Συγκριτική αξιολόγηση της απόδοσης και των χαρακτηριστικών ασφάλειας των πρωτοκόλλων AAA, RADIUS & Diameter

---

Η Διπλωματική Εργασία
παρουσιάστηκε ενώπιον
του Διδακτικού Προσωπικού του
Πανεπιστημίου Αιγαίου

Σε Μερική Εκπλήρωση
των Απαιτήσεων για το Δίπλωμα του
Μηχανικού Πληροφοριακών και Επικοινωνιακών Συστημάτων

του
Κολλαρά Αντώνιου
ΧΕΙΜΕΡΙΝΟ ΕΞΑΜΗΝΟ 2007-2008

Η ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΔΙΔΑΣΚΟΝΤΩΝ ΕΠΙΚΥΡΩΝΕΙ ΤΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ ΤΟΥ Κολλαρά Αντώνιου:

Ημερομηνία 15/02/2008

Καμπουράκης Γεώργιος, Επιβλέπων
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Γκρίτζαλης Στέφανος, Μέλος
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Λαμπρινουδάκης Κωνσταντίνος, Μέλος
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΧΕΙΜΕΡΙΝΟ ΕΞΑΜΗΝΟ 2008

ΠΕΡΙΛΗΨΗ

Η ανάγκη χρήσης υπηρεσιών αυθεντικοποίησης, εξουσιοδότησης και λογιστικής καταγραφής στις σημερινές εφαρμογές και υπηρεσίες είναι δεδομένη. Το πρωτόκολλο RADIUS δημιουργήθηκε για την κάλυψη της ανάγκης αυθεντικοποίησης απομακρυσμένων χρηστών αλλά σύντομα επέκτεινε τη λειτουργικότητα του με τις υπηρεσίες εξουσιοδότησης και λογιστικής καταγραφής, προσφέροντας ένα ολοκληρωμένο πλαίσιο Authentication, Authorization, Accounting (AAA). Η σημερινή μορφή του RADIUS είναι αποτέλεσμα ενός συνονθυλεύματος προτύπων, το καθένα από τα οποία προσθέτει ένα κομμάτι λειτουργικότητας στο πρωτόκολλο, καθιστώντας το σύγχρονο στις τρέχουσες απαιτήσεις. Ωστόσο, το RADIUS δεν δομήθηκε πάνω σε ένα συγκεκριμένο πλαίσιο ΑΑΑ, αλλά μορφοποιήθηκε σταδιακά εξελισσόμενο από τις ανάγκες της εποχής. Το γεγονός αυτό αποτελεί τροχοπέδη στις περαιτέρω δυνατότητες εξέλιξης του. Σήμερα, προκειμένου να εφαρμοστεί αποδοτικά, και με ασφάλεια στην πληρότητα της μια υλοποίηση του RADIUS, απαιτείται να υποστηρίζει πληθώρα προτύπων και προδιαγραφών που καθορίζονται σε διαφορετικά RFC.

Το Diameter, το νεότερο πρωτόκολλο ΑΑΑ, παρουσιάζεται ως το διάδοχο πρωτόκολλο του RADIUS που αναμένεται να επικρατήσει τα επόμενα χρόνια. Το Diameter δομήθηκε στη βάση συγκεκριμένων απαιτήσεων που θα έπρεπε να πληρεί ένα σύγχρονο πρωτόκολλο ΑΑΑ. Επιπλέον, μοιάζει σε αρκετά δομικά χαρακτηριστικά του RADIUS και ενσωματώνει μηχανισμούς που επιτρέπουν την ευκολότερη μετάβαση σε αυτό. Το Diameter φιλοδοξεί να επιλύσει τα προβλήματα του προκατόχου του, αλλά παράλληλα να προσφέρει τα ίδια επίπεδα ευχρηστίας και αποδοτικότητας που διέκριναν το RADIUS.

Στην εργασία αυτή συγκρίνουμε κι αξιολογούμε δυο πρωτόκολλα ΑΑΑ, του RADIUS και του Diameter. Η σύγκριση πραγματοποιείται υπό το πρίσμα της ευχρηστίας υλοποίησης των πρωτοκόλλων, της επεκτασιμότητας αυτών, της αξιοπιστίας μετάδοσης των μηνυμάτων και της εγγενούς ασφάλειας που προσφέρουν. Επίσης, αναλύονται ζητήματα σχετικά με τις διαχειριστικές ικανότητες των πρωτοκόλλων σε περιβάλλοντα με μεγάλο αριθμό συμμετεχόντων υπολογιστικών συστημάτων (scalability), αλλά και τις δυνατότητες συμβατότητας που προσφέρουν.

Κολλαρά Αντώνιου

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ABSTRACT

Today, the necessity of Authentication, Authorization and Accounting services in applications and services is considered a fact. RADIUS protocol was created to cover the need of authenticating remote users, but soon enough it expanded its functionality to become the first Authentication, Authorization, and Accounting (AAA) protocol. Today, RADIUS is an intermixture of multiple standards, where each one of these adds a piece to the overall functionality of the protocol. RADIUS was not built upon a specific AAA framework, but it was gradually created through time, adapting to the current trends. But this was to be, RADIUS's main obstacle to evolution. Today, RADIUS implementations are dictated by a numerous of different standards and specifications in order to be fully functional, and secure enough.

Diameter, aspires to become the major AAA protocol of the next generation. Its creation was based on specific requirements of an ideal, modern AAA protocol. In addition, it has similar structural units with RADIUS and integrates functions to moderate the transition effects from one protocol to the other. Diameter's objective is to address RADIUS's deficiencies while providing the same level of usability and efficiency.

In this thesis we compare and evaluate two AAA protocols; RADIUS and Diameter. The comparison is performed in aspects of usability, expandability of protocols, reliability of transport mechanisms and by the inherent security provisions they provide. Moreover, scalability and compatibility issues are subject of discussion in this thesis.

Kollaras Antonios

Department of Information and Communication Systems Engineering

UNIVERSITY OF THE AEGEAN

ΕΥΧΑΡΙΣΤΙΕΣ

Ευχαριστώ τον επιβλέποντα της εργασίας, κ. Καμπουράκη Γεώργιο για την πολύτιμη βοήθεια του στην περάτωση αυτής, καθώς και τη μεταπτυχιακή φοιτήτρια του τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Κωνσταντινίδου Ελευθερία για τις παρατηρήσεις της.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ

1 Εισαγωγή

Το 1985 το Εθνικό Ίδρυμα Επιστημών (National Science Foundation) των Η.Π.Α. χρηματοδότησε τη δημιουργία ερευνητικών τμημάτων σε 5 πανεπιστήμια της χώρας, εξοπλισμένα με υπέρ-υπολογιστές. Προκειμένου να επιτευχθεί η διασύνδεση αυτών των υπολογιστικών μηχανών δημιουργήθηκε το NSFNet [23] βασιζόμενο στη δικτυακή σουίτα πρωτοκόλλων TCP/IP (όπως το στρατιωτικό δίκτυο ARPANET [20]), με σκοπό να αποτελέσει τη ραχοκοκαλιά του δικτύου των Ακαδημαϊκών ιδρυμάτων των Η.Π.Α.. Το δίκτυο ξεκίνησε τη λειτουργία του το 1986, ενώ το 1987 μετά από σχετικό διαγωνισμό, ανέλαβε τη διαχείρισή του η εταιρεία Merit.

Ένα από τα πρώτα προβλήματα που αντιμετώπισε η εταιρεία ήταν η αλλαγή των dial-in εξυπηρετητών που χρησιμοποιούσε αφού ήταν σχεδιασμένοι να λειτουργούν στο ιδιόκτητο πρωτόκολλο επικοινωνίας της εταιρείας, κι όχι επάνω από τη σουίτα πρωτοκόλλων TCP/IP. Μία βασική απαίτηση που θα έπρεπε να κληρονομηθεί στο TCP/IP ήταν αυτή της κατανεμημένης dial-in πρόσβασης που παρείχε ήδη η εταιρεία στο δικό της δίκτυο. Κάθε απομακρυσμένος χρήστης (remote user) θα έπρεπε να μπορεί να έχει πρόσβαση στο NSFNet κάνοντας κλήση μέσω του τηλεφωνικού δικτύου. Για να συμβεί αυτό χρειαζόταν ένα νέο πρωτόκολλο που θα επέτρεπε την απομακρυσμένη αυθεντικοποίηση των χρηστών.

Για να βρεθεί λύση στο πρόβλημα, συντάχθηκε και δημοσιεύτηκε ένα έγγραφο Request For Instructions (RFI) βάσει των σχεδιαστικών απαιτήσεων του νέου πρωτοκόλλου. Χρειάστηκαν να περάσουν αρκετοί μήνες έως ότου η εταιρεία Livingstone παρουσιάσει τη δική της πρόταση. Ουσιαστικά λοιπόν, εκείνη ήταν η στιγμή της δημιουργίας του RADIUS πρωτοκόλλου, που ήταν το πρώτο ιστορικά πρωτόκολλο που χρησιμοποιήθηκε για παροχή υπηρεσιών αυθεντικοποίησης, εξουσιοδότησης και λογιστικής καταγραφής (Authentication, Authorization, Accounting - AAA).

Από την εποχή εκείνη έως σήμερα μεσολάβησαν γεγονότα όπως, η ραγδαία ανάπτυξη του Διαδικτύου με τους ολοένα και ταχύτερους κεντρικούς διαύλους επικοινωνίας, η μετάβαση από τις dial-up συνδέσεις στις ευρυζωνικές (DSL), η επικράτηση της GMS κινητής τηλεφωνίας. Η επανάσταση της ασύρματης επικοινωνίας μικρών και μεσαίων αποστάσεων (π.χ. το πρότυπο IEEE 802.11), και η σύγκλιση των υπηρεσιών φωνής και δεδομένων.

Κοινός παρονομαστής σε όλες αυτές τις υπηρεσίες που απευθύνονται μαζικά στους χρήστες τους είναι το πλαίσιο Authentication Authorization Accounting (AAA). Το πλαίσιο AAA απάντα σε τρεις απλές μα θεμελιώδεις για τη ζωτικότητα μιας υπηρεσίας ερωτήσεις:

- Ποιος είσαι; (Αυθεντικοποίηση)
- Τι επιτρέπεται να κάνεις; (Εξουσιοδότηση)

- Τι έκανες (Λογιστική καταγραφή)

Σήμερα το πλαίσιο ΑΑΑ αποτελεί βασικό δομικό στοιχείο της αρχιτεκτονικής ενός συστήματος ή μιας υπηρεσίας, σε βαθμό που οι υπηρεσίες που το χρησιμοποιούν να είναι απολύτως εξαρτώμενες από αυτό, προκείμενου να συνεχίσουν να λειτουργούν. Αν αναλογιστούμε την ύπαρξη ενός σύγχρονου λειτουργικού συστήματος που δεν εφαρμόζει με συνέπεια το πλαίσιο ΑΑΑ προκύπτουν τα ακόλουθα ερωτήματα: (α) Ποιος χρήστης θα μπορεί να κάνει τι; (β) Ποιος είναι ο τρέχων συνδεδεμένος; (γ) Πώς θα εφαρμοστεί ο έλεγχος πρόσβασης στους χρήστες και τις εφαρμογές του λειτουργικού συστήματος; (δ) Οι dial-up και ευρυζωνικές συνδέσεις, οι υπηρεσίες κινητής τηλεφωνίας, η ηλεκτρονική διακυβέρνηση, τα συστήματα αποθήκευσης βάσεων δεδομένων κ.α. δεν θα μπορούσαν να υπάρξουν δίχως την εφαρμογή ενός πλαισίου ΑΑΑ στη λειτουργία τους.

Στην εργασία αυτή συγκρίνονται και αξιολογούνται δυο από τα πλέον δημοφιλή πρωτόκολλα ΑΑΑ, το RADIUS [1, 25, 37-39] με τη μεγαλύτερη εγκατεστημένη βάση συστημάτων, και το Diameter [6-9, 13, 21] που φιλοδοξεί να είναι το πρωτόκολλο ΑΑΑ που θα αντικαταστήσει το πρώτο. Στο κεφάλαιο 2 γίνεται ανάλυση των βασικών εννοιών που συνιστά ένα πρωτόκολλο ΑΑΑ, δηλαδή τις υπηρεσίες αυθεντικοποίησης, εξουσιοδότησης και λογιστικής καταγραφής. Στα κεφάλαια 3 και 4 γίνεται μία αναλυτική παρουσίαση των δυο πρωτοκόλλων. Τέλος, στο κεφάλαιο 5, που αποτελεί το κυριότερο τμήμα της εργασίας, γίνεται μία θεωρητική αξιολόγηση και σύγκριση των πρωτοκόλλων σχετικά την παρεχομένη ασφάλεια, την ευελιξία στην ενσωμάτωση νέων τεχνολογιών και υπηρεσιών καθώς και στην ευκολία υλοποίησης αυτών.

2 Η τριπλέτα υπηρεσιών Authentication, Authorization, Accounting

2.1 Αυθεντικοποίηση

Στην ασφάλεια πληροφοριακών και επικοινωνιακών συστημάτων, ο όρος *αυθεντικοποίηση* σημαίνει η διαδικασία επιβεβαίωσης της ταυτότητας ενός χρήστη, διεργασίας ή κάποιου άλλου ενεργού υπολογιστικού συστήματος. Στα παρακάτω θεωρούμε ότι η οντότητα που αιτείται αυθεντικοποίησης είναι ένας τυπικός χρήστης.

Η αυθεντικοποίηση αποτελείται από δύο επιμέρους λειτουργίες. Στην πρώτη από αυτές πραγματοποιείται η επίδειξη της επικαλούμενης ταυτότητας του χρήστη και έπειτα ακολουθεί η επιβεβαίωσης της στην πράξη. Ο χρήστης επιδεικνύει συγκεκριμένες πληροφορίες στο άλλο άκρο που μπορεί να είναι ένας άλλος χρήστης ή πληροφοριακό σύστημα,, το οποίο διαθέτει την ικανότητα πιστοποίησης της επικαλούμενης ταυτότητας. Ο χρήστης αποστέλλει τις πληροφορίες αυθεντικοποίησης υπό μορφή αναγνώσιμη και αναγνωρίσιμη από την οντότητα με την οποία επιθυμεί να συνδιαλλαγεί. Η επιβεβαίωση της ταυτότητας του χρήστη μπορεί να πραγματοποιείται στιγμιαία, ή μπορεί να απαιτεί κάποιο χρονικό διάστημα που εξαρτάται από την αρχιτεκτονική δόμησης του συστήματος αυθεντικοποίησης, αλλά και από το απαιτούμενο επιθυμητό επίπεδο ασφάλειας.

Είναι σημαντικό να τονιστεί η ειδοποιός διαφορά μεταξύ των εννοιών *αναγνώριση (identification)* και *επιβεβαίωση (authentication)*. Η αναγνώριση του χρήστη απαιτεί συνήθως μικρό όγκο πληροφοριών, και αποτελεί πρόταση ή επιθυμία του χρήστη στη συνδιαλεγόμενη με αυτόν οντότητα. Δηλαδή, κατά την έναρξη της συναλλαγής ο χρήστης επικαλείται μία οντότητα, με την οποία θα αναγνωριστεί επιτυχώς ή όχι από τον έτερο συνδιαλεγόμενο. Προκειμένου να αναγνωριστεί επιτυχώς ο χρήστης πρέπει να επιδείξει τις κατάλληλες πληροφορίες αυθεντικοποίησης.

2.1.1 Αυθεντικοποίηση χρήστη-συσκευής

Αυθεντικοποίηση χρήστη έχουμε όταν κάποιος χρήστης επιχειρεί να συνδεθεί σε ένα υπολογιστικό σύστημα, δίκτυο, ή να προσπελάσει κάποιου είδους προστατευόμενη πληροφορία. Προκειμένου να αποδείξει την ταυτότητα που επικαλείται, ο χρήστης επιδεικνύει την πληροφορία αυθεντικοποίησης που στην πλέον εύχρηστη μορφή της σήμερα είναι ένας προσωπικός κωδικός πρόσβασης (password). Η πληροφορία αυθεντικοποίησης μαζί με το επικαλούμενο όνομα χρήστη ορίζουν τα *διαπιστευτήρια του χρήστη*. Στην αυθεντικοποίηση συσκευής, ο χρήστης εισάγει τα διαπιστευτήρια του σε μία

τερματική συσκευή, η οποία επίσης πρέπει να αυθεντικοποιηθεί προκειμένου να καταστεί δυνατή η πρόσβαση. Υπάρχει δηλαδή κι ένα δεύτερο επίπεδο αυθεντικοποίησης. Κατά αυτόν τον τρόπο, ένας εξουσιοδοτημένος χρήστης δεν μπορεί να προσπελάσει μία υπηρεσία ή κάποιους πόρους χρησιμοποιώντας μία μη αυθεντικοποιημένη συσκευή πρόσβασης.

2.1.2 Τεχνικές αυθεντικοποίησης

Ένας χρήστης μπορεί να αυθεντικοποιηθεί με πληθώρα τεχνικών. Οι βασικές κατηγορίες είναι οι εξής:

- Αυθεντικοποίηση με κάτι που γνωρίζει ο χρήστης (π.χ. μυστική πληροφορία-κωδικός πρόσβασης)
- Αυθεντικοποίηση με κάτι που κατέχει ο χρήστης (π.χ. κάρτα πρόσβασης)
- Αυθεντικοποίηση βάσει συγκεκριμένων βιομετρικών χαρακτηριστικών του χρήστη (π.χ. δακτυλικό αποτύπωμα, χροιά φωνής, μορφολογία αμφιβληστροειδούς χιτώνα)
- Αυθεντικοποίηση με συνδυασμό των παραπάνω τεχνικών

2.1.3 Αυθεντικοποίηση μηνύματος

Στην περίπτωση της αυθεντικοποίησης χρήστη, μία οντότητα διαπιστώνεται ότι είναι αυτή που ισχυρίζεται αφότου επιβεβαιωθούν επιτυχώς οι πληροφορίες αυθεντικοποίησης που παρουσίασε σε προηγούμενο στάδιο. Ωστόσο, είναι αναγκαίο να εξασφαλισθεί πως αυτές οι πληροφορίες θα μεταφερθούν στον παραλήπτη δίχως να υποστούν κάποια αλλοίωση, ενώ σε αν συμβεί κάτι τέτοιο η αλλοίωση θα πρέπει να είναι εμφανής. Με άλλα λόγια εστιάζουμε στην διαδικασία αυθεντικοποίησης μηνυμάτων. Αυτό σημαίνει ότι η επιβεβαίωση της ταυτότητας του αποστολέα αλλά και η εξασφάλιση της αρχικής μορφής και περιεχομένου του αρχικού μηνύματος, πρέπει να είναι δυνατή μέσω σχετικών διαδικασιών. Ουσιαστικά, η αυθεντικοποίηση μηνυμάτων είναι η εξασφάλιση της ακεραιότητας τους. Η αυθεντικοποίηση των μηνυμάτων, σε αντίθεση με αυτή του χρήστη, πρέπει να πραγματοποιείται σε συνεχή βάση και καθ' όλη τη διάρκεια της επικοινωνίας, εάν απαιτείται διασφάλιση της μεταδιδόμενης πληροφορίας.

2.1.4 Μονόδρομη / αμοιβαία αυθεντικοποίηση

Μονόδρομη αυθεντικοποίηση έχουμε όταν μόνο το ένα τμήμα των δύο επικοινωνούντων μερών πρέπει να αυθεντικοποιηθεί στο άλλο. Αντίθετα, αμοιβαία πιστοποίηση ταυτότητας έχουμε όταν και

τα δύο μέρη που μετέχουν στη συνομιλία, πρέπει να αλληλο-αυθεντικοποιηθούν μεταξύ τους. Προφανώς, η τελευταία περίπτωση προσφέρει αυξημένο επίπεδο ασφάλειας στο σύστημα.

2.1.5 **Μοντέλα αυθεντικοποίησης**

Πρακτικά, στα σημερινά πληροφοριακά συστήματα, η διαδικασία της αυθεντικοποίησης υλοποιείται με δύο διακριτά μοντέλα:

- Το μοντέλο πελάτη-εξυπηρετητή (client-server): Σε αυτό το μοντέλο η διαδικασία της αυθεντικοποίησης πραγματοποιείται ανάμεσα σε δύο επικοινωνούντα μέρη δίχως τη μεσολάβηση κανενός άλλου. Το μοντέλο αυτό υποστηρίζει μονόδρομη αυθεντικοποίηση του ενός μέρους στο άλλο, για παράδειγμα η αυθεντικοποίηση ενός ιστοχώρου στους χρήστες ή η αυθεντικοποίηση κάποιου χρήστη για πρόσβαση στο λογαριασμό e-mail. Επίσης, είναι δυνατή η αμοιβαία αυθεντικοποίηση και των δύο επικοινωνούντων μερών (αυθεντικοποίηση ιστοσελίδας webmail στο χρήστη, αυθεντικοποίηση χρήστη για πρόσβαση στο λογαριασμό του μέσω της ιστοσελίδας).
- Το μοντέλο 3 μερών (3 party): Το μοντέλο αυτό αναπτύχθηκε λόγω του αυξανόμενου πλήθους χρηστών σε επικοινωνιακά δίκτυα και υπηρεσίες, όπου ήταν αναγκαία η υπηρεσία της αυθεντικοποίησης των χρηστών. Υπάρχει μία αναβάθμιση ισχύος του συστήματος που πραγματοποιεί την επιβεβαίωση της ταυτότητας των χρηστών. Ο ρόλος αυτός, αποδίδεται στον *εξυπηρετητή αυθεντικοποίησης (authentication server),* ο οποίος τοποθετείται κεντρικά στο σύστημα-επικοινωνιακό δίκτυο και μπορεί να διαχειρίζεται ταυτόχρονα πολλαπλές αιτήσεις αυθεντικοποίησης από διαφορετικά επιμέρους δίκτυα. Ο εξυπηρετητής αυθεντικοποίησης δε συνδέεται άμεσα με το χρήστη-*αιτούμενο (supplicant)* πρόσβασης σε κάποια υπηρεσία / πόρους / δίκτυα κλπ. Ανάμεσα τους υπάρχει και μία τρίτη οντότητα, ο *αυθεντικοποιητής (authenticator).* Ο αυθεντικοποιητής δεν είναι αρμόδιος να καθορίσει εάν θα επιτραπεί ή όχι η πρόσβαση σε ένα αιτούμενο χρήστη. Αυτό ανήκει στη δικαιοδοσία του εξυπηρετητή αυθεντικοποίησης. Ο τελευταίος μεταβιβάζει τις αιτήσεις των χρηστών προς τον εξυπηρετητή και λαμβάνει τις αντίστοιχες αποκρίσεις που καθορίζουν τη συμπεριφορά του απέναντι στους χρήστες. Για ένα δεδομένο χρήστη ο αυθεντικοποιητής είτε επιτρέπει την πρόσβαση είτε την απορρίπτει και πάντα μετά από σχετική «εντολή» από τον εξυπηρετητή αυθεντικοποίησης.

2.1.6 Αυθεντικοποίηση πρόκλησης-απόκρισης (challenge-response)

Στην αυθεντικοποίηση πρόκλησης-απόκρισης, ο χρήστης λαμβάνει έναν τυχαίο αριθμό από τον έτερο συνομιλητή, και καλείται να τον κρυπτογραφήσει και να επιστρέψει το αποτέλεσμα της κρυπτογράφησης. Οι εξουσιοδοτημένοι χρήστες διαθέτουν το απαραίτητο λογισμικό ή/και υλισμικό προκειμένου να πραγματοποιήσουν την κρυπτογράφηση, καθώς και το μυστικό κλειδί που χρησιμοποιείται στη συνάρτηση κρυπτογράφησης. Χωρίς αυτά ένας μη-εξουσιοδοτημένος χρήστης δεν μπορεί αυθεντικοποιηθεί. Η ασφάλεια της μεθόδου βασίζεται στην ασφάλεια που παρέχει η ίδια η συνάρτηση κρυπτογράφησης αλλά και στη χρήση ενός κοινού μυστικού κωδικού μεταξύ των συνδιαλεγόμενων.

2.2 Εξουσιοδότηση

Ως *Εξουσιοδότηση* νοείται η κάθε είδους εκχώρηση προνομίων προσπέλασης υπολογιστικών πόρων και αρχείων σε ένα χρήστη, ο οποίος αιτείται σχετικά. Η εξουσιοδότηση έχει άμεση σχέση με την αυθεντικοποίηση και λογικά έπεται αυτής, αφού προκειμένου να χορηγηθεί ένα σύνολο προνομίων σε ένα χρήστη, πρέπει να προηγηθεί η αναγνώριση και επιβεβαίωση της ταυτότητας του (όχι απαραίτητα αλλά ως συνήθως). Η εκχώρηση του συνόλου προνομίων εξαρτάται από το βαθμό εξουσίας που κατέχει το υποκείμενο, ενώ κατά περίπτωση δύναται να εφαρμόζονται κι άλλοι κανόνες ή περιορισμοί που σχετίζονται με παράγοντες όπως η ώρα, τοποθεσία χρήστη, υπέρβαση του ορίου χρήσης μιας υπηρεσίας. Για παράδειγμα, ένας χρήστης-υπάλληλος μιας εταιρείας μπορεί να έχει το δικαίωμα της μεταφοράς απεριόριστου όγκου αρχείων εντός του τοπικού δικτύου της εταιρείας, αλλά ο όγκος αυτός να περιορίζεται σημαντικά για αρχεία από και προς το Διαδίκτυο. Ωστόσο, για την ίδια εταιρεία ο προϊστάμενος ενδέχεται να μην έχει κανένα περιορισμό στη μεταφορά αρχείων. Τα προνόμια που εκχωρούνται μπορεί να είναι δικαίωμα χρήσης κάποιας υπηρεσίας, εκτέλεση εφαρμογών, πρόσβασης σε συγκεκριμένα αρχεία, δικαίωμα και ποσοστό χρήσης ενός τηλεπικοινωνιακού διαύλου κ.α.

Η έννοια της εξουσιοδότησης προνομίων δημιουργήθηκε τη στιγμή της κατηγοριοποίησης των χρηστών βάσει μιας ιεραρχικής κλίμακας. Τυπική εφαρμογή διαφοροποίησης των χρηστών και αντίστοιχα των προνομίων που απολαμβάνουν από το πληροφοριακό σύστημα είναι τα πληροφοριακά συστήματα του στρατού. Σε αυτή την περίπτωση το πληροφοριακό σύστημα κληρονομεί σε μεγάλο βαθμό την ιεραρχία ρόλων που υπάρχει στην πραγματικότητα. Εάν το σύστημα δεν είχε δυνατότητα παροχής της υπηρεσίας εξουσιοδότησης, τότε ένας νεοσύλλεκτος στρατιώτης θα είχε τα ίδια δικαιώματα πρόσβασης στο πληροφοριακό σύστημα με έναν υψηλόβαθμο

αξιωματούχο. Σε εμπορικές εφαρμογές, η υλοποίηση της εξουσιοδότησης χρηστών προστατεύει την επένδυση του παρόχου μιας υπηρεσίας, και προσφέρει έλεγχο της κατανομής των πόρων στους χρήστες.

Συνήθως η εξουσιοδότηση και η αυθεντικοποίηση είναι στενά συνδεδεμένες, αφού τα διαπιστευτήρια για την αυθεντικοποίηση χρησιμοποιούνται επίσης για την εξουσιοδότηση.

Η εξουσιοδότηση γίνεται δεδομένης της επιτυχούς αυθεντικοποίησης ενός χρήστη. Ωστόσο, η τάση που επικρατεί σήμερα στους κόλπους της ομάδας εργασίας για θέματα AAA της Internet Engineering Task Force (IETF) , είναι να διαχωριστούν, όπου αυτό είναι δυνατό, τα ζητήματα της εξουσιοδότησης από αυτά της αυθεντικοποίησης. Πιο συγκεκριμένα, η ομάδα εργασίας AAA έχει δημιουργήσει μία νέα υπό-ομάδα υπεύθυνη για θέματα που αφορούν τη διαδικασία της εξουσιοδότησης αλλά και της προτυποποίησης συγκεκριμένων διαδικασιών. Με το πέρας του χρόνου, η ομάδα αυτή κατάληξε στην τελική μορφή της σήμερα ως ερευνητική ομάδα του Internet Research Task Force (IRTF) γνωστή ως η ομάδα της αρχιτεκτονικής AAA (AAA Architecture Group). Η ομάδα έχει παρουσιάσει έγγραφα-προτάσεις για το γενικότερο πλαίσιο, τις απαιτήσεις αλλά και παραδείγματα εφαρμογών σχετικά με την εξουσιοδότηση [50-51].

2.3 Λογιστική καταγραφή

Η λογιστική καταγραφή έπεται των δύο προηγούμενων διαδικασιών. *Λογιστική καταγραφή* είναι η συνεχής συλλογή πληροφοριών σχετικά με τη χρήση πόρων του συστήματος από το χρήστη με σκοπό τη χρέωση, παρακολούθηση μιας υπηρεσίας αλλά και την ανάλυση των προτιμήσεων των χρηστών.

- Χρέωση: Ανάλογα με τη χρήση των πόρων ένας χρήστης χρεώνεται για την υπηρεσία την οποία λαμβάνει. Παραδείγματος χάριν, ένας χρήστης καρτοκινητής τηλεφωνίας χρεώνεται ανά 30 δευτερόλεπτα ομιλίας και του αφαιρούνται οι αντίστοιχες μονάδες από το λογαριασμό του.
- Παρακολούθηση: Είναι αναγκαίο να παρακολουθείται συνεχώς η χρήση των υπηρεσιών για τον έλεγχο καλής χρήσης των πόρων και υπηρεσιών. Για παράδειγμα, ένας χρήστης καρτοκινητής τηλεφωνίας δεν μπορεί να συνεχίζει να πραγματοποιεί κλήσεις, εφόσον δεν έχει επάρκεια μονάδων.
- Ανάλυση προτιμήσεων: Τα στατιστικά χρήσης μιας υπηρεσίας που καταγράφονται από την υπηρεσία λογιστικής καταγραφής αποτελούν σπουδαίο εργαλείο για τους σχεδιαστές μελλοντικών υπηρεσιών σχετικά με την προσδοκώμενη χρήση μιας υπηρεσίας.

2.3.1 Μοντέλα συλλογής πληροφοριών

Για να λειτουργήσει η υπηρεσία της λογιστικής καταγραφής απαιτείται η συνεχής παρακολούθηση της χρήσης των πόρων από τους χρήστες και η συλλογή των σχετικών πληροφοριών χρέωσης. Οι πληροφορίες συλλέγονται από εξειδικευμένες για το ρόλο αυτό δικτυακές συσκευές, οι οποίες αποστέλλονται σε έναν ή και περισσότερους εξυπηρετητές της υπηρεσίας λογιστικής καταγραφής. Ο τρόπος επικοινωνίας μεταξύ αυτών των δικτυακών οντοτήτων μπορεί να διαφοροποιηθεί εφαρμόζοντας ένα από τα πολλά μοντέλα που υπάρχουν σήμερα για το σκοπό αυτό. Στην παράγραφο αυτή περιγράφονται μερικά από τα πλέον χρησιμοποιούμενα μοντέλα συλλογής πληροφοριών λογιστικής καταγραφής.

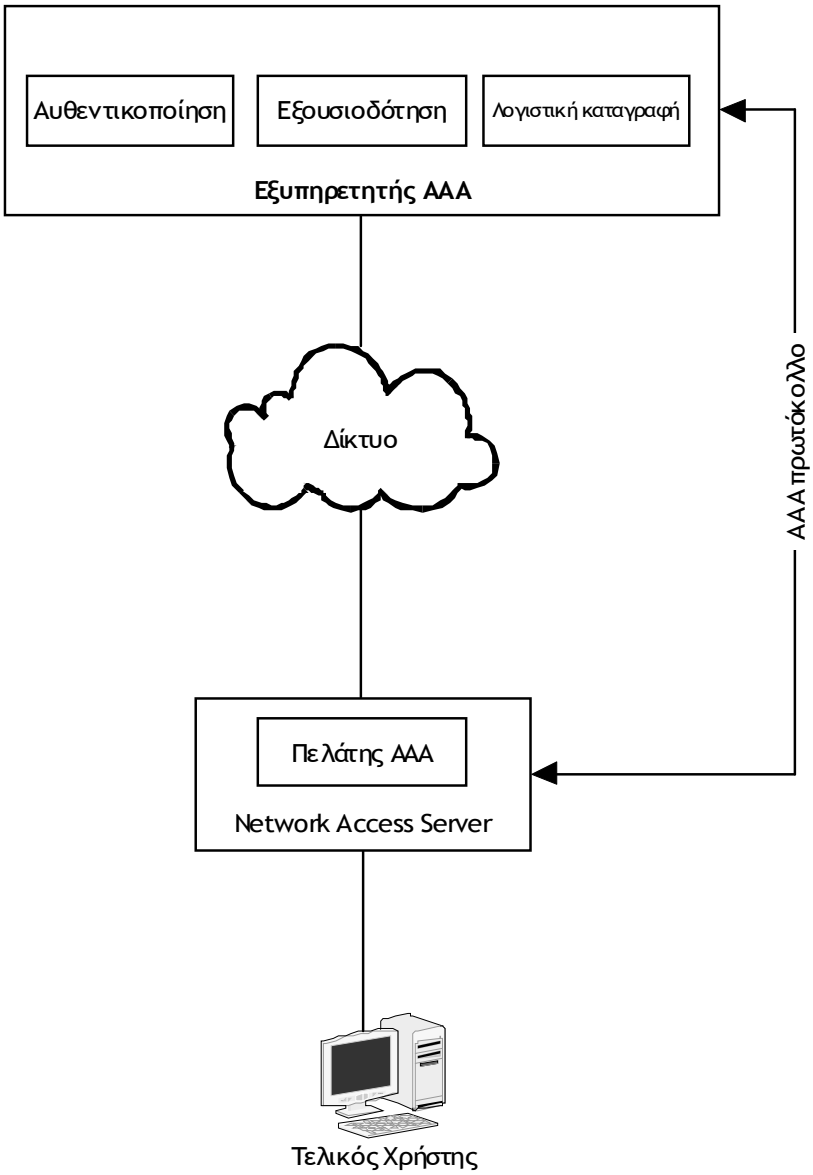
- Μοντέλο Polling: Σύμφωνα με το μοντέλο αυτό, ο εξυπηρετητής ζητά από τις δικτυακές συσκευές συλλογής δεδομένων λογιστικής καταγραφής να του αποστείλουν τυχόν δεδομένα που έχουν συλλέξει. Η διαδικασία επαναλαμβάνεται σε τακτά χρονικά διαστήματα βάση του ορισθέντος μεσοδιαστήματος αναμονής για τη συλλογή νέων δεδομένων. Το μεσοδιάστημα πρέπει να ορισθεί μικρότερο από το μέγιστο χρόνο παραμονής ενός καταγεγραμμένου γεγονότος στη μνήμη μιας συσκευής-καταγραφέα. Το μοντέλο αυτό δεν αποδίδει στην περίπτωση που οι χρήστες μπορούν να μετακινούνται σε διαφορετικά δίκτυα διαφορετικών παρόχων υπηρεσιών. Δηλαδή, καθ' όλη τη σύνοδο ενός χρήστη, και καθώς αυτός μετακινείται μεταξύ των δικτύων, χρησιμοποιούνται πολλαπλές συσκευές καταγραφής των χρήσιμων για τη λογιστική καταγραφή γεγονότων. Προκειμένου ο εξυπηρετητής της υπηρεσίας να συλλέξει σωστά όλα τα δεδομένα για μία σύνοδο του χρήστη, απαιτείται να ρωτήσει όλες τις συσκευές που κατέγραψαν την κίνηση του συγκεκριμένου χρήστη (καθώς αυτός μετακινούμενος στα δίκτυα συνέχιζε να χρησιμοποιεί μία υπηρεσία) και να αποκριθούν αποστέλλοντας τα αντίστοιχα δεδομένα. Κάτι τέτοιο έχει ως άμεση συνέπεια την αύξηση του υπολογιστικού κόστους, δηλαδή την καθυστέρηση στον υπολογισμό της χρέωσης και ενδεχομένως την απώλεια πληροφοριών.
- Οδηγούμενα από γεγονότα (event driven): Στο μοντέλο αυτό, οι συσκευές που καταγράφουν τις πληροφορίες χρέωσης επικοινωνούν με τον εξυπηρετητή μόλις θεωρήσουν ότι είναι έτοιμες να μεταδώσουν δεδομένα. Μέχρι στιγμής υπάρχουν δύο διαφοροποιήσεις στα μοντέλα αυτά. Είναι το μοντέλο όπου κάθε απεσταλμένο πακέτο περιέχει ένα καταγεγραμμένο γεγονός λογιστικής καταγραφής, και το μοντέλο όπου μεταδίδονται περισσότερα γεγονότα ανά πακέτο. Στην πρώτη περίπτωση, το μοντέλο χαρακτηρίζεται μάλλον μη αποδοτικό και παρόλο που έχει μικρές απαιτήσεις για μνήμη είναι το λιγότερο

αξιόπιστο. Πλεονέκτημα του είναι η αμεσότητα παράδοσης των μηνυμάτων, συνεπώς ενδείκνυται η χρήση του σε εφαρμογές όπου χρησιμοποιούνται τεχνικές καταπολέμησης πλαστών μηνυμάτων. Εάν υλοποιηθεί το μοντέλο της ταυτόχρονης αποστολής πολλαπλών συμβάντων με ένα μήνυμα, αυξάνει η απόδοση του. Ταυτόχρονα όμως αυξάνεται ο χρόνος παράδοσης των μηνυμάτων στον εξυπηρετητή λογιστικής καταγραφής. Εάν η εφαρμογή που χρησιμοποιείται απαιτεί μικρούς χρόνους παράδοσης των πληροφοριών στον εξυπηρετητή, τότε το μοντέλο μπορεί να τροποποιηθεί έτσι ώστε τα κρίσιμης σημασίας συμβάντα να αποστέλλονται άμεσα μετά την καταγραφή τους, ενώ τα υπόλοιπα να αποστέλλονται ομαδικά.

2.4 Το πλαίσιο AAA (AAA Framework)

Στις προηγούμενες παραγράφους περιγράφηκαν οι βασικές δομικές έννοιες, τις οποίες υλοποιεί ως υπηρεσίες ένα πρωτόκολλο AAA. Προκειμένου οι υπηρεσίες αυτές να συνεργάζονται με απλό και αποδοτικό τρόπο, και να προσφέρουν δυνατότητες περαιτέρω επέκτασης του συστήματος ώστε να καλύπτει πολυπληθείς και ανομοιογενείς μεταξύ τους ομάδες συστημάτων, είναι απαραίτητη η ύπαρξη ενός πλαισίου λειτουργίας. Το πλαίσιο AAA ουσιαστικά είναι ένα πλαίσιο συνεργασίας των υπηρεσιών μεταξύ διαφορετικών δικτύων, τεχνολογιών και χρηστών. Είναι το δομικό και λειτουργικό στοιχείο που ενώνει τις μεμονωμένες υπηρεσίες υπό κοινή σκέπη. Στην πράξη το πλαίσιο αυτό υλοποιείται από έναν εξυπηρετητή AAA που διαθέτει δυνατότητες αποθήκευσης των προφίλ των χρηστών και επικοινωνεί με δικτυακές συσκευές (στο ρόλο του πελάτη), ώστε να πραγματοποιείται αποκεντρωμένη παροχή των υπηρεσιών. Ο εξυπηρετητής γενικά είναι μια μηχανή η οποία δέχεται αιτήσεις προσπέλασης πόρων/χρήσης υπηρεσιών από τους αντίστοιχους πελάτες.

Σύμφωνα με το πλαίσιο AAA, ο εξυπηρετητής είναι αυτός που αυθεντικοποιεί και εξουσιοδοτεί τους χρήστες αλλά και καταγράφει τη χρήση των πόρων από αυτούς. Ο πελάτης, στη γενική του έννοια, είναι μια μηχανή που πραγματοποιεί αιτήσεις και χρησιμοποιεί πόρους και υπηρεσίες οι οποίες παρέχονται από άλλα μηχανήματα. Στο πλαίσιο AAA, ο όρος πελάτης έχει την έννοια της αποστολής αιτήσεων χρήσης πόρων στον εξυπηρετητή αλλά όχι της χρήσης τους. Ο πελάτης-NAS λειτουργεί ως μεσολαβητής προκειμένου να αποστείλει το αίτημα χρήσης κάποιου πόρου από ένα τελικό χρήστη στον τελικό εξυπηρετητή AAA.



Σχήμα 1 Αρχιτεκτονική πλαισίου AAA

Σε γενικές γραμμές το πλαίσιο AAA μπορεί απλά να συνοψιστεί σε αυτό που απεικονίζεται στο σχήμα 1. Ένας εξυπηρετητής αυθεντικοποίησης (ενδεχομένως και περισσότεροι, ώστε να αντιμετωπίζονται ενδεχόμενες αστοχίες του υπολογιστικού μηχανήματος που λειτουργεί ως κύριος εξυπηρετητής) τοποθετείται κεντρικά στην αρχιτεκτονική του συστήματος και προσφέρει υπηρεσίες αυθεντικοποίησης, εξουσιοδότησης και λογιστικής καταγραφής. Ο εξυπηρετητής μπορεί να

πλαισιώνεται από πλήθος δικτυακών συσκευών (NAS) που λειτουργούν ως το σημείο σύνδεσης ενός χρήστη στο δίκτυο. Ο χρήστης αιτείται σύνδεσης στο NAS και αποστέλλει σε αυτόν τα διαπιστευτήρια του. Ο NAS προωθεί το αίτημα αυτό κάνοντας χρήση του πρωτοκόλλου επικοινωνίας AAA στον εξυπηρετητή. Μετά την εξέταση του αιτήματος, ο εξυπηρετητής ειδοποιεί το NAS με σχετικό μήνυμα για το αποτέλεσμα της αίτησης. Εάν γίνει δεκτό, ο NAS παραμετροποιεί τη λειτουργία του ώστε να επιτρέψει στον πελάτη να χρησιμοποιήσει την υπηρεσία που ζήτησε.

3 Το πρωτόκολλο Remote Dial In User Service (RADIUS)

Το πρωτόκολλο Remote Authentication Dial-In Service (RADIUS) αρχικά δημιουργήθηκε για να επιτρέπει ένα Network Access Server (NAS) να προωθεί τις αιτήσεις και τα διαπιστευτήρια των χρηστών σε ένα εξυπηρετητή αυθεντικοποίησης. Σήμερα, χρησιμοποιείται ευρέως σε υπηρεσίες dial-up για IP συνδεσιμότητα, σε συνδυασμό με το πρωτόκολλο Point-to-Point (PPP) [44].

Αρχικά το RADIUS σχεδιάστηκε ώστε να υποστηρίζει τα πρωτόκολλα Password Authentication Protocol (PAP) [42] και Challenge-Handshake Authentication Protocol (CHAP) [43], ωστόσο λόγω της επεκτασιμότητας που το χαρακτηρίζει, κι άλλες μέθοδοι αυθεντικοποίησης υποστηρίχθηκαν διάμεσου του πρωτοκόλλου Extensible Authentication Protocol (EAP) [3]. Αργότερα, το RADIUS εμπλουτίστηκε προκείμενου να παρέχει υπηρεσίες εξουσιοδότησης και λογιστικής καταγραφής. Σήμερα το πρωτόκολλο RADIUS μετά από αρκετές τροποποιήσεις (RFC 2058, 2138), αναπτύσσεται στο έγγραφο RFC 2865 [38]. Το RADIUS είναι το πιο διαδεδομένο AAA πρωτόκολλο παρόλο που έχει να ανταγωνιστεί άλλα, ίσως σχεδιαστικά καλύτερα, πρωτόκολλα. Στην ενότητα αυτή παρουσιάζεται το πρωτόκολλο RADIUS.

3.1 Σύντομο ιστορικό

Το πρωτόκολλο RADIUS δημιουργήθηκε για να καλύψει την ανάγκη της αυθεντικοποίησης απομακρυσμένων χρηστών που επιθυμούσαν να συνδεθούν σε ένα διαδίκτυο υπολογιστικών συστημάτων. Η σύνδεση των χρηστών την εποχή εκείνη (αρχές δεκαετίας 90) γινόταν με τις τυπικές dial-up συνδέσεις. Στην Εισαγωγή περιγράφηκε εν συντομία η ιστορία της δημιουργίας του πρωτοκόλλου. Στα χρόνια που ακολούθησαν (1990-1995), το RADIUS έγινε το de facto πρωτόκολλο παροχής υπηρεσιών αυθεντικοποίησης στους απομακρυσμένους χρήστες. Το 1994 το RADIUS δημοσιεύτηκε ως Internet Draft κι από τη στιγμή εκείνη και έπειτα κάθε προϊόν NAS υποστήριζε το RADIUS. Ωστόσο, η στιγμή της πλήρους αποδοχής του RADIUS από την επιστημονική κοινότητα δεν είχε έρθει. Στους κόλπους της IETF επικρατούσε σκεπτικισμός για το αν και κατά πόσο το RADIUS ήταν το κατάλληλο πρωτόκολλο και ιδιαίτερα σε ό,τι αφορούσε την ασφάλεια που προσέφερε. Παρόλα αυτά, το 1997 το RADIUS αφού είχε κατακτήσει την αγορά των NAS και χρησιμοποιούνταν από συντριπτικό ποσοστό παρόχων, έγινε επισήμως αποδεκτό από την IETF. Στο RFC 2039 περιγράφονται όλες οι λεπτομέρειες του πρωτοκόλλου, όπως αυτό δημοσιεύτηκε στο αρχικό draft του 1994. Αργότερα, το 2000, το RFC 2865 αντικατέστησε το προηγούμενο και είναι αυτό που ισχύει έως σήμερα.

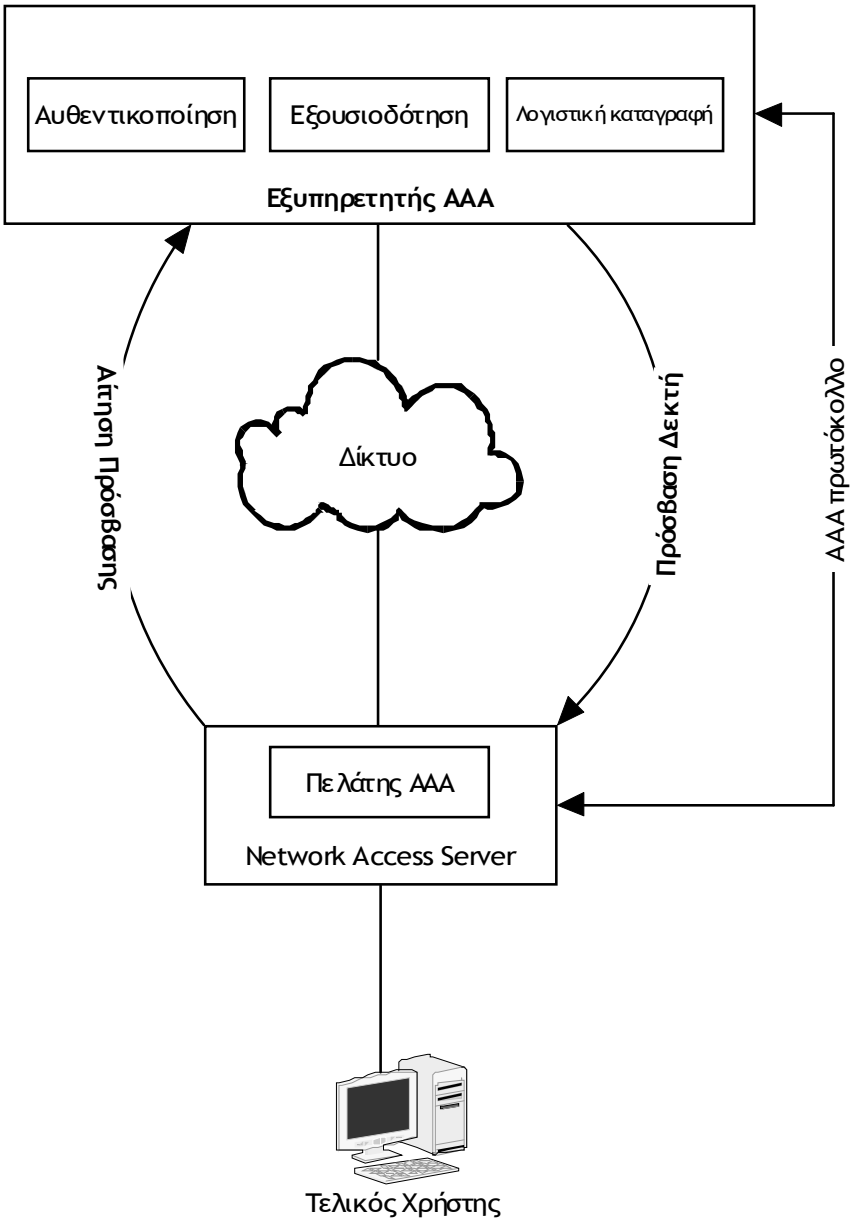
3.2 Μοντέλο λειτουργίας

Το πρωτόκολλο RADIUS υλοποιείται με βάση το μοντέλο εξυπηρετητή-πελάτη (client-server). Το ρόλο του πελάτη αναλαμβάνει ο NAS ενώ ο εξυπηρετητής είναι το υπολογιστικό σύστημα που εκτελεί το πρόγραμμα του RADIUS εξυπηρετητή. Ως πελάτης δεν νοείται ο τελικός χρήστης (end-user) που αναμένεται να συνδεθεί στο δίκτυο, αλλά η δικτυακή συσκευή που λειτουργεί ως διαμεσολαβητής μεταξύ χρήστη και δικτύου. Ο όρος πελάτης προσδίδεται στο NAS και αφορά την επικοινωνία μεταξύ αυτού και του εξυπηρετητή RADIUS.

Κατά την έναρξη της επικοινωνίας ο τελικός χρήστης ή αιτούμενος (supplicant), αιτείται πρόσβασης στο δίκτυο, αποστέλλοντας τις απαιτούμενες πληροφορίες αυθεντικοποίησης στην προεπιλεγμένη πύλη δικτύου, δηλαδή το NAS. Οι πληροφορίες αυτές αποστέλλονται με τη μορφή αιτήσεων (requests), ενώ οι απαντήσεις δίδονται από τον εξυπηρετητή με τη μορφή των αποκρίσεων (responses). Σημειώνεται, πως η επικοινωνία αυτή πραγματοποιείται στο δεύτερο επίπεδο του μοντέλου OSI (ζεύξης δεδομένων). Ο αιτούμενος δεν λαμβάνει σε καμία φάση της επικοινωνίας διεύθυνση IP, πριν πιστοποιηθεί με επιτυχία η ταυτότητά του.

Ο NAS κατά τη διάρκεια αυτής της φάσης προωθεί τα πακέτα από και προς τον εξυπηρετητή δίχως να εξετάζει το περιεχόμενο τους. Ο εξυπηρετητής RADIUS είναι υπεύθυνος για τη διαχείριση των αιτήσεων από τους αιτούμενους χρήστες, την αυθεντικοποίηση αυτών και την αποστολή μηνυμάτων στον πελάτη-NAS προκειμένου να τον πληροφορήσει για το αποτέλεσμα της αυθεντικοποίησης. Σε περίπτωση αποτυχίας ο NAS δεν πραγματοποιεί καμία ενέργεια και δεν ανοίγει τη θύρα πρόσβασης (port) στον αιτούμενο χρήστη. Αντίθετα, σε περίπτωση επιτυχούς αυθεντικοποίησης, ο εξυπηρετητής RADIUS αποστέλλει στο NAS ανάλογο μήνυμα επιτυχίας, και, όπου είναι απαραίτητο, επιπλέον πληροφορίες παραμετροποίησης του. Στο σχήμα 2 περιγράφεται σχηματικά η εξέλιξη μιας τυπικής σύνδεσης ενός χρήστη στο δίκτυο του παρόχου.

Σε όλη τη διάρκεια της επικοινωνίας μεταξύ πελάτη-NAS και εξυπηρετητή, τα μηνύματα που ανταλλάσσονται θεωρούνται ότι είναι αυθεντικοποιημένα χρησιμοποιώντας ένα μυστικό κωδικό. Ο κωδικός αυτός, ο οποίος είναι εκ των προτέρων γνωστός και στα δύο μέρη δεν αποστέλλεται ποτέ μέσω του δικτύου επικοινωνίας. Επιπλέον, όλοι οι κωδικοί του χρήστη που αποστέλλονται από τον πελάτη-NAS στον εξυπηρετητή είναι κρυπτογραφημένοι. Παρακάτω περιγράφονται λεπτομερώς οι διαδικασίες προστασίας των μεταδιδόμενων μηνυμάτων.

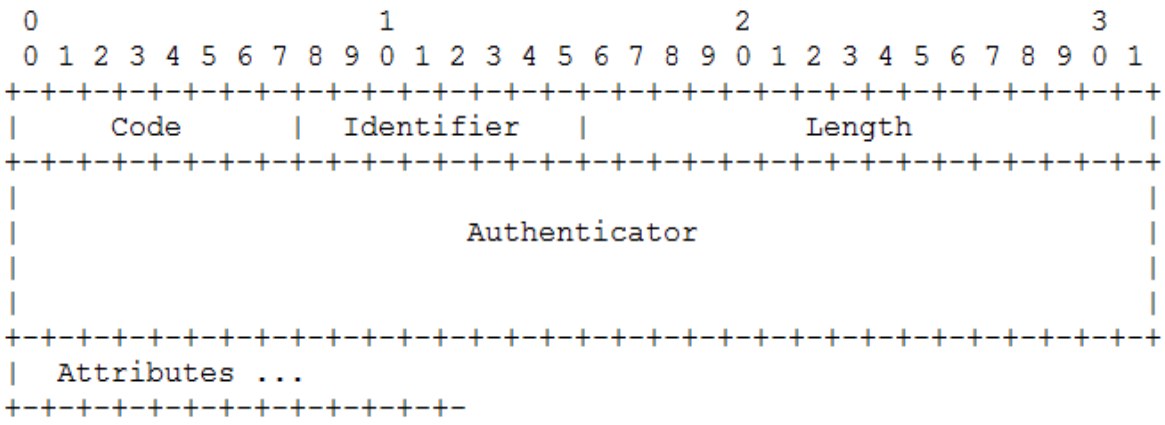


Σχήμα 2 Ανταλλαγή μηνυμάτων αιτήσεων-αποκρίσεων σε μία τυπική επικοινωνία RADIUS

3.3 Επικοινωνία με βάση το πρωτόκολλο RADIUS

3.3.1 Δομή πακέτου

Το πρωτόκολλο RADIUS χρησιμοποιεί το UDP[1] ως πρωτόκολλο υπεύθυνο για τη μεταφορά των πακέτων από άκρη σε άκρη, δηλαδή, μεταξύ πελάτη εξυπηρετητή. Η επικοινωνία πραγματοποιείται στην πύλη 1812 του UDP (στο παρελθόν χρησιμοποιήθηκε η πύλη 1645 αλλά εγκαταλείφθηκε λόγω κοινής χρήσης με την υπηρεσία datametrics).



Σχήμα 3 Δομή ενός πακέτου RADIUS [38]

Η δομή του πακέτου, όπως απεικονίζεται στο σχήμα 3, είναι ιδιαίτερα απλή. Η επικεφαλίδα αποτελείται από 4 διακριτά τμήματα (Κώδικας, Προσδιοριστής, Μήκος, Αυθεντικοποιητής) ακολουθούμενο από το κύριο σώμα του πακέτου που είναι οι Ιδιότητες (attributes).

- Κωδικός: 8 bit: Τα πρώτα 8 bit πληροφορίας του πακέτου προσδιορίζουν τον τύπο του μηνύματος που φέρει το συγκεκριμένο πακέτο. Κάθε πακέτο που φέρει ένα μη αναμενόμενο κώδικα αναγνώρισης απορρίπτεται κατευθείαν δίχως ανακοίνωση (silent discard). Αξίζει να σημειωθεί ότι νεότερα RFC [37, 39] έχουν προσθέσει νέους τύπους μηνυμάτων επεκτείνοντας τη λειτουργικότητα του. Ωστόσο, λόγω της μεγάλης εγκατεστημένης βάσης μηχανημάτων που χρησιμοποιούν την αρχική έκδοση του RADIUS, οι νέες προσθήκες δεν

[1] Γιατί UDP κι όχι TCP: Η επιλογή χρήσης του stateless πρωτοκόλλου UDP αντί του πιο αξιόπιστου TCP ως επίπεδο μεταφοράς ήταν συνειδητή επιλογή των σχεδιαστών και έγινε για συγκεκριμένους τεχνικούς λόγους. Η ευκολία υλοποίησης του λογισμικού του εξυπηρετητή για χειρισμό πολλών ταυτόχρονων αιτήσεων αυθεντικοποίησης, η γενικότερη stateless επικοινωνία του RADIUS αλλά και η μη ανάγκη ύπαρξης ενός αυστηρού πλαισίου σχετικά με την αναφορά χαμένων πακέτων ήταν μερικοί από τους λόγους προτίμησης του UDP αντί του TCP [29].

τυγχάνουν ευρείας αποδοχής, λόγω των πιθανών προβλημάτων συμβατότητας που μπορεί να παρουσιαστούν μεταξύ διαφορετικών εκδόσεων.

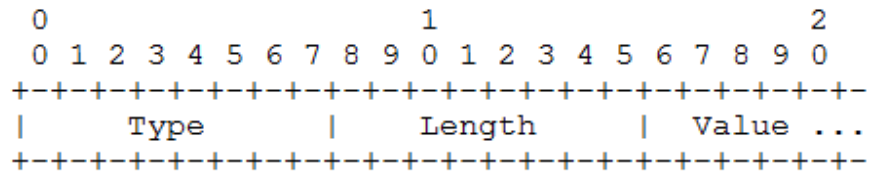
Πίνακας 1 Κωδικοποίηση τύπων μηνυμάτων στο RADIUS

Κωδικοποίηση	Πακέτο	Περιγραφή
1	Access-Request	Ο NAS δημιουργεί ένα τέτοιο μήνυμα κάθε φορά που προωθεί μία αίτηση σύνδεσης από ένα χρήστη στον εξυπηρετητή RADIUS.
2	Access-Accept	Ειδοποιεί τον πελάτη-NAS ότι η διαδικασία αυθεντικοποίησης πραγματοποιήθηκε με επιτυχία και μπορεί να επιτραπεί η πρόσβαση από τον χρήστη.
3	Access-Reject	Ειδοποιεί τον πελάτη-NAS για την απόρριψη της αίτησης πρόσβασης.
4	Accounting-Request	Το μήνυμα αποστέλλεται από τον πελάτη-NAS στον εξυπηρετητή και μεταφέρει πληροφορίες λογιστικής καταγραφής σχετικά με την παρεχόμενη υπηρεσία.
5	Accounting-Response	Αποστέλλεται από τον εξυπηρετητή λογιστικής καταγραφής στον πελάτη-NAS ώστε να επιβεβαιώσει την ορθή λήψη των ληφθέντων δεδομένων. Επίσης δηλώνει το αποτέλεσμα των λογιστικών πράξεων που πραγματοποιούνται στον εξυπηρετητή.
11	Access-Challenge	Το μήνυμα αποστέλλεται από τον εξυπηρετητή RADIUS στον NAS. Χρησιμοποιείται για να ρωτηθεί ο NAS ή ο χρήστης για κάτι.
12	Status-Server	Πειραματική χρήση
13	Status-Client	Πειραματική χρήση
255	Reserved	Δεσμευμένο

- Προσδιοριστής: 8 bit: Χρησιμοποιείται για να αντιστοιχίζονται τα μηνύματα των αιτήσεων με αυτά των αποκρίσεων. Ο εξυπηρετητής RADIUS μπορεί να αναγνωρίσει μία διπλότυπη αίτηση εάν η IP διεύθυνση και αριθμός πύλης προέλευσης καθώς και το πεδίο του Προσδιοριστή είναι ίδια (για ένα σύντομο σχετικά χρονικό μεσοδιάστημα μεταξύ της λήψης των δύο αιτήσεων).
- Μήκος: 16 bit: Σε αυτό το πεδίο προσδιορίζεται το μέγεθος του πακέτου RADIUS. Η τιμή αυτή είναι το άθροισμα όλων των πεδίων του πακέτου. Το πεδίο Μήκος ελέγχεται όταν ο εξυπηρετητής RADIUS λαμβάνει ένα πακέτο προκειμένου να εξασφαλιστεί η ακεραιότητα των δεδομένων. Εάν το ληφθέν πακέτο είναι μικρότερο από αυτό που υποδεικνύει το πεδίο

Μέγεθος, το πακέτο απορρίπτεται δίχως ανακοίνωση. Οι προδιαγραφές ορίζουν ελάχιστο μέγεθος πακέτου τα 160 bit ενώ μέγιστο τα 32768 bit.

- Αυθεντικοποιητής: 128bit: Χρησιμοποιείται για τον έλεγχο και την επιβεβαίωση της ακεραιότητας των δεδομένων του μηνύματος. Περιγράφεται αναλυτικά παρακάτω.
- Ιδιότητες: Μεταβλητού μεγέθους. Οι ιδιότητες αποτελούν το κύριο σώμα του πακέτου και συνήθως το μεγαλύτερο σε μέγεθος. Με τη χρήση των ιδιοτήτων γίνεται εφικτή η μεταφορά πληροφοριών για διαφορετικές υπηρεσίες που χρειάζονται την υποδομή AAA που προσφέρει το RADIUS πρωτόκολλο.



Σχήμα 4 Δομή μιας τυπικής ιδιότητας RADIUS [38]

Κάθε ιδιότητα (attribute) είναι ένα αυτοτελές μήνυμα που περιλαμβάνει πληροφορίες μεταβλητού μεγέθους, ενώ έχει συγκεκριμένη δομή. Αποτελείται από τον Τύπο της ιδιότητας, το συνολικό Μέγεθος της και φυσικά το περιεχόμενο της (Τιμή). Στο σχήμα 4 παρουσιάζεται διαγραμματικά η δομή μιας ιδιότητας. Οι ιδιότητες παρέχουν δυνατότητες επεκτασιμότητας του πρωτοκόλλου ώστε να καλύπτει νέες υπηρεσίες, αλληλεπιδρώντας με διαφορετικές οντότητες και για ποικίλους σκοπούς. Αυτό το χαρακτηριστικό εκμεταλλεύονται οι εξειδικευμένες ιδιότητες κατασκευαστών, που φέρουν τον κωδικό 26 (Vendor Specific Attributes, VSA) με βάση τις οποίες καθίσταται εφικτή η επικοινωνία μεταξύ συσκευών NAS διαφορετικών κατασκευαστών με τον εξυπηρετητή RADIUS. Αυτό δεν είναι πάντα προφανές, αφού η εσωτερική υλοποίηση ενός NAS ενδεχομένως να είναι διαφορετική μεταξύ διαφορετικών κατασκευαστών ή να μην υπακούει στο πλαίσιο απαιτήσεων ενός σύγχρονου NAS. Στον πίνακα 2 παρουσιάζεται η κωδικοποίηση των ιδιοτήτων όπως προδιαγράφεται στο RFC2865.

Πίνακας 2 Υποστηριζόμενες ιδιότητες RADIUS σύμφωνα με το RFC 2865

Α/Α	Περιγραφή
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
9	Framed-IP-Netmask
10	Framed-Routing
11	Filter-Id
12	Framed-MTU
13	Framed-Compression
14	Login-IP-Host
15	Login-Service
16	Login-TCP-Port
17	Χωρίς ανάθεση
18	Reply-Message
19	Callback-Number
20	Callback-Id
21	Χωρίς ανάθεση
22	Framed-Route
23	Framed-IPX-Network
24	State
25	Class
26	Vendor-Specific
27	Session-Timeout
28	Idle-Timeout

29	Termination-Action
30	Called-Station-Id
31	Calling-Station-Id
32	NAS-Identifier
33	Proxy-State
34	Login-LAT-Service
35	Login-LAT-Node
36	Login-LAT-Group
37	Framed-AppleTalk-Link
38	Framed-AppleTalk-Network
39	Framed-AppleTalk-Zone
40-59	δεσμευμένα για τη λογιστική καταγραφή
60	CHAP-Challenge
61	NAS-Port-Type
62	Port-Limit
63	Login-LAT-Port

3.3.2 Επεκτασιμότητα

Η επεκτασιμότητα στο RADIUS επιτυγχάνεται κατά κύριο λόγο με τη χρήση διαφορετικών ιδιοτήτων. Το βασικό πρότυπο για το RADIUS [38], καθορίζει περίπου 40 διαφορετικές ιδιότητες ενώ αργότερα, στα επόμενα RFC [37, 39], προστέθηκαν κι άλλες. Ο μέγιστος αριθμός διαφορετικών ιδιοτήτων είναι 256, αφού χρησιμοποιούνται 8 bits πληροφορίας στο αντίστοιχο πεδίο μιας ιδιότητας. Ο περιορισμένος αριθμός των ιδιοτήτων αλλά και η ανάγκη διατήρησης συμβατότητας μεταξύ εκδόσεων του πρωτοκόλλου είχε ως αποτέλεσμα την ιδιαίτερα εγκρατή και φειδωλή στάση της ομάδας εργασίας της IETF στην προτυποποίηση νέων ιδιοτήτων.

3.3.3 Πληρεξούσιοι εξυπηρετητές (proxies)

Οι εξυπηρετητές RADIUS μπορούν να λειτουργούν ως πληρεξούσιοι κόμβοι σε ένα τηλεπικοινωνιακό μονοπάτι προωθώντας αιτήσεις από ένα NAS σε άλλο εξυπηρετητή. Όταν ένας πληρεξούσιος εξυπηρετητής RADIUS λάβει ένα μήνυμα αίτησης αυθεντικοποίησης, το προωθεί στον αποκρουσμένο εξυπηρετητή. Σε δεύτερη φάση, λαμβάνει τις αποκρίσεις του απομακρυσμένου εξυπηρετητή και τις αποστέλλει στον πελάτη. Ο πληρεξούσιος εξυπηρετητής έχει δικαίωμα να

τροποποιήσει τα μηνύματα προκειμένου να εφαρμόζεται μια συγκεκριμένη πολιτική ασφάλειας. Η χρήση των πληρεξούσιων εξυπηρετητών βρίσκει εφαρμογή όταν παρέχονται υπηρεσίες περιαγωγής (roaming). Σε αυτή την περίπτωση, ένας χρήστης μπορεί να χρησιμοποιεί τηλεπικοινωνιακά δίκτυα και πόρους από διαφορετικούς παρόχους (ενώ είναι συμβεβλημένος μόνο σε ένα) προκειμένου να απολαμβάνει ολοκληρωμένες υπηρεσίες.

Η επιλογή των εξυπηρετητών που θα λειτουργούν ως πληρεξούσιοι ή ως τελικοί (αυτοί δηλαδή που θα επεξεργαστούν την αίτηση) καθορίζεται βάσει των περιοχών διαχείρισης μεταξύ των παρόχων, της τοπολογίας του δικτύου επικοινωνίας και φυσικά τον τύπο της παρεχόμενης υπηρεσίας.

Ένας εξυπηρετητής RADIUS μπορεί να λειτουργεί είτε ως πληρεξούσιος ή ως απομακρυσμένος εξυπηρετητής ανάλογα με τη διαχειριστική περιοχή που ανήκει και τις απαιτήσεις. Ένας πληρεξούσιος εξυπηρετητής μπορεί να χρησιμοποιηθεί ώστε να προωθεί μηνύματα σε περισσότερους από έναν απομακρυσμένους εξυπηρετητές. Για λόγους καλύτερης κατανόησης του ρόλου των πληρεξούσιων εξυπηρετητών περιγράφονται τα βήματα που ακολουθούνται σε μια τυπική σύνοδο ενός χρήστη όταν εμπλέκεται κι ένας πληρεξούσιος εξυπηρετητής.

1. Ο NAS αποστέλλει το μήνυμα αίτησης πρόσβασης (Access-Request) στον πληρεξούσιο εξυπηρετητή. Ο πληρεξούσιος αποκρυπτογραφεί το κωδικό πρόσβασης, εάν αυτός υπάρχει χρησιμοποιώντας το μυστικό κωδικό που μοιράζεται με το NAS.
2. Ο πληρεξούσιος εξυπηρετητής κρυπτογραφεί τον κωδικό χρήστη, με το μυστικό κωδικό που μοιράζεται με τον απομακρυσμένο εξυπηρετητή, θέτει το πεδίο Προσδιοριστής κατάλληλα και προωθεί την αίτηση στον απομακρυσμένο χρήστη.
3. Ο απομακρυσμένος εξυπηρετητής, αν είναι ο τελικός παραλήπτης της αίτησης, ξεκινά τη διαδικασία επεξεργασίας της. Έτσι, επαληθεύει την ταυτότητα του χρήστη βάσει του κωδικού πρόσβασης και επιστρέφει ανάλογο μήνυμα (Access-Accept, Access-Reject, Access-Challenge) στον πληρεξούσιο εξυπηρετητή.
4. Ο πληρεξούσιος εξυπηρετητή πιστοποιεί τον Αυθεντικοποιητή Απόκρισης χρησιμοποιώντας το μυστικό κωδικό που μοιράζεται με τον απομακρυσμένο εξυπηρετητή. Αν δεν επαληθευτεί, το μήνυμα απορρίπτεται δίχως ανακοίνωση. Στην περίπτωση επιτυχούς επαλήθευσης, υπογράφει τον Αυθεντικοποιητή Απόκρισης με το μυστικό κωδικό που μοιράζεται με το NAS και του το αποστέλλει.

Προκειμένου η παραπάνω διαδικασία να είναι ασφαλής, πρέπει να εξασφαλίζεται η δίχως προϋποθέσεις εμπιστοσύνη στους ενδιάμεσους πληρεξουσίους εξυπηρετητές, αφού εκεί γίνεται

έκθεση των μυστικών κωδικών των χρηστών. Σε κάθε άλλη περίπτωση κάνουμε λόγο για έλλειψη εμπιστευτικότητας του συστήματος αυθεντικοποίησης χρηστών.

3.4 Λογιστική καταγραφή

Επιπρόσθετα με τις υπηρεσίες αυθεντικοποίησης και εξουσιοδότησης, το πρωτόκολλο RADIUS εμπλουτίστηκε με δυνατότητες λογιστικής καταγραφής προκειμένου να παραμένει σύγχρονο στις απαιτήσεις της εποχής. Το αρχικό RFC2138, το οποίο αντικαταστάθηκε από το νεότερο 2865, παρείχε τις απαιτούμενες προδιαγραφές ώστε το πρωτόκολλο να είναι λειτουργικό όσον αφορά τις υπηρεσίες αυθεντικοποίησης και εξουσιοδότησης. Στο έγγραφο RFC2866 περιγράφεται λεπτομερώς η υπηρεσία λογιστικής καταγραφής καθώς αυτή έγινε κομμάτι του RADIUS πρωτοκόλλου. Η παράγραφος αυτή αναλύει τις τεχνικές λεπτομέρειας της λογιστικής καταγραφής, όπως αυτή υλοποιείται στο πρωτόκολλο RADIUS και βασίζεται στο RFC 2866[37].

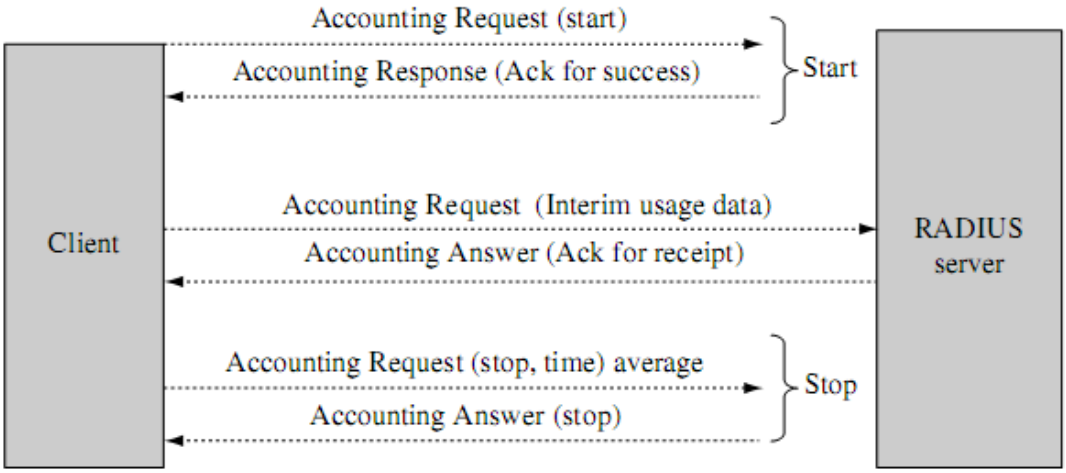
3.4.1 Βασική λειτουργία

Η υπηρεσία λογιστικής καταγραφής σε γενικές γραμμές ακολουθεί το ίδιο μοτίβο επικοινωνίας, όπως αυτό περιγράφηκε παραπάνω για τις άλλες υπηρεσίες. Το μοντέλο επικοινωνίας, η δομή των πακέτων, το επίπεδο ασφάλειας επικοινωνίας, οι δυνατότητες επεκτασιμότητας παραμένουν ως είχαν στο βασικό RFC, αλλά χρησιμοποιούνται διαφορετικοί τύποι (πεδίο Κώδικας) μηνυμάτων. Επίσης, υπάρχει ένα διαφορετικό σετ Ιδιοτήτων που είναι διαθέσιμο για χρήση στην υπηρεσία λογιστικής καταγραφής.

Όπως και στις άλλες υπηρεσίες, έτσι και στη λογιστική καταγραφή υπάρχουν τα βασικά μηνύματα επικοινωνίας μεταξύ πελάτη-εξυπηρετητή, δηλαδή τα Αίτησης-Απόκρισης. Κατά την έναρξη της συνόδου ο πελάτης αποστέλλει το εναρκτήριο μήνυμα Accounting (Start) Request στον εξυπηρετητή, το οποίο περιλαμβάνει πληροφορίες για την υπηρεσία που αναμένεται να κάνει χρήση ο τελικός χρήστης αλλά και το αναγνωριστικό του. Ο εξυπηρετητής αποκρίνεται αποστέλλοντας ένα μήνυμα Accounting Response επιβεβαιώνοντας την επιτυχημένη λήψη του πρώτου και παράλληλα ξεκινάει τη διαδικασία καταγραφής για τη συγκεκριμένη σύνοδο. Μετά το τέλος της συνόδου, ο πελάτης-NAS αποστέλλει ένα μήνυμα Accounting (Stop) Request δηλώνοντας τον τερματισμό χρήσης της υπηρεσίας κι επιπλέον στοιχεία, όπως τον τύπο της υπηρεσίας, στατιστικά στοιχεία της συνόδου (χρόνος χρήσης, ποσό διακινούμενης πληροφορίας, μέσος ρυθμός μετάδοσης κ.α.). Ο εξυπηρετητής απαντά με ανάλογο μήνυμα Accounting Response και τερματίζεται η σύνοδος.

Καθ' όλη τη διάρκεια της συνόδου, ο πελάτης ενδέχεται να αποστείλει ένα ή περισσότερα μηνύματα σχετικά με τα στατιστικά χρήσης που διαθέτει μέχρι τη δεδομένη χρονική στιγμή. Ο

εξυπηρετητής είναι υποχρεωμένος να απαντήσει με ανάλογο μήνυμα επιβεβαίωσης μετά την επιτυχημένη λήψη του μηνύματος από τον πελάτη-NAS. Στο σχήμα 5 απεικονίζεται διαγραμματικά μία τυπική σύνοδος λογιστικής καταγραφής, όπως αυτή περιγράφεται στο RFC2866.



Σχήμα 5 Λειτουργία λογιστικής καταγραφή στο RADIUS [37]

Πίνακας 3 Κωδικοποίηση ιδιοτήτων για τη λογιστική καταγραφή στο RADIUS

Α/Α	Περιγραφή
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
50	Acct-Multi-Session-Id
51	Acct-Link-Count

3.5 Ασφάλεια στο RADIUS

Κατά το σχεδιασμό του πρωτοκόλλου η ασφάλεια δεν θεωρήθηκε ζήτημα κρίσιμης σημασίας και αυτό αποτυπώνεται από τις μεθόδους προστασίας που προσφέρει εγγενώς το RADIUS. Υπάρχουν δύο λειτουργίες αναφορικά με την προστασία που παρέχει το RADIUS. Η *απόκρυψη ιδιοτήτων* (attribute hiding), και η αυθεντικοποίηση συγκεκριμένων μηνυμάτων. Και οι δύο μέθοδοι προστασίας υλοποιούνται στη βάση ενός πολύ γνωστού μηχανισμού ασφάλειας, των συναρτήσεων κατακερματισμού. Πιο συγκεκριμένα, χρησιμοποιείται η συνάρτηση κατακερματισμού MD5 [40] σε συνδυασμό με μία μυστική πληροφορία μεταξύ του πελάτη-NAS και του εξυπηρετητή RADIUS. Στην παράγραφό αυτή αναλύονται οι δύο αυτές μέθοδοι, ενώ περισσότερες πληροφορίες σχετικά με τις ευπάθειες του πρωτοκόλλου περιγράφονται στο κεφάλαιο 5.

3.5.1 Η χρήση του πεδίου Αυθεντικοποιητής

Όπως παρουσιάστηκε παραπάνω, το πεδίο Αυθεντικοποιητής έχει μήκος 128 bit και χρησιμοποιείται για τη διασφάλιση της ακεραιότητας των μεταδιδόμενων μηνυμάτων. Κατά την αποστολή ενός μηνύματος αίτησης πρόσβασης (Access-Request) από τον πελάτη-NAS στον εξυπηρετητή RADIUS, θα ονομάζουμε το πεδίο Αυθεντικοποιητής Αίτησης. Κατά την αντίθετη κατεύθυνση, από τον εξυπηρετητή στο NAS, και στις περιπτώσεις των μηνυμάτων Access-Accept, Access-Reject, Access-Challenge θα καλείται Αυθεντικοποιητής Απόκρισης. Η διάκριση αυτή είναι πολύ σημαντική αφού διαφοροποιείται έτσι το παρεχόμενο επίπεδο προστασίας κατά τη μετάδοση των μηνυμάτων.

Στην πρώτη περίπτωση, Αυθεντικοποιητής Αίτησης, δεν παρέχεται εγγενώς καμία απολύτως προστασία της ακεραιότητας του μεταδιδόμενου μηνύματος, τουλάχιστον όπως προβλέπουν οι προδιαγραφές του πρωτοκόλλου [38]. Το πεδίο Αυθεντικοποιητής φέρει έναν ψευδοτυχαίο αριθμό, ο οποίος παράγεται από το NAS όταν ένα χρήστης αιτείται πρόσβασης σε μία υπηρεσία. Σε αυτή την φάση δεν εφαρμόζεται καμία κρυπτογραφική μέθοδος προστασίας. Το μόνο που πραγματοποιεί ο εξυπηρετητής RADIUS (ως μέτρο ασφάλειας) είναι ο έλεγχος της IP διεύθυνσης αποστολέα, συγκρίνοντας τη δηλαδή με μία λίστα γνωστών διευθύνσεων. Αυτό ωστόσο δεν παρέχει καμία προστασία στην ακεραιότητα του μηνύματος ενώ η αυθεντικοποίηση βάσει της λίστας των γνωστών διευθύνσεων είναι ανεπαρκής αφού σήμερα θεωρείται ιδιαίτερα εύκολη η πλαστογράφηση IP διευθύνσεων [48].

Για να αντιμετωπιστεί το κενό αυτό, προτάθηκε η χρήση μιας νέας εξειδικευμένης ιδιότητας που θα παρείχε το απαιτούμενο επίπεδο ασφάλειας. Η ιδιότητα Αυθεντικοποιητής Μηνύματος

(κωδικός 80) περιέχει το αποτέλεσμα της συνάρτησης κατακερματισμού MD5 ολόκληρου του προς μετάδοση μηνύματος με είσοδο το μυστικό κωδικό.

Αυθεντικοποιητής Μηνύματος= MD5(Κώδικας, Προσδιοριστής, Μέγεθος, Αυθεντικοποιητής Αίτησης, Ιδιότητες, Μυστικός Κωδικός)

Κατά τη λήψη του μηνύματος ο εξυπηρετητής, εκτελεί την ίδια συνάρτηση με τις ίδιες εισόδους, χρησιμοποιώντας το μυστικό κωδικό, τον οποίο μοιράζεται με το NAS. Εάν το αποτέλεσμα της συνάρτησης είναι ίδιο με αυτό που περιέχεται στην ιδιότητα Αυθεντικοποιητής Μηνύματος που έλαβε, σημαίνει ότι το πακέτο λήφθηκε σωστά και στάλθηκε από έναν εξουσιοδοτημένο πελάτη-NAS. Σε κάθε άλλη περίπτωση το απορρίπτει.

Στις μεταδόσεις-αποκρίσεις του εξυπηρετητή το πρότυπο περιγράφει εξ αρχής έναν τρόπο προστασίας του μηνύματος. Στις μεταδόσεις μηνυμάτων Access-Accept, Access-Reject, Access-Challenge ο Αυθεντικοποιητής Απόκρισης περιέχει το αποτέλεσμα της συνάρτησης κατακερματισμού MD5 των παρακάτω στοιχείων του μηνύματος:

Αυθεντικοποιητής Μηνύματος= MD5(Κώδικας, Προσδιοριστής, Μέγεθος, Αυθεντικοποιητής Αίτησης, Ιδιότητες)

3.5.2 Απόκρυψη ιδιοτήτων

Το πρωτόκολλο RADIUS προβλέπει ακόμη μία μέθοδο προστασίας των μεταδιδόμενων μηνυμάτων από κακόβουλους χρήστες. Η μέθοδος αυτή καλείται απόκρυψη ιδιοτήτων (attribute hiding) και εφαρμόζεται σε συγκεκριμένα μηνύματα, τα οποία κατά απαίτηση χρειάζονται προστασία κατά τη μετάδοση τους. Τα μηνύματα αυτά είναι εκείνα που φέρουν τους μυστικούς κωδικούς (password) με τους οποίους ένας χρήστης αυθεντικοποιείται ώστε να χρησιμοποιήσει μία υπηρεσία ή να προσπελάσει ορισμένους προστατευμένους πόρους. Οι μηχανισμοί αυθεντικοποίησης Password Authentication Protocol (PAP) και Challenge-handshake authentication protocol (CHAP) απαιτούν προφύλαξη των μεταδιδόμενων μηνυμάτων. Σε αυτή την περίπτωση έχουμε απόκρυψη κωδικών πρόσβασης. Η σχετική διαδικασία ακολουθεί τα παρακάτω βήματα:

1. Εάν ο κωδικός πρόσβασης(UP) είναι μικρότερος από 128 bits, ο πελάτης-NAS παράγει ένα τυχαίο Αυθεντικοποιητή Αίτησης τον οποίο συνενώνει με τον κοινό μυστικό που κατέχει (και μοιράζεται με τον εξυπηρετητή αυθεντικοποίησης).

2. Ο πελάτης-NAS υπολογίζει τη συνάρτηση κατακερματισμού MD5 με είσοδο την ένωση (Ε) του Αυθεντικοποιητή Αίτησης και του κοινού μυστικού και έπειτα χρησιμοποιεί τη συνάρτηση του αποκλειστικού Ή (XOR) στο αποτέλεσμα με τον κωδικό του χρήστη.

$$E = MD5 \text{ (κοινό μυστικό RADIUS + Αυθεντικοποιητής Αίτησης)}$$

$$\text{Κρυπτομήνυμα} = E \text{ XOR Κωδικός Χρήστη}$$

3. Το αποτέλεσμα της πράξης τοποθετείται σε μία ιδιότητα τύπου Κωδικός-Χρήστη και μεταφέρεται στον προορισμό του με ένα μήνυμα RADIUS Αίτηση Πρόσβασης.
4. (Υπό προϋποθέσεις) Εάν ο κωδικός χρήστη είναι μεγαλύτερος από 128 bits, τότε κατακερματίζεται σε κομμάτια των 128 bits (KX_1, KX_2...), ενώ το τελευταίο κομμάτι συμπληρώνεται με μηδενικά (padding), όπου είναι απαραίτητο προκειμένου να έχει κι αυτό το ίδιο μέγεθος.

$E_1 = MD5$ (κοινό μυστικό RADIUS + Αυθεντικοποιητής Αίτησης) $\text{Κρυπτομήνυμα}_1 = E_1 \text{ XOR } KX_1$

$E_2 = MD5$ (κοινό μυστικό RADIUS $\oplus$ Κρυπτομήνημα_1) $\text{Κρυπτομήνυμα}_2 = E_2 \text{ XOR } KX_2$

. . .

. . .

. . .

$E_N = MD5$ (κοινό μυστικό RADIUS $\oplus$ $\text{Κρυπτομήνυμα}_{N-1}$) $\text{Κρυπτομήνυμα}_N = E_N \text{ XOR } KX_N$

Το πρόβλημα που δημιουργείται με την παραπάνω διαδικασία, είναι ότι βασίζεται σε ένα τυχαίο αριθμό που παράγει ο NAS. Είναι γνωστό ότι οι υπολογιστικές μηχανές παράγουν ψευδοτυχαίους αριθμούς κι όχι πραγματικά τυχαίους [45]. Για την παραγωγή ψευδοτυχαίων αριθμών χρησιμοποιούνται συγκεκριμένες γεννήτριες αριθμών. επίσης, χρησιμοποιούνται ειδικοί έλεγχοι μετά την παραγωγή των αριθμών ώστε να ελεγχθεί η ποιότητα τους, ως προς το βαθμό τυχαιότητας που έχουν. Οι έλεγχοι αυτοί είναι ιδιαίτερα δαπανηροί σε επεξεργαστική ισχύ και πιθανότατα να μην εφαρμόζονται κανονικά και όπως θα έπρεπε σε ένα NAS, ο οποίος είναι πιθανό να διαθέτει χαμηλής ισχύος επεξεργαστική μονάδα. Το γεγονός αυτό έχει επίπτωση στην τυχαιότητα του παραγόμενου ψευδό-τυχαίου Αυθεντικοποιητή Αίτησης που δημιουργείται. Εάν ο Αυθεντικοποιητής Αίτησης δεν είναι αρκούντως τυχαίος τότε σύντομα θα αρχίσει να επαναλαμβάνεται. Δηλαδή, μετά από ορισμένο πλήθος μηνυμάτων το πρώτο κομμάτι που μετέχει στη δημιουργία του κρυπτομηνύματος, το E_1, θα εμφανιστεί ξανά. Μία γνωστή επίθεση βασισμένη στα παραπάνω έχει ως εξής:

Ένας κακόβουλος χρήστης υποβάλει μία αίτηση αυθεντικοποίησης με ένα γνωστό σε αυτόν κωδικό πρόσβασης ΚΧ και επίσης συλλέγει το κρυπτομήνυμα ΚΡ που μεταδίδει ο πελάτης-NAS

στον Αυθεντικοποιητή RADIUS. Υπολογίζοντας το αποτέλεσμα της συνάρτησης XOR μεταξύ των ΚΧ και ΚΡ, ο επιτιθέμενος έχει βρει το Ε ή τμήμα αυτού E_N. Γνωρίζοντας όλα τα πιθανά Ε ή E_N (εάν η περίοδος επανάληψης του Αυθεντικοποιητή Αίτησης είναι μικρή και ο επιτιθέμενος μπορεί να τα αποθηκεύσει) ο επιτιθέμενος μπορεί να εντοπίσει τους Κωδικούς πρόσβασης όλων των χρηστών που προσπαθούν να αυθεντικοποιηθούν σε σύντομο χρονικό διάστημα. Βασική προϋπόθεση για την επιτυχία μιας τέτοιας επίθεσης είναι η δυνατότητα του επιτιθέμενου να συλλέξει πακέτα από το δίαυλο επικοινωνίας του πελάτη-NAS με τον εξυπηρετητή.

Στο [38], οι συγγραφείς τονίζουν ότι η παραπάνω μέθοδος προστασίας δεν έχει δοκιμαστεί επαρκώς από την επιστημονική κοινότητα σχετικά με την αντοχή της σε κρυπτανάλυση. Διατυπώνονται επιφυλάξεις για το βαθμό προφύλαξης της εμπιστευτικότητας των μεταδιδομένων κωδικών πρόσβασης των χρηστών και προτείνεται η χρήση επιπρόσθετων μέτρων προφύλαξης όπου αυτό κρίνεται απαραίτητο.

4 Το πρωτόκολλο Diameter

4.1 Εισαγωγή

Το πρωτόκολλο RADIUS χρησιμοποιείται έως σήμερα, ευρύτατα και με επιτυχία σε υπηρεσίες οι οποίες χρειάζονται ένα ρωμαλέο AAA πλαίσιο. Η παροχή υπηρεσιών αυθεντικοποίησης, εξουσιοδότησης και λογιστικής καταγραφής για υπηρεσίες πρόσβασης μέσω dial-up συνδέσεων (Point-to-Point Protocol), ήταν η πρώτη εφαρμογή του πρωτοκόλλου. Ωστόσο, με την αύξηση του πλήθους των παρεχόμενων υπηρεσιών από τους παρόχους, του πλήθους των εξυπηρετούμενων χρηστών αλλά συνεπικουρούμενης και της πολυδιάστατης φύσης της επικοινωνίας, το RADIUS άρχισε να δείχνει πραγματικά σημάδια γήρανσης και δυσκολίας να προσαρμοστεί στις σύγχρονες απαιτήσεις. Επιπλέον, η τεράστια αύξηση χρήσης του Διαδικτύου και ως αποτέλεσμα αυτού της αυξημένης χρήσης διαδικτυακών συσκευών, όπως δρομολογητές και NAS, κατέστησε το RADIUS κατά ένα βαθμό δύσχρηστο και πολλές φορές ανήμπορο να αντεπεξέλθει σε αυτούς του ρυθμούς ανάπτυξης.

Ήδη από τα μέσα του 2000 η IETF άρχισε να δρομολογεί τις εξελίξεις για τη δημιουργία ενός νέου πρωτοκόλλου που θα αντικαθιστούσε το RADIUS. Για το σκοπό αυτό δημιουργήθηκε μία ειδική ομάδα εργασίας (AAA WG) υπεύθυνη για το σχεδιασμό και την εξέλιξη του νέου πρωτοκόλλου. Η ομάδα συνέταξε ένα RFC [2] στο οποίο καθορίζεται επακριβώς το σύνολο απαιτήσεων που θα έπρεπε να πληρεί το νέο AAA πρωτόκολλο. Αυτό το σύνολο των απαιτήσεων περιελάμβανε μεταξύ άλλων τα εξής: Αμοιβαία αυθεντικοποίηση μεταξύ πελάτη-εξυπηρετητή, ασφάλεια στο επίπεδο μεταφοράς, εμπιστευτικότητα και ακεραιότητα των δεδομένων, μεταφορά πιστοποιητικών, δυνατότητα λειτουργίας σε IPv4/IPv6, υποστήριξη πληρεξούσιων συσκευών (proxies), δυνατότητες εξασφαλισμένης λειτουργίας (failover), επεκτασιμότητας (scalability) και μεταφοράς εξειδικευμένων για υπηρεσίες ιδιοτήτων, audibility.

Μία ομάδα ειδικών εξέτασε όλες τις υποψήφιες προτάσεις προκείμενου να βρεθεί αυτό που θα ταίριαζε περισσότερο στις καταγεγραμμένες απαιτήσεις. Τα τέσσερα πρωτόκολλα που ανταγωνίστηκαν το RADIUS ήταν: το Simple Network Management Protocol (SNMP) [10], το Common Open Policy Service Protocol (COPS) [12], το RADIUS++ (η έκδοση 2 του RADIUS) και το Diameter. Τα αποτελέσματα της μελέτης αυτής δημοσιεύτηκαν στο [31]. Σύμφωνα με αυτό, τα πρώτα τρία πρωτόκολλα κρίθηκαν ανεπαρκή για τους εξής λόγους: Το SMNP κρίθηκε ακατάλληλο αφού δεν πληρούσε επακριβώς τις απαιτήσεις σχετικά με την υπηρεσία αυθεντικοποίησης παρόλο που είναι πλήρες σχετικά με τη λογιστική καταγραφή. Το COPS γενικά κρίθηκε κατάλληλο για την

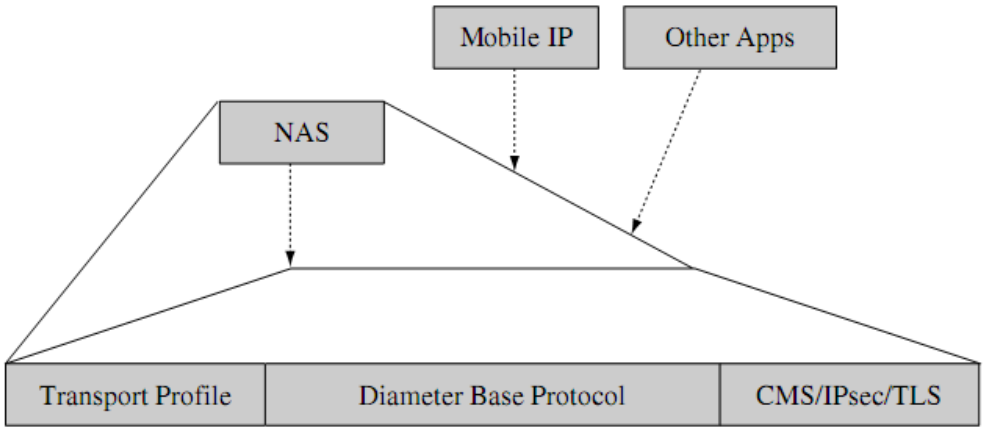
παροχή ενός ολοκληρωμένου AAA πλαισίου. Παρόλα αυτά, η αρμόδια επιτροπή θεώρησε πως η αποδοχή του COPS θα δημιουργούσε προβλήματα αφού θα σήμαινε την υιοθέτηση διπλής λειτουργίας για το πρωτόκολλο. Το RADIUS++ κρίθηκε εντελώς ανεπαρκές αφού γενικά χρειαζόταν τεράστια προσπάθεια προκειμένου να φτάσει στο επίπεδο των απαιτήσεων. Η επιλογή υπέρ του Diameter έγινε οριακά λόγω του ότι παρουσιαζόταν ως πιο ευπροσάρμοστο απέναντι στα firewalls[2] συγκριτικά με το COPS. Σημείο προβληματισμού παρέμενε η πρόταση υιοθέτησης ενός νέου πρωτοκόλλου στο επίπεδο μεταφοράς, του SCTP.

4.2 Αρχιτεκτονική λειτουργίας

Το βασικό πρωτόκολλο Diameter, που καθορίζεται στο RFC3588 [6], ορίζει ένα σετ ελάχιστων απαιτήσεων για το AAA πρωτόκολλο. Η προτυποποίηση έγινε το Σεπτέμβριο του 2003. Ουσιαστικά εκτός από τα θεμελιώδη χαρακτηριστικά του πρωτοκόλλου (βασικά δομικά στοιχεία, ιδιότητες και δομή αυτών, τύποι μηνυμάτων κλπ), και όσων αφορά τη λειτουργικότητα του, το RFC3588 εξαντλείται στην περιγραφή μόνο της υπηρεσίας λογιστικής καταγραφής. Περαιτέρω επέκταση της λειτουργικότητας του Diameter γίνεται μέσω των εφαρμογών του Diameter. Οι *εφαρμογές* δεν έχουν σχέση με τις τυπικές εφαρμογές που εκτελούνται σε υπολογιστικά συστήματα, αλλά ενδέχεται να είναι άλλα πρωτόκολλα, υπηρεσίες και διεργασίες που προσδίδουν επιπλέον λειτουργικότητα στο πρωτόκολλο, χρησιμοποιώντας το βασικό πρωτόκολλο και τις δυνατότητες που αυτό προσφέρει. Συνήθως, προδιαγράφονται σε ξεχωριστά RFC. Τυπικές εφαρμογές επέκτασης του Diameter είναι η NAS που προσθέτει τις υπηρεσίες αυθεντικοποίησης και εξουσιοδότησης, αλλά και η Mobile IP. Παρακάτω εξετάζονται λεπτομερώς μερικές από αυτές.

Στο σχήμα 6 παρουσιάζεται η αρχιτεκτονική δόμησης του Diameter. Γύρω από το βασικό πρωτόκολλο είναι δυνατόν να προστεθούν επιπλέον εφαρμογές, οι οποίες προσθέτουν συγκεκριμένη λειτουργικότητα. Όπως μπορούμε να παρατηρήσουμε, στη βάση της αρχιτεκτονικής, πέραν του βασικού πρωτοκόλλου υπάρχει το Transport Profile και τα πρωτόκολλα IP Security (IPsec)/ Transport Layer Security(TLS) με την εφαρμογή Cryptographic Message Syntax (CMS) [8]. Από αυτό το απλοϊκό σχήμα φαίνεται πως οι σχεδιαστές του Diameter έλαβαν ιδιαίτερα σοβαρά το θέμα της ασφάλειας. Στη συνέχεια αναλύεται η αλληλεπίδραση του πρωτοκόλλου με τους μηχανισμούς ασφάλειας, αλλά και η έννοια του Transport Profile.

[2] Σύμφωνα με το [2], ένα πρωτόκολλο «φιλικό» με τα firewall είναι αυτό το οποίο είναι σχεδιασμένο ώστε να διευκολύνει την χρήση αυτών δίχως να επηρεάζεται σημαντικά η λειτουργία του. Επίσης, ένα «φιλικό» πρωτόκολλο είναι αυτό για το οποίο το firewall δεν χρειάζεται να επιτελεί εκτεταμένους και εις βάθος των πακέτων ελέγχους, πλην αυτού για την διαπίστωση του αριθμού πύλης που χρησιμοποιείται.



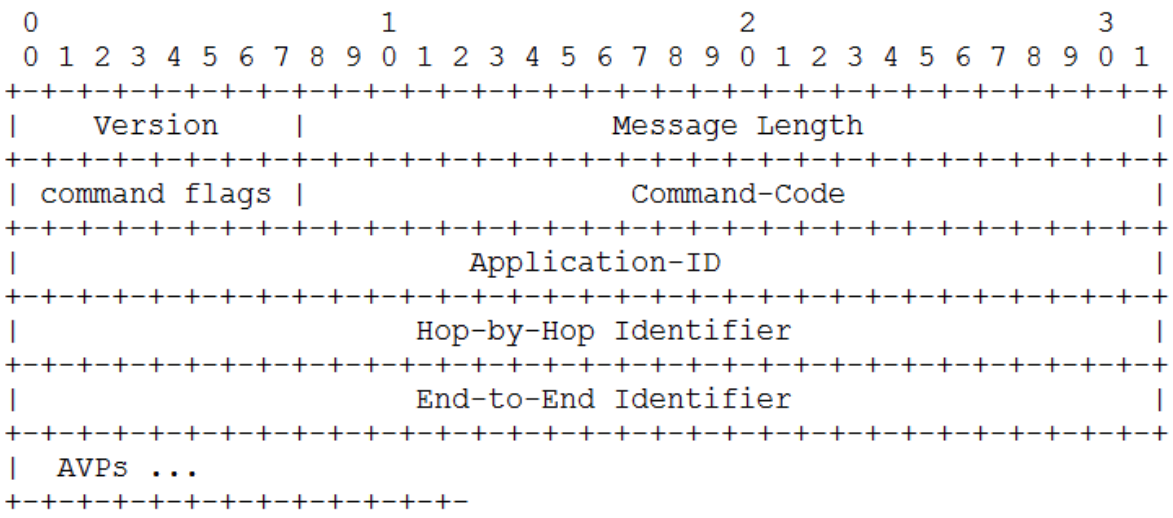
Σχήμα 6 Αρχιτεκτονική δόμησης Diameter [34]

4.3 Το βασικό πρωτόκολλο Diameter

Το βασικό πρωτόκολλο χρησιμοποιείται σε συνδυασμό με κάποια εφαρμογή για το Diameter. Κάθε εφαρμογή βασίζεται στις λειτουργίες που επιτελεί το βασικό πρωτόκολλο. Τέτοιες είναι οι εξής: (α) διαπραγμάτευση δυνατοτήτων μεταξύ των κόμβων, (β) δομή και κωδικοποίηση των πακέτων και των ιδιοτήτων, (γ) την αποστολή και λήψη των μηνυμάτων, (δ) καθορισμός συγκεκριμένων κανόνων που εφαρμόζονται στην επικοινωνία των κόμβων Diameter κ.α.. Επίσης, περιγράφεται ο τρόπος επικοινωνίας των κόμβων που ανήκουν σε διαφορετικές διαχειριστικά περιοχές (inter-realm επικοινωνία) με το να καθορίζει αυστηρά τους ρόλους των κόμβων και τις αρμοδιότητες αυτών (βλέπε ενότητα 4.2.5). Στο βασικό πρωτόκολλο, σε αντίθεση με το κύριο πρωτόκολλο του RADIUS, ορίζεται η υπηρεσία λογιστικής καταγραφής. Το βασικό πρωτόκολλο προαπαιτείται για την ανάπτυξη άλλων εφαρμογών και κατά συνέπεια κάθε συσκευή υποχρεούται να το υλοποιεί.

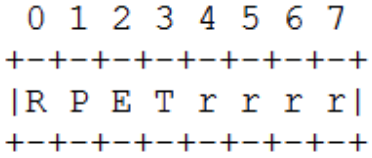
4.2.1 Δομή πακέτων

Ένα πακέτο (Protocol Data Unit, PDU) Diameter αποτελείται από μία επικεφαλίδα σταθερού μεγέθους 160 bit ακολουθούμενη από ένα μεταβλητό αριθμό ιδιοτήτων (Attribute Value Pair, AVP). Η δομή του πακέτου παρουσιάζεται αναλυτικότερα στο σχήμα 7.



Σχήμα 7 Δομή ενός πακέτου Diameter [6]

- **Έκδοση**: 8 bit. Το πεδίο υποδεικνύει την έκδοση του πρωτοκόλλου Diameter που χρησιμοποιείται. Προς το παρόν χρησιμοποιείται μόνο η τιμή 1.
- **Μέγεθος**: 24 bit. Δηλώνει το μέγεθος του μηνύματος συμπεριλαμβανομένης της επικεφαλίδας.
- **Flags εντολών**: 8 bit. Υπάρχουν τέσσερα διαφορετικά flags (τα 4 τελευταία είναι δεσμευμένα προς μελλοντική χρήση). R (από το Request) υποδεικνύει εάν το μήνυμα είναι αίτησης (1) ή απόκρισης (0). P (από το Proxiable) δηλώνει εάν το συγκεκριμένο πακέτο δύναται να ανακατευθυνθεί, αναμεταδοθεί από κάποιον από τους αντιπροσώπους (1) ή προορίζεται για απευθείας τοπική επεξεργασία από τον εξυπηρετητή (0). Η σημαία E (από το Error) δηλώνει ότι κάποιο σφάλμα υπάρχει στο μήνυμα(1). Η σημαία T δηλώνει ότι το μήνυμα αυτό δύναται να επανα-μεταδοθεί σε ένα εναλλακτικό fail-over δίαυλο ή/και χρησιμοποιείται για αφαίρεση διπλότυπων μηνυμάτων.



Σχήμα 8 Flags εντολών [6]

- **Κωδικός εντολής**: 24 bit. Δηλώνει την εντολή με την οποία είναι συσχετισμένο το συγκεκριμένο μήνυμα. Η συσχέτιση ενός κωδικού με μια εντολή καθορίζεται και ελέγχεται από την Internet Assigned Numbers Authority IANA. Κάθε μήνυμα πρέπει να περιέχει έναν κώδικα εντολής ώστε ο παραλήπτης να είναι ικανός να γνωρίζει τον τρόπο ερμηνείας του περιεχομένου του μηνύματος. Τα μηνύματα αιτήσεων/αποκρίσεων χρησιμοποιούν τον ίδιο κωδικό, ωστόσο διαφοροποιούνται μεταξύ τους από το σχετικό flag, όπως σημειώνεται παραπάνω. Τα μηνύματα αιτήσεων έχουν ενεργοποιημένο το flag R στο πεδίο των flags, ενώ των αποκρίσεων όχι. Υπάρχει πλήθος μηνυμάτων καθορισμένων στο βασικό πρωτόκολλο ενώ υπάρχει επίσης δυνατότητα προσθήκης νέων κωδικών, συγκεκριμένων κάθε φορά για μία εφαρμογή. Χαρακτηριστικό παράδειγμα οι κωδικοί εντολών για τις υπηρεσίες αυθεντικοποίησης και εξουσιοδότησης, που ορίζονται στις προδιαγραφές της εφαρμογής NAS. Οι κωδικοί εντολών του βασικού πρωτοκόλλου περιγράφονται στον πίνακα 2.
- **Ταυτότητα εφαρμογής**: 32 bit. Προσδιορίζει την εφαρμογή για την οποία προορίζεται το μήνυμα π.χ. υπηρεσία αυθεντικοποίησης, λογιστικής καταγραφής ή άλλης εφαρμογής.
- **Προσδιοριστής hop-by-hop**: 32 bit. Περιέχει τον προσδιοριστή που χρησιμοποιείται για να συνδέονται μεταξύ τους τα μηνύματα αιτήσεων με αυτά των αποκρίσεων. Ο αποστολέας πρέπει να εξασφαλίσει ότι ο προσδιοριστής είναι μοναδικός στη γραμμή επικοινωνίας μεταξύ δύο κόμβων. Ο προσδιοριστής hop-by-hop που υπάρχει σε κάθε μήνυμα χρησιμοποιείται για την αναφορά των εξερχόμενων μηνυμάτων κάθε κόμβου. Ωστόσο, αυτό ενδέχεται να προκαλέσει τη λήψη διπλότυπων μηνυμάτων από ένα κόμβο. Για το λόγο αυτό ο κόμβος υποχρεούται να χρησιμοποιεί το συνδυασμό του end-to-end προσδιοριστή και της ιδιότητας Original-Host, ώστε να αναγνωρίζει μοναδικά ένα μήνυμα που προέρχεται από ένα συγκεκριμένο κόμβο Diameter.
- **Προσδιοριστής από άκρο-σε-άκρο**: 32 bit. Μεταφέρει τον προσδιοριστή που χρησιμοποιείται για να εντοπίζονται τα διπλότυπα μηνύματα. Ο προσδιοριστής σε ένα μήνυμα απόκρισης πρέπει να είναι ο ίδιος με αυτόν που περιείχε το μήνυμα αίτησης με το οποίο συνδέεται. Ο προσδιοριστής πρέπει να είναι τοπικά μοναδικός για τουλάχιστον τέσσερα λεπτά. Ο προσδιοριστής αυτός και η ιδιότητα Origin-Host, χρησιμοποιούνται από κοινού για την ανίχνευση των διπλότυπων μηνυμάτων.

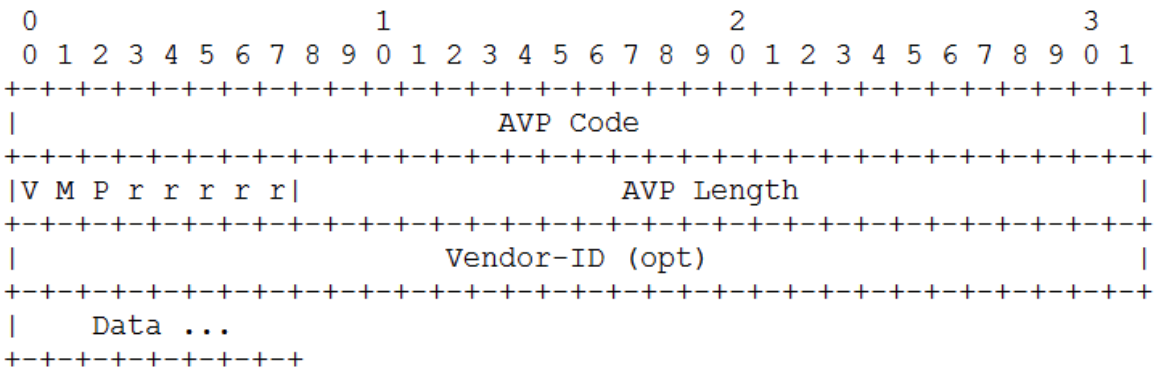
Πίνακας 4 Κωδικοί εντολών όπως προδιαγράφονται στο βασικό πρωτόκολλο του Diameter

Τύπος	Σύντμηση	Κωδικός	Περιγραφή
Abort-Session-Request	ASR	274	Αποστέλλεται από τον εξυπηρετητή στο NAS για τον τερματισμό μία συνοδού η οποία ορίζεται από το Session-Id
Abort-Session-Answer	ASA	274	
Accounting-Request	ACR	271	Αποστέλλεται από ένα κόμβο Diameter που λειτούργει ως πελάτης προκειμένου να ανταλλαχτούν πληροφορίες λογιστικής καταγραφής με ένα άλλο κόμβο
Accounting-Answer	ACA	271	
Capabilities-Exchange-Request	CER	257	Ανίχνευση της ταυτότητα και των δυνατοτήτων ενός κόμβου όπως οι υποστήριξη εφαρμογών Diameter, μηχανισμών ασφάλειας κ.α.
Capabilities-Exchange-Answer	CEA	257	
Device-Watchdog-Request	DWR	280	Αποστέλλεται από έναν κόμβο σε άλλο όταν μεταξύ των δύο δεν έχουν αποσταλεί μηνύματα
Device-Watchdog-Answer	DWA	280	
Disconnect-Peer-Request	DPR	282	Αποστέλλεται από ένα κόμβο σε άλλο προκειμένου να πληροφορηθεί ο δεύτερος για την πρόθεση του πρώτου να κλείσει τη σύνδεση
Disconnect-Peer-Answer	DPA	282	
Re-Auth-Request	RAR	258	Αποστέλλεται από ένα εξυπηρετητή στο NAS, ώστε να ζητήσει επανάληψη της αυθεντικοποίησης ή/και εξουσιοδότησης ενός χρήστη
Re-Auth-Answer	RAA	258	
Session-Termination-Request	STR	275	Αποστέλλεται από το NAS στον εξυπηρετητή, εκ μέρους του χρήστη, δηλώνοντας την πρόθεση του να τερματίσει τη σύνοδο
Session-Termination-Answer	STA	275	

4.2.2 Δομή ιδιότητας

Όπως και στο RADIUS, το κύριο τμήμα ενός πακέτου Diameter είναι αυτό που περιέχει τις ιδιότητες. Ωστόσο, η δομή μιας ιδιότητας είναι διαφορετική από ότι στο RADIUS. Στο σχήμα 9 φαίνονται διαγραμματικά τα πεδία που περιέχει μία ιδιότητα.

- Κωδικός ιδιότητας (AVP code): 32 bit. Ο κωδικός αυτός προσδιορίζει τον τύπο των πληροφοριών που περιέχονται στην ιδιότητα. Οι κωδικοί αυτοί είναι εκ των προτέρων αυστηρά καθορισμένοι και ελεγχόμενοι από την Internet Assigned Number Authority (IANA). Γενικά προτείνεται οι νέες εφαρμογές να χρησιμοποιούν τους υφιστάμενους κωδικούς στο μέγιστο δυνατό βαθμό. Σημειώνεται ότι οι κωδικοί 1-255 είναι δεσμευμένοι προς αντίστοιχη χρήση με αυτών του RADIUS, προκειμένου να διατηρείται η συμβατότητα με αυτό.



Σχήμα 9 Δομή ιδιότητας στο Diameter [6]

- Flags: 8 bit. Το V bit (από το Vendor) δηλώνει εάν το προαιρετικό πεδίο Vendor-ID υπάρχει στο συγκεκριμένο μήνυμα. Το M bit (από το Mandatory = υποχρεωτικό) υποδεικνύει αν ένας κόμβος Diameter απαιτεί ο συνομιλητής του να υποστηρίζει τη συγκεκριμένη ιδιότητα ώστε να επεξεργαστεί το μήνυμα. Εάν ένας κόμβος λάβει μία ιδιότητα με το M bit στην κατάσταση «αληθές» αλλά δεν μπορεί να αναγνωρίσει την ιδιότητα ή την τιμή της, τότε απορρίπτει το μήνυμα που φέρει την ιδιότητα αυτή. Η τιμή του M bit καθορίζεται βάσει των κανόνων που ορίζονται για μία συγκεκριμένη ιδιότητα. Το P bit υποδεικνύει την ανάγκη κρυπτογράφησης του περιεχομένου για ασφάλεια από άκρο σε άκρο. Το βασικό πρωτόκολλο ορίζει ποιες ιδιότητες πρέπει να προστατεύονται με από άκρο-σε-άκρο ασφάλεια με χρήση κρυπτογράφησης (εάν φυσικά οι συνδέσεις μεταξύ των κόμβων δεν είναι σημείο-προς-σημείο αλλά μεσολαβούν κι άλλοι κόμβοι-αντιπρόσωποι). Εάν δεν έχει εξασφαλιστεί η από άκρο-σε-άκρο ασφάλεια ενός μηνύματος, τότε αυτό δεν αποστέλλεται. Επίσης, υπάρχουν ακόμη 5 bit τα οποία δεσμεύονται για μελλοντική χρήση.
- Μέγεθος ιδιότητας: 24 bit. Δηλώνει το μέγεθος του της ιδιότητας σε bytes περιλαμβάνοντας τα πεδία Κώδικας ιδιότητας, Μέγεθος, Flags, το προαιρετικό πεδίο Ταυτότητα κατασκευαστή και τα δεδομένα της Ιδιότητας.
- Ταυτότητα κατασκευαστή (προαιρετικό): 32 bit. Ειδικό πεδίο που χρησιμοποιείται για ιδιότητες που έχουν δημιουργηθεί από κάποιον κατασκευαστή. Περιέχει την τιμή SMI Network Management Private Enterprise Codes που καθορίζεται από την IANA.

4.2.3 Ταυτότητα Diameter

Κάθε διεργασία Diameter που εκτελείται σε ένα κόμβο δημιουργεί ή είναι από πριν παραμετροποιημένη με μία ταυτότητα Diameter. Η ταυτότητα αυτή είναι μία συμβολοσειρά

σύνταξης Uniform Resource Identifier (URI) [26] που αναπαριστά το πλήρες όνομα του τομέα της (Fully Qualified Domain Name), τις πύλες επικοινωνίας του πρωτοκόλλου μεταφοράς στις οποίες «ακούει» για εισερχόμενες συνδέσεις, το πρωτόκολλο μεταφοράς (TCP/SCTP), το πρωτόκολλο AAA και ενδεχομένως την ασφάλεια που παρέχεται στο επίπεδο μεταφοράς (π.χ. TLS). Για παράδειγμα:

aaa://host.aegean.gr:1812; transport=tcp; protocol=diameter

Η πληροφορία που μεταφέρει η ταυτότητα (πλήρες όνομα διεργασίας) σε συνδυασμό με την μοναδική πύλη (port) που χρησιμοποιεί μια εφαρμογή, έχει ως αποτέλεσμα την μοναδικότητα της ταυτότητας Diameter για κάθε εφαρμογή.

4.2.4 Διαπραγμάτευση δυνατοτήτων (Capabilities exchange)

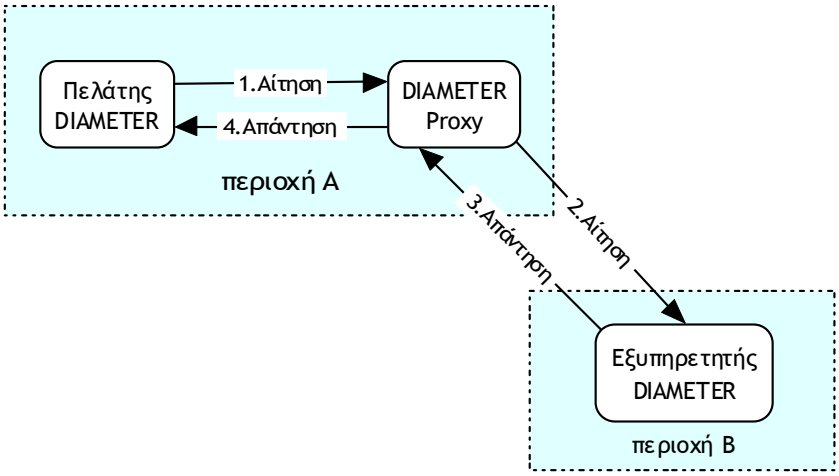
Τα πρώτα μηνύματα που ανταλλάσσονται μεταξύ δύο κόμβων στο Diameter, μετά την εγκαθίδρυση της σύνδεσης, είναι τα μηνύματα Διαπραγμάτευσης δυνατοτήτων. Ένα τέτοιο μήνυμα μεταφέρει την ταυτότητα και τις δυνατότητες ενός κόμβου (έκδοση πρωτοκόλλου, υποστηριζόμενες εφαρμογές Diameter κτλ). Ένας κόμβος μεταδίδει μόνο τις εντολές εκείνες για τις οποίες ο παραλήπτης κόμβος έχει προηγούμενα δηλώσει ότι μπορεί να χειριστεί. Περιληπτικά, οι κόμβοι Diameter ανταλλάσσουν μηνύματα μόνο για τις εφαρμογές που υποστηρίζουν.

4.2.5 Τύποι κόμβων στο Diameter

Στην υποδομή ενός συστήματος Diameter, υπάρχει πλήθος τύπων κόμβων που διαδραματίζουν σημαντικό ρόλο στην αξιοπιστία και ασφάλεια του πρωτοκόλλου. Οι ρόλοι αυτοί καθορίζονται στο βασικό πρότυπο του Diameter και συνεπώς είναι υποχρεωτική η υλοποίηση τους από όλες τις εφαρμογές/συσκευές. Το Diameter λειτουργεί βάσει ενός μοντέλου που δανείζεται χαρακτηριστικά από το μοντέλο ομότιμων κόμβων (Peer-To-Peer), και αυτό του πελάτη-εξυπηρετητή. Η διαφοροποίηση από το μοντέλο που εφαρμόζει το RADIUS, είναι ότι ο εξυπηρετητής πέραν του χειρισμού των αιτήσεων που λαμβάνει από τον πελάτη, μπορεί κι ίδιος να αποστείλει μηνύματα αιτήσεων για να ζητήσει συγκεκριμένες πληροφορίες από τους πελάτες. Όταν αναφερόμαστε σε κόμβο Diameter αυτός μπορεί να είναι ένας πελάτης, εξυπηρετητής ή αντιπρόσωπος όπως θα δούμε παρακάτω.

- Πελάτης: Ο πελάτης στο Diameter είναι μία δικτυακή συσκευή που εγκαθίσταται στα όρια ενός δικτύου και πραγματοποιεί έλεγχο πρόσβασης. Χαρακτηριστικό παράδειγμα τέτοιας συσκευής είναι, όπως και στο RADIUS, ο Network Access Server ή το Σημείο Πρόσβασης (Access Point) στα ασύρματα δίκτυα του προτύπου IEEE 802.11.

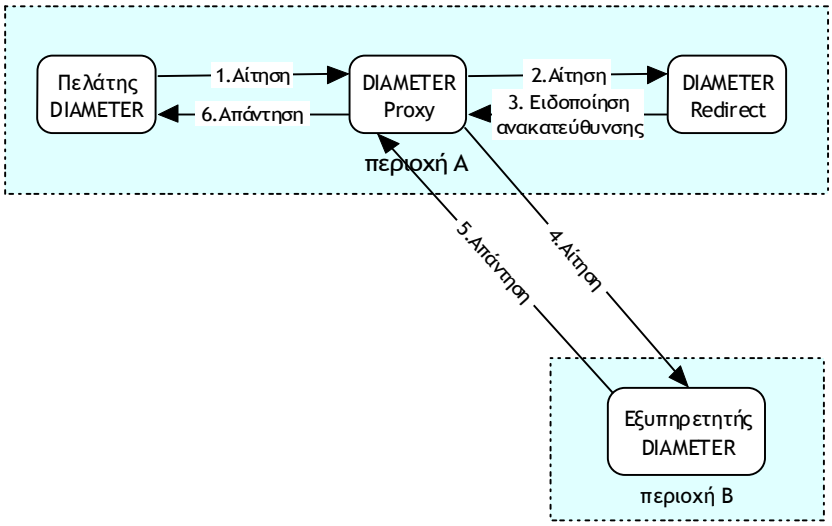
- Εξυπηρετητής: Ο εξυπηρετητής Diameter είναι το κεντρικό υπολογιστικό σύστημα που διαχειρίζεται τις αιτήσεις αυθεντικοποίησης, εξουσιοδότησης και λογιστικής καταγραφής σε μία συγκεκριμένη διαχειριστική περιοχή (network realm).



Σχήμα 10 Επικοινωνία Diameter με χρήση πληρεξούσιου αντιπρόσωπου κόμβου

- Αντιπρόσωπος αναμετάδοσης (Relay Agent): Δρομολογεί τα Diameter μηνύματα βάσει των πληροφοριών που υπάρχουν σε αυτά. Η απόφαση δρομολόγησης λαμβάνεται αφού πρώτα συμβουλευτεί τη λίστα των γνωστών κόμβων και περιοχών. Η λειτουργία των αντιπροσώπων αναμετάδοσης είναι κατά κανόνα διαφανής στους συμμετέχοντες κόμβους. Ο αντιπρόσωπος αναμετάδοσης ενδέχεται να τροποποιήσει ένα μήνυμα μόνο σε ό,τι αφορά την πληροφορία δρομολόγησης, κι όχι στο υπόλοιπο περιεχόμενο του.
- Πληρεξούσιος αντιπρόσωπος (Proxy Agent): Δρομολογεί τα μηνύματα Diameter όπως ο αντιπρόσωπος αναμετάδοσης, και επιπλέον έχει τη δυνατότητα τροποποίησης αυτών ώστε να εφαρμόζει τις κατάλληλες πολιτικές, όπως τον έλεγχο χρήσης πόρων (σχήμα 10).
- Αντιπρόσωπος ανακατεύθυνσης (Redirect Agent): Και αυτός ο αντιπρόσωπος διαθέτει ικανότητες δρομολόγησης μηνυμάτων Diameter. Ωστόσο, και συγκριτικά με τους υπόλοιπους, ο αντιπρόσωπος ανακατεύθυνσης μπορεί να δημιουργεί και να αποστέλλει ο ίδιος μηνύματα. Ο αντιπρόσωπος ανακατεύθυνσης επιστρέφει ένα ειδικό τύπο μηνύματος στον κόμβο που απέστειλε την αίτηση. Το μήνυμα αυτό εμπεριέχει πληροφορίες δρομολόγησης που επιτρέπουν τον κόμβο να στείλει ξανά την αίτηση του από άλλο μονοπάτι

άμεσα στο σωστό προορισμό. Ο αντιπρόσωπος ανακατεύθυνσης δεν αναμεταδίδει αιτήσεις (σχήμα 11).

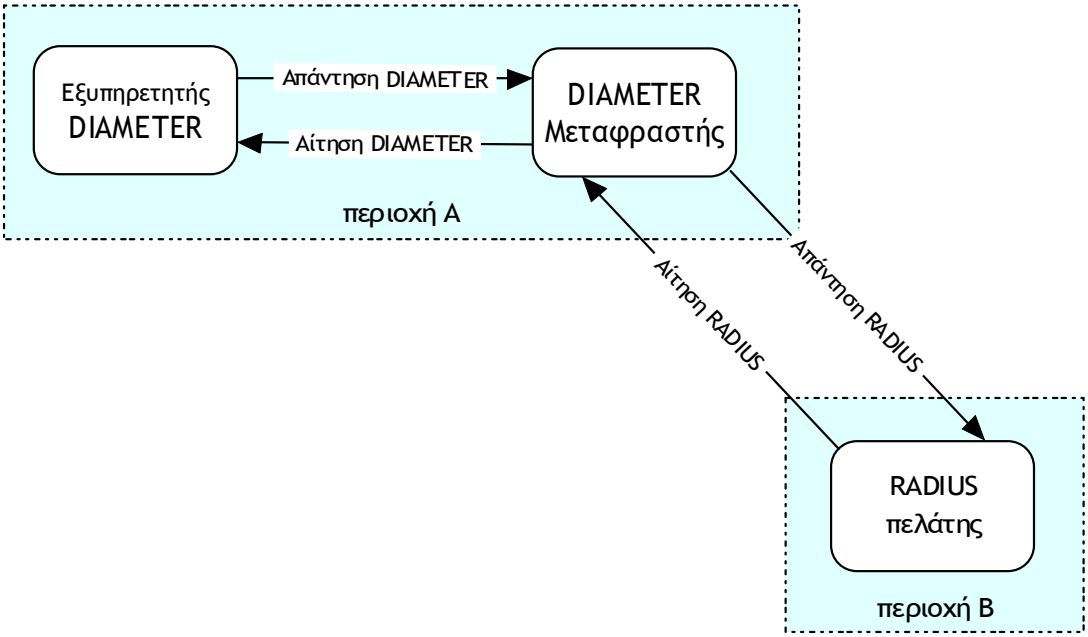


Σχήμα 11 Επικοινωνία Diameter με χρήση πληρεξούσιου και αντιπρόσωπου κόμβου ανακατεύθυνσης.

- Αντιπρόσωπος μετάφρασης (Translation Agent): Μεταφράζει τα μηνύματα μεταξύ 2 πρωτοκόλλων AAA, συνήθως μεταξύ RADIUS και Diameter. Η διαδικασία της μετάφρασης γίνεται ώστε να υποστηριχτεί η λειτουργία συσκευών που εκτελούν το πρωτόκολλο RADIUS σε ένα περιβάλλον με Diameter εξυπηρετητές. Με άλλα λόγια είναι χρήσιμη ώστε να ομαλοποιηθεί η περίοδος μετάβασης από το ένα πρωτόκολλο στο άλλο (σχήμα 12).

4.2.6 Δυναμική ανίχνευση ομότιμων κόμβων

Στο πρωτόκολλο RADIUS προκειμένου να πραγματοποιηθεί η σύνδεση και επικοινωνία μεταξύ πελάτη-εξυπηρετητή έπρεπε αρχικά να ρυθμιστούν χειροκίνητα οι συσκευές με το όνομα ή τη διεύθυνση των δικτυακών συσκευών και επιπλέον να εισαχθεί ο κοινός μυστικός κωδικός επικοινωνίας. Το Diameter χρησιμοποιώντας το πρωτόκολλο DNS [33] επιτυγχάνει δυναμική ανίχνευση των κόμβων.



Σχήμα 12 Επικοινωνία Diameter RADIUS με χρήση αντιπρόσωπου κόμβου μετάφρασης

4.2.7 Δρομολόγηση μηνυμάτων

Η διαδικασία δρομολόγησης πακέτων στις προδιαγραφές του RADIUS δεν είναι ξεκάθαρη και κατά συνέπεια οδηγεί σε διαφορετικές υλοποιήσεις. Αντίθετα στο Diameter η δρομολόγηση πακέτων μεταξύ διαφορετικών περιοχών προδιαγράφεται με μεγάλη ακρίβεια. Στη δρομολόγηση μηνυμάτων συμμετέχουν διαφορετικές συσκευές με ξεχωριστό ρόλο η κάθε μία, όπως περιγράφηκαν παραπάνω. Για να πραγματοποιείται η δρομολόγηση μηνυμάτων μεταξύ διαφορετικών περιοχών διαχωριστικής αρμοδιότητας οι κόμβοι Diameter διατηρούν κατά τη λειτουργία τους δυο πινάκες δρομολόγησης:

- Πίνακας κόμβων (peer table): Ο πίνακας χρησιμοποιείται στην προώθηση μηνυμάτων. Κάθε κόμβος Diameter διατηρεί τον πίνακα κόμβων που περιλαμβάνει καταχωρήσεις για καθένα από τους γνωστούς του κόμβους. Κάθε καταχώρηση στον πίνακα περιέχει πληροφορίες για την ταυτότητα του κόμβου, το αν έχει ανιχνευτεί δυναμικά ή είναι προϊόν χειροκίνητης προσθήκης, και τέλος το χρόνο λήξης της καταχώρησης (στην περίπτωση που έχει ανιχνευτεί δυναμικά).
- Πίνακας δρομολόγησης περιοχών (realm-based routing table): Οι αντιπρόσωποι κόμβοι του Diameter συμβουλεύονται τον εν λόγω πίνακα ώστε να προωθήσουν ένα μήνυμα στον

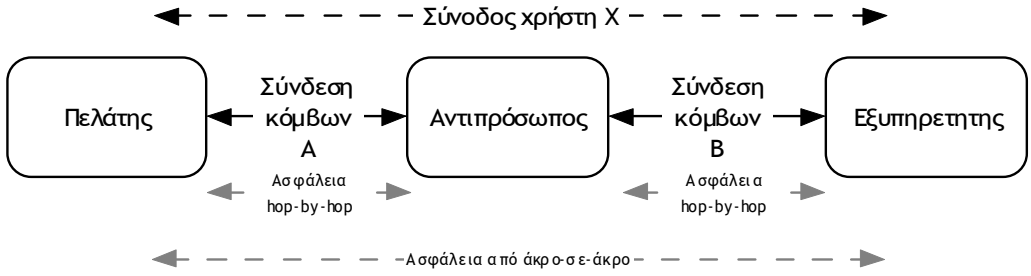
τελικό προορισμό του ή στον επόμενο αντιπρόσωπο που ενδεχομένως βρίσκεται σε διαφορετική περιοχή. Ο πίνακας περιέχει τα εξής στοιχεία: Όνομα περιοχής, πεδία προσδιοριστών εφαρμογής, περιοχή εκτέλεσης επεξεργασίας (προσδιορίζει το αν το μήνυμα θα επεξεργαστεί τοπικά, προωθηθεί στον επόμενο κόμβο ή θα ανακατευθυνθεί στον εξυπηρετητή), προσδιοριστής εξυπηρετητή, στατική ή δυναμική ανίχνευση και χρόνος λήξης της δεύτερης.

4.2.8 Σύνδεση και σύνοδος

Στο πρωτόκολλο Diameter ορίζονται οι έννοιες της σύνδεσης και της συνόδου προκειμένου να καθίσταται σαφής η λειτουργία των κόμβων στους διαφορετικούς ρόλους που αυτοί δύναται να έχουν.

- «Σύνοδος» είναι μία λογική έννοια στο επίπεδο εφαρμογής και εγκαθιδρύεται από άκρο-σε-άκρο μεταξύ μιας συσκευής και ενός εξυπηρετητή. Μία σύνοδος προσδιορίζεται από την ιδιότητα ταυτότητα συνόδου (session ID AVP) και μπορεί να εγκαθιδρύεται πάνω σε πολλαπλές συνδέσεις.
- Με τον όρο «Σύνδεση» εννοούμε τη φυσική σύνδεση στο επίπεδο μεταφοράς μεταξύ δύο κόμβων που ανταλλάσσουν μηνύματα Diameter.

Στο σχήμα 13 παρουσιάζονται διαγραμματικά οι έννοιες σύνοδος και σύνδεση στο πρωτόκολλο Diameter.



Σχήμα 13 Σύνδεση και σύνοδος στο Diameter

4.2.9 Το πρωτόκολλο επιπέδου μεταφοράς Stream Control Transmission Protocol (SCTP)

Το Diameter σε αντίθεση με το RADIUS βασίζεται και λειτουργεί πάνω σε ένα αξιόπιστο πρωτόκολλο επιπέδου μεταφοράς που παρέχει έλεγχο ροής, επιβεβαίωση λήψης πακέτων και χρήση επανα-μεταδόσεων. Σύμφωνα με το βασικό πρωτόκολλο Diameter, οι κόμβοι που λειτουργούν ως

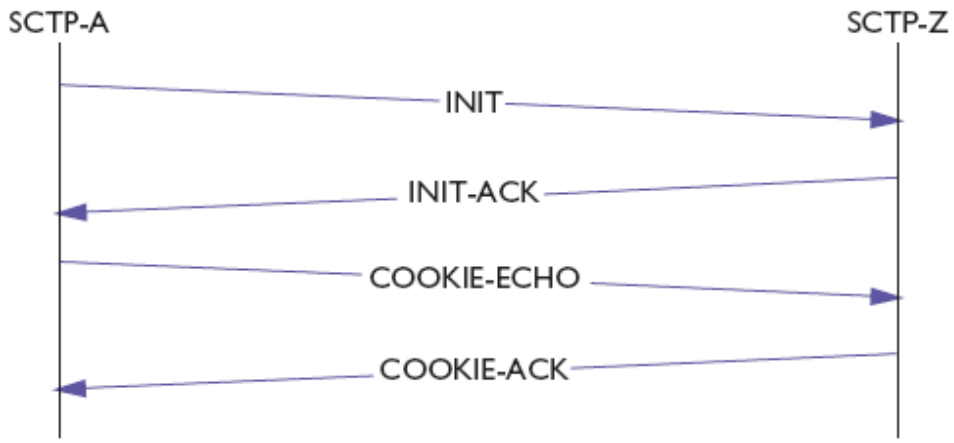
πελάτες Diameter υποχρεούνται να υποστηρίζουν είτε το TCP ή το SCTP ως πρωτόκολλο επιπέδου μεταφοράς ενώ οι αντιπρόσωποι και οι εξυπηρετητής θα πρέπει να υποστηρίζουν ταυτόχρονα και τα δύο. Το SCTP [46-47] δημιουργήθηκε από τις προσπάθειες της ομάδας εργασίας Signaling Transport (Sigtrans) της IETF και προοριζόταν ως το εξειδικευμένο πρωτόκολλο επίπεδου μεταφοράς για υποστήριξη των μηνυμάτων σηματοδοσίας σε δίκτυα Voice over IP (VoIP). Το SCTP, όπως το TCP, προσφέρει υπηρεσίες αξιόπιστης μεταφοράς δεδομένων σε point-to-point επικοινωνία για εφαρμογές που λειτουργούν επάνω από το IP πρωτόκολλο. Κληρονομεί πολλά από το βασικά χαρακτηριστικά του TCP όπως ο έλεγχος συμφόρησης, και η ανάκτηση «χαμένων» πακέτων. Επιπλέον, οι εφαρμογές που λειτουργούν επάνω από το TCP μπορούν πολύ εύκολα να μετατραπούν ώστε να χρησιμοποιούν το SCTP ως το πρωτόκολλο επιπέδου μεταφοράς. Το SCTP προσφέρει κάποια νέα χαρακτηριστικά όπως το multihoming, επιλογή του τρόπου μεταφοράς των πακέτων σχετικά με την τήρηση σειράς (order of arrival), αντιμετώπιση DoS επιθέσεων κ.α.. Στην παράγραφο αυτή αναλύουμε τα πλέον σημαντικά χαρακτηριστικά του πρωτόκολλου SCTP που μπορούν να βρουν εφαρμογή στο πρωτόκολλο Diameter. Για περισσότερες πληροφορίες ο αναγνώστης παραπέμπεται στα [46-47].

- Multihoming: Το πρωτόκολλο υποστηρίζει συνόδους πολλαπλών διεπαφών δικτύου (interfaces) με διαφορετικές IP διευθύνσεις, προκειμένου να παρέχονται, διαφανώς στον χρήστη, υπηρεσίες failover μεταξύ εναλλακτικών διαδρομών δικτύου. Κατά τη διάρκεια αρχικοποίησης του SCTP, οι συμμετέχοντες κόμβοι ανταλλάσουν λίστες με τις χρησιμοποιούμενες IP διευθύνσεις τους. Στην περίπτωση ανίχνευσης αδυναμίας αποστολής στην προεπιλεγμένη IP διεύθυνση, τα πακέτα μπορούν να δρομολογούνται σε άλλο προορισμό, δίχως να επηρεάζεται η σύνοδος στο επίπεδο μεταφοράς. Η λειτουργία αυτή χρησιμοποιείται μόνο για τον σκοπό της αξιοπιστίας μετάδοσης (redundancy) και όχι για τον καταμερισμό του φόρτου μεταδιδόμενων δεδομένων.
- Επιλογή ταξινομημένης αποστολής-λήψης πακέτων: Το TCP εφαρμόζει αυστηρά τη σειριακή λήψη και επανασύνδεση των πακέτων ενώ το UDP δεν ενδιαφέρεται για τη σειρά λήψης (unordered delivery) . Το SCTP επιτρέπει την επιλογή του τρόπου παράληψης και επανασύνδεσης των πακέτων χρησιμοποιώντας μιαν εκ των τριών διαθέσιμων επιλογών. Επιπλέον με τις μεθόδους που χρησιμοποιούνται στα TCP και UDP, ορίζεται η μερική ή κατ' επιλογή χρήση της ταξινομημένης επανασύνδεσης (partially ordered) των πακέτων.
- Αντιμετώπιση DoS επιθέσεων: Για να μετριαστεί η ευπάθεια του TCP σε επιθέσεις DoS (επίθεση SYN flooding), χρησιμοποιείται ο ένας μηχανισμός ασφάλειας cookie κατά την

αρχικοποίηση ενός συσχετισμού[3] SCTP. Πριν την εγκαθίδρυση ενός συσχετισμού, οι κόμβοι ανταλλάσουν μηνύματα που περιλαμβάνουν την τηλεπικοινωνιακή τους κατάσταση καθώς και τις IP διευθύνσεις των διεπαφών που διαθέτουν. Η διαδικασία αποτελείται από τέσσερα βήματα (four way handshake) και καταπολεμά την ευπάθεια της 3μερους χειραψίας του TCP (three way handshake). Η διαδικασία περιγράφεται στο σχήμα 14.

Η διαφορά με το TCP, είναι ότι ο παραλήπτης του μηνύματος αίτησης σύνδεσης (INIT), δεν χρειάζεται να δεσμεύσει πόρους για την επικείμενη σύνδεση ή να διατηρήσει κάποιες πληροφορίες για την κατάσταση του συσχετισμού. Αντίθετα, αποκρίνεται με ένα μήνυμα INIT-ACK, ενός ψηφιακά υπογεγραμμένου cookie που περιλαμβάνει όλες τις απαραίτητες πληροφορίες που χρειάζεται προκειμένου να εισέρθει σε κατάσταση επίτευξης συσχετισμού (ESTABLISHED). Ο αιτούμενος του συσχετισμού, επιστρέφει το cookie που έλαβε αποστέλλοντας το μήνυμα COOKIE-ECHO το οποίο έχει ως αποτέλεσμα την τροποποίηση της κατάστασης του παραλήπτη και την εγκαθίδρυση του συσχετισμού. Το τελικό μήνυμα (COOKIE-ACK) της χειραψίας πληροφορεί τον αποστολέα για την επιτυχημένη εγκαθίδρυση συσχετισμού.

Περισσότερες πληροφορίες και λεπτομέρειες για την τετραμερή χειραψία του SCTP μπορεί κάνεις να αναζητήσει εδώ [29].



Σχήμα 14 Εγκαθίδρυση συσχετισμού με τη χειραψία τεσσάρων σταδίων στο SCTP [46]

[3] Στην ορολογία του SCTP ένας συσχετισμός αναφέρεται σε μια σύνδεση μεταξύ δυο κόμβων η όποια περιλαμβάνει περισσότερες της μιας διεπαφής δικτύου με διαφορετική IP διεύθυνση.

4.2.10 Διαχείριση σφαλμάτων

Τα σφάλματα στο Diameter διαχωρίζονται σε δύο επιμέρους κατηγορίες, στα σφάλματα πρωτοκόλλου και αυτά των εφαρμογών. Τα σφάλματα πρωτοκόλλου σχετίζονται με κάποιο λάθος στα υποκείμενα πρωτόκολλα μεταφοράς, όπως εσφαλμένη πληροφορία δρομολόγησης ή αστοχία δικτύου. Τα σφάλματα εφαρμογών είναι αποτέλεσμα μιας αποτυχίας του ίδιου του πρωτοκόλλου Diameter, και υπάρχει πληθώρα περιπτώσεων που μπορεί να ανιχνευτεί ένα σφάλμα. Για παράδειγμα εάν σε ένα μήνυμα δεν υπάρχει μία υποχρεωτική ιδιότητα για ένα συγκεκριμένη εντολή Diameter, τότε επιστρέφεται ένας κωδικός σφάλματος Diameter_MISSING_AVP. Κάθε μήνυμα απόκρισης περιέχει το πεδίο Result-Code AVP, με το οποίο ο παραλήπτης μπορεί να ελέγξει εάν το προηγούμενο μήνυμα που απεστάλη αναγνωρίστηκε με επιτυχία. Για να ανιχνεύσει μία αποτυχημένη προσπάθεια σύνδεσης το Diameter ορίζει τα μηνύματα Device-Watchdog-Request. Όταν δύο κόμβοι δεν ανταλλάσσουν μεταξύ τους μηνύματα για ένα συγκεκριμένο χρονικό διάστημα, τα μηνύματα αυτά αποστέλλονται από τους κόμβους ώστε να ανιχνεύουν πιθανά προβλήματα δικτύου. Το πρωτόκολλο Diameter χρησιμοποιεί την ίδια κωδικοποίηση σφαλμάτων όπως το πρωτόκολλο Hypertext Transfer (HTTP) . Αυτό σημαίνει ότι η κατάσταση των απεσταλμένων μηνυμάτων μπορεί να προσδιοριστεί εύκολα εξετάζοντας το πρώτο ψηφίο του κώδικα επιστροφής.

- 1xxx: η αίτηση δεν γίνεται δεκτή και απαιτούνται επιπλέον πληροφορίες για χορηγηθεί άδεια χρήσης για τη συγκεκριμένη υπηρεσία
- 2xxx: Η αίτηση έχει διεκπεραιωθεί με επιτυχία
- 3xxx: Έχει ανιχνευτεί ένα σφάλμα πρωτοκόλλου κατά τη μετάδοση του μηνύματος.
- 4xxx: Η αίτηση δεν μπορεί να διεκπεραιωθεί τη δεδομένη στιγμή αλλά ενδέχεται να γίνει σε σύντομο χρονικό διάστημα. Αυτό συμβαίνει εάν ο εξυπηρετητής δεν έχει αρκετό αποθηκευτικό χώρο ώστε να επεξεργαστεί τις αιτήσεις.
- 5xxx: Υπάρχει ένα σφάλμα εφαρμογής κατά την επεξεργασία της αίτησης από τον εξυπηρετητή. Ο αποστολέας δεν πρέπει να στείλει ξανά το μήνυμα αίτησης αλλά να προσδιορίσει και να διορθώσει το σφάλμα εξετάζοντας τον κωδικό του.

Εκτός του κωδικού επιστροφής Return-Code AVP, ο αποστολέας μπορεί επίσης να ελέγξει άλλες ιδιότητες που φέρουν επιπλέον πληροφορίες για τη διαχείριση σφαλμάτων. Το Error-Message AVP μεταφέρει μηνύματα σφαλμάτων σε κοινή γλώσσα (human readable error messages) και χρησιμοποιείται για να προσδιοριστεί ο ακριβής σκοπός της δημιουργίας σφάλματος. Το Error-Reporting-Host AVP περιέχει την ταυτότητα του κόμβου που δημιούργησε το Result-Code. Η συγκεκριμένη ιδιότητα είναι πολύ χρήσιμη για επίλυση προβλημάτων και εντοπισμού του

προβληματικού σημείου. Το Failed-AVP περιέχει την ομάδα των ιδιοτήτων που προκαλούν το πρόβλημα.

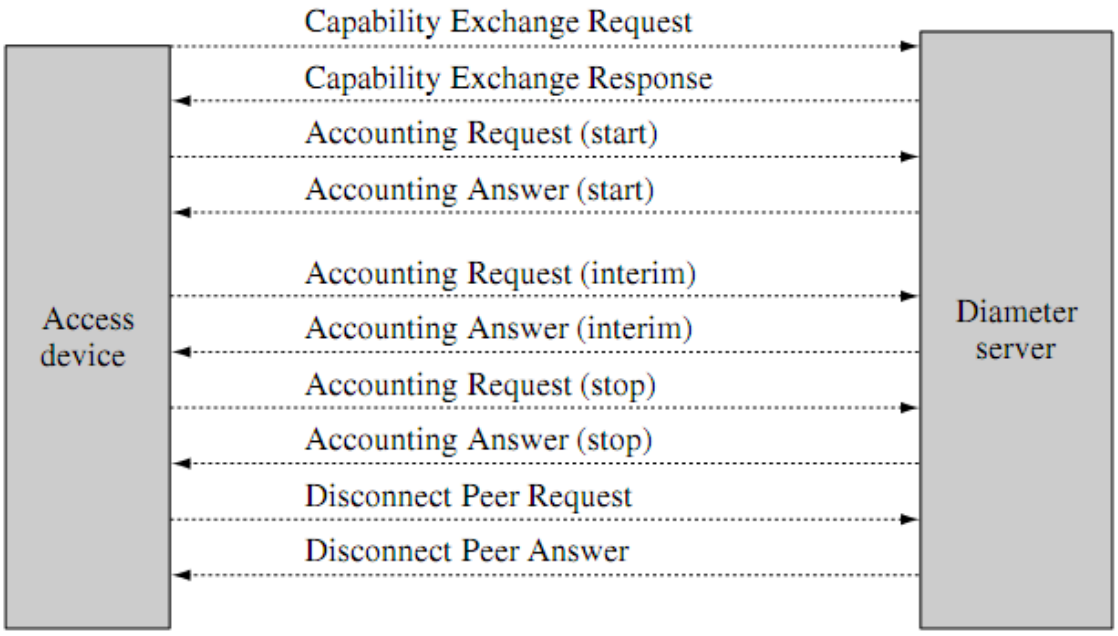
4.2.11 Διαδικασίες Fail-over /Fail-back

Μετά την ανίχνευση ενός σφάλματος, ο αποστολέας προωθεί όλα τα προς αποστολή μηνύματα σε ένα εναλλακτικό κόμβο Diameter. Η διαδικασία αυτή καλείται Failover. Εκκρεμή προς αποστολή μηνύματα θεωρούνται εκείνα τα οποία έχουν σταλεί σε πρώτη φάση αλλά δεν έχει επιστραφεί επιβεβαίωση επιτυχούς λήψης από τον έτερο κόμβο-συνομιλητή. Επίσης, απαίτηση του πρωτοκόλλου είναι κάθε κόμβος να διατηρεί τοπικά ένα αντίγραφο των εξερχόμενων μηνυμάτων του προκειμένου να υπάρχει δυνατότητα επανάληψης της αποστολής μετά από σφάλμα.

Ένα κόμβος Diameter περιοδικά ελέγχει την κατάσταση της αρχικής σύνδεσης με τον κόμβο επιχειρώντας να εγκαθιδρύσει μια νέα σύνδεση. Εάν αυτό επιτευχθεί τότε ο κόμβος δρομολογεί ξανά όλα τα μηνύματα του στον αρχικό κόμβο-παραλήπτη (failback κατάσταση).

4.2.12 Υπηρεσία λογιστικής καταγραφής

Η υπηρεσία λογιστικής καταγραφής στο πρωτόκολλο Diameter προδιαγράφεται ως τμήμα του βασικού πρωτοκόλλου (σε αντίθεση με το RADIUS που προδιαγράφεται σε ξεχωριστό RFC). Το πρωτόκολλο λογιστικής καταγραφής βασίζεται σε ένα μοντέλο που υποστηρίζει πραγματικού χρόνου παράδοση των πληροφοριών λογιστικής καταγραφής. Το μοντέλο αυτό είναι πλήρως διαχειριζόμενο από τον εξυπηρετητή. Αυτό σημαίνει ότι οι συσκευές που δημιουργούν τις πληροφορίες λογιστικής καταγραφής δέχονται οδηγίες από τον εξυπηρετητή σχετικά με το τρόπο και το χρόνο παράδοσης αυτών των πληροφοριών βάσει συγκεκριμένων απαιτήσεων. Η ομαδική αποστολή μηνυμάτων λογιστικής καταγραφής δεν αποτελεί απαίτηση στο πρωτόκολλο Diameter και κατά συνέπεια δεν υποστηρίζεται. Ωστόσο, και παρότι η επεξεργασία των μηνυμάτων λογιστικής καταγραφής γίνεται ανά ένα από τον εξυπηρετητή, η ομαδική αποστολή μπορεί να επιτευχθεί χάρις τους μηχανισμούς των υποκείμενων πρωτοκόλλων επιπέδου μεταφοράς. Μία τυπική ανταλλαγή μηνυμάτων λογιστικής καταγραφής απεικονίζεται στο σχήμα 15.



Σχήμα 15 Ανταλλαγή μηνυμάτων λογιστικής καταγραφής στο Diameter [34]

4.2.13 Απαιτήσεις ασφάλειας Diameter

Το βασικό πρωτόκολλο Diameter προϋποθέτει ότι η ανταλλαγή των μηνυμάτων γίνεται ασφαλώς χρησιμοποιώντας τα πρωτόκολλα IPsec ή TLS. Τα πρωτόκολλα IPsec και TLS θεωρούνται θεμέλιοι λίθοι στην παρεχομένη ασφάλεια του πρωτοκόλλου. Οι Diameter πελάτες, όπως είναι οι δικτυακές συσκευές NAS, πρέπει υποχρεούνται εκ του προτύπου να υποστηρίζουν το πρωτόκολλο IPsec και προαιρετικά το TLS. Οι εξυπηρετητές Diameter υποχρεούνται να υλοποιούν και τα δύο πρωτοκόλλα ασφάλειας. Γενικά θεωρείται απαραίτητη προϋπόθεση για τη δημιουργία σύνδεσης μεταξύ δύο κόμβων η παροχή ασφάλειας στα χαμηλότερα επίπεδα μεταφοράς. Εάν δεν υπάρχει υποστήριξη για κανένα από τα δύο πρωτόκολλα τότε η ανταλλαγή μηνυμάτων μεταξύ κόμβων περιορίζεται μόνο στην ανταλλαγή των δυνατοτήτων που αυτοί υποστηρίζουν.

Όταν χρησιμοποιείται το πρωτόκολλο TLS, ένα κόμβος αρχικοποιεί τη σύνδεση έχοντας το ρόλο του πελάτη TLS ενώ ο έτερος κόμβος που αποδέχεται τη σύνδεση λειτουργεί ως εξυπηρετητής TLS. Οι δύο κόμβοι επιδεικνύουν την υποστήριξη τους στο TLS χρησιμοποιώντας την ιδιότητα Inband-Security-ID. Μετά την ανταλλαγή των μηνυμάτων δυνατοτήτων οι κόμβοι ξεκινούν τη χειραψία TLS. Προκειμένου να επιτευχθεί η σύνδεση, είναι απαραίτητη η αμοιβαία αυθεντικοποίηση μεταξύ των κόμβων. Ο κόμβος που λειτουργεί ο εξυπηρετητής TLS αιτείται του κόμβου-πελάτη TLS

να του χορηγήσει το πιστοποιητικό του. Προκειμένου να λειτουργήσει το σύστημα ανταλλαγής πιστοποιητικών είναι απαραίτητο οι κόμβοι να έχουν εμπιστοσύνη στις αρχές έκδοσης των πιστοποιητικών.

Όλοι οι κόμβοι Diameter πρέπει υποχρεωτικά να υλοποιούν το πρωτόκολλο IPsec σε transport mode χρησιμοποιώντας τους αλγόριθμους κρυπτογράφησης και αυθεντικοποίησης ώστε να παρέχεται εμπιστευτικότητα και αυθεντικοποίηση όλων των μεταδιδομένων μηνυμάτων. Επίσης πρέπει να υποστηρίζονται οι μηχανισμοί αποτροπής replay επιθέσεων που διαθέτει το IPsec. Επιπρόσθετα, το Diameter, προδιαγράφει ως υποχρεωτική τη χρήση του Internet Key Exchange (IKE) για την αυθεντικοποίηση των κόμβων, τη διαχείριση κλειδιών, και τη διαπραγμάτευση των συσχετισμών ασφάλειας του IPsec.

Σημειώνεται ότι οι παραπάνω μηχανισμοί ασφάλειας είναι αποδεκτοί σε περιβάλλοντα όπου όλοι οι συμμετέχοντες στην επικοινωνία κόμβοι θεωρούνται έμπιστοι. Σε κάθε άλλη περίπτωση είναι αναγκαία η από άκρο-σε-άκρο ασφάλεια και γι' αυτό το λόγο προτείνεται η χρήση της εφαρμογής CMS.

4.4 Το προφίλ μεταφοράς

Σύμφωνα με τους σχεδιαστές του Diameter, το πρωτόκολλο βασίζεται σε δύο θεμελιώδη σύνολα προδιαγραφών. Το ένα είναι το βασικό πρωτόκολλο Diameter, όπως ήδη αναφέρθηκε στην προηγούμενη ενότητα, ενώ το άλλο είναι το προφίλ μεταφοράς [4]. Στο προφίλ μεταφοράς περιγράφονται οι σχέσεις ενός πρωτοκόλλου AAA και του υποκείμενου επιπέδου μεταφοράς.

4.5 Εφαρμογές Diameter

4.5.1 Η εφαρμογή NAS

Όπως περιγράφηκε στο κεφάλαιο 3, πρωταρχικός στόχος του RADIUS είναι η παροχή απομακρυσμένης πρόσβασης ενός χρήστη σε ένα δίκτυο του παρόχου υλοποιώντας μεθόδους για την αυθεντικοποίηση και εξουσιοδότηση των χρηστών. Το βασικό πρωτόκολλο Diameter δεν προδιαγράφει τις υπηρεσίες αυθεντικοποίησης και εξουσιοδότησης αλλά τις «αναθέτει» σε ξεχωριστές εφαρμογές. Η εφαρμογή που λειτουργεί ως αντικαταστάτης του RADIUS είναι η Network Access Server (NAS) [7] .

Η εφαρμογή NAS προσδιορίζει το σύνολο των εντολών προς το χρήση από τις υπηρεσίες αυθεντικοποίησης και εξουσιοδότησης. Η εφαρμογή μπορεί να χρησιμοποιηθεί σε συνεργασία με ποικίλες μεθόδους αυθεντικοποίησης όπως PAP, CHAP, και EAP. Κατά το μέτρο του δυνατού, η

εφαρμογή χρησιμοποιεί τις υπάρχουσες ιδιότητες όπως ορίζονται στο RADIUS προκειμένου να μεταφέρονται τα δεδομένα. Με αυτόν τον τρόπο γίνεται πιο εύκολη η μετάβαση από τις υπάρχουσες εγκατεστημένες εφαρμογές RADIUS στο Diameter. Επιπλέον, απαιτούνται λιγότεροι πόροι για την επεξεργασία των μηνυμάτων από τους αντιπροσώπους μετάφρασης (translation agents) του Diameter ώστε να πραγματοποιείται η απρόσκοπτη συνεργασία μεικτών συστημάτων ταυτόχρονα (RADIUS/Diameter). Η εφαρμογή NAS περιλαμβάνει 3 επιμέρους τμήματα. Στο πρώτο από αυτά καθορίζονται οι κωδικοί εντολών και οι ιδιότητες Diameter κατά αντιστοιχία αυτών που ισχύουν στο RADIUS (χάρη συμβατότητας με παλαιότερες συσκευές που το χρησιμοποιούν). Το δεύτερο τμήμα περιλαμβάνει τους κωδικούς εντολών και τις ιδιότητες Diameter που χρησιμοποιούνται από το πρωτόκολλο EAP. Στο τρίτο τμήμα εμπεριέχονται οι ιδιότητες που χρησιμοποιούνται για τη εξουσιοδότηση διαφόρων υπηρεσιών που παρέχονται από το σύστημα.

Η εφαρμογή NAS περιγράφει μία εφαρμογή Diameter που χρησιμοποιείται για την παροχή υπηρεσιών AAA σε Point-to-Point Protocol (PPP) /SLIP dial-up περιβάλλοντα. Ο συνδυασμός της εφαρμογής NAS με το βασικό πρωτόκολλο που περιγράφηκε παραπάνω ικανοποιεί τις απαιτήσεις των προδιαγραφών AAA NASREQ.

4.5.2 Η εφαρμογή Cryptographic Message Syntax (CMS)

Στην παράγραφο 4.2.13 περιγράφηκαν οι απαιτήσεις ασφάλειας του βασικού πρωτοκόλλου Diameter, οι οποίες εξασφαλίζουν την ασφαλή επικοινωνία μεταξύ των κόμβων. Η υποχρεωτική υλοποίηση του IPsec και η προαιρετική του TLS προσφέρει σημαντικό επίπεδο ασφάλειας όσο αφορά την εμπιστευτικότητα και ακεραιότητα των μηνυμάτων Diameter με ένα σημαντικό περιορισμό. Η ασφάλεια της επικοινωνίας περιορίζεται στο επίπεδο μεταφοράς και δεν περιλαμβάνει το επίπεδο εφαρμογής. Όπως έχει ήδη ειπωθεί, σε ένα σύστημα Diameter ορίζονται ποικίλοι ρόλοι για του κόμβους, οι οποίοι συμμετέχουν σε μία σύνοδο μεταξύ πελάτη και εξυπηρετητή. Μία σύνοδος αποτελείται όμως από επιμέρους συνδέσεις μεταξύ των κόμβων.

Σχήμα 16 Ασφάλεια από άκρο-σε-άκρο έναντι hop-by-hop

Ανάμεσα στα δύο αυτά άκρα (πελάτης-εξυπηρετητής), υπάρχουν ενδιάμεσοι σταθμοί-κόμβοι, οι οποίοι προωθούν τα πακέτα στο σωστό προορισμό. Η διασφάλιση της επικοινωνίας με τα πρωτόκολλα IPsec/TLS γίνεται hop-by-hop, δηλαδή στην επικοινωνία μεταξύ δυο κόμβων. Για να έχει νόημα η χρήση των πρωτοκόλλων αυτών, θεωρείται ότι όλοι οι ενδιάμεσοι κόμβοι είναι έμπιστοι. Η ανάπτυξη εμπιστοσύνης για τους ενδιάμεσους κόμβους είναι βασική προϋπόθεση για την ασφάλεια από άκρο-σε-άκρο και ορίζεται ρητά στο βασικό πρωτόκολλο. Τι γίνεται όμως στην περίπτωση που ένας ή περισσότεροι κόμβοι δεν θεωρούνται έμπιστοι; Σε αυτή την περίπτωση είναι αναγκαία η καθολική και από-άκρο-σε-άκρο προστασία της επικοινωνίας Diameter. Για το σκοπό αυτό προτείνεται η χρήση της εφαρμογής CMS.

Η εφαρμογή CMS παρέχει από άκρο-σε-άκρο αυθεντικοποίηση, ακεραιότητα, εμπιστευτικότητα και μη απάρνηση στο επίπεδο εφαρμογής ή καλύτερα στο επίπεδο της ιδιότητας. Κάνοντας χρήση ψηφιακών υπογραφών ή/και κρυπτογράφησης μπορούν να προστατεύουν κατ΄ επιλογή συγκεκριμένοι τύποι «ευαίσθητων» ιδιοτήτων. Οι υπόλοιπες, δίχως προστασία, ιδιότητες μπορούν να τροποποιηθούν, διαγράφουν, προστεθούν κατά βούληση από τους ενδιάμεσους σε μία επικοινωνία Diameter κόμβους (π.χ. πληρεξούσιοι αντιπρόσωποι). Η εφαρμογή CMS χρησιμοποιεί δύο τεχνικές για την επίτευξη του επιθυμητού επιπέδου ασφάλειας. Με τη χρήση των ψηφιακών υπογραφών και πιστοποιητικών παρέχονται αυθεντικοποίηση, ακεραιότητα και μη αποποίηση (non repudiation) των μηνυμάτων, ενώ η εμπιστευτικότητα πραγματοποιείται με τη κρυπτογράφηση του περιεχομένου των ιδιοτήτων. Στο έγγραφο προδιαγραφών της εφαρμογής CMS περιγράφεται το πόσο ισχυρή μπορεί να είναι η αυθεντικοποίηση και κρυπτογράφηση χρησιμοποιώντας την εφαρμογή στο Diameter. Επίσης, καθορίζονται τα μηνύματα και οι ιδιότητες που χρησιμοποιούνται προκειμένου να εγκαθιδρυθεί ένας συσχετισμός ασφάλειας μεταξύ δυο κόμβων Diameter, καθώς και τις ιδιότητες που θα χρησιμοποιηθούν για να μεταφέρουν τα προς μετάδοση δεδομένα.

Δυστυχώς μέχρι σήμερα η εφαρμογή CMS δεν έχει προτυποποιηθεί και βρίσκεται ακόμη στη φάση του draft.

5 Συγκριτική αξιολόγηση των πρωτοκόλλων RADIUS και Diameter

Μετά την επιμέρους παρουσίαση των πρωτοκόλλων RADIUS και Diameter που επιχειρήθηκε στα προηγούμενα κεφάλαια, παρουσιάζεται στο παρόν μια συγκριτική προσέγγισή τους. Η σύγκριση χρησιμοποιεί διάφορες παραμέτρους δηλαδή γίνεται υπό το πρίσμα της εγγενούς ασφάλειας και αξιοπιστίας στη μετάδοση των μηνυμάτων, της επεκτασιμότητας και της ευελιξίας αλλά της μεταξύ τους συμβατότητας. Επίσης, αναλύονται ζητήματα σχετικά με τις διαχειριστικές ικανότητες των πρωτοκόλλων σε περιβάλλοντα με μεγάλο αριθμό συμμετεχόντων υπολογιστικών συστημάτων (scalability), αλλά και της γενικότερης ευχρηστίας του κάθε πρωτοκόλλου.

Τα υπολογιστικά μηχανήματα που εμπλέκονται και διαχειρίζονται τις υπηρεσίες AAA, γίνονται συχνά στόχοι επιθέσεων από κακόβουλους χρήστες λόγω του νευραλγικού ρόλου που διαδραματίζουν στη λειτουργία συστημάτων που υποστηρίζουν. Κατά συνέπεια είναι μείζονος σημασίας θέμα το κατά πόσον το πρωτόκολλο AAA είναι εξοπλισμένο με τέτοιους μηχανισμούς ασφάλειας που αποτρέπουν πιθανές επιθέσεις, αλλά και μη εσκεμμένα λάθη ή παραλείψεις από εξουσιοδοτημένους χρήστες. Επίσης, σημαντικό σημείο στη σύγκριση των πρωτοκόλλων είναι οι μηχανισμοί μεταφοράς των πακέτων που χρησιμοποιούν αυτά. Φυσικά αυτό εξαρτάται σε μεγάλο βαθμό από το υποκείμενο πρωτόκολλο επιπέδου μεταφοράς που χρησιμοποιεί το εκάστοτε πρωτόκολλο AAA.

Ένα απαραίτητο στοιχείο που πρέπει να διαθέτει σήμερα ένα σύγχρονο πρωτόκολλο AAA είναι δυνατότητα επεκτασιμότητας του για χρήση από τυχόν υπηρεσίες που θα προκύψουν μελλοντικά. Το RADIUS για παράδειγμα στις πρώτες του εκδόσεις (drafts) δεν περιείχε προδιαγραφές για την υπηρεσία λογιστικής καταγραφής. Αργότερα, όταν θεωρήθηκε απαραίτητη η ενσωμάτωση της υπηρεσίας στο πρωτόκολλο, πραγματοποιήθηκε αυτή η προσθήκη της επιπλέον λειτουργικότητας χάρις στις δυνατότητες επέκτασης που το χαρακτηρίζει.

Το RADIUS λειτουργεί στη βάση του μοντέλου πελάτη-εξυπηρετητή, όπου το ρόλο του πελάτη διαδραματίζει η δικτυακή συσκευή στην οποία συνδέονται οι τελικοί χρήστες. Ο εξυπηρετητής RADIUS δεν αποστέλλει μηνύματα αιτήσεων παρά μόνο αποκρίνεται στα μηνύματα που λαμβάνει από τους πελάτες. Το RADIUS είναι ένα stateless πρωτόκολλο και οι κόμβοι που το υλοποιούν δεν διατηρούν παρά ελάχιστες πληροφορίες σχετικά με την κατάσταση των συνδέσεων. Ένα χαρακτηριστικό παράδειγμα διατήρησης πληροφοριών σύνδεσης είναι το πεδίο Προσδιοριστής που χρησιμοποιείται για το συσχετισμό μηνυμάτων αίτησης με των αντιστοιχών αποκρίσεων. Το Diameter επίσης χρησιμοποιεί το μοντέλο πελάτη-εξυπηρετητή, ωστόσο διαφοροποιείται στο γεγονός ότι οι εξυπηρετητές μπορούν να αποστείλουν κι ίδιοι μηνύματα αιτήσεων για περάτωση

συγκεκριμένων λειτουργιών (π.χ. η επανάληψη της διαδικασίας αυθεντικοποίησης / εξουσιοδότησης). Έτσι, μπορεί να υποστηριχθεί πως το μοντέλο λειτουργίας του Diameter ομοιάζει εν μέρει με το μοντέλο peer to peer (P2P). Επιπλέον, οι κόμβοι του Diameter διατηρούν περισσότερες πληροφορίες σύνδεσης κατά τη λειτουργία τους, ενώ διαχωρίζονται οι έννοιες της σύνδεσης και συνόδου.

Το Diameter είναι ο επίσημος αντικαταστάτης ενός πολύ επιτυχημένου και ιδιαίτερα διαδεδομένου πρωτοκόλλου γι' αυτό προκειμένου η μετάβαση να γίνει το δυνατόν ομαλότερα, υλοποιεί κάποιους μηχανισμούς και τεχνικές που το καθιστούν εν μέρει συμβατό με το RADIUS.

5.1 Ανάγκη δημιουργίας νέου AAA πρωτοκόλλου

Η ανάγκη ύπαρξης ενός νέου πρωτόκολλο AAA προήρθε από τη δημιουργία νέων υπηρεσιών που απαιτούσαν υπηρεσίες AAA. Οι νέες υπηρεσίες έφεραν και επιπλέον απαιτήσεις από το πρωτόκολλο AAA, που το RADIUS δεν ήταν κατάλληλα σχεδιασμένο να καλύπτει. Για να πληρωθεί αυτό το κενό στο πρωτόκολλο, οι σχεδιαστές του, δηλαδή η αρμόδια ομάδα εργασίας της IETF, αναγκαζόταν να δημιουργεί και να δημοσιεύει βελτιώσεις (patches) που προσέθεταν την επιπλέον απαιτούμενη λειτουργικότητα Το αρχικό πρότυπο του πρωτοκόλλου δεν μπορούσε να μεταβληθεί, αφού μία επιπλέον απαίτηση της ομάδας εργασίας ήταν η διατήρηση συμβατότητας με τις υφιστάμενες δικτυακές συσκευές που το χρησιμοποιούσαν. Αυτό είχε ως αποτέλεσμα τη δημιουργία πλήθους συμπληρωματικών προτύπων προς το αρχικό, προκειμένου το RADIUS να παραμένει σύγχρονο στις τρέχουσες απαιτήσεις τις εποχής. Το πλήθος των επιπρόσθετων βελτιώσεων είχε αντίκτυπο στη ομοιογένεια των υλοποιήσεων του RADIUS, αφού δεν τηρούνταν πάντα όλα τα δημοσιευμένα πρότυπα της IETF από όλους τους κατασκευαστές υλισμικού / λογισμικού. Φαινόταν πως το ίδιο το γεγονός της συνεχούς υποστήριξης του RADIUS με επιπλέον λειτουργίες, αποτελούσε τροχοπέδη στην αποδοτική ικανοποίηση των απαιτήσεων των νέων εφαρμογών. Ήταν διάχυτη δηλαδή η εντύπωση ότι χρειαζόταν ένα νέο πρωτόκολλο AAA που θα αντικαθιστούσε το RADIUS.

5.2 Δομικά χαρακτηριστικά των πρωτοκόλλων

Το Diameter δεν αποτέλεσε ένα καθολικά νέο πρωτόκολλο αλλά βασίστηκε εν μέρει στο RADIUS. Κατά συνέπεια, υπάρχουν αρκετές ομοιότητες αλλά και ουσιαστικές διαφορές μεταξύ των πρωτοκόλλων.

5.2.1 Δομή των πακέτων

Η βασική δομή των πακέτων είναι ίδια και στα δύο πρωτόκολλα. Αποτελούνται από μία επικεφαλίδα σταθερού μήκους ακολουθούμενη από μεταβλητό αριθμό ιδιοτήτων, τις γνωστές και ως Attibute Value Pairs (AVPs). Η επικεφαλίδα περιλαμβάνει μόνο βασικές πληροφορίες για τη λειτουργία του πρωτοκόλλου ενώ τα οι υπόλοιπες, εξειδικευμένες πληροφορίες περιέχονται στις ιδιότητες.

Η επικεφαλίδα αποτελείται από το πεδίο Κωδικός που καθορίζει τον τύπο του μηνύματος και το πεδίο Μήκος που περιέχει την τιμή του μεγέθους του πακέτου. Στην επικεφαλίδα του RADIUS υπάρχει επίσης το πεδίο Προσδιοριστής, το οποίο περιέχεται και στο Diameter ως Προσδιοριστής hop-by-hop. Το πεδίο αυτό χρησιμοποιείται για τη συσχέτιση των μηνυμάτων αίτησης με τα αντίστοιχα των αποκρίσεων καθώς και για την ανίχνευση διπλότυπων μηνυμάτων. Στην επικεφαλίδα του RADIUS υπάρχει και το πεδίο Αυθεντικοποιητής για την αυθεντικοποίηση μηνυμάτων, διαδικασία που ήδη αναφέρθηκε στην ενότητα 3.5.1, ενώ μόνο στην επικεφαλίδα ενός πακέτου Diameter περιέχονται τα πεδία Αριθμός Έκδοσης, Ταυτότητα Εφαρμογής, Προσδιοριστής από άκρο-σε-άκρο και το πεδίο των Flags.

Οι ιδιότητες μεταφέρουν όλες τις εξειδικευμένες πληροφορίες. Περιλαμβάνουν τα πεδία Κωδικός ιδιότητας, Μέγεθος και Τιμή της ιδιότητας. Επιπλέον, σε μία ιδιότητα Diameter περιέχονται κάποια Flags και προαιρετικά η Ταυτότητα κατασκευαστή (vendor ID). Μία σημαντική διαφοροποίηση του Diameter είναι το μέγεθος του πεδίου Κωδικός ιδιότητας, το οποίο καταλαμβάνει 32 bit έναντι των 8 που δεσμεύονται σε μία ιδιότητα RADIUS. Αυτό έχει άμεση επίπτωση στις δυνατότητες επεκτασιμότητας του πρωτοκόλλου Diameter, αφού δύναται να οριστεί τεράστιος αριθμός νέων ιδιοτήτων έναντι των μόλις 256 που ορίζονται στο RADIUS. Σημειώνεται ότι η κωδικοποίηση των ιδιοτήτων στο Diameter, για τις πρώτες 256, διατηρείται ως είχε στο RADIUS χάριν συμβατότητας μεταξύ των δύο πρωτοκόλλων.

5.2.2 Αντιπρόσωποι (agents) και πληρεξούσιοι (proxies) κόμβοι

Τόσο το RADIUS αλλά και το Diameter, προβλέπουν τη λειτουργία τρίτων κόμβων στο τηλεπικοινωνιακό μονοπάτι επικοινωνίας μεταξύ πελάτη και εξυπηρετητή. Στην ορολογία του RADIUS αυτοί οι κόμβοι αναφέρονται ως πληρεξούσιοι εξυπηρετητές (proxies) ενώ στο Diameter, όπως αναλυτικά περιγράφηκε στην ενότητα 4.2.5, υπάρχει πληθώρα κόμβων που επιτελούν διαφορετικές λειτουργίες (με τον πληρεξούσιο κόμβο να είναι ένας από αυτούς). Και τα δύο πρωτόκολλα επιτρέπουν τη δημιουργία αλυσίδων από πληρεξούσιους κόμβους. Επίσης, επιτρέπεται ο ενδιάμεσος κόμβος να λειτουργεί είτε ως εξυπηρετητής σε ορισμένα μηνύματα αιτήσεων ή σε αλλά

ως αντιπρόσωπος. Η ειδοποιός διαφορά μεταξύ των πρωτοκόλλων είναι ότι στις προτυποποιήσεις του RADIUS, δεν υπάρχει ακριβής περιγραφή των πληρεξούσιων κόμβων και κατά συνέπεια ενδέχεται να υπάρχουν διαφοροποιήσεις μεταξύ υλοποιήσεων. Αντίθετα, στο βασικό πρωτόκολλο του Diameter υπάρχει λεπτομερής περιγραφή της συμπεριφοράς που πρέπει να έχουν όλα τα είδη των αντιπρόσωπων κόμβων.

5.2.3 Μηνύματα αιτήσεων από τον εξυπηρετητή

Το RADIUS λειτουργεί βάσει του μοντέλου πελάτη-εξυπηρετητή. Ο πελάτης αποστέλλει αιτήσεις και ο εξυπηρετητής αποκρίνεται. Το RADIUS δεν προβλέπει υποστήριξη για αποστολή μηνυμάτων αίτησης από τον εξυπηρετητή προς τους πελάτες. Αντίθετα, η υποστήριξη τέτοιων μηνυμάτων στο Diameter είναι υποχρεωτική. Με αυτόν τον τρόπο επιτρέπεται στον εξυπηρετητή να στείλει ένα μήνυμα αίτησης ώστε να διακόψει την παροχή μιας υπηρεσίας για ένα συγκεκριμένο χρήστη ή να απαιτήσει επανάληψη της διαδικασία αυθεντικοποίησης ή εξουσιοδότησης ενός χρήστη. Για το RADIUS υπάρχει ένα συγκεκριμένο RFC [11], το οποίο προβλέπει την ενσωμάτωση της δυνατότητας αυτής, αλλά η υποστήριξη του είναι προαιρετική.

5.2.4 Απόρριψη μηνυμάτων δίχως ανακοίνωση - μηνύματα σφαλμάτων

Το RADIUS δεν υποστηρίζει μηνύματα σφαλμάτων. Όταν προκύπτει ένα σφάλμα, το RADIUS απλά απορρίπτει το μήνυμα δίχως περαιτέρω επεξεργασία και χωρίς ανακοίνωση στον αποστολέα. Χαρακτηριστικό παράδειγμα είναι τα μηνύματα με άγνωστο Κωδικό μηνύματος, ή τα πακέτα με μέγεθος μικρότερο από αυτό που περιέχεται στην τιμή του πεδίου Μήκος. Αντίθετα, το Diameter έχει σχεδιαστεί με ενσωματωμένο ένα μηχανισμό ανακοίνωσης σφαλμάτων. Τα μηνύματα Diameter απορρίπτονται δίχως ανακοίνωση μόνο όταν αυτή είναι η καλύτερη επιλογή για την επίλυση του προβλήματος. Για παράδειγμα, εάν ένας κόμβος λάβει ένα μήνυμα απόκρισης περισσότερες από μία φορές, τότε τα πλεονάζοντα πακέτα απορρίπτονται δίχως ειδοποίηση.

Στο Diameter υπάρχουν, γενικά, δυο διαφορετικοί τύποι σφαλμάτων. Τα σφάλματα πρωτοκόλλου και τα σφάλματα εφαρμογής. Τα σφάλματα εφαρμογής είναι πληροφοριακά, περιγράφουν μία προσωρινή ή μόνιμη αποτυχία. Η επεξήγηση του σφάλματος περιέχεται στο πεδίο Result-Code AVP. Τα σφάλματα πρωτοκόλλου διαφέρουν από αυτά της εφαρμογής στο γεγονός ότι κάθε αντιπρόσωπος αναμετάδοσης ή πληρεξούσιος[4] που λαμβάνει το εσφαλμένο μήνυμα επιχειρεί να διορθώσει το σφάλμα. Η ένδειξη για την παρουσία σφάλματος πρωτοκόλλου είναι η τιμή ενός συγκεκριμένου flag ελέγχου στην επικεφαλίδα του πακέτου (με τιμή “E”).

[4] Σε μία αλυσίδα αντιπροσώπων

5.2.5 Αυτόκλητες αποσυνδέσεις (unsolicited disconnects)

Στο βασικό πρωτόκολλο του Diameter καθορίζεται μία ομάδα μηνυμάτων τερματισμού συνόδου, που χρησιμοποιούνται στις αυτόκλητες συνδέσεις. Ο εξυπηρετητής Diameter αποστέλλει ένα μήνυμα Session Termination Request στον πελάτη προκειμένου να τερματίσει τη σύνοδο για κάποιο τρέχοντα συνδεδεμένο χρήστη. Ο πελάτης αποκρίνεται με αντίστοιχο μήνυμα επιβεβαίωσης. Το RADIUS δεν διαθέτει μηχανισμό κατ΄ επιλογή διακοπής της συνόδου από τον εξυπηρετητή αφού δεν υποστηρίζονται τέτοιου είδους μηνύματα.

5.2.6 Διαπραγμάτευση δυνατοτήτων

Στο RADIUS ο πελάτης και ο εξυπηρετητής δεν έχουν κάποιο μηχανισμό ώστε να γνωρίζουν τις δυνατότητες του άλλου άκρου σχετικά με τις υποστηριζόμενες ιδιότητες. Επίσης το RADIUS δεν υποστηρίζει μηνύματα σφαλμάτων. Κάτι τέτοιο κάνει πολύ δύσκολη τη διαπραγμάτευση μεταξύ πελάτη και εξυπηρετητή προς μία κοινά χρησιμοποιούμενη υπηρεσία. Αντίθετα το Diameter υποστηρίζει τη διαχείριση σφαλμάτων, τη διαπραγμάτευση ιδιοτήτων καθώς και άλλους τρόπους υπόδειξης υποστήριξης προς μία συγκεκριμένη ιδιότητα.

5.3 Υπηρεσίες AAA

5.3.1 Αυθεντικοποίηση

Και τα δυο πρωτόκολλα χρησιμοποιούν για την υπηρεσία αυθεντικοποίησης Network Access Identifier (NAI) , το πρωτόκολλα CHAP, PAP, και EAP. Σύμφωνα με το RFC3127 [31], και τα δυο πρωτόκολλα πληρούν εξολοκλήρου τις απαιτήσεις για την υπηρεσία αυθεντικοποίησης. Ωστόσο, το RADIUS θέτει κάποιους περιορισμούς. Στην αυθεντικοποίηση με χρήση του πρωτοκόλλου CHAP, υπάρχει μία ευπάθεια ενώ στο PAP οι κωδικοί πρόσβασης προστατεύονται μόνο σε συνδέσεις μεταξύ δύο κόμβων (hop-by-hop προστασία). Η υποστήριξη για το πρωτόκολλο EAP δεν προτυποποιείται στο πρότυπο RADIUS αλλά σε συμπληρωματικά έγγραφα. Παρομοίως, το βασικό πρωτόκολλο Diameter προδιαγράφει υποστήριξη μόνο για το NAI ενώ τα πρωτόκολλα CHAP, PAP, και EAP προδιαγράφονται στην εφαρμογή NAS.

Στο RADIUS μόνο οι πελάτες μπορούν να πραγματοποιήσουν επανάληψη της διαδικασίας αυθεντικοποίησης, αποστέλλοντας σχετικό μήνυμα στον εξυπηρετητή. Ο εξυπηρετητής μπορεί να αιτηθεί έναρξη της διαδικασίας αυθεντικοποίησης αφού δεν προδιαγράφεται η δυνατότητα αποστολής μηνυμάτων αιτήσεων από αυτόν. Αντίθετα, το Diameter υποστηρίζει αυτή τη δυνατότητα, περιλαμβάνοντας δυο νέα ειδικού τύπου μηνύματα, τα Re-Auth-Request και Re-Auth-Answer.

Επιπλέον, το Diameter υποστηρίζει αυθεντικοποίηση δίχως εξουσιοδότηση, ενώ κάτι τέτοιο δεν συμβαίνει στο RADIUS. Ο λόγος είναι ότι το RADIUS απαιτεί πάντα κάποιου είδους διαπιστευτήρια από το χρήστη.

5.3.2 Εξουσιοδότηση

Συμφώνα με το RFC 3127 τα πρωτόκολλα RADIUS και Diameter υποστηρίζουν κάποια στοιχεία σχετικά με την υπηρεσία εξουσιοδότησης, όπως η χρήση κανόνων πρόσβασης, περιορισμούς εξουσιοδότησης και φίλτρα. Κανένα, ωστόσο, πρωτόκολλο δεν καλύπτει όλες τις απαιτούμενες προϋποθέσεις. Το Diameter, όπως και στην περίπτωση της αυθεντικοποίησης, υποστηρίζει την κατά απαίτηση από τον εξυπηρετητή, επανάληψη της διαδικασίας εξουσιοδότησης. Στο RADIUS, η εξουσιοδότηση είναι στενά συνδεδεμένη με την αυθεντικοποίηση, και συνεπώς μοιράζονται κοινά προβλήματα. Στο RADIUS δεν υπάρχει δυνατότητα επανάληψης της διαδικασίας εξουσιοδότησης, όπως και της αυθεντικοποίησης, από αίτημα του εξυπηρετητή.

Μία ακόμη διαφορά μεταξύ των πρωτοκόλλων είναι ότι στο Diameter ο εξυπηρετητής έχει τη δυνατότητα να ζητήσει από τον πελάτη να διακόψει τη σύνοδο ενός χρήστη βάση συγκεκριμένων πολιτικών εξουσιοδότησης (βλέπε ενότητα 5.2.5)

5.3.3 Λογιστική καταγραφή

Τα βασικά χαρακτηριστικά της υπηρεσίας λογιστικής καταγραφής είναι παρόμοια και στα δύο πρωτόκολλα επιτρέποντας την υποστήριξη λογιστικής καταγραφής πραγματικού χρόνου. Αυτό σημαίνει ότι υπάρχει ένας σύγχρονος τρόπος αναφοράς των συμβάντων που ενδιαφέρουν την υπηρεσία λογιστικής καταγραφής και αυτό πραγματοποιείται σε πολύ μικρό χρονικό διάστημα. Επιπλέον, το Diameter υποστηρίζει χρονοσφραγίδες (timestamps) και δυναμική λογιστική καταγραφή[5] . Το RADIUS υποστηρίζει τις ίδιες δυνατότητες με επιπλέον επέκταση του πρωτοκόλλου, όπως περιγράφεται στο έγγραφο[39].

5.3 Αξιοπιστία μετάδοσης

Το RADIUS δεν καθορίζει τον ακριβή τρόπο επαναμετάδοσης πακέτων μετά από αποτυχημένη προσπάθεια αποστολής. Οι προδιαγραφές απλά αναφέρουν, σχετικά με τα μηνύματα αιτήσεων Access-Request, ότι εάν δεν ληφθεί μήνυμα απόκρισης σε ένα προκαθορισμένο χρονικό διάστημα μετά την αποστολή αίτησης, τότε επαναλαμβάνεται η αποστολή για συγκεκριμένο πλήθος προσπαθειών. Κατά συνέπεια, δεν προσδιορίζεται με ακρίβεια ένας μηχανισμός ανίχνευσης

[5] Λογιστική καταγραφή για υπηρεσίες δυναμικής αυθεντικοποίησης και εξουσιοδότησης.

εσφαλμένης αποστολής μηνυμάτων αλλά αυτό αφήνεται στη διακριτική ευχέρεια του κατασκευαστή. Παρομοίως, οι προδιαγραφές του RADIUS δεν περιγράφουν μεθόδους και μηχανισμούς failover, όπου ένας κόμβος-πελάτης μπορεί προσωρινά να αποστέλλει τα μηνύματα αιτήσεων σε ένα εναλλακτικό εξυπηρετητή σε περίπτωση αστοχίας του κυρίου. Συνέπεια όλων αυτών των «χαλαρών» προδιαγραφών είναι η διαφοροποίηση μεταξύ διαφορετικών υλοποιήσεων RADIUS συστημάτων.

Στο Diameter προδιαγράφεται με περισσότερες λεπτομέρειες η συμπεριφορά του πρωτοκόλλου σε περίπτωση αποτυχημένης μετάδοσης μηνυμάτων. Υπάρχει ένας συγκεκριμένος αλγόριθμος αποτυχημένης μετάδοσης που ορίζεται στο AAA Transport Profile, τον οποίο υποχρεούνται να ενσωματώνουν όλες οι υλοποιήσεις του Diameter. Το Diameter διαθέτει δυο ειδικά μηνύματα για την ανίχνευση των σφαλμάτων μετάδοσης (Device-Watchdog-Request, Device-Watchdog-Answer). Επίσης, στο Diameter προδιαγράφονται οι διαδικασίες failover/failback. Η διαδικασία failover είναι πολύ πιο ακριβής από την αντίστοιχη του RADIUS. Οι κόμβοι Diameter υποχρεούνται να διατηρούν μία προσωρινή μνήμη στην οποία αποθηκεύονται τα μηνύματα τα οποία έχουν αποσταλεί αλλά δεν έχει ληφθεί απάντηση για αυτά. Μετά την ανίχνευση μία αποτυχημένης μετάδοσης, τα μηνύματα που υπάρχουν στη μνήμη προωθούνται σε ένα εναλλακτικό κόμβο. Κατά τη διάρκεια αποστολής των μηνυμάτων προς τον εναλλακτικό κόμβο ελέγχεται η κατάσταση της σύνδεσης με τον αρχικό. Στην περίπτωση που επανέλθει κανονικά, τα μηνύματα δρομολογούνται ξανά στον αρχικό τους προορισμό. Η κατάσταση αυτή περιγράφεται ως failback.

Σύμφωνα με το RFC 3127, τόσο το RADIUS αλλά και το Diameter πληρούν εν μέρει τις απαιτούμενες προϋποθέσεις για τους μηχανισμούς failover. Από το Diameter εκλείπουν οι λεπτομέρειες σχετικά με το πώς και το ποτέ γίνεται η διαδικασία failback.

5.3.1 Πρωτόκολλο επιπέδου μεταφοράς

Τα πρωτόκολλα RADIUS και Diameter χρησιμοποιούν διαφορετικά πρωτόκολλα επιπέδου μεταφοράς. Το RADIUS χρησιμοποιεί το UDP, ενώ το Diameter το TCP ή το νεότερο SCTP. Την εποχή της δημιουργίας του RADIUS το UDP θεωρήθηκε καταλληλότερο έναντι του TCP ως πρωτόκολλο για τη μεταφορά πληροφοριών από άκρο σε άκρο. Το UDP είναι ένα χαμηλότερων απαιτήσεων πρωτόκολλο, συγκριτικά με το TCP, και είναι απλούστερη η συγγραφή εφαρμογών για αυτό. Επιπλέον, σχετικά με το RADIUS, είναι πιο απλή η χρήση πολύ-νηματικών εξυπηρετητών που χρησιμοποιούν το UDP. Ωστόσο και αφού το UDP λειτουργεί δίχως να απαιτεί προηγούμενη σύνδεση των δύο άκρων (connectionless), και δεν διαθέτει μηχανισμούς επανα-μετάδοσης των

χαμένων πακέτων, το ίδιο το RADIUS στις υλοποιήσεις του θα πρέπει να προβλέπει τρόπους ανίχνευσης των χαμένων πακέτων. Αυτό υλοποιείται με τη χρήση time-out μετρητών.

Σε αντίθεση των παραπάνω, το Diameter «χτίστηκε» στη βάση ενός αξιόπιστου πρωτοκόλλου μεταφοράς. Το Diameter χρησιμοποιεί είτε το TCP ή το SCTP για τη μεταφορά των πληροφοριών και ως αποτέλεσμα κληρονομεί όλα τα χαρακτηριστικά τους. Ωστόσο, η υλοποίηση τους είναι περισσότερο πολύπλοκη και απαιτεί περισσότερους πόρους κατά τη λειτουργία του πρωτοκόλλου.

5.4 Αποδοτικότητα πρωτοκόλλων

Ένα από κυριότερα προβλήματα του RADIUS και συνάμα λόγος για τη δημιουργία του Diameter είναι ότι δεν το RADIUS δεν συμπεριφέρεται αποδοτικά σε δικτυακά περιβάλλοντα με μεγάλο πλήθος δικτυακών συσκευών-NAS. Το γεγονός της έλλειψης μηχανισμού ελέγχου συμφόρησης από το RADIUS, το καθιστά ακατάλληλο για χρήση σε πληθυσμιακά μεγάλα δικτυακά περιβάλλοντα. Στο RFC του RADIUS [38] αναφέρονται χαρακτηριστικά τα εξής:

«Η πρακτική εφαρμογή του πρωτοκόλλου έχει δείξει ότι όταν χρησιμοποιείται σε μεγάλης κλίμακας συστήματα, υποβαθμίζεται σημαντικά η απόδοση του και παρουσιάζονται απώλειες στα δεδομένα, εν μέρει λόγω του ότι δεν περιλαμβάνει μεθόδους έλεγχου συμφόρησης».

5.4.1 Επικεφαλίδες πρωτοκόλλου

Τόσο το RADIUS και το Diameter περιέχουν το πεδίου προσδιοριστής στην επικεφαλίδα κάθε μηνύματος προκειμένου να συσχετίζονται τα μηνύματα αιτήσεων με τα αντίστοιχα αποκρίσεων. Η διαφορά μεταξύ των πρωτοκόλλων είναι στο RADIUS το πεδίο προσδιοριστής έχει μέγεθος 8 bit, ενώ στο Diameter 32. Αυτό σημαίνει ότι ταυτόχρονα ένας RADIUS εξυπηρετητής μπορεί να συσχετίσει και να επεξεργαστεί μόνο 256 μηνύματα αιτήσεων. Αντίθετα, το μέγεθος των ταυτόχρονων αιτήσεων μπορεί να χειριστεί ένα εξυπηρετητής Diameter ξεπερνά τα 4 δισεκατομμύρια.

Για να ξεπεραστεί αυτό το πρόβλημα στις υλοποιήσεις RADIUS χρησιμοποιείται ένα τέχνασμα. Είναι γνωστό ότι ο προσδιοριστής χρησιμοποιείται για να προσδιορίζει συνδέσεις μεταξύ κόμβων με βάση πέντε χαρακτηριστικά (IP διεύθυνση και αριθμός πύλης πελάτη, UDP, IP διεύθυνση και αριθμός πύλης εξυπηρετητή). Αλλάζοντας τον αριθμό πύλης του πελάτη, αυξάνονται και το πλήθος των ταυτόχρονων συνδέσεων που μπορεί να χειριστεί ο εξυπηρετητής RADIUS. Επιπλέον, το RADIUS εκ των προδιαγραφών του απαιτεί ότι οι τα μηνύματα αιτήσεων που επανα-μεταδίδονται,

και περιέχουν τροποποιήσεις συγκριτικά με το πρώτο πακέτο που απεστάλη ανεπιτυχώς, πρέπει να φέρουν μία καινούρια τιμή στο πεδίο του προσδιοριστή. Αναλογιζόμενοι το γεγονός ότι η πλειονότητα των περιπτώσεων επανα-μετάδοσης πακέτων περιέχουν τροποποιημένα δεδομένα, το πλήθος των δεσμευμένων αριθμών για την τιμή του προσδιοριστή μεγαλώνει περαιτέρω. Αυτό οδηγεί σε ακόμη μικρότερο αριθμό ταυτόχρονων συνδέσεων πελατών με εξυπηρετητή. Στο Diameter δεν υπάρχει αυτό το πρόβλημα αφού ο προσδιοριστής συνόδου είναι πάντα ο ίδιος για κάθε μήνυμα που αποστέλλεται σε μία δεδομένη συνόδου, είτε αποστέλλεται μία η περισσότερες φορές.

5.4.2 Έλεγχος συμφόρησης

Για την αποφυγή συμφόρησης, ο πελάτης δεν θα πρέπει να μεταδίδει πακέτα σε ένα εξυπηρετητή πριν διαπιστώσει με σχετική βεβαιότητα ότι ο αποδέκτης έχει τη δυνατότητα λήψης τους, και το δίκτυο έχει διαθέσιμο εύρος ζώνης για τη μετάδοση τους. Συνεπώς, ο πελάτης πρέπει να ανιχνεύσει σε πρώτη φάση για επάρκεια εύρους ζώνης πριν ξεκινήσει την αποστολή ενός μηνύματος. Αυτό μπορεί να πραγματοποιηθεί εξετάζοντας τα μηνύματα απόκρισης που λαμβάνει από τον εξυπηρετητή και προσαρμόζοντας το ρυθμό αποστολής των πακέτων βάση αυτών των πληροφοριών [4].

Το RADIUS δεν προβλέπει κάποιο μηχανισμό ελέγχου συμφόρησης. Αυτό, όπως ήδη ειπώθηκε, είναι ένας από τους λόγους που το RADIUS κρίνεται ακατάλληλο σε υλοποιήσεις που συμμετέχει μεγάλος αριθμός κόμβων, αφού είναι πιθανή η σημαντική μείωση της απόδοσης του πρωτοκόλλου ή/και η απώλεια δεδομένων [38].

Το Diameter επίσης δεν διαθέτει κάποιο μηχανισμό ελέγχου συμφόρησης ωστόσο χρησιμοποιεί στο υποκείμενο επίπεδο μεταφοράς τα πρωτόκολλα TCP ή SCTP, τα οποία είναι αξιόπιστα. Με αυτόν τον τρόπο αυτό ο έλεγχος συμφόρησης γίνεται στο επίπεδο μεταφοράς κάτι που εγγενώς προσφέρουν τα συγκεκριμένα πρωτόκολλα εν αντιθέσει με το UDP που χρησιμοποιεί το RADIUS. Ωστόσο, η εμβέλεια επίδρασης των μηχανισμών των πρωτοκόλλων TCP και SCTP είναι περιορισμένη. Ο έλεγχος συμφόρησης και ο χρονισμός των πακέτων λειτουργεί με επιτυχία όσο η σύνδεση μεταξύ των κόμβων είναι hop-by-hop, δηλαδή ο πελάτης επικοινωνεί απευθείας με τον εξυπηρετητή δίχως τη μεσολάβηση άλλων κόμβων. Εάν στο μονοπάτι μετάδοσης υπάρχουν κι άλλοι κόμβοι που προωθούν τα μηνύματα στον εξυπηρετητή, τότε ο από άκρο-σε-άκρο συγχρονισμός είναι σχεδόν αδύνατο να πραγματοποιηθεί. Η ύπαρξη κόμβων, όπως οι αντιπρόσωποι αναμετάδοσης (relay agents) ή πληρεξούσιοι (proxies) δημιουργεί δυο ή περισσότερες ξεχωριστές συνδέσεις. Για παράδειγμα, αν μεταξύ ενός πελάτη και ενός εξυπηρετητή τοποθετηθεί ένας πληρεξούσιος αντιπρόσωπος δημιουργείται μία σύνδεση μεταξύ πελάτη-αντιπρόσωπου και μία μεταξύ

αντιπρόσωπου-εξυπηρετητή. Αυτό έχει ως αποτέλεσμα η ροή των δεδομένων να μην γίνεται άμεσα μεταξύ των ακριανών κόμβων και να μην μπορεί να πραγματοποιηθεί χρονισμός των πακέτων (ή αυτός να είναι πολύ δύσκολο να πραγματοποιηθεί με ακρίβεια και αξιοπιστία). Οι αντιπρόσωποι κόμβοι ανακατεύθυνσης επιτρέπουν το χρονισμό μεταφοράς πακέτων αφού δημιουργείται μόνο μία σύνδεση μεταξύ των τελικών κόμβων [4].

5.4.3 Απαίτηση ευθυγράμμισης δεδομένων

Η IETF σε κάθε νέο πρωτόκολλο που προτυποποιεί περιλαμβάνει σε αυτό την απαίτηση ευθυγράμμισης σε τμήματα των 32 bit των προς επεξεργασία δεδομένων. Αυτό συμβαίνει γιατί οι σημερινοί μικροεπεξεργαστές είναι περισσότερο αποδοτικοί όταν επεξεργάζονται τμήματα δεδομένων σε δεσμίδες μήκους 32 bit. Προκειμένου να είναι περισσότερο αποδοτική η διαδικασία επεξεργασίας των μηνυμάτων Diameter, έχει ενσωματωθεί η απαίτηση της τοποθέτησης των πεδίων της επικεφαλίδας αλλά και των ιδιοτήτων σε τμήμα των 32 bit. Αντίθετα, το RADIUS δεν προβλέπει κάτι ανάλογο κι αυτό έχει ως αποτέλεσμα τη χρονική επιβάρυνση κατά την επεξεργασία των πακέτων. Τα δεδομένα των πακέτων RADIUS επεξεργάζονται ανά τμήμα των 8 bit.

5.5 Επεκτασιμότητα

Τα πρωτόκολλα RADIUS και Diameter είναι σχεδιασμένα να είναι επεκτάσιμα ωστόσο το Diameter διαθέτει περισσότερους μηχανισμούς που το κάνουν να είναι περισσότερο ευέλικτο σε μελλοντικές προσθήκες υπηρεσιών. Και στα δυο πρωτόκολλα ο βασικός μηχανισμός με τον οποίο επιτυγχάνεται η επεκτασιμότητα είναι οι ιδιότητες. Νέες υπηρεσίες, εφαρμογές και λειτουργίες μπορούν να υποστηρίζονται από τα πρωτόκολλα AAA, με την κωδικοποίηση νέων ιδιοτήτων. Επίσης, επιτρέπεται η χρήση εξειδικευμένων ιδιοτήτων από τους κατασκευαστές δίχως την ανάγκη προηγούμενης αδειοδότησης από την επιτροπή διαχείρισης των κωδικών αριθμών για τις ιδιότητες. Ο μηχανισμός αυτός για τέτοιες ιδιότητες βασίζεται στη χρήση μία συγκεκριμένης προκαθορισμένης ειδικά για αυτή τη χρήση ιδιότητας. Η ιδιότητα με κωδικό 26, Vendor-Specific, μπορεί να χρησιμοποιείται από όλους τους κατασκευαστές προκειμένου να υλοποιήσουν άμεσα μία συγκεκριμένη λειτουργία. Τα πρώτα 4 bytes του πεδίου τιμή της ιδιότητας προσδιορίζουν τον κατασκευαστή ενώ το υπόλοιπο σώμα της ιδιότητας χρησιμοποιείται για να μεταφέρει τις εξειδικευμένες για την εκάστοτε λειτουργία πληροφορίες. Η δομή των πληροφοριών αυτών καθορίζεται από τον κατασκευαστή. Γενικά, οι ιδιότητες πρέπει να καθορίζονται με προσοχή ώστε να μην επηρεάζουν την κανονική λειτουργία του πρωτοκόλλου. Εάν ένας εξυπηρετητής RADIUS δεν μπορεί να αναγνωρίσει μία εξειδικευμένη ιδιότητας κατασκευαστή, πρέπει να την αγνοήσει.

Το RADIUS είναι σχεδιασμένο να είναι επεκτάσιμο, όταν οι βασικές ιδιότητες δεν προσφέρουν την απαιτούμενη λειτουργικότητα. Αντίθετα, το Diameter δομείται στη λογική της επεκτασιμότητας. Στο βασικό πρωτόκολλο του Diameter προδιαγράφονται μόνο οι λειτουργίες σχετικά με την υπηρεσία λογιστικής καταγραφής. Για όλες τις άλλες χρήσεις (αυθεντικοποίηση, εξουσιοδότηση) το βασικό πρωτόκολλο πρέπει να επεκταθεί με επιπλέον λειτουργικότητα. Στο Diameter υπάρχουν αρκετοί μηχανισμοί που επεκτείνουν το βασικό πρωτόκολλο. Σε αυτούς περιλαμβάνονται η δημιουργία νέων ιδιοτήτων ή ο καθορισμός νέων τιμών για τις ήδη υπάρχουσες, τη δημιουργία νέων εφαρμογών αυθεντικοποίησης κι εξουσιοδότησης ή και λογιστικής καταγραφής.

Σε αντίθεση με τις επεκτάσεις του RADIUS που είναι εξειδικευμένες για τον κατασκευαστή, οι επεκτάσεις του Diameter είναι γενικής χρήσης. Η IANA μεταξύ των άλλων αρμοδιοτήτων της, ελέγχει και την κωδικοποίηση του Diameter σχετικά με τις τιμές των ιδιοτήτων, του τύπους τους καθώς και τους προσδιοριστές εφαρμογών. Για προστεθεί μια νέα καταχώρηση στην υπάρχουσα κωδικοποίηση, ο ενδιαφερόμενος πρέπει πρώτα να αποστείλει σχετική αίτηση στην IANA εξηγώντας την αναγκαιότητα μιας τέτοιας ενέργειας. Η αρμόδια επιτροπή εξετάζει την κάθε περίπτωση και μόνο αφού εγκριθεί η αίτηση μπορεί να χρησιμοποιηθεί ο νέος τύπος. Η επιτροπή προτείνει χάριν απλούστευσης της διαδικασίας προτυποποίησης και ομοιογενείας μεταξύ των υλοποιήσεων του πρωτοκόλλου, να χρησιμοποιούνται κατά το δυνατόν οι υπάρχουσες ιδιότητες.

Ένα σημαντικό σημείο διαφοροποίησης μεταξύ των δυο πρωτοκόλλων είναι το μέγεθος του πεδίου που αναφέρεται ο τύπος της ιδιότητας. Στο RADIUS το πεδίο αυτό έχει μήκος 8 bit επιτρέποντας μόνο 256 διαφορετικές ιδιότητες. Για να καλυφτούν επιπλέον ανάγκες, χρησιμοποιείται ο κωδικός 26, Vendor-Specific. Ωστόσο, με τον τρόπο αυτό η ιδιότητα που θα χρησιμοποιείται δεν θα έχει καθολική ισχύ, παρά μόνο τοπική υπό την έννοια μία συγκεκριμένης υλοποίησης. Στο Diameter το πεδίο τύπος ιδιότητας έχει μήκος 32 bit επιτρέποντας τη δημιουργία και χρήση πάνω από 4 δισεκατομμυρίων καθολικής ισχύος ιδιότητες. Το μέγεθος του πεδίου Τύπος ιδιότητας είναι σημαντικός περιοριστικός παράγοντας για την επεκτασιμότητα του πρωτοκόλλου.

5.6 Συμβατότητα

Η υποστήριξη διαφορετικών εκδόσεων από το πρωτόκολλο RADIUS υποτυπώδης. Οι προδιαγραφές του πρωτοκόλλου αναφέρουν ότι κατά τη λήψη ενός μηνύματος με μη αναμενόμενη τιμή στο πεδίο κωδικός, ο κόμβος πρέπει να απορρίψει το συγκεκριμένο μήνυμα δίχως να το ανακοινώσει στον έτερο συνομιλητή του. Επιπλέον οι ιδιότητες με άγνωστο κωδικό τύπο αγνοούνται ως προς το περιεχόμενο τους. Το RADIUS δεν υποστηρίζει δυνατότητες διαπραγμάτευσης δυνατοτήτων και οι

ιδιότητες του δεν περιλαμβάνουν πληροφορίες για το αν η υποστήριξη σε μία συγκεκριμένη ιδιότητα είναι απαραίτητη. Κατά συνέπεια, οι διαφορετικές εκδόσεις του RADIUS θα είναι συμβατές μεταξύ τους, αρκεί να διατηρείται η ίδια κωδικοποίηση για τα μηνύματα και τις ιδιότητες. Επιπλέον, καθώς το RADIUS δεν υποστηρίζει αναφορά σφαλμάτων, οι συμμετέχοντες κόμβοι που δεν λαμβάνουν απάντηση στις αιτήσεις τους δεν έχουν τρόπο να προσδιορίσουν την αιτία αυτής της συμπεριφοράς. Δηλαδή, αν ο κόμβος έχει απορρίψει το μήνυμα ή υπάρχει κάποιο άλλο πρόβλημα στο δίκτυο, π.χ. συμφόρηση δικτύου και το αρχικό μήνυμα της αίτησης δεν έχει παραληφτεί από το άλλο άκρο.

Το Diameter είναι περισσότερο ώριμο σε θέματα συμβατότητας υποστηρίζοντας εγγενώς τη διαπραγμάτευση δυνατοτήτων, τη διαχείριση σφαλμάτων και κάνοντας χρήση συγκεκριμένων flags ελέγχου στις ιδιότητες. Κάθε φορά που εγκαθιδρύεται μία σύνδεση μεταξύ δύο κόμβων Diameter, αυτοί ανταλλάσσουν μηνύματα Ανταλλαγής Δυνατοτήτων (Capabilities Exchange). Τα μηνύματα αυτά επιτρέπουν τους κόμβους να ανακαλύψουν μεταξύ τους την έκδοση πρωτοκόλλου, τις υποστηριζόμενες εφαρμογές Diameter, τους μηχανισμούς ασφάλειας και άλλα χαρακτηριστικά που υποστηρίζει ο καθένας. Κάθε ιδιότητα στο Diameter περιέχει ένα flag ελέγχου, το λεγόμενο υποχρεωτικό bit (mandatory bit), το οποίο καθορίζει το αν η συγκεκριμένη ιδιότητα απαιτεί απαραίτητα την υποστήριξη της από τον έτερο κόμβο. Όταν ένας κόμβος λάβει ένα μήνυμα με μία υποχρεωτικά υποστηριζόμενη ιδιότητα (το M bit αληθές) την οποία δεν αναγνωρίζει, τότε αποστέλλει πίσω στον αποστολέα μία απάντηση που καθορίζει την ιδιότητα που απέτυχε να αναγνωρίσει.

Η επικεφαλίδα του Diameter περιέχει ένα πεδίο 8 bit που περιέχει την έκδοση του πρωτοκόλλου ενώ για την αντίστοιχη του RADIUS δεν προβλέπεται κάτι τέτοιο. Προς το παρόν υπάρχει μόνο μία έκδοση του Diameter, αλλά δεν αποκλείεται μελλοντικά να προκύψουν κι άλλες.

Η συμβατότητα μεταξύ των πρωτοκόλλων Diameter και RADIUS είναι κάτι το οποίο απασχόλησε τους σχεδιαστές του πρώτου. Το Diameter θεωρείται πως είναι αρκούντως συμβατό με το RADIUS. Για παράδειγμα, η κωδικοποίηση των πρώτων ιδιοτήτων (1-255) του Diameter διατηρείται ως είχε και στο RADIUS. Το ίδιο ισχύει και για την κωδικοποίηση των τύπων μηνυμάτων (0-255). Επιπλέον, για την πιο ομαλή μετάβαση μεταξύ των δύο πρωτοκόλλων, χρησιμοποιείται ένα ειδικός τύπος αντιπρόσωπου κόμβου. Ο αντιπρόσωπος μετάφρασης τοποθετείται μεταξύ ενός πελάτη RADIUS και ενός εξυπηρετητή Diameter με σκοπό τη μετάφραση των πακέτων αιτήσεων και αποκρίσεων στην κατάλληλη δομή για τον κάθε κόμβο, καθώς επίσης και της απενθυλάκωσης και ενθυλάκωσης των πακέτων AAA πρωτοκόλλου στο αντίστοιχο πρωτόκολλο επιπέδου μεταφοράς (RADIUS-UDP, Diameter-TCP/SCTP).

5.6 Ασφάλεια

5.6.1 Αυθεντικοποίηση οντοτήτων

Η αυθεντικοποίηση οντότητας, δηλαδή η επιβεβαίωση της ταυτότητας του έτερου συνομιλητή, προσφέρει προστασία απέναντι σε πολλούς τύπους επιθέσεων. Εξοπλίζει το συνδιαλεγόμενο απέναντι σε επιθέσεις μεταμφίεσης (masquerading), man-in-the-middle, μη εξουσιοδοτημένης πρόσβασης, ενώ ενδεχομένως αποτρέπει και επιθέσεις πλαστογραφήσεις και άρνησης χρήσης υπηρεσίας (denial of service). Η αυθεντικοποίηση των εμπλεκομένων οντοτήτων μπορεί να πραγματοποιείται μεταξύ γειτονικών κόμβων (hop-by-hop), οι οποίοι χρησιμοποιούνται για να προωθήσουν ένα μήνυμα ή από άκρο-σε-άκρο (end-to-end), δηλαδή μεταξύ των δύο τελικών επικοινωνούντων μερών. Η δεύτερη λύση είναι περισσότερο πολύπλοκη να υλοποιηθεί και απαιτεί αφού στο μονοπάτι μεταφοράς των πληροφοριών αυθεντικοποίησης συμμετέχουν κι άλλοι κόμβοι οι οποίοι πολλές φορές δεν είναι έμπιστοι.

5.6.2 Ασφάλεια στο RADIUS

Η αυθεντικοποίηση μηνυμάτων στο πρωτόκολλο RADIUS πραγματοποιείται μόνο μεταξύ δύο γειτονικών κόμβων, μεταξύ δύο κόμβων που έχουν απευθείας τηλεπικοινωνιακή σύνδεση (hop-by-hop). Η αυθεντικοποίηση μηνυμάτων του RADIUS βασίζεται στη χρήση ενός κοινού μυστικού κωδικού, τον οποίο κατέχουν οι συμμετέχοντες στην επικοινωνία κόμβοι. Στο RADIUS χρησιμοποιείται το πεδίο Αυθεντικοποιητής αίτησης κατά την αποστολή μία αίτησης αυθεντικοποίησης και το αντίστοιχο πεδίο Αυθεντικοποιητής απόκρισης κατά την απάντηση από τον εξυπηρετητή. Στην παράγραφο 3.5.1 περιγράφεται λεπτομερώς ο τρόπος χρήσης του πεδίου Αυθεντικοποιητής.

Όταν χρησιμοποιούνται πληρεξούσιου κόμβοι (proxies), τότε κάθε ζεύγος απευθείας συνδεδεμένων κόμβων μπορεί να έχει το δικό μυστικό κωδικό. Κατά τη λήψη ενός μηνύματος Access-Request ο πληρεξούσιος κόμβος αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας τον κοινό μυστικό κωδικό με τον πελάτη και έπειτα το ξανά κρυπτογραφεί με το κοινό μυστικό κωδικό που μοιράζεται με τον εξυπηρετητή και το αποστέλλει σε αυτόν. Στην αντίθετη κατεύθυνση οι πληρεξούσιοι κόμβοι χρειάζεται να υπολογίσουν ξανά τον Αυθεντικοποιητή αυθεντικοποίησης.

Η χρήση αυτού του τρόπου αυθεντικοποίησης και διασφάλισης της ακεραιότητας των μηνυμάτων, προκαλεί αρκετά προβλήματα ασφάλειας. Βασική προϋπόθεση είναι η προστασία των κωδικών κατά τη διάρκεια που βρίσκονται αποθηκευμένοι στη μνήμη των πελατών και εξυπηρετητών από τέτοιου είδους επιθέσεις. Μεγάλη προσοχή πρέπει να δοθεί στον τρόπο

μετάδοσης των κωδικών πρόσβασης, ώστε να εξαλείφει πιθανή αποκάλυψη τους σε μη εξουσιοδοτημένους χρήστες. Ο τρόπος διανομής γίνεται out-of-the-band αφού δεν προδιαγράφεται διαφορετικός τρόπος διαμοιρασμού από το πρωτόκολλο. Οι δυσκολίες αυτές γίνονται περισσότερο ορατές κατά τη χρήση μεγάλου αριθμού συστημάτων, όπου είναι αναγκαία η προστασία και ο διαμοιρασμός πολλών διαφορετικών μυστικών κωδικών. Το διαχειριστικό κόστος μιας τέτοιας υλοποίησης είναι ιδιαίτερα μεγάλο, ενώ πολλές φορές στην προσπάθεια απλούστευσης της διαχείρισης γίνεται χρήση του ίδιου κωδικού για διαφορετικά συστήματα υποβαθμίζονται ακόμη περισσότερο τη συνολική ασφάλεια.

Ακόμη κι αν ληφθούν τα απαραίτητα μέτρα προφύλαξης και οι κατάλληλες μέθοδοι διαμοιρασμού των μυστικών κωδικών στους πελάτες και εξυπηρετητές, έχει αποδειχθεί ότι ο τρόπος υλοποίησης των υποκείμενων μηχανισμών ασφάλειας από το πρωτόκολλο δεν προσφέρει επαρκής ασφάλεια. Επιπλέον, το πρωτόκολλο είναι ευάλωτο σε επιθέσεις λόγω της ίδιας της αδυναμίας των μηχανισμών. Οι ευπάθειες ασφάλειας του RADIUS περιγράφονται παρακάτω.

- Επιθέσεις αποκάλυψης του μυστικού κωδικού πελάτη-εξυπηρετητή RADIUS

  Ο Αυθεντικοποιητής απόκρισης περιέχει το αποτέλεσμα της συνάρτησης κατακερματισμού MD5. Αυτός ο τρόπος προστασίας είναι ευάλωτος σε επιθέσεις αποκάλυψης του μυστικού κωδικού που μοιράζονται ο πελάτης κι ο εξυπηρετητής RADIUS. Αν ο επιτιθέμενος υποκλέψει ένα έγκυρο μήνυμα αίτησης Access-Request καθώς και την αντίστοιχη απάντηση (Access-Reject, Access-Accept), μπορεί να εκκινήσει μια εξαντλητική αναζήτηση του μυστικού κωδικού. Ο επιτιθέμενος μπορεί σε προγενέστερο χρόνο να υπολογίσει το κομμάτι των γνωστών στοιχείων που εισάγονται στην συνάρτηση κατακερματισμού, δηλαδή τα πεδία Κωδικός, Προσδιοριστής, Μέγεθος, Αυθεντικοποιητής Αίτησης και Ιδιότητες. Έπειτα δοκιμάζει διαφορετικές τιμές για το μυστικό κωδικό έως ότου το αποτέλεσμα της συνάρτησης κατακερματισμού είναι αυτό που περιέχεται στο πεδίο Αυθεντικοποιητής Απόκρισης.

  Μια άλλη επίθεση αποκάλυψης του μυστικού κωδικού γίνεται από έναν επιτιθέμενο, εκμεταλλευόμενος την ιδιότητα User-Password. Ο επιτιθέμενος επιχειρεί να αυθεντικοποιηθεί σε έναν πελάτη-NAS με ένα γνωστό σε αυτόν κωδικό πρόσβασης. Έπειτα, υποκλέπτει το μήνυμα αίτησης Access-Request που αποστέλλει ο πελάτης στον εξυπηρετητή καθώς και την απόκριση του δεύτερου. Πραγματοποιώντας την πράξη XOR μεταξύ της προστατευόμενης περιοχής της ιδιότητας User-Password, και του κωδικού χρήστη που ίδιος

παρείχε, εξάγει το αποτέλεσμα της συνάρτησης κατακερματισμού MD5(Μυστικός κωδικός + Αυθεντικοποιητής Αίτησης). Από τα δύο αυτά ορίσματα, το δεύτερο είναι γνωστό στον επιτιθέμενο αφού περιέχεται στο μήνυμα Access-Request που ήδη συνέλεξε. Εκτελώντας μια εξαντλητική αναζήτηση, μπορεί να ανακαλύψει το μυστικό κωδικό που χρησιμοποιείται μεταξύ του πελάτη και του εξυπηρετητή RADIUS.

- Επίθεση έναντι του κωδικού χρήστη

  Ο επιτιθέμενος επιχειρεί να αυθεντικοποιηθεί σε έναν πελάτη-NAS χρησιμοποιώντας ένα έγκυρο όνομα χρήστη (username) και ένα γνωστό, αλλά πιθανότατα εσφαλμένο κωδικό χρήστη (password). Μετά την υποκλοπή του μηνύματος απόκρισης Access-Request, ο επιτιθέμενος προσδιορίζει το αποτέλεσμα της συνάρτησης κατακερματισμού MD5(Μυστικός κωδικός + Αυθεντικοποιητής Αίτησης). Έπειτα, ο επιτιθέμενος αποστέλλει τροποποιημένα μηνύματα αιτήσεων, χρησιμοποιώντας τον ίδιο Αυθεντικοποιητή Αίτησης και τιμή της MD5(Μυστικός κωδικός + Αυθεντικοποιητής Αίτησης), αλλάζοντας τον κωδικό πρόσβασης στην ιδιότητα User-Password. Η διαδικασία επαναλαμβάνεται έως ότου γίνει δεκτή η αίτηση αυθεντικοποίησης. Η επίθεση μπορεί πολύ εύκολα να αποφευχθεί εάν ο εξυπηρετητής διατηρεί ένα μετρητή προσπαθειών αυθεντικοποίησης ανά χρήστη.

5.6.3 Ασφάλεια στο Diameter

Το Diameter χρησιμοποιεί δυο γνωστά και ευρέως χρησιμοποιούμενα πρωτόκολλα ασφάλειας για την προστασία των συναλλαγών μεταξύ γειτονικών κόμβων. Η χρήση ενός από αυτά, είναι πάντα υποχρεωτική. Τα πρωτόκολλα TLS και IPsec είναι ιδιαίτερα διαδεδομένα ενώ η ασφάλεια που παρέχουν είναι δεδομένη λόγω της μακροχρόνιας επιστημονικής έρευνας σε αυτά. Η από άκρο-σε-άκρο ασφάλεια των μεταδιδόμενων δεδομένων είναι ένα θέμα το όποιο βρίσκει μερικώς λύση στο Diameter. Για την προστασία από άκρο-σε-άκρο μπορεί να χρησιμοποιηθεί η εφαρμογή Cryptographic Message Syntax η οποία δυστυχώς δεν αποτελεί επίσημο πρότυπο ακόμη και κατά συνέπεια δεν είναι υποχρεωτική η υλοποίηση της.

5.6.4 Επιθέσεις άρνησης παροχής υπηρεσιών

Κανένα από τα δυο πρωτόκολλα δεν υποστηρίζουν άμεσα κάποιο μηχανισμό έναντι των επιθέσεων άρνησης παροχής υπηρεσιών Denial of Service (DoS). Οι επιθέσεις DoS συνήθως πραγματοποιούνται με την αποστολή υπερβολικά μεγάλου αριθμού πακέτων στο υπολογιστικό σύστημα-στόχο ώστε να μην μπορεί αυτό να διεκπεραιώσει τις εισερχόμενες αιτήσεις από κανονικούς χρήστες. Ακόμη κι αν το υπολογιστικό σύστημα είχε τη δυνατότητα αναγνώρισης των

πακέτων από τον κακόβουλο χρήστη ως κατεστραμμένα ή μη αναγνώσιμα, αυτή η διαδικασία θα απαιτούσε αρκετή επεξεργαστική ισχύ για να πραγματοποιηθεί, και πιθανότατα θα είχε το ίδιο αποτέλεσμα, την παράλυση του μηχανήματος-στόχο. Ειδικά για το Diameter, και στην περίπτωση που χρησιμοποιείται ως πρωτόκολλο επίπεδο μεταφοράς το SCTP, υπάρχει μία μερική αντίσταση στις επιθέσεις flooding λόγω των μηχανισμών ασφάλειας που υλοποιεί το SCTP. [47]

Μία άλλη περίπτωση που μπορεί να πραγματοποιηθεί DoS επίθεση, είναι μία ευπάθεια στο μηχανισμό failover των πρωτοκόλλων που εν μέρει υποστηρίζουν και τα δυο πρωτόκολλα AAA. Η επίθεση πραγματοποιείται με την προϋπόθεση ότι ο επιτιθέμενος γνωρίζει την ύπαρξη και τις συνθήκες ενεργοποίησης του μηχανισμό failover. Ο επιτιθέμενος πλημμυρίζει με άχρηστα πακέτα το δίκτυο επικοινωνίας μεταξύ του πελάτη και του εξυπηρετητή. Ο πελάτης ανιχνεύοντας την αδυναμία αποστολής πακέτων στον εξυπηρετητή, ενεργοποιεί τη διαδικασία failover δρομολογώντας τα πακέτα σε έναν εναλλακτικό εξυπηρετητή. Ο επιτιθέμενος, αναμένοντας αυτή τη συμπεριφορά από τον πελάτη, παύει για ένα χρονικό διάστημα το πλημμύρισμα του δικτύου με πακέτα και έπειτα συνεχίζει. Επαναλαμβάνοντας περιοδικά αυτή την συμπεριφορά, ο επιτιθέμενος επιτυγχάνει την DoS επίθεση έναντι του συστήματος. Ο πελάτης βρίσκεται σε μία συνεχή εναλλαγή εξυπηρετητών (διαδικασίες failover-failback) με αποτέλεσμα να μην στέλνει καθόλου τα πακέτα του στον εξυπηρετητή και τελικά να μην απολαμβάνει τις υπηρεσίες AAA [4].

5.6.5 Replay Επιθέσεις

Τα πρωτόκολλα RADIUS και Diameter προσφέρουν κάποιου είδους προστασία σε επιθέσεις replay. Το Diameter έχει γενικά καλύτερο επίπεδο προστασίας αφού βασίζεται στα πρωτόκολλα IPsec και TLS που ενσωματώνουν μηχανισμούς άμυνας έναντι στις επιθέσεις replay. Το πρωτόκολλο IPSec μπορεί επίσης να χρησιμοποιηθεί σε συνδυασμό με το RADIUS προκειμένου να προσφέρει το ίδιο επίπεδο ασφάλειας σχετικά με τις επιθέσεις replay, όπως γίνεται και στο Diameter.

6 Συμπεράσματα

Στην εργασία αυτή παρουσιάσαμε τα δυο πρωτόκολλα AAA που μονοπωλούν το ενδιαφέρον σήμερα. Αναλύσαμε τα επιμέρους χαρακτηριστικά και των δύο στα κεφάλαια 2 και 3, και επιχειρήσαμε μια σύγκριση αυτών στο κεφάλαιο 5. Το πρωτόκολλο RADIUS χρησιμοποιείται ευρέως τα τελευταία χρόνια ως το κύριο πρωτόκολλο AAA. Ωστόσο, αυτό συνέβαινε και λόγω έλλειψης ενός ανταγωνιστικού προς αυτό πρωτόκολλο AAA. Μετά την προτυποποίηση του Diameter, το RADIUS βρίσκεται αντιμέτωπο με ένα καλύτερο σχεδιαστικά πρωτόκολλο που επιλύει

την πλειονότητα των αδυναμιών που χαρακτηρίζουν το δεύτερο. Το Diameter επεκτείνει ακόμη περισσότερο τις δυνατότητες του RADIUS προσφέροντας κάποια μοναδικά χαρακτηριστικά. Στον πινάκα 5 παρουσιάζονται συνοπτικά μερικά από τα σημεία διαφοροποίησης των πρωτοκόλλων.

Παρόλο που το Diameter είναι σχεδιαστικά καλύτερο πρωτόκολλο από αυτό του RADIUS, δεν μπορούμε να ισχυριστούμε με βεβαιότητα ότι θα επικρατήσει ολοκληρωτικά και άμεσα έναντι του προκάτοχου του. Το RADIUS θα συνεχίσει να χρησιμοποιείται στα επόμενα χρόνια, ιδιαίτερα σε εφαρμογές και υλοποιήσεις που εμπλέκονται μικρός αριθμός χρηστών ή χρησιμοποιούνται παλαιότερης τεχνολογίας δικτυακές συσκευές πρόσβασης- NAS. Κύριο πλεονέκτημα του RADIUS είναι η τεράστια εγκατεστημένη βάση υλοποιήσεων του, και ιδιαίτερα απλή λειτουργία του, συγκριτικά με το Diameter.

Σε νέες εφαρμογές ή υλοποιήσεις το Diameter αναμένεται να αποτελέσει πρώτη προτίμηση των σχεδιαστών αφού δεν θα υπάρχει η δεσμευτική παράμετρος των ήδη υπαρχόντων εγκατεστημένων υλοποιήσεων. Στα επόμενα χρόνια αναμένεται σταδιακή μετάβαση προς το Diameter.

Πίνακας 5 Σύγκριση χαρακτηριστικών των πρωτοκόλλων RADIUS και Diameter

Χαρακτηριστικό	RADIUS	Diameter
Πρωτόκολλο επιπέδου μεταφοράς	UDP	TCP ή SCTP
Ανίχνευση κόμβων	Στατική	Στατική ή δυναμική
Εύρος διαθέσιμων ιδιοτήτων	Δέσμευση 8 bit. Μόνο 256 διαφορετικές ιδιότητες	Δέσμευση 16 bit. Μεγαλύτερο διαθέσιμο εύρος
Αλγόριθμος επανα-μετάδοσης	Δέσμευση 8 bit για το πεδίο του προσδιοριστή. Περιορισμός των ταυτόχρονων αιτήσεων σε 256 ανά εξυπηρετητή.	Δέσμευση 32 bit για το πεδίο του προσδιοριστή. Πολύ μεγάλος αριθμός ταυτόχρονων αιτήσεων στον εξυπηρετητή
Έλεγχος ροής πακέτων στον εξυπηρετητή	Δεν εφαρμόζεται κανένας έλεγχος ροής αφού λειτουργεί επάνω από το πρωτόκολλο UDP.	Τόσο το TCP και το SCTP, διαθέτουν μηχανισμούς έλεγχου ροής πακέτων.
Απόρριψη πακέτων δίχως ειδοποίηση	Τα πακέτα που δεν περιέχουν την αναμενόμενη πληροφορία ή έχουν σφάλματα απορρίπτονται δίχως ειδοποίηση	Ο εξυπηρετητής πληροφορεί τον πελάτη σε περίπτωση προβλήματος αποστέλλοντας ένα μήνυμα σφάλματος
Ασφάλεια hop-by-hop	Μέτριο επίπεδο ασφάλειας επικοινωνιών και μόνο μεταξύ γειτονικών κόμβων.	Υψηλό επίπεδο ασφάλειας με την χρήση των TLS/Ipsec
Ασφάλεια end-to-end	Δεν προβλέπεται - Δεν υποστηρίζεται	Προβλέπεται σχετικά από την εφαρμογή CMS αλλά δεν αποτελεί επίσημο πρότυπο

Κόστος επεξεργασίας	Δεν ενσωματώνει τις απαιτήσεις ευθυγράμμισης προσθέτοντας επιπλέον κόστος στους σύγχρονους επεξεργαστές	Υποστηρίζει την 32-bit ευθυγράμμιση δεδομένων. Αποδοτική επεξεργασία των πακέτων.
Αποστολή μηνυμάτων αίτησης από τον εξυπηρετητή	Δεν υποστηρίζεται	Υποστηρίζεται. Χρησιμοποιούνται από τον εξυπηρετητή για την κατά απαίτηση επανάληψη της διαδικασίας αυθεντικοποίησης-εξουσιοδότησης
Αυτόκλητες αποσυνδέσεις	Δεν υποστηρίζεται	Υλοποιείται βάσει του προηγούμενου χαρακτηριστικού. Ο εξυπηρετητής μπορεί να διακόψει τη σύνοδο ενός χρήστη, αποστέλλοντας σχετικό μήνυμα στον πελάτη
Διαπραγμάτευση δυνατοτήτων	Δεν υποστηρίζεται	Οι κόμβοι ανταλλάσουν τέτοια μηνύματα για να ενημερώσουν σχετικά για την υποστήριξη τους σε μια ομάδα ιδιοτήτων
Scalability	Μη αποδοτικό πρωτόκολλο σε μεγάλης κλίμακας υλοποιήσεις	Ιδιαίτερα αποδοτικό

7 Βιβλιογραφικές αναφορές

[1] Aboba, B., Calhoun, P., RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP), RFC 3579, September 2003

[2] Aboba, B. et al., "Criteria for Evaluating AAA Protocols for Network Access", IETF, RFC2989, November 2000

[3] Aboba, B. et al., "Extensible Authentication Protocol (EAP)", IETF, RFC3748, June 2004

[4] Aboba, B., Wood, J., "Authentication, Authorization and Accounting (AAA) Transport Profile",IETF, RFC 3539, June 2003

[5] Beadles, M., Mitton, D., "Criteria for Evaluating Network Access Server Protocols", IETF, RFC 3169, September 2001

[6] Calhoun, P., "Diameter Base Protocol", RFC 3588, IETF, September 2003

[7] Calhoun, P. et al., "Diameter Network Access Server Application", IETF, RFC 4005, Aug 2005

[8] Calhoun, P.,Bulley, W., Farrell, S., "Diameter CMS Security Application", Internet draft, IETF work in progress, draft-ietf-aaa-diameter-cms-sec-04.txt, March 2002

[9] Calhoun, P. et al., "Diameter Mobile IPv4 Application", IETF, RFC 4004, August 2005

[10] Case, J., et al., "A Simple Network Management Protocol (SNMP)", IETF, May 1990

[11] Chiba, M. et al., "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", IETF, RFC 3576, July 2003

[12] Durham, D., et al., "The COPS (Common Open Policy Service) Protocol", IETF, Jan 2000

[13] Eronen, P. et al., "Diameter Extensible Authentication Protocol (EAP) Application", IETF work in progress, Internet draft, draft-ietf-aaa-eap-07.txt, June 2004

[14] Farrell, S. et al., "AAA Authorization Requirements", IETF, RFC 2906, August 2000.

[15] FreeRADIUS Server Project, http://www.freeradius.org/

[16] Hassell, J., "RADIUS", O'Reilly, ISBN 0-596-00322-6, 2003

[17] Hill, J., "An analysis of RADIUS Authentication protocol", http://www.untruth.org/~josh/security/radius/radius-auth.html , 2001

[18] Hosia, A., "Comparison between RADIUS and Diameter", http://www.tml.tkk.fi/Studies/T-110.551/2003/papers/11.pdf , May 2003

[19] Housley, R., "Cryptographic Message Syntax (CMS) Algorithms", RFC 3370, IETF, August 2002

[20] http://en.wikipedia.org/wiki/Arpanet

[21] http://en.wikipedia.org/wiki/Diameter_%28protocol%29

[22] http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

[23] http://en.wikipedia.org/wiki/NSFNET

[24] http://en.wikipedia.org/wiki/Point-to-Point_Protocol

[25] http://en.wikipedia.org/wiki/RADIUS

[26] http://en.wikipedia.org/wiki/Uniform_Resource_Identifier

[27] Internet Assigned Number Authority, website URL, http://www.iana.org/

[28] "Introduction to Diameter", White paper, www.docs.hp.com, September 2002

[29] Jungmaier, A., "SCTP States", http://tdrwww.exp-math.uni-essen.de/inhalt/forschung/sctp_fb/sctp_states.html

[30] Liu, J. et al, "Introduction to Diameter, get the next generation AAA protocol", http://www-128.ibm.com/developerworks/library/wi-diameter/index.html, January 2006

[31] Mitton, D. et al., "Authentication, Authorization and Accounting Protocol Evaluation", IETF, RFC 3127, June 2001.

[32] Metz, C., "AAA PROTOCOLS:Authentication, Authorization, and Accounting for the Internet", IEEE Internet Computing online, 2001

[33] Mockapetris, P., "Domain Names - Concepts and facilities", IETF, Nov 1987

[34] Nakhjiri Madjid, Nakhjiri Mahsa, "AAA and Network Security for Mobile Access RADIUS, Diameter, EAP, PKI AND IP MOBILITY", John Wiley & Sons Ltd, ISBN 0-470-01194-7, 2005

[35] Ong, L."An Introduction to the Stream Control Transmission Protocol (SCTP)", IETF, RFC 3286, May 2002

[36] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980

[37] Rigney, C.,"Radius Accounting", IETF, RFC2866, June 2000

[38] Rigney, C. et al., "Remote Authentication Dial In User Service (RADIUS)", IETF, RFC 2865, June 2000.

[39] Rigney, C., "RADIUS Extensions", IETF, RFC 2869, June 2000.

[40] Rivest, R., Dusse, S., "The MD5 Message-Digest Algorithm", IETF, RFC 1321, April 1992

[41] Roser Ken, "HOWTO: EAP/TLS Setup for FreeRADIUS and Windows XP Supplicant", 2002

[42] Simpson, W., "PPP Authentication Protocols", IETF, RFC1334, October 1992

[43] Simpson, W., “PPP Challenge Handshake Authentication Protocol (CHAP)”, IETF, RFC 1994, August 1996

[44] Simpson, W., “The Point-to-Point Protocol (PPP)”, IETF, RFC 1661, July 1994

[45] Schneier, B., "Applied Cryptography", J. Wiley & Sons, ISBN 0-471-12845-7, σ. 44-46, 1996

[46] Stewart, R., Metz, C., "SCTP: new transport protocol for TCP/IP," *Internet Computing, IEEE* , vol.5, no.6, pp.64-69, Nov/Dec 2001
URL: http://ieeexplore.ieee.org/iel5/4236/20897/00968833.pdf?isnumber=20897[]=JNL&arnumber=968833&arnumber=968833&arSt=64&ared=69&arAuthor=Stewart%2C+R.%3B+Metz%2C+C

[47] Stewart, R. "Stream Control Transmission Protocol", IETF, RFC 4960, September 2007

[48] Tanase, M., “IP spoofing: An introduction”, http://www.securityfocus.com/infocus/1674, March 2003

[49] Ventura, H., “Diameter next generation’s AAA protocol”, Master thesis at Linkopings Tekniska Hogskola, 2002

[50] Vollbrecht, J. et al., “AAA Authorization Application Examples”, IETF, RFC 2905,August 2000.

[51] Vollbrecht, J. et al., “AAA Authorization Framework”, IETF, RFC 2904, August 2000.

[52] Zhao, P. et al, “Attack on RADIUS Authentication Protocol”, *Proceedings of the International Conference on Communication Technology*, pp. 208-212, 2003

[53] Καμπουράκης Γ., Γκρίτζαλης Σ., Κάτσικας Σ., “Ασφάλεια Ασύρματων και Κινητών Δικτύων Επικοινωνιών”, Εκδ. ΠΑΠΑΣΩΤΗΡΙΟΥ, ISBN 9607530810, 2006

[54] Κολλαράς Α., “Ασφαλή ασύρματα δίκτυα 802.11 με χρήση μηχανισμών EAP/TLS”, Πανεπιστήμιο Αιγαίου, Ιούνιος 2007

[55] Πάγκαλος, Γ., Μαυρίδης, Ι., “Ασφάλεια πληροφοριακών συστημάτων και δικτύων”, Εκδ. Ανίκουλα, ISBN 960-516-018-8