΤΟΤΗΤΑ

Ο δεύτερος και ενδεχομένως πιο επιβλαβής λόγος τη «δηλητηρίαση» της προσωρινής μνήμης είναι η ανακατεύθυνση των επικοινωνιών για να τον μετασχηματισμό σε μια αξιόπιστη οντότητα. Αν αυτό επιτευχθεί, ένας επιτιθέμενος μπορεί να παρακολουθεί, να αναλύει, ή/και σκόπιμα να διακόπτει τις επικοινωνίες.

Η εσφαλμένη κατεύθυνση της κίνησης μεταξύ δύο επικοινωνούντων συστημάτων διευκολύνει επιθέσεις, όπως η βιομηχανική κατασκοπεία και μπορεί να πραγματοποιηθεί σχεδόν απαρατήρητα. Ένας επιτιθέμενος μπορεί να δώσει στην παραποιημένη προσωρινή μνήμη ένα σύντομο χρονικό διάστημα ισχύος έτσι ώστε να εμφανίζεται και να εξαφανίζεται αρκετά γρήγορα για να αποφύγει τον εντοπισμό.

Οι συγκαλυμμένες επιθέσεις είναι δυνατόν απλώς να οφείλονται στο γεγονός ότι αρκετές εφαρμογές που βασίζονται στις IP χρησιμοποιούν τα ονόματα των κεντρικών υπολογιστών και / ή τις διευθύνσεις IP ως ένα μηχανισμό για την παροχή αυθεντικοποίησης που βασίζεται στον κεντρικό υπολογιστή. Αυτό επιβαρύνει το DNS με την ευθύνη της διατήρησης των ενημερώσεων και των ακριβών πληροφοριών, καμία από τις οποίες δεν μπορεί το DNS να τα εξασφαλίσει από μόνο του. Ένας επιτιθέμενος μπορεί να κάνει χρήση αυτών των ελλείψεων του DNS για να μετασχηματιστεί σε έναν αξιόπιστο κεντρικό υπολογιστή. Η αυθεντικοποίηση που βασίζεται στον κεντρικό υπολογιστή είναι τρωτή στην πλαστογράφηση του ονόματος του.

Αυτό το πρόβλημα καταδεικνύεται στην επόμενη εικόνα. Σε αυτό το παράδειγμα, ένας επιτιθέμενος επωφελείται από την εξάρτηση του προγράμματος «rshd» στο περιεχόμενο του «.rhosts» αρχείου ως μορφή της αυθεντικοποίησης που βασίζεται στον κεντρικό υπολογιστή.



Εικόνα 6. Πλαστογράφηση του ονόματος του κεντρικού υπολογιστή

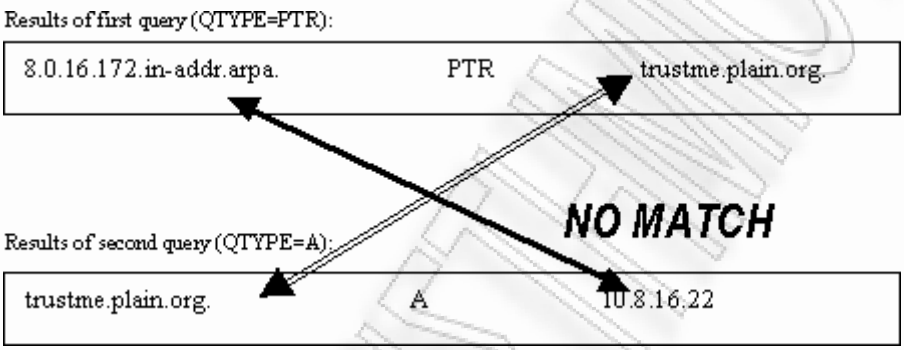
Ο DNS εξυπηρετητής του εισβολέα, ο «evildns.example.org», είναι έγκυρος για την 0.6.172. στην «-addr.arpa» και ο επιτιθέμενος έχει την ακόλουθη είσοδο σε έγκυρα δεδομένα της ζώνης, ακόμα κι αν ο επιτιθέμενος δεν έχει εξουσία στο «plain.org»:

8.0.16.172.in-addr.arpa. IN PTR trustme.plain.org.

Ο κεντρικός υπολογιστής, ο «trustme.plain.org», έχει την εμπιστοσύνη από το «victim.example.edu» απλώς και μόνο επειδή ένας μαθητής έχει το «trustme.plain.org» σωστά καταχωρημένο στο αρχείο«.rhosts» του φοιτητή στο «victim.example.edu». Για τους σκοπούς αυτού του παραδείγματος, ο «victim.example.edu» δεν προστατεύεται από κανένα firewall και δεν απασχολεί κανένα είδος λογικού ελέγχου. Το στάδιο έχει οριστεί όπου ο επιτιθέμενος μπορεί να προέρχεται πλέον από τη διεύθυνση IP του 172.16.0.8 και να συνδεθεί στο «victim.example.edu» ως φοιτητής, χωρίς κωδικό πρόσβασης και εμφανίζεται ως μία σύνδεση που όντως προήλθε από τον αξιόπιστο κεντρικό υπολογιστή ονομάτων.

Για να βοηθήσει στη διόρθωση αυτής της ευπάθειας, εφαρμογές όπως η «rlogind» έχουν τροποποιηθεί ώστε να εκτελείται ένας λογικός έλεγχος. Μετά την ανάκτηση της εγγραφής PTR, στέλνεται άλλο ένα ερώτημα που ζητά την εγγραφή "A" χρησιμοποιώντας το FQDN που καθορίζεται στο τμήμα της απάντηση της εγγραφής PTR που επιστράφηκε.

Αντί να επιβαρύνουν κάθε εφαρμογή για την εκτέλεση ενός ελέγχου ταιριάσματος, πολλά λειτουργικά συστήματα Unix έρχονται με την ίδια ικανότητα που επιτρέπει να συμβεί ο λογικός έλεγχος κατά τη διάρκεια μιας κλήσης της συνάρτησης gethostbyaddr() της βιβλιοθήκης του αναλυτή. Η συνάρτηση αυτή συνήθως χρησιμοποιείται για να βρεθεί ένα όνομα κεντρικού υπολογιστή χρησιμοποιώντας μια γνωστή διεύθυνση IP (δηλαδή, στέλνει ένα ερώτημα PTR). Η ενημερωμένη έκδοση της παρούσας συνάρτησης κάνει μια ανέξοδη αναζήτηση για την αντίστοιχη εγγραφή "A" και στη συνέχεια βεβαιώνεται ότι τα δεδομένα που ανακτώνται στις εγγραφές πόρων είναι σωστά ελεγμένα το ένα με το άλλο. Ένα παράδειγμα από τον διαγώνιο έλεγχο DNS φαίνεται στην Εικόνα 7.



Εικόνα 7. Παράδειγμα ενός διαγώνιου ελέγχου DNS που αποτυγχάνει

Δεδομένου ότι πολλές βιβλιοθήκες αναλυτών έχουν λάβει τα αναγκαία μέτρα για να εμποδίσουν την πλαστογράφηση του ονόματος του κεντρικού υπολογιστή, το στοίχημα για μια επιτυχημένη επίθεση με αυτή τη μεθοδολογία έχει αυξηθεί. Οι επιτιθέμενοι μπορούν να κάνουν χρήση της πλαστογράφησης του DNS σε συνδυασμό με την πλαστογράφηση του ονόματος του κεντρικού υπολογιστή.

Ο επιτιθέμενος ρυθμίζει τις παραμέτρους της εγγραφής πόρων PTR με το αξιόπιστο όνομα του κεντρικού υπολογιστή, όπως εξηγήθηκε παραπάνω και στη συνέχεια προσπαθεί να εισάγει στην προσωρινή μνήμη του εξυπηρετητή του θύματος την αντίστοιχη "A" εγγραφή που χαρτογραφεί το αξιόπιστο όνομα του κεντρικού υπολογιστή πίσω στην διεύθυνση IP του εισβολέα.

Όπως αναφέρθηκε προηγουμένως, οι παλαιότερες εκδόσεις του BIND είναι ιδιαίτερα ευαίσθητες σε αυτήν την επίθεση, ενώ οι πιο πρόσφατες εκδόσεις κάνουν την επιτυχία μιας τέτοιας επίθεσης πιο δύσκολη, αλλά όχι εντελώς αδύνατη. Ως εκ τούτου, η ακεραιότητα των πληροφοριών που περιέχονται στην προσωρινή μνήμη ενός εξυπηρετητή DNS θα πρέπει να παραμείνει ύποπτη μέχρι να είναι διαθέσιμες μεγαλύτερες δυνατότητες επικύρωσης.

3.2.5 ΕΠΕΚΤΕΙΝΟΝΤΑΣ ΤΟ ΠΕΔΙΟ ΔΡΑΣΗΣ

Σε τέτοιες περιπτώσεις το πεδίο δράσης είναι ακόμα περιορισμένο σε μια εγγραφή για κάποιο χρόνο και σε έναν εξυπηρετητή για κάποιο χρόνο. Ίσως μόνο μία εταιρεία να μην είναι ικανή να φτάσει τα συστήματα με μία μόνο διεύθυνση διαδικτύου ή ακόμα και με μερικές διευθύνσεις. Σε αυτήν την περίπτωση η επίδραση σε ολόκληρη την κοινότητα του Διαδικτύου θα είναι μικρή.

Θα ήταν πολύ πιο αποτελεσματικό εάν ένας επιτιθέμενος θα μπορούσε να επιτεθεί στην επίσημη πηγή των dns εγγραφών ενός οργανισμού. Σε κάποιες περιπτώσεις είναι πιθανή μία τέτοια επίθεση. Πολλές εταιρείες σήμερα χρησιμοποιούν ένα δεύτερο πρόσωπο να λειτουργεί σαν ένας εξωτερικός επίσημος DNS εξυπηρετητής. Αν και το δεύτερο πρόσωπο έχει καταχωρηθεί σαν να είναι εξουσιαστικό για τις DNS πληροφορίες, ο έλεγχος τον πληροφοριών παραμένει ουσιαστικά στην εταιρεία. Ο εξυπηρετητής του δεύτερου προσώπου είναι «σκλάβος» και μεταφέρει όλες τις πληροφορίες από τον πραγματικά πρωταρχικό εξυπηρετητή του οργανισμού. Αυτός είναι γνωστός ως αόρατος πρωταρχικός. Είναι επίσης ευπαθής σε επιθέσεις «δηλητηρίασης».

Αντί να προσπαθήσει να εξαπατήσει την απάντηση σε ένα μόνο ερώτημα, ο επιτιθέμενος προσπαθεί να επηρεάσει την μεταφορά μιας ολόκληρης ζώνης ανάμεσα στον πρωταρχικό DNS εξυπηρετητή και στον «σκλάβο» λειτουργώντας ως η επίσημη απάντηση. Καθώς υπάρχει μικρή διαφορά ανάμεσα στην τυποποίηση του DNS μηνύματος και της μεταφοράς ζώνης, οι επιθέσεις είναι παρόμοιες με αυτές που περιγράφηκαν προηγουμένως. Μία από τις μεγαλύτερες διαφορές είναι ότι τα μηνύματα στέλνονται μέσω UDP ενώ οι ζώνες μεταφέρονται μέσω TCP. Η επίδραση της επίθεσης στις πληροφορίες ενός εξουσιαστικού DNS εξυπηρετητή θα είναι πολύ μεγαλύτερη.

Τελικά κάθε σύστημα που επιθυμεί να μάθει τις μεταφρασμένες πληροφορίες για αυτή τη διεύθυνση ονόματος θα κάνει το ερώτημα στον εξυπηρετητή που έχει δεχτεί την επίθεση. Οι ψευδείς πληροφορίες θα πολλαπλασιαστούν σε κάθε DNS εξυπηρετητή που κάνει αναζήτηση στη «δηλητηριασμένη» διεύθυνση ονόματος. Κανένας δε θα μπορεί να φτάσει τη διεύθυνση στην οποία πραγματοποιήθηκε η επίθεση και ο επιτιθέμενος θα ανακατευθύνει την κίνηση όποτε το επιθυμεί.

Η διαφορά ανάμεσα σε αυτήν την επίθεση και στην επίθεση «δηλητηρίασης» της κρυφής μνήμης είναι λεπτή αλλά ουσιώδης. Στη «δηλητηρίαση» της κρυφής μνήμης μόνο τα συστήματα που χρησιμοποιούν τον «δηλητηριασμένο» εξυπηρετητή ονόματος μπορούν να επηρεαστούν. Όταν η βάση δεδομένων μιας διεύθυνσης ονόματος δημοσιεύσει τον εξυπηρετητή ονόματος που έχει δεχτεί την επίθεση όλοι ζητούν μία επίσημη απάντηση για πληροφορίες σχετικά με την διεύθυνση ονόματος που επηρεάστηκε.

3.3 ΥΠΕΡΧΕΙΛΙΣΗ ΠΕΛΑΤΩΝ

Η υπερχείλιση πελατών συμβαίνει όταν ένα σύστημα-πελάτη στέλνει ένα ερώτημα, αλλά λαμβάνει και αποδέχεται χιλιάδες DNS απαντήσεις από τον επιτιθέμενο. Η επιτυχία της επίθεσης βασίζεται στην έλλειψη της αυθεντικοποίησης των απαντήσεων αυτών. Η επίθεση εμφανίζεται σαν να προέρχεται από τον αναμενόμενο εξυπηρετητή ονόματος, αλλά χωρίς ισχυρή αυθεντικοποίηση, και ο πελάτης δεν έχει τη δυνατότητα να ελέγξει την προέλευση των απαντήσεων. Αυτή η επίθεση μπορεί να χρησιμοποιηθεί αντί της πλαστογράφησης DNS στην προσπάθεια να πλαστογραφήσει ένα όνομα κεντρικού υπολογιστεί μια εφαρμογή.

3.4 ΑΔΥΝΑΜΙΕΣ ΤΗΣ ΔΥΝΑΜΙΚΗΣ ΕΝΗΜΕΡΩΣΗΣ ΤΟΥ DNS

Το RFC 1035, στο οποίο περιγράφονται οι λεπτομέρειες του συστήματος και του πρωτόκολλου DNS, προσδοκά τις ζώνες DNS να αλλάζουν αργά, και έτσι ορίζει ένα στατικό DNS όπου οι αλλαγές πραγματοποιούνται μόνο στα αρχεία ζώνης στον πρωταρχικό εξυπηρετητή και συνήθως μέσω μιας αυτόματης διαδικασίας. Οι δυναμικές ενημερώσεις DNS είναι μια τροποποίηση στο RFC 1035 που επιτρέπει δυναμική ενημέρωση των πληροφοριών DNS που περιέχονται σε μια ζώνη για όσο διάστημα πληρούνται αρκετές προϋποθέσεις.

Πρωτόκολλα όπως το Πρωτόκολλο Δυναμικών Διαμορφώσεων του κεντρικού υπολογιστή (Dynamic Host Configuration Protocol - DHCP) μπορούν να κάνουν τότε

χρήση του πρωτόκολλου δυναμικής ενημέρωσης για να προσθέσουν και να διαγράψουν εγγραφές πόρων σε πρώτη ζήτηση. Οι ενημερώσεις αυτές πραγματοποιούνται στον πρωταρχικό εξυπηρετητή για τη ζώνη. Οι ενημερώσεις λαμβάνουν τη μορφή προσθηκών και διαγραφών.

Το πρωτόκολλο δυναμικών ενημερώσεων διαθέτει προβλέψεις για τον έλεγχο των συστημάτων που επιτρέπεται να ενημερώσουν δυναμικά τον πρωταρχικό εξυπηρετητή. Ακόμη και αν είναι απασχολημένος, αποτελεί μια αδύναμη μορφή του ελέγχου πρόσβασης και είναι ευάλωτος σε απειλές όπως η πλαστογράφηση της IP του συστήματος που εκτελεί τις ενημερώσεις ή την έκθεση του συστήματος.

Ένας επιτιθέμενος μπορεί να εκτελέσει μια ποικιλία επιθέσεων δυναμικής ενημέρωσης εναντίον του πρωταρχικού εξυπηρετητή. Μπορούν να κυμανθούν από επιθέσεις άρνησης της υπηρεσίας, όπως η διαγραφή των εγγραφών, σε κακόβουλες ανακατευθύνσεις, για παράδειγμα, αλλάζοντας τις πληροφορίες της διεύθυνσης IP για μία εγγραφή πόρων που στέλνεται σε μια ενημέρωση.

3.5 ΔΙΑΡΡΟΗ ΠΛΗΡΟΦΟΡΙΩΝ

Άλλες απειλές για το DNS περιλαμβάνουν μεταφορές ζώνης που μπορούν να διαρρεύσουν πληροφορίες σχετικά με εσωτερικά δίκτυα σε έναν πιθανό εισβολέα. Συχνά, τα ονόματα των κεντρικών υπολογιστών μπορούν να αντιπροσωπεύσουν τα ονόματα των προγραμμάτων που μπορεί να ενδιαφέρουν ή να αποκαλύψουν το λειτουργικό σύστημα μιας μηχανής. Ο αποκλεισμός των μεταφορών ζώνης αποδεικνύεται ότι είναι μια μάταιη προσπάθεια για την πρόληψη τέτοιου είδους διαρροών πληροφοριών.

Ένας επιτιθέμενος μπορεί να κάνει χρήση των εργαλείων DNS για αυτόματα ερωτήματα, κάθε διεύθυνση IP για ένα διάστημα διεύθυνσης ονόματος, μία προς μία, σε μια προσπάθεια να μάθει το όνομα του κεντρικού υπολογιστή DNS ή να βρει τις διευθύνσεις IP που δεν έχουν εκχωρηθεί. Το τελευταίο κίνητρο για την αποκάλυψη αχρησιμοποίητων διευθύνσεων IP μπορεί να επιτρέψει σε έναν επιτιθέμενο να χρησιμοποιήσει την πλαστογράφηση της IP για να μετασχηματιστεί σε έναν κεντρικό υπολογιστή ενός αξιόπιστου δικτύου. Εάν ένα σύστημα εμπιστεύεται ένα ολόκληρο δίκτυο IP, αντί να καθορίσει κάθε κεντρικό υπολογιστή που εμπιστεύεται, τότε το σύστημα μπορεί να είναι ευάλωτο σε μια επίθεση με τη χρήση μιας μη προσδιορισμένης διεύθυνση IP.

3.6 ΕΚΘΕΣΗ ΤΩΝ ΕΓΚΥΡΩΝ ΔΕΔΟΜΕΝΩΝ ΕΝΟΣ DNS ΕΞΥΠΗΡΕΤΗΤΗ

Άλλες απειλές κατά των DNS εξυπηρετητές περιλαμβάνουν την εξής απειλή: όταν ένας επιτιθέμενος αποκτήσει δικαιώματα διαχειριστή (π.χ. αποτελεί τον ριζικό υπολογιστή σε συστήματα Unix) με σκοπό την τροποποίηση των πληροφοριών ζώνης για την οποία ο εξυπηρετητής είναι επίσημος. Αυτό επιτυγχάνεται μέσω των άλλων αδυναμιών στον εξυπηρετητή που δεν σχετίζονται απαραίτητα με το DNS. Η προσεκτική διαμόρφωση του εξυπηρετητή μπορεί να παρέχει κάποια προστασία για αυτές τις απειλές.

Τέτοια πράγματα όπως η χρήση της τελευταίας έκδοσης του BIND, η ελαχιστοποίηση του αριθμού των άλλων υπηρεσιών που προσφέρονται στο ίδιο μηχάνημα, ο περιορισμός της πρόσβασης μόνο σε διαχειριστές, η ενασχόληση της διαιρεμένης τεχνολογίας DNS, κλπ. είναι ζωτικής σημασίας για μια ασφαλέστερη υπηρεσία DNS για έναν οργανισμό. Δυστυχώς, αυτό δεν παρέχει ισχυρή προστασία κατά της παραποίησης των δεδομένων στα αρχεία DNS στον εξυπηρετητή. Τα κατάλληλα μέτρα ασφαλείας που απαιτούνται για την παροχή επαρκούς προστασίας στο πλαίσιο του DNS θα μπορούσαν να επιτευχθούν μόνο με τη DNSSEC.

ΚΕΦΑΛΑΙΟ 4. DNSSEC

4.1 ΕΙΣΑΓΩΓΗ

Το 1994, ο IETF συγκρότησε μία ομάδα εργασίας για να παράσχει επεκτάσεις ασφάλειας στο DNS πρωτόκολλο ως απάντηση στα θέματα ασφαλείας που περιέβαλλαν το DNS [10]. Αυτές οι επεκτάσεις συνήθως αναφέρονται ως επεκτάσεις DNSSEC. Αυτές οι βελτιώσεις ασφάλειας στο πρωτόκολλο σχεδιάστηκαν για να είναι διαλειτουργικές με τις εφαρμογές του DNS που δε ήταν ενήμερες για την ασφάλεια.

Οι βελτιώσεις αυτές επιτεύχθηκαν με τη χρήση της διάταξης των εγγραφών πόρων του DNS οι οποίες ήταν σχεδιασμένες με τέτοιο τρόπο ώστε να δέχονται επεκτάσεις. Η ομάδα εργασίας όρισε ένα νέο σύνολο εγγραφών πόρων για να κρατήσει την ασφαλή πληροφορία που παρέχει ισχυρή ασφάλεια στις ζώνες του DNS επιθυμώντας να εφαρμόσει την DNSSEC. Αυτοί οι νέοι τύποι των εγγραφών πόρων χρησιμοποιούνται σε συνδυασμό με τις υπάρχουσες εγγραφές πόρων. Αυτό επιτρέπει τις απαντήσεις στα ερωτήματα για τις ασφαλείς πληροφορίες που ανήκουν σε μία ζώνη να προστατεύονται από την DNSSEC αλλά και να υποστηρίζονται από μη ασφαλείς DNS εξυπηρετητές.

Για να αποκτήσει διαδεδομένη αποδοχή η ομάδα εργασίας αναγνώρισε ότι η DNSSEC πρέπει να παρέχει συμβατότητα και να έχει τη δυνατότητα να συνυπάρχει με μη ασφαλείς εφαρμογές. Αυτό επιτρέπει στους ιστοχώρους να εφαρμόσουν την DNSSEC όταν είναι έτοιμοι και επιτρέπει λιγότερη πολυπλοκότητα όταν αναβαθμίζεται. Αυτό σημαίνει επίσης ότι το λογισμικό του πελάτη που δεν χρησιμοποιεί DNSSEC μπορεί ακόμα να επεξεργαστεί σωστά σύνολα εγγραφών που λαμβάνονται από έναν εξυπηρετητή DNSSEC.

Οι ήδη υπάρχοντες μηχανισμοί ασφάλειας καθώς και κάποιοι που βρίσκονταν υπό κατασκευή, δεν αποτελούσαν ακόμη πρότυπα τα οποία θα μπορούσαν να παίξουν ένα ρόλο στην ασφάλεια της αρχιτεκτονικής. Επίσης τα υπάρχοντα εργαλεία ασφάλειας δεν παρείχαν επαρκή προστασία και ανάμεσα στα διάφορα πρωτόκολλα ασφαλείας αναγνωρίστηκε πως ο πυρήνας είναι η DNSSEC. Η προστασία που παρέχει στην έγχυση λανθασμένων πληροφοριών προσωρινής μνήμης είναι ζωτικής σημασίας για τις απαιτήσεις ασφαλείας του Διαδικτύου.

4.2 ΠΕΔΙΟ ΔΡΑΣΗΣ ΤΗΣ DNSSEC

Ο σκοπός των επεκτάσεων ασφάλειας στο σύστημα ονοματοδοσίας των διευθύνσεων μπορεί να συνοψιστεί σε τρεις υπηρεσίες [5]: κατανομή κλειδιού, αυθεντικοποίηση της προέλευσης των δεδομένων και διεξαγωγή και αίτηση της αυθεντικοποίησης.

4.2.1 ΚΑΤΑΝΟΜΗ ΚΛΕΙΔΙΟΥ

Η υπηρεσία κατανομής κλειδιού όχι μόνο επιτρέπει την ανάκτηση του δημοσίου κλειδιού ενός ονόματος διεύθυνσης για να πιστοποιήσει την αυθεντικότητα των δεδομένων ζώνης του DNS, αλλά επίσης παρέχει έναν μηχανισμό διαμέσου του οποίου κάθε κλειδί που σχετίζεται με ένα όνομα μπορεί να χρησιμοποιηθεί για σκοπούς εκτός του συστήματος DNS. Η υπηρεσία κατανομής του δημοσίου κλειδιού υποστηρίζει μερικούς διαφορετικούς τύπους κλειδιών και μερικούς διαφορετικούς τύπους αλγορίθμων κλειδιού.

4.2.2 ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΤΗΣ ΠΡΟΕΛΕΥΣΗΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Η αυθεντικοποίηση της προέλευσης των δεδομένων είναι κρίσιμη για τον σχεδιασμό της DNSSEC. Η υπηρεσία αυτή μετριάζει απειλές όπως η παραποίηση της κρυφής μνήμης και ο συμβιβασμός των δεδομένων ζώνης σε έναν DNS εξυπηρετητή. Το σύνολο των εγγραφών πόρων σε μία ζώνη υπογράφεται κρυπτογραφικά και έτσι δίνει ένα υψηλό επίπεδο βεβαιότητας στους αναλυτές και στους εξυπηρετητές ότι τα δεδομένα που μόλις λήφθηκαν είναι έμπιστα.

Η DNSSEC χρησιμοποιεί την τεχνολογία των ψηφιακών υπογραφών για να υπογράψει ένα σύνολο εγγραφών πόρων. Η ψηφιακή υπογραφή περιέχει τον κρυπτογραφημένο κατακερματισμό του συνόλου των εγγραφών πόρων. Ο κατακερματισμός είναι ένας κρυπτογραφημένος έλεγχος αθροίσματος των δεδομένων που περιέχονται στο

σύνολο των εγγραφών πόρων. Ο κατακερματισμός υπογράφεται (για παράδειγμα κρυπτογραφείται ηλεκτρονικά) με τη χρήση ενός ιδιωτικού κλειδιού το οποίο συνήθως ανήκει στον εισηγητή της πληροφορίας, ο οποίος είναι γνωστός ως ο υπογράφων ή η αρχή υπογραφής. Ο παραλήπτης του συνόλου των εγγραφών πόρων μπορεί τότε να ελέγξει την ψηφιακή υπογραφή ενάντια στα δεδομένα του συνόλου των εγγραφών πόρων που μόλις λήφθηκαν.

Ο παραλήπτης το κάνει αυτό αποκρυπτογραφώντας πρώτα την ψηφιακή υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του υπογράφοντος για να αποκτήσει τον αυθεντικό κατακερματισμό των δεδομένων. Στη συνέχεια ο παραλήπτης υπολογίζει τον δικό του κατακερματισμό στο σύνολο εγγραφών πόρων των δεδομένων χρησιμοποιώντας τον ίδιο κρυπτογραφικό αλγόριθμο υπολογισμού αθροίσματος, και συγκρίνει τα αποτελέσματα του κατακερματισμού που βρέθηκε στην ψηφιακή υπογραφή με τον κατακερματισμό που υπολόγισε. Εάν οι δύο τιμές ταιριάζουν, τα δεδομένα είναι ακέραια και η προέλευση των δεδομένων είναι αυθεντική.

4.2.3 ΔΙΕΞΑΓΩΓΗ ΚΑΙ ΑΙΤΗΣΗ ΤΗΣ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ

Η διεξαγωγή και η αίτηση της αυθεντικοποίησης παρέχει την ικανότητα για αυθεντικοποίηση των DNS αιτημάτων και των DNS επικεφαλίδων των μηνυμάτων. Αυτό εγγυάται ότι η απάντηση είναι η απόκριση του αυθεντικού ερωτήματος και ότι η απόκριση προήλθε από τον εξυπηρετητή στον οποίο απευθυνόταν το ερώτημα. Έτσι πραγματοποιείται η παροχή της βεβαιότητας και για τα δύο.

Μέρος της πληροφορίας, που επιστράφηκε σαν απάντηση σε ένα ερώτημα για από έναν ασφαλή εξυπηρετητή, είναι μια υπογραφή. Αυτή η υπογραφή παράγεται από την αλληλουχία του ερωτήματος και της απόκρισης. Αυτό επιτρέπει σε έναν αναλυτή που αντιλαμβάνεται την ασφάλεια να εκτελεί κάθε αναγκαία επαλήθευση σχετικά με τη διεξαγωγή.

Άλλη μία ιδιότητα της χρήσης της διεξαγωγής και της αίτησης για αυθεντικοποίηση είναι για τις δυναμικές ενημερώσεις του DNS. Χωρίς τη DNSSEC η δυναμική ενημέρωση του DNS δεν παρέχει ένα μηχανισμό ο οποίος να απαγορεύει κάθε σύστημα με πρόσβαση σε έναν επιτακτικό DNS εξυπηρετητή να ενημερώνει τις πληροφορίες ζώνης. Για να παράσχει η ασφάλεια για τέτοιες τροποποιήσεις, η ασφαλής δυναμική ενημέρωση DNS ενσωματώνει τη DNSSEC για δώσει ισχυρή αυθεντικοποίηση στα συστήματα που επιτρέπουν τον δυναμικό χειρισμό της πληροφορίας της ζώνης στον πρωταρχικό εξυπηρετητή.

4.3 ΕΓΓΡΑΦΕΣ ΠΟΡΩΝ ΤΗΣ DNSSEC

Ο IETF δημιούργησε μερικές νέες DNS εγγραφές πόρων για να υποστηρίξει τις δυνατότητες ασφάλειας που παρέχονται από τις επεκτάσεις της DNSSEC. Οι συναφείς με το DNS εγγραφές είναι η KEY RR [6], η SIG RR [6] και η NXT RR [6]. Η DNSSEC χρησιμοποιεί την KEY RR για την αποθήκευση κρυπτογραφικών δημοσίων κλειδιών, ένα δημόσιο κλειδί για κάθε KEY RR.

Η KEY RR χρησιμοποιείται για την επαλήθευση της υπογραφής ενός συνόλου DNS εγγραφών πόρων. Η υπογραφή για ένα σύνολο εγγραφών πόρων αποθηκεύεται στην SIG RR. Η υπογραφή χρησιμοποιείται για να αποδείξει την αυθεντικότητα και την ακεραιότητα της πληροφορίας που περιέχεται στο σύνολο εγγραφών των πόρων. Η NXT RR είναι μία ανύπαρκτη εγγραφή και χρησιμοποιείται για να διαβεβαιώσει κρυπτογραφικά την μη ύπαρξη ενός συνόλου εγγραφών πόρων.

Υπάρχει και άλλη εγγραφή, γνωστή ως CERT RR [6], η οποία δεν φέρνει επιπρόσθετες λειτουργίες ασφάλειας στο DNS, αλλά παρέχεται έτσι ώστε τα πιστοποιητικά δημοσίου κλειδιού να μπορούν να φυλαχθούν εντός του συστήματος για χρήση σε εφαρμογές έξω από το DNS. Με τον ίδιο τρόπο όπως μια εφαρμογή που επιθυμεί να επικοινωνήσει με έναν απομακρυσμένο υπολογιστή IP δημιουργεί ένα ερώτημα A για την ανάλυση του ονόματος του κεντρικού υπολογιστή, μια εφαρμογή ασφαλείας που επιθυμεί να εκτελέσει κρυπτογράφηση με άλλη οντότητα δημιουργεί ένα CERT ερώτημα για να ανακτήσει το δημόσιο κλειδί του πιστοποιητικού της οντότητας.

4.3.1 KEY RR

Το κλειδί για ένα όνομα DNS κρατιέται σε μία KEY RR. Οποιοσδήποτε τύπος ερωτήματος για ένα όνομα DNS, που βρίσκεται σε μία ασφαλή ζώνη, οδηγεί σε μια απόκριση που περιέχει την απάντηση στο ερώτημα. Η KEY RR που συνδέεται με το όνομα DNS μπορεί να συνοδεύσει αυτή την απάντηση. Ο αναλυτής που δημιουργεί το ερώτημα μπορεί να επικυρώσει, στη συνέχεια, τα δεδομένα χρησιμοποιώντας τη KEY RR χωρίς να χρειάζεται να στείλει ένα άλλο ερώτημα για το την KEY RR. Αυτό ελαχιστοποιεί τον αριθμό των ερωτημάτων που απαιτούνται για κάθε συγκεκριμένο όνομα DNS που βρίσκεται σε μία ασφαλή ζώνη.

Η DNSSEC χρησιμοποιεί τη KEY RR για την αποθήκευση των κρυπτογραφικών δημόσιων κλειδιών: ωστόσο, αυτό δεν είναι ένα πιστοποιητικό δημόσιου κλειδιού. Αντ' αυτού, η CERT RR χρησιμοποιείται για την αποθήκευση των πιστοποιητικών δημόσιου κλειδιού. Το κλειδί που βρίσκεται στο τμήμα RDATA της KEY RR ανήκει στο όνομα DNS που καταχωρήθηκε πρώτη στην KEY RR (δηλαδή, το όνομα του κατόχου). Το όνομα του κατόχου μπορεί να αντιπροσωπεύει μια ζώνη, έναν κεντρικό υπολογιστή, έναν χρήστη κλπ.

Η KEY RR περιέχει πληροφορίες που δηλώνουν τα χαρακτηριστικά ασφαλείας του κλειδιού και την επιτρεπόμενη χρήση του για το συγκεκριμένο όνομα κατόχου. Παρέχει πληροφορίες για την ασφάλεια, όπως το δημόσιο κλειδί, τον τύπο του αλγόριθμου, τον τύπο του πρωτοκόλλου, καθώς και τις ετικέτες που καθορίζουν αυτά τα πράγματα ως προς το εάν ή όχι το όνομα DNS έχει ένα δημόσιο κλειδί.

Ο αλγόριθμος δημόσιου κλειδιού καθορίζει την πραγματική μορφή του δημόσιου κλειδιού που βρίσκεται στο τμήμα RDATA της KEY RR. Διάφοροι αλγόριθμοι κλειδιού έχουν ήδη υποστηριχθεί, όπως ο αλγόριθμος RSA/MD5, ο αλγόριθμος Diffie-Hellman, ο αλγόριθμος Ψηφιακής υπογραφής (DSA), και ο αλγόριθμος ελλειπτικής καμπύλης. Μόνο η υποστήριξη του Αλγόριθμου Ψηφιακής υπογραφής είναι υποχρεωτική.

Ένας άλλος τομέας είναι γνωστός ως το πρωτόκολλο των bytes. Αυτό δείχνει για ποιο πρωτόκολλο είναι έγκυρο το δημόσιο κλειδί. Μερικά πρωτόκολλα έχουν ήδη ανατεθεί και είναι το TLS, το e-mail, η DNSSEC, και το IPsec. Δεδομένου ότι και το πεδίο αλγόριθμων δημοσίου κλειδιού και το πρωτόκολλο των bytes είναι ένα πεδίο των 8 bit, θεωρητικά μπορούν να χρησιμοποιηθούν έως και 255 διαφορετικοί αλγόριθμοι και 255 διαφορετικά πρωτόκολλα σε συνδυασμό με το δημόσιο κλειδί.

Δύο bits από τα δεκαέξι που χρησιμοποιούνται για τον καθορισμό των διαφόρων ετικετών είναι γνωστά ως bits τύπου. Και οι τέσσερις συνδυασμοί των bits τύπου δείχνουν τον τρόπο με τον οποίο μπορεί να χρησιμοποιηθεί η KEY RR. Πρόκειται για την εμπιστευτικότητα, την αυθεντικοποίηση, την εμπιστευτικότητα και την αυθεντικοποίηση, ή κανένα. Το τελευταίο υποδηλώνει ότι δεν υπάρχει κλειδί για το όνομα DNS.

Με αυτόν τον τρόπο, μπορεί κανείς να βεβαιώσει κρυπτογραφικά ότι το συγκεκριμένο όνομα κατόχου δεν διαθέτει ένα κλειδί ακόμα και αν βρίσκεται σε μία ασφαλή ζώνη. Τα άλλα δύο bits χρησιμοποιούνται για τον εντοπισμό τριών ειδών των οντοτήτων στις οποίες ανήκει αυτό το κλειδί, όπως ο χρήστης, η ζώνη, ή κάτι που δεν είναι ζώνη. Υποδεικνύοντας έναν κεντρικό υπολογιστή με αυτές τις ετικέτες στην πραγματικότητα γίνεται με τη χρήση των ετικετών για να δείξει ότι το όνομα DNS δεν είναι μια ζώνη. Έτσι ένας κεντρικός υπολογιστής υπονοείται και δεν καθορίζεται από τις ετικέτες.

4.3.2 SIG RR

Μια υπογραφή που φυλάσσεται σε έναν άλλο τύπο εγγραφών πόρου είναι γνωστή ως SIG RR. Η SIG RR παρέχει την αυθεντικοποίηση για ένα σύνολο εγγραφής πόρων και το χρόνο ισχύος της υπογραφής του. Σε μια ασφαλή ζώνη, το σύνολο εγγραφών πόρων έχει μία ή περισσότερες SIG RR που συνδέονται με αυτό. Η κατάσταση των περισσότερων από μίας SIG RR για ένα δεδομένο σύνολο εγγραφών πόρων μπορεί να προκύψει όταν περισσότεροι από έναν αλγόριθμο κρυπτογράφησης χρησιμοποιούνται για την υπογραφή του συνόλου εγγραφών πόρων. Μερικοί ιστοχώροι μπορούν να επιλέξουν να το κάνουν αυτό για ζητήματα όπως η κρυπτογραφική έξοδος περιορισμών.

Ένας αριθμός πεδίων βρίσκεται επίσης στο τμήμα RDATA μιας SIG RR. Το πεδίο υπογραφής κατέχει την υπογραφή που ανήκει σε ένα συγκεκριμένο σύνολο εγγραφών πόρων. Για να υποδηλωθεί ο τύπος της εγγραφής του συνόλου εγγραφών πόρων (δηλαδή,

NS, PTR, MX, κ.λπ.), χρησιμοποιείται ένα πεδίο «κρυφού τύπου». Για να ελεγχθεί η υπογραφή, ένας αναλυτής ή ένας εξυπηρετητής θα πρέπει να γνωρίζει το όνομα του υπογράφοντος. Αυτό διευκρινίζεται στο πεδίο του υπογράφοντος. Η SIG RR έχει ένα πεδίο αλγορίθμου όμοιο με εκείνο στην KEY RR. Αφού οι υπογραφές έχουν χρόνους λήξης, όπως και οι μεμονωμένες εγγραφές πόρων, η SIG RR έχει κάποια πεδία χρόνου.

Εκτός από τις SIG RR που χρησιμοποιήθηκαν για τις διεξαγωγές και που ζήτησαν την αυθεντικοποίηση και εκτός από τις SIG RR που αποτελούν συγκεκριμένα το στόχο για ένα ερώτημα, οι εξυπηρετητές που αντιλαμβάνονται την ασφάλεια προσπαθούν να συμπεριλάβουν στην απόκριση τις SIG RR που χρειάζονται για την αυθεντικοποίηση του συνόλου εγγραφών πόρων. Έτσι, ένας αναλυτής μπορεί ακόμη να λάβει απάντηση από ένα σύνολο εγγραφών πόρων που ανήκει σε μια ασφαλή ζώνη η οποία δεν έχει τη SIG RR. Η κατάσταση αυτή μπορεί να συμβεί, κατά κανόνα, όταν ο περιορισμός μεγέθους υπερβαίνεται εξ αιτίας της SIG RR ή όταν η απάντηση προέρχεται από έναν εξυπηρετητή που δεν αντιλαμβάνεται την ασφάλεια. Υπό αυτές τις συνθήκες, οι αναλυτές που αντιλαμβάνονται την ασφάλεια χρειάζεται να διαμορφώσουν ένα άλλο ερώτημα το οποίο θα ζητούσε συγκεκριμένα όλες τις ελλείποντες SIG RR που χρειάζονται για να ολοκληρωθεί η διαδικασία επαλήθευσης.

4.3.3 NXT RR

Το DNS παρέχει τη δυνατότητα προσωρινής αποθήκευσης των αρνητικών απαντήσεων. Μια αρνητική απάντηση, σημαίνει ότι ένα αντίστοιχο σύνολο εγγραφών πόρων δεν υπάρχει για το ερώτημα. Η DNSSEC παρέχει υπογραφές για αυτά τα ανύπαρκτα σύνολα εγγραφών πόρων έτσι ώστε η μη ύπαρξη τους σε μια ζώνη να μπορεί να πιστοποιηθεί. Αυτό επιτυγχάνεται μέσω της χρήσης του NXT RR. Οι NXT RR χρησιμοποιούνται για να υποδείξουν μια κλίμακα ονομάτων DNS που δεν είναι διαθέσιμα ή μια κλίμακα τύπων εγγραφών πόρων που δεν είναι διαθέσιμα για ένα υπάρχον όνομα DNS.

Δύο πιθανότητες υπάρχουν για τα ανύπαρκτα ονόματα DNS. Η μία είναι ότι το ίδιο το όνομα δεν έχει καθόλου εγγραφές πόρων: απλά δεν υπάρχει. Η άλλη πιθανότητα είναι το όνομα DNS να μην υπάρχει (για παράδειγμα, έχει τουλάχιστον ένα τύπο εγγραφής πόρων), αλλά ο τύπος αυτός δεν υπάρχει στο ερώτημα για αυτό το όνομα.

Για να χειριστεί απόδειξη της μη ύπαρξης ενός ονόματος DNS, όλες οι εγγραφές σε μια ζώνη ταξινομούνται με έναν τρόπο που μοιάζει με κάποιους τρόπους αλφαβητικής σειρά. Η τεχνική που χρησιμοποιείται είναι γνωστή ως κανονική σειρά.

Στη συνέχεια, όταν ένα ερώτημα έχει ληφθεί για ένα ανύπαρκτο όνομα, μία NXT RR στέλνεται πίσω και περιέχει το όνομα DNS του επόμενου αλφαβητικά, ή μάλλον κανονικά, συνόλου εγγραφών DNS μετά το όνομα του ερωτήματος. Για να χειριστεί την απόδειξη της μη ύπαρξης ενός τύπου εγγραφής πόρων για ένα υπάρχον όνομα DNS, ένα NXT RR στέλνεται πίσω με το όνομα DNS και τους τύπους των εγγραφών πόρων που έχει το όνομα στην πραγματικότητα. Όταν οι SIG RR έχουν δημιουργηθεί για μια ζώνη, πρέπει να δημιουργηθούν και όλες οι NXT RR για μια ζώνη.

4.4 ΕΞΥΠΗΡΕΤΗΤΕΣ ΠΟΥ ΑΝΤΙΛΑΜΒΑΝΟΝΤΑΙ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι εξυπηρετητές που αντιλαμβάνονται την ασφάλεια είναι η πηγή όλων των σχετικών με την ασφάλεια πληροφοριών στο πλαίσιο του DNS. Κάθε δοσμένος πρωταρχικός DNS εξυπηρετητής έχει τρεις βασικές λειτουργίες: τη διαχείριση των έγκυρων πληροφοριών της ζώνης, τη διαχείριση της προσωρινής αποθήκευσης των πληροφοριών DNS, και την ανταπόκριση στα ερωτήματα του πελάτη.

Ένας πρωταρχικός DNS εξυπηρετητής που αντιλαμβάνεται την ασφάλεια έχει αυξημένες αρμοδιότητες σε κάθε μία από αυτές τις λειτουργίες. Η διαχείριση των αυθεντικών πληροφοριών ζώνης για έναν εξυπηρετητή που αντιλαμβάνεται την ασφάλεια περιλαμβάνει την προσθήκη της SIG RR, του κλειδιού, και της NXT RR στο αρχείο της κύριας βάσης δεδομένων μιας ζώνης. Οι SIG RR δημιουργούνται για τα σύνολα των εγγραφών των πόρων που ανήκουν σε μια ζώνη. Το ιδιωτικό κλειδί χρησιμοποιείται για να παράγει τη SIG RR που ανήκει στην ίδια ζώνη.

Από τη στιγμή που τα ιδιωτικά κλειδιά των εξυπηρετητών είναι περισσότερο από πιθανό ότι βρίσκονται σε απευθείας σύνδεση, είναι πιθανό ότι αυτά τα κλειδιά θα

μπορούσαν να τεθούν σε κίνδυνο. Το ιδιωτικό κλειδί της ζώνης, σε αντίθεση, διατηρείται εκτός σύνδεσης για τις περισσότερους σκοπούς, έτσι η έκθεση του είναι λιγότερο πιθανή και η εγκυρότητα των δεδομένων είναι περισσότερο εξασφαλισμένη. Το ιδιωτικό κλειδί της ζώνης ανακτάται περιοδικά για να υπογραφούν εκ νέου όλες τις εγγραφές που βρίσκονται μέσα στη ζώνη. Από τη στιγμή που δημιουργούνται οι νέες SIG RR περιλαμβάνονται με τις υπόλοιπες πληροφορίες στο κύριο αρχείο της ζώνης .Οι NXT RR, επίσης, θα πρέπει να δημιουργούνται στον εξυπηρετητή και να τοποθετούνται στο κύριο αρχείο μιας ζώνης κάθε φορά που δημιουργούνται οι SIG RR.

Η σε απευθείας σύνδεση υπογραφή διεξάγεται επίσης στον εξυπηρετητή. Για κάθε διεξαγωγή και αυθεντικοποίηση για τα ερωτήματα DNS, ο εξυπηρετητής που διατυπώνει την απάντηση πρέπει να χρησιμοποιήσει το ιδιωτικό του κλειδί για την υπογραφή, και όχι το κλειδί της ζώνης, δεδομένου ότι διατηρείται εκτός σύνδεσης.

Μια άλλη περίπτωση στην οποία ένα κλειδί ζώνης δεν χρησιμοποιείται για την υπογραφή είναι για διεξαγωγή και αυθεντικοποίηση ενός αιτήματος για δυναμικές ενημερώσεις. Πρέπει να χρησιμοποιηθεί το ιδιωτικό κλειδί του κεντρικού υπολογιστή που διαμορφώνει το αίτημα. Επειδή τα ερωτήματα DNS και τα αιτήματα δυναμικής ενημέρωσης μπορεί να συμβούν αρκετά συχνά, τα ιδιωτικά κλειδιά του υπογράφοντος πρέπει να διατηρηθούν εντός σύνδεσης. Η προστασία αυτών των συνδεδεμένων ιδιωτικών κλειδιών είναι υψίστης σημασίας.

Για να πραγματοποιηθεί η προσωρινή αποθήκευση, ένας εξυπηρετητής που αντιλαμβάνεται την ασφάλεια πρέπει να διαχειριστεί σωστά την προσωρινή αποθήκευση όλων των εγγραφών πόρων που αφορούν την ασφάλεια. Η πρόσθετη ευθύνη για την προσωρινή αποθήκευση ξεκινά με τη διατήρηση των τεσσάρων καταστάσεων προσωρινή αποθήκευσης.

Μία κατάσταση, η οποία έχει μια αντίστοιχη κατάσταση σε έναν εξυπηρετητή που δεν αντιλαμβάνεται την ασφάλεια, είναι η "Κακή". Σε σε έναν εξυπηρετητή που δεν αντιλαμβάνεται την ασφάλεια, όταν ληφθεί μια κακή απάντηση οι πληροφορίες που περιέχονται διαφθείρονται κατά κάποιο τρόπο, ο εξυπηρετητής πετάει το μήνυμα απόκρισης χωρίς να το αποθηκεύσει προσωρινά (και συνήθως καταγράφει το συμβάν). Με τον ίδιο τρόπο, ένας εξυπηρετητής που δεν αντιλαμβάνεται την ασφάλεια μπορεί να πετάξει μια κακή απάντηση, αλλά στην προκειμένη περίπτωση, μια κακή απάντηση σημαίνει ότι η SIG RR απέτυχε να επαληθεύσει τα δεδομένα. Ακόμη και αν το σύνολο των εγγραφών των πόρων στην απάντηση μπορεί να φαίνεται θεμιτό, η αποτυχία ελέγχου των δεδομένων με την αντίστοιχη υπογραφή είναι μια μοιραία κατάσταση.

Οι τρεις άλλες καταστάσεις είναι «Ανασφαλής», «Αυθεντικοποιημένος», και «Εκκρεμής». Η κατάσταση «Ανασφαλής» σημαίνει ότι δεν υπάρχουν διαθέσιμα στοιχεία ώστε να χρησιμοποιηθούν για να ελεγχθεί η γνησιότητα του συνόλου εγγραφών πόρων. Αυτό δεν σημαίνει ότι τα δεδομένα είναι κακά, απλά ότι δεν μπορούν να αυθεντικοποιηθούν. Αυτό συμβαίνει συνήθως για σύνολα εγγραφών πόρων από μη ασφαλείς ζώνες. Η κατάσταση «Αυθεντικοποιημένη» σημαίνει ότι η προσωρινή αποθήκευση του συνόλου εγγραφών πόρων έχει επικυρωθεί πλήρως μέσω της χρήσης των SIG RR και KEY RR. Η κατάσταση «Εκκρεμής» σημαίνει τα προσωρινά αποθηκευμένα δεδομένα βρίσκονται ακόμα στη διαδικασία ελέγχου.

Μια άλλη ευθύνη ενός εξυπηρετητή με προσωρινή αποθήκευση, είναι όταν λήγει ένα αποθηκευμένο σύνολο εγγραφών πόρων. Μόλις ένα σύνολο εγγραφών πόρων αποθηκεύεται στην κρυφή μνήμη, μια αντίστροφη μέτρηση προς το μηδέν από τον αρχικό χρόνο ισχύος ξεκινά και διατηρείται για τα προσωρινά αποθηκευμένα αρχεία. Μόλις φτάσει στο μηδέν, το σύνολο εγγραφών πόρων αφαιρείται από την προσωρινή μνήμη.

Για τους εξυπηρετητές που αντιλαμβάνονται την ασφάλεια, αυτό έχει αλλάξει λίγο. Ο χρόνος ισχύος δεν μπορεί να είναι ο μόνος χρόνος που υπάρχει έτσι ώστε να διαπιστωθεί πότε ένα προσωρινά αποθηκευμένο σύνολο εγγραφών πόρων έχει λήξει. Σε συνδυασμό με τον χρόνο ισχύος χρησιμοποιούνται δύο νέοι χρόνοι και τελικά καθορίζουν την χρονική στιγμή που θα λήξει το σύνολο των εγγραφών πόρων από την προσωρινή μνήμη. Οι νέοι χρόνοι χρησιμοποιούνται για να καθοριστεί πότε λήγει η χρονική περίοδος εγκυρότητας της υπογραφής για το αυθεντικοποιημένο σύνολο των εγγραφών πόρων, και όχι μόνο για τη χρονική στιγμή που το σύνολο των εγγραφών πόρων θα πρέπει να λήξει. Αυτοί οι νέα χρόνοι φυλάσσονται στη SIG RR και είναι γνωστοί ως χρόνος έναρξης της υπογραφής και χρόνος λήξης της υπογραφής.

Για εξυπηρετητές και τους πελάτες που αντιλαμβάνονται την ασφάλεια αυτές οι πληροφορίες είναι πολύ πιο σημαντικές για να βασίσουν τη λήξη δεδομένου ότι είναι κρυπτογραφικά βεβαιωμένη. Αν και ο χρόνος λήξης της υπογραφής φαίνεται να έχει σχέση με τον χρόνο ισχύος, λόγω των προς τα πίσω ζητημάτων συμβατότητας, το πεδίο χρόνου ισχύος δεν μπορεί να εξαλειφθεί.

Ο χρόνος ισχύος είναι ακόμα ενσωματωμένος για τη λήξη των αυθεντικοποιημένων συνόλων εγγραφών πόρων. Εάν ο χρόνος ισχύος λήγει πριν από το χρόνο λήξης της υπογραφή, ο χρόνος ισχύος είναι μειωμένος και το σύνολο των εγγραφών πόρων λήγει όταν ο χρόνος ισχύος μηδενιστεί. Εάν ο χρόνος λήξης της υπογραφής λήγει πριν από το χρόνο ισχύος, χρόνο ισχύος προσαρμόζεται με το χρόνο λήξης της υπογραφής και στη συνέχεια προχωρά η κανονική αντίστροφη μέτρηση του χρόνου ισχύος.

Η απόκριση στα ερωτήματα του πελάτη, περιλαμβάνει τώρα τις απαντήσεις στα ερωτήματα και από αναλυτές που αντιλαμβάνονται την ασφάλεια και από αυτούς που δεν την αντιλαμβάνονται. Όταν ένας αναλυτής που δεν αντιλαμβάνεται την ασφάλεια δημιουργήσει ένα ερώτημα για τις πληροφορίες που περιέχονται σε ασφαλή ζώνη και το στείλει σε έναν εξυπηρετητή που αντιλαμβάνεται την ασφάλεια, ο εξυπηρετητής μπορεί να ανταποκριθεί είτε με κατάσταση «Αυθεντικοποιημένες» είτε με την κατάσταση «Ανασφαλείς».

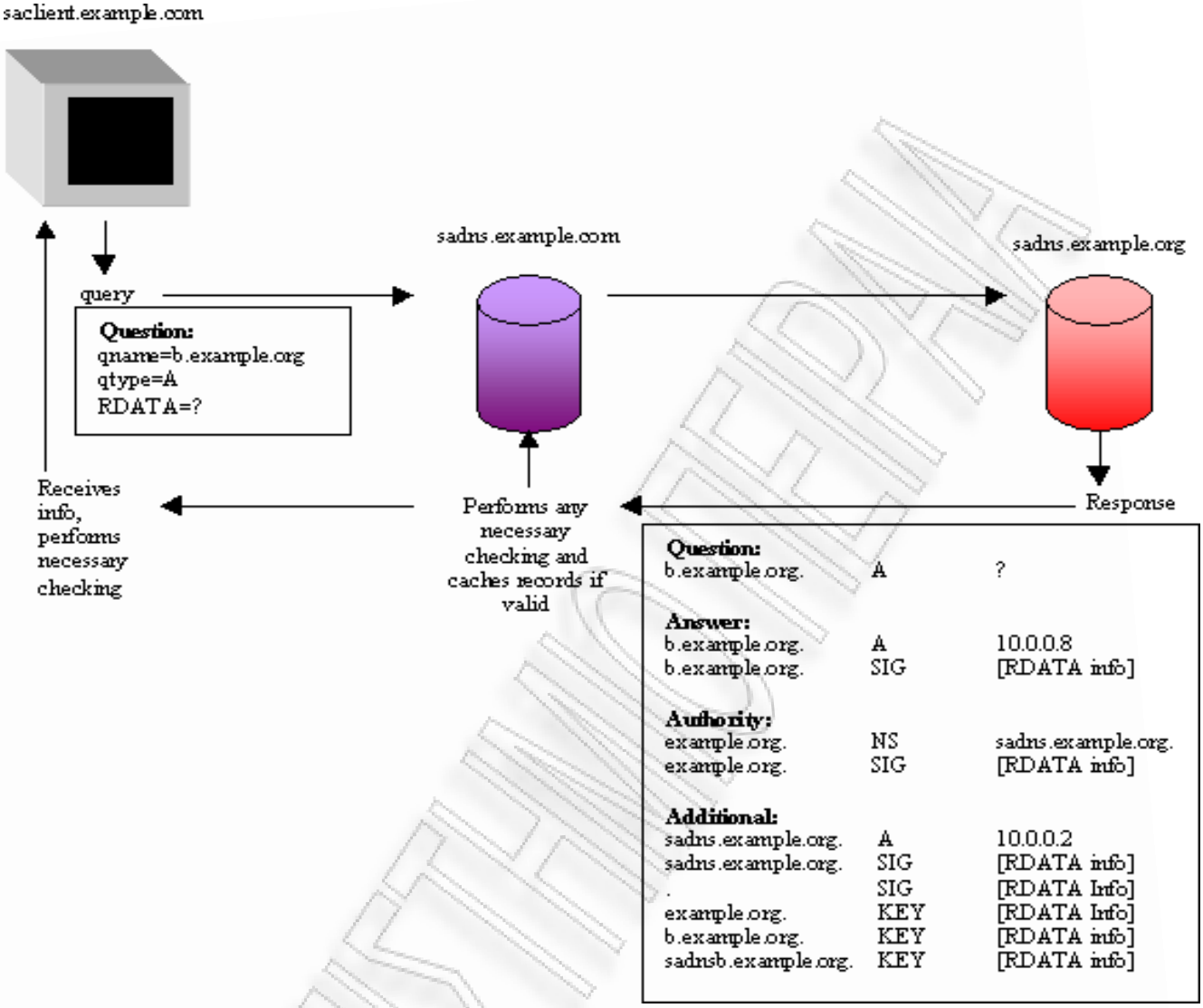
Ο εξυπηρετητής μπορεί να στείλει την κατάσταση «Εκκρεμή» δεδομένα μόνο όταν τεθεί η ετικέτα απενεργοποιημένου ελέγχου(CD). Ο εξυπηρετητής που αντιλαμβάνεται την ασφάλεια μπορεί γνωρίζει να μη στείλει δεδομένα με εκκρεμή κατάσταση, επειδή ένας αναλυτής ο οποίος δεν συμμετέχει στη DNSSEC ποτέ δε θέτει την ετικέτα CD σε ένα ερώτημα DNS. Από τη στιγμή που θα σταλούν δεδομένα με «ανασφαλή» κατάσταση είναι το ίδιο με το DNS χωρίς την DNSSEC, ο αναλυτής που δεν αντιλαμβάνεται την ασφάλεια επεξεργάζεται το μήνυμα απόκρισης ως συνήθως. Όσον αφορά τη λήψη δεδομένων με κατάσταση «Αυθεντικοποιημένα»,ο αναλυτής που δεν αντιλαμβάνεται την ασφάλεια βασικά αγνοεί τις πρόσθετες πληροφορίες ασφάλειας και προχωράει στην διαδικασία της απόκρισης ως συνήθως.

Όταν τα ερωτήματα προέρχονται από αναλυτές που αντιλαμβάνονται την ασφάλεια, είναι ιδιαίτερα ενθαρρυντικό το γεγονός ότι ο αναλυτής θέτει την ετικέτα CD. Με την ετικέτα αυτή στο ερώτημα, οι εξυπηρετητές που αντιλαμβάνονται την ασφάλεια μπορεί να στέλνουν δεδομένα με «Εκκρεμή» κατάσταση. Η αποστολή των δεδομένων αυτών επιτυγχάνει δύο πράγματα. Μειώνει το χρόνο απόκρισης απελευθερώνοντας πόρους του εξυπηρετητή για το χειρισμό των ερωτημάτων και επιτρέπει σε έναν αναλυτή να εφαρμόσει τις πολιτικές του για τα δεδομένα που εκκρεμούν, ανεξάρτητα από τους εξυπηρετητές.

Εάν η απάντηση στο ερώτημα είναι ήδη αυθεντικοποιημένα δεδομένα στο εξυπηρετητή, ο εξυπηρετητής δημιουργεί την ετικέτα αυθεντικοποιημένων δεδομένων (AD) για να δηλώσει στον αναλυτή ότι οι αναγκαίοι έλεγχοι έχουν ήδη πραγματοποιηθεί. Με αυτό τον τρόπο ο αναλυτής δεν χρειάζεται να κάνει όλους τους ελέγχους επαλήθευσης της ασφαλείας.

4.5 ΠΕΛΑΤΕΣ ΠΟΥ ΑΝΤΙΛΑΜΒΑΝΟΝΤΑΙ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι πελάτες που αντιλαμβάνονται την ασφάλεια έχουν επίσης αυξημένες αρμοδιότητες σε σχέση με τους πελάτες που δεν την αντιλαμβάνονται. Αυτές οι αυξημένες αρμοδιότητες υπεισέρχονται στη γνώση της επεξεργασίας των εγγραφών πόρων της DNSSEC. Η Εικόνα 8 παρουσιάζει μια DNSSEC διεξαγωγή που επικαλείται από έναν αναλυτή που αντιλαμβάνεται την ασφάλεια σε έναν εξυπηρετητή που αντιλαμβάνεται την ασφάλεια:



Εικόνα 8. Μηνύματα αιτήματος και απόκρισης της DNSSEC

Στην πιο απλή του μορφή, ένας πελάτης που αντιλαμβάνεται την ασφάλεια, ο «saclient.example.com», θέτει ερώτημα για μία εγγραφή πόρου τύπου A για το όνομα «b.example.org». Ο εξυπηρετητής που αντιλαμβάνεται την ασφάλεια, ο «sadns.example.com», στέλνει το ερώτημα στο «sadns.example.com». Η ζώνη, «example.org», είναι μια ασφαλής ζώνη και ας υποθέσουμε, για αυτό το παράδειγμα μόνο, ότι δεν υπάρχει περιορισμός μεγέθους στο μήνυμα απάντησης. Αφού το όνομα «b.example.org» έχει μια εγγραφή τύπου A και ο «sadns.example.org» είναι εξυπηρετητής που αντιλαμβάνεται την ασφάλεια, η απάντηση έρχεται πίσω με όλες τις απαραίτητες εγγραφές πόρων της DNSSEC.

Πρώτα να σημειωθεί ότι υπάρχει ένα SIG RR που επιστρέφεται μαζί με την A RR στον τομέα της απάντησης του μηνύματος απόκρισης. Οι εξυπηρετητές που αντιλαμβάνονται την ασφάλεια θα πρέπει να προσπαθήσουν να επιστρέψουν τη SIG RR που χρειάζεται σε μια ασφαλή διεξαγωγή. Η συμπερίληψη της SIG RR δεν αποτελεί προϋπόθεση, διότι, εάν το όριο μεγέθους του μηνύματος απόκρισης υπερβεί όταν προστεθεί η SIG RR, η SIG RR θα πρέπει να παραλειφθεί, αλλά αν συμβεί αυτό, ο πελάτης πρέπει να εξετάσει την απάντηση που έχει περικοπεί.

Ο πελάτης έπειτα θέτει ερώτημα για τη SIG RR ξεχωριστά. Από τη στιγμή που αυτό το παράδειγμα δεν έχει περιορισμούς χώρου, περιλαμβάνεται εδώ. Αυτή η SIG RR απαιτείται στο τμήμα της απάντησης, διότι παρέχει την απαραίτητη αυθεντικοποίηση και την απόδειξη της ακεραιότητας των δεδομένων που αφορούν ειδικά στην A RR για το

«b.example.org». Ο υπογράφων της SIG RR είναι η ζώνη (δηλαδή, το ιδιωτικό κλειδί της ζώνης χρησιμοποιήθηκε για την υπογραφή για τα δεδομένα).

Η εγγραφή NS στο τμήμα της αρχής φαίνεται να υπάρχει, επειδή ο «sadns.example.org» είναι ο μοναδικός εξυπηρετητής DNS για τη ζώνη «example.org» και είναι επιτακτική για τις πληροφορίες στον τομέα της απάντησης. Όπως και με τη SIG RR που εμφανίζονται στον τομέα της απάντησης, αυτή η SIG RR καλείται να εμφανιστεί στο τμήμα αυτό, δεδομένου ότι περιλαμβάνει την υπογραφή για την εγγραφή NS. Ο υπογράφων της SIG RR είναι και πάλι η ζώνη.

Η δεύτερη εγγραφή "A" είναι η εγγραφή της διεύθυνσης που ανήκει στον εξυπηρετητή «sadns.example.org» και εμφανίζεται στον πρόσθετο τομέα όπως θα εμφανιζόταν σε ένα κανονικό μήνυμα απόκρισης. Συνοδευτικά με την εγγραφή A υπάρχει η αντίστοιχη SIG RR, έτσι ώστε ο πελάτης να μπορεί να ελέγξει και αυτή την A RR. Η μόνη περίπτωση στην οποία ο πελάτης δεν πρόκειται να εξετάσει μια περικομμένη απάντηση είναι όταν η παραληφθείσα SIG RR ανήκει σε μια RR στον πρόσθετο τομέα. Τέτοια είναι η περίπτωση αυτής της SIG RR. Με άλλα λόγια, αν το πακέτο απόκρισης δεν θα μπορούσε να ταιριάξει αυτή τη SIG RR χωρίς να ξεπεράσει το όριο μεγέθους, η SIG RR παραλείπεται, αλλά η απόκριση δεν θεωρείται ότι έχει περικοπεί.

Επίσης, εμφανίζεται στον πρόσθετο τομέα η τέταρτη SIG RR. Δεδομένου ότι ο πελάτης αντιλαμβάνεται την ασφάλεια, έχει ζητήσει διεξαγωγή και αυθεντικοποίηση.. Ως αποτέλεσμα, ο εξυπηρετητής «sadns.example.org» δημιουργεί μία SIG RR υπολογίζοντας την υπογραφή της συνένωσης των μηνυμάτων του ερωτήματος και της απάντησης.

Να σημειωθεί ότι το όνομα του κατόχου αυτής της εγγραφής πόρου SIG είναι η "." για να αντιπροσωπεύσει το μηδενικό μήκος της ετικέτα που είναι κρατημένη για τον ριζικό εξυπηρετητή. Το όνομα του κατόχου, η κατηγορία και ο χρόνος ισχύος αυτού του τύπου της SIG RR δεν έχουν σημασία για τη διεξαγωγή και την αίτηση της διαδικασίας της αυθεντικοποίησης και, συνεπώς, συνιστάται ότι η "." μπορεί να χρησιμοποιηθεί για εξοικονόμηση χώρου.

Το πεδίο του υπογράφοντος, ωστόσο, αυτής της SIG RR είναι σημαντικό για τη διαδικασία επαλήθευσης και θα πρέπει να είναι το όνομα του εξυπηρετητή που δημιουργεί την απόκριση. Το πεδίο αυτό βρίσκεται στον τομέα RDATA. Δεδομένου ότι ο πελάτης ζήτησε διεξαγωγή και αυθεντικοποίηση, ένας εξυπηρετητής που αντιλαμβάνεται την ασφάλεια δεν πρέπει να παραλείψει αυτή τη SIG RR. Θεωρείται ύψιστης προτεραιότητας και η ένταξή της είναι υποχρεωτική.

Τρεις KEY RR εμφανίζονται στο πρόσθετο τμήμα του μηνύματος απόκρισης. Η πρώτη KEY RR ανήκει στην ζώνη «example.org». Ο πελάτης μπορεί να χρησιμοποιήσει αυτό το κλειδί για την επαλήθευση όλων των SIG RR εκτός από την τελευταίο που αφορά τη διεξαγωγή και την αυθεντικοποίηση. Ο εξυπηρετητής περιλαμβάνει δύο ακόμα KEY RR, ως αποτέλεσμα των A εγγραφών που περιλαμβάνονται στο τμήμα της απάντησης και στο πρόσθετο τμήμα. Αυτές είναι οι KEY RR για το «b.example.org» και τον «sadns.example.org».

Σε ένα πραγματικό κόσμο, οι περιορισμοί του μεγέθους έχουν εφαρμογή στα μηνύματα απάντησης. Αν το μήνυμα απόκρισης είναι μεγαλύτερο από το όριο, τότε οι KEY RR είναι οι πρώτες που θα μείνουν έξω από το μήνυμα. Στο τμήμα των πρόσθετων πληροφοριών, οι A RR έχουν μεγαλύτερη προτεραιότητα από ό, τι οι KEY RR. Σε γενικές γραμμές, οι SIG RR έχουν μεγαλύτερη προτεραιότητα από ό, τι οι KEY RR και, ως εκ τούτου, ο εξυπηρετητής παραλείπει τις KEY RR πριν παραλείψει οποιαδήποτε SIG RR. Η μόνη εξαίρεση σε αυτό είναι όταν ο τύπος του ερωτήματος είναι για την KEY RR. Εάν πρόκειται για ερώτημα τέτοιου τύπου, ο εξυπηρετητής πρέπει να την συμπεριλάβει, εάν υπάρχει.

4.5.1 ΑΝΑΚΤΗΣΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Οι αναλυτές μπορούν να αποκτήσουν τα δημόσια κλειδιά των ζωνών με έναν από δύο τρόπους. Μπορούν να χρησιμοποιήσουν το DNS για την αναζήτηση για ένα δημόσιο κλειδί ή μπορούν να είναι στατικά ρυθμισμένοι με το κλειδί [7]. Ανεξάρτητα από τη μέθοδο που χρησιμοποιείται, προβλήματα υπάρχουν και με τα δύο.

Στην περίπτωση όπου τα κλειδιά έχουν ανακτηθεί μέσω του DNS, προκύπτει το ζήτημα της εμπιστοσύνης του κλειδιού. Για να είναι έμπιστο το ανακτηθέν κλειδί, πρέπει

να υπογραφεί και αυτή η υπογραφή πρέπει να είναι αξιόπιστη. Για να υπάρχει η διαβεβαίωση ότι η υπογραφή για το κλειδί είναι αξιόπιστη αυτό σημαίνει ότι το δημόσιο κλειδί από την αρχή της υπογραφής πρέπει επίσης να ληφθεί, να υπογραφεί και να βρεθεί αξιόπιστο και ούτω καθεξής. Η λύση για να σταματήσει αυτή η αναδρομική αλυσίδα των γεγονότων είναι να ρυθμιστεί ο μεσολαβητής με το δημόσιο κλειδί που επικυρώνει τα υπογεγραμμένα κλειδιά κάτω από αυτό. Με άλλα λόγια, ένα αξιόπιστο κλειδί ζώνης μπορεί να χρησιμοποιηθεί ως σημείο εκκίνησης για την επαλήθευση όλων των κλειδιών που βρέθηκαν κάτω από αυτό. Ένα πιθανό σύνολο των αξιόπιστων δημόσιων κλειδιών με τα οποία μια ασφαλή ζώνη μπορεί να είναι στατικά ρυθμισμένη είναι εκείνο του από τη ριζική ζώνη.

Η στατική ρύθμιση ενός μεσολαβητή με τα δημόσια κλειδιά από πολλές διαφορετικές ζώνες έχει ένα πλεονέκτημα στο ότι ο συμβιβασμός ενός ιδιωτικού κλειδιού της ζώνης δεν έχει ως αποτέλεσμα τον συμβιβασμό από τα κλειδιά για όλες τις άλλες ζώνες. Το μειονέκτημα της στατικής ρύθμισης κάθε μεσολαβητή με τα κλειδιά για πολλές διαφορετικές ζώνες είναι ότι δεν έχει καλή διαβάθμιση. Εάν ένα κλειδί για μια ζώνη πρέπει να αλλάξει, τότε όλοι οι μεσολαβητές πρέπει να ρυθμιστούν ώστε να αντικατοπτρίζουν αυτή την αλλαγή.

ΚΕΦΑΛΑΙΟ 5. ΣΥΝΔΥΑΣΜΟΣ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΜΕ ΤΑ DOMAIN NAMES

5.1 ΕΙΣΑΓΩΓΗ

Τα TLS και DTLS χρησιμοποιούν πιστοποιητικά για την αυθεντικοποίηση του εξυπηρετητή. Οι χρήστες θέλουν οι αιτήσεις τους να επιβεβαιώνουν ότι το πιστοποιητικό που παρέχεται από τον TLS εξυπηρετητή συνδέεται στην πραγματικότητα με το όνομα διεύθυνσης που αναμένουν.

Η DNSSEC παρέχει έναν μηχανισμό για έναν χειριστή ζώνης για να υπογράψει άμεσα τις dns πληροφορίες. Κατ αυτόν τον τρόπο, οι συνδέσεις των κλειδιών για τα ονόματα διευθύνσεων βεβαιώνονται όχι από εξωτερικές οντότητες, αλλά από τις οντότητες που χειρίζονται το dns. Στη συνέχεια θα καθοριστεί πότε ένας εξυπηρετητής υποστηρίζει TLS και θα περιγράφει ο τρόπος χρήσης ασφαλούς dns για τη σύνδεση του πιστοποιητικού του κεντρικού υπολογιστή TLS με το προοριζόμενο όνομα περιοχών. Τέλος, θα οριστεί η εγγραφή πόρων έγκρισης της αρχής πιστοποίησης του DNS.

5.2 ΚΑΘΟΡΙΖΟΝΤΑΣ ΟΤΙ ΕΝΑΣ ΕΞΥΠΗΡΕΤΗΤΗΣ ΥΠΟΣΤΗΡΙΖΕΙ TLS

Οι περισσότερες εφαρμογές πελάτη-εξυπηρετητή που είναι τυποποιημένες στην IETF έχουν δύο τρόπους: έναν μη ασφαλή τρόπο που δεν περιλαμβάνει την αυθεντικοποίηση ή προστασία της ακεραιότητας των δεδομένων, και έναν ασφαλή τρόπο που απαιτεί (τουλάχιστον) ότι ο πελάτης αυθεντικοποιεί τον εξυπηρετητή και να δημιουργεί ένα κανάλι επικοινωνίας με προστασία της ακεραιότητας των δεδομένων. Στις περισσότερες περιπτώσεις, ο ασφαλής τρόπος επιτυγχάνεται με την έναρξη μιας συνεδρίας TLS και, όταν είναι επιτυχής, εκτελεί τον μη-ασφαλή τρόπο μέσα σε αυτή.

Στο σημείο αυτό να σημειωθεί ότι το TLS είναι ένας τύπος μεθόδου ελέγχου ταυτότητας που χρησιμοποιεί το πρωτόκολλο επεκτάσιμης αυθεντικοποίησης (Extensible Authentication Protocol - EAP) και ένα πρωτόκολλο ασφάλειας που καλείται Transport Layer Security (TLS). Το EAP-TLS χρησιμοποιεί πιστοποιητικά που χρησιμοποιούν κωδικούς πρόσβασης. Ο έλεγχος ταυτότητας EAP-TLS υποστηρίζει δυναμική διαχείριση κλειδιών. Το πρωτόκολλο TLS προορίζεται για την ασφάλεια και τον έλεγχο ταυτότητας επικοινωνιών σε δημόσιο δίκτυο μέσω κρυπτογράφησης δεδομένων. Το πρωτόκολλο TLS επιτρέπει στο εξυπηρετητή και τον πελάτη να παρέχουν αμοιβαίο έλεγχο ταυτότητας και να διαπραγματεύονται έναν αλγόριθμο κρυπτογράφησης και κρυπτογραφημένα κλειδιά πριν τη μετάδοση των δεδομένων.

5.2.1 ΕΠΙΛΟΓΕΣ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΟΥΣ ΠΕΛΑΤΕΣ ΚΑΙ ΤΟΥΣ ΕΞΥΠΗΡΕΤΗΤΕΣ

Αυτή η ενότητα περιγράφει τους διάφορους τύπους πελατών και εξυπηρετητών που ασχολούνται με μη-ασφαλή πρωτόκολλα που μπορεί να εξασφαλιστούν με την κάλυψη του πρωτόκολλου στο TLS. Επίσης περιγράφει τους τύπους των πολιτικών ασφαλείας που οι πελάτες και εξυπηρετητές μπορούν να εμπεριέχουν. Δεν υποστηρίζει ρητά ότι μια πολιτική είναι καλύτερη από μία άλλη σε κάποιο συγκεκριμένο περιβάλλον: αντ 'αυτού, θεωρεί ότι ο χειριστής του εξυπηρετητή και του πελάτη μπορούν να αποφασίσουν μόνοι τους αν τους δίνονται τα κατάλληλα εργαλεία.

Αυτή η συζήτηση προϋποθέτει ένα πρωτόκολλο πελάτη-εξυπηρετητή που ορίζεται για έναν αβέβαιο τρόπο διαμόρφωσης και επίσης ορίζεται για ένα ασφαλή τρόπο που χρησιμοποιεί μια συνεδρία TLS για την ασφάλεια. Για παράδειγμα, «το HTTP τρέχει στη θύρα 80» και «το HTTP-in-TLS τρέχει στη θύρα 443» ικανοποιούν αυτήν την προϋπόθεση, καθώς και «το SMTP χωρίς STARTTLS» και το «SMTP με STARTTLS» ικανοποιούν επίσης αυτήν την προϋπόθεση,. Μερικά ισάξια πρωτοκόλλα μπορεί να συναντούν αυτήν την προϋπόθεση, εάν οι ενέργειες εκκίνησης μοιάζουν με τις τυπικές αλληλεπιδράσεις πελάτη-εξυπηρετητή.

Με δεδομένη μια συγκεκριμένη διαμόρφωση εφαρμογής πελάτη, υπάρχουν τρεις ενδιαφέροντες τύποι πελατών:

- Πελάτης Μόνο Μη-ασφαλής (CIO): Ο πελάτης έχει ρυθμιστεί έτσι ώστε να προσπαθεί για επικοινωνία για την εφαρμογή μόνο στην μη-ασφαλή μορφή της. Για παράδειγμα, ένας POP πελάτης μπορεί να έχει ρυθμιστεί ώστε να προσπαθεί μόνο μη-ασφαλή POP στη θύρα 110.
- Πελάτης Μόνο Ασφαλής(CSO): Ο πελάτης έχει ρυθμιστεί έτσι ώστε να προσπαθεί για επικοινωνία για την εφαρμογή μόνο στην ασφαλή, με TLS μορφή της. Για παράδειγμα, ένας POP client μπορεί να ρυθμιστεί ώστε να προσπαθήσει μόνο ασφαλή POP στη θύρα 995.
- Πελάτης που παρέχει υποβάθμιση από ασφαλή σε μη-ασφαλή (CFB): Ο πελάτης έχει ρυθμιστεί έτσι ώστε να επιχειρήσει επικοινωνία για την εφαρμογή της σε ασφαλή, TLS μορφή, αλλά εάν αποτύχει να δημιουργήσει μια συνεδρία TLS, ο πελάτης θα προσπαθήσει να επιχειρήσει επικοινωνία με τον ίδιο εξυπηρετητή χρησιμοποιώντας τη μη-ασφαλή μορφή. Η διαμόρφωση αυτή μπορεί να προσφερθεί για διάφορους λόγους, όπως αν ο πελάτης δεν εμπιστεύονται την αρχή πιστοποίησης που χρησιμοποιεί ο εξυπηρετητής για να πιστοποιήσει τον εαυτό του.

Με δεδομένη μια συγκεκριμένη διαμόρφωση ενός εξυπηρετητή, υπάρχουν τρεις ενδιαφέροντες τύποι εξυπηρετητών:

- Εξυπηρετητής Μόνο Μη-ασφαλής (SIO): Ο εξυπηρετητής ανταποκρίνεται χωρίς TLS για την κύρια θύρα για την εφαρμογή. Ένας κεντρικός υπολογιστής για έναν εξυπηρετητή που ανταποκρίνεται στα αιτήματα HTTP στη θύρα 80 είναι ένα παράδειγμα αυτού.
- Εξυπηρετητής Μόνο Ασφαλής (SSO): Ο εξυπηρετητής απαντά με χρήση TLS για τη συγκεκριμένη θύρα TLS για την εφαρμογή. Για παράδειγμα, ένας κεντρικός υπολογιστής για έναν εξυπηρετητή που ανταποκρίνεται μόνο στα αιτήματα HTTP στη θύρα 443. Εναλλακτικά, αν η εφαρμογή υποστηρίζει ενημερώσεις ασφαλείας στη ζώνη (όπως STARTTTLS για SMTP), ο εξυπηρετητής απαντά στην κανονική θύρα, προσπαθεί να δημιουργήσει μια περίοδο λειτουργίας TLS, και δεν προχωρά με το πρωτόκολλο αν μια συνεδρία TLS δεν μπορεί να δημιουργηθεί.
- Εξυπηρετητής και ασφαλής και μη-ασφαλής (SSB) - Ο εξυπηρετητής αποκρίνεται χωρίς TLS στο κεντρική θύρα για την εφαρμογή και ανταποκρίνεται χρησιμοποιώντας TLS για τη συγκεκριμένη TLS θύρα για την εφαρμογή, όπως για τις δύο θύρες 80 και 443 για το HTTP. Εναλλακτικά, εάν η εφαρμογή υποστηρίζει ενημερώσεις ασφαλείας στη ζώνη (όπως STARTTTLS για SMTP), ο εξυπηρετητής ανταποκρίνεται στην κανονική θύρα, προσπαθεί να δημιουργήσει μια συνεδρία TLS, και προχωρεί με το κανονικό πρωτόκολλο, αν μια συνεδρία TLS δεν μπορεί να δημιουργηθεί.

Αναμένεται ότι η ρύθμιση του πελάτη θα είναι ανά-κεντρικό υπολογιστή. Δηλαδή, έναν πελάτης που είναι μόνο ασφαλής για κάποιους κεντρικούς υπολογιστές μπορεί να παρέχει υποβάθμιση από ασφαλή σε μη-ασφαλή για άλλους υπολογιστές. Η ρύθμιση του εξυπηρετητή, βέβαια, ισχύει για όλους τους πελάτες που έχουν πρόσβαση σε αυτόν. Σε αυτή την ταξινόμηση, ένας πελάτης μόνο μη-ασφαλής μπορεί πάντα να επικοινωνεί με εξυπηρετητές μόνο ασφαλείς και εξυπηρετητές και ασφαλείς και μη-ασφαλείς.

Ένας πελάτης μόνο ασφαλής μπορεί να επικοινωνήσει με μόνο ασφαλή εξυπηρετητή, και μπορεί να επικοινωνήσει και με εξυπηρετητές και ασφαλείς και μη-ασφαλείς, εφόσον η συνεδρία TLS έχει δημιουργηθεί με επιτυχία. Ένας πελάτης που παρέχει υποβάθμιση από ασφαλή σε μη-ασφαλή μπορεί να επικοινωνήσει και με τους τρεις τύπους εξυπηρετητών.

Δεδομένου αυτού, ένας κεντρικός υπολογιστής που δίνει στους πελάτες μόνο τη δυνατότητα να χρησιμοποιούν την ασφαλή μορφή ενός πρωτόκολλου πρέπει να διαμορφωθεί ώστε να είναι μόνο ασφαλής: ένας πελάτη που θέλει να επικοινωνεί με έναν εξυπηρετητή μόνο με ασφάλεια πρέπει να ρυθμιστεί έτσι ώστε να είναι μόνο ασφαλής.

Να σημειωθεί ότι ένας κεντρικός υπολογιστής μπορεί να θέλει να εξυπηρετήσει τόσο μη-ασφαλή όσο και ασφαλής μορφή ενός πρωτόκολλου, αλλά θέλει τους πελάτες να χρησιμοποιούν μόνο την ασφαλή μορφή. Για παράδειγμα, η μη-ασφαλής μορφή μπορεί να

κάνει αμέσως μια αναβάθμιση στην ασφαλή μορφή, ή θα μπορούσε να κάνει μία ανακατεύθυνση που βασίζεται στο πρωτόκολλο σε έναν εξυπηρετητή που χρησιμοποιεί την ασφαλή μορφή. Ένας τέτοιος κεντρικός υπολογιστής θα θέλει να είναι σε θέση να υποδείξει ότι, ακόμη και αν έχει τόσο ασφαλείς όσο και μη-ασφαλείς θύρες ανοιχτές για ένα πρωτόκολλο, θέλει πελάτες που μπορούν να παρέχουν υποβάθμιση από ασφαλή σε μη-ασφαλή ή που να είναι ασφαλείς να διαμορφώνονται μόνο ως ασφαλείς.

Αυτή η ταξινόμηση εκθέτει ένα πρόβλημα με τον τρόπο με τον οποίο οι πελάτες και εξυπηρετητές αλληλεπιδρούν σήμερα: ένας μη-ασφαλής πελάτης που ξεκινά μία αβέβαιη επικοινωνία με έναν εξυπηρετητή, ή ένας πελάτης που παρέχει υποβάθμιση από ασφαλή σε μη-ασφαλή και πέφτει πίσω σε μη-ασφαλή επικοινωνία με τον εξυπηρετητή, δεν έχει καμία ιδέα εάν ο ιστοχώρος με τον οποίον επιθυμεί να επικοινωνήσει φιλοξενείται σε έναν μη-ασφαλή εξυπηρετητή. Ο εξυπηρετητής μπορεί να ρυθμιστεί έτσι ώστε να είναι οποιοσδήποτε από τους τρεις τύπους εξυπηρετητών, αλλά ο πελάτης δεν μπορεί να το γνωρίζει. Εάν ένας μη-ασφαλής πελάτης ή ένας πελάτης που παρέχει υποβάθμιση από ασφαλή σε μη-ασφαλή γνωρίζει εκ των προτέρων ότι ένας κεντρικός υπολογιστής δεν υποστηρίζει τη μη-ασφαλή επικοινωνία, ο πελάτης δεν θα ξεκινήσει καθόλου την επικοινωνία, επειδή είτε θα σπαταλούσε το χρόνο αναμονής για ένα συγκεκριμένο χρονικό διάστημα, ή θα επικοινωνήσει με έναν απατεώνα.

Είναι απολύτως λογικό για έναν εξυπηρετητή να εκτελεί μια υπηρεσία με ένα μη-ασφαλή τρόπο διαμόρφωσης, με έναν ασφαλή τρόπο, ή και με τα δύο, χωρίς να χρησιμοποιεί το πρωτόκολλο που περιγράφεται εδώ. Σκοπός του πρωτοκόλλου είναι να αφήσουμε έναν πελάτη να μάθει, με ασφάλεια, αν ένα συγκεκριμένο πρωτόκολλο του εξυπηρετητή εκτελείται με ασφάλεια και όχι αν πρόκειται να εκτελεστεί.

5.2.2 Η ΕΓΓΡΑΦΗ ΠΟΡΩΝ HASTLS

Ο τύπος της εγγραφή πόρων HASTLS [1], του οποίου η τιμή είναι TBD1, αναγράφει ένα ζεύγος μη-ασφαλούς και ασφαλούς θύρας που εξυπηρετείται στον κεντρικό υπολογιστή και καθορίζεται από το όνομα διευθύνσεως για την εφαρμογή και το πρωτόκολλο που δίνεται στο ερώτημα. Εφαρμόζεται μόνο σε εφαρμογές που είναι εξασφαλισμένες με TLS, και όχι σε εφαρμογές που έχουν μη-ασφαλείς και ασφαλείς εκδόσεις που χρησιμοποιούν ορισμένα άλλα πρωτοκόλλα ασφαλείας. Η μορφή παρουσίασης είναι:

```
_appname._protoname.hostname IN HASTLS ins-port sec-port pol-pref
```

Το όνομα της εφαρμογής («APPNAME») και το όνομα του πρωτόκολλου («protoname») που ερωτούνται είναι τα ίδια που χρησιμοποιούνται στη SRV εγγραφή πόρων που περιγράφεται στο [RFC2782]. Ο μη-ασφαλής αριθμός θύρας (που ονομάζεται «ins-port»),ο ασφαλής αριθμός θύρας (που ονομάζεται «sec-port»), και η προτίμηση της πολιτική του πελάτη (που ονομάζεται «pol-pref») είναι ο καθένας δύο οκταδικοί θετικοί ακέραιοι.

Αν ένας εξυπηρετητής δεν προσφέρει μία από τις δύο υπηρεσίες, η υπηρεσία αυτή υποδεικνύεται από τη θύρα 0. Για πρωτόκολλα που χρησιμοποιούν συνθηματικά στη ζώνη για τις αναβαθμίσεις ασφάλειας, ο μη-ασφαλής αριθμός θύρας " και ο ασφαλής αριθμός θύρας έχουν την ίδια τιμή. Μία εγγραφή πόρων HASTLS δεν πρέπει να έχουν και τους δύο αριθμούς θύρας τιθέμενους στο 0.

Ένα ερώτημα για μια συγκεκριμένη εφαρμογή μπορεί να επιστρέψει περισσότερες από μία εγγραφές πόρων HASTLS, και οι συμμορφούμενοι πελάτες πρέπει να μπορούν να επεξεργάζονται πολλαπλές απαντήσεις από ένα και μόνο ερώτημα. Για παράδειγμα, ένας ιστοχώρος που προσφέρει HTTP και στη θύρα 80 και στη θύρα 8080 μπορεί να επιστρέψει δύο εγγραφές, μία για τη θύρα 80 και το ασφαλές αντίγραφό του (αν υπάρχει), και μία για τη θύρα 8080 και το ασφαλές αντίγραφό του (αν υπάρχει).

Η εγγραφή πόρων HASTLS δεν είναι χρήσιμη για την ανεύρεση των υπηρεσιών. Οι πελάτες δεν πρέπει να κάνουν υποθέσεις σχετικά με μία εφαρμογή για την οποία δεν υπάρχει μία εγγραφή πόρων HASTLS. Η έλλειψη της HASTLS για μια συγκεκριμένη εφαρμογή δεν λέει τίποτα για το εάν ή όχι η υπηρεσία προσφέρεται στον κεντρικό υπολογιστή σε μία συγκεκριμένη θύρα.

Η προτίμηση της πολιτικής του byte του πελάτη καθορίζει την προτίμηση του κεντρικού υπολογιστή για την πολιτική του πελάτη. Έχει δύο πιθανές τιμές:

- Τιμή 0 – Ο διαχειριστής του κεντρικού υπολογιστή δεν έχει καμία προτίμηση για την πολιτική του πελάτη για αυτό το πρωτόκολλο.
- Τιμή 1 - Αν ο πελάτης μπορεί να ρυθμιστεί είτε ως πελάτης που παρέχει υποβάθμιση από ασφαλή σε μη-ασφαλή είτε ως μόνο Ασφαλής(CSO) πελάτης για αυτό το πρωτόκολλο, και ο διαχειριστής του κεντρικού υπολογιστή ήταν σε θέση να διαμορφώσει τον πελάτη για το πρωτόκολλο, αυτός ο διαχειριστής θα διαμορφώσει τον πελάτη ως μόνο-ασφαλή. Με αλλά λόγια, ο διαχειριστής του κεντρικού υπολογιστή δεν θέλει κανέναν πελάτη που παρέχει υποβάθμιση από ασφαλή σε μη-ασφαλή να έχει πρόσβαση στον κεντρικό υπολογιστή για αυτό το πρωτόκολλο.

Να σημειωθεί ότι ο προσδιορισμός 1 για την προτίμηση της πολιτικής του πελάτη όταν ένας κεντρικός υπολογιστής δεν υποστηρίζει ένα ασφαλές πρωτόκολλο δεν έχει νόημα, αλλά ούτε δημιουργεί κάποια ζημιά. Περαιτέρω, για έναν κεντρικό υπολογιστή που είναι μόνο ασφαλής, οι προτιμήσεις της πολιτικής έχουν το ίδιο αποτέλεσμα.

Για παράδειγμα, ο εξυπηρετητής στο www.example.com προσφέρει SMTP και με ασφάλεια και χωρίς ασφάλεια. Ο διαχειριστής του κεντρικού υπολογιστή SMTP έχει μια προτίμηση πολιτικής πελάτη με βάση την οποία πελάτες που παρέχουν υποβάθμιση από ασφαλή σε μη-ασφαλή τρόπο διαμόρφωσης να μην έχουν πρόσβαση στον κεντρικό υπολογιστή. Η εγγραφή πόρων HASTLS θα είναι:

_smtp._tcp.www.example.com IN HASTLS 25 25 1

Άλλο ένα παράδειγμα είναι ο εξυπηρετητής στο www.example.com να προσφέρει HTTP μόνο με ασφάλεια. Η προκύπτουσα εγγραφή πόρων HASTLS θα μπορούσε να είναι είτε:

_http._tcp.www.example.com IN HASTLS 0 443 0

ή

_http._tcp.www.example.com IN HASTLS 0 443 1

5.2.3 ΕΦΑΡΜΟΖΟΝΤΑΣ ΤΗΝ ΠΟΛΙΤΙΚΗ ΜΕ HASTLS

Οι εξυπηρετητές που έχουν μια πολιτική για να δηλωθούν ως μόνο μη-ασφαλής, μόνο ασφαλής, ή ως εξυπηρετητές και ασφαλείς και μη-ασφαλείς μπορούν να χρησιμοποιήσουν την HASTLS για να ανακοινώσουν την πολιτική για κάθε εφαρμογή που εξυπηρετούν.

Ένας εξυπηρετητής του οποίου η πολιτική είναι ότι πρόκειται για έναν εξυπηρετητή με μη-ασφαλή τρόπο διαμόρφωσης θα έθετε τον μη-ασφαλή αριθμό θύρας σε ένα μη-μηδενικό αριθμό και τον ασφαλή αριθμό θύρας στο 0.

Ένας εξυπηρετητής του οποίου η πολιτική είναι ότι πρόκειται για έναν εξυπηρετητή με ασφαλή τρόπο διαμόρφωσης θα έθετε τον μη-ασφαλή αριθμό θύρας στο 0 και τον ασφαλή αριθμό θύρας σε ένα μη-μηδενικό αριθμό.

Ένας εξυπηρετητής του οποίου η πολιτική είναι ότι πρόκειται για έναν εξυπηρετητή και με ασφαλή και με μη-ασφαλή τρόπο διαμόρφωσης θα θέτει και τον μη-ασφαλή αριθμό θύρας και τον ασφαλή αριθμό θύρας σε μη-μηδενικούς αριθμούς.

Οι απαιτήσεις συμμόρφωσης για έναν πελάτη που χρησιμοποιεί το ρεκόρ την εγγραφή πόρων HASTLS εξαρτώνται από την πολιτική που διαμορφώνεται για τον πελάτη ή για τον εξυπηρετητή:

- Ένας πελάτης επικοινωνεί με έναν εξυπηρετητή που έχει θέσει την προτίμηση της πολιτικής του πελάτη του στο 1 δεν πρέπει να προσπαθήσει να επικοινωνήσει με μη ασφαλή τρόπο με αυτόν τον εξυπηρετητή, ακόμα και αν ο εξυπηρετητής έχει θέσει τον μη-ασφαλή αριθμό θύρας σε ένα μη-μηδενικό αριθμό. Αυτό είναι το ισοδύναμο της προσωρινής ρύθμισης της πολιτικής για τον εξυπηρετητή να έχει πελάτες με ασφαλή τρόπο διαμόρφωσης για την εν λόγω εφαρμογή. Αυτή η προσωρινή

πολιτική με βάση την προτίμησή της πολιτικής του πελάτη του εξυπηρετητή υπερισχύει οποιασδήποτε άλλης για τον εξυπηρετητή.

- Ένας πελάτης του οποίου η πολιτική είναι ότι πρόκειται για έναν πελάτη με μη-ασφαλή τρόπο διαμόρφωσης δεν πρέπει να προσπαθεί να επικοινωνήσει χωρίς ασφάλεια με ένα εξυπηρετητή που έχει ορίσει τον μη-ασφαλή αριθμό θύρας σε 0.
- Ένας πελάτης του οποίου η πολιτική είναι ότι πρόκειται για έναν πελάτη με ασφαλή τρόπο διαμόρφωσης πρέπει μόνο να προσπαθήσει να επικοινωνήσει με ασφάλεια με έναν εξυπηρετητή που έχει θέσει τον ασφαλή αριθμό θύρας σε μια μη-μηδενική τιμή.

- Ένας πελάτης του οποίου η πολιτική είναι ότι πρόκειται για έναν πελάτη με ασφαλή τρόπο διαμόρφωσης δεν πρέπει να προσπαθήσει να επικοινωνήσει με τον εξυπηρετητή, εάν δίνεται μία τιμή για τον μη-ασφαλή αριθμό θύρας.

- Ένας πελάτης του οποίου η πολιτική είναι ότι πρόκειται για έναν πελάτη που παρέχει υποβάθμιση από ασφαλή σε μη-ασφαλή τρόπο διαμόρφωσης δε πρέπει να προσπαθεί να επικοινωνήσει με ασφάλεια με έναν εξυπηρετητή που έχει θέσει τον ασφαλή αριθμό θύρας σε 0.

- Ένας πελάτης του οποίου η πολιτική είναι ότι πρόκειται για έναν πελάτη που παρέχει υποβάθμιση από ασφαλή σε μη-ασφαλή τρόπο διαμόρφωσης δεν πρέπει να προσπαθεί να επικοινωνήσει χωρίς ασφάλεια με έναν εξυπηρετητή που έχει θέσει τον μη-ασφαλή αριθμό θύρας σε 0.

- Ένας πελάτης του οποίου η πολιτική είναι ότι πρόκειται για έναν πελάτη που παρέχει υποβάθμιση από ασφαλή σε μη-ασφαλή τρόπο διαμόρφωσης και προσπαθεί να επικοινωνήσει με έναν εξυπηρετητή του οποίου ο ασφαλής αριθμός θύρας έχει οριστεί σε μια έναν μη μηδενικό αριθμό θα έπρεπε πρώτα να επικοινωνήσει με ασφάλεια πάνω από την ασφαλή θύρα, εκτός αν ξέρει από άλλες πηγές ότι η συνεδρία TLS δεν θα δημιουργηθεί σωστά.

5.3 ΧΡΗΣΗ ΑΣΦΑΛΟΥΣ DNS ΓΙΑ ΤΟΝ ΣΥΝΔΥΑΣΜΟ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΜΕ ΤΑ ΟΝΟΜΑΤΑ ΔΙΕΥΘΥΝΣΕΩΝ

Η πρώτη απάντηση από τον κεντρικό υπολογιστή σε TLS μπορεί να περιέχει ένα πιστοποιητικό. Για να επιβεβαιώνεται ο TLS πελάτης ότι μιλάει με τον αναμενόμενο εξυπηρετητή TLS, ο πελάτης πρέπει να επικυρώσει ότι αυτό το πιστοποιητικό συνδέεται με το όνομα της διεύθυνσης που χρησιμοποιείται από τον πελάτη για να φτάσει στον εξυπηρετητή. Τότε, ο πελάτης πρέπει να εξαγάγει το όνομα διεύθυνσης από το πιστοποιητικό, πρέπει να εμπιστευθεί ένα σύνδεσμο εμπιστοσύνης επάνω στον οποίο δρομολογείται το πιστοποιητικό του εξυπηρετητή, και πρέπει να επικυρώσει επιτυχώς το πιστοποιητικό.

Μερικοί άνθρωποι θέλουν έναν διαφορετικό τρόπο να πιστοποιήσουν την σχέση του πιστοποιητικού του εξυπηρετητή με το προοριζόμενο όνομα διεύθυνσης χωρίς να εμπιστευθούν μια αρχή πιστοποίησης. Δεδομένου ότι ο DNS διαχειριστής για ένα domain name έχει την εξουσιοδότηση να δώσει προσδιοριστικές πληροφορίες σχετικά με τη ζώνη, έχει νόημα να επιτραπεί σε εκείνο τον διαχειριστή να κάνει επίσης μία επιτακτική δέσμευση μεταξύ του ονόματος διεύθυνσης και ενός πιστοποιητικού που ίσως χρησιμοποιηθούν από έναν κεντρικό υπολογιστή σε εκείνο το όνομα διεύθυνσης. Ο ευκολότερος τρόπος να γίνει αυτό είναι με τη χρήση του DNS.

Μια σύνδεση πιστοποιητικών είναι βασισμένη σε μια κρυπτογραφική διαδικασία κατακερματισμού ενός πιστοποιητικού (μερικές φορές αποκαλούμενου "δακτυλικό αποτύπωμα") ή το ίδιο στο πιστοποιητικό. Για ένα δακτυλικό αποτύπωμα, λαμβάνεται ένας κατακερματισμός από το δυαδικό, DER-κωδικοποιημένο πιστοποιητικό, και εκείνος ο κατακερματισμός είναι η ένωση πιστοποιητικών: ο τύπος της λειτουργίας του κατακερματισμού αν χρησιμοποιηθεί μπορεί να επιλεχτεί από τον εξυπηρετητή dns. Κατά

τη χρήση του ίδιου του πιστοποιητικού στη σύνδεση πιστοποιητικών, χρησιμοποιείται ολόκληρο το πιστοποιητικό με την κανονική του μορφή.

Καθορίζεται μια ασφαλής μέθοδος για να συνδεθεί το πιστοποιητικό που λαμβάνεται από τον εξυπηρετητή TLS με ένα domain name χρησιμοποιώντας DNS το οποίο προστατεύεται από τη DNSSEC. Επειδή η σύνδεση των πιστοποιητικών ανακτάται βασιζόμενη σε μια DNS ερώτηση, το domain name στην ερώτηση είναι εξ ορισμού συσχετισμένο με το πιστοποιητικό.

Η DNSSEC χρησιμοποιεί κρυπτογραφικά κλειδιά και ψηφιακές υπογραφές για να παρέχει την αυθεντικοποίηση των δεδομένων DNS. Οι πληροφορίες που ανακτούνται από τον DNS και επιβεβαιώνονται με τη χρήση της DNSSEC είναι αποδεδειγμένα τα επιτακτικά δεδομένα. Η υπογραφή DNSSEC πρέπει να επικυρώνεται σε όλες τις απαντήσεις προκειμένου να βεβαιωθεί η προέλευση των δεδομένων.

Έχει αναφερθεί ότι αυτό το πρωτόκολλο είναι μια μορφή «αποκλεισμού πιστοποιητικών». Αυτό ισχύει, αλλά μόνο υπό την έννοια ότι μια DNS απάντηση που περιέχει δύο από τους τύπους πιστοποιητικών που καθορίζονται αποκλείει κάθε άλλο πιθανό πιστοποιητικό στον κόσμο. Ο τύπος των πιστοποιητικών που ορίζεται είναι καλύτερη σκέψη ως «απαρίθμηση» ενός μικρού αριθμού ενώσεων πιστοποιητικών, όχι ως «αποκλεισμός» ενός κοντινός-άπειρου αριθμού άλλων πιστοποιητικών.

5.3.1 ΑΠΟΚΤΗΣΗ ΕΝΩΣΕΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ TLS ΑΠΟ ΤΟ ΣΥΣΤΗΜΑ DNS

Στη συνέχεια θα αναφερθεί ένας νέος τύπος εγγραφής πόρων DNS, ο «TLSA» [2]. Μια ερώτηση σε ένα προετοιμασμένο domain name για την TLSA RR μπορεί να επιστρέψει ένα ή περισσότερα αρχεία/εγγραφές (records) του τύπου TLSA.

5.3.1.1 ΖΗΤΟΥΜΕΝΟ ΟΝΟΜΑ ΠΕΡΙΟΧΩΝ

Τα domain name είναι προετοιμασμένα για αιτήματα με τον ακόλουθο τρόπο:

1. Η δεκαδική αντιπροσώπευση του αριθμού θύρας στον οποίο μια υπηρεσία βασισμένη στο TLS υποτίθεται ότι υπήρξε είναι με μια κάτω παύλα («_») για να γίνει η πιο αριστερή ετικέτα στο προετοιμασμένο domain name.
2. Το όνομα του πρωτοκόλλου της μεταφοράς στο οποίο μια υπηρεσία βασισμένη στο TLS υποτίθεται ότι υπάρχει είναι με έναν χαρακτήρα κάτω παύλας («_») για να γίνει η δεύτερη πιο αριστερή ετικέτα στο έτοιμο domain name.Τα ονόματα μεταφοράς που ορίζονται για αυτό το πρωτόκολλο είναι «tcp» «udp» και «sctp».
3. Το όνομα περιοχών επισυνάπτεται στο αποτέλεσμα του βήματος 2 για να ολοκληρώσει το έτοιμο όνομα περιοχών.

Παραδείγματος χάριν, για να ζητηθεί μία TLSA RR για έναν http εξυπηρετητή που τρέχει TLS στη θύρα 443 «στο www.example.com», θα χρησιμοποιηθεί «_443. _tcp.www.example.com» στο αίτημα σας. Για να ζητήσετε ένα TLSA αρχείο εγγραφών για έναν SMTP server που τρέχει το πρωτόκολλο STARTTLS στη θύρα 25 στο «mail.example.com», θα χρησιμοποιηθεί «_25. _tcp.mail.example.com»

5.3.1.2 ΜΟΡΦΗ ΤΗΣ ΕΓΓΡΑΦΗΣ ΠΟΡΩΝ

Ο τύπος των δεδομένων στο αρχείο των εγγραφών είναι μία δυαδική εγγραφή με τρεις τιμές, οι οποίες πρέπει να είναι με την ακόλουθη σειρά:

1. Μία one-byte τιμή αποκαλούμενη «τύπος πιστοποιητικού», η οποία διευκρινίζει την παρεχόμενη ένωση που θα χρησιμοποιηθεί για να ταιριάξει με το πιστοποιητικό-στόχο. Αυτό θα είναι μία καταγραφή IANA προκειμένου να γίνει πιο εύκολη η προσθήκη επιπλέον τύπων πιστοποιητικών στο μέλλον. Οι τύποι αυτοί είναι οι ακόλουθοι: -- Ένα πιστοποιητικό που προσδιορίζει μια οντότητα τέλους

   --Το πιστοποιητικό μιας αρχής πιστοποίησης
2. - Μία one-byte τιμή, η οποία αναφέρεται ως «τύπος αναφοράς» και διευκρινίζει πώς παρουσιάζεται η σύνδεση των πιστοποιητικών. Αυτή η τιμή ορίζεται σε μία νέα

καταγραφή IANA. Οι τύποι που καθορίζονται είναι οι εξής:

0 -- Πλήρες πιστοποιητικό

1 -- Sha-256 κατακερματισμός του πιστοποιητικού

2 -- Sha-512 κατακερματισμός του πιστοποιητικού

Χρησιμοποιώντας τον ίδιο αλγόριθμο κατακερματισμού με εκείνον που χρησιμοποιείται στην υπογραφή του πιστοποιητικού καταστά πιο πιθανό το γεγονός ότι ο πελάτης TLS θα καταλάβει αυτό το δεδομένο TLSA.

3. Το «πιστοποιητικό για την ένωση». Αυτό είναι τα bytes που περιέχουν το πλήρες πιστοποιητικό ή τον κατακερματισμό του σχετικού πιστοποιητικού (δηλαδή το πιστοποιητικό ή τον κατακερματισμό του ίδιου του πιστοποιητικού, όχι του αντικειμένου TLS ASN.1Cert).

5.3.1.3 ΚΑΘΙΣΤΩΝΤΑΣ ΣΥΝΔΕΣΕΙΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Οι δύο τύποι πιστοποιητικών για το TLS έχουν πολύ διαφορετική σημασιολογία. Ο TLS πελάτης που προσαρμόζεται σε αυτό το πρωτόκολλο λαμβάνοντας ένα πιστοποιητικό για μία ένωση τύπου - 1 πρέπει να το συγκρίνει, χρησιμοποιώντας το συγκεκριμένο hash τύπο, με το πιστοποιητικό της τελευταίας οντότητας που παραλαμβάνεται στο TLS. Ένας TLS πελάτης που λειτουργεί με αυτό το πρωτόκολλο και λαμβάνει ένα πιστοποιητικό για μια ένωση τύπου - 2 πρέπει να το διαχειρίζεται ως σύνδεσμο εμπιστοσύνης για εκείνο το domain name.

Τα πιστοποιητικά τύπου - 1 (ένα πιστοποιητικό που προσδιορίζει μια οντότητα τέλους) αντιστοιχίζεται έναντι στο πρώτο πιστοποιητικό που προσφέρεται από τον TLS εξυπηρετητή. Το πιστοποιητικό για την σύνδεση χρησιμοποιείται μόνο για την ακριβή αντιστοίχηση, και όχι για αλυσιδωτή επικύρωση. Με τον τύπο αναφοράς 0, το πιστοποιητικό ένωσης είναι έγκυρο εάν το πιστοποιητικό στις αντιστοιχίες των δεδομένων της εγγραφής πόρων TLSA ταιριάζει με το πρώτο πιστοποιητικό που προσφέρεται από τον TLS. Με άλλους τύπους αναφοράς εκτός από τον τύπο 0, η ένωση πιστοποιητικών είναι έγκυρη αν το hash του πρώτου πιστοποιητικού που προσφέρεται από τον TLS server ταιριάζει με την τιμή των δεδομένων της εγγραφής πόρων TLSA.

Τα πιστοποιητικά τύπου - 2 (πιστοποιητικό της αρχής πιστοποίησης) μπορούν να χρησιμοποιηθούν με δύο τρόπους. Με τον τύπο αναφοράς 0, το πιστοποιητικό στην εγγραφή πόρων TLSA χρησιμοποιείται στο ταίριασμα από την οντότητα τέλους που δίνεται στο TLS. Η ένωση πιστοποιητικών είναι έγκυρη εάν το πρώτο πιστοποιητικό στο πακέτο των πιστοποιητικών μπορεί να εμφωλευτεί στον σύνδεσμο εμπιστοσύνης από τα δεδομένα της εγγραφής πόρων TLSA.

Με τύπους αναφοράς διαφορετικούς από τον τύπο 0, εάν ο κατακερματισμός οποιουδήποτε πιστοποιητικού μετά από το πρώτο στο πακέτο πιστοποιητικών από το TLS ταιριάζει με τον σύνδεσμο εμπιστοσύνης από τα δεδομένα της εγγραφής TLSA, και η αλυσίδα στο πακέτο πιστοποιητικών είναι έγκυρη μέχρι εκείνη την άγκυρα εμπιστοσύνης της TLSA RR, η ένωση των πιστοποιητικών ισχύει. Εναλλακτικά, εάν το πρώτο πιστοποιητικό προσέφερε τις αλυσίδες σε έναν υπάρχων σύνδεσμο εμπιστοσύνης στην αποθήκη συνδέσμων εμπιστοσύνης του πελάτη TLS, και ο κατακερματισμός εκείνου του συνδέσμου ταιριάζει με την τιμή από την TLSA RR, τότε η ένωση των πιστοποιητικών ισχύει.

Το πιστοποιητικό της τελικής οντότητας από το TLS, ανεξάρτητα από το εάν αντιστοιχιζόταν με πιστοποιητικό τύπου- 1 ή αν ήταν εμφωλευμένο σε ένα πιστοποιητικό τύπου- 2, πρέπει να έχει τουλάχιστον ένα προσδιοριστικό στο θέμα ή στο subjectAltName πεδίο των αντιστοιχημένων πιστοποιητικών που ταιριάζουν με το αναμενόμενο προσδιοριστικό για τον TLS server. Περαιτέρω, η συνεδρία TLS που πρόκειται να δημιουργηθεί πρέπει να είναι για το συγκεκριμένο αριθμό θύρας και μεταφοράς ονόματος που δόθηκε στην εγγραφή πόρων TLSA. Το ταίριασμα πρέπει να έχει γίνει εντός της ύπαρξης του χρόνου ισχύος στην εγγραφή TSLA.

ΜΟΡΦΗ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ ΓΙΑ ΝΑ ΠΡΟΣΔΙΟΡΙΣΟΥΝ ΤΙΣ ΤΕΛΙΚΕΣ ΟΝΤΟΤΗΤΕΣ

Αναφέρονται δύο κατηγορίες πιστοποιητικών: Τα πιστοποιητικά της αρχής πιστοποίησης και τα πιστοποιητικά τελικής οντότητας. Τα πιστοποιητικά της αρχής πιστοποίησης μπορούν χωριστούν σε τρεις κατηγορίες: τα διαγώνια-πιστοποιητικά, τα αυτό-εκδιδόμενα πιστοποιητικά, και αυτό-υπογεγραμμένα πιστοποιητικά..

Τα αυτό-εκδιδόμενα πιστοποιητικά είναι πιστοποιητικά της αρχής πιστοποίησης στα οποία ο εκδότης και το θέμα είναι η ίδια οντότητα. Τα αυτό-υπογεγραμμένα πιστοποιητικά είναι αυτό-εκδιδόμενα πιστοποιητικά όπου η ψηφιακή υπογραφή μπορεί να ελεγχθεί από το δημόσιο κλειδί που δεσμεύεται στο πιστοποιητικό. Τα αυτό-υπογεγραμμένα πιστοποιητικά χρησιμοποιούνται για να μεταβιβάσουν ένα δημόσιο κλειδί για χρήση για να αρχίσουν τα μονοπάτια πιστοποίησης.

Τα πιστοποιητικά τελικής οντότητας σχετίζονται με θέματα που δεν είναι εξουσιοδοτημένα να εκδώσουν πιστοποιητικά.»

Αυτό σημαίνει ότι ένα αυτό-υπογεγραμμένο πιστοποιητικό (ένα όπου το θέμα και ο εκδότης είναι ίδια, και το δημόσιο κλειδί στο πιστοποιητικό μπορεί να χρησιμοποιηθεί για να εκτιμήσει άμεσα την υπογραφή στο πιστοποιητικό) πρέπει να ακολουθεί όλους τους κανόνες σημασιολογίας PKIX για τις αρχές πιστοποίησης, και πιθανώς να χρειαστεί να ακολουθήσει όλους τους κανόνες πολιτικής επίσης. Αυτό σαφώς δεν αρκεί για τους ανθρώπους που θέλουν έναν απλό τρόπο να συνδέσουν το δημόσιο κλειδί υπογραφής τους με το domain name τους σε ένα πιστοποιητικό τελικής οντότητας που μπορεί να χρησιμοποιηθεί στο TLS.

Λόγω αυτών των απαιτήσεων του PKIX στα πιστοποιητικά τελικής οντότητας, οι κανόνες επεξεργασίας για τα TLSA είναι πολύ διαφορετικοί για τα πιστοποιητικά που προσδιορίζουν τις τελικές οντότητες απευθείας και για τα πιστοποιητικά της αρχής πιστοποίησης που μπορούν να χρησιμοποιηθούν για να επικυρώσουν τα PKIX πιστοποιητικά τελικής οντότητας. Οι κανόνες επιτρέπουν εδώ τα αυτό-υπογεγραμμένα πιστοποιητικά που προσφέρονται ως πιστοποιητικά τύπου – 1 να μην ακολουθούν όλους τους κανόνες σημασιολογίας των PKIX.

5.3.1.4 ΜΟΡΦΗ ΠΑΡΟΥΣΙΑΣΗΣ

Τα RDATA του σχήματος παρουσίασης του αρχείου των εγγραφών πόρων TLSA αποτελείται από δύο αριθμούς (τύπος πιστοποιητικού και κατακερματισμός) που ακολουθούνται από bytes που περιέχουν το πιστοποιητικό ή τον κατακερματισμό του ίδιου του συνδεμένου πιστοποιητικού, σε δεκαεξαδική μορφή. Ένα παράδειγμα κατακερματισμού Sha-256 (τύπου - 1) ενός πιστοποιητικού τελικής οντότητας (τύπου - 1) θα ήταν:

```
_443._tcp.www.example.com. IN TLSA (
    1 1 5c1502a6549c423be0a0aa9d9a16904de5ef0f5c98
      c735fcca79f09230aa7141 )
```

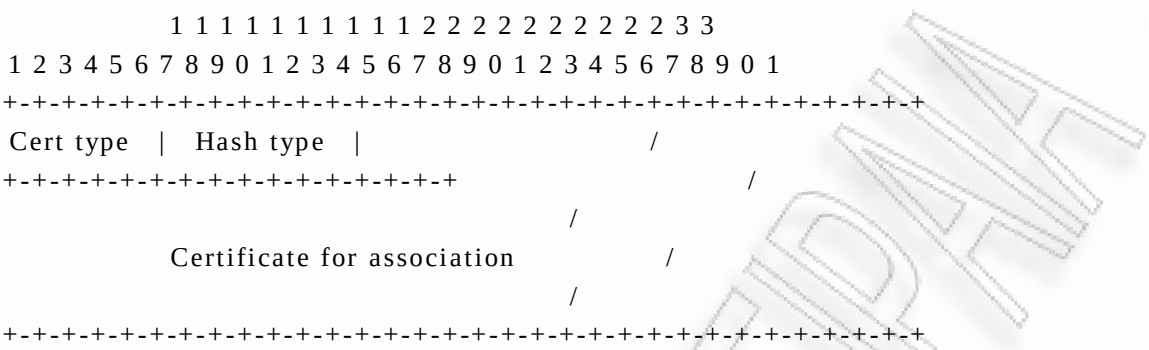
Ένα παράδειγμα πιστοποιητικού της αρχής πιστοποίησης (τύπου- 2) θα ήταν:

```
_443._tcp.www.example.com. IN TLSA (
    2 0 308202c5308201ada00302010202090... )
```

Επειδή το μήκος των κατακερματισμών και των πιστοποιητικών μπορεί να είναι αρκετά μεγάλο, η μορφή της παρουσίασης επιτρέπει ρητά τα σπασίματα γραμμών και το κενό στις δεκαεξαδικές τιμές: αυτοί οι χαρακτήρες αφαιρούνται κατά τη μετατροπή στη wire τυποποίηση.

5.3.1.5 WIRE ΤΥΠΟΠΟΙΗΣΗ

Η wire τυποποίηση είναι η εξής:



Η wire τυποποίηση για τα RDATA στο πρώτο παράδειγμα που δόθηκε παραπάνω θα ήταν:

```
_443._tcp.www.example.com. IN TYPE65534 \# 34 ( 01015c1502a6549c42
        3be0a0aa9d9a16904de5ef0f5c98c735fcca79f09230aa7141 )
```

Η wire τυποποίηση για τα RDATA στο δεύτερο παράδειγμα που δόθηκε παραπάνω θα ήταν:

```
_443._tcp.www.example.com. IN TYPE65534 \# 715 0200308202c5308201a...
```

Στα προηγούμενα παραδείγματα , το «TYPE65534» δίνεται ως παράδειγμα. Εκείνος ο τύπος RR ανήκει σε «ιδιωτικής χρήσης» κλίμακα. Ο πραγματικός τύπος RR για το TLSA θα εκδοθεί από την IANA.

5.3.2 ΧΡΗΣΗ ΤΗΣ ΕΝΩΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ TLS ΣΤΟ TLS

Προκειμένου να χρησιμοποιηθούν μια ή περισσότερες συνδέσεις πιστοποιητικών TLS που λαμβάνονται από το DNS, μια εφαρμογή πρέπει να βεβαιώνει ότι τα πιστοποιητικά λήφθηκαν χρησιμοποιώντας προστατευμένο DNS μέσω της DNSSEC. Οι εγγραφές TLSA πρέπει να είναι αξιόπιστες μόνο εάν λήφθηκαν από μία έμπιστη πηγή. Μία τέτοια έμπιστη πηγή θα μπορούσε να είναι ένας τοπικός εξυπηρετητής DNS απάντησης με το AD σύνολο bit, μια ευθύγραμμη βιβλιοθήκη αναλυτή επικύρωσης που αρχικοποιείται με τον κατάλληλο έμπιστο σύνδεσμο, ή να αποκτηθεί από έναν μακρινό εξυπηρετητή στον οποίο βρίσκεται ένα ασφαλές κανάλι επικοινωνίας.

Εάν μία σύνδεση πιστοποιητικών περιέχει έναν τύπο κατακερματισμού που δεν είναι κατανοητός από τον πελάτη TLS, αυτή η σύνδεση πιστοποιητικών πρέπει να χαρακτηριστεί ακατάλληλη προς χρήση.

Μια εφαρμογή που ζητά συνδέσεις πιστοποιητικών TLS με τη χρήση της συγκεκριμένης μεθόδου λαμβάνει μηδέν ή πιο χρήσιμες συνδέσεις πιστοποιητικών. Εάν η εφαρμογή λάβει μηδέν χρήσιμες συνδέσεις πιστοποιητικών, τότε τα TLS λειτουργούν με τον συνηθισμένο τρόπο.

Εάν βρεθεί μια αντιστοιχία μεταξύ μιας από τις συνδέσεις πιστοποιητικών και του πιστοποιητικού τελικής οντότητας του εξυπηρετητή στο TLS, ο πελάτης TLS συνεχίζει τη TLS απευθείας σύνδεση επικοινωνίας. Εάν δε βρεθεί καμία αντιστοιχία μεταξύ της χρησιμοποιήσιμης σύνδεσης πιστοποιητικού και του πιστοποιητικού τελικής οντότητας του εξυπηρετητή στο TLS, ο TLS πελάτης πρέπει να διακόψει την απευθείας σύνδεση με την εμφάνιση του μηνύματος "access_denied".

5.3.3 ΥΠΟΧΡΕΩΤΙΚΗ ΥΛΟΠΟΙΗΣΗ ΤΩΝ ΑΛΓΟΡΙΘΜΩΝ

Τα DNS συστήματα που προσαρμόζονται σε αυτήν την προδιαγραφή πρέπει να είναι σε θέση να δημιουργήσουν TLSA εγγραφές πόρων που περιλαμβάνουν πιστοποιητικά τύπου 1 και 2. Επίσης πρέπει να μπορούν να δημιουργήσουν τις TLSA RR χρησιμοποιώντας hash τύπου 0 (κανένα hash χρησιμοποιούμενο) και hash τύπου 1 (Sha-256), και να είναι σε θέση να δημιουργήσουν TLSA RR χρησιμοποιώντας hash τύπου - 2 (Sha-512).

Οι TLS πελάτες που προσαρμόζονται σε αυτήν την προδιαγραφή πρέπει να είναι σε θέση να ερμηνεύσουν σωστά τις εγγραφές πόρων TLSA που περιλαμβάνουν πιστοποιητικά τύπου 1 και 2, να συγκρίνουν ένα πιστοποιητικό για σύνδεση με ένα πιστοποιητικό από TLS χρησιμοποιώντας hash τύπου 0 (κανένα hash χρησιμοποιούμενο) και hash τύπου - 1 (Sha-256), καθώς επίσης και να πραγματοποιούν τέτοιες συγκρίσεις με hash τύπου - 2 (Sha-512).

5.3.4 ΘΕΩΡΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Η ασφάλεια των πρωτόκολλων που περιγράφηκαν προηγουμένως στηρίζεται στην ασφάλεια DNSSEC όπως χρησιμοποιείται από τον πελάτη που ζητά τις εγγραφές πόρων.

Ένας DNS διαχειριστής που αλλάζει και τις άλλες εγγραφές πόρων και τις εγγραφές TLSA για ένα όνομα διεύθυνσης μπορεί να αναγκάσει το χρήστη να πάει σε έναν μη αρμόδιο εξυπηρετητή που θα εμφανιστεί ως εξουσιοδοτημένος, εκτός αν ο πελάτης εκτελεί την επικύρωση πιστοποιητικών και απορρίπτει το πιστοποιητικό. Αυτός ο διαχειριστής θα μπορούσε πιθανώς να πάρει ένα πιστοποιητικό που εκδίδεται ούτως ή άλλως, έτσι αυτό δεν είναι μια πρόσθετη απειλή.

Οι τιμές στις TLSA RR θα εισαχθούν κανονικά στο DNS μέσω του ίδιου του συστήματος που χρησιμοποιείται για να εισαχθούν οι υπόλοιπες εγγραφές, και οι άλλες πληροφορίες DNS για το όνομα του κεντρικού υπολογιστή. Εάν η επικύρωση για τις αλλαγές στις πληροφορίες των οικοδεσποτών είναι αδύναμη, ένας επιτιθέμενος μπορεί εύκολα να αλλάξει οποιαδήποτε από αυτές οι πληροφορίες. Δεδομένου ότι οι TLSA RR δεν είναι εύκολα αναγνώσιμο από τον άνθρωπο, ένας επιτιθέμενος μπορεί να αλλάξει εκείνες τις εγγραφές και τις υπόλοιπες εγγραφές και να μην παρατηρηθεί η αλλαγή εάν οι αλλαγές σε μια ζώνη είναι μόνο οπτικά ελεγχόμενες.

Εάν ο μηχανισμός επαλήθευσης για την πρόσθεση ή την αλλαγή των εγγραφών TLSA στη ζώνη είναι πιο αδύναμος από το μηχανισμό επικύρωσης για την αλλαγή των υπόλοιπων εγγραφών, ένα ενδιάμεσο άτομο που μπορεί να επαναπροσανατολίσει την κίνηση στον ιστοχώρο τους μπορεί να είναι σε θέση στο υποδυθεί τον επιτιθέμενος κεντρικό υπολογιστή στο TLS εάν μπορεί να χρησιμοποιήσει τον πιο αδύναμο μηχανισμό επικύρωσης. Ένας καλύτερος σχεδιασμός για την επικύρωση του DNS επρόκειτο να έχει το ίδιο επίπεδο επικύρωσης που χρησιμοποιείται για όλες τις DNS προσθήκες και τις αλλαγές για έναν μεμονωμένο οικοδεσπότη.

Τα πληρεξούσια SSL μπορούν μερικές φορές να ενεργήσουν ως ενδιάμεσο άτομο για τους πελάτες TLS. Σε αυτά τα σενάρια, οι πελάτες προσθέτουν έναν νέο έμπιστο σύνδεσμο του οποίου το ιδιωτικό κλειδί κρατιέται στο πληρεξούσιο SSL: το πληρεξούσιο παρεμποδίζει τα αιτήματα TLS, δημιουργεί μια νέα περίοδο TLS με τον προοριζόμενο οικοδεσπότη, και θέτει μία TLS περίοδο με τον πελάτη χρησιμοποιώντας ένα πιστοποιητικό που οδηγεί στον σύνδεσμο που εγκαθίσταται στον πελάτη από το πληρεξούσιο.

Σε τέτοια περιβάλλοντα, το πρωτόκολλο TLSA θα εμποδίσει το πληρεξούσιο SSL από τη λειτουργία του όπως αναμενόταν επειδή ο πελάτης TLS θα πάρει μια σύνδεση πιστοποιητικών από τον DNS που δεν θα ταιριάξει με το πιστοποιητικό που το πληρεξούσιο SSL χρησιμοποιεί με τον πελάτη. Ο πελάτης, που βλέπει το νέο πιστοποιητικό του πληρεξούσιου για τον υποτιθέμενο προορισμό δεν θα δημιουργήσει μια περίοδο TLS.

5.4 DNS ΕΓΓΡΑΦΗ ΠΟΡΩΝ ΕΓΚΡΙΣΗΣ ΤΗΣ ΑΡΧΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ (CAA)

Η DNS εγγραφή πόρων έγκρισης της αρχής πιστοποίησης (CAA) [3] επιτρέπει σε έναν DNS κάτοχο ονόματος διεύθυνσης να προσδιορίσει ότι το υπογεγραμμένο πιστοποιητικό εγκρίνεται για να εκδώσει τα πιστοποιητικά για εκείνο το όνομα. Οι CAA εγγραφές πόρων επιτρέπουν σε μια δημόσια αρχή πιστοποίησης να εφαρμόσει πρόσθετους έλεγχους για να μειώσει τον κίνδυνο ακούσια υπογεγραμμένου πιστοποιητικού.

Η προσαρμογή με μία δημοσιευμένη εγγραφή CAA είναι ένας απαραίτητος αλλά όχι ικανοποιητικός όρος για την έκδοση ενός πιστοποιητικού. Πριν εκδοθεί ένα πιστοποιητικό, απαιτείται μία υποδομή δημοσίου κλειδιού (PKIX) της αρχής πιστοποίησης (CA) για να επικυρώσει το αίτημα σύμφωνα με τις πολιτικές που καθορίζονται στην δήλωση πρακτικών πιστοποίησης, η οποία διευκρινίζει τα μέσα με τα οποία ικανοποιούνται τα κριτήρια της προστασίας πιστοποίησης. Στην περίπτωση μιας δημόσιας αρχής πιστοποίησης που επικυρώνει τα αιτήματα πιστοποιητικών ως τρίτο πρόσωπο, το πιστοποιητικό θα εκδοθεί τυπικά κάτω από ένα πιστοποιητικό δημόσιας ρίζας που ενσωματώνεται σε μια ή περισσότερες σχετικές αξιόπιστες εφαρμογές.

Τα κριτήρια για το συνυπολογισμό των ενσωματωμένων πιστοποιητικών ρίζας στις εφαρμογές τυπικά απαιτούν την αρχή πιστοποίησης να δημοσιεύσει μια κατάσταση των πρακτικών των πιστοποιητικών (CPS) που διευκρινίζει πώς επιτυγχάνονται οι απαιτήσεις της ασφάλειας των πιστοποιητικών (CP) και να παρέχει μια ετήσια κατάσταση ελέγχου της απόδοσής τους ενάντια στους CPS που εκτελούνται από έναν ανεξάρτητο ελεγκτή.

Οι εγγραφές CAA περιγράφουν μόνο την τρέχουσα κατάσταση των εκδιδόμενων πιστοποιητικών της αρχής πιστοποίησης. Δεδομένου ότι ένα πιστοποιητικό είναι χαρακτηριστικά έγκυρο για τουλάχιστον ένα έτος, είναι πιθανό ότι ένα πιστοποιητικό που δεν είναι προσαρμοσμένο με τις εγγραφές CAA αυτήν την περίοδο να ήταν προσαρμοσμένο με τις εγγραφές CAA όταν εκδόθηκε. Κατά συνέπεια οι επικαλούμενες εφαρμογές δεν πρέπει να χρησιμοποιήσουν την αποτυχία της προσαρμογής στις τωρινές δημοσιευμένες εγγραφές CAA ως κριτήρια απόρριψης για τα πιστοποιητικά εκτός αν τα δημοσιευμένα αρχεία έχουν επισημανθεί ότι προορίζονται για τέτοια χρήση.

5.4.1 Ο ΤΥΠΟΣ CAA RR

Μία εγγραφή πόρων CAA δημοσιεύει μία ιδιότητα εισόδου CAA που αντιστοιχεί σε ένα προσδιορισμένο όνομα διεύθυνσης. Οι πολλαπλάσιες καταχωρήσεις ιδιότητας μπορούν να συνδεθούν με το ίδιο domain name με την έκδοση πολλαπλάσιων CAA RRs σε αυτό το domain name. Κάθε ιδιότητα εισόδου μπορεί να επισημανθεί με μία ή περισσότερες από τι ακόλουθες τιμές επισήμανσης:

- Κρίσιμη: Εάν τεθεί, δείχνει ότι η αντίστοιχη ετικέτα εισόδου πρέπει να γίνεται κατανοητή εάν η σημασιολογία του αρχείου CAA πρόκειται να είναι κατανοητή από το προσδιορισμένο κοινό. Οι εκδότες δεν πρέπει να εκδίδουν τα πιστοποιητικά για ένα domain εάν το επεκταμένο σύνολο εκδοτών έγκρισης περιέχει άγνωστες ετικέτες εισόδου οι οποίες έχουν επισημανθεί ως κρίσιμες. Τα επικαλούμενα πρόσωπα δεν πρέπει να προσπαθήσουν να ενεργοποιήσουν τις CAA RRs εάν το σύνολο των επικαλούμενων εξουσιοδοτημένων προσώπων περιέχει άγνωστες ετικέτες εισόδου οι οποίες έχουν επισημανθεί ως κρίσιμες.
- Πρέπει να είναι μηδέν: Αυτό το bit φυλάσσεται για μελλοντική χρήση. Οι εκδότες δεν πρέπει να εκδώσουν τα πιστοποιητικά για ένα domain εάν το επεκταμένο σύνολο εκδοτών έγκρισης περιέχει ιδιότητες εισόδου με σύνολο ετικετών «Πρέπει να είναι μηδέν». Τα επικαλούμενα πρόσωπα δεν πρέπει να προσπαθήσουν να θέσουν σε ενέργεια τις CAA RRs εάν το σύνολο των επικαλούμενων εξουσιοδοτημένων προσώπων περιέχει ιδιότητες εισόδου με σύνολο ετικετών «Πρέπει να είναι μηδέν».

Το επικαλούμενο πρόσωπο διευκρινίζει ότι η αντίστοιχη ιδιότητα εισόδου

πρόκειται να χρησιμοποιηθεί από τις επικαλούμενες εφαρμογές και αποτελεί μέρος από το σύνολο επικαλούμενων προσώπων εξουσιοδότησης για το domain. Ο εκδότης διευκρινίζει ότι η αντίστοιχη ιδιότητα εισόδου πρόκειται να χρησιμοποιηθεί από τους εκδότες και αποτελεί μέρος του εκτεταμένου συνόλου εκδοτών έγκρισης για το domain. Οι ιδιότητες εισόδου είναι οι ακόλουθες:

- πολιτική < Certificate Policy OID >: δηλώνει μια εξουσιοδότηση εισόδου που χορηγεί την έγκριση να εκδώσει με βάση την διευκρινισμένη πολιτική πιστοποιητικών.
- μονοπάτι <Object Digest Identifier> < Αναγνωριστικό σύνοψης αντικειμένου>: δηλώνει μια εξουσιοδότηση εισόδου που χορηγεί την έγκριση να εκδώσει πιστοποιητικά τελικής οντότητας κάτω από μία έμπιστη διαδρομή που περιλαμβάνει την προσδιοριζόμενη υπογραφή του πιστοποιητικού.

Ένα Αναγνωριστικό σύνοψης αντικειμένου (ODI) είναι ένας τρόπος προσδιορισμού μιας αναφοράς σε μια περίπτωση αντικειμένου με τη βοήθεια μιας κρυπτογραφικής συνάρτησης σύνοψης. Μια CAA RR ιδιότητα διαδρομής μπορεί να χρησιμοποιήσει ένα ODI για να διευκρινίσει μία έμπιστη διαδρομή πιστοποιητικού με τη βοήθεια ενός πιστοποιητικού που υπογράφεται από πιστοποιητικό και ενός δημοσίου κλειδιού υπογραφής. Και στις δύο περιπτώσεις μια διαδρομή εξουσιοδότησης εισόδου εγκρίνει έναν εκδότη να εκδώσει ένα πιστοποιητικό τελικής οντότητας στο αντίστοιχο domain αν και μόνο αν είναι δυνατό να διαμορφωθεί μια έγκυρη διαδρομή πιστοποιητικών σε αυτό από το παραπεφθέν/αναφερόμενο πιστοποιητικό ή κλειδί.

5.4.2 ΠΑΡΑΔΕΙΓΜΑΤΑ ΧΡΗΣΗΣ

Το ακόλουθο παράδειγμα ενημερώνει τις CAs ότι τα πιστοποιητικά δεν πρέπει να εκδοθούν παρά μόνο κάτω από την προεπιλογή άρνησης της ασφάλειας της πολιτικής του πιστοποιητικού(1.3.6.1 .4.1.35405.666.1). Δεδομένου ότι η πολιτική δημοσιεύεται στο σημείο δημόσιας αποστολής, η πολιτική ισχύει για όλα τα υφιστάμενα domains κάτω από το example.com.

```
$ORIGIN example.com
.       CAA 1 policy 1.3.6.1.4.1.35405.666.1
```

Το ακόλουθο παράδειγμα ενημερώνει τις CAs ότι τα πιστοποιητικά δεν πρέπει να εκδοθούν παρά μόνο κάτω από το πιστοποιητικά της αρχικής πιστοποίησης:

```
$ORIGIN example.com
.       CAA 1 path MDIGA1UEJQYJYIZIAWUDBAIBBCAXzJgPaoT7Fe
            XaPzKv6mI2D0yilif+7WhzmhMGLe/oBA==
```

Μια περιοχή μπορεί να επιτρέπει σε πολλαπλές αρχές πιστοποίησης να εκδώσουν πιστοποιητικά την ίδια στιγμή. Το ακόλουθο παράδειγμα επιτρέπει την έκδοση κάτω από το Default Deny Security certification policy 'Example 1' or 'Example 2':

```
$ORIGIN example.com
.       CAA 1 policy 1.3.6.1.4.1.35405.666.1
.       CAA 1 policy 1.3.6.1.4.1.35405.666.2
```

Εάν οι καταχωρήσεις(entry) έγκρισης που χρησιμοποιούν τις ιδιότητες διαδρομής και πολιτικής εμφανίζονται σε ένα δεδομένο domain, η συμβατότητα με την καθεμία είναι ικανοποιητική για την έγκριση του αιτήματος.

Οι μελλοντικές εκδόσεις αυτής της προδιαγραφής ίσως χρησιμοποιούν την κρίσιμη επισήμανση για να εισάγουν νέες σημασιολογίες που πρέπει να είναι κατανοητές για τη

σωστή επεξεργασία του αρχείου, εμποδίζοντας τις αρχές πιστοποίησης που δεν αναγνωρίζουν το αρχείο από την έκδοση των πιστοποιητικών.

Στο ακόλουθο παράδειγμα, η ιδιότητα «tbs» επισημαίνεται ως κρίσιμη. Η Default Deny Security CA δεν εξουσιοδοτείται να εκδώσει κάτω ούτε από την πολιτική εκτός και αν οι κανόνες επεξεργασίας για την ιδιότητα της ετικέτας «tbs» είναι κατανοητοί.

$ORIGIN example.com

. CAA 1 policy 1.3.6.1.4.1.35405.666.1

. CAA 1 policy 1.3.6.1.4.1.35405.666.2

. CAA 129 tbs MDIGA1UEJQYJYIZIAWUDBAIBBCAXzJgPaoT7Fe

XaPzKv6mI2D0yilif+7WhzmhMGLe/oBA==

Η επιβολή από τις εφαρμογές επικαλούμενου προσώπου ακολουθεί τις ίδιες γενικές αρχές. Μια εφαρμογή επικαλούμενου προσώπου δεν πρέπει να θέτει σε ενέργεια τα αρχεία CAA εκτός και αν τουλάχιστον μια ιδιότητα εισόδου/καταχώρησης θέσει το σύνολο των επισημασμένων επικαλουμένων προσώπων, το οποίο δεν θα είναι κενό.

Στο ακόλουθο παράδειγμα, τα πιστοποιητικά δεν πρέπει να εκδοθούν παρά μονό κάτω από τη Default Deny Security του παραδείγματος της πολιτικής πιστοποιητικών και οι εφαρμογές επικαλούμενου προσώπου μπορούν να απορρίπτουν πιστοποιητικά τα οποία δε συμβαδίζουν με αυτήν την απαίτηση:

$ORIGIN example.com

. CAA 3 policy 1.3.6.1.4.1.35405.666.1

Στη συνηθισμένη πορεία της επιχείρησης ένας διαχειριστής ενός ονόματος μπορεί να αποσύρει την έγκριση για την έκδοση νέων πιστοποιητικών πριν τη λήξη των προηγούμενων εκδοθέντων πιστοποιητικών.

Στο ακόλουθο παράδειγμα, οι εφαρμογές επικαλούμενου προσώπου ενημερώνονται ότι τα πιστοποιητικά που εκδίδονται κάτω ακόμη και από την πολιτική πρόκειται να εξεταστούν για να εγκριθούν αλλά τα νέα πιστοποιητικά μπορούν μόνο να εκδοθούν κάτω από πρώτα.

$ORIGIN example.com

. CAA 3 policy 1.3.6.1.4.1.35405.666.1

. CAA 2 policy 1.3.6.1.4.1.35405.666.2

5.4.3 ΕΠΕΞΕΡΓΑΣΙΑ ΤΗΣ ΑΡΧΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ

Πριν από την έκδοση ενός πιστοποιητικού μία συμβατή αρχή πιστοποίησης πρέπει να ελέγξει για δημοσίευση ενός σχετικού αρχείου εγγραφών CAA και εάν έχει δημοσιευτεί τέτοιο αρχείο, πρέπει να ελέγξει εάν το ζητούμενο πιστοποιητικό είναι συνεπές μαζί τους. Εάν το ζητούμενο πιστοποιητικό δεν είναι σύμφωνο με τις σχετικές CAA RRs, η αρχή πιστοποίησης δεν πρέπει να εκδώσει το πιστοποιητικό.

Το σύνολο των εξουσιοδοτημένων εκδοτών για ένα όνομα διεύθυνσης αποτελείται από το σύνολο όλων των εξουσιοδοτημένων εγγραφών CAA που δηλώνονται για την κανονική μορφή του διευκρινισμένου ονόματος.

Το εκτεταμένο σύνολο των εξουσιοδοτημένων εκδοτών για ένα όνομα διεύθυνσης αποτελείται από το σύνολο όλων των εξουσιοδοτημένων εκδοτών για εκείνο το όνομα εάν το σύνολο δεν είναι κενό.

Διαφορετικά το εκτεταμένο σύνολο των εξουσιοδοτημένων εκδοτών για ένα όνομα διεύθυνσης αποτελείται από το σύνολο των εξουσιοδοτημένων εκδοτών για το αντίστοιχο κοινό σημείο εξουσιοδότησης για εκείνο το όνομα.

Εάν το εκτεταμένο σύνολο των εξουσιοδοτημένων εκδοτών για ένα όνομα διεύθυνσης δεν είναι κενό, μια αρχή πιστοποίησης δεν πρέπει να εκδώσει ένα πιστοποιητικό αν δεν προσαρμόζεται τουλάχιστον σε μια είσοδο έγκρισης στο εκτεταμένο σύνολο των εξουσιοδοτημένων εκδοτών.

Να σημειωθεί ότι ενώ πρέπει να είναι δυνατό να διαμορφωθεί μια διαδρομή επικύρωσης πιστοποιητικών που περιέχει τουλάχιστον ένα πιστοποιητικό το οποίο να έχει προσδιοριστεί με αυτόν τον τρόπο, αυτό μπορεί να είναι επίσης δυνατό να διαμορφώσει έγκυρες διαδρομές πιστοποιητικών ενώ δεν είναι (έγκυρες).

Παραδείγματος χάριν, μία αρχή πιστοποίησης που έχει ενημερώσει το πιστοποιητικό ρίζα για να επεκτείνει την ημερομηνία λήξης έχει δικαίωμα να εκδώσει πιστοποιητικά για domains όπου η εγγραφή CAA μόνο διευκρινίζει το παλαιότερο πιστοποιητικό ρίζα υπό τον όρο ότι το παλαιότερο πιστοποιητικό ρίζα δεν έχει λήξει και κατά συνέπεια είναι πιθανό να διαμορφώσει μια έγκυρη διαδρομή πιστοποιητικών.

5.4.3.1 ΚΑΝΟΝΙΚΟ ΟΝΟΜΑ ΔΙΕΥΘΥΝΣΗΣ

Το DNS καθορίζει τους μηχανισμούς CNAME και DNAME για διευκρινισμένα ψευδώνυμα των domain name. Το κανονικό όνομα ενός DNS ονόματος είναι το όνομα εκείνο που εξάγεται από την εκτέλεση όλων των DNS διαδικασιών ψευδώνυμων. Πρόκειται δηλαδή για ένα όνομα διεύθυνσης το οποίο δεν είναι ψευδώνυμο.

5.4.4 ΕΠΕΞΕΡΓΑΣΙΑ ΕΦΑΡΜΟΓΗΣ ΕΠΙΚΑΛΟΥΜΕΝΟΥ ΠΡΟΣΩΠΟΥ

Οι εφαρμογές επικαλούμενου προσώπου μπορούν να επιβάλλουν τους περιορισμούς έκδοσης της CAA στην επιλογή τους, υπό τον όρο ότι το σύνολο επικαλούμενων προσώπων εξουσιοδότησης δεν είναι κενό.

Τα ονόματα διευθύνσεων που επιλέγουν να επισημαίνουν τα αρχεία προς χρήση από τις εφαρμογές επικαλούμενου προσώπου πρέπει να είναι ενήμερα ότι οι καταχωρήσεις ιδιοτήτων που υποστηρίζονται σε αυτή την έκδοση της προδιαγραφής έχει σχεδιαστεί μόνο για να υποστηρίξει τις απαιτήσεις των περιορισμών των επιβαλλόμενων εκδοτών. Ενώ αυτές οι καταχωρήσεις ιδιοτήτων μπορούν να είναι επαρκείς για να επιτρέψουν την επιβολή από τις εφαρμογές επικαλούμενου προσώπου σε μερικές περιστάσεις, δεν προορίζονται για να παρέχουν πλήρη κάλυψη των απαιτήσεων για αυτόν τον σκοπό.

Τα ονόματα διευθύνσεων που περιέχουν περιορισμούς της έκδοσης της CAA RR που προορίζονται για χρήση από τις εφαρμογές επικαλούμενου προσώπου πρέπει να επικυρωθούν με τη χρήση της DNSSEC ή με άλλα ισοδύναμα μέσα.

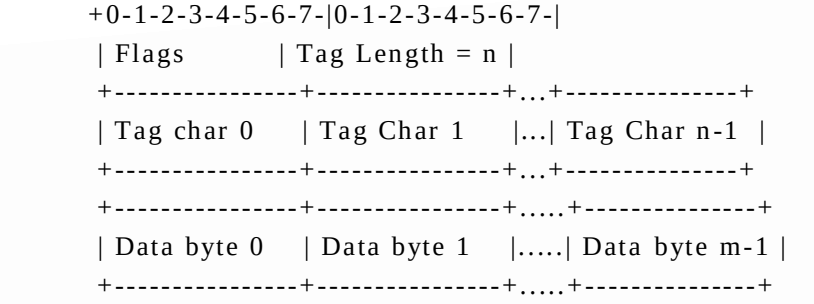
Εάν η DNSSEC αναπτύσσεται σε ένα όνομα των εφαρμογών επικαλούμενου προσώπου πρέπει να μεταχειριστεί την αποτυχία να επικυρωθούν οι υπογραφές των CAA RR ή της απουσίας των CAA RR των οποίων η παρουσία υποδεικνύεται ως ισοδύναμη με μία ασυμβίβαστη CAA RR.

5.4.5 ΜΗΧΑΝΙΣΜΟΣ

5.4.5.1 ΣΥΝΤΑΞΗ

Μία CAA RR περιέχει μια ενιαία ιδιότητα εισόδου που αποτελείται από ζεύγος ετικετών. Κάθε ετικέτα αντιπροσωπεύει μια ιδιότητα της εγγραφής CAA. Η τιμή από μια CAA ιδιότητα είναι αυτή που διευκρινίζεται στον αντίστοιχο τομέα τιμών.

Ένα όνομα περιοχών μπορεί να έχει πολλαπλάσια CAA RRs που συνδέονται με αυτό και μία δοσμένη ιδιότητα μπορεί να διευκρινιστεί παραπάνω από μία φορά. Το πεδίο στοιχείων της CAA περιέχει μια ιδιότητα εισόδου. Μια ιδιότητα εισόδου αποτελείται από τα ακόλουθα πεδία στοιχείων



Όπου το n είναι το μήκος που διευκρινίζεται στο πεδίο μήκους ετικετών και το m είναι η παραμονή των bytes στον πεδίο των στοιχείων (m =d – n – 2) όπου το d είναι το μήκος του πεδίου των στοιχείων. Ακολουθεί ο ορισμός των πεδίων των δεδομένων:

- Bit 0: Κρίσιμη επισήμανση. Εάν η τιμή τεθεί (1), η κρίσιμη επισήμανση βεβαιώνεται και η ιδιότητα πρέπει να γίνει κατανοητή εάν η CAA RR πρόκειται να υποβληθεί σε επεξεργασία σωστά. Μια αρχή πιστοποίησης δεν πρέπει να εκδώσει τα πιστοποιητικά για οποιαδήποτε περιοχή που περιέχει μια κρίσιμη ιδιότητα CAA για έναν άγνωστο ή αστήρικτο τύπο ιδιότητας.
- Bit 5: Πρέπει να είναι μηδέν. Το Bit 5 είναι κρατημένο και πρέπει να τεθεί μηδέν. Επεξεργαστές που αντιμετωπίζουν ένα αρχείο CAA που περιέχει μια ιδιότητα με αυτό το Bit τιθέμενο πρέπει να μεταχειριστούν το σύνολο των αρχείων σαν να βεβαιώθηκε η κρίσιμη ιδιότητα για ένα άγνωστο αρχείο.
- Bit 6: Χρήση των επικαλούμενων εφαρμογών. Εάν τεθεί, η ιδιότητα εισόδου περιέχει μια είσοδο έγκρισης που αποτελεί μέρος του συνόλου επικαλούμενων εξουσιοδοτημένων προσώπων που τίθεται για την αντίστοιχη περιοχή.
- Bit 7: Χρήση εκδοτών Εάν τεθεί, η ιδιότητα εισόδου περιέχει είσοδο έγκρισης που αποτελεί μέρος της εφαρμογής εκδοτών Έγκρισης που τίθεται για την αντίστοιχη περιοχή.

Το Bit 0 είναι το σημαντικότερο Bit και το Bit 7 είναι το λιγότερο σημαντικό. Κατά συνέπεια μια τιμή επισήμανσης 0x51 δείχνει ένα μήκος ετικετών των 5 bytes και ότι η ιδιότητα εισόδου δεν είναι κρίσιμη και δεν χρησιμοποιείται για την επεξεργασία των συμβαλλόμενων μερών.
ΤΙΜΗ ΤΗΣ ΙΔΙΟΤΗΤΑΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

Η τιμή της ιδιότητας της πολιτικής ορίζει μια είσοδο έγκρισης μέσω ενός ASN.1 OID που διευκρινίζει μια πολιτική πιστοποίησης. Μια αρχή πιστοποίησης εξουσιοδοτείται για να εκδώσει τα πιστοποιητικά υπό μια πολιτική εισόδου έγκρισης εάν και μόνο εάν:

- η αρχή πιστοποίησης έχει το δικαίωμα να εκδώσει τα πιστοποιητικά υπό τη διευκρινισμένη πολιτική, ΚΑΙ
- το αίτημα πιστοποιητικών είναι συμβατό με τις απαιτήσεις της διευκρινισμένης πολιτική, ΚΑΙ
- το αίτημα πιστοποιητικών ικανοποιεί όλα τα κριτήρια κάτω από την πολιτική πιστοποίησης υπό την οποία το πιστοποιητικό πρόκειται να εκδοθεί.

Κάθε ιδιότητα της πολιτική διευκρινίζει μια ενιαία ASN.1 OID τιμή που αποτελείται από τον τύπο ASN.1, το προσδιοριστικό του μήκους και τα δεδομένα OID.

Η ιδιότητα της πολιτικής ισχύει για τι διευκρινισμένη πολιτική OID και όλες τις πολιτικές OIDs που εμπίπτουν στο ίδιο τόξο OID. Εάν το τόξο OID 1.3.6.1 .4.1.35405.666 διευκρινίζεται, τότε οι OIDs πολιτικές 1.3.6.1 .4.1.35405.666, 1.3.6.1 .4.1.35405.666.1, 1.3.6.1 .4.1.35405.666.2 κ.λπ. είναι όλες διευκρινισμένες.

Το πιστοποιητικό που εκδίδεται μπορεί να ενσωματώσει μόνο του τη διευκρινισμένη πολιτική OID αλλά δεν απαιτείται υπό τον όρο ότι η έκδοση του

πιστοποιητικού είναι σύμφωνη με τις απαιτήσεις της διευκρινισμένης πολιτικής.

Παραδείγματος χάριν, μια αρχή πιστοποίησης που προσφέρει δύο επίπεδα πολιτικής πιστοποίησης τέτοια ώστε το υψηλότερο επίπεδο της διαβεβαίωσης να περιλαμβάνει όλες τις απαιτήσεις του χαμηλότερου μπορεί να στηρίζεται σε μια ιδιότητα της πολιτικής που διευκρινίζει τη χαμηλότερη πολιτική διαβεβαίωσης ως έγκριση για την έκδοση κάτω από την υψηλότερη πολιτική διαβεβαίωσης αλλά όχι αντίστροφα.

ΤΙΜΗ ΤΗΣ ΙΔΙΟΤΗΤΑΣ ΜΟΝΟΠΑΤΙΟΥ

Η τιμή της ιδιότητας του μονοπατιού διευκρινίζει μια είσοδο έγκρισης με τη βοήθεια ενός πιστοποιητικού που υπογράφει πιστοποιητικά ή από ένα κλειδί που υπογράφει το πιστοποιητικό.

Η αρχή πιστοποίησης εξουσιοδοτείται για να εκδώσει τα πιστοποιητικά κάτω από ένα μονοπάτι εισόδου έγκρισης εάν και μόνο εάν

- ένα έγκυρο και έμπιστο μονοπάτι PKIX μπορεί να διαμορφωθεί από το διευκρινισμένο πιστοποιητικό που υπογράφει πιστοποιητικά ή από ένα κλειδί που υπογράφει το πιστοποιητικό για το πιστοποιητικό που πρόκειται να εκδοθεί, ΚΑΙ
- το αίτημα πιστοποιητικών ικανοποιεί όλα τα κριτήρια κάτω από την πολιτική πιστοποίησης υπό την οποία το πιστοποιητικό πρόκειται να εκδοθεί.

5.4.6 ΘΕΩΡΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Οι εγγραφές πόρων CAA παρέχουν έναν έλεγχο υπευθυνότητας. Προορίζονται να εμποδίσουν παρά να αποτρέψουν κάποια ανεπιθύμητη συμπεριφορά.

Ενώ μια αρχή πιστοποίησης μπορεί να επιλέξει να αγνοήσει τις δημοσιευμένα CAA εγγραφές, αυξάνει έτσι την πιθανότητα να υπογραφεί λανθασμένα ένα πιστοποιητικό και τις συνέπειες που θα έχει αυτό. Μόλις είναι γνωστό ότι μια αρχή πιστοποίησης παρατηρεί τις εγγραφές CAA, κακόβουλα αιτήματα εγγραφής θα στοχεύσουν στις αμελές αρχές πιστοποίησης που δεν το κάνουν αυτό, και έτσι το ποσοστό των λάθος υπογεγραμμένων μεταξύ των αμελών αρχών πιστοποίησης θα αυξηθεί.

Δεδομένου ότι μια αρχή πιστοποίησης μπορεί σαφώς να αποφύγει να υπογράψει λανθασμένα πραγματοποιώντας τη διαδικασία CAA, η πιθανότητα των κυρώσεων ενάντια στην αμελή αρχή πιστοποίησης αυξάνεται. Η αποτυχία να παρατηρηθούν οι περιορισμοί έκδοσης της CAA παρέχει αντικειμενικά κριτήρια για τον αποκλεισμό των εκδοτών από τις ενσωματωμένες έμπιστες ρίζες.

Αντίθετα, μια αρχή πιστοποίησης που επεξεργάζεται τις CAA εγγραφές σωστά μπορεί εύλογα να υποστηρίξει ότι οποιοδήποτε υπολειμματικό γεγονός λανθασμένης έκδοσης θα μπορούσε να έχει αποφευχθεί αν ο κάτοχος του ονόματος δημοσίευε κατάλληλες εγγραφές CAA.

5.4.6.1 ΛΑΝΘΑΣΜΕΝΗ ΕΚΔΟΣΗ ΑΠΟ ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΗ ΑΡΧΗ ΠΙΣΤΟΠΟΙΗΣΗΣ

Η χρήση των εγγραφών CAA δεν παρέχει προστασία ενάντια σε λανθασμένη έκδοση από μια εξουσιοδοτημένη αρχή πιστοποίησης. Οι κάτοχοι των domain πρέπει να εξασφαλίσουν ότι οι αρχές πιστοποίησης που εγκρίνουν για να εκδώσουν τα πιστοποιητικά τους χρησιμοποιούν τους κατάλληλους ελέγχους για να εξασφαλίσουν ότι τα πιστοποιητικά διανέμονται μόνο στα εξουσιοδοτημένα συμβαλλόμενα μέρη στον οργανισμό. Τέτοιοι έλεγχοι είναι πιο κατάλληλο να καθορίζονται από τον κάτοχο και από την εξουσιοδοτημένη αρχή πιστοποίησης απευθείας.

5.4.6.2 ΠΛΑΣΤΟΓΡΑΦΗΣΗ ΤΩΝ ΕΓΓΡΑΦΩΝ CAA

Η πλαστογράφηση μιας εγγραφής CAA ή η εισαγωγή μίας ψευδούς εγγραφής θα μπορούσε να επιτρέψει σε έναν επιτιθέμενο να λάβει ένα πιστοποιητικό από μία αρχή πιστοποίησης που δεν ήταν εξουσιοδοτημένη να εκδώσει για εκείνο το όνομα περιοχών.

Οι εφαρμογές που εκτελούν τον έλεγχο CAA πρέπει να μετριάσουν τον κίνδυνο καταστολής ή υποκρισίας των εγγραφών CAA με τη βοήθεια της επικύρωσης της DNSSEC.

Σε περιπτώσεις όπου η επικύρωση DNSSEC δεν είναι διαθέσιμη, ο έλεγχος CAA έχει περιορισμένη ασφάλεια.

Από τότε που ένα πιστοποιητικό που εκδίδεται από μία αρχή πιστοποίησης μπορεί να ισχύσει για αρκετά έτη, οι συνέπειες μιας επίθεσης υποκρισίας ή καταστολής είναι πολύ μεγαλύτερες για τις αρχές πιστοποίησης και έτσι πρόσθετα αντίμετρα είναι δικαιολογημένα.

Μία αρχή πιστοποίησης πρέπει να μετριάσει αυτόν τον κίνδυνο με την υιοθέτηση της επαλήθευσης από την DNSSEC όποτε είναι δυνατό και να απορρίπτει τα αιτήματα πιστοποιητικού εν πάση περιπτώσει όπου δεν είναι δυνατό να ελεγχθεί η μη ύπαρξη ή το περιεχόμενο της σχετικής CAA εγγραφής.

Σε περιπτώσεις όπου η DNSSEC δεν επεκτείνεται σε μια αντίστοιχη περιοχή, μία αρχή πιστοποίησης πρέπει να προσπαθήσει να μετριαστεί αυτός ο κίνδυνος με την υιοθέτηση κατάλληλων ελέγχων ασφαλείας DNS. Παραδείγματος χάριν όλα τα τμήματα της διαδικασίας DNS αναζήτησης πρέπει να εκτελεσθούν ενάντια στον επιτακτικό κεντρικό υπολογιστή.

Τα εναποθηκευμένα στοιχεία μπορούν να χρησιμοποιηθούν στην πρόσθετη υποστήριξη για την πλαστογράφησης ή στους έλεγχους καταστολής χωρίς όμως να βασιζόμαστε σε αυτά.

Η εισαγωγή μιας δύσμορφης ή κακόβουλης CAA RR θα μπορούσε θεωρητικά να επιτρέψει την άρνηση της υπηρεσίας. Αυτή η συγκεκριμένη απειλή δεν θεωρείται ότι προσθέτει σημαντικούς κίνδυνους σε μια επισφαλή DNS υπηρεσία.

5.4.7 ΚΑΤΑΧΡΗΣΗ ΤΗΣ ΚΡΙΣΙΜΗΣ ΕΠΙΣΗΜΑΝΣΗΣ

Μια αρχή πιστοποίησης θα μπορούσε να χρησιμοποιήσει την κρίσιμη επισήμανση ως τέχνασμα προς τους πελάτες στην έκδοση των αρχείων που αποτρέπουν άλλες Αρχές πιστοποίησης από την έκδοση των πιστοποιητικών ακόμα κι αν ο πελάτης σκοπεύει να εγκρίνει πολλαπλάσιους προμηθευτές.

Στην πράξη, μια τέτοια επίθεση θα ήταν ελάχιστης επίδρασης από οποιονδήποτε ικανό ανταγωνιστή που βρέθηκε ανίκανος να εκδώσει τα πιστοποιητικά λόγω της έλλειψης υποστήριξης για μία ιδιότητα που έχει χαρακτηριστεί κρίσιμη.

ΚΕΦΑΛΑΙΟ 6. DNSCURVE: ΜΙΑ ΕΝΑΛΛΑΚΤΙΚΗ ΓΙΑ ΤΗ DNSSEC

6.1 ΕΙΣΑΓΩΓΗ

Το Domain Name System (DNS) χρησιμοποιείται για πολύ καιρό, μετατρέποντας τα ονόματα των διευθύνσεων σε διευθύνσεις IP. Στην πορεία βρέθηκαν αρκετές ελλείψεις στο πρωτόκολλο, συμπεριλαμβανομένης της έλλειψης του Kaminsky το 2008, η οποία απλά προστίθεται στην επιθυμία για την αντικατάστασή του. Όμως το DNS εξακολουθεί χρησιμοποιείται και δε φαίνεται να σταματήσει η χρήση του, τουλάχιστον εν μέρει, επειδή η αντικατάστασή του, η DNSSEC, δεν επιλύει πραγματικά όλα τα προβλήματα, και επίσης δημιουργεί και κάποια δικά του. Μια πρόταση από τον Daniel J. Bernstein, που ονομάζεται DNSCurve, έχει μερικά ενδιαφέροντα χαρακτηριστικά που θα μπορούσαν να την κάνουν μια βιώσιμη εναλλακτική λύση για το DNS και τη DNSSEC - ίσως αυτή που θα μπορούσε να υιοθετηθεί ευρέως. Ο Bernstein τείνει να χρησιμοποιεί τους δικούς του κανόνες έναντι των «πρότυπων» εργαλείων UNIX. Όμως, τα αποτελέσματα που παρουσιάζει είναι καλά, η εγγύηση της ασφάλειας που έχει προσφέρει δεν έχει ακόμη διεκδικηθεί.

Η DNSCurve συνεχίζει την ανορθόδοξη τάση του Bernstein. Η θεμελιώδης διαφορά μεταξύ της DNSCurve και της DNSSEC είναι ότι η τελευταία έθεσε ως στόχο τη διαβεβαίωση ότι δεν θα υπήρχε η αναγκαιότητα για κρυπτογραφία σε κάθε ερώτημα. Αυτό το κάνει με τις υπογραφές πριν από τον υπολογισμό, το οποίο το καθιστά ευάλωτο σε επιθέσεις επανάληψης. Αντ 'αυτού, η DNSCurve δέχεται την κρυπτογράφηση ανά ερώτημα, αλλά το κάνει με τη χρήση ενός αλγόριθμου κρυπτογράφησης, που ονομάζεται Ελλειπτική Κρυπτογραφική Καμπύλη (Elliptic Curve Cryptography - ECC), ο οποίος είναι πολύ πιο γρήγορος από τον RSA.

Μέρος του τι κάνει τον ECC πιο αποτελεσματικό είναι ότι μπορεί να χρησιμοποιεί πολύ μικρότερα κλειδιά από ότι ο RSA (256 bits έναντι 1024 ή περισσότερα bits) για να δώσει το ισοδύναμο επίπεδο ασφάλειας. Επιπλέον, οι πιο γνωστές επιθέσεις στον ECC δεν έχουν καταφέρει κάτι καλύτερο στα σχεδόν 25 χρόνια από τότε που θεσπίστηκε. Σε μια πρόσφατη παρουσίαση, ο Bernstein δείχνει ένα σημείο αναφοράς της επίδοσης από την πλευρά του εξυπηρετητή: "Με αυτό το λογισμικό, ένας υπολογιστής χαμηλού κόστους με 2.4GHz Core 2 Quad CPU μπορεί να κρυπτογραφήσει και να αυθεντικοποιήσει 50 δισεκατομμύρια πακέτα ανά ημέρα έως 500 εκατομμύρια πελάτες. Η συνολική φόρτωση στο .com είναι 38 δισεκατομμύρια πακέτα ανά ημέρα από 5 εκατομμύρια πελάτες. ".

Ο Bernstein χρησιμοποιεί μια συγκεκριμένη καμπύλη, την Curve25519, για την DNSCurve. Βασίζεται σε μια "βολική" αρχή, 2 ^ 255 - 19, από την οποία παίρνει το όνομά της. Αυτή η καμπύλη αποτελεί το αντικείμενο μιας εργασίας του Bernstein με τίτλο "Curve25519: νέες Diffie-Hellman ταχείς εγγραφές". Ο ECC εκτιμάται ότι θα είναι μία ευρεσιτεχνία, αλλά ο Bernstein αμφισβητεί την ιδέα ότι η Curve25519 καλύπτεται από τις ευρεσιτεχνίες. Όπως και με τόσες πολλές από τις νεότερες τεχνολογίες, όμως, τα προβλήματα ευρεσιτεχνίας πρέπει να παρακολουθούνται όσο αναφορά την DNSCurve.

Η DNSCurve αλλάζει επίσης τον τρόπο με τον οποίο ονομάζονται οι εξυπηρετητές ονόματος για τα domains. Αντί για τα αυθαίρετα ονόματα των κεντρικών υπολογιστών, όπως το ns3.lwn.net (ένα ανύπαρκτο παράδειγμα), το τμήμα ns3 θα αλλάξει σε μια κωδικοποίηση του δημόσιου κλειδιού του domain. Με τον τρόπο αυτό, δεν απαιτείται η αποστολή επιπλέων πακέτων για να τον χειρισμό την ανταλλαγής των κλειδιών, καθώς η κανονική σειρά ερωτημάτων DNS θα προσφέρει αυτό το όνομα.

Ένα ερώτημα DNS θα αποτελείται από ένα μήνυμα που περιέχει το δημόσιο κλειδί του πελάτη, μαζί με το πραγματικό ερώτημα, κρυπτογραφημένο με το δημόσιο κλειδί του εξυπηρετητή. Η απόκριση θα είναι επίσης κρυπτογραφημένη, αυτή τη φορά χρησιμοποιώντας το δημόσιο κλειδί του πελάτη. Και στις δύο περιπτώσεις, τα πακέτα θα πρέπει να υπογραφούν κατά τέτοιο τρόπο, ώστε κάθε πλευρά μπορεί να βεβαιωθεί ότι το πακέτο ήρθε από τον σωστό υπολογιστή.

Η DNSCurve προστατεύει από διάφορες επιθέσεις που βασίζονται στο DNS καλύτερα από τη DNSSEC, αλλά υπάρχουν μερικοί τομείς όπου η DNSSEC είναι πιο ασφαλής. Συγκεκριμένα, τα ιδιωτικά κλειδιά στους DNSSEC υπολογιστές δεν μπορούν να διακυβευτούν από έναν επιτιθέμενο που έχει αποκτήσει τον έλεγχο του εξυπηρετητή που παρέχεται από το διαχειριστή του οποίου του έχει αφαιρεθεί το κλειδί από εκείνον τον

εξυπηρετητή. Επειδή η DNSSEC υπολογίζει προηγουμένως τα κρυπτογραφημένα δεδομένα, το ιδιωτικό κλειδί δεν χρειάζεται να εγκατασταθεί στον εξυπηρετητή, σε αντίθεση με τη DNSCurve.

Η DNSCurve είναι μόνο ένα μέρος της προσπάθειας του Bernstein για να δει το διαδίκτυο κρυπτογραφημένο σε ολόκληρη την κυκλοφορία του. Το όραμά του είναι ότι με τη χρήση του ECC και της Curve25519 (ή κάποιας άλλης, αποτελεσματικής, αλλά και ισχυρής κρυπτογράφησης), δεν θα υπήρχε κίνηση του απλού κειμένου στο δίκτυο. Αυτό το όραμα είναι λογικό, ανεξάρτητα από το αν οι ιδέες εφαρμογής του Bernstein, υιοθετούνται ή όχι. Τελικά, η καθολική κρυπτογράφηση της κυκλοφορίας στο internet είναι κάτι που είναι πολύ πιθανό να δούμε.

6.2 DNCURVE: ΑΣΦΑΛΕΙΑ ΣΥΝΔΕΣΗΣ-ΕΠΙΠΕΔΟΥ ΓΙΑ ΤΟ DOMAIN NAME SYSTEM

Η DNSCurve προσθέτει ασφάλεια σύνδεσης επιπέδου για το Domain Name System. Περιλαμβάνει ένα μηχανισμό κατανομής κλειδιού, συμβατού με το λογισμικό του εξυπηρετητή ονόματος και με τις υπηρεσίες του μητρώου, καθώς και δύο μορφές πακέτων: μία απλή, απλοποιημένη μορφή που απαιτεί ελάχιστο χώρο και επεξεργασία από πάνω και μία κυρίως προς τα πίσω-συμβατή μορφή που προορίζεται για χρήση με αυστηρά firewalls και DNS proxies.

Τα πακέτα DNSCurve περιλαμβάνουν ένα κρυπτογραφικό MAC (γνωστός και ως αυθεντικοποιητής) για την παροχή της ακεραιότητας και της διαθεσιμότητας. Οι πελάτες μπορούν να είναι βέβαιοι ότι οι επαληθευμένες απαντήσεις προέρχονταν από τον κατάλληλο εξυπηρετητή και δεν ήταν παραποιημένες από κάποιον επιτιθέμενο, ενώ οι εξυπηρετητές μπορούν να είναι βέβαιοι ότι οι απαντήσεις δεν θα επαναληφθούν σε βάρος άλλων ακούσιων πελατών. Επιπλέον, τα πακέτα DNSCurve είναι κρυπτογραφημένα για να παρέχουν κάποια αξιοπιστία.

6.2.1 ΥΠΟΒΑΘΡΟ

Η DNSCurve χρησιμοποιεί την Curve25519XSalsa20Poly1305, δηλαδή έναν συγκεκριμένο συνδυασμό των θεμελιακών Curve25519, Salsa20, και Poly1305. Ειδικότερα, πρόκειται για ένα κρυπτογραφικό σύστημα που διαθέτει δημόσια και μυστικά κλειδιά των 256bit, nonces των 192 bit, και αυθεντικοποιητές των 128 bit.

Κάθε πελάτης και εξυπηρετητής DNSCurve έχει ένα μυστικό κλειδί και ένα αντίστοιχο δημόσιο κλειδί. Οι DNSCurve εξυπηρετητές διανέμουν τα δημόσια κλειδιά τους κωδικοποιώντας τα στα ονόματα των εξυπηρετητών ενσωματωμένα στις πρότυπες NS εγγραφές του DNS, ενώ οι DNSCurve πελάτες διανέμουν τα δημόσια κλειδιά τους, εντάσσοντάς τα στα πακέτα ερωτημάτων τους.

Όταν ένας DNSCurve πελάτης πρόκειται να στείλει ένα ερώτημα DNS για έναν εξυπηρετητή ονομάτων, αν ο πελάτης γνωρίζει ένα δημόσιο κλειδί DNSCurve για το όνομα του εξυπηρετητή, μπορεί να πραγματοποιήσει απευθείας χρήση του δημόσιου κλειδιού μαζί με το δικό ιδιωτικό κλειδί DNSCurve και ενός nonce για την προστασία των ερωτημάτων του σε ένα «κρυπτογραφικό κουτί». Ο πελάτης κωδικοποιεί, στη συνέχεια, αυτό το «κρυπτογραφικό κουτί» μαζί με το nonce και το δικό του δημόσιο κλειδί ως ένα εκτεταμένο πακέτο DNSCurve ερωτήματος, το οποίο στέλνει στον DNSCurve εξυπηρετητή αντί για το αρχικό ερώτημα DNS.

Με τη λήψη ενός πακέτου ερωτήματος DNS, ένας DNSCurve εξυπηρετητής ονομάτων πρέπει να αντιμετωπίσει πρώτα το πακέτο ως ένα DNSCurve πακέτο ερωτήματος, με την εξαγωγή του DNSCurve δημόσιου κλειδιού του πελάτη nonce, και του ερωτήματος και να προσπαθήσει να ανοίξει «το κουτί» με τη χρήση του εξαγόμενου δημόσιο κλειδιού και με το ιδιωτικό κλειδί του . Ωστόσο, εάν αυτό αποτύχει (όπως για παράδειγμα εάν το πακέτο δεν έχει μορφοποιηθεί ως ένα διευρυμένο DNSCurve πακέτο ερωτήματος ή αν ο αυθεντικοποιητής του κουτιού δεν είναι έγκυρος), τότε ο εξυπηρετητής απαντά στο πακέτο ως ένα κανονικό πακέτο DNS.

Υποθέτοντας ότι η παραπάνω διαδικασία επιτυγχάνει, τότε ο εξυπηρετητής ανακαλύπτει το αρχικό πακέτο ερωτήματος του πελάτη. Για να στείλει μια απόκριση, ο εξυπηρετητής επιλέγει μια επέκταση nonce για να προσαρτήσει στην επιλεγμένη nonce του

πελάτη, και προστατεύει το πακέτο απόκρισης του σε ένα «κρυπτογραφικό κουτί» χρησιμοποιώντας το εκτεταμένο nonce και τα ίδια κλειδιά που χρησιμοποίησε για να φτάσει στο αρχικό ερώτημα του πελάτη DNS. Ο εξυπηρετητής κωδικοποιεί τότε αυτό το κρυπτογραφικό κουτί ώς ένα εκτεταμένο πακέτο απόκρισης DNSCurve, το οποίο στέλνει στον DNSCurve πελάτη αντί της αρχικής απόκρισης.

Εν τω μεταξύ, ο DNSCurve πελάτης περιμένει για μία εκτεταμένη απόκριση DNSCurve. Εάν λάβει ένα πακέτο απόκρισης που δεν είναι μη DNSCurve, ένα εκτεταμένη πακέτο απόκρισης DNSCurve με ένα άκυρο nonce (δηλαδή, όχι μια επέκταση του αρχικού nonce του) ή ένα μη έγκυρο κρυπτογραφικό κουτί (δηλαδή, δεν μπορεί να ανοίξει με τα ίδια κλειδιά και με το εκτεταμένο nonce) , τότε απορρίπτει το πακέτο και συνεχίζει να περιμένει. Από τη στιγμή που θα παραλάβει έγκυρο εκτεταμένο πακέτο απόκρισης DNSCurve, ανοίγει το κρυπτογραφικό κουτί για να ανακαλύψει αρχική απάντηση του εξυπηρετητή DNS.

6.2.2 Η ΚΩΔΙΚΟΠΟΙΗΣΗ ΤΩΝ 32 BITS

Μερικές φορές η DNSCurve μεταβιβάζει αυθαίρετα σειρές byte στα ονόματα διευθύνσεων. Ενώ το DNS πρωτόκολλο έχει ασφάλεια των 8 bit για τα ονόματα και τις ετικέτες (εκτός από τον χειρισμό για τον μη-διαχωρισμό πεζών και κεφαλαίων των αλφαβητικών χαρακτήρων ASCII), πολλά εργαλεία έχουν πρόβλημα με τους αυθαίρετους χαρακτήρες στα ονόματα διευθύνσεων, ιδιαιτέρως τα λογισμικά καταχώρησης του ονόματος της διεύθυνσης. Για την αντιμετώπιση αυτού του περιορισμού, η DNSCurve κωδικοποιεί σειρές byte χρησιμοποιώντας ένα σύνολο από ασφαλής αλφαριθμητικούς χαρακτήρες.

Στην κωδικοποίηση των 32 bit DNSCurve[4], μια σειρά byte ερμηνεύεται ως ένας αριθμός σε little-endian μορφή. Κάθε ακολουθία των 5 bit αυτού του αριθμού, από τη λιγότερο σημαντική στην πιο σημαντική, είναι κωδικοποιημένη ως ένα από τα τυπικά "ψηφία" "0123456789bcdfghjklmnpqrstuvwxyz". Μια τελική ακολουθία με λιγότερα από 5 bits είναι μηδέν-εκτεταμένη πριν την κωδικοποίηση. Οι αποκωδικοποιητές πρέπει να αποδεχθούν το "BCDFGHJKLMNPQRSTUVWXYZ" ως συνώνυμα για το «bcdfghjklmnpqrstuvwxyz".

Για παράδειγμα, οι δύο-byte σειρές με bytes {0x64, 0x88} (για παράδειγμα, {100.136} δεκαδικοί) ερμηνεύεται ως ο ακέραιος 0x8864 (δηλαδή, 34 916). Τα bits 1000100001100100 αυτού του ακέραιου χωρίζονται σε 5 τμήματα bits, 00100, 00011, 00010, 00001, τα οποία με τη σειρά τους κωδικοποιούνται ως "4", "3", "2", "1". Η αρχική σειρά είναι ως εκ τούτου κωδικοποιημένη σαν τη σειρά "4321".

6.2.2.1 ΠΑΡΑΔΕΙΓΜΑΤΑ

Byte string	Base-32 encoding
{}	""
{0x88}	"84"
{0x9f,0x0b}	"zw20"
{0x17,0xa3,0xd4}	"rs89f"
{0x2a,0xa9,0x13,0x7e}	"b9b71z1"
{0x7e,0x69,0xa3,0xef,0xac}	"ycu6urmp"
{0xe5,0x3b,0x60,0xe8,0x15,0x62}	"5zg06nr223"
{0x72,0x3c,0xef,0x3a,0x43,0x2c,0x8f}	"l3hygxd8dt31"
{0x17,0xf7,0x35,0x09,0x41,0xe4,0xdc,0x01}	"rsxcm44847r30"

6.2.3 ΚΩΔΙΚΟΠΟΙΗΣΗ ΤΩΝ ΔΗΜΟΣΙΩΝ ΚΛΕΙΔΙΩΝ ΣΕ ΟΝΟΜΑΤΑ ΕΞΥΠΗΡΕΤΗΤΩΝ ΟΝΟΜΑΤΩΝ

Τα δημόσια κλειδιά DNSCurve κωδικοποιούνται στα ονόματα των εξυπηρετητών ονομάτων ως μία ετικέτα των 54 byte που αποτελείται από τη σειρά "uz5", ακολουθούμενη από τα πρώτο 51 bytes της κωδικοποίησης των 32 bit του δημόσιου κλειδιού. (Τα δημόσια

κλειδιά Curve25519 είναι στην πραγματικότητα ακέραιοι των 255 bit σε little-endian, έτσι ώστε το 52ο byte της κωδικοποίησης των 32 bit να είναι πάντα "0".)

Όταν ένας πελάτης DNSCurve ψάχνει το όνομα του εξυπηρετητή ονομάτων για ένα DNSCurve δημόσιο κλειδί, πρέπει να ελέγξει κάθε ετικέτα για ένα κωδικοποιημένο δημόσιο κλειδί. Εάν βρεθούν πολλαπλά δημόσια κλειδιά, πρέπει να επιλεχθεί η πιο αριστερή ετικέτα. Η σύγκριση της σειράς με τη σειρά "uz5" πρέπει να πραγματοποιείται χωρίς να λαμβάνονται υπόψη κεφαλαίοι και πεζοί χαρακτήρες.

6.2.4 ΔΗΜΙΟΥΡΓΙΑ ΤΟΥ NONCE

Για κάθε αίτημα, οι DNSCurve πελάτες δημιουργούν ένα nonce των 96 bit, και για κάθε απάντηση, οι DNSCurve εξυπηρετητές δημιουργούν μία επέκταση των 96 bit του nonce. Τα nonces πρέπει να είναι μοναδικά για ξεχωριστά πακέτα για το ίδιο ζεύγος κλειδιών πελάτη/εξυπηρετητή. Ένας απλός τρόπος για να επιτευχθεί αυτό είναι να επιλεγεί ένα μοναδικό nonce για κάθε πακέτο και για κάθε αναμετάδοση. Επιπλέον, οι εξυπηρετητές πρέπει να χρησιμοποιούν μια μη μηδενική επέκταση nonce (επειδή τα nonces είναι μηδενικά-εκτεταμένα στα πακέτα ερωτημάτων). Ωστόσο, με την επιφύλαξη των περιορισμών αυτών, πελάτες και εξυπηρετητές ενδέχεται να δημιουργήσουν nonces που όμως επιλέγουν.

Δύο συνιστώμενοι τρόποι για να δημιουργήσουν ένα nonce των 96 bit ή μία επέκταση nonce και είναι οι ακόλουθοι:

- ένας μετρητής των 64 bit (ξεκινώντας από το 1), ακολουθούμενος από έναν τυχαίο αριθμό των 32 bit και
- ένα χρονικό σημείο των 96 bit (π.χ., νανοδευτερόλεπτα από το 1970) που ακολουθείται από έναν τυχαίο αριθμό των 32 bit.

Σε κάθε περίπτωση η τιμή των 64 bit δεν πρέπει να μειωθεί ακόμη και αν η επανεκκίνηση του λογισμικού ή το ρολόι του συστήματος κάνει άλματα προς τα πίσω.

Εάν πολλαπλοί πελάτες ή πολλαπλοί εξυπηρετητές μοιράζονται ένα ιδιωτικό κλειδί DNSCurve, τότε θα πρέπει να βεβαιωθείτε ότι δεν υπάρχουν δύο ξεχωριστοί πελάτες ή εξυπηρετητές που παράγουν το ίδιο nonce. Ένας απλός τρόπος για να επιτευχθεί αυτό είναι να χρησιμοποιηθεί ο διαχωρισμός nonce: Για παράδειγμα, εάν δύο εξυπηρετητές μοιράζονται ένα ζεύγος κλειδιών DNSCurve, ένας εξυπηρετητής θα μπορούσε να χρησιμοποιήσει μόνο ζυγά nonces και το άλλο θα μπορούσε να χρησιμοποιήσει μόνο περιττά nonces.

6.2.5 ΔΙΕΥΡΥΜΕΝΕΣ ΜΟΡΦΕΣ DNSCURVE

Η DNSCurve ορίζει δύο διευρυμένες μορφές: την «εξορθολογισμένη» [4] και την "TXT"[4]. Κάθε μία περιλαμβάνει μία μορφή για εκτεταμένα ερωτήματα και μια μορφή για εκτεταμένες αποκρίσεις. Οι DNSCurve πελάτες μπορούν να στείλουν εκτεταμένα ερωτήματα χρησιμοποιώντας οποιαδήποτε μορφή της επιλογής τους, αλλά ενθαρρύνονται να χρησιμοποιούν το εξορθολογισμένη/απλοποιημένη μορφή όπου αυτό είναι δυνατό. Ένας DNSCurve εξυπηρετητής πρέπει να υποστηρίζει τα DNSCurve εκτεταμένα ερωτήματα κάθε μορφής και πρέπει να στείλει εκτεταμένες αποκρίσεις χρησιμοποιώντας την αντίστοιχη μορφή.

6.2.5.1 «ΕΞΟΡΘΟΛΟΓΙΣΜΕΝΗ» ΜΟΡΦΗ

Ένα εκτεταμένο πακέτο ερωτήματος στην εξορθολογισμένη μορφή έχει τα ακόλουθα bytes:

- 8 bytes: τη συμβολοσειρά "Q6fnvWj8".
- 32 bytes: το DNSCurve δημόσιο κλειδί του πελάτη.
- 12 bytes: ένα nonce που έχει επιλέξει ο πελάτης για αυτό το πακέτο.
- Ένα «κρυπτογραφικό κουτί» που περιέχει το αρχικό πακέτο ερωτήματος DNS.

Ένα εκτεταμένο πακέτο απόκρισης στην εξορθολογισμένη μορφή μα έχει τα ακόλουθα bytes:

- 8 bytes: τη συμβολοσειρά "R6fnvWJ8".
- 12 bytes: τη nonce του πελάτη.
- 12 bytes: μία επέκταση nonce που έχει επιλέξει ο εξυπηρετητής
- Ένα «κρυπτογραφικό κουτί» που περιέχει το αρχικό πακέτο απόκρισης.

Να σημειωθεί ότι αυτή η εξορθολογισμένη μορφή απόκρισης δεν επαναλαμβάνει το όνομα του ερωτήματος του πελάτη, και ιδίως δεν επαναλαμβάνει το δημόσιο κλειδί του πελάτη. Ωστόσο, επαναλαμβάνει το nonce του πελάτη.

6.2.5.2 ΜΟΡΦΗ «TXT»

Η "TXT" μορφή λαμβάνει το όνομά της από το γεγονός ότι το εκτεταμένο ερώτημα και τα πακέτα απόκρισης σε αυτήν τη μορφή φαίνονται στον περιστασιακό έλεγχο να είναι πρότυπα πακέτα DNS με δύο δυνατές εξαιρέσεις: 1) το όνομα του ερωτήματος ίσως υπερβαίνει τα 255 byte και 2) το συνολικό πακέτο ίσως υπερβαίνει τα 512 bytes.

Κατά την κωδικοποίηση ενός εκτεταμένου πακέτου ερωτήματος σε μορφή TXT, ένας DNSCurve πελάτης πρέπει να δημιουργήσει ένα τυπικό πακέτο ερωτήματος DNS με τα bits AA, TC, RD, RA, Z, και RCODE κενά, μία ενιαία καταχώρηση στο τμήμα ερώτησης, και με καμία εγγραφή στην απάντηση, μία αρχή ή πρόσθετα τμήματα εγγραφών. Το ένα ερώτημα πρέπει να ζητήσει εγγραφές κατηγορίας Internet TXT για το όνομα του ερωτήματος το οποίο κατασκευάζεται από την αλληλουχία των εξής ετικετών:

- Μία ή περισσότερες ετικέτες, κάθε ετικέτα εκτός από την τελευταία να είναι ακριβώς 50 bytes, με την τελευταία ετικέτα να έχει μέγεθος το πολύ 50 bytes. Η αλληλουχία αυτών των ετικετών είναι η κωδικοποίηση των 32 bit ενός nonce των 96 bit που έχει επιλεγεί από τον πελάτη για αυτό το πακέτο ακολουθημένο από ένα «κρυπτογραφικό κουτί» που περιέχει το αρχικό πακέτο ερωτήματος DNS.
- Μία ετικέτα των 54 bit: το DNSCurve δημόσιο κλειδί του πελάτη, κωδικοποιημένο όπως περιγράφηκε στην παράγραφο 4, με εξαίρεση τη συμβολοσειρά "x1a" αντί για την "uz5".
- Μηδέν ή περισσότερες πρόσθετες ετικέτες που προσδιορίζουν το όνομα της ζώνης που εξυπηρετείται από αυτόν το εξυπηρετητή: Δηλαδή, το όνομα του κατόχου της σχετικής εγγραφής NS.

Ένας DNSCurve εξυπηρετητής πρέπει να είναι επιεικής όσον αφορά την αποκρυπτογράφηση των εκτεταμένων πακέτων ερωτημάτων σε μορφή TXT. Ειδικότερα, πρέπει να επιτρέπει στο bit RD είτε να τεθεί είτε να καταργηθεί, να επιτρέπει τις εγγραφές στην απάντηση, τις εγγραφές της αρχής, και επιπλέον τμήματα εγγραφών, και να επιτρέπει όλες τις ετικέτες για να ακολουθήσουν το DNSCurve δημόσιο κλειδί στο όνομα ερωτήματος. Ωστόσο, πρέπει να απορρίψει τα πακέτα με τιθέμενο το QR bit.

Κατά την κωδικοποίηση ενός εκτεταμένου πακέτου απόκρισης σε μορφή TXT, ένας DNSCurve εξυπηρετητής πρέπει να δημιουργήσει ένα τυπικό πακέτο απόκρισης DNS αντιγράφοντας το ID, το RD bit, και το τμήμα των ερωτήσεων από το εκτεταμένο πακέτο ερωτήματος, θέτοντας το AA bit, αφήνοντας τα bit TC και RA κενά και τις τιμές Z και RCODE στο 0, συμπεριλαμβάνοντας μία εγγραφή στο τμήμα απάντησης, και καθόλου εγγραφές της αρχή διαπιστώνει ή επιπρόσθετα τμήματα εγγραφών. Η εγγραφή στο τμήμα της απάντησης πρέπει να είναι μια TXT εγγραφή κατηγορίας Internet για το όνομα του ερωτήματος από το τμήμα των ερωτήσεων με χρόνο ισχύος 0. Τα RDATA αυτής της εγγραφής είναι η επέκταση nonce των 96 bit που έχει επιλεγεί από τον εξυπηρετητή ακολουθούμενη από ένα «κρυπτογραφικό κουτί» που περιέχει το αρχικό πακέτο απόκρισης, κωδικοποιημένο ως μια ακολουθία από μία ή περισσότερες συμβολοσειρές το πολύ 255 bytes στην τυπική μορφή DNS TXT RDATA.

Ομοίως, ένας DNSCurve πελάτης θα πρέπει να είναι επιεικής όσον αφορά την αποκρυπτογράφηση των εκτεταμένων πακέτων απόκρισης στην TXT μορφή. Ειδικότερα, πρέπει να επιτρέπει στον εξυπηρετητή να αλλάζει την περίπτωση του ονόματος του ερωτήματος όταν επαναλαμβάνεται στο τμήμα ερωτήσεων.

6.2.6 UDP ΚΑΙ TCP

Εάν ένα κανονικό πακέτο απόκρισης είναι μεγαλύτερο από 512 bytes τότε ο εξυπηρετητής το αντικαθιστά από ένα ρητά κατατετμημένο πακέτο. Ο πελάτης μετά προσπαθεί πάλι μέσω TCP. Οι εξυπηρετητές δεν απαιτούνται για την υποστήριξη του TCP αν δεν υπάρχουν αποκρίσεις μεγαλύτερες από 512 bytes: οι πελάτες έχουν το δικαίωμα να προσπαθούν το TCP μόνο αν ο εξυπηρετητής έχει δηλώσει ρητά κατάτμηση.

Η DNSCurve δεν απαιτεί την υποστήριξη του TCP από τους εξυπηρετητές που δεν υποστηρίζουν ήδη το TCP. Αν το αρχικό πακέτο απόκρισης είναι το πολύ 512 bytes τότε ο εξυπηρετητής επιτρέπεται να στείλει το διευρυμένο πακέτο απόκρισης ως ένα πακέτο UDP. Οι DNSCurve πελάτες υποχρεούνται να παραμερίσουν έναν 4096-μπιρο απομονωτή για τη λήψη ενός πακέτου απόκρισης UDP.

Αν το αρχικό πακέτο απόκρισης είναι μεγαλύτερο από 512 bytes, τότε αντικαθίσταται από ένα ρητά κατατετμημένο πακέτο και το κατατετμημένο πακέτο προστατεύεται από την DNSCurve. Σε αυτή την περίπτωση ο πελάτης προσπαθεί ξανά μέσω του TCP, στέλνοντας το δικό του DNSCurve πακέτο ερωτήματος του μέσω του TCP και την λαμβάνοντας την DNSCurve απάντηση μέσω TCP.

Το TCP είναι αρκετά πιο δαπανηρό για τους πελάτες και τους εξυπηρετητές από ότι το UDP, και το TCP δεν έχει καμία προστασία από την άρνηση υπηρεσίας, έτσι οι διαχειριστές των εξυπηρετητών συμβουλεύονται να παραμείνουν κάτω από το μέγεθος των 512 bytes αν αυτό είναι δυνατόν. Η DNSCurve προσθέτει κάποια προστασία για την άρνηση της υπηρεσίας για το UDP, αλλά δεν μπορεί να κάνει τίποτα για να βοηθήσει το πρωτόκολλο TCP.

Εάν το προστατευόμενο ερώτημα DNS περιλαμβάνει μια EDNS0 OPT εγγραφή, τότε το πεδίο μεγέθους αναφέρεται στο πόσο μεγάλο μπορεί να είναι το αρχικό πακέτο απόκρισης πριν την κωδικοποίηση ως ένα DNSCurve εκτεταμένο πακέτο απόκρισης. Οι πελάτες πρέπει να μειώσουν το μέγεθος που εξαγγέλλουν για να υπολογίσουν για την επιβάρυνση από την κωδικοποίηση της απάντησης από ένα διευρυμένο πακέτο απόκρισης. Εάν ένας εξυπηρετητής δημιουργεί μια απόκριση εντός του ορίου μεγέθους, αλλά στη συνέχεια δεν μπορεί να χωρέσει την κωδικοποιημένη απόκριση σε 4096 bytes, τότε μπορεί να απορρίψει «εχέμυθα» την απάντηση.

Ακόμα και όταν πραγματοποιούνται οι DNSCurve διεξαγωγές στο UDP, μπορεί να εξακολουθούν να είναι ευάλωτες σε επιθέσεις άρνησης της υπηρεσίας των λόγω πλαστογραφημένων τμημάτων IP εάν τα πακέτα απόκρισης είναι αρκετά μεγάλα ώστε να απαιτείται IP κατακερματισμός. Ως εκ τούτου, οι εξυπηρετητές πρέπει να προσπαθήσετε να κρατήσουν τα πακέτα εντός των ορίων του μονοπατιού MTU.

6.2.7 ΘΕΩΡΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Η DNSCurve μόνο παρέχει ασφάλεια σύνδεσης-επιπέδου μεταξύ ενός ζεύγους πελάτη/εξυπηρετητή. Δεν προσπαθεί να εξασφαλίσει ασφάλεια σε όλο το εύρος για τα ερωτήματα και τις απαντήσεις που αναμεταδίδονται από μη αξιόπιστες DNS εξουσιοδοτήσεις και προσωρινές μνήμες.

Οι DNSCurve πελάτες είναι ελεύθεροι να επιλέξουν εάν θα χρησιμοποιήσουν ή όχι τη DNSCurve για κάθε περίπτωση ερωτήματος ξεχωριστά Για παράδειγμα, ένας πελάτης μπορεί να αποφασίσει την επαναφορά στο πρότυπο DNS μετά από μερικά αποτυχημένα DNSCurve ερωτήματα. Φυσικά, η DNSCurve δεν μπορεί να προβεί σε καμία εγγύηση ασφάλειας για τις διεξαγωγές που δεν χρησιμοποιούν DNSCurve, έτσι οι πελάτες ενθαρρύνονται να χρησιμοποιούν DNSCurve αν αυτό είναι δυνατόν.

Η DNSCurve προσθέτει κάποια αξιοπιστία με την κρυπτογράφηση των περιεχομένων του DNS πακέτου, αλλά δεν προσπαθεί να κρύψει το μήκος του αρχικού πακέτου DNS ούτε την προέλευση ή τον προορισμό αυτού. Επιπλέον, η μορφή TXT απαιτεί από τους πελάτες να αποκαλύψουν τη ζώνη για την οποία ρωτούν.

ΚΕΦΑΛΑΙΟ 7. ΕΠΙΛΟΓΟΣ

Το Σύστημα Ονοματοδοσίας των Διευθύνσεων επικυρώθηκε ως πρότυπο του Διαδικτύου για την μετατροπή των ονομάτων των διευθύνσεων σε διευθύνσεις IP. Από τότε, η διαδεδομένη χρήση του DNS και η ικανότητά του να αναλύσει τα ονόματα κεντρικών υπολογιστών σε διευθύνσεις IP για τους χρήστες και τις εφαρμογές έγκαιρα και με αρκετά αξιόπιστο τρόπο, το κάνει να είναι ένα σημαντικό συστατικό του Διαδικτύου. Η κατανεμημένη διαχείριση του DNS και η υποστήριξη για πλεονασμό των ζωνών DNS σε πολλούς εξυπηρετητές προωθεί τα ισχυρά χαρακτηριστικά του. Ωστόσο, οι αρχικές προδιαγραφές του πρωτοκόλλου DNS δεν περιλαμβάνουν την ασφάλεια. Χωρίς ασφάλεια, το DNS είναι ευάλωτο σε επιθέσεις που απορρέουν από τις τεχνικές «δηλητηρίασης» της προσωρινής μνήμης, τις υπερχειλίσεις των πελατών, τις δυναμικές ενημερώσεις των τρωτών σημείων, τη διαρροή των πληροφοριών, και της έκθεσης των έγκυρων αρχείων των εξυπηρετητών του.

Για να προστεθεί ασφάλεια στο DNS και να αντιμετωπιστούν αυτές οι απειλές, ο IETF πρόσθεσε επεκτάσεις ασφαλείας στο DNS, γνωστές ως DNSSEC. Η DNSSEC παρέχει έλεγχο ταυτότητας και ακεραιότητα στο DNS. Με εξαίρεση τη διαρροή των πληροφοριών, αυτές οι επεκτάσεις βελτιώνουν την πλειονότητα των προβλημάτων που κάνουν τέτοιες επιθέσεις να είναι δυνατόν να συμβούν. Η «δηλητηρίαση» της προσωρινής μνήμης και οι επιθέσεις υπερχείλισης πελατών μετριάζονται με την προσθήκη της ταυτότητας της προέλευσης των δεδομένων για τα σύνολα εγγραφών πόρων. Οι δυναμικές ενημερώσεις των τρωτών σημείων μετριάζονται με την προσθήκη των διεξαγωγών της DNSSEC και των αιτημάτων αυθεντικοποίησης, παρέχοντας την αναγκαία εξασφάλιση στους εξυπηρετητές DNS ότι η ενημέρωση είναι αυθεντική.

Επιπλέον, διάφορα πρωτόκολλα προτείνουν νέες εγγραφές πόρων, όπως η HASTLS RR, η TLSA RR και η CAA RR, για να επιτευχθεί ακόμη μεγαλύτερη ασφάλεια συνδυάζοντας τα ονόματα διευθύνσεων με τα πιστοποιητικά. Η ασφάλεια των πρωτοκόλλων που προτείνουν τις εγγραφές αυτές στηρίζεται στην DNSSEC όπως χρησιμοποιείται από τον πελάτη που ζητά τις εγγραφές πόρων.

Τέλος, προτείνεται η DNSCURVE, η οποία αποτελεί μια εναλλακτική λύση έναντι του DNS και της DNSSEC. Η DNSCURVE χρησιμοποιεί κρυπτογραφικούς αλγόριθμους για την ανταλλαγή μηνυμάτων μεταξύ πελατών και εξυπηρετητών, προσθέτοντας κάποια αξιοπιστία με την κρυπτογράφηση των περιεχομένων ενός πακέτου DNS και κάνοντας την διαρροή των πληροφοριών πιο δύσκολο να επιτευχθεί.

ΚΕΦΑΛΑΙΟ 8. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] P. Hoffman, (2011) “Specifying That a Server Supports TLS”

[2] Hoffman & Schlyter (2011) “USing Secure DNS to Associate Certificates with Domain Names For TLS”

[3] P. Hallam-Baker, R. Stradling & B. Laurie, (2011), “DNS Certification Authority Authorization (CAA) Resource Record”

[4] M. Dempsky, (2010), “DNSCurve”: Link-Level Security for the Domain Name System”

[5] R. Arends, (2005), “DNS Security Introduction and Requirements”

[6] R. Arends, (2005), “Resource Records for the DNS Security Extensions”

[7] R. Arends, (2005), “Protocol Modifications for the DNS Security Extensions”

[8] Luis Grangeia (2004), DNS Cache Snooping

[9] Men & Mice, (1999) "What is DNS Spoofing"

[10] D. Eastlake, (1999), “Domain Name System Security Extensions”

[11] “How DNS Works” 2003, http://technet.microsoft.com

[12] http://en.wikipedia.org