Απειλές, Ευπάθειες, Ζητήματα και Σχεδιασμός Ασφαλείας στην IPTV

Διπλωματική εργασία για το τμήμα Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων, του Πανεπιστημίου Πειραιά.

Φοιτητής : Νίκος Λημνιός (ΑΜ: Ε / 03095)

Επιβλέπων καθηγητής : Χρήστος Ξενάκης

Περιεχόμενα

Περίληψη

Στο **1ο Κεφάλαιο : Εισαγωγή** , δίνεται ο ορισμός της IPTV, γίνεται αναφορά στα πρωτόκολλα IP, TCP, UDP, RTP, αναφέρονται οι μέθοδοι δρομολόγησης unicast, broadcast και multicast. Επιπλέον, περιγράφεται η αρχιτεκτονική της τεχνολογίας IPTV, οι μέθοδοι παράδοσης της υπηρεσίας IPTV, το broadcasting, το video on demand και τα πρότυπα παράδοσης video MPEG. Τέλος, εξηγείται το Quality of Service.

Στο **2ο Κεφάλαιο : Ζητήματα Ασφαλείας στην IPTV** , γίνεται η περιγραφή των έξι πιο βασικών απειλών στο περιβάλλον της IPTV. Αυτές είναι η κλοπή στοιχείων της IPTV, η κλοπή της υπηρεσίας, η κλοπή δεδομένων, η διακοπή της υπηρεσίας η παραβίαση της ιδιωτικότητας και η έκθεση της ακεραιότητας της πλατφόρμας. Στη συνέχεια εξετάζονται αυτές οι απειλές στα διάφορα τμήματα της υποδομής της IPTV. Δηλαδή, οι απειλές στο head end, στο δίκτυο του πάροχου της υπηρεσίας και στο home end.

Στο **3ο Κεφάλαιο : Συστήματα Ασφαλείας στην IPTV** , περιγράφονται τα αντίμετρα, ο σχεδιασμός και οι μηχανισμοί ασφαλείας για την αντιμετώπιση των απειλών στην IPTV. Αρχικά αναφέρονται τρόποι προστασίας των λειτουργικών συστημάτων, και κάποιες βασικές εφαρμογές για την αντιμετώπιση εισβολών και εξαπάτησης. Στην συνέχεια, εξετάζεται ξεχωριστά ο σχεδιασμός ασφαλείας, στο head end, στο δίκτυο του πάροχου της υπηρεσίας και στο home end. Στο τέλος του κεφαλαίου περιγράφεται το μοντέλο ασφαλείας κατά ITU-T X.805, όπου αναφέρει πώς οι οκτώ διαστάσεις ασφαλείας οι οποίες είναι έλεγχος πρόσβασης, αυθεντικοποίηση, μη άρνηση αναγνώρισης (*nonrepudiation*), εμπιστευτικότητα δεδομένων, ασφάλεια επικοινωνίας, ακεραιότητα δεδομένων, διαθεσιμότητα και ιδιωτικότητα, εφαρμόζονται στα τρία πεδία της ασφάλειας, στην ασφάλεια της διαχείρισης (*management security*), στην ασφάλεια ελέγχου (*control security*) και στην ασφάλεια χρήστη (*end user security*).

1. Εισαγωγή

<u>Ορισμός</u> **:** *Η IPTV είναι ένα σύστημα, όπου περιεχόμενο ψηφιακού βίντεο, συμπεριλαμβανομένων καναλιών τηλεόρασης, παραδίδεται με τη χρήση Internet Protocols (IP).*

Το internet δεν είναι απαραίτητο για την παράδοση του ψηφιακού βίντεο και της τηλεόρασης. Η IPTV χρησιμοποιεί το IP ως μηχανισμό παράδοσης, που σημαίνει ότι μπορεί ή να γίνει χρήση του internet, που είναι ένα δημόσιο IP-based δίκτυο, ή να γίνει χρήση κάποιου άλλου ιδιωτικού IP-based δικτύου.

Επειδή η IPTV χρειάζεται το IP μόνο ως μηχανισμό παράδοσης *(delivery mechanism)*, το IP μπορεί να χρησιμοποιηθεί για την παράδοση ποικίλων τύπων περιεχομένου, μέσω του internet και ιδιωτικών IP-based δικτύων. Το περιεχόμενο μπορεί να είναι μουσικά βίντεο ή show τηλεόρασης, ταινίες, συναυλίες, αθλητικά παιχνίδια κτλ.

Για τους απλούς χρήστες, η IPTV παρέχεται συχνά από κοινού μαζί με την υπηρεσία Video on Demand (VoD) και μπορεί να συνδυαστεί μαζί με υπηρεσίες διαδικτύου όπως είναι το World Wide Web και το Voice Over IP (VoIP).

1.1 Πρωτόκολλα IP, TCP, UDP, RTP, RTCP, RTSP

1.1.1 Πρωτόκολλο Διαδικτύου (IP)

Το Πρωτόκολλο Διαδικτύου (*Internet Protocol , IP*) βρίσκεται στο επίπεδο δικτύου του μοντέλου OSI. Η βασική λειτουργία του πρωτοκόλλου IP είναι να παρέχει πληροφορίες για τη δρομολόγηση των δεδομένων που κινούνται σε διαδίκτυα. Παρέχει μεταφορά των μονάδων δεδομένων από άκρο σε άκρο (*end-to-end*) μέσω των διαδικτύων. Το πρωτόκολλο IP δεν εξασφαλίζει αξιόπιστη μεταφορά δεδομένων, αλλά αυτό δεν αποτελεί πρόβλημα εάν τα ανώτερα επίπεδα παρέχουν αξιοπιστία και έλεγχο σφαλμάτων.

Το πρωτόκολλο IP ενθυλακώνει πληροφορίες μέσα στις επικεφαλίδες του (*που ονομάζονται επικεφαλίδες IP*), οι οποίες στη συνέχεια διαβιβάζονται στο επίπεδο γραμμής δεδομένων (*data link*), δηλαδή σε ένα δίκτυο όπως το Ethernet. Το πρωτόκολλο του επιπέδου γραμμής δεδομένων ενσωματώνει την επικεφαλίδα IP

και τα δεδομένα στη δική του μονάδα δεδομένων. Η μονάδα αυτή διαβιβάζεται στη συνέχεια στο δίκτυο ως μια σειριακή ακολουθία από bits.

Για να εγκαταλείψουν τα δεδομένα το τοπικό δίκτυο, θα πρέπει να οδηγηθούν σε έναν δρομολογητή. Οι δρομολογητές είναι συσκευές του επιπέδου δικτύου και είναι ικανοί να επεξεργάζονται τις επικεφαλίδες που τοποθετεί, για παράδειγμα το Ethernet και το πρωτόκολλο IP. Εάν τα δεδομένα πρέπει να διαβιβαστούν σε κάποιο άλλο δίκτυο, η επικεφαλίδα του Ethernet αποκόπτεται από τα δεδομένα και τυγχάνει επεξεργασίας η επικεφαλίδα IP.

Προτού μεταδοθούν τα δεδομένα μέσω μιας θύρας προς το επόμενο δίκτυο, ο δρομολογητής πρέπει να κατασκευάσει μια νέα επικεφαλίδα IP και να τοποθετήσει τα δεδομένα πίσω από την επικεφαλίδα IP, όταν το IP πακέτο φτάσει στον προορισμότου. Το σύνολο που προκύπτει (*δηλαδή η ομάδα datagram*) διαβιβάζεται στο επίπεδο σύνδεσης δεδομένων και η διαδικασία επαναλαμβάνεται.

1.1.2 Πρωτόκολλο Ελέγχου Μεταφοράς (TCP)

Το Πρωτόκολλο Ελέγχου Μεταφοράς (Transmission Control Protocol, TCP) βρίσκεται στο επίπεδο μεταφοράς του internet. Δημιουργεί μια σειρά από μηνύματα (segments), τα οποία φαίνονται σαν μια συνεχής ροή δεδομένων. Αυτή η ροή είναι δύο κατευθύνσεων (αποστολέας-παραλήπτης) και ταυτόχρονα αξιόπιστη. Παρακάτω αναφέρονται τα κυριότερα χαρακτηριστικά του TCP.

Είναι πρωτόκολλο με σύνδεση (connection protocol). Άρα χρησιμοποιείται μόνο μεταξύ δύο υπολογιστών. Πριν ξεκινήσει η μεταφορά δεδομένων πρέπει να γίνει ένα τριπλό handshaking (SYN, SYN-ACK, ACK) μεταξύ των δύο υπολογιστών (connection establishment) και ένα αντίστοιχο στον τερματισμό της αποστολής (connection termination).

Είναι αξιόπιστο. Η πλευρά του παραλήπτη ενημερώνει συνεχώς την πλευρά του αποστολέα, για το πιο είναι το επόμενο πακέτο που περιμένει, σύμφωνα με τον αύξοντα αριθμό των πακέτων που έχει ήδη λάβει και αν αντιληφθεί ότι κάποιο πακέτο χάθηκε στην πορεία, τότε επιβάλλει αναμετάδοση (retransmission). Αν το πακέτο δεν μπορεί να ληφθεί μετά από πολλαπλές αναμεταδόσεις, τότε η σύνδεση διακόπτεται (timeout).

Εγγυάται την σωστή σειρά άφιξης των δεδομένων στην εφαρμογή του παραλήπτη. Όταν τα δεδομένα εισέλθουν στην είσοδο του παραλήπτη με λάθος σειρά, τότε το TCP layer “κρατάει” αυτά τα δεδομένα μέχρι να έρθουν τα προηγούμενα τους. Αφού έρθουν τα διατάσσει στην σωστή σειρά και έπειτα τα παραδίδει στην εφαρμογή.

Αποτρέπει την αποστολή διπλότυπων, δηλαδή δύο ακριβώς ίδιων δεδομένων.

Προσφέρει αυτοματοποιημένο έλεγχο ροής δεδομένων (flow control). Όταν ο buffer του παραλήπτη γεμίσει, τότε σταματάει προσωρινά την μετάδοση ή ελαττώνει τον ρυθμό μετάδοσης του, μέχρι να αδειάσει ο buffer.

Προσφέρει αυτοματοποιημένο έλεγχο συμφόρησης (congestion control). Το TCP χρησιμοποιεί μια πληθώρα μηχανισμών για να επιτύχει τη μέγιστη απόδοση μεταφοράς δεδομένων, αποφεύγοντας την συμφόρηση δεδομένων στους δρομολογητές του Internet, μια κατάσταση κατά την οποία μειώνεται η απόδοση του δικτύου κατά μεγάλο βαθμό. Αυτοί οι μηχανισμοί ελέγχουν το ρυθμό με τον οποίο τα δεδομένα εισέρχονται στο δίκτυο, κρατώντας αυτό το ρυθμό κάτω από ένα ασφαλές όριο.

Εγγυάται την ακεραιότητα του "μονοπατιού επικοινωνίας". Αυτό βέβαια δεν εμποδίζει την υποκλοπή των δεδομένων από τρίτους. Όμως είναι σχετικά δύσκολη η υποκλοπή, αφού ο κακόβουλος χρήστης θα πρέπει να παρακολουθήσει όλη την ροή δεδομένων, καθώς δεν υπάρχουν συγκεκριμένου μεγέθους πακέτα.

Εξαιτίας των παραπάνω χαρακτηριστικών του, το TCP χρησιμοποιείται και επιβάλλεται να χρησιμοποιείται, όπου η ακεραιότητα των δεδομένων είναι ύψιστης σημασίας. Δηλαδή σε web surfing, e-mails, και οποιαδήποτε άλλη μεταφορά αρχείων δεδομένων ανάμεσα σε δύο υπολογιστές.

1.1.3 Πρωτόκολλο Δεδομενογραφημάτων Χρήστη (UDP)

Το Πρωτόκολλο Δεδομενογραφημάτων Χρήστη (*User Datagram Protocol, UDP*) βρίσκεται στο επίπεδο μεταφοράς του internet. Χρησιμοποιώντας το UDP τα προγράμματα μπορούν να στείλουν μικρά μηνύματα, γνωστά ως datagrams, το ένα στο άλλο. Παρακάτω αναφέρονται τα κυριότερα χαρακτηριστικά του UDP.

Είναι αναξιόπιστο. Δε μπορεί να εγγυηθεί την ακεραιότητα ή τη σωστή σειρά άφιξης των δεδομένων, όπως το TCP. Τα πακέτα μπορούν να φτάσουν με διαφορετική σειρά, να εμφανίζονται διπλά ή να μην έρθουν καθόλου χωρίς καμία ειδοποίηση.

Το UDP εξασφαλίζει μικρό delay και είναι πιο γρήγορο από το TCP.

Έχει πολλαπλή χρηστικότητα. Μπορεί να χρησιμοποιηθεί τόσο σε unicast όσο και σε multicast δίκτυα, καθώς δεν είναι connection protocol.

Είναι λιγότερο απαιτητικό σε πόρους, σε σχέση με το TCP. Δεν επιβαρύνει το δίκτυο, καθώς δεν ελέγχει αν όντως κάποιο πακέτο έφτασε ή όχι.

Έχει μικρότερο header. Το UDP έχει 8 bytes header, σε σχέση με το TCP που έχει 20 bytes header.

Το UDP υπάρχει ακριβώς γιατί υπάρχουν εφαρμογές, όπου δεν μας ενδιαφέρει τόσο η ακεραιότητα των δεδομένων, όσο τα δεδομένα να φτάσουν όσο δυνατόν γρηγορότερα στον παραλήπτη, έστω και με κάποια απώλεια. Εκεί δηλαδή που το TCP είναι αργό και δεν εξυπηρετεί, έρχεται να πάρει τη θέση του το UDP. Μερικές εφαρμογές που χρησιμοποιούν το UDP είναι οι παρακάτω:

- Εφαρμογές οι οποίες μεταδίδουν real time audio/video, όπως η IPTV. Εδώ μας ενδιαφέρει τα δεδομένα να φτάνουν την σωστή χρονική στιγμή. Οποιαδήποτε απώλεια τους μας επηρεάζει μόνο στην ποιότητα του αναπαραγόμενου σήματος.
- Servers, οι οποίοι απαντάνε σε μικρά αιτήματα ενός τεράστιου αριθμού από clients, όπως στα online παιχνίδια. Οι servers δεν απασχολούνται με το να ελέγχουν την κατάσταση της κάθε σύνδεσης και των παραμέτρων της χρησιμοποιώντας UDP, και έτσι μπορούν να εξυπηρετήσουν ένα πολύ μεγαλύτερο αριθμό χρηστών σε αντίθεση με την χρήση του TCP.

Ένα πρόγραμμα που χρησιμοποιεί το πρωτόκολλο UDP πρέπει να ασχοληθεί το ίδιο με τα προβλήματα επικοινωνίας που μπορεί να προκύψουν. Δηλαδή την αξιόπιστη παράδοση, το packetization και την επανασυναρμολόγηση, τον έλεγχο ροής, την αποφυγή συμφόρησης, κλπ. Επίσης, δεδομένου ότι το UDP στερείται μηχανισμών αποφυγής και ελέγχου δικτυακής συμφόρησης, απαιτούνται network based μηχανισμοί για να ελαχιστοποιηθούν τα πιθανά προβλήματα κατάρρευσης δικτύου λόγω ανεξέλεγκτα υψηλών ρυθμών αποστολής πακέτων UDP. Δεδομένου ότι οι αποστολείς UDP δεν μπορούν να ανιχνεύσουν τη συμφόρηση, τα στοιχεία των δικτύων, όπως οι δρομολογητές, πρέπει να χρησιμοποιούν τεχνικές packet queuing και απόρριψης πακέτων για να ελέγχουν την υπερβολική κίνηση πακέτων UDP στα δίκτυα.

Το Datagram Congestion Control Protocol (*DCCP*) σχεδιάζεται ως μια μερική λύση σε αυτό το πιθανό πρόβλημα προσθέτοντας TCP μηχανισμούς ελέγχου συμφόρησης σε ροές πακέτων UDP υψηλής ταχύτητας (*πχ media streaming*).

1.1.4 Πρωτόκολλο Μεταφοράς σε Πραγματικό Χρόνο (RTP)

Το Real-time Transport Protocol (*RTP*) παρέχει λειτουργίες μεταφοράς στο δίκτυο από άκρο σε άκρο (*end to end network transport functions*), οι οποίες διευκολύνουν την παράδοση real time δεδομένων όπως audio και video μέσω unicast και multicast υπηρεσιών. Οι υπηρεσίες που παρέχει το RTP είναι οι παρακάτω:

- Ένδειξη του τύπου του περιεχομένου που μεταφέρεται
- Αρίθμηση πακέτων
- Δυνατότητα υπολογισμού του jitter (ορίζεται στην παράγραφο QoS)
- Παρακολούθηση της διαδικασίας αποστολής.
- Δεν παρέχει flow & congestion control από μόνο του

Το RTP δεν έχει κάποια συγκεκριμένη TCP/UDP θύρα από την οποία επικοινωνεί. Το μόνο στο οποίο υπακούει είναι ότι οι UDP επικοινωνίες γίνονται σε ζυγές θύρες και η αμέσως επόμενη μονή θύρα χρησιμοποιείται για το RTP Control Protocol (RTCP).

1.1.5 RTP Control Protocol (RTCP)

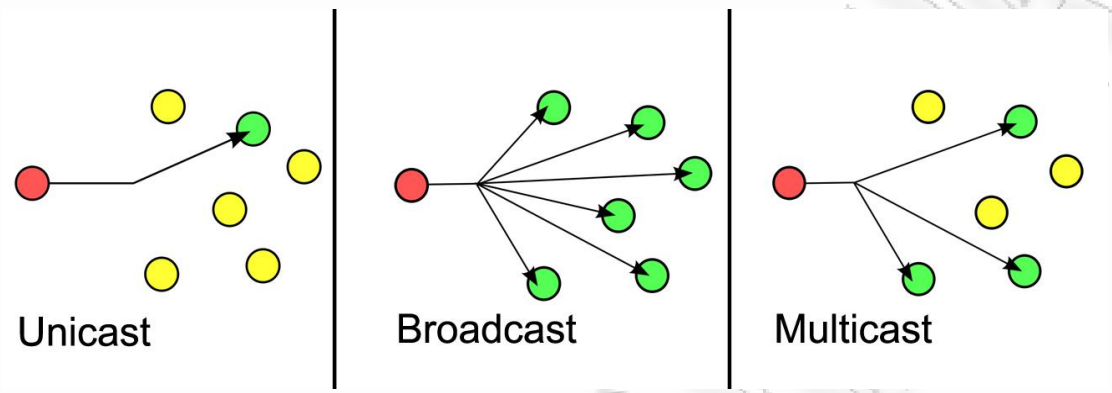
Το RTCP προσφέρει πληροφορίες (*feedback*) για το quality of service που παρέχει το RTP. Μαζεύει στατιστικά, όπως τα πακέτα που στάλθηκαν, τα χαμένα πακέτα, το jitter και το round trip delay. Μια εφαρμογή μπορεί να χρησιμοποιήσει αυτές τις πληροφορίες για να αυξήσει το quality of service.

1.1.6 Real Time Streaming Protocol (RTSP)

Το RTP μπορεί να δουλέψει παράλληλα με το Real Time Streaming Protocol (*RTSP*) το οποίο επιτρέπει τον απομακρυσμένο έλεγχο ενός media server με εντολές παρόμοιες ενός βίντεο. Μερικές από τις εντολές που παρέχει το RTSP είναι το Describe, Setup, Play, Pause, Record και Teardown. Οι εντολές αυτές αφορούν την περιγραφή του αρχείου προς μετάδοση, τον έλεγχο της αναπαραγωγής και τον τερματισμό της συνόδου με τον server.

1.2 Μέθοδοι δρομολόγησης

Στην συνέχεια παρουσιάζονται τρείς βασικοί μέθοδοι δρομολόγησης, το unicast, το broadcast και το multicast.



Εικόνα 1.1 Μέθοδοι δρομολόγησης Unicast, Broadcast, Multicast

1.2.1 Unicast

Ο πιο συνηθισμένος τύπος για μια IP διεύθυνση, είναι μια unicast διεύθυνση και είναι ο πιο διαδεδομένος τρόπος μετάδοσης της πληροφορίας στο σημερινό Internet. Αναφέρεται σε έναν μεμονωμένο αποστολέα ή παραλήπτη και μπορεί να χρησιμοποιηθεί τόσο για την αποστολή όσο και την παραλαβή. Συνήθως μια unicast διεύθυνση αντιστοιχίζεται με μια μόνο συσκευή. Ωστόσο, ορισμένοι υπολογιστές έχουν πολλές διαφορετικές unicast διευθύνσεις, η κάθε μια για την δικιά της ξεχωριστή χρήση. Στέλνοντας την ίδια πληροφορία σε διαφορετικές unicast διευθύνσεις, ο αποστολέας πρέπει να στείλει την ίδια πληροφορία τόσες φορές όσοι είναι και οι παραλήπτες του.

Στην unicast δρομολόγηση κάθε δρομολογητής εξετάζει την διεύθυνση προορισμού (*destination address*) του λαμβανόμενου πακέτου και ψάχνει αυτήν την διεύθυνση σε έναν πίνακα, για να προσδιορίσει ποια διασύνδεση να χρησιμοποιήσει ώστε το πακέτο να φτάσει στον προορισμό του. Η διεύθυνση πηγής (*source address*) του πακέτου δεν παίζει κανένα ρόλο.

1.2.2 Broadcast

Με το broadcast, η πληροφορία αποστέλλεται σε όλους τις πιθανούς προορισμούς, έτσι ο αποστολέας έχει την δυνατότητα, να στείλει την πληροφορία μόνο μια φορά και όλοι οι παραλήπτες να την λάβουν. Στο IP πρωτόκολλο, η διεύθυνση 255.255.255.255 παριστάνει ένα περιορισμένο τοπικό broadcast. Για παράδειγμα, για να γίνει αποστολή σε όλες τις διευθύνσεις σε ένα τοπικό δίκτυο που αρχίζουν με 192.0.2, η directed broadcast διεύθυνση είναι 192.0.2.255, υποθέτοντας ότι η μάσκα δικτύου (*netmask*) είναι 255.255.255.0.

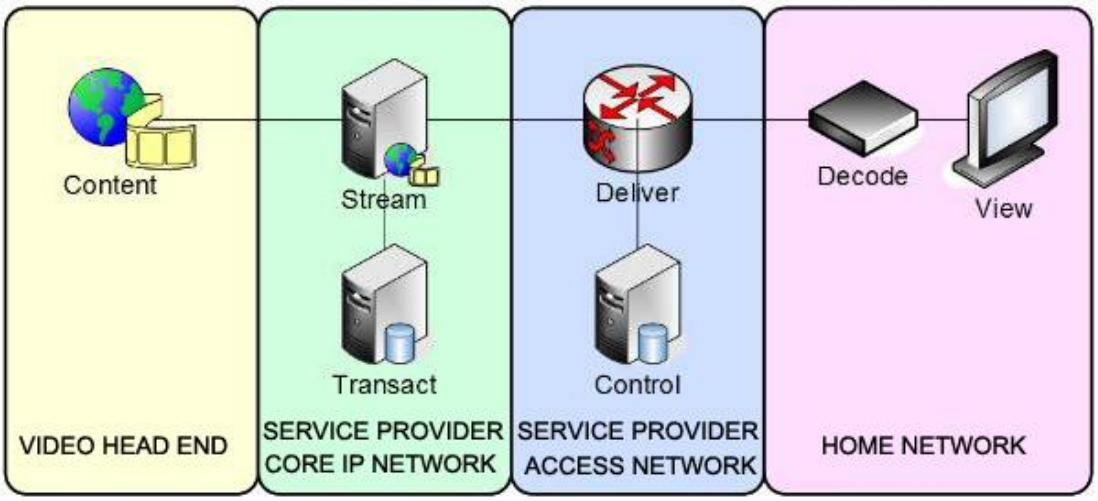
1.2.3 Multicast

Μια multicast διεύθυνση αντιστοιχίζεται με μια ομάδα από ενδιαφερόμενους χρήστες. Σύμφωνα με το RFC3171 της IANA (Internet Assigned Numbers Authority), οι διευθύνσεις 224.0.0.0 μέχρι 239.255.255.255 είναι ορισμένες ως multicast διευθύνσεις. Αυτές οι διευθύνσεις ήταν γνωστές παλαιότερα και με την ονομασία Class D. Ο αποστολέας στέλνει ένα datagram UDP πακέτο από την unicast διεύθυνση του, στην multicast διεύθυνση και οι δρομολογητές αναλαμβάνουν να κάνουν αντίγραφα του πακέτου μόνο όταν χρειάζεται και να το στείλουν σε όσους παραλήπτες δήλωσαν ενδιαφέρον για το συγκεκριμένο πακέτο από τον συγκεκριμένο αποστολέα. Δεν απαιτείται προηγούμενη γνώση για το ποιοι ή πόσοι παραλήπτες υπάρχουν στο δίκτυο.

Σε αντίθεση με τη unicast δρομολόγηση που αναφέραμε παραπάνω, η source address, που είναι μια απλή unicast διεύθυνση, χρησιμοποιείται για να προσδιορίσει την κατεύθυνση της ροής δεδομένων. Η πηγή της multicast κίνησης (traffic) θεωρείται σαν upstream. Ο δρομολογητής προσδιορίζει ποιες downstream διασυνδέσεις είναι προορισμοί για αυτό το multicast group και στέλνει το πακέτο μέσω των κατάλληλων διασυνδέσεων.

1.3 Η Αρχιτεκτονική της Τεχνολογίας IPTV

Υπάρχουν τέσσερα βασικά στοιχεία στην αρχιτεκτονική ενός IPTV συστήματος, που είναι κοινά στην δομή του συστήματος κάθε παρόχου υπηρεσίας IPTV. Αυτά είναι το video head end, το δίκτυο του πάροχου της υπηρεσίας IPTV, το δίκτυο πρόσβασης του πάροχου της υπηρεσίας και το οικιακό δίκτυο. Στην εικόνα 2.2 φαίνεται η σχέση των στοιχείων του IPTV δικτύου και η ροή των δεδομένων από τον πάροχο περιεχομένου μέχρι τον καταναλωτή.



Εικόνα 1.2 Βασικά στοιχεία της δομής IPTV

Περισσότεροι του ενός παρόχου μπορούν να παρέχουν το κάθε στοιχείο του IPTV δικτύου. Για παράδειγμα, αν ένας καταναλωτής χρησιμοποιεί την IPTV για να κάνει download μια ταινία μέσω του internet, το video head end μπορεί να αντιπροσωπεύει μια εταιρεία, ενώ το δίκτυο του πάροχου της υπηρεσίας IPTV μπορεί να αποτελείται από πολλά IP networks διασυνδεδεμένα (*interconnected*) σε ένα peering point, ώστε να σχηματίζουν την ραχοκοκαλιά του internet (*internet backbone*). Το δίκτυο πρόσβασης μπορεί να αντιπροσωπεύει έναν ISP (*internet service provider*) και το οικιακό δίκτυο μπορεί να αποτελείται από ένα δρομολογητή (*router*) και προϊόντα wireless LAN από έναν ή παραπάνω κατασκευαστές.

Αντίθετα, αν ένας καταναλωτής έχει πρόσβαση σε μια ταινία ή ένα TV show μέσω ιδιωτικού IP network, το video head end , το δίκτυο του πάροχου της υπηρεσίας και το δίκτυο πρόσβασης θα έχουν ως πάροχο μια συγκεκριμένη εταιρεία. Η οποία εταιρεία πιθανότατα θα προσέφερε μια από άκρη σε άκρη (*end-to-end*) υπηρεσία,

που θα συμπεριλάμβανε ολόκληρο τον εξοπλισμό που θα απαιτούσε για το οικιακό δίκτυο.

Στη συνέχεια ακολουθεί περιγραφή των τεσσάρων βασικών στοιχείων της δομής της IPTV, που αναφέραμε παραπάνω.

1.3.1 Video Head End

Αυτό είναι το σημείο στο δίκτυο στο οποίο το περιεχόμενο συλλαμβάνεται (*captured*) και μετασχηματίζεται (*formatted*) για διανομή στο IP δίκτυο. Το video head end σε ένα IP δίκτυο, μοιάζει πολύ με τα head ends που χρησιμοποιούνται από την καλωδιακή τηλεόραση και τα δορυφορικά ψηφιακά συστήματα. Αυτό σημαίνει, ότι ένα video head end μπορεί να συνδεθεί και με δορυφορικούς δέκτες για να λάβει broadcast television και premium television, που εκπέμπονται μέσω δορυφόρου. Άλλα τηλεοπτικά προγράμματα μπορεί να τα λάβει μέσω επίγειας σύνδεσης (*fiber based*), ή να αναπαράγει ταινίες μέσω dvd και hard disc servers, που προσφέρουν μια υπηρεσία content on demand.

Το head end λαμβάνει ροές δεδομένων (*data stream*) και τις κωδικοποιεί σε μια ψηφιακή μορφή βίντεο, όπως mpeg-2 ή mpeg-4. Τα πρότυπα αυτά περιγράφονται σε παρακάτω ενότητα.

Μετά την κωδικοποίηση, δεδομένα της ροής ενθυλακώνονται μέσα σε μια IP ροή δεδομένων (*IP data stream*) η οποία μεταδίδεται σε μια συγκεκριμένη IP διεύθυνση αποστολής (*IP destination address*), ως ανταπόκριση στην αίτηση κάποιου πελάτη για ένα συγκεκριμένο κανάλι.

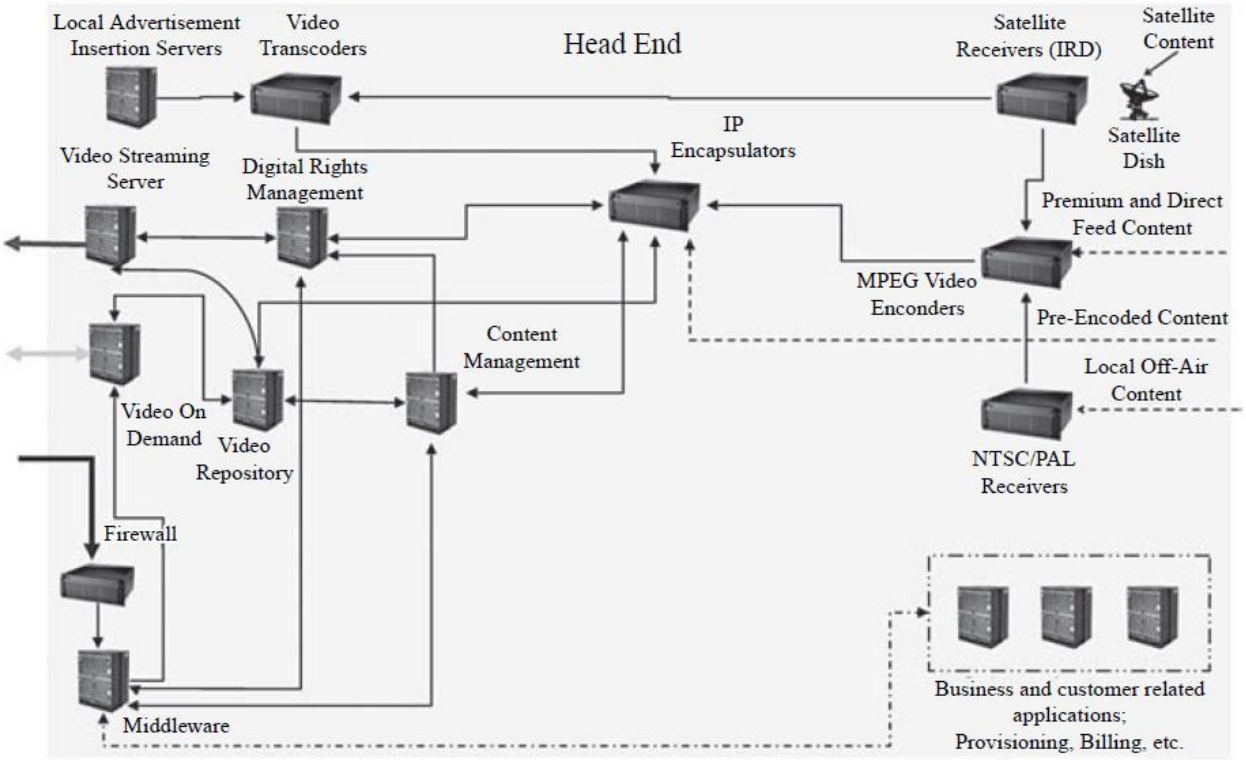
Επιπλέον στοιχεία του head end, είναι η εφαρμογή DRM (*Digital Rights Management*) και τα συστήματα διαχείρισης περιεχομένου (*content management systems*). Όλες οι επικοινωνίες με τους συνδρομητές συντονίζονται από τον middleware server, ο οποίος λαμβάνει αιτήσεις από τα set top box. Όπως φαίνεται και στην *εικόνα 1.3*, συνολικά το head end αποτελείται από τα παρακάτω.

- Δορυφορικούς δέκτες
- Αποθήκη video η οποία περιλαμβάνει :
    - Βιβλιοθήκη Video (*Video library*)

- Βιβλιοθήκη Μέσων (*Media library*)
- Library servers
- Δίκτυο αποθήκευσης
- Αρχεία ήχου και Εικόνας (*Film servers*)

- Σύστημα διαχείρισης περιεχομένου το οποίο περιλαμβάνει:
  - Κέντρο εντολών
  - Σύστημα διαχείρισης αγαθών (*asset*)
  - Διαχείριση ψηφιακών δικαιωμάτων (*DRM*)
- Master video streaming server που είναι υπεύθυνος για την διάδοση του περιεχομένου video. Περιλαμβάνει:
  - Υπηρεσία διάδοσης (*propagation*)
  - Υπηρεσία streaming
- Πύλη εισαγωγής του video που συλλαμβάνεται. Η οποία περιλαμβάνει :
  - Σύστημα εγγραφής
  - Διαχείριση εγγραφής
  - Server για σύλληψη και διανομή
- Video cache streaming server, που είναι υπεύθυνος για την διάδοση του περιεχομένου video που βρίσκεται την κρυφή μνήμη (cache). Περιλαμβάνει:
  - Caching server
  - Συστάδα μέσων (*media cluster*)
- Το middleware το οποίο περιλαμβάνει τους middleware servers.
- Συστήματα σχετικά με την επιχείρηση, τα οποία περιλαμβάνουν :

- Λογαριασμούς και χρεώσεις
- Πληροφορίες πελατών



Εικόνα 1.3 Το Head End

1.3.2 Το δίκτυο του πάροχου της υπηρεσίας IPTV

Το δίκτυο του πάροχου της υπηρεσίας IPTV, είναι ένα σύστημα (*delivery system*) που επιτρέπει την μετάδοση δεδομένων από τον πυρήνα του δικτύου, που είναι συνδεδεμένος στο head end, μέχρι την άκρη του δικτύου. Στο service provider core network, τα κανάλια ρέουν (*flows*) με την μορφή κωδικοποιημένων ροών video. Αυτές οι ροές αποτελούνται από δεδομένα που έχουν προέλθει από unicast, multicast ή broadcast εκπομπές. Για παράδειγμα, ο οδηγός TV (*tv guide*) που ρέει σε κάθε συνδρομητή μπορεί να είναι broadcast εκπομπή. Μια συγκεκριμένη ταινία που έχει ζητηθεί από έναν συνδρομητή, μπορεί να φτάσει στον συνδρομητή με unicast

εκπομπή, ενώ ένα δημοφιλές κανάλι μπορεί να φτάσει σε όλους τους συνδρομητές με multicast εκπομπή.

1.3.3 Το δίκτυο πρόσβασης

Το δίκτυο πρόσβασης προσφέρει σύνδεση από τη στέγη του καταναλωτή μέχρι το δίκτυο του πάροχου της υπηρεσίας. Το μέσο μεταφοράς (*transport facility*), που στηρίζεται το δίκτυο πρόσβασης, μπορεί να είναι Asymmetrical Digital Subscriber Lines (*ADSL*), very high bit rate Digital Subscriber Lines (*VDSL*) και διάφοροι τύποι τεχνολογίας οπτικών ινών, όπως passive optical networking (*PON*).

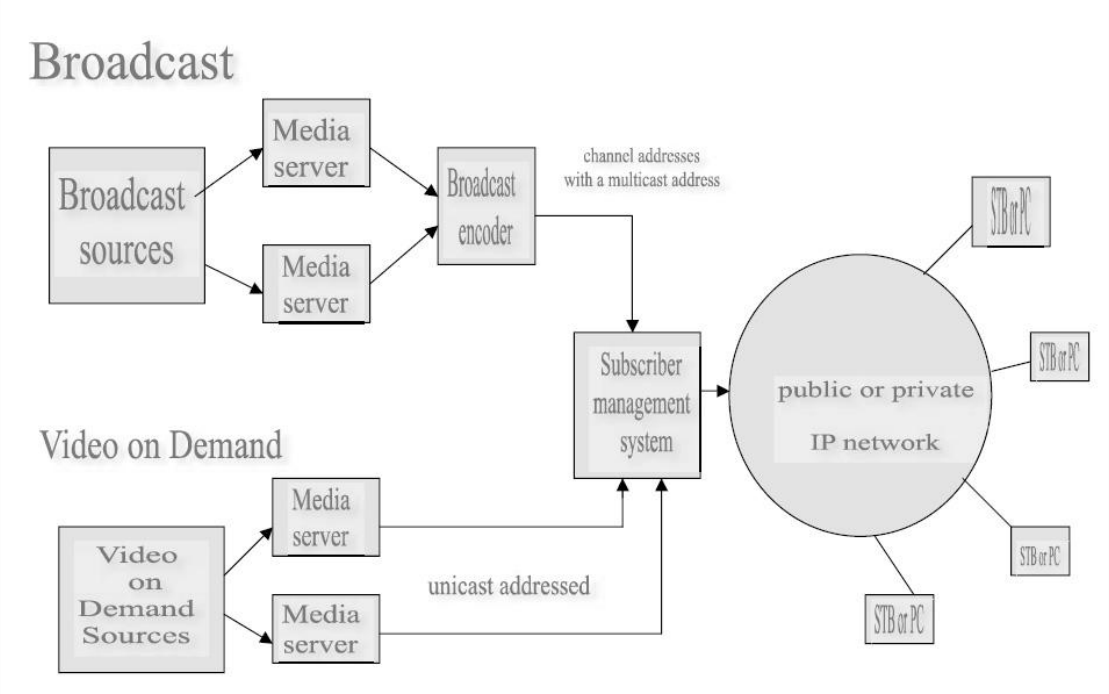
Ο πάροχος υπηρεσίας χρησιμοποιεί το δίκτυο πρόσβασης, για να μπορεί να παρέχει στους συνδρομητές μια σύνδεση υψηλού bandwidth (*υψίρυθμη σύνδεση*). Αυτή η σύνδεση προσφέρει την δυνατότητα πρόσβασης σε πολλαπλά κανάλια τηλεόρασης, σε voice over IP (VoIP) και σε internet υψηλών ταχυτήτων.

1.3.4 Το οικιακό δίκτυο

Το οικιακό δίκτυο είναι υπεύθυνο για την διανομή της υπηρεσίας IPTV στο σπίτι. Μπορεί να αποτελείται από ενσύρματο Ethernet, ασύρματο Ethernet ή από εξοπλισμό Home Plug audio-visual (*AV*). Το ασύρματο Ethernet μπορεί να προσφέρει ρυθμό δεδομένων (*data rate*) μέχρι 100 Mbps και το Home Plug AV μέχρι 200 Mbps για την μετάδοση δεδομένων μέσω ηλεκτρικού καλωδίου στο σπίτι. Τα τελικά σημεία (*endpoints*) στο οικιακό δίκτυο, είναι τα τηλέφωνα, οι ηλεκτρονικοί υπολογιστές και τα set top box που είναι απαραίτητα για κάθε τηλεόραση.

1.4 Μέθοδοι παράδοσης της IPTV

Υπάρχουν δύο βασικοί μέθοδοι για την παράδοση περιεχομένου IPTV. Αυτές είναι το broadcast και το video on demand (*VOD*), που χρησιμοποιούνται για την παρακολούθηση σε πραγματικό χρόνο (*real time viewing*) ταινιών, show τηλεόρασης, συναυλιών κτλ.



Εικόνα 1.4 Μετάδοση της IPTV, μέσω broadcast και unicast video on demand μετάδοσης

1.4.1 Broadcasting

Στην broadcast μετάδοση video, σε κάθε εκπομπή (*feed*) παρέχεται και ένας μοναδικός αριθμός καναλιού, ώστε το set top box να έχει την δυνατότητα να επιλέξει την εκπομπή (*feed*), που επιθυμεί να παρακολουθήσει ο χρήστης. Όταν ένας χρήστης χρησιμοποιεί το set top box για να επιλέξει ένα κανάλι, το set top box θα εγκαθιδρύσει μια multicast σύνδεση με το κανάλι αυτό που έχει γίνει broadcast. Έτσι δεν χρειάζεται όλα τα ψηφιοποιημένα κανάλια να ρέουν στο home end του συνδρομητή, όπως γίνεται για παράδειγμα στην καλωδιακή τηλεόραση.

Πηγές της broadcast μετάδοσης μπορεί να είναι ταινίες αποθηκευμένες σε κάποιον server, ή ζωντανή εκπομπή από κάποιον τηλεοπτικό σταθμό που εκπέμπει

απευθείας μετάδοση. Όπως φαίνεται και στην εικόνα 1.4, κάθε πηγή εισάγεται σε έναν κωδικοποιητή broadcast. Οι media servers και ο κωδικοποιητής αντιστοιχούν στο Video head end που περιγράψαμε προηγουμένως. Ο κωδικοποιητής μετατρέπει την ροή video σε πακέτα (packetizes) και συμπεριλαμβάνει σε αυτά έναν αριθμό καναλιού και την multicast address group. Σε αυτήν την διεύθυνση θα συνδεθούν τα set top box, όταν ο χρήστης επιλέγει ένα κανάλι χρησιμοποιώντας το STB.

Το σύστημα της broadcast μετάδοσης, μπορούμε να το περιγράψουμε ως μια σειρά από media servers που περιλαμβάνουν (host) έναν αριθμό από ροές broadcast. Οι media servers υποστηρίζουν τόσο την μετάδοση multicast όσο και unicast. Το unicast χρησιμοποιείται στο video on demand όπως θα δούμε στην συνέχεια. Ένα σύστημα διαχείρισης συνδρομητών (subscriber management system) είναι απαραίτητο για την διαχείριση των χρεώσεων των υπηρεσιών που προσφέρει η IPTV. Εκτός από τις χρεώσεις των συνδρομητών, το σύστημα διαχείρισης συνδρομητών μπορεί να προσφέρει επιπλέον λειτουργίες όπως την μετάδοση broadcast ενός ηλεκτρονικού οδηγού προγραμμάτων τηλεόρασης και να υποστηρίξει διαδραστικές λειτουργίες στο set top box, όπως να προσφέρει περιεχόμενο που έχουν επιλέξει οι συνδρομητές, για παράδειγμα video on demand.

1.4.2 Video on Demand

Στο κάτω μέρος της εικόνας 1.4 φαίνεται η χρήση του video on demand για την παράδοση της υπηρεσίας IPTV. Το video on demand ανταποκρίνεται στην αίτηση κάποιου συνδρομητή που έγινε μέσω του set top box ή του υπολογιστή του. Η ανταπόκριση ρέει, ως μια ακολουθία (sequence) από unicast datagrams, στην IP διεύθυνση του set top box ή του υπολογιστή. Το σύστημα διαχείρισης συνδρομητών (subscriber management system), αναπαράγει μια λίστα από video on demand events, από τα οποία ο συνδρομητής μπορεί να επιλέξει ένα πρόγραμμα. Από την άλλη, ένας IPTV operator, μπορεί να εισάγει μια κάρτα με τη μηνιαία χρέωση του συνδρομητή, που θα περιλαμβάνει λίστα με εκατοντάδες events, το κόστος προβολής τους και τον κωδικό πρόσβασης για την λήψη των επιλεγμένων προγραμμάτων.

Και στις δύο περιπτώσεις, η ροή των IP datagrams θα είναι μια unicast μετάδοση στο set top box ή στον υπολογιστή του συνδρομητή.

1.4.3 Πρότυπα παράδοσης Video

Τα πιο δημοφιλή πρότυπα που μπορούν να χρησιμοποιηθούν, για την παράδοση (delivery) video, σε ένα IPTV σύστημα, είναι το MPEG-1 και το MPEG-2. Ένα πιο πρόσφατο πρότυπο είναι το MPEG-4, που σχεδιάστηκε για να παραδίδει video ποιότητας DVD, παρόμοιο με το MPEG-2, αλλά σε χαμηλότερο ρυθμό δεδομένων (data rates). Το MPEG-4 αλλάζει τις διαστάσεις του video, ώστε να είναι δυνατή η μεταφορά του με οποιονδήποτε ρυθμό δεδομένων, από χαμηλών ταχυτήτων dial up συνδέσεις, μέχρι συνδέσεις υψηλού bandwidth.

Το 2002 η Apple Computer πρόσθεσε την υποστήριξη του MPEG-4 στην τεχνολογία QuickTime και συνεργάστηκε με την Cisco, την IBM, την Philips και άλλες 20 περίπου εταιρείες για να σχηματίσουν την Internet Streaming Media Alliance (ISMA), έτσι ώστε να είναι σίγουρο ότι μια ροή media MPEG-4 που έχει δημιουργηθεί με το προϊόν μιας εταιρείας, θα μπορεί να αναπαραχθεί από την μηχανή αναπαραγωγής κάποιας άλλης.

Το πρότυπο H.264 στην ουσία είναι το μέρος 16 του προτύπου MPEG-4. Παρόλο που το MPEG-4 και το H.264 πλεονεκτούν έναντι του MPEG-2, είναι πολύ δύσκολο για τους πάροχους που διαθέτουν μεγάλη εγκαταστημένη βάση με MPEG-2 set top box, να τα αναβαθμίσουν σε συσκευές συμβατές με το MPEG-4 και το H.264. Αντίθετα, οι νέοι πάροχοι της υπηρεσίας IPTV, όπου οι συνδρομητές τους θα λαμβάνουν καινούργια set top box ή θα χρησιμοποιούν Pentium 4 ή κάποιο διπύρηνο PC για την αναπαραγωγή video, είναι πολύ εύκολο να εξυπηρετηθούν από την τεχνολογία MPEG-4. Κάποια συστήματα δορυφορικής τηλεόρασης, όπως το Direct TV και το DVB-T/S έχουν υιοθετήσει το MPEG-4 για την παράδοση ψηφιακής τηλεόρασης. Εξαιτίας της ποιότητας εικόνας σε χαμηλότερο ρυθμό δεδομένων, προσφέρεται η δυνατότητα να εκπέμπονται περισσότερα κανάλια εντός των ορίων συχνότητας που τους επιτρέπεται να χρησιμοποιούν.

Στην συνέχεια θα δούμε με ποιόν τρόπο γίνεται η παράδοση του video, όταν χρησιμοποιείται το MPEG-2 ως μέθοδος συμπίεσης.

1.4.3.1 Παράδοση με χρήση MPEG-2

Η πιο διαδεδομένη μέθοδος για την παράδοση της IPTV, είναι μέσω της ενθυλάκωσης του MPEG-2 χρησιμοποιώντας το UDP στο επίπεδο μεταφοράς.

Το video μπορεί και να μεταφερθεί απευθείας σε UDP πακέτα χωρίς την χρήση RTP (real time transport protocol). Σε αυτήν την περίπτωση η ροή μετάδοσης ονομάζεται UDP/RAW. Όταν χρησιμοποιείται το UDP/RAW μπορούν να εντοπιστούν κάποιες περιπτώσεις σφαλμάτων ή αλλαγές κατάστασης όπως :

- Να αλλάξει ο αποστολέας
- Να λείπουν synchronization bytes
- Να είναι εσφαλμένο το μέγεθος πακέτου
- Time-outs
- Να υπάρχει υπερβολικό jitter
- Να είναι λάθος το UDP bit rate

Όταν το RTP χρησιμοποιείται με το UDP, δηλαδή στην περίπτωση του UDP/RTP, τα πακέτα γίνονται time stamped και αναγνωρίζονται με την χρήση ενός sequence number. Έτσι επιτρέπεται η ανίχνευση επιπλέον σφαλμάτων εκτός αυτών που αναφέραμε στην περίπτωση του UDP/RAW. Συγκεκριμένα :

- Καθορισμός πακέτων που λαμβάνονται σε λάθος σειρά
- Ανίχνευση πανομοιότυπα πακέτα (duplicate packets)
- Καθορισμός αν υπάρχει απώλεια πακέτου
- Καθορισμός πακέτων που έχουν εσφαλμένο μέγεθος

1.5 Ποιότητα της Υπηρεσίας (Qos)

Η υπηρεσία IPTV συνήθως λειτουργεί πάνω σε ιδιωτικά IP δίκτυα και όχι στο δημόσιο internet. Σε ένα ιδιωτικό IP δίκτυο, ειδικά σχεδιασμένο για IPTV, ο πάροχος υπηρεσιών μπορεί να εξασφαλίσει ποιότητα της υπηρεσίας (*Quality of Service, Qos*) για τους καταναλωτές.

Το IP Qos καθιστά ικανό το δίκτυο να μεταφέρει δεδομένα από χρήστη σε χρήστη (*end-to-end*) με εγγυημένη μέγιστη καθυστέρηση και εγγυημένο ρυθμό μεταφοράς, προκειμένου να καλύψει τις απαιτήσεις του χρήστη, πάντοτε με καθορισμένα συμφωνημένα όρια λάθους.

Σύμφωνα με το CCITT Recommendation E.800, το QoS περιγράφεται ως εξής :

"*Η συλλογική συνέπεια της ποιότητας υπηρεσίας, η οποία καθορίζει τον βαθμό ικανοποίησης του χρήστη ως προς την υπηρεσία*."

Αυτός ο ορισμός συνδέει το QoS με την υπηρεσία που παρέχεται στους χρήστες. Εντούτοις βλέποντας το από την οπτική γωνία ενός δικτύου που παρέχει υπηρεσίες, υπάρχουν συγκεκριμένα σημαντικά ποσοτικά χαρακτηριστικά τα οποία μπορούν να ελεγχθούν έτσι ώστε να παρέχονται συγκεκριμένα επίπεδα ποιότητας υπηρεσίας. Αυτά είναι οι κλήσεις και διασυνδέσεις και η ρυθμοαπόδοση (throughput).

1.5.1 Κλήσεις και διασυνδέσεις

Η καθυστέρηση που υφίστανται τα πακέτα λόγω της κίνησης στο δίκτυο είναι ένας σημαντικός παράγοντας που επηρεάζει αισθητά το QoS. Διάφοροι παράγοντες καθυστέρησης, έχουν διαφορετική επίδραση σε διαφορετικά είδη υπηρεσιών :

- **End-to-end delay**:

Είναι το χρονικό διάστημα της μεταφοράς του πακέτου από τον αποστολέα στον παραλήπτη, μέσω του δικτύου. Όσο πιο μεγάλο είναι το delay, τόσο πιο μεγάλη είναι η πίεση που υποβάλλεται στο πρωτόκολλο μεταφοράς για να λειτουργήσει αποδοτικά. Για το πρωτόκολλο TCP, τα ψηλά επίπεδα καθυστέρησης υπονοούν μεγαλύτερα ποσά δεδομένων που κρατούνται στο δίκτυο εν αναμονή, πράγμα που σημαίνει ότι θα υπάρχει πίεση στους timers και στους counters που σχετίζονται με

το πρωτόκολλο. Πρέπει να σημειωθεί ότι το TCP είναι ένα πρωτόκολλο με "αυτορυθμιζόμενο ρολόι". Ο ρυθμός μετάδοσης του αποστολέα προσαρμόζεται δυναμικά με την ροή των σημάτων πληροφορίας που έρχονται από τον παραλήπτη, μέσω της αντίστροφης κατεύθυνσης των acknowledgments (ACK), που ειδοποιούν τον αποστολέα ότι τα δεδομένα έχουν παραλειφθεί επιτυχώς. Όσο πιο μεγάλη είναι η καθυστέρηση μεταξύ του αποστολέα και του παραλήπτη, τόσο πιο μη ευαίσθητο είναι το πρωτόκολλο σε μικρού χρονικού διαστήματος, δυναμικές αλλαγές στην φόρτιση του δικτύου. Σε εφαρμογές με διαδραστικό ήχο και video, η ύπαρξη καθυστέρησης, προκαλεί μη ανταπόκριση από το σύστημα.

- **Delay variation or jitter:**

Αναφέρεται στην ποικιλία της χρονικής διάρκειας μεταξύ όλων των πακέτων της ίδιας ακολουθίας που ακολουθούν τον ίδιο router. Με μαθηματικούς όρους, το jitter μετρείται σαν η απόλυτη τιμή της πρώτης παραγώγου της ακολουθίας των ατομικών μέτρων καθυστέρησης. Πολύ ψηλά επίπεδα του jitter, προκαλεί την δημιουργία πολύ συντηρητικών υπολογισμών του round trip time από το πρωτόκολλο TCP. Το πρωτόκολλο δηλαδή δεν λειτουργεί αποδοτικά όταν επανέρχεται σε time out για να ξανά-εγκαθιδρύσει την ροή δεδομένων. Ψηλά επίπεδα jitter, δεν μπορούν να γίνουν αποδεκτά από εφαρμογές που βασίζονται στο UDP και είναι εφαρμογές πραγματικού χρόνου, όπως για παράδειγμα το audio ή το video signal.

Οι διαδραστικές εφαρμογές πραγματικού χρόνου (Interactive Real Time applications), όπως για παράδειγμα η μεταφορά ήχου, είναι ευαίσθητες στο end-to-end delay και στο jitter. Οι μεγάλες καθυστερήσεις έχουν ως αποτέλεσμα την μείωση της διάδρασης στην επικοινωνία. Μη διαδραστικές εφαρμογές πραγματικού χρόνου (non-interactive real time applications) , όπως για παράδειγμα εκπομπή μονής κατεύθυνσης (one-way broadcast) , δεν είναι ευαίσθητες ως προς το end-to-end delay αλλά επηρεάζονται από το jitter. Το jitter συνήθως διευθετείται με την χρησιμοποίηση ενός buffer στον παραλήπτη, όπου αποθηκεύονται τα παραλαμβανόμενα πακέτα και αναπαράγονται στην κατάλληλη χρονική μετατόπιση (time offset). Η χρονική μετατόπιση – που ονομάζεται επίσης και "playback point" – καθορίζεται σύμφωνα με το μέγιστο jitter. Εφαρμογές οι οποίες μπορούν να προσαρμόσουν το "playback point" βασισμένες στις αλλαγές της τιμής του jitter

ονομάζονται προσαρμοζόμενες εφαρμογές (adaptive applications). Πακέτα που φτάνουν στον παραλήπτη αφού περάσει το “playback point” που τους αντιστοιχεί, δεν είναι χρήσιμα ως προς την εφαρμογή.

Οι εφαρμογές που δεν είναι πραγματικού χρόνου, συνήθως δεν επηρεάζονται από τυχόν καθυστερήσεις. Εντούτοις, επειδή αυτές οι εφαρμογές μπορεί να χρησιμοποιήσουν την καθυστέρηση ως μέτρο για να ελέγξουν τα ποσοστά της κίνησης στο δίκτυο (π.χ. TCP), ή μπορεί να χρειαστεί να φυλάξουν προσωρινά δεδομένα μέχρι αυτά να γίνουν acknowledged (π.χ. FTP), γι’ αυτό μεγάλες καθυστερήσεις μπορούν επίσης να επηρεάσουν το QoS των εφαρμογών αυτών. Υπάρχουν διάφοροι παράμετροι που επηρεάζουν το end-to-end delay :

- **Καθυστέρηση Μετάδοσης (Transmission Delay)**

Ο χρόνος που χρειάζεται για να μεταφέρουμε όλα τα bits του πακέτου πάνω στην σύνδεση.

- **Καθυστέρηση Μεταφοράς (Propagation Delay)**

Ο χρόνος που χρειάζεται ένα bit για να διασχίσει την σύνδεση μέσω της οποίας γίνεται η μεταφορά δεδομένων.

- **Καθυστέρηση Επεξεργασίας (Processing Delay)**

Ο χρόνος που χρειάζεται για επεξεργασία πακέτου και μετατροπή του σε στοιχείο δικτύου (*network element*).

- **Καθυστέρηση Ουράς (Queuing Delay)**

Ο χρόνος που πρέπει να περιμένει το πακέτο στην ουρά πριν να προγραμματιστεί η μετάδοση του.

Καθυστερήσεις μπορούν επίσης να υπάρχουν στην μεταφορά του πακέτου από το επίπεδο δικτύου στο επίπεδο εφαρμογής και τελικά στον χρήστη. Το QoS δεν δημιουργεί bandwidth. Είναι αδύνατο για κάποιο δίκτυο να δώσει κάτι που δεν έχει, έτσι το bandwidth availability είναι σημείο αναφοράς. Το QoS διαχειρίζεται το bandwidth ανάλογα με τις απαιτήσεις κάποιας εφαρμογής και τα settings κάποιου δικτύου.

Το bandwidth, είναι ο μέγιστος ρυθμός μεταφοράς δεδομένων, ο οποίος μπορεί να εγκαθιδρυθεί μεταξύ δύο σημείων. Πρέπει να σημειωθεί ότι αυτό δεν περιορίζεται μόνο από τη φυσική εσωτερική δόμηση του μονοπατιού που δημιουργείται μεταξύ των επικοινωνούντων δικτύων και παρέχει ένα ανώτατο όριο στο bandwidth που μπορεί να προσφέρει, αλλά επηρεάζεται επίσης από τον αριθμό των άλλων ροών δεδομένων που μοιράζονται κοινούς συντελεστές του ίδιου μονοπατιού.

Το bandwidth που κρατείται για κάποια εφαρμογή δεν είναι πλέον ελεύθερο για τις best effort υπηρεσίες. Η προτεραιότητα των QoS σχεδιαστών ήταν να διασφαλίσουν ότι το best effort traffic δεν θα παρουσιάζει φαινόμενα παρατεταμένης στέρησης μετά τις κρατήσεις που έχουν γίνει. Η χειρότερη περίπτωση πρέπει να είναι οι υπηρεσίες με low priority στις οποίες απλά θα προσφέρονται λιγότερες υπηρεσίες.

1.5.2 Ρυθμοαπόδοση (Throughput)

Το bandwidth είναι σημαντικός παράγοντας για το throughput. Αυτό καθορίζει πόση κίνηση μπορεί να ανεχθεί η εφαρμογή μέσα στο δίκτυο. Άλλοι σημαντικοί παράγοντες είναι τα λάθη, που συνήθως σχετίζονται με το link error rate και οι απώλειες, που συνήθως σχετίζονται με την χωρητικότητα του buffer.

Ορισμένες εφαρμογές, μπορούν να μειώσουν το ποσοστό της κίνησης όταν υπάρχουν ενδείξεις ότι το throughput βρίσκεται σε χαμηλά επίπεδα. Τέτοιες εφαρμογές ονομάζονται rate adaptive. Το εύρος ζώνης εξαρτάται από τα ακόλουθα :

Χαρακτηριστικά σύνδεσης : bandwidth, error rate
Χαρακτηριστικά κόμβου : buffer, processing power

Αξιοπιστία μπορεί να θεωρηθεί σαν ο μέσος όρος σφάλματος στο μέσο. Η αξιοπιστία μπορεί να θεωρηθεί ότι παράγεται από το switching system υπό την έννοια ότι αν το τελευταίο έχει φτωχή διαμόρφωση ή φτωχή εκτέλεση, τότε μπορεί να αλλάξει την σειρά των πακέτων που μεταφέρονται και να τα παραδώσει στον παραλήπτη με διαφορετική σειρά από αυτή που πραγματικά τα μετάδωσε ο αποστολέας ή μπορεί ακόμη να χαθούν πακέτα κατά την μεταφορά τους από τον

ένα router στον άλλο. Η αναξιοπιστία μπορεί να προκαλέσει την αναμετάδοση των πακέτων. Το TCP δεν μπορεί να διακρίνει αν ένα πακέτο χάθηκε λόγω διακοπής στην μεταφορά ή λόγω της συμφόρησης στο δίκτυο. Γι' αυτό όταν χαθεί ένα πακέτο λόγω διακοπής, ο αποστολέας συμπεριφέρεται με τον ίδιο τρόπο που συμπεριφέρεται όταν υπάρχει συμφόρηση. Ο ρυθμός μεταφοράς δεδομένων του αποστολέα δηλαδή μειώνεται με την ενεργοποίηση των αλγορίθμων αποφυγής συμφόρησης, παρόλο που δεν παρατηρήθηκε συμφόρηση στο δίκτυο.

Στην περίπτωση του UDP, σε εφαρμογές που βασίζονται στον ήχο και στο video, η αναξιοπιστία προκαλεί παραμόρφωση του πραγματικού αναλογικού σήματος στο άκρο του παραλήπτη. Ανάλογα, όταν αναφερόμαστε στην διαφοροποίηση ποιότητας υπηρεσίας, αναφερόμαστε στην διαφοροποίηση ενός ή περισσότερων, από τους τέσσερις συντελεστές μέτρησης της ποιότητας (*delay, jitter, bandwidth, loss of data*) για μια συγκεκριμένη κατηγορία του traffic.

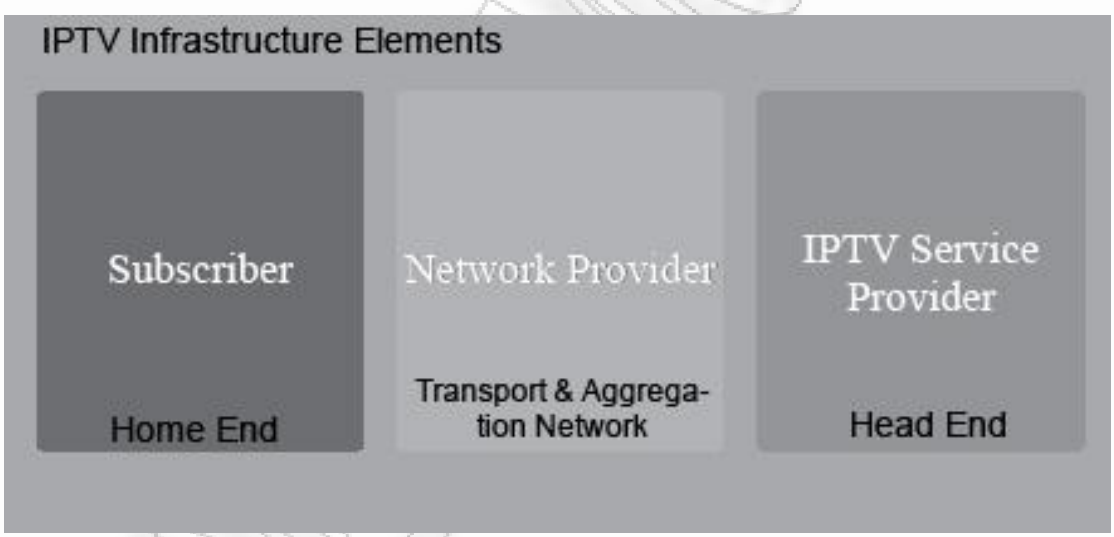
Το Internet αποτελείται από μια συλλογή από routers και συνδέσμους μετάδοσης. Οι routers παραλαμβάνουν ένα εισερχόμενο πακέτο, καθορίζουν το επόμενο interface στο οποίο θα κατευθυνθούν και τοποθετούν το πακέτο στην ουρά εξόδου του επιλεγμένου interface. Οι σύνδεσμοι μεταφοράς έχουν χαρακτηριστικά για το delay, το bandwidth και την αξιοπιστία. Φτωχή ποιότητα υπηρεσίας παρατηρείται όταν το επίπεδο της κίνησης (traffic) που επιλέγει ένα συγκεκριμένο interface, ξεπεράσει το bandwidth μεταφοράς του interface για μια παρατεταμένη χρονική περίοδο. Σε αυτές τις περιπτώσεις, οι ουρές εξόδου του router που σχετίζονται με το συγκεκριμένο interface, αρχίζουν να γεμίζουν , προκαλώντας επιπλέον καθυστέρηση στη μεταφορά (*αυξανόμενο jitter και delay*), μέχρι που σε κάποιο σημείο η ουρά γεμίζει και ο router τότε αναγκάζεται να αρχίσει να απορρίπτει πακέτα (*μειωμένη αξιοπιστία*). Το γεγονός αυτό αναγκάζει τις προσαρμοζόμενες ροές δεδομένων να μειώσουν το ρυθμό που στέλνουν τα δεδομένα (*sending rate*) για να μειωθούν έτσι οι απώλειες λόγω της συμφόρησης με την μείωση του bandwidth για κάθε εφαρμογή.

Ανάλογα, όταν αναφερόμαστε στην ποιότητα υπηρεσίας, κοιτάζουμε αυτά τα τέσσερα μετρικά σαν τις βασικές παραμέτρους της ποιότητας και πρέπει να σημειωθεί ότι υπάρχει μια ποικιλία από γεγονότα που συμβαίνουν στο δίκτυο και επηρεάζουν τις τιμές των παραμέτρων αυτών.

2. Ζητήματα Ασφαλείας στην IPTV

Το περιβάλλον της IPTV θα έχει διαφορετικά σύνολα απειλών, ανάλογα με τη λειτουργία της. Συγκεκριμένα, ο αντίκτυπος των γεγονότων παραβίασης ασφάλειας στο head end είναι μεγαλύτερος από τον αντίκτυπο των γεγονότων παραβίασης ασφάλειας στο home end. Το aggregation και το δίκτυο μεταφορών θα έχουν διάφορες απειλές εξ αιτίας των κοινών υπηρεσιών που υποστηρίζονται.

Στην συνέχεια, εστιάζουμε στον προσανατολισμό της ασφάλειας με βάση την αρχιτεκτονική της IPTV . Αρχικά θα γίνει μια εισαγωγή στις απειλές στο περιβάλλον της IPTV και μετά θα παρουσιάσουμε παραδείγματα των ευπαθειών (vulnerabilities) στα διαφορετικά τμήματα της υποδομής. Τα τμήματα αντιπροσωπεύονται στο σχήμα.



Εικόνα 2.1 : Τμήματα της Αρχιτεκτονικής της IPTV

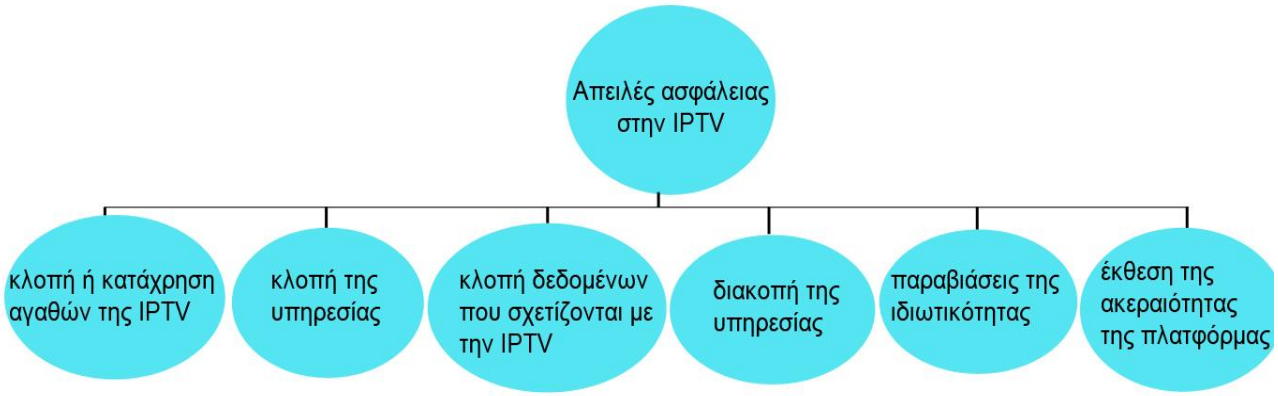
2.1 Απειλές στο περιβάλλον IPTV

Η IPTV κληρονομεί όλες τις αδυναμίες ασφαλείας που έχει το δίκτυο που χρησιμοποιείται για μεταφορά. Δηλαδή, διατηρεί τις ευπάθειες που υπάρχουν στο TCP/IP και στα τμήματα του δικτύου μεταφοράς. Επομένως, τα ίδια βασικά μέτρα που απαιτούνται για να προστατεύσουν οποιοδήποτε άλλο δίκτυο TCP/IP ισχύουν για την υποδομή IPTV.

Υπάρχουν μερικά κρίσιμα χαρακτηριστικά στοιχείων σχετικών με την IPTV που πρέπει να προστατευθούν. Το βίντεο και ο ήχος είναι ευαίσθητοι στις καθυστερήσεις και στην απώλεια πακέτων και ακόμα κι αν τα πρωτόκολλα και οι εφαρμογές έχουν κάποια ενσωματωμένη ανθεκτικότητα, η κακή επικοινωνία έχει αρνητικές επιπτώσεις στην εμπειρία πελατών.

Ειδικοί μηχανισμοί πρέπει να εφαρμοστούν για να ελέγξουν τις ευπάθειες που σχετίζονται με το TCP/IP και να εξασφαλίσουν την σωστή λειτουργία της υπηρεσίας IPTV. Τα συστατικά της IPTV έχουν συγκεκριμένα χαρακτηριστικά που πρέπει να εξεταστούν κατά τη διάρκεια της αξιολόγησης ασφάλειας. Για παράδειγμα, οι υπηρεσίες middleware τείνουν να τρέχουν πάνω σε HTTP/HTTPS, και υπάρχουν πολλές γνωστές αδυναμίες ασφάλειας που θα μπορούσε να εκμεταλλευτεί μια κακόβουλη οντότητα για να αποκτήσει τον έλεγχο του middleware server. Επιπλέον, τα συστατικά μέρη της IPTV έχουν μη εμφανείς αδυναμίες ασφαλείας που δεν εντοπίζονται, αναφέρονται ή αξιολογούνται από τις στάνταρ διαδικασίες και τα IT tools ελέγχου ασφαλείας.

Στο σχήμα απεικονίζονται οι απειλές ασφαλείας τις οποίες θα εξετάσουμε στην συνέχεια. Αυτές είναι: κλοπή ή κατάχρηση αγαθών της IPTV, κλοπή της υπηρεσίας, κλοπή δεδομένων που σχετίζονται με την IPTV, διακοπή της υπηρεσίας, παραβιάσεις ιδιωτικότητας και έκθεση της ακεραιότητας της πλατφόρμας.



Εικόνα 2.2 : Απειλές στην ασφάλεια της IPTV.

2.1.1 Κλοπή ή κατάχρηση αγαθών (assets) της IPTV

Τα βασικά επιχειρηματικά προσόντα της υπηρεσίας IPTV είναι τα ψηφιακά αντίγραφα του περιεχομένου που αποθηκεύεται μέσα στην υποδομή, ή μεταφέρονται μέσω της υποδομής. Υπάρχει ο κίνδυνος να κλαπούν από τρίτους ή να μετατραπούν έτσι ώστε να επηρεάσουν την δυνατότητα του πάροχου υπηρεσίας να αποκομίσει αξία από αυτή. Η παραποίηση σχετίζεται με κακόβουλες ενέργειες στο χειρισμό της υποδομής της IPTV, από τον επιτιθέμενο, για την εκπλήρωση σκοπών εκτός των καθορισμένων. Ακολουθεί κατάλογος πιθανών κακόβουλων πράξεων :

- Σύλληψη του ψηφιακού πιστοποιητικού από ένα STB, για την χρήση περιεχομένου και την εκπομπή ή την αναδιανομή της ροής σε άλλους συνδρομητές.
- Σύλληψη πακέτων στο οικιακό δίκτυο και το IP υποδίκτυο.
- Έξοδος του περιεχομένου από μια αναλογική θύρα εξόδου σε μια εξωτερική συσκευή εγγραφής.
- Έξοδος του περιεχομένου από μια ψηφιακή θύρα εξόδου σε μια εξωτερική συσκευή εγγραφής.
- Εκτέλεση μεγαλύτερου αριθμού αναπαραγωγών, από τον επιτρεπόμενο.
- Πρόσβαση σε παράνομο περιεχόμενο (π.χ. πειρατικό περιεχόμενο)

- Παράκαμψη συμβατικών συστημάτων έλεγχου πρόσβασης, για να αποκτήσουν πρόσβαση σε περιεχόμενο.
- Αντιγραφή περιεχομένου από τον αποθηκευτικό ενός βίντεο server ή ενός STB.

2.1.2 Κλοπή της υπηρεσίας

Κλοπή της υπηρεσίας θεωρείται οποιαδήποτε δραστηριότητα με την οποία ένας τελικός χρήστης λαμβάνει τις υπηρεσίες της IPTV, χωρίς να καταβάλει το απαιτούμενο επίπεδο συνδρομής. Αυτό περιλαμβάνει σφάλματα στο σύστημα ή μικρές τροποποιήσεις που αυξάνουν τον αριθμό των καναλιών καθώς και την πρόσβαση σε Video on Demand, χωρίς την κατάλληλη συνδρομή. Με την κατάχρηση των middleware και άλλων διαθέσιμων εφαρμογών, μπορεί να επιτραπεί σε συνδρομητές η δυνατότητα να προσθέσουν κανάλια στην συνδρομή τους χωρίς να πληρώσουν γι αυτά. Αυτό μπορεί να συμβεί σε περίπτωση που τα VLANs και τα access controls δεν έχουν αναπτυχθεί σωστά. Οι εισβολείς μπορούν να προωθήσουν το video broadcast stream σε μη εξουσιοδοτημένα set top box, τα οποία χρησιμοποιούν έγκυρη άδεια από διαφορετικό πακέτο. Ένας άλλος τρόπος κλοπής υπηρεσίας, είναι η τροποποίηση του λογισμικού εντός του set top box και ο προγραμματισμός του ώστε να δίνει πρόσβαση σε μπλοκαρισμένα κανάλια. Ακολουθεί κατάλογος πιθανών κακόβουλων ενεργειών :

- Παράνομη απόκτηση ενός πλεονεκτήματος του πάροχου υπηρεσίας, με σκοπό να του στερήσει τις νόμιμες απολαβές από αυτό.
- Κατάχρηση (defrauding) του πάροχου υπηρεσίας IPTV.
- Μη εξουσιοδοτημένη διαγραφή ή μετατροπή, των πληροφοριών χρέωσης.
- Κλωνοποίηση (cloning) του STB ή της έξυπνης κάρτας.
- Εφαρμογή στοιχείων αναπαραγωγής του VOD, όπως η μακριά παύση (long pause), για παραπάνω χρόνο από τον καθορισμένο.
- Παράκαμψη συμβατικών συστημάτων ελέγχου πρόσβασης.

- Μαζική ανακατασκευή και διασπορά πληροφορίας.

2.1.3 Κλοπή δεδομένων που σχετίζονται με την IPTV

Το περιβάλλον της IPTV περιλαμβάνει μεγάλο ποσό δεδομένων σχετικό με τους συνδρομητές, την υποδομή και την υπηρεσία. Η απειλή των δεδομένων των συνδρομητών, βρίσκεται στα πλαίσια της απειλής της ιδιωτικότητας. Τα δεδομένα που σχετίζονται με την IPTV, μπορούν να χρησιμοποιηθούν από ανταγωνιστές ή από υποκλοπείς. Η απειλή αυτή μπορεί να προκαλέσει μεγάλη απώλεια πελατών. Τα δεδομένα αυτά αποθηκεύονται στο head end και στο δίκτυο εγγραφής (aggregation network). Για παράδειγμα, το middleware περιέχει πληροφορίες για τις προτιμήσεις των συνδρομητών και το DSLAM πληροφορίες για τις αιτήσεις video. Πληροφορίες για τον λογαριασμό και την χρέωση, περιλαμβάνονται στους servers που σχετίζονται με την επιχείρηση. Αυτά θα μπορούσαν να χρησιμοποιηθούν για κλοπή ταυτότητας ή κάτι αντίστοιχο. Ακολουθεί κατάλογος πιθανών κακόβουλων πράξεων :

- Μη εξουσιοδοτημένη πρόσβαση σε ιδιωτικά δεδομένα.
- Κλοπή της καταγραφής (records) ενεργειών των συνδρομητών.
- Κλοπή δεδομένων διαχείρισης της υπηρεσίας και των συνδρομητών.
- Κλοπή των metadata.

2.1.4 Διακοπή της υπηρεσίας

Οι εισβολείς θα μπορούσαν να αποκτήσουν τον έλεγχο, μεγάλου αριθμού set top box. Θα μπορούσαν να προκαλέσουν μια επίθεση άρνησης υπηρεσίας, στοχεύοντας τον middleware server , μπλοκάροντας έτσι την πρόσβαση στην υπηρεσία IPTV. Άλλες πιθανές επιθέσεις περιλαμβάνουν αλλαγή των ρυθμίσεων του DSLAM, ή των κανόνων multicast, ώστε να προκληθεί διακοπή της υπηρεσίας. Παρακάτω ακολουθεί κατάλογος πιθανών κακόβουλων πράξεων :

- Δημιουργία κίνησης (traffic) και υπερχείλισης πακέτων. Αυτό έχει ως αποτέλεσμα τα εξής :

- Άρνηση υπηρεσίας σε ένα τελικό σημείο χρήστη (user end point), στέλνοντας μεγάλο αριθμό έγκυρων πακέτων, μερικά από τα οποία μπορεί να επηρεάσουν και στοιχεία του δικτύου. Έτσι η εφαρμογή παύει, λόγω υπερφόρτωσης.
- Υπερχείλιση πακέτων στο endpoint, προκαλούν στα στοιχεία του δικτύου και στον video server, κατάρρευση (crash), επανεκκίνηση ή εξάντληση όλων των πόρων.
- Άρνηση υπηρεσίας, που μπορεί να επιτευχθεί με κατανάλωση bandwidth ή πόρων.
- Υπάρχουν πιθανές αρνητικές επιπτώσεις για χιλιάδες συνδρομητές.

- Μετατροπή σε πακέτα και μηνύματα, έχει τα ακόλουθα αποτελέσματα.
  - Αχρήστευση των endpoints με άκυρα μηνύματα. Επίθεση άρνησης υπηρεσίας σε endpoints, στέλνοντας μεγάλο αριθμό άκυρων μηνυμάτων, προκαλώντας στο endpoint παύση λειτουργίας, επανεκκίνηση ή εξάντληση όλων των πόρων.
  - Μετατροπή σε μηνύματα πρωτοκόλλου. Στέλνοντας τέτοια μηνύματα στην συσκευή, μειώνεται η επίδοση σε σημείο που είναι αδύνατο να επεξεργάζεται κανονικά μηνύματα.
  - Μηνύματα που έχουν υποστεί μετατροπή μπορούν να δημιουργήσουν υπερχείλιση στο buffer.
  - Πιθανές αρνητικές επιπτώσεις για χιλιάδες συνδρομητές.
- Μηνύματα εξαπάτησης (spoofed), έχουν τα ακόλουθα αποτελέσματα.
  - Είναι επίθεση άρνησης υπηρεσίας που προκαλεί διακοπή της υπηρεσίας IPTV, προκαλώντας μια συνεδρία IPTV να λήξει πρόωρα.
  - Εξαπάτηση μηνυμάτων έλεγχου. Κακόβουλη κίνηση έλεγχου (traffic control), εισάγεται στις επικοινωνίες, προκαλώντας δυσλειτουργία στις εφαρμογές και στους video server ή στέλνεται η κίνηση (traffic) σε λάθος

προορισμό. Κατασκευασμένα μηνύματα έλεγχου χρησιμοποιούνται για να αλλάξουν την δομή των δέντρων διανομής multicast και να επηρεάσουν την διανομή δεδομένων.

- Κατασκευασμένα υποτιθέμενα μηνύματα συνδρομητών IPTV οδηγούν σε ανταποκρίσεις εφαρμογών ή βίντεο server.
- Αλλαγή των IP και Mac διευθύνσεων για να εξαπατήσουν τις αντίστοιχες διευθύνσεις άλλων χρηστών και να κλέψουν IPTV streams.

2.1.5 Παραβιάσεις Ιδιωτικότητας

Οι εισβολείς μπορούν να αποκτήσουν πρόσβαση σε servers με βάσεις δεδομένων, που βρίσκονται αποθηκευμένες προσωπικές πληροφορίες, ή μπορούν να υποκλέψουν transactions από τα set top boxes. Πρέπει να αναπτυχθούν μηχανισμοί για να μην εκτεθούν οι προσωπικές πληροφορίες των συνδρομητών. Ακολουθεί κατάλογος πιθανών κακόβουλων πράξεων :

- Διείσδυση στην ιδιωτικότητα του συνδρομητή και υποκλοπή δεδομένων.
- Χρήση tracking pattern για την ανακάλυψη ταυτότητας, παρουσίας και χρήσης της υπηρεσίας IPTV.
- Υποκλοπή κίνησης, μη εξουσιοδοτημένη καταγραφή κίνησης, συμπεριλαμβανομένης καταγραφής πακέτων, packet logging και packet snooping.
- Μη εξουσιοδοτημένη πρόσβαση σε media stream συνδρομητών.
- Μη εξουσιοδοτημένη πρόσβαση σε management traffic.
- Υποκλοπή ταυτότητας κάποιου συνδρομητή, που δίνει την δυνατότητα σε μη εξουσιοδοτημένη επικοινωνία και κλοπή πληροφοριών.
- Ανακατασκευή των media. Μη εξουσιοδοτημένη παρακολούθηση, καταγραφή, αποθήκευση, ανακατασκευή, μετάφραση και εξαγωγή στοιχείων από οποιαδήποτε πτυχή της επικοινωνίας μέσω video,

συμπεριλαμβανομένου της ταυτότητας, παρουσίας και στατιστικών του συνδρομητή.

- Μη εξουσιοδοτημένη αποκάλυψη των δυνατοτήτων των συνδρομητών IPTV.
- Μη εξουσιοδοτημένη αποκάλυψη προηγούμενης ή πρόσφατης χρήσης ή δραστηριότητας των συνδρομητών IPTV.
- Επιθέσεις αναπαραγωγής που περιλαμβάνουν media. Αναπαραγωγή των media που έχουν υποκλαπεί για κακόβουλο κέρδος, ή εισβολή στην ιδιωτικότητα με την αναπαραγωγή media που προορίζονται για προσωπική χρήση.
- Παρεμπόδιση και μετατροπή στοιχείων μπορεί να προκαλέσει τα παρακάτω :
    - Πλαστοπροσωπία και υποκλοπή κατά την διάρκεια της επικοινωνίας. Η εισαγωγή, η διαγραφή, η αντικατάσταση ή οποιαδήποτε άλλη μετατροπή της επικοινωνίας με την χρήση πληροφοριών που αλλάζουν το περιεχόμενο , την ταυτότητα και τα στατιστικά οποιουδήποτε μέλους της επικοινωνίας.
    - Μη εξουσιοδοτημένη πρόσβαση, μετατροπή ή διαγραφή των πληροφοριών του οδηγού ηλεκτρονικού προγράμματος (electronic program guide, EPG).
    - Πειρατεία στο video stream. Εισαγωγή, μετατροπή ή διαγραφή κάποιου video stream, με παράνομο τρόπο.
    - Spam στο IPTV. Εμφάνιση αυθαίρετων pop – up διαφημίσεων.
    - Μη εξουσιοδοτημένη εκπομπή υλικού.
- Έκθεση των δεδομένων εφαρμογής των συνδρομητών μπορεί να προκαλέσει τα εξής :

- μη εξουσιοδοτημένη αποκάλυψη, δημιουργία, μετατροπή, διαγραφή δεδομένων που έχουν δημιουργηθεί και χρησιμοποιούνται σε εφαρμογές που έχουν αποκλειστική πρόσβαση συνδρομητές.
- Εκτίθενται οι πληροφορίες που είναι αποθηκευμένες στο δίκτυο του πάροχου υπηρεσίας, εκ μέρους των συνδρομητών.

- Έκθεση πληροφοριών για τους συνδρομητές, μπορεί να προκαλέσει :
  - Social engineering για να αποκτηθούν πληροφορίες για τους συνδρομητές.
  - Μη εξουσιοδοτημένη αποκάλυψη, δημιουργία, μετατροπή, διαγραφή πληροφοριών για τους συνδρομητές. Για παράδειγμα διεύθυνση, τηλέφωνο, αριθμός λογαριασμού, πληροφορίες πιστωτικής κάρτας κτλ.

2.1.6 Έκθεση της ακεραιότητας της πλατφόρμας

Η ακεραιότητα της πλατφόρμας που προσφέρει την υπηρεσία IPTV, πρέπει να επιτευχθεί, για να μην κλιμακώνονται περιστατικά ασφάλειας. Αν κάποιος εισβολέας καταφέρει να εκθέσει την ακεραιότητα της πλατφόρμας, θα μπορεί να κλιμακώσει τις επιθέσεις του και να καταλάβει μεγαλύτερο μέρος της υπηρεσίας. Οι εισβολείς μπορούν να χρησιμοποιήσουν την υπηρεσία web, από τον middleware server ώστε να αποκτήσουν τον έλεγχό της υπηρεσίας IPTV και να κλιμακώσουν την επίθεση με το να συνδεθούνε και σε άλλες υπηρεσίες στο head-end δίκτυο. Ακολουθεί κατάλογος πιθανών κακόβουλων πράξεων :

- Παρουσίαση ψευδών στοιχείων δικαιωμάτων και εξουσιοδότησης. Έχει ως αποτέλεσμα τα εξής :
  - Παρουσίαση ψεύτικης εξουσιοδότησης ως αληθινή, με σκοπό την παραπλάνηση.
  - Παρουσίαση κωδικού πρόσβασης, κλειδιού ή ψηφιακού πιστοποιητικού που ανήκει σε κάποιον άλλο.

- Μη εξουσιοδοτημένη λήψη και χρήση πληροφοριών εξουσιοδότησης που σχετίζονται με υπηρεσίες συνδρομητών.(π.χ.username / password, κλειδιά συνόδου).
- Μη εξουσιοδοτημένη λήψη και χρήση πληροφοριών εξουσιοδότησης που σχετίζονται με την διαχείριση.

- Έκθεση εγκατεστημένου λογισμικού, δεδομένων σχετικών με την υπηρεσία και της διαχείρισης του συστήματος. Έχει ως αποτέλεσμα τα εξής :
  - Εισαγωγή κακόβουλου λογισμικού, malware, spyware στην υπηρεσία.
  - Μη εξουσιοδοτημένη αντιγραφή, εγκατάσταση, μετατροπή ή διαγραφή λογισμικού και αρχείων διαχείρισης.
  - Μη εξουσιοδοτημένη αντιγραφή, προβολή, δημιουργία, μετατροπή ή διαγραφή δεδομένων που σχετίζονται με την υπηρεσία (π.χ.system logs, πληροφορίες χρέωσης, κλειδιά κρυπτογράφησης, κτλ).
  - Μη εξουσιοδοτημένη δημιουργία ή μετατροπή πληροφοριών που σχετίζονται με την υπηρεσία συνδρομητών.
  - Μη εξουσιοδοτημένη ενεργοποίηση ή απενεργοποίηση θυρών πρωτοκόλλου (protocol ports).

- Εξάντληση πόρων, μπορεί να οδηγήσει στα παρακάτω :
  - Ελαττώματα σε λογισμικό και hardware, που προκαλούν εξάντληση των πόρων μνήμης σε ένα στοιχείο του δικτύου (π.χ. buffers).
  - Ελαττώματα σε λογισμικό και hardware, που προκαλούν κατανάλωση των περισσότερων πόρων CPU σε ένα στοιχείο του δικτύου.
  - Σφάλματα σε λογισμικό και hardware που περιορίζουν το διαθέσιμο bandwidth σε ένα σύνδεσμο επικοινωνίας.
  - Σφάλματα σε λογισμικό και hardware που δημιουργούν άχρηστα μηνύματα που μειώνουν τους πόρους του bandwidth.

- Μη εξουσιοδοτημένα scans και εξερεύνηση δικτύου, έχει ως αποτέλεσμα :
    - Οι εισβολείς μπορούν να τρέξουν ένα λογισμικό για scan, που είναι διαθέσιμο στο κοινό, σε έναν host που έχει σύνδεση σε ένα IPTV δίκτυο και οι υπηρεσίες στις συσκευές που παρακολουθούνται θα ανταποκριθούν, προσφέροντας πληροφορίες στον επιτιθέμενο.
    - Vulnerability scanning και χαρτογράφηση δικτύου. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν ένα λογισμικό για scan, σε έναν host με σύνδεση σε ένα δίκτυο IPTV, αναλύοντας την δομή της συσκευής και την τοπολογία του δικτύου.
    - Μη εξουσιοδοτημένη απομακρυσμένη πρόσβαση σε λογισμικό ή σε λειτουργίες που ανήκουν σε μια συσκευή.
- Μη εξουσιοδοτημένη διαχείριση, έχει τα παρακάτω αποτελέσματα :
    - Μη εξουσιοδοτημένη χρήση μιας αίτησης διαχείρισης ή εκτέλεση εντολών διαχείρισης.
    - Μετατροπή σε μηνύματα πρωτοκόλλου διαχείρισης, για παράδειγμα, μετατροπή του configuration του modem για να επιτρέψει ή να αποκλείσει συγκεκριμένα πρωτόκολλα, όπως το SNMP.
    - Μετατροπή μηνυμάτων διαχείρισης από απόσταση.
    - Μη εξουσιοδοτημένο περιεχόμενο διαχείρισης. Για παράδειγμα, διαγραφή περιεχομένου video ή μετατροπή της ημερομηνίας που θα είναι το video διαθέσιμο στο κοινό (trigger date).
    - Μη εξουσιοδοτημένη διαχείριση συνδρομητών. Για παράδειγμα, ενέργειες εφοδιασμού από συνδρομητές, που περιλαμβάνουν αναβάθμιση ή υποβάθμιση προνομίων.

2.2 Απειλές στο Head End

Μέσα στο head end, είναι σημαντικό να εξεταστούν οι απειλές που τίθενται από το προσωπικό του πάροχου της υπηρεσίας IPTV. Τα συστήματα που εδρεύουν σε κέντρα δεδομένων ή σε κεντρικά γραφεία είναι περισσότερο εκτεθειμένα σε εσωτερικές παρά σε εξωτερικές απειλές. Μερικές φορές οι υπάλληλοι έχουν πρόσβαση σε περισσότερες πληροφορίες απ' ότι θα έπρεπε να έχουν.

Οι εσωτερικές εφαρμογές πρέπει να είναι οργανωμένες κατά τέτοιο τρόπο ώστε η πρόσβαση να περιορίζεται μόνο στους εξουσιοδοτημένους χρήστες και οι εσωτερικές τροποποιήσεις πρέπει πάντα να καταγράφονται και να επιβεβαιώνονται από ένα δεύτερο πρόσωπο. Έτσι μειώνονται οι πιθανότητες να υπάρξει εσωτερική απάτη.

Οι επιχειρήσεις επενδύουν εκατομμύρια στην εφαρμογή μιας ασφαλούς υποδομής, σε monitoring hardware και σε εργαλεία λογισμικού. Εντούτοις, οι operators είναι συνήθως χαμηλόμισθοι και λαμβάνουν την ελάχιστη κατάρτιση, δημιουργώντας την τέλεια ευκαιρία για τους χάκερ να αποκτήσουν ιδιωτικές πληροφορίες.

Στην συνέχεια εξετάζονται οι ευπάθειες διαφόρων τμημάτων του head end, καθώς και οι απειλές που τα επηρεάζουν.

2.2.1 Απειλές στις Ανατροφοδοτήσεις Βίντεο

Υπάρχει η απειλή ***διακοπής της υπηρεσίας***. Αυτό το αγαθό (asset) είναι εκτεθειμένο στην καταστροφή των φυσικών μέσων. Ο απρόσεκτος χειρισμός των φυσικών μέσων μπορεί να οδηγήσει στην καταστροφή τους. Η διακοπή υπηρεσίας της ζωντανής τηλεοπτικής ανατροφοδότησης μπορεί να προκληθεί μέσω του δικτύου μεταφοράς ή μέσω της δυσλειτουργίας του εξοπλισμού.

Υπάρχουν διάφορες απειλές που έχουν επιπτώσεις στην ***ακεραιότητα της πλατφόρμας***. Ένας πάροχος υπηρεσίας IPTV μπορεί να χρησιμοποιήσει παράνομο περιεχόμενο κατά λάθος ή μετά από μια σκόπιμη τροποποίηση νόμιμου περιεχομένου, από έναν χειριστή (operator). Ο πάροχος υπηρεσίας IPTV μπορεί να λάβει τηλεοπτική ανατροφοδότηση από έναν παράνομο προμηθευτή που πιθανόν

θα συμπεριλαμβάνει τροποποιημένο ακατάλληλο περιεχόμενο. Επιπλέον, μπορεί να υπάρξει φυσική ζημιά στα media, προκαλώντας αρνητικές επιπτώσεις σε διάφορα τμήματα του περιεχομένου. Τα ψηφιακά αντίγραφα του περιεχομένου μπορούν να υποστούν βλάβη κατά τη μεταφορά τους ή κατά την αποθήκευσή τους.

Υπάρχουν μερικοί κίνδυνοι ***κλοπής ή αφαίρεσης***, όπου στις περισσότερες περιπτώσεις αποτελούν εσωτερική επίθεση. Θα μπορούσε να υπάρξει μη εξουσιοδοτημένη αντιγραφή (replication) ή αφαίρεση των φυσικών μέσων, ενώ οι χειριστές της υπηρεσίας IPTV, με την πρόσβαση που έχουν στα ψηφιακά μέσα, θα μπορούσαν να αντιγράψουν (replicate) το περιεχόμενο.

2.2.2 Απειλές στο Video Switch

Υπάρχει η απειλή της ***διακοπής υπηρεσίας*** σε αυτό το αγαθό. Η μη εξουσιοδοτημένη πρόσβαση στο video switch μπορεί να οδηγήσει στην αποδοχή μιας μη εξουσιοδοτημένης ανατροφοδότησης video, προς φόρτωση, από την υπηρεσία IPTV. Αυτή η κακόβουλη ενέργεια θα ήταν πιθανότατα το αποτέλεσμα μιας εσωτερικής επίθεσης. Μη εξουσιοδοτημένες εντολές διαχείρισης μπορούν να σταματήσουν την ανατροφοδότηση video και να προκαλέσουν διακοπή της υπηρεσίας στους συνδρομητές. Το overwriting του λογισμικού ή των δεδομένων του video switch, θα μπορούσε να προκαλέσει στο video switch αναμονή (hang), crash ή πρόωρο τερματισμό.

Στο video switch υπάρχουν μερικές πρόσθετες απειλές που σχετίζονται με την ***κλοπή των αγαθών της IPTV***. Η μη εξουσιοδοτημένη πρόσβαση στο video switch μπορεί να οδηγήσει στην εισαγωγή μιας νόμιμης ροής video σε μια συσκευή καταγραφής με σκοπό την αναρμόδια χρήση και διανομή της ροής.

2.2.3 Απειλές στην πύλη εισαγωγής Video (Ingest Gateway, Video Capture)

Η πύλη εισαγωγής εκτίθεται σε απειλές σχετικές με ***την κλοπή ή την αφαίρεση***. Η μη εξουσιοδοτημένη πρόσβαση στην πύλη εισαγωγής μπορεί να οδηγήσει στην αποθήκευση του εισαγόμενου περιεχομένου σε μια συσκευή αποθήκευσης, με σκοπό την αναρμόδια χρήση και διανομή του.

Υπάρχουν πρόσθετες απειλές οι οποίες σχετίζονται με τη ***διακοπή της υπηρεσίας***. Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης μπορεί να οδηγήσει στην χρήση της για να στείλει κακόβουλες εντολές στο δίκτυο διαχείρισης περιεχομένου (π.χ. kill command). Το overwriting του λογισμικού ή των δεδομένων μιας πύλης εισαγωγής, θα μπορούσαν να προκαλέσουν στην πύλη εισαγωγής αναμονή, crash ή πρόωρο τερματισμό.

2.2.4 Απειλές στο λογισμικό της πλατφόρμας

Τα παρακάτω ισχύουν για όλα τα λειτουργικά συστήματα που υποστηρίζουν IPTV εφαρμογές. Τα worms, οι ιοί και οι κατευθυνόμενες (directed) επιθέσεις μπορούν να χρησιμοποιηθούν για να προκαλέσουν ***άρνηση παροχής της υπηρεσίας*** μέσα στην πλατφόρμα IPTV.

Η μη εξουσιοδοτημένη πρόσβαση στο λειτουργικό σύστημα, μπορεί να οδηγήσει στη διαγραφή αρχείων που είναι απαραίτητα για το λειτουργικό σύστημα. Μη εξουσιοδοτημένα αιτήματα ή πακέτα που έχουν υποστεί κακόβουλη μετατροπή, μπορούν να σταλούν στο λειτουργικό σύστημα και να προκαλέσουν την αφαίρεση κρίσιμων αρχείων.

Τα λειτουργικά συστήματα έχουν πολλές υπηρεσίες που τρέχουν σε ανοικτές θύρες. Οι εισβολείς είναι σε θέση να χρησιμοποιήσουν αυτές τις θύρες για να ***διακόψουν την υπηρεσία***, αν δεν υπάρχει κατάλληλο configuration του λειτουργικού.

Τα worms και οι ιοί θα μπορούσαν να χρησιμοποιηθούν για να μολύνουν έναν μεγάλο αριθμό κεντρικών υπολογιστών μέσα στο head end και να προκαλέσουν διακοπή της υπηρεσίας.

Επιπλέον, υπάρχουν απειλές που επηρεάζουν την ***ακεραιότητα της πλατφόρμας***. Υπό ορισμένες συνθήκες, για παράδειγμα με την κακόβουλη χρήση ενός rootkit από τους εισβολείς, θα μπορούσε να γίνει τροποποίηση των αρχείων configuration της πλατφόρμας software/OS.

2.2.5 Απειλές στο Σύστημα διαχείρισης περιεχομένου

Το σύστημα διαχείρισης περιεχομένου, είναι εκτεθειμένο σε απειλές της ***ακεραιότητας της πλατφόρμας*** που σχετίζονται με τις ευπάθειες υπερχείλισης των buffer. Αυτός ο τύπος ευπάθειας προκύπτει εξ αιτίας των φτωχών ελέγχων ασφαλείας στον αρχικό κώδικα εφαρμογής. Οι εισβολείς μπορούν να εκμεταλλευτούν αυτές τις ευπάθειες εισάγοντας strings μεγαλύτερα σε διάρκεια από τον buffer. Τροποποιήσεις στο σύστημα διαχείρισης περιεχομένου μπορούν να επιτρέψουν στους εισβολείς για να εισάγουν backdoors ή malware στο σύστημα και να λάβουν αντίγραφα των ψηφιακών αγαθών.

Οι εισβολείς μπορούν να προκαλέσουν ***διακοπή της υπηρεσίας***. Μπορούν να στείλουν μηνύματα πρωτοκόλλου που προκαλούν στην εφαρμογή παύση, ή μπορούν να στείλουν εντολές (management commands) που διακόπτουν την εφαρμογή. Το overwriting του λογισμικού ή των δεδομένων του συστήματος διαχείρισης περιεχομένου, μέσω υπερχείλισης του buffer θα μπορούσε προκαλέσει στο σύστημα αναμονή, crash ή πρόωρο τερματισμό.

Υπάρχει η απειλή ***κλοπής των αγαθών της IPTV***. Το λογισμικό του συστήματος διαχείρισης περιεχομένου, μπορεί να χειριστεί με κακόβουλο τρόπο από τους εισβολείς για να λάβουν αντίγραφα των ψηφιακών προτερημάτων.

2.2.6 Απειλές στα κλειδιά SRTP

Το SRTP (*secure real-time transport protocol*) ορίζει ένα προφίλ του RTP (*real-time transport protocol*), το οποίο παρέχει κρυπτογράφηση, αυθεντικοποίηση και ακεραιότητα μυνημάτων και προστασία από επιθέσεις τύπου replay, στα δεδομένα του RTP, στις multicast και unicast εφαρμογές.

Μπορεί να χρησιμοποιηθεί μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης για να διαγραφεί κάποιο SRTP κλειδί. Αυτό το είδος της επίθεσης μπορεί να πραγματοποιηθεί τόσο από εσωτερικούς όσο και εξωτερικούς εισβολείς και θα μπορούσε να προκαλέσει την ***διακοπή της υπηρεσίας*** IPTV στους συνδρομητές. Τα SRTP κλειδιά μπορούν να συλληφθούν από τους εισβολείς και να χρησιμοποιηθούν για να δημιουργήσουν ψεύδη κλειδιά ή για να αποκτήσουν πρόσβαση σε κρυπτογραφημένο περιεχόμενο. Το υλικό που σχετίζεται με τα SRTP κλειδιά μπορεί να συλληφθεί κατά τη μεταφορά, μέσω packet sniffer ή MITM. Αυτού του είδους οι επιθέσεις απαιτούν πρόσβαση στο middleware VLAN μεταξύ του CA / DRM συστήματος και του head-end σημείου εξόδου.

2.2.7 Απειλές στην εφαρμογή Vod

Η υπηρεσία διανομής περιεχομένου είναι υπεύθυνη για την προσωρινή αποθήκευση του περιεχομένου βίντεο. Η μη εξουσιοδοτημένη διαγραφή, τροποποίηση ή παρακολούθηση των μεταδεδομένων του περιεχομένου βίντεο που είναι αποθηκευμένα σε μια προσωρινή μνήμη σε ένα βίντεο streaming server, μπορεί να επιτευχθεί μέσω πρόσβασης στην κονσόλα διαχείρισης ή μέσω κακόβουλου λογισμικού. Αυτό το είδος της επίθεσεις θα προκαλέσει την ***διακοπή της υπηρεσίας IPTV***.

Στην περίπτωση που τα μεταδεδομένα δεν είναι κρυπτογραφημένα, ο επιτιθέμενος μπορεί να ανακτήσει αντίγραφα των μεταδεδομένων, για να τα χρησιμοποιήσει μελλοντικά.

2.2.8 Απειλές στο Video Streaming Software

- Υπερχείλιση του buffer, μπορεί να προκληθεί από μηνύματα που λαμβάνονται μέσω του VOD VLAN ή μέσω του δικτύου διανομής περιεχομένου και έχει ως αποτέλεσμα το overwriting του video streaming software.
- Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, δίνει στον επιτιθέμενο την δυνατότητα να στείλει εντολές μέσω του management network ή εντολές και μηνύματα πρωτοκόλλου μέσω του VOD VLAN, που μπορούν να τερματίσουν την λειτουργία του video streaming λογισμικού (π.χ. εντολές “kill”, “exit”).

2.3 Απειλές στο Δίκτυο του Πάροχου της Υπηρεσίας IPTV

2.3.1 Ευπάθειες πρωτοκόλλου multicast (IGMP)

Οι ευπάθειες που υπάρχουν στο πρωτόκολλο multicast είναι πολύ μεγαλύτερης σημασίας από τις ευπάθειες άλλων πρωτοκόλλων. Αυτό συμβαίνει εξαιτίας του μεγάλου αντίκτυπου, που έχει η εκμετάλλευση αυτών των ευπαθειών. Με μία μόνο επίθεση επηρεάζονται αρκετές εκατοντάδες συνδρομητές και set top box, αντίστοιχα. Με βάση τον τρόπο λειτουργίας του πρωτοκόλλου multicast εντοπίζονται τρία ζητήματα ασφαλείας.

- Εμπιστευτικότητα
- Έλεγχος πρόσβασης
- Κίνηση πρωτοκόλλου ελέγχου (control protocol traffic)

Η κίνηση (traffic) του multicast προορίζεται για πολλαπλούς αποδέκτες. Η κρυπτογράφηση του περιεχομένου για τον κάθε ένα αποδέκτη είναι μια διαδικασία υψηλής πολυπλοκότητας. Για αυτό το λόγο η διαδικασία αυτή γίνεται από το DRM λογισμικό.

Οποιαδήποτε πληροφορία διανέμεται από το πρωτόκολλο multicast δεν προστατεύεται από μηχανισμούς που παρέχει το ίδιο το πρωτόκολλο, για αυτό υπάρχει η ανάγκη επιπρόσθετων εφαρμογών για την εξασφάλιση της προστασίας των πληροφοριών. Όσον αφορά τον έλεγχο πρόσβασης, τα set top box επιτρέπεται να μπουν σε ομάδες (groups) χωρίς ιδιαίτερους περιορισμούς. Το πρωτόκολλο multicast δεν παρέχει μηχανισμούς ελέγχου πρόσβασης (access control) και στηρίζεται σε λειτουργίες των DSLAM και edge gateway για αυθεντικοποίηση και επικύρωση (validate) χρηστών. Από τη στιγμή που ένα set top box θα έχει μπει επιτυχώς σε ένα multicast group κάποιος hacker μπορεί να στείλει traffic στο group και να προκαλέσει ***διακοπή της υπηρεσίας***.

Ένα άλλο είδος επίθεσης είναι η αποστολή ενός broadcast μηνύματος, που να ισχυρίζεται ότι υπάρχει υψηλός ρυθμός απωλειών στο κανάλι ή υψηλή συμφόρηση

(high congestion), έτσι ώστε να μειωθεί ο ρυθμός μετάδοσης, επηρεάζοντας με αυτόν τον τρόπο τους υπόλοιπους συνδρομητές.

Επιπλέον μπορεί να εισαχθεί κακόβουλη κίνηση (traffic) στην επικοινωνία, που μπορεί να προκαλέσει δυσλειτουργία σε εφαρμογές ή να στείλει την traffic σε λάθος προορισμό. Η Traffic του πρωτοκόλλου multicast μπορεί εύκολα να γίνει spoofed, το οποίο οφείλεται στην έλλειψη ελέγχου αυθεντικοποίησης μέσα στην ροή.

2.3.2 Απειλές κατά την multicast μετάδοση περιεχομένου

Τροποποιημένα ή κατασκευασμένα πακέτα igmp μπορούν να σταλούν, μέσω του δικτύου διανομής περιεχομένου, στο σύστημα διαχείρισης περιεχομένου και στους video cache streaming servers και να προκαλέσουν υπερχείλιση του buffer και κατάρρευση στο σύστημα. Μια επίθεση αναπαραγωγής (replay attack), μπορεί να έχει ως αποτέλεσμα τη μη εξουσιοδοτημένη συμμετοχή του επιτιθέμενου σε μια ροή multicast. Για παράδειγμα, ένα κατασκευασμένο μήνυμα συμμετοχής (join) μπορεί να έχει ως αποτέλεσμα τη συμμετοχή του επιτιθέμενου στην ομάδα διανομής περιεχομένου. Με αυτόν τον τρόπο μπορεί να επιτύχει την απόκτηση περιεχομένου χωρίς την καταβολή της απαιτούμενης συνδρομής. Κατασκευασμένα μηνύματα αποχώρησης μπορεί να προκαλέσουν την δημιουργία μεγάλου αριθμού bogus query μηνυμάτων από τον multicast δρομολογητή.

Κατασκευασμένα πακέτα igmp μπορούν να χρησιμοποιηθούν από ένα επιτιθέμενο, για να προσποιηθούν (masquerade) έναν multicast δρομολογητή με σκοπό την απόκτηση περιεχομένου. Υπάρχει ο κίνδυνος ο επιτιθέμενος να έχει την δυνατότητα να χρησιμοποιήσει εργαλεία packet sniffing χρησιμοποιώντας έναν αναλυτή (analyzer) πρωτοκόλλου ή χρησιμοποιώντας hosts στο IP υποδίκτυο. Με την χρήση εργαλείων sniffing ή μιας man in the middle (mitm) επίθεσης στο δίκτυο διανομής περιεχομένου, ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση και να παρακολουθήσει το περιεχόμενο το οποίο διανέμεται μέσω του δικτύου αυτού. Τα igmp πακέτα τα οποία παρακολουθούνται από κάποιον επιτιθέμενο παρέχουν πληροφορίες για τα

multicast τα οποία είναι ενεργά και για τις αντίστοιχες συσκευές οι οποίες συμμετέχουν σε αυτά. Αυτές οι επιθέσεις απαιτούν πρόσβαση στο δίκτυο διανομής περιεχομένου που βρίσκεται ανάμεσα στο κεντρικό σύστημα διαχείρισης περιεχομένου και στους video cache streaming servers που βρίσκονται στα περιφερειακά head ends.

2.3.3 Απειλές κατά την unicast μετάδοση περιεχομένου

Το FTP (*File Transfer Protocol*) είναι ένα ευρέως χρησιμοποιούμενο πρωτόκολλο σε δίκτυα τα οποία υποστηρίζουν το πρωτόκολλο TCP/IP, όπως το internet. Ο υπολογιστής που τρέχει εφαρμογή FTP client μόλις συνδεθεί με τον server μπορεί να εκτελέσει ένα πλήθος διεργασιών όπως ανέβασμα αρχείων στον server, κατέβασμα αρχείων από τον server, μετονομασία ή διαγραφή αρχείων από τον server κτλ. Το πρωτόκολλο είναι ένα ανοιχτό πρότυπο. Είναι δυνατό κάθε υπολογιστής που είναι συνδεδεμένος σε ένα δίκτυο, να διαχειρίζεται αρχεία σε ένα άλλο υπολογιστή του δικτύου, ακόμη και εάν ο δεύτερος διαθέτει διαφορετικό λειτουργικό σύστημα.

Η μη εξουσιοδοτημένη τροποποίηση των πακέτων ftp κατά την μεταφορά τους, έχει ως αποτέλεσμα την απώλεια της αξιοπιστίας (fidelity) της ροής video. Τα πακέτα ftp μπορούν να συλληφθούν κατά τη μεταφορά τους με την χρήση packet sniffer ή μιας επίθεσης man in the middle (mitm). Όταν συλληφθούν, μπορούν μέσω μιας συσκευής εγγραφής να αποθηκευτούν, ώστε να είναι διαθέσιμα για προσωπική χρήση ή διανομή.

Ένας επιτιθέμενος μπορεί να δημιουργήσει υπερχείλιση (flood) πακέτων ftp στον video cache streaming server, έτσι ώστε να προκαλέσει κατάρρευση στο server. Η υπερχείλιση στην traffic του δικτύου διανομής περιεχομένου μπορεί να καταναλώσει όλο το bandwidth στις συνδέσεις του συστήματος περιεχομένου με τους video cache servers.

2.3.4 Απειλές στο real time protocol (RTP)

Κατασκευασμένα πακέτα rtp ή μη εξουσιοδοτημένη τροποποίηση πακέτων rtp κατά την μεταφορά τους, έχουν ως αποτέλεσμα την απώλεια της αξιοπιστίας της ροής video ή την εισαγωγή πλαστού περιεχομένου, στο περιεχόμενο που μεταφέρεται. Αυτό μπορεί να επιτευχθεί με την εισαγωγή κατασκευασμένων πακέτων στη ροή rtp ή μέσω μιας επίθεσης man in the middle. Πακέτα rtp μπορούν να συλληφθούν κατά την μεταφορά τους με τη χρήση packet sniffer ή μέσω μιας επίθεσης man in the middle. Όταν συλληφθούν μπορεί να εισαχθούν σε μια συσκευή εγγραφής έτσι ώστε να είναι διαθέσιμα για προσωπική χρήση ή διανομή.

Ένας επιτιθέμενος μπορεί να στείλει μια υπερχείλιση rtp πακέτων στον video cache streaming server με σκοπό να προκαλέσει κατάρρευση στον server. Η υπερχείλιση της traffic στο δίκτυο διανομής περιεχομένου μπορεί να καταναλώσει όλο το bandwidth του δικτύου.

2.3.5 Απειλές στο real time streaming protocol (RTSP)

Οι εντολές του rtsp προωθούνται από τον middleware server στον master video streaming server, έτσι ώστε να εδραιωθεί η σύνδεση μεταξύ του συνδρομητή και του video cache streaming server. Τα rtsp πακέτα μπορούν συλληφθούν, να τροποποιηθούν ή να κατασκευαστούν κατά την μεταφορά τους. Απειλές που σχετίζονται με την κακόβουλη τροποποίηση και την χρήση των rtsp πακέτων, είναι οι παρακάτω:

- Υπερχείλιση του buffer
- Κατάρρευση του master video streaming server
- Κατάρρευση συστήματος με αποτέλεσμα την ***διακοπή της υπηρεσίας video on demand (vod)***

2.3.6 Απειλές στην ροη video mpeg-2/mpeg-4

Οι απειλές και οι ευπάθειες τη ροής video mpeg-2 και της ροής video mpeg-4 είναι κοινές και παρουσιάζονται παρακάτω:

- Υπερχείλιση του buffer και κατάρρευση του συστήματος
- Απώλεια της πιστότητας (fidelity) της ροής mpeg-2/mpeg-4 με την εισαγωγή θορύβου στην ροή mpeg-2/mpeg-4 ή μέσω επίθεσης mad in the middle (mitm).
- Πρόσβαση σε περιεχόμενο χωρίς την καταβολή απαιτούμενης συνδρομής με την χρήση packet sniffer ή μέσω επίθεσης mad in the middle (mitm).
- Επιθέσεις αποκρυπτογράφησης σε mpeg-2/mpeg-4 κρυπτογραφημένα πακέτα, που έχουν συλληφθεί με τη χρήση packet sniffer ή μέσω επίθεσης mad in the middle (mitm).
- Κατάρρευση στο set top box (stb) δημιουργώντας μια υπερχείλιση από mpeg-2/mpeg-4 πακέτα στο set top box.
- Κατανάλωση του bandwidth δημιουργώντας υπερχείλιση της traffic σε μια σύνδεση video on demand (vod).

2.3.7 Σηματοδότηση της Ποιότητας Υπηρεσίας (Qos signaling)

Το RSVP είναι ένα πρωτόκολλο σηματοδοσίας, που παρέχει αρχικοποίηση καιέλεγχο κράτησης πόρων για την υλοποίηση ολοκληρωμένων υπηρεσιών, που σκοπόέχουν την παροχή προσομοίωσης μεταγωγής σε IP δίκτυα. Παρέχει το υψηλότερο επίπεδο QoS ,σε όρους εγγύησης υπηρεσιών και γραμμικότητας στην κράτηση πόρων από όλες τις υπάρχουσες τεχνολογίες. Το πρωτόκολλο λειτουργεί ως εξής:

- Οι αποστολείς χαρακτηρίζουν την εξερχόμενη κίνηση με όρους ορίων bandwidth και καθυστέρησης. Το RSVP στέλνει ένα PATH μήνυμα από τον αποστολέα που περιέχει την πληροφορία για την κίνηση και τον προορισμό. Το μήνυμα αυτό μεταδίδεται στον παραλήπτη.

- Για να κάνει κράτηση πόρων ο παραλήπτης στέλνει ένα μήνυμα RESV (reservation request) προς την κατεύθυνση του αποστολέα, με τον τύπο της υπηρεσίας που θέλει.
- Αν έστω και ένας δρομολογητής, στην διαδρομή προς τον αποστολέα, δεν μπορεί να εξασφαλίσει τους ζητούμενους πόρους στέλνει μήνυμα λάθους στον παραλήπτη. Ειδάλλως το μήνυμα προωθείται στον επόμενο δρομολογητή.
- Όταν ο πιο κοντινός στον αποστολέα δρομολογητής μπορεί να εξασφαλίσει τους πόρους στέλνει ένα μήνυμα επιβεβαίωσης στον αποστολέα. Κατόπιν αρχίζει η μετάδοση.

Εδώ εντοπίζεται η απειλή της ***έκθεσης της ακεραιότητας της πλατφόρμας***. Τα μηνύματα rsvp μπορούν να κατασκευαστούν ή να τροποποιηθούν για κακόβουλη χρήση από έναν επιτιθέμενο κατά τη μεταφορά τους και να σταλούν στο σύστημα διαχείρισης περιεχομένου ή στους video cache streaming servers. Οι απειλές που σχετίζονται με την κακόβουλη χρήση των rsvp μηνυμάτων αναφέρονται παρακάτω:

- Δημιουργία μη εξουσιοδοτημένης ροής δεδομένων που σχετίζεται με την QoS στο δίκτυο διανομής περιεχομένου.
- Τροποποίηση μιας υπάρχουσας ροής δεδομένων που σχετίζεται με την QoS.
- Κατάρευση στον server με την κακόβουλη χρήση τροποποιημένων δρομολογητών οι οποίοι τροποποιούν τα περιεχόμενα των rsvp μηνυμάτων.
- Τροποποίηση του πεδίου dscp στην επικεφαλίδα του ip πακέτου με σκοπό την υπερχείλιση του συγκεκριμένου dscp ή την τροποποίηση μιας συγκεκριμένης ροής που σχετίζεται με την QoS.
- Κατάρρευση στο σύστημα διαχείρισης περιεχομένου ή στους video cache streaming servers λόγω υπερχείλισης του buffer.
- Κατάρρευση στο σύστημα διαχείρισης περιεχομένου ή στους video cache streaming servers λόγω υπερφόρτωσης τους συστήματος.
- Κατανάλωση ολόκληρου του bandwidth στο δίκτυο διανομής περιεχομένου λόγω υπερχείλισης της κίνησης στο δίκτυο.

2.4 Απειλές στο Home End του συνδρομητή της IPTV

2.4.1 Set Top Box (STB)

Υπάρχουν αρκετά διαφορετικά μοντέλα STB διαθέσιμα στην αγορά. Κάποια είναι κατασκευασμένα έχοντας λογισμικό σχεδιασμένο αποκλειστικά για αυτά. Κάποια άλλα βασίζονται σε λειτουργικά συστήματα ανοικτού κώδικα. Πρόσφατα, σχεδιάστηκαν κάποια STB που μπορούν να χρησιμοποιήσουν τεχνολογίες PC, επιτρέποντας έτσι στους συνδρομητές να φορτώσουν το δικό τους λειτουργικό σύστημα, middleware και DRM clients.

Τα STB χρησιμοποιούνται από την βιομηχανία της καλωδιακής τηλεόρασης εδώ και αρκετά χρόνια. Ο σκοπός τους είναι η αποκωδικοποίηση του ψηφιακού σήματος σε αναλογικό σήμα, για την αναπαραγωγή του από την τηλεόραση. Η IPTV, ομοίως, χρησιμοποιεί τα STB για την αποκωδικοποίηση της ψηφιακής πληροφορίας, εφ' όσον η τηλεόραση δεν διαθέτει τέτοιους μηχανισμούς.

Τα STB, περιλαμβάνουν κάποια βασικά επίπεδα ασφαλείας, τα οποία διαχειρίζονται οι ιδιοκτήτες του περιεχομένου. Αυτά περιλαμβάνουν την δυνατότητα να δίνεται εξουσιοδότηση, από τον ιδιοκτήτη στον συνδρομητή, για πρόσβαση στον τύπο του περιεχομένου που έχει επιλέξει ο συνδρομητής. Τα περισσότερα συστήματα πρόσβασης, υποστηρίζονται από έξυπνες κάρτες, για την αποθήκευση πληροφοριών αυθεντικοποίησης του συνδρομητή. Αυτές οι έξυπνες κάρτες χρησιμοποιούν την ευελιξία και την δύναμη των συστημάτων PKI, που υποστηρίζονται από το ITU X.509.

Η PKI (*Public Key Infrastructure*) αποτελεί ένα συνδυασμό λογισμικού, τεχνολογιών ασύμμετρης κρυπτογραφίας και διαδικασιών, ο οποίος κατά βάση πιστοποιεί την εγκυρότητα κάθε εμπλεκόμενου σε μια ψηφιακή συναλλαγή. Η PKI πιστοποιεί την ταυτότητα μιας πιστοποιημένης οντότητας υπογράφοντας το δημόσιο κλειδί της και δημοσιεύοντάς το, μαζί με πληροφορίες σχετικά με την ταυτότητα της οντότητας, σε ένα πιστοποιητικό. Παράλληλα διατηρεί καταλόγους με τα έγκυρα, τα ληγμένα αλλά και τα ανακληθέντα πιστοποιητικά. Οι κυριότεροι μηχανισμοί ασφάλειας τους οποίους καλύπτει η PKI είναι οi εξής:

- Απόρρητο της επικοινωνίας (Confidentiality): Τα δεδομένα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση με μηχανισμούς ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κρυπτογράφησης κατά την αποστολή τους.
- Ακεραιότητα (Integrity): Τα δεδομένα προστατεύονται από μη εξουσιοδοτημένη τροποποίηση μέσω μηχανισμών κρυπτογράφησης όπως οι ηλεκτρονικές υπογραφές.
- Αυθεντικοποίηση (Authentication): Πραγματοποιείται επιβεβαίωση της ταυτότητας ενός ατόμου ή της πηγής αποστολής δεδομένων.
- Μη Αρνηση Αποδοχής (Non-Repudiation): Η Μη Αρνηση Αποδοχής συνδυάζει τις υπηρεσίες της Πιστοποίησης και της Ακεραιότητας και διασφαλίζει ότι μία συναλλαγή η οποία πραγματοποιήθηκε ηλεκτρονικά δε μπορεί να αμφισβητηθεί από τα συμβαλλόμενα μέρη. Για παράδειγμα ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε το μήνυμα.

Το X.509 προσδιορίζει τη δομή, τα πεδία και τα γενικά πρότυπα, που πρέπει να κατέχουν τα ψηφιακά πιστοποιητικά και οι ψηφιακές υπογραφές. Χρησιμοποιώντας τα πιστοποιητικά του X.509 , ως μέρος του περιεχομένου του STB, ο πάροχος της υπηρεσίας, έχει την δυνατότητα να εφαρμόζει μέτρα ασφαλείας ανά συνδρομητή. Για παράδειγμα, τα αιτήματα των συνδρομητών μπορούν να υπογράφονται ψηφιακά, με την χρήση του ψηφιακού πιστοποιητικού του συνδρομητή. Ωστόσο, υπάρχει ο κίνδυνος κάποιος hacker να πάρει τον έλεγχο του STB. Συλλαμβάνοντας το ψηφιακό πιστοποιητικό του STB, θα έχει την δυνατότητα να αιτείται περιεχόμενο και να διανέμει με broadcast μετάδοση κάποια ροή, σε άλλους συνδρομητές. Ακόμα χειρότερη είναι η περίπτωση στην οποία ο hacker θα συλλάβει το ψηφιακό πιστοποιητικό του πάροχου του περιεχομένου, όπου θα έχει την δυνατότητα να τροποποιεί την ροή και να περιλαμβάνει σε αυτήν ό,τι πληροφορία επιθυμεί. Στην συνέχεια, θα δούμε πώς τα set top box μπορούν να χειραγωγηθούν από έναν hacker, πραγματοποιώντας επιθέσεις που θα έχουν ως αποτέλεσμα να αποκτήσει ελεύθερη πρόσβαση σε περιεχόμενο ή να προκαλέσει διακοπή στην υπηρεσία.

2.4.2 Απειλές στα λογισμικά που εκτελούνται στο STB

2.4.2.1 Απειλές στο λογισμικό του DRM

- Υπερχείλιση του buffer, μπορεί να προκληθεί από μηνύματα που λαμβάνονται μέσω του middleware VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου (π.χ. WLAN). Αυτή η ευπάθεια του DRM μπορεί να προκαλέσει αντικατάσταση (overwriting) του λογισμικού DRM, που θα έχει ως αποτέλεσμα την ***διακοπή της υπηρεσίας***.

- Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, δίνει στον επιτιθέμενο την δυνατότητα να στείλει εντολές, όπως “kill” και “exit” στο λογισμικό DRM, μέσω του middleware VLAN ή μέσω κάποιου μη ασφαλούς οικιακού δικτύου και να προκαλέσει τον τερματισμό του DRM λογισμικού. Τέτοιες εντολές διαχείρισης μπορούν να εκτελεστούν και με την χρήση κακόβουλου λογισμικού (malware) και θα έχουν το ίδιο αποτέλεσμα.

2.4.2.2 Απειλές στο λογισμικό middleware client

- Υπερχείλιση του buffer, μπορεί να προκληθεί από μηνύματα που λαμβάνονται μέσω του middleware VLAN ή ενός μη ασφαλούς οικιακού δικτύου και έχει ως αποτέλεσμα την αντικατάσταση (overwriting) του λογισμικού του middleware client. Η αντικατάστασή του, προκαλεί στο λογισμικό κατάρρευση ή πρόωρο τερματισμό, που οδηγούν σε ***διακοπή της υπηρεσίας.***

- Με την χρήση packet sniffer ή μέσω μιας επίθεσης man in the middle (MITM) στο middleware VLAN ή με την εγκατάσταση spyware στο STB, μπορεί να γίνει υποκλοπή των αλληλεπιδράσεων των χρηστών.

- Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, δίνει στον επιτιθέμενο την δυνατότητα να στείλει εντολές όπως “kill” και “exit”, μέσω του middleware VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου και να προκαλέσουν στο λογισμικό κατάρρευση ή πρόωρο τερματισμό, οδηγώντας σε ***διακοπή της υπηρεσίας***.

2.4.2.3 Απειλές στο λογισμικό της πλατφόρμας του STB

- Υπερχείλιση του buffer μπορεί να προκληθεί από μηνύματα που λαμβάνονται μέσω της σύνδεσης WAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου και έχει ως αποτέλεσμα την αντικατάσταση (overwriting) του λογισμικού της πλατφόρμας του STB. Η αντικατάσταση του λογισμικού προκαλεί κατάρρευση ή πρόωρο τερματισμό στο λογισμικό, που οδηγεί στην ***διακοπή της υπηρεσίας***.

- Με την εγκατάσταση spyware στο STB μπορεί να γίνει υποκλοπή των αλληλεπιδράσεων των χρηστών.

- Οι μη εξουσιοδοτημένες εντολές διαχείρισης ή τα μηνύματα πρωτοκόλλου (π.χ. snmp), που λαμβάνονται μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου, μπορούν να προκαλέσουν τερματισμό στο σύστημα (π.χ. εντολή “reboot”), οδηγώντας σε ***διακοπή της υπηρεσίας***. Το ίδιο αποτέλεσμα μπορεί να επιτευχθεί και με την χρήση κακόβουλου λογισμικού (malware).

2.4.2.4 Απειλές στα διαπιστευτήρια του STB

- Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, δίνει στον επιτιθέμενο την δυνατότητα να στείλει εντολές μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου, που έχουν ως αποτέλεσμα την διαγραφή των διαπιστευτηρίων του STB. Η διαγραφή των διαπιστευτηρίων του STB, εμποδίζει την αυθεντικοποίηση του STB στην υπηρεσία IPTV, που οδηγεί στην ***διακοπή της υπηρεσίας***.

- Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, δίνει στον επιτιθέμενο την δυνατότητα να στείλει εντολές μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου, που έχουν ως αποτέλεσμα την τροποποίηση ή την αλλοίωση των διαπιστευτηρίων του STB. Η αλλοίωση των διαπιστευτηρίων του STB, μπορεί να οδηγήσει στην τροποποίηση της λήξης τους,

υποδεικνύοντας ότι δεν έχουν λήξει, που έχει ως αποτέλεσμα την ***κλοπή της υπηρεσίας IPTV***. Επιπλέον, η αλλοίωση των διαπιστευτηρίων του STB μπορεί να οδηγήσει στην τροποποίηση της λήξης τους, υποδεικνύοντας ότι έχουν λήξει, που έχει ως αποτέλεσμα την ***διακοπή της υπηρεσίας IPTV***.

2.4.2.5 Απειλές στο Ψηφιακό Πιστοποιητικό του πάροχου του λογισμικού και του STB

- Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης μπορεί να δώσει στον επιτιθέμενο την δυνατότητα να στείλει εντολές, μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου, που έχουν ως αποτέλεσμα την διαγραφή ή την τροποποίηση του ψηφιακού πιστοποιητικού του παρόχου του λογισμικού και του ψηφιακού πιστοποιητικού του STB. Μια τέτοια εισβολή μπορεί να είναι αποτέλεσμα εξωτερικής ή εσωτερικής επίθεσης. Μια εσωτερική επίθεση μπορεί να προέλθει από κάποιον διαχειριστή (operator). Μια εξωτερική επίθεση απαιτεί πρώτα πρόσβαση στο STB. Η διαγραφή ή η τροποποίηση του ψηφιακού πιστοποιητικού, εμποδίζει την αυθεντικοποίηση του νόμιμου παρόχου του λογισμικού και την αυθεντικοποίηση του STB, αποτρέποντας έτσι την αναβάθμιση του λογισμικού, patches κτλ. και προκαλώντας ***διακοπή της υπηρεσίας IPTV***.

- Ένας ανεξάρτητος (rogue) πάροχος λογισμικού, μπορεί να στείλει ένα πλαστό ψηφιακό πιστοποιητικό μαζί με ένα παράνομο λογισμικό, έτσι ώστε να παρουσιάσει (masquerade) το λογισμικό ως νόμιμο.

- Μια πλαστή λίστα ανάκλησης πιστοποιητικού μπορεί να σταλεί στο STB, ανακαλώντας το ψηφιακό πιστοποιητικό ενός νόμιμου πάροχου λογισμικού. Αυτό θα έχει ως αποτέλεσμα την διακοπή της αναβάθμισης του λογισμικού, των patches και θα προκαλέσει ***διακοπή της υπηρεσίας IPTV***.

2.4.2.6 Απειλές στα Δημόσια Κλειδιά που χρησιμοποιούνται για τα Ψηφιακά Πιστοποιητικά

Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, μπορεί να δώσει την δυνατότητα στον επιτιθέμενο να στείλει εντολές, μέσω του management VLAN ή ενός μη ασφαλούς οικιακού δικτύου, που θα έχουν ως αποτέλεσμα τη διαγραφή ή την τροποποίηση των αποθηκευμένων δημοσίων κλειδιών του STB, ή την εισαγωγή πλαστών δημοσίων κλειδιών.

Η διαγραφή ή η αλλοίωση των αποθηκευμένων δημοσίων κλειδιών, μπορεί να εμποδίσει την αυθεντικοποίηση των νόμιμων ψηφιακών υπογραφών και των ψηφιακών πιστοποιητικών, που θα έχει ως αποτέλεσμα την ***διακοπή της υπηρεσίας IPTV***.

2.4.3 Απειλές στο User Storage

2.4.3.1 Απειλές στο κατεβασμένο περιεχόμενο

- Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, δίνει στον επιτιθέμενο την δυνατότητα να στείλει εντολές μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου που θα έχουν ως αποτέλεσμα την διαγραφή, την αλλοίωση ή την τροποποίηση του κατεβασμένου περιεχομένου. Αυτό οδηγεί στην αδυναμία της αναπαραγωγής (playback) του κατεβασμένου περιεχομένου.

- Εάν ο επιτιθέμενος έχει πρόσβαση στο υλικό που σχετίζεται με τα κλειδιά αποκρυπτογράφησης, μπορεί να δημιουργήσει ένα bit by bit αντίγραφο του μη κρυπτογραφημένου κατεβασμένου περιεχομένου και να το διανείμει σε άλλους χρήστες στερώντας τα έσοδα στον ιδιοκτήτη του περιεχομένου.

- Η αλλοίωση του αντίγραφο (local copy) των δικαιωμάτων του περιεχομένου, του συνδρομητή, που είναι αποθηκευμένα στο DRM, έχει ως αποτέλεσμα ο συνδρομητής να μην έχει πρόσβαση στο περιεχόμενο.

- Η τροποποίηση της λήξης του αντιγράφου, των δικαιωμάτων περιεχομένου του συνδρομητή η οποία θα υποδεικνύει ότι αυτά έχουν λήξει (ενώ δεν έχουν), έχει ως αποτέλεσμα την διακοπή της πρόσβασης του συνδρομητή στο κατεβασμένο περιεχόμενο.

- Η διαγραφή του αντιγράφου των δικαιωμάτων περιεχομένου του συνδρομητή, μπορεί να υποδείξει στο λογισμικό DRM ότι ο συνδρομητής δεν έχει δικαιώματα στο κατεβασμένο περιεχόμενο. Αυτό θα έχει ως αποτέλεσμα την διακοπή της πρόσβασης του συνδρομητή στο κατεβασμένο περιεχόμενο.

2.4.3.2 Απειλές στο περιεχόμενο που έχει δημιουργηθεί από χρήστη

Αυτού του είδος το περιεχόμενο έχει δημιουργηθεί από third party εφαρμογές που είναι προαιρετικά αποθηκευμένες στο stb. Ένα παράδειγμα μιας τέτοιας εφαρμογής είναι η οργάνωση video, φωτογραφιών, μουσικής κ.τ.λ. σε album ή σε θέματα (themes)

- Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης δίνει στον επιτιθέμενο την δυνατότητα να στείλει εντολές μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου που θα έχουν ως αποτέλεσμα την διαγραφή ή την τροποποίηση του περιεχομένου που έχει δημιουργηθεί από χρήστη. Η εισβολή αυτή μπορεί να είναι αποτέλεσμα εσωτερικής ή εξωτερικής επίθεσης. Μια εσωτερική επίθεση μπορεί να πραγματοποιηθεί από έναν διαχειριστή. Μια εξωτερική επίθεση απαιτεί πρώτα πρόσβαση στο stb. Η μη εξουσιοδοτημένη διαγραφή ή τροποποίηση του περιεχομένου που έχει δημιουργηθεί από χρήστη εμποδίζει την αναπαραγωγή του.

2.4.4 Απειλές στην οικιακή πύλη πολυμεσικής επικοινωνίας

- Κατασκευασμένες snmp εντολές μπορούν να ληφθούν μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου.
- Επιθέσεις άρνησης υπηρεσίας (dos) για παράδειγμα αλλοιωμένα μηνύματα, υπερχείλιση κίνησης, υπερχείλιση του buffer στην οικιακή πύλη πολυμεσικής επικοινωνίας, μπορούν να ληφθούν μέσω ενός μη ασφαλούς οικιακού δικτύου ή μέσω οποιουδήποτε VLAN στο wan interface. Από τη στιγμή που ο επιτιθέμενος θα έχει αποκτήσει πρόσβαση στην οικιακή πύλη πολυμεσικής επικοινωνίας μπορεί να εκτελέσει αυθαίρετες διοικητικές εντολές συμπεριλαμβανομένου του τερματισμού του συστήματος.

2.4.5 Απειλές στο DSLAM

2.4.5.1 Απειλές στις πληροφορίες audience metering

- Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, μπορεί να δώσει στον επιτιθέμενο την δυνατότητα, να στείλει εντολές μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου που θα έχουν ως αποτέλεσμα την διαγραφή ή την τροποποίηση των πληροφοριών audience metering, ή την δημιουργία διπλότυπων αυτών των πληροφοριών. Αυτή η απειλή θα μπορούσε να πραγματοποιηθεί μέσω μιας εσωτερικής ή εξωτερικής επίθεσης ή με την χρήση κακόβουλου λογισμικού (malware).

- Με τη χρήση εργαλείων που είναι διαθέσιμα στο ευρύ κοινό, ένας επιτιθέμενος μπορεί να ανακαλύψει την ύπαρξη του DSLAM, τον αριθμό έκδοσης και τον αριθμό εκδότη (κατασκευαστή). Αυτές τις πληροφορίες μπορεί να τις χρησιμοποιήσει για να ανακαλύψει γνωστές ευπάθειες, τις οποίες μπορεί να εκμεταλλευτεί για να αποκτήσει πρόσβαση στο DSLAM και μη εξουσιοδοτημένη παρακολούθηση των audience metering πληροφοριών.

2.4.5.2 Εξαπάτηση πληροφοριών ελέγχου

Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, μπορεί να δώσει στον επιτιθέμενο τη δυνατότητα, να στείλει εντολές μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου που θα έχουν ως αποτέλεσμα τη διαγραφή ή την τροποποίηση των πληροφοριών ελέγχου απάτης. Αυτή η απειλή θα μπορούσε να πραγματοποιηθεί μέσω μιας εσωτερικής ή εξωτερικής επίθεσης.

Ο επιτιθέμενος με την αλλοίωση των πληροφοριών ελέγχου απάτης, μπορεί να αποτρέψει την ανίχνευση της απάτης, με σκοπό την επιτυχή ***κλοπή της υπηρεσίας IPTV*** και την ***έκθεση της ακεραιότητας της πλατφόρμας***.

2.4.5.3 Απειλές στα φίλτρα IP

- Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, μπορεί να δώσει στον επιτιθέμενο τη δυνατότητα, να στείλει εντολές μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου που θα έχουν ως αποτέλεσμα τη διαγραφή ή την τροποποίηση των φίλτρων IP. Με αυτόν τον τρόπο ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε κάποια ροή video χωρίς να καταβάλλει την απαιτούμενη συνδρομή. Επιπλέον τα τροποποιημένα IP φίλτρα μπορούν να αποτρέψουν τη νόμιμη πρόσβαση σε μια ροή video.

- Ένα πλαστό μήνυμα του προτοκόλλου multicast (IGMP) μπορεί να σταλεί στο DSLAM, το οποίο να υποδεικνύει την διαγραφή των IP φίλτρων, με σκοπό να επιτραπεί η πρόσβαση σε μια ροή video χωρίς να πληρώσει. Αυτά τα μηνύματα μπορεί να προέλθουν από ένα οικιακό δίκτυο ή μέσω της εισαγωγής τους στο broadcast TVLAN ή στο VOD LAN.

2.4.6 Απειλές στη υπηρεσία LAN και στις εφαρμογές Broadcast/Multicast TV

2.4.6.1 Απειλές κλειδιών αποκρυπτογράφησης

- Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, μπορεί να δώσει στον επιτιθέμενο την δυνατότητα, να στείλει εντολές μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου που θα έχουν ως αποτέλεσμα τη διαγραφή ή την τροποποίηση των κλειδιών αποκρυπτογράφησης των media. Αυτή η απειλή θα μπορούσε να πραγματοποιηθεί μέσω μιας εσωτερικής ή εξωτερικής επίθεσης ή με την χρήση κακόβουλου λογισμικού (malware). Το αποτέλεσμα αυτής της απειλής είναι η DRM υπηρεσία να μην επιτρέψει στο συνδρομητή την πρόσβαση σε εξουσιοδοτημένο περιεχόμενο.

- Αν ο επιτιθέμενος αποκτήσει πρόσβαση στο υλικό των κλειδιών αποκρυπτογράφησης, μπορεί να δημιουργήσει ένα αντίγραφο των κλειδιών αποκρυπτογράφησης του συνδρομητή και να το χρησιμοποιήσει για να αποκτήσει πρόσβαση σε περιεχόμενο χωρίς να καταβάλει την απαιτούμενη συνδρομή.

- Αν ένας συνδρομητής αποκτήσει πρόσβαση στο υλικό των κλειδιών αποκρυπτογράφησης, μπορεί να τροποποιήσει τη διάρκεια ζωής των κλειδιών ώστε να αποκτήσει επιπρόσθετο περιεχόμενο χωρίς να καταβάλει την απαιτούμενη συνδρομή. Για παράδειγμα, μπορεί να παρακολουθήσει video περιεχόμενο περισσότερη ώρα από την καθορισμένη.

- Αν ο επιτιθέμενος αποκτήσει πρόσβαση στο υλικό των κλειδιών αποκρυπτογράφησης, μπορεί να εισάγει μη έγκυρη διάρκεια ζωής κλειδιού, που θα έχει ως αποτέλεσμα τη διακοπή της πρόσβασης του συνδρομητή σε έγκυρο περιεχόμενο.

2.4.6.2 Απειλές στο NTP/SNTP

- Υπάρχει η απειλή της εισαγωγής κατασκευασμένων NTP/SNTP πακέτων στην management σύνδεση του STB, στο περιφερειακό gateway ή στο DSLAM. Επίσης υπάρχει η απειλή της τροποποίησης των NTP/SNTP πακέτων κατά την μεταφορά τους, μέσω μιας man in the middle (MITM) επίθεσης.

- Τα pay-per-view multicast, οι πληροφορίες χρέωσης και οι πληροφορίες λογαριασμών, απαιτούν σφιχτό χρονικό συγχρονισμό δικτύου (networking time synchronization). Τα κατασκευασμένα ή τροποποιημένα NTP/SNTP μηνύματα μπορούν να δημιουργήσουν συγχρονισμό στον χρόνο του δικτύου, μεταξύ των συσκευών, έχοντας ως αποτέλεσμα την ***διακοπή της υπηρεσίας IPTV***.

2.4.6.3 Απειλές στην ροή video mpeg-2/mpeg-4

- Κατασκευασμένα mpeg πακέτα ή μη εξουσιοδοτημένη τροποποίηση των mpeg πακέτων κατά την μεταφορά τους, θα οδηγήσει στην απώλεια της αξιοπιστίας της ροής mpeg. Αυτό μπορεί να συμβεί εισάγοντας θόρυβο στην ροή mpeg ή μέσω μιας man in the middle επίθεσης.

- Ένας επιτιθέμενος μπορεί να δημιουργήσει υπερχείλιση πακέτων mpeg στο STB, με σκοπό να προκαλέσει κατάρρευση στο STB.

- Η υπερχείλιση της κίνησης στην broadcast TV μπορεί να καταναλώσει όλο το bandwidth της σύνδεσης.

2.4.7 Απειλές στην εφαρμογή middleware

2.4.7.1 Απειλές στα διαπιστευτήρια των συνδρομητών (subscriber credentials)

Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, μπορεί να δώσει στον επιτιθέμενο την δυνατότητα, να στείλει εντολές μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου που θα έχουν ως αποτέλεσμα τη διαγραφή, την τροποποίηση ή την αντιγραφή των διαπιστευτηρίων του συνδρομητή.

Η τροποποίηση των διαπιστευτηρίων μπορεί να επιτευχθεί με την εισαγωγή πακέτων στην σύνδεση μεταξύ του STB και του middleware server ή μέσω μιας man in the middle επίθεσης. Η σύλληψη των διαπιστευτηρίων κατά την μεταφορά τους μπορεί να συμβεί με την χρήση packet sniffer στην σύνδεση μεταξύ του STB και του middleware server ή μέσω μιας επίθεσης man in the middle.

Ένα πιθανό κίνητρο για αυτού του είδους την απειλή, είναι η πλαστογράφηση των διαπιστευτηρίων του συνδρομητή, με σκοπό την ***κλοπή της υπηρεσίας***.

2.4.7.2 Απειλές στις πληροφορίες αγορών

Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, μπορεί να δώσει στον επιτιθέμενο τη δυνατότητα, να στείλει εντολές μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου που θα έχουν ως αποτέλεσμα τη διαγραφή ή την τροποποίηση των πληροφοριών αγοράς, από το STB. Ένα πιθανό κίνητρο για τον επιτιθέμενο, είναι η πλαστοποίηση των πληροφοριών αγοράς του συνδρομητή, έτσι ώστε ο συνδρομητής να αποκτήσει πρόσβαση στην υπηρεσία ή σε περιεχόμενο, χωρίς να καταβάλλει την απαιτούμενη συνδρομή.

2.4.7.3 Απειλές στα οικογενειακά φίλτρα

Τα οικογενειακά φίλτρα περιλαμβάνουν ρυθμίσεις στο STB, με τις οποίες μπορεί να προστατευτεί ένας ανήλικος χρήστης από έκθεση σε κατάλληλο περιεχόμενο.

Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, μπορεί να δώσει στον επιτιθέμενο την δυνατότητα, να στείλει εντολές μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου που θα έχουν ως αποτέλεσμα την διαγραφή ή την τροποποίηση των οικογενειακών φίλτρων από το STB. Επιπλέον, ο επιτιθέμενος μπορεί να υποκριθεί τον "γονέα" και να διαγράψει τα οικογενειακά φίλτρα από το STB, επιτρέποντας την πρόσβαση σε ακατάλληλο περιεχόμενο. Με την τροποποίηση των οικογενειακών φίλτρων ο επιτιθέμενος μπορεί να προκαλέσει την άρνηση της πρόσβασης του συνδρομητή σε εξουσιοδοτημένο περιεχόμενο.

2.4.8 Απειλές στις πληροφορίες χρήσης και χρέωσης της IPTV

Η μη εξουσιοδοτημένη πρόσβαση στην κονσόλα διαχείρισης, μπορεί να δώσει στον επιτιθέμενο την δυνατότητα, να στείλει εντολές μέσω του management VLAN ή μέσω ενός μη ασφαλούς οικιακού δικτύου που θα έχουν ως αποτέλεσμα την διαγραφή ή την τροποποίηση των πληροφοριών χρήσης και χρέωσης της υπηρεσίας IPTV, που είναι αποθηκευμένες στο STB ή στο DSLAM. Το αποτέλεσμα αυτής της απειλής είναι ο συνδρομητής να μην χρεώνεται για την υπηρεσία IPTV.

Ο επιτιθέμενος με την δημιουργία διπλότυπων (duplicate) των πληροφοριών χρήσης και χρέωσης της υπηρεσίας IPTV, μπορεί να αποκομίσει κέρδος πουλώντας αυτές τις πληροφορίες.

3. Συστήματα Ασφαλείας στην IPTV

3.1 Βασικές εφαρμογές ασφαλείας

3.1.1 Προστασία Λειτουργικών Συστημάτων

Είναι πολύ σημαντικό να διασφαλίσουμε πως όλα τα λειτουργικά συστήματα, τα οποία τρέχουν στα διάφορα συστατικά στοιχεία της IPTV, έχουν τις κατάλληλες ρυθμίσεις και τα απαραίτητα patch για να αντιμετωπίσουν γνωστά προβλήματα ασφαλείας. Ανεξάρτητα από των αριθμό των επιπέδων ασφαλείας και των μηχανισμών ασφαλείας που έχουν υλοποιηθεί σε ένα περιβάλλον IPTV, ένας επιτιθέμενος μπορεί να παραβιάσει την ασφάλεια αν τα λειτουργικά συστήματα δεν έχουν γίνει patched και δεν έχουν τις κατάλληλες ρυθμίσεις. Ωστόσο, ένα περιβάλλον IPTV μπορεί να έχει εκατοντάδες servers και χιλιάδες STB. Η χειροκίνητη ρύθμιση και το patch, δεν είναι βιώσιμα οικονομικά. Η χρήση προσωπικού υποστήριξης το οποίο θα ρυθμίζει χειροκίνητα όλα τα συστήματα, απαιτεί υπερβολικά μεγάλα έξοδα και μεγάλο χρόνο ανταπόκρισης για την λύση των προβλημάτων ασφαλείας. Μια λύση για την προστασία των λειτουργικών συστημάτων, με την οποία μπορεί να γίνει εξοικονόμηση χρόνου και πόρων, είναι η χρήση αυτοματοποιημένων εργαλείων για την ανάπτυξη των ρυθμίσεων ασφαλείας.

Το Υπουργείο Δημόσιας Τάξης (*Department of Homeland Security*) στις Η.Π.Α. έχει χρηματοδοτήσει την ανάπτυξη κάποιων έργων που υποστηρίζουν την τεχνολογία που απαιτείται για να αυτοματοποιηθούν οι διαδικασίες εξασφάλισης της ασφάλειας σε ηλεκτρονικές πλατφόρμες. Η MITRE Corporation στα πλαίσια αυτών των έργων, έχει αναπτύξει τα παρακάτω πρότυπα :

i. **Κοινές Ευπάθειες και Εκθέσεις** (***CVE***, *common vulnerabilities and exposures*)
ii. **Απαρίθμηση Κοινών Πλατφόρμων** (***CPE***, *common platform enumeration,*)
iii. **Απαρίθμηση Κοινών Ρυθμίσεων** (***CCE***, *common configuration enumeration*)

Όλα αυτά τα προϊόντα είναι διαθέσιμα στο Internet στην διεύθυνση : http://nvd.nist.gov/scap.cfm .

Το πρότυπο **CVE** παρέχει συχνές ενημερώσεις οι οποίες περιγράφουν ευπάθειες που βρίσκονται στα λειτουργικά συστήματα, βασικές υπηρεσίες και εφαρμογές. Αυτές οι πληροφορίες συμπεριλαμβάνουν απαρίθμηση και κατηγοριοποίηση των ευπαθειών, προσφέροντας έτσι την δυνατότητα αναγνώρισης διαφόρων ζητημάτων ασφαλείας. Το CVE βελτιώνεται από την εθνική βάση δεδομένων ευπαθειών NVD (*National Vulnerability Database*) που είναι ένα προϊόν του NIST (*Us National Institute of Standards and Technology*), η οποία περιλαμβάνει κατηγοριοποίηση απειλών που σχετίζονται με γνωστές ευπάθειες. Χρησιμοποιώντας το CVE μπορούμε να προσδιορίσουμε ποια patch και ποιες τροποποιήσεις είναι απαραίτητες για ένα συγκεκριμένο σύστημα. Οι πληροφορίες αυτές αξιοποιούνται στην αρχή της συγκεκριμένης ρύθμισης. Οι καταχωρήσεις της NVD παρέχονται σε μορφή XML και είναι διαθέσιμες online. Το CVE προσφέρει συνεπή ονοματοδοσία των ευπαθειών ασφαλείας, το οποίο είναι κρίσιμο εάν θέλουμε να έχουμε μια ενοποιημένη διαχείριση ασφαλείας στο περιβάλλον IPTV. Με το CVE, μπορούν να χρησιμοποιηθούν διαφορετικά εργαλεία λογισμικού για να εκτιμηθεί η ασφάλεια της πλατφόρμας και όσον αφορά τις ονομασίες των αποτελεσμάτων, αυτές θα είναι ταυτόσημες.

Το πρότυπο **CPE** παρέχει μια δομή κοινής ονοματοδοσίας και στοιχεία αναγνώρισης λειτουργικών συστημάτων, επιτρέποντας αυτόματα inventories δικτύων υπολογιστών. Αυτό μπορεί να χρησιμοποιηθεί για τη δημιουργία μιας αναπαράστασης σε XML του inventory με τα συστήματα του δικτύου. Με το CPE μπορούμε να δημιουργήσουμε ένα κοινό inventory που θα αντιπροσωπεύει όλα τα στοιχεία στο περιβάλλον IPTV και θα αντιστοιχίζεται με το inventory των γνωστών ευπαθειών για αυτά τα συστήματα. Αυτό το εργαλείο μπορεί να χρησιμοποιηθεί ως η βάση της μηχανής του inventory και να μας δώσει τη δυνατότητα να έχουμε μια καθαρή οπτική στον αριθμό και στο είδος των στοιχείων που είναι διαθέσιμα στο περιβάλλον IPTV. Έχοντας ένα αναβαθμισμένο inventory, η διαδικασία διασφάλισης της ασφάλειας του περιβάλλοντος IPTV απλοποιείται. Κατά τον έλεγχο του inventory μπορούμε να ανιχνεύσουμε μη εξουσιοδοτημένα στοιχεία μέσα στην υποδομή. Σε ορισμένες περιπτώσεις, διαχειριστές συστημάτων ή διαχειριστές δικτύων προσθέτουν συστήματα ή αλλάζουν τις ρυθμίσεις σε συστήματα που ήδη υπάρχουν. Μπορεί να γίνει επανεγκατάσταση κάποιων συστημάτων, χωρίς όλα τα

απαραίτητα patch, ή μπορεί να γίνει αντικατάσταση κάποιων server, χωρίς να γίνουν οι απαραίτητες ρυθμίσεις. Με την χρήση του CPE μπορούμε να διατηρούμε ενημερωμένες λίστες των συστημάτων και του επιπέδου ασφαλείας τους.

Το πρότυπο **CCE** προσφέρει μια αναπαράσταση σε XML των ρυθμίσεων των λειτουργικών συστημάτων και σημαντικών εφαρμογών. Σε αυτές τις πληροφορίες συμπεριλαμβάνονται γνωστά ζητήματα ασφαλείας στα λειτουργικά συστήματα καθώς και προτεινόμενοι παράμετροι ασφαλείας. Γενικά, το CCE παρέχει κοινή ονοματοδοσία για ζητήματα που αφορούν τις ρυθμίσεις λογισμικών. Για παράδειγμα, παρέχει κοινή γλώσσα για την αναφορά στις παραμέτρους των ρυθμίσεων των κωδικών πρόσβασης (*password*), σε όλες τις πλατφόρμες. Με το CCE, μπορούμε να καταγράψουμε τη συγκεκριμένη ρύθμιση ασφαλείας που απαιτείται για την κάθε πλατφόρμα. Αυτές οι πληροφορίες, αν προστεθούν στην λίστα καταχωρήσεων του CVE που εφαρμόζονται στην πλατφόρμα, θα αποκτήσουμε μια ολοκληρωμένη εικόνα των γνωστών προβλημάτων ασφαλείας σε ένα σύστημα. Τα προβλήματα στις ρυθμίσεις ασφαλείας διευκολύνουν την μη εξουσιοδοτημένη πρόσβαση και τη διακοπή πρόσβασης στα συστήματα. Με την χρήση του CCE μπορούμε να ορίσουμε ένα λεπτομερές μοντέλο ρυθμίσεων που να περιγράφει όλες τις παραμέτρους που πρέπει να εφαρμοστούν στα διαθέσιμα συστήματα. Υπάρχει η περίπτωση μέσα σε διαφορετικά συστήματα, τα οποία παρέχουν διαφορετικές υπηρεσίες, να υπάρχουν παρόμοιες λειτουργίες που απαιτούν ρύθμιση. Για παράδειγμα, οι απαιτήσεις για το μήκος του κωδικού πρόσβασης, εφαρμόζονται με τον ίδιο τρόπο στα λειτουργικά συστήματα και στις εφαρμογές. Το CCE μπορεί να χρησιμοποιηθεί για να μεταφράσει τις απαιτήσεις συμμόρφωσης σε συγκεκριμένες παραμέτρους ρυθμίσεων, σε κάθε λειτουργικό σύστημα. Μπορούμε να πάρουμε ένα διεθνές πρότυπο όπως το ISO/IEC 17799 ή ένα βιομηχανικό πρότυπο όπως το PCI DSS και να μεταφράσουμε τις περισσότερες απαιτήσεις στην γλώσσα του CCE. Από τη στιγμή που το πρότυπο για μια συγκεκριμένη πλατφόρμα θα είναι σε CCE μορφή, θα λειτουργεί ως template το οποίο θα μπορεί να χρησιμοποιηθεί σε όλες τις παρόμοιες πλατφόρμες.

Το NIST έχει αναπτύξει λίστες ελέγχου (*checklists*) που έχουν σκοπό να παρέχουν πληροφορίες ασφαλείας για τα λειτουργικά συστήματα και για ευρέως διαδεδομένες εφαρμογές. Οι λίστες ελέγχου ασφαλείας περιλαμβάνουν οδηγίες για

τις ρυθμίσεις και τον έλεγχο ενός συγκεκριμένου συστήματος. Οι λίστες ελέγχου μπορούν να είναι αυτοματοποιημένες, και να υποστηρίζουν τις εργασίες που απαιτούνται για την συμμόρφωση με νόμους και κανονισμούς και να επιταχύνουν τον ρυθμό εύρεσης των ευπαθειών. Ένας τρόπος για την αυτοματοποίηση των λιστών ελέγχου είναι μέσω scripts. Μπορούμε να χρησιμοποιήσουμε τα scripts έτσι ώστε να εισάγουμε ρυθμίσεις στην πλατφόρμα με τις οποίες θα εμποδίζουμε συγκεκριμένες επιθέσεις. Επιπλέον, τα scripts μπορούν να χρησιμοποιηθούν σε περίπτωση που ξαναχτίζουμε την πλατφόρμα ή μετά από ένα προγραμματισμένο refresh στο σύστημα. Το SCAP (*security content automation program*) που έχει δημιουργηθεί από την NIST, στοχεύει στην υποστήριξη της ανάπτυξης αυτοματοποιημένων λιστών ελέγχου, που να είναι συμβατές με το XCCDF (*extensible configuration checklist description format*) και με το OVAL (*open vulnerability and assessment language*). Το XCCDF χρησιμοποιείται για να προσδιορίσει πολιτικές (*policies*) και απαιτήσεις ρυθμίσεων και το OVAL χρησιμοποιείται για τον έλεγχο των ρυθμίσεων μιας συγκεκριμένης πλατφόρμας.

Συνδυάζοντας όλα αυτά τα στοιχεία μαζί για την εφαρμογή τους στην IPTV, μας δίνεται η δυνατότητα να χρησιμοποιήσουμε αυτόματα ένα CPE βασισμένο σε XML, για να συγκεντρώσουμε ένα inventory με όλα τα στοιχεία που υπάρχουν στο περιβάλλον της IPTV. Αυτό το inventory μπορεί να ελεγχθεί από το CVE και το NVD για να δούμε τι είδους ευπάθειες υπάρχουν στα λειτουργικά συστήματα που έχουμε.

Η τεχνολογία αυτή είναι διαθέσιμη για να δημιουργήσουμε μηχανισμούς ελέγχου με τους οποίους μπορούμε να ελέγξουμε αν τα set top box έχουν τα απαιτούμενα επίπεδα ασφαλείας. Αυτά τα οποία αποτυγχάνουν στον έλεγχο ασφαλείας μπορούμε να τα θέσουμε σε καραντίνα. Όταν ένα STB στέλνει αίτηση για μία έγκυρη διεύθυνση IP μέσω του DSLAM, μπορούμε να επιβεβαιώσουμε μέσω ενός τοπικού inventory, αν το συγκεκριμένο STB έχει επαληθεύσει την ταυτότητά του και αν συμμορφώνεται με τις πολιτικές ασφαλείας. Σε κάποιες περιπτώσεις, το STB μπορεί συνδεθεί σε ένα συγκεκριμένο τμήμα του δικτύου, έχοντας περιορισμένη πρόσβαση, μέχρι να γίνει ο έλεγχος και το patch.

Οι ευπάθειες του λογισμικού δεν είναι τα μόνα προβλήματα ασφαλείας που πρέπει να λάβουμε υπ’ όψιν μας κατά την διαδικασία της ασφάλειας της

πλατφόρμας. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν λανθασμένες ρυθμίσεις για να αποκτήσουν πρόσβαση στο σύστημα. Η λίστα ρυθμίσεων του NIST, όταν μεταφραστεί χρησιμοποιώντας το XCCDF, μπορεί να χρησιμοποιηθεί για τον έλεγχο και την ρύθμιση όλων των συστημάτων. Χρησιμοποιώντας το OVAL ως γλώσσα ελέγχου και το CCE ως γλώσσα κοινών ρυθμίσεων για όλα τα συστήματα, έχουμε την δυνατότητα να εξακριβώσουμε το επίπεδο συμμόρφωσης έναντι του αναμενόμενου επιπέδου των ρυθμίσεων και να εκδώσουμε λεπτομερείς αναφορές για τις απαιτούμενες αλλαγές στις ρυθμίσεις.

Χρησιμοποιώντας όλα τα στοιχεία μαζί, βασισμένα σε ένα XML σχήμα, θα μειωθεί ο χρόνος και ο φόρτος εργασίας που απαιτείται για την συντήρηση της ασφάλειας των λειτουργικών συστημάτων και των βασικών εφαρμογών. Επιπλέον, οι αλλαγές στις ρυθμίσεις και τα patch θα γίνονται με αυτοματοποιημένες διαδικασίες σε όλα τα λειτουργικά συστήματα.

Η διαδικασία της προστασίας των λειτουργικών συστημάτων θα περιλαμβάνει τις παρακάτω δραστηριότητες :

I. Εκτέλεση των patch
II. Αφαίρεση περιττών εφαρμογών και υπηρεσιών
III. Αφαίρεση περιττών λογαριασμών χρηστών
IV. Περιορισμοί στους κωδικούς πρόσβασης
V. Ενεργοποίηση ελέγχου και αρχείου καταγραφής
VI. Εκτέλεση ελέγχου πρόσβασης
VII. Λίστα εξουσιοδοτημένων εφαρμογών
VIII. Προεπιλεγμένη άδεια σε αρχεία και φακέλους

Η εκτέλεση των patch, σε όλους τους servers, στα στοιχεία δικτύου και στα set top box, είναι μια από τις πιο βασικές δραστηριότητες για να διατηρήσουμε την ασφάλεια στο περιβάλλον της IPTV. Είναι επίσης σημαντικό να διασφαλίσουμε ότι οι αλλαγές στο εσωτερικό των STB δεν θα επηρεάσουν τη λειτουργία της υπηρεσίας.

Τα λειτουργικά συστήματα συνήθως συμπεριλαμβάνουν έναν μεγάλο αριθμό από υπηρεσίες που δεν είναι απαραίτητες για την λειτουργία της υπηρεσίας. Τα STB

που χρησιμοποιούν λειτουργικά συστήματα ανοιχτού κώδικα, συνήθως συμπεριλαμβάνουν υπηρεσίες email, υπηρεσίες Web και άλλες TCP/IP υπηρεσίες που δεν είναι απαραίτητες για τις βασικές λειτουργίες τους. Αυτές οι επιπρόσθετες υπηρεσίες δίνουν ευκαιρίες παραβίασης στους επιτιθέμενους και εκθέτουν το σύστημα στη μη εξουσιοδοτημένη πρόσβασή τους. Αφαιρώντας τις περιττές υπηρεσίες, θα υπάρχουν περισσότεροι πόροι διαθέσιμοι, όσον αφορά την μνήμη και τον επεξεργαστή (CPU), για άλλες δραστηριότητες και θα μειωθούν τα τρωτά σημεία εισόδου των επιτιθέμενων, των ιών και των worms.

Τα περισσότερα λειτουργικά συστήματα κατά την εγκατάσταση με προεπιλεγμένες ρυθμίσεις, θα προσθέσουν περιττούς λογαριασμούς χρηστών, οι οποίοι μπορούν να χρησιμοποιηθούν από τους επιτιθέμενους για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στο σύστημα. Είναι σημαντικό κατά την διάρκεια της εγκατάστασης αυτοί οι περιττοί λογαριασμοί να διαγραφούν.

Όλα τα λειτουργικά συστήματα και οι εφαρμογές πρέπει να ρυθμιστούν ώστε να απαιτούν κάποια ελάχιστα επίπεδα πολυπλοκότητας στους κωδικούς πρόσβασης. Έτσι θα εξασφαλίσουμε ότι οι κωδικοί πρόσβασης δεν θα είναι τετριμμένοι και οι επιτιθέμενοι δεν θα μπορούν να τους μαντέψουν προεπιλεγμένες τιμές ή απλές λέξεις. Επιπλέον η απομακρυσμένη πρόσβαση στο STB, πρέπει να απαιτεί έγκυρο κωδικό πρόσβασης ακόμα και αν η πρόσβαση μπορεί να γίνει μόνο από το οικιακό δίκτυο.

Όλες οι δραστηριότητες στο περιβάλλον της IPTV πρέπει να καταγράφονται καταλλήλως. Αυτό γίνεται χρησιμοποιώντας τις λειτουργίες αρχείων καταγραφής και ελέγχου, των λειτουργικών συστημάτων και των εφαρμογών. Για κρίσιμα στοιχεία, όπως head end servers, πρέπει να υπάρχει συγκεκριμένη εγκατάσταση, για την αποθήκευση των αρχείων καταγραφής. Υπάρχει διαθέσιμη τεχνολογία που μπορεί να χρησιμοποιηθεί για να στέλνεται η κάθε καταχώρηση καταγραφής σε μια κεντρική αποθήκη (repository). Με αυτόν τον τρόπο προστατεύονται οι πληροφορίες ελέγχου από μη εξουσιοδοτημένη τροποποίηση από τους εισβολείς και διασφαλίζεται ότι οι μελλοντικές έρευνες θα έχουν όλες τις απαραίτητες πληροφορίες για την αναγνώριση παρόμοιων ή ίδιων περιστατικών ασφαλείας. Αυτοί οι servers δεν πρέπει να ελέγχονται από τους διαχειριστές που είναι υπεύθυνοι για τα λειτουργικά συστήματα και για τις εφαρμογές καθώς μπορεί να

υπάρχει σύγκρουση συμφερόντων εάν η ίδια οντότητα διαχειρίζεται τα συστήματα και προστατεύει τα αρχεία καταγραφής.

Τα λειτουργικά συστήματα πρέπει να έχουν περιορισμούς στον έλεγχο πρόσβασης και να εμποδίζουν τη μη εξουσιοδοτημένη πρόσβαση σε όλες τις υπηρεσίες και τις λειτουργίες.

Καθώς όλες οι εφαρμογές είναι γνωστές και εγκεκριμένες από τον πάροχο της υπηρεσίας IPTV, μπορεί να γίνει η ανάπτυξη λιστών εξουσιοδοτημένων εφαρμογών στους servers και στα set top box. Κάθε εφαρμογή θα έχει ένα συγκεκριμένο fingerprint/checksum με το οποίο θα μπορεί επικυρωθεί από το λειτουργικό σύστημα πριν επιτραπεί η εκτέλεσή της. Έτσι εμποδίζονται κάποιοι ιοί και rootkits, εφ' όσον δεν θα είναι εξουσιοδοτημένη η εκτέλεσή τους. Οποιαδήποτε μη εξουσιοδοτημένη τροποποίηση σε κομμάτια του λειτουργικού συστήματος ή των εφαρμογών όταν συγκριθεί με τις λίστες, μπορεί να αναγνωριστεί και να εμποδιστεί.

Τα λειτουργικά συστήματα και οι εφαρμογές δημιουργούν ένα αριθμό από τοπικούς φακέλους με προεπιλεγμένες άδειες χρήσης. Αυτές οι άδειες είναι ακατάλληλες για την ασφαλή λειτουργία των εφαρμογών και μπορούν να χρησιμοποιηθούν από τους επιτιθέμενους για να τρέξουν κώδικα ή για να τροποποιήσουν αρχεία. Πρέπει να ανατεθούν σε όλα τα αρχεία και σε όλους τους φακέλους, κατάλληλες άδειες σύμφωνα με τις απαιτήσεις για ασφαλή λειτουργία.

3.1.2 Ανίχνευση και αποτροπή εισβολής

Όλη η κίνηση στο περιβάλλον της IPTV πρέπει να παρακολουθείται για να ανιχνευτούν γνωστές επιθέσεις και προσπάθειες εισβολής. Οι εισβολείς, οι ιοί και τα worms έχουν αρκετούς εναλλακτικούς τρόπους εισβολής, για αυτό πρέπει να αναπτύξουμε ειδικά συστήματα που θα ανιχνεύουν την εισβολή και θα παίρνουν ακαριαία μέτρα.

Παρακάτω αναφέρονται κάποια κρίσιμα στοιχεία τα οποία πρέπει να προστατεύονται από ένα σύστημα ανίχνευσης και αποτροπής εισβολής (IDS/IPS system) :

- Η αποθήκη του video (*repository*)
- Ο DRM server
- Ο middleware server
- Ο video streaming server
- Το video on demand (*VOD*)
- Ο Mpeg encapsulator
- Ο server διαχείρισης περιεχομένου
- Η κίνηση από το home end στο head end (όλα τα VLANs)
- Η κίνηση στο middleware content management VLAN
- Η κίνηση στο video repository content management VLAN
- Η κίνηση στο DRM middleware VLAN

3.1.3 Τοίχος προστασίας δικτύου

Τα τείχη προστασίας δικτύου πρέπει να χρησιμοποιηθούν για τον έλεγχο της κίνησης μέσα στο head end. Η ροή της κίνησης μεταξύ των server, σε ένα VLAN είναι γνωστή και τεκμηριωμένη. Ως εκ τούτου, ένα τείχος προστασίας δικτύου, μπορεί να χρησιμοποιηθεί για να διασφαλίσει ότι μόνο έγκυρα αιτήματα θα μεταδίδονται. Επιπλέον, θα μειώσουν την κίνηση μεταξύ των στοιχείων του δικτύου και θα διευκολύνουν τη διαδικασία της ανίχνευσης μη εξουσιοδοτημένης πρόσβασης. Τα τείχη προστασίας δικτύου, συνήθως χρησιμοποιούνται σε συνδέσεις χαμηλού bandwidth, για παράδειγμα στο head end ή στον έλεγχο μιας ροής κίνησης προς το middleware VLAN. Η κίνηση υψηλού bandwidth, για παράδειγμα η κίνηση από τον video streaming server προς τα STB σε ένα broadcast TV VLAN, συνήθως μένουν χωρίς προστασία εξαιτίας της αδυναμίας των τοίχων προστασίας να αντέξουν τέτοιο επίπεδο κίνησης. Σε αυτές τις περιπτώσεις μπορούμε να χρησιμοποιήσουμε δρομολογητές, switches και το DSLAM, για να παρέχουμε λειτουργίες φιλτραρίσματος.

3.1.4 Αποτροπή εξαπάτησης

Η υπηρεσία της IPTV πρέπει να έχει την δυνατότητα να αποτρέπει περιπτώσεις εξαπάτησης (*fraud*). Στη συνέχεια θα περιγράψουμε κάποια στοιχεία της IPTV, τα οποία μπορούν να συμμετάσχουν στον έλεγχο και στην αποτροπή εξαπάτησης.

Το middleware μπορεί να αναφέρει δραστηριότητες των συνδρομητών και να ανιχνεύει πότε ένας συνδρομητής αιτείται περιεχόμενο, χρησιμοποιώντας δύο ξεχωριστές IP διευθύνσεις.

Ο middleware server μπορεί να ανιχνεύει πότε ένα set top box αιτείται έναν πολύ μεγάλο αριθμό από τίτλους VOD. Κάτι τέτοιο μπορεί να προκαλείται από μη εξουσιοδοτημένη πρόσβαση στο STB. Μπορούμε για παράδειγμα να θέσουμε έναν μηχανισμό ορίου (trigger), όπως μέχρι πέντε τίτλους την ημέρα ή δέκα τίτλους την βδομάδα. Έτσι ώστε αν κάποιος επιτιθέμενος έχει πάρει τον έλεγχο του STB και κατεβάζει όσους περισσότερους τίτλους μπορεί, αυτός ο μηχανισμός θα ενεργοποιηθεί και θα υποδείξει ύποπτη συμπεριφορά του συγκεκριμένου STB.

Οι DSLAM servers μπορούν να αναφέρουν στους εμπορικούς servers ποιους unicast τίτλους έχουν λάβει οι συνδρομητές. Αυτές οι πληροφορίες μπορούν να συνδυαστούν με τις καταγραφές χρέωσης και να διαπιστωθεί αν υπάρχει εκμετάλλευση του συστήματος.

3.2 Ασφάλεια στο Head End

Όπως αναφέραμε και στο 1^{ο} κεφάλαιο το head end είναι το σημείο στο δίκτυο στο οποίο το περιεχόμενο συλλαμβάνεται (*captured*) και μετασχηματίζεται (*formatted*) για διανομή στο IP δίκτυο. Το head end λαμβάνει ροές δεδομένων (*data stream*) και τις κωδικοποιεί σε μια ψηφιακή μορφή βίντεο, όπως mpeg-2 ή mpeg-4. Μετά την κωδικοποίηση, δεδομένα της ροής ενθυλακώνονται μέσα σε μια IP ροή δεδομένων (*IP data stream*) η οποία μεταδίδεται σε μια συγκεκριμένη IP διεύθυνση αποστολής (*IP destination address*), ως ανταπόκριση στην αίτηση κάποιου πελάτη για ένα συγκεκριμένο κανάλι.

Οι περισσότεροι servers που βρίσκονται μέσα στο head end προστατεύονται από έξι επίπεδα ασφαλείας, τα οποία αποτελούνται συνήθως από ανεξάρτητους μηχανισμούς. Αυτά τα επίπεδα τείνουν να συμπεριλαμβάνουν διαφορετικές τεχνολογίες και να τα διαχειρίζονται διαφορετικές ομάδες. Έτσι αυξάνεται ο αριθμός των ελέγχων και μειώνονται οι πιθανότητες απάτης.

Το πρώτο επίπεδο αποτελείται από ένα δίκτυο από τείχη προστασίας και ένα δίκτυο στοιχείων ελέγχου και αποτροπής εισβολής (IDS/IPS). Αυτά παρέχουν έλεγχο πρόσβασης ανάμεσα στις κεντρικές λειτουργίες και στις ανταλλαγές, καθώς και προστασία από γνωστές επιθέσεις, όπως ιούς και worms.

Το δεύτερο επίπεδο περιλαμβάνει το VLAN που είναι εγκατεστημένο στα switches. Το VLAN ρυθμίζεται έτσι ώστε να επιτρέπει μόνο σε εγκεκριμένους hosts να συνδέονται στο δίκτυο. Οι servers έχουν μια κάρτα δικτύου αφοσιωμένη στο VLAN διαχείρισης και διάφορες NIC κάρτες για άλλα VLANs, ανάλογα με τις ανάγκες των απαιτούμενων επικοινωνιών. Η πρόσβαση στο VLAN ελέγχεται από την MAC διεύθυνση του NIC ή από την IP διεύθυνση του host. Σε ορισμένες περιπτώσεις, οι servers μπορούν να αυθεντικοποιηθούν χρησιμοποιώντας διαπιστευτήρια, πριν συνδεθούν στο VLAN.

Το τρίτο επίπεδο αποτελείται από την λίστα έλεγχου πρόσβασης στο network switch. Στις περισσότερες περιπτώσεις, οι επικοινωνίες ξεκινούν από έναν host και γίνονται δεκτές από τον host προορισμού. Αυτή η κίνηση ρέει σε εγκεκριμένες κατευθύνσεις και προς συγκεκριμένες θύρες και υπηρεσίες. Για παράδειγμα, ο

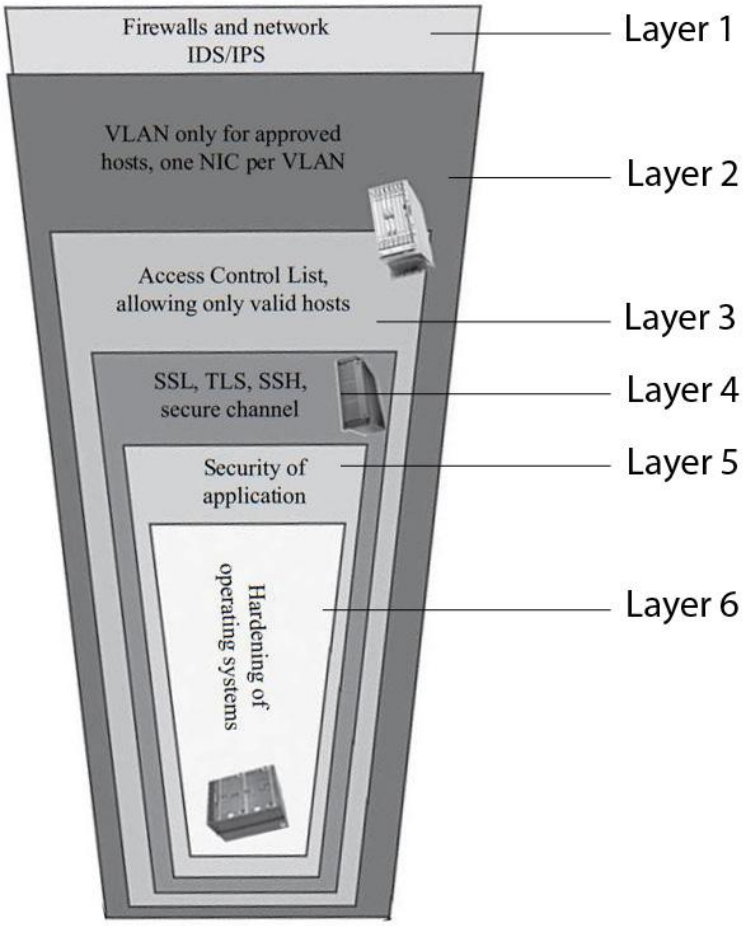
server ενθυλάκωσης IP, δεν έχει την δυνατότητα να στείλει πακέτα στην θύρα SNTP του server διαχείρισης περιεχομένου. Οι κονσόλες διαχείρισης έχουν πιο ευέλικτη πρόσβαση σε servers, ωστόσο επικυρώνονται από το τοίχος προστασίας.

Το τέταρτο επίπεδο αποτελείται από την ενθυλάκωση που παρέχεται από τα πρωτόκολλα ασφαλείας. Στην ουσία αυτή είναι μια εγκατεστημένη δίοδος μεταξύ των hosts που χρησιμοποιούν SSL, TSL, SSH, SNMPv3 ή άλλα παρόμοια κανάλια ασφαλούς επικοινωνίας, τα οποία προστατεύουν τις συνεδρίες από διακοπή και τροποποιήσεις, και επιπλέον μειώνουν τις πιθανότητες για επιθέσεις τύπου man in the middle.

Το πέμπτο επίπεδο αποτελείται από συγκεκριμένους μηχανισμούς ασφαλείας που εφαρμόζονται από τον δημιουργό του κάθε λογισμικού, σε συγκεκριμένες εφαρμογές τις οποίες έχει δημιουργήσει ο καθένας. Στις περισσότερες περιπτώσεις, οι εφαρμογές θα ζητήσουν διαπιστευτήρια, προτού επιτρέψουν πρόσβαση σε χρήστη ή σε διαχειριστή και θα αναθέσουν διαφορετικό προφίλ σε κάθε χρήστη.

Το έκτο επίπεδο είναι η προστασία των λειτουργικών συστημάτων, το οποίο περιλαμβάνει την εφαρμογή κατάλληλων ρυθμίσεων και το patch, όπως αναφέραμε στην αρχή του κεφαλαίου.

Με την προσέγγιση ασφαλείας των έξι επιπέδων, γίνεται πολύ δύσκολο για τους επιτιθέμενους να καταλάβουν τον έλεγχο των στοιχείων του head end. Στην εικόνα 3.1 παρουσιάζονται τα έξι επίπεδα ασφαλείας.



Εικόνα 3.1 - Έξι επίπεδα ασφαλείας στο Head End

3.2.1 Ασφάλεια στην εισαγωγή περιεχομένου

Στο περιβάλλον του head end, το περιεχόμενο video μπορεί να βρεθεί σε διάφορα μέσα και με διάφορες μορφές. Ο κάθε τύπος περιεχομένου αντιμετωπίζει διαφορετικές απειλές και υπάρχουν διαφορετικά αντίμετρα που μπορούν να εφαρμοστούν ενάντια στην κάθε απειλή. Στην συνέχεια θα αναφέρουμε κάποια αντίμετρα με τα οποία μπορεί να μειωθεί η πιθανότητα μη εξουσιοδοτημένης πρόσβασης στο περιεχόμενο του video.

Κάποιοι ιδιοκτήτες περιεχομένου διανέμουν το περιεχόμενο μέσω δορυφορικών συνδέσεων. Οι πάροχοι της υπηρεσίας IPTV χρησιμοποιούν δορυφορικούς δέκτες για να αποκτήσουν το σήμα. Οι περισσότεροι δορυφορικοί δέκτες περιλαμβάνουν βασικές εφαρμογές διαχείρισης, οι οποίες επιτρέπουν στους αποστολείς να κρυπτογραφήσουν την ροή και να μοιραστούν το κλειδί με τους παραλήπτες για

τους οποίους προορίζεται το σήμα. Αυτά τα σήματα μπορούν να χρησιμοποιηθούν για μεγάλο χρονικό διάστημα και αποτελούν πολύτιμα αγαθά. Πρέπει να εφαρμοστούν κατάλληλες διαδικασίες για να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση στα κλειδιά.

Ένας συνηθισμένος μηχανισμός για την παροχή του περιεχομένου, είναι η χρήση των φυσικών μέσων. Όταν το περιεχόμενο video πρέπει να τροποποιηθεί από τρίτους, για παράδειγμα η δημιουργία υποτίτλων ή η μεταγλώττιση, ο διαμεσολαβητής θα παραδώσει φυσικά μέσα. Τα φυσικά μέσα πρέπει να μεταφερθούν χρησιμοποιώντας ελεγμένους μεταφορείς και ασφαλή δοχεία μεταφοράς που δεν επιδέχονται αλλοίωση. Τα δεδομένα πρέπει να είναι κρυπτογραφημένα για να αποτροπή η μη εξουσιοδοτημένη πρόσβαση στο περιεχόμενο κατά την μεταφορά των μέσων. Στον πίνακα 3.1 αναφέρεται η βασική διαχείριση των αντίμετρων που πρέπει να ληφθούν για την αποτροπή αυτών απειλών.

ΔΙΑΧΕΙΡΙΣΗ ΑΝΤΙΜΕΤΡΩΝ	**ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ IPTV**		
	Κλοπή ή κατάχρηση αγαθών	**Διακοπή της Υπηρεσίας**	**Έκθεση ακεραιότητας**
Διαχείριση αντιμέτρων στην Δορυφορική Ανατροφοδότηση	Τα αντίμετρα θα μειώσουν τις πιθανότητες η δορυφορική ανατροφοδότηση να ληφθεί από μη εξουσιοδοτημένες ομάδες.	Τα αντίμετρα θα μειώσουν τις πιθανότητες μη εξουσιοδοτημένης τροποποίησης ή απώλειας των κλειδιών του δορυφορικού δέκτη.	-
Διαχείριση αντιμέτρων στα Φυσικά Μέσα	Τα αντίμετρα θα μειώσουν τις πιθανότητες κλοπής του περιεχομένου που υπάρχει στα φυσικά μέσα.	Τα αντίμετρα θα μειώσουν τις πιθανότητες διακοπής της υπηρεσίας λόγω απώλειας του περιεχομένου.	Τα αντίμετρα θα μειώσουν την πιθανότητα εισαγωγής μη εξουσιοδοτημένου περιεχόμενου στο περιβάλλον της IPTV, καθώς και την πιθανότητα τροποποίησης του περιεχομένου.

Πίνακας 3.1 – Διαχείριση αντιμέτρων στην εισαγωγή περιεχομένου

3.2.2 Ασφάλεια στις λειτουργίες κωδικοποίησης Video

Ο κωδικοποιητής Mpeg είναι το πρώτο στοιχείο το οποίο διαχειρίζεται ψηφιακό video. Δέχεται εισαγωγές από τους δέκτες NTSC/PAL και από τους δορυφορικούς δέκτες. Μέχρι την στιγμή της εισαγωγής το περιεχόμενο δεν έχει κωδικοποιηθεί και οποιαδήποτε απόπειρα κλοπής του περιεχομένου θα αντιμετωπίζει προβλήματα λόγω του μεγάλου μεγέθους του.

Οι κωδικοποιητές Mpeg απαιτούν σύνδεση στο δίκτυο για να επιτραπούν δραστηριότητες διαχείρισης και υποστήριξης. Οι επιτιθέμενοι μπορούν να καταχραστούν την σύνδεση στο λειτουργικό σύστημα ή στις εφαρμογές. Το λειτουργικό σύστημα του κωδικοποιητή Mpeg πρέπει να δεχτεί το κατάλληλο patch για να μπορέσουμε να αποφύγουμε γνωστούς τρόπους εκμετάλλευσης της ασφάλειας και γνωστούς ιούς. Επιπλέον, η πρόσβαση στο δίκτυο πρέπει να ελέγχεται για να αποφύγουμε την μη εξουσιοδοτημένη πρόσβαση στο σύστημα. Πρέπει να εγκαταστήσουμε VLANs για την επικοινωνία του κωδικοποιητή MPEG με τα εργαλεία ενθυλάκωσης του IP που βρίσκονται σε ένα συγκεκριμένο VLAN, αφήνοντας ένα άλλο VLAN για τις λειτουργίες διαχείρισης.

Οι servers οι οποίοι φιλοξενούν τις εφαρμογές του κωδικοποιητή πρέπει να ρυθμιστούν έτσι ώστε να αφαιρέσουν οποιαδήποτε αφαιρούμενα μέσα ή USB υποδοχείς. Με αυτόν τον τρόπο θα μειωθούν οι πιθανότητες αφαίρεσης των ψηφιακών αγαθών. Στον πίνακα 3.2 αναφέρεται η βασική διαχείριση των αντίμετρων που πρέπει να ληφθούν για την αποτροπή των απειλών.

ΔΙΑΧΕΙΡΙΣΗ ΑΝΤΙΜΕΤΡΩΝ	ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ IPTV		
	Κλοπή ή κατάχρηση αγαθών	**Διακοπή της Υπηρεσίας**	**Έκθεση ακεραιότητας**
Διαχείριση αντιμέτρων στον κωδικοποιητή MPEG	Τα αντίμετρα θα μειώσουν τις πιθανότητες κλοπής των αγαθών της IPTV, κυρίως τα MPEG κωδικοποιημένα αγαθά.	Τα αντίμετρα θα μειώσουν τις πιθανότητες διακοπής της υπηρεσίας IPTV, η οποία θα οφείλεται στην μη διαθεσιμότητα της εφαρμογής MPEG.	Τα αντίμετρα θα μειώσουν την πιθανότητα εισαγωγής μη εξουσιοδοτημένου περιεχόμενου στο περιβάλλον της IPTV, καθώς και την πιθανότητα τροποποίησης του περιεχομένου.

Πίνακας 3.2 – Διαχείριση αντιμέτρων στον κωδικοποιητή MPEG

3.2.3 Ασφάλεια στην Ενθυλάκωση του IP

Το σύστημα ενθυλάκωσης του IP δέχεται ανατροφοδότηση από τους κωδικοποιητές MPEG. Αυτές οι πληροφορίες βρίσκονται σε ψηφιακή μορφή και είναι εύκολο να τροποποιηθούν ή να κλαπούν. Κατά την ενθυλάκωση του IP δημιουργείται ένα περιεχόμενο με έτοιμο IP, που κάνει πιο εύκολη και γρήγορη την ροή του σε ένα IP δίκτυο.

Αυτό το σύστημα πρέπει να έχει μια σύνδεση με το τοπικό δίκτυο διαχείρισης και τους κωδικοποιητές MPEG. Το VLAN πρέπει να ρυθμιστεί έτσι ώστε να επιτρέπει στο σύστημα ενθυλάκωσης του IP να δέχεται ανατροφοδότηση από το σύστημα κωδικοποίησης MPEG και να επιτρέπει την επικοινωνία του με το DRM, την διαχείριση περιεχομένου και την αποθήκη του video. Τα VLANs μπορούν να περιλαμβάνουν λίστες ελέγχου και να φιλτράρουν την πηγή και τον προορισμό των επικοινωνιών. Επιπλέον, πρέπει να επιτρέπουν μόνο εγκεκριμένα συστήματα να αλληλεπιδρούν με το σύστημα ενθυλάκωσης του IP. Οποιαδήποτε πρόσβαση διαχείρισης πρέπει να γίνεται με την χρήση ασφαλών καναλιών επικοινωνίας, όπως τα SSH, TLS, SSL και SNMPv3.

Πρέπει να εφαρμοστεί έλεγχος πρόσβασης ώστε να επιτρέπεται μόνο εξουσιοδοτημένη πρόσβαση στο σύστημα. Αυτό συμπεριλαμβάνει αυθεντικοποίηση, ταυτοποίηση και εξουσιοδότηση χρηστών και συστημάτων που έχουν πρόσβαση στο σύστημα ενθυλάκωσης του IP.

Οι servers που φιλοξενούν τις εφαρμογές της ενθυλάκωσης του IP πρέπει να ρυθμιστούν έτσι ώστε να αφαιρέσουν οποιαδήποτε αφαιρούμενα μέσα ή USB υποδοχείς. Με αυτόν τον τρόπο θα μειωθούν οι πιθανότητες αφαίρεσης των ψηφιακών αγαθών. Στον πίνακα 3.3 αναφέρεται η βασική διαχείριση των αντίμετρων που πρέπει να ληφθούν για την αποτροπή των απειλών.

ΔΙΑΧΕΙΡΙΣΗ ΑΝΤΙΜΕΤΡΩΝ	**ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ IPTV**		
	Κλοπή ή κατάχρηση αγαθών	**Διακοπή της Υπηρεσίας**	**Έκθεση ακεραιότητας**
Διαχείριση αντιμέτρων στο σύστημα Ενθυλάκωσης IP	Τα αντίμετρα θα μειώσουν τις πιθανότητες κλοπής των αγαθών της IPTV, κυρίως τις ροές με ενθυλάκωση IP.	Τα αντίμετρα θα μειώσουν τις πιθανότητες διακοπής της υπηρεσίας IPTV, η οποία θα οφείλεται στην μη διαθεσιμότητα της λειτουργίας ενθυλάκωση IP.	Τα αντίμετρα θα μειώσουν την πιθανότητα εισαγωγής μη εξουσιοδοτημένου περιεχόμενου στο περιβάλλον της IPTV, καθώς και την πιθανότητα τροποποίησης του περιεχομένου.

Πίνακας 3.3 – Διαχείριση αντιμέτρων στο σύστημα Ενθυλάκωσης IP

3.2.4 Ασφάλεια στον server διαχείρισης περιεχομένου

Ο server διαχείρισης περιεχομένου είναι ένα από τα βασικότερα στοιχεία μέσα στο head end. Δεν συμπεριλαμβάνει ψηφιακά αγαθά, αλλά παρέχει αλληλεπίδραση και έλεγχο στην διακίνηση των ροών. Οποιαδήποτε ζημιά σε αυτό το στοιχείο θα επηρεάσει τη λειτουργία της υπηρεσίας IPTV εξ αιτίας της έλλειψης περιεχομένου, ή θα διευκολύνει την μη εξουσιοδοτημένη πρόσβαση σε περιεχόμενο.

Το σύστημα διαχείρισης περιεχομένου πρέπει να είναι μέρος ενός συγκεκριμένου VLAN με το οποίο θα επιτρέπεται να αλληλεπιδρούν μόνο

εξουσιοδοτημένα συστήματα. Ένα συγκεκριμένο περιβάλλον δικτύου μπορεί να χρησιμοποιηθεί αποκλειστικά για την επικοινωνία του VLAN με την κονσόλα διαχείρισης, ένα άλλο για την επικοινωνία με το σύστημα ενθυλάκωσης IP, ένα τρίτο για την επικοινωνία με την αποθήκη video κτλ. Με αυτόν τον τρόπο, το VLAN παρέχει ένα ασφαλές περιβάλλον όπου μόνο τα αναμενόμενα συστήματα θα ανταλλάσσουν πληροφορίες. Επιπλέον, η λίστα ελέγχου πρόσβασης επιτρέπει μόνο εξουσιοδοτημένες ροές πληροφορίας. Οι επικοινωνίες πρέπει να πραγματοποιούνται ενθυλακωμένες σε ασφαλή κανάλια επικοινωνίας, όπως για παράδειγμα στα SSL, TLS, SSH, ή στο SNMPv3.

Όλα τα μεταδεδομένα που έχουν ανατεθεί στα ψηφιακά αγαθά, πρέπει να προστατεύονται με την χρήση μηχανισμών επικύρωσης, όπως τα checksums και οι ψηφιακές υπογραφές. Με αυτόν τον τρόπο θα αποφύγουμε τις μη εξουσιοδοτημένες τροποποιήσεις. Στον πίνακα 3.4 αναφέρεται η βασική διαχείριση των αντίμετρων που πρέπει να ληφθούν για την αποτροπή των απειλών.

ΔΙΑΧΕΙΡΙΣΗ ΑΝΤΙΜΕΤΡΩΝ	**ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ IPTV**			
	Κλοπή ή κατάχρηση αγαθών	**Κλοπή δεδομένων που σχετίζονται με την IPTV**	**Διακοπή της Υπηρεσίας**	**Έκθεση ακεραιότητας**
Διαχείριση αντιμέτρων στον Server Διαχείρισης Περιεχομένου	Τα αντίμετρα θα μειώσουν τις πιθανότητες κλοπής των αγαθών της IPTV, κυρίως της ανακατεύθυνσης του περιεχομένου της IPTV.	Τα αντίμετρα θα μειώσουν τις πιθανότητες κλοπής των μεταδεδομένων που συνδέονται με τα αγαθά της IPTV.	Τα αντίμετρα θα μειώσουν τις πιθανότητες διακοπής της υπηρεσίας IPTV, η οποία θα οφείλεται στην αδυναμία λειτουργίας του server διαχείρισης περιεχομένου.	Τα αντίμετρα θα μειώσουν την πιθανότητα εισαγωγής μη εξουσιοδοτημένου περιεχόμενου στο περιβάλλον της IPTV, καθώς και την πιθανότητα τροποποίησης του περιεχομένου.

Πίνακας 3.4 – Διαχείριση αντιμέτρων στον Server Διαχείρισης Περιεχομένου

3.2.5 Ασφάλεια στην αποθήκη του VIDEO

Η αποθήκη του video είναι ο πιο πολύτιμος host στο περιβάλλον της IPTV εξ αιτίας των δεδομένων που είναι αποθηκευμένα. Πρέπει να επιτρέπεται η επικοινωνία αυτού του host με πολλούς servers, όπως με τον DRM server, με τον server διαχείρισης περιεχομένου, με το video on demand και σε μερικές περιπτώσεις με τον video streaming server.

Ο server της αποθήκης του video, απαιτεί επιπλέον τροποποίηση σκληρών δίσκων, για να διασφαλίσουμε ότι το video είναι κατάλληλα προστατευμένο ακόμα και σε περιπτώσεις όπου διαχειριστές, προσωπικό τεχνικής υποστήριξης ή κάποιος επιτιθέμενος αποπειραθούν να αποσπάσουν ψηφιακό περιεχόμενο.

Οι servers οι οποίοι φιλοξενούν την εφαρμογή της αποθήκης του video πρέπει να ρυθμιστούν έτσι ώστε να αφαιρέσουν οποιαδήποτε αφαιρούμενα μέσα ή USB υποδοχείς. Με αυτόν τον τρόπο θα μειωθούν οι πιθανότητες αφαίρεσης των ψηφιακών αγαθών.

Όλα τα μεταδεδομένα που έχουν ανατεθεί στα ψηφιακά αγαθά, πρέπει να προστατεύονται με την χρήση μηχανισμών επικύρωσης, όπως τα checksums και οι ψηφιακές υπογραφές. Με αυτόν τον τρόπο θα αποφύγουμε τις μη εξουσιοδοτημένες τροποποιήσεις. Στον πίνακα 3.5 αναφέρεται η βασική διαχείριση των αντίμετρων που πρέπει να ληφθούν για την αποτροπή των απειλών.

ΔΙΑΧΕΙΡΙΣΗ ΑΝΤΙΜΕΤΡΩΝ	**ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ IPTV**			
	Κλοπή ή κατάχρηση αγαθών	**Κλοπή δεδομένων που σχετίζονται με την IPTV**	**Διακοπή της Υπηρεσίας**	**Έκθεση ακεραιότητας**
Διαχείριση αντιμέτρων στην Αποθήκη του Video	Τα αντίμετρα θα μειώσουν τις πιθανότητες κλοπής των αγαθών της IPTV, κυρίως του αποθηκευμένου περιεχομένου.	Τα αντίμετρα θα μειώσουν τις πιθανότητες κλοπής των μεταδεδομένων που συνδέονται με τα αγαθά της IPTV.	Τα αντίμετρα θα μειώσουν τις πιθανότητες διακοπής της υπηρεσίας IPTV, η οποία θα οφείλεται στην καταστροφή ή στην τροποποίηση του περιεχομένου.	Τα αντίμετρα θα μειώσουν την πιθανότητα εισαγωγής μη εξουσιοδοτημένου περιεχόμενου στο περιβάλλον της IPTV, καθώς και την πιθανότητα τροποποίησης του περιεχομένου.

Πίνακας 3.5 – Διαχείριση αντιμέτρων στην Αποθήκη του Video

3.2.6 Digital Rights Management (DRM)

Το DRM είναι ένα βασικό στοιχείο το οποίο απαιτείται για να μπορέσουμε να διασφαλίσουμε την προστασία των ψηφιακών αγαθών που παρέχονται από την υπηρεσία IPTV. Σε κάποιες περιπτώσεις το set top box επιτρέπεται να συνδεθεί με τον DRM server. Τα έξι επίπεδα ασφαλείας που αναφέραμε προηγουμένως δεν εφαρμόζονται στην υπηρεσία DRM όταν επιτρέπεται να συνδεθούν οι συνδρομητές. Σε αυτήν την περίπτωση τα τείχη προστασίας και τα VLANs πρέπει να περιλαμβάνουν πρόσβαση σε ένα URL από το οποίο τα set top box θα κατεβάζουν τα κλειδιά για να αποκρυπτογραφήσουν το περιεχόμενο. Σε αυτόν τον τύπο πρόσβασης τα έξι επίπεδα ασφαλείας θα είναι ανοιχτά και θα επιτρέπουν την πρόσβαση.

Το τοίχος προστασίας επιτρέπει την πρόσβαση σε όλα τα set top box, για τις εξειδικευμένες συνδέσεις στην θύρα 80/443 στον DRM server. Το VLAN είναι ανοιχτό για όλα τα set top box που ζητάνε κλειδιά, το οποίο αυξάνει τσε μεγάλο βαθμό τις πιθανές επιθέσεις. Στο επίπεδο switch μπορούν να εφαρμοστούν φίλτρα, τα οποία θα φιλτράρουν τις συνδέσεις σε θύρες διαφορετικές από την 80/443, που προέρχονται από τα set top box. Οι συνδέσεις θα πραγματοποιούνται με τη χρήση SSL, ωστόσο με αυτόν τον τρόπο δεν παρέχεται προστασία απέναντι σε κάποιον επιτιθέμενο ο οποίος προσπαθεί να εκμεταλλευτεί ευπάθειες μέσα στις υπηρεσίες web. Οι ευπάθειες των εφαρμογών web μπορεί να επιτρέψουν στους επιτιθέμενους να καταλάβουν τον έλεγχο του server.

Για τους servers που επιτρέπουν την πρόσβαση των set top box σε υπηρεσίες web, υπάρχουν τρία βασικά αντίμετρα τα οποία πρέπει να εφαρμοστούν :

i. Web services gateway (WSG)

Το WSG επιτρέπει στους αρχιτέκτονες να ενοποιήσουν όλες τις υπηρεσίες web σε ένα μέτωπο που έχει κοινή αυθεντικοποίηση, ασφάλεια και λειτουργίες ελέγχου. Αν εμφανιστεί ένα περιστατικό ασφαλείας, θα περιοριστεί στο WSG και δεν θα επηρεάσει άμεσα τους web servers. Με αυτόν τον τρόπο έχουμε επιπλέον χρόνο για την ανίχνευση και την αντιμετώπιση της επίθεσης. Ο DRM server μπορεί να έχει μόνο ένα NIC αποκλειστικά για τις επικοινωνίες με το WSG .

ii. Reverse proxy

Αυτό το στοιχείο είναι ο μεσολαβητής ανάμεσα στα set top box και στον DRM server. Το reverse proxy τερματίζει τη συνεδρία με το set top box και εγκαθιδρύει νέα συνεδρία με τον DRM server. Το DRM μπορεί να έχει μόνο ένα NIC αποκλειστικά για τις επικοινωνίες με το reverse proxy. Με αυτόν τον τρόπο μειώνεται αρκετά ο αριθμός των host που επιτρέπεται να συνδεθούν με τον DRM server.

Τα reverse proxy ελέγχουν την εγκυρότητα των αιτημάτων HTTP και επιβεβαιώνουν αν είναι συμβατά με το πρωτόκολλο. Με αυτόν τον τρόπο θα φλιτραριστούν οι περισσότερες υπερχειλίσεις του buffer και οι επιθέσεις διακοπής υπηρεσίας. Οι λειτουργίες αυθεντικοποίησης και εξουσιοδότησης θα επιτρέψουν μόνο τις συνδέσεις που έχουν έγκυρες διευθύνσεις στον DRM server.

iii. Web application firewall

Το τοίχος προστασίας της εφαρμογής web, εμποδίζει την πρόσβαση σε μη εξουσιοδοτημένες σελίδες του DRM web site. Επιπλέον, εμποδίζει τα αιτήματα τα οποία δεν είναι συμμορφωμένα με τις αποφασισμένες αξίες και δομές. Οι απαντήσεις σε αιτήματα θα είναι επικυρωμένες και κάθε αφύσικη απάντηση θα εμποδίζεται. Το DRM μπορεί να έχει μόνο ένα NIC αποκλειστικά για τις επικοινωνίες με το τοίχος προστασίας της εφαρμογής web.

Οι τρείς αυτές λύσεις για την ασφάλεια στις εφαρμογές web είναι απόλυτα εφαρμόσιμες σε ένα περιβάλλον IPTV και η εφαρμογή της κάθε μιας θα έχει διαφορετικές απαιτήσεις και διαφορετικό κόστος.

Όσον αφορά τα ιδιωτικά κλειδιά της υπηρεσίας DRM, πρέπει να προστατεύονται διαρκώς, εφ’ όσον χρησιμοποιούνται συνέχεια. Ο server πρέπει να διαθέτει μηχανισμούς για να προστατεύει αυτά τα κλειδιά. Επιπλέον, πρέπει να προστατευτούν όλα τα κρίσιμα στοιχεία τα οποία σχετίζονται με τα set top boxes, καθώς και τα συμμετρικά κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση των ροών video. Υπάρχουν εξωτερικές κρυπτογραφημένες συσκευές αποθήκευσης και τεχνολογίες κρυπτογράφησης δίσκων, τις οποίες μπορούμε να

χρησιμοποιήσουμε. Πριν αποφασίσουμε ποια λύση θα εφαρμόσουμε, πρέπει να λάβουμε υπ' όψιν την αξία των αγαθών και το επίπεδο της έκθεσης.

Η κρυπτογράφηση πρέπει να λειτουργεί ακόμα και σε περιπτώσεις που ο διαχειριστής του server, ο διαχειριστής του δικτύου ή οποιαδήποτε οντότητα που έχει εξουσιοδότηση για πρόσβαση στον server, αλλά όχι στα κλειδιά, προσπαθεί να αποκτήσει τα κλειδιά.

Η αυθεντικοποίηση του DRM, του middleware και του VOD πρέπει να διαθέτει επιπρόσθετους μηχανισμούς για να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση, κυρίως εξ αιτίας επιθέσεων τύπου brute force.

Σε περιπτώσεις όπου οι συνδρομητές πρέπει να εισάγουν PINs ή κωδικούς πρόσβασης, το σύστημα πρέπει να περιλαμβάνει τυχαίες παύσεις κατά τον έλεγχο των πληροφοριών του κωδικού πρόσβασης. Έτσι θα δημιουργείται πρόβλημα στα αυτοματοποιημένα scripts τα οποία χρησιμοποιούνται στις επιθέσεις τύπου brute force. Το σύστημα πρέπει να καταγράφει την IP διεύθυνση και τα στοιχεία του συνδρομητή που χρησιμοποιήθηκαν για τις αποτυχημένες προσπάθειες και να κλειδώνει τις IP διευθύνσεις όταν έχει καταγραφεί μεγάλος αριθμός αποτυχημένων αιτημάτων πρόσβασης. Στον πίνακα 3.6 αναφέρεται η βασική διαχείριση των αντίμετρων που πρέπει να ληφθούν για την αποτροπή των απειλών.

ΔΙΑΧΕΙΡΙΣΗ ΑΝΤΙΜΕΤΡΩΝ	**ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ IPTV**			
	Κλοπή ή κατάχρηση αγαθών	**Κλοπή δεδομένων που σχετίζονται με την IPTV**	**Διακοπή της Υπηρεσίας**	**Έκθεση ακεραιότητας**
Διαχείριση αντιμέτρων στο Digital Rights Management (DRM)	Τα αντίμετρα θα μειώσουν τις πιθανότητες κλοπής των αγαθών της IPTV, κυρίως μέσω κλεμμένων κλειδιών DRM.	Τα αντίμετρα θα μειώσουν τις πιθανότητες κλοπής των κλειδιών DRM.	Τα αντίμετρα θα μειώσουν τις πιθανότητες διακοπής της υπηρεσίας IPTV, η οποία θα οφείλεται στα DRM κλειδιά τα οποία δεν θα είναι διαθέσιμα στα STBs για να αποκρυπτογραφήσουν το περιεχόμενο.	Τα αντίμετρα θα μειώσουν την πιθανότητα τα ιδιωτικά DRM κλειδιά να βρεθούν στην κατοχή των επιτιθέμενων.

Πίνακας 3.6 – Διαχείριση αντιμέτρων στο DRM

3.2.7 Ασφάλεια στον Video streaming server

Ο video streaming server δέχεται κρυπτογραφημένο περιεχόμενο από την αποθήκη video ή από το DRM. Πρέπει να υπάρχει ένα VLAN αποκλειστικά για την επικοινωνία αυτών των στοιχείων. Έτσι, το VLAN παρέχει ένα ασφαλές περιβάλλον όπου μόνο τα αναμενόμενα συστήματα ανταλλάσσουν πληροφορίες. Επιπλέον, πρέπει να διασφαλίσουμε ότι οι επικοινωνίες θα πραγματοποιούνται σε ασφαλή κανάλια, για παράδειγμα σε SSL, TLS,SSH και SNMPv3.

Η αποθήκη video συμμετέχει και στο VLAN της broadcast TV. Αυτό το VLAN συμπεριλαμβάνει την multicast κίνηση με όλα τα διαθέσιμα κανάλια TV. Το βασικό πλεονέκτημα ασφαλείας σε αυτήν την περίπτωση είναι ότι το multicast δεν προσφέρει αμφίδρομη επικοινωνία μεταξύ των STB και των video streaming servers. Το VLAN πρέπει να ρυθμιστεί έτσι ώστε να εμποδίζει οποιαδήποτε κίνηση που προέρχεται από το δίκτυο των STB.

Σε ορισμένες περιπτώσεις ο video streaming server στέλνει αρχεία για αποθήκευση στο STB. Είναι σημαντικό να παρθούν τα παρακάτω μέτρα ασφαλείας :

- Να γίνεται απενεργοποίηση ανώνυμων FTP log-in.
- Πρέπει να χρησιμοποιείται secure FTP (*SFTP*) αντί για FTP. Ωστόσο, το SFTP δεν παρέχει αυθεντικοποίηση και ακεραιότητα, επομένως αυτά θα πρέπει να τα παρέχει το πρωτόκολλο. Συνήθως το SFTP χρησιμοποιείται ως υποσύστημα του SSHv2, το οποίο παρέχει προστασία της ακεραιότητας και αυθεντικοποίηση.
- Πρέπει να ρυθμιστούν τα ACL στα τείχη προστασίας ώστε να εμποδίζουν τα πακέτα SFTP τα οποία προέρχονται από ακατάλληλα περιβάλλοντα ή από πηγές με ακατάλληλες IP διευθύνσεις.

Η κίνηση multicast η οποία προέρχεται από το head end και ενθυλακώνεται στα VLANs πρέπει να προστατεύεται από μη εξουσιοδοτημένες τροποποιήσεις. Με την χρήση του IPSec μπορούμε να επιτύχουμε αυθεντικοποίηση και προστασία της ακεραιότητας. Η επικεφαλίδα αυθεντικοποίησης του IPSec παρέχει ακεραιότητα χωρίς σύνδεση (connectionless) και αυθεντικοποίηση της προέλευσης των πακέτων, μειώνοντας έτσι της έκθεση σε επιθέσεις τύπου replay. Επιπλέον, μπορεί να

χρησιμοποιηθεί σε συνδυασμό με το ESP (*IP encapsulating security payload*). Το ESP παρέχει προστασία στο ωφέλιμο φορτίο (*payload*). Τα τείχη προστασίας πρέπει να ρυθμιστούν έτσι ώστε να εμποδίζει όποια κίνηση IGMPv2/v3 δεν προέρχεται από εξουσιοδοτημένη broadcast διεύθυνση. Όλα τα STB και οι περιφερειακές θύρες εισόδου, πρέπει να επικυρώνουν τα πακέτα IGMP που δέχονται και να τα απορρίπτουν σε περίπτωση που η Ethernet MAC διεύθυνση, δεν είναι μια multicast διεύθυνση.

Για να μειώσουμε τον κίνδυνο έκθεσης σε πλαστά ή τροποποιημένα RTP πακέτα, πρέπει να χρησιμοποιούμε το SRTP αντί το RTP. Το SRTP παρέχει αυθεντικοποίηση και προστασία της ακεραιότητας στα RTP και στα RTCP πακέτα. Πιο συγκεκριμένα παρέχει εμπιστευτικότητα μέσω της κρυπτογράφησης, αυθεντικοποίηση μηνυμάτων και προστασία ενάντια σε επιθέσεις τύπου reply, στο RTP και στο RTCP. Στα τείχη προστασίας πρέπει να ρυθμιστούν τα ACL έτσι ώστε να εμποδίζουν τα πακέτα RTP/SRTP τα οποία προέρχονται από πηγές με ακατάλληλες IP διευθύνσεις.

Για να αποφύγουμε την μη εξουσιοδοτημένη τροποποίηση των RTSP πακέτων, πρέπει να ενεργοποιηθούν οι βασικές λειτουργίες αυθεντικοποίησης στους κατάλληλους VOD servers και στα STB. Επιπλέον είναι σημαντικό να προστατεύσουμε τα RTSP πακέτα χρησιμοποιώντας το Imascrypt, το οποίο χρησιμοποιεί το SRTP για να παρέχει αυθεντικοποίηση, ακεραιότητα και κρυπτογράφηση στην μεταφορά. Για επιπρόσθετη προστασία ενάντια σε μη εξουσιοδοτημένη πρόσβαση και σε επιθέσεις τύπου διακοπής της υπηρεσίας, πρέπει να ρυθμιστούν τα ACL στα τείχη προστασίας έτσι ώστε να εμποδίζουν τα RTSP μηνύματα τα οποία μεταφέρουν RTSP πακέτα, που προέρχονται από πηγές με ακατάλληλες IP διευθύνσεις.

3.2.8 Ασφάλεια στον Middleware server

Όλα τα STBs επιτρέπεται να επικοινωνούν με τον middleware server, για να στείλουν αίτηση για το συγκεκριμένο περιεχόμενο που επιθυμούν. Σε ορισμένες περιπτώσεις ο middleware server παρέχει κλειδιά DRM και μπορεί να δεχτεί αιτήματα για VOD περιεχόμενο, τα οποία θα προωθηθούν στον VOD server. Η επικοινωνία μεταξύ των STBs και του middleware server, γίνεται συνήθως με την

χρήση HTTP (HTTPS, SSL, TLS). Ένας φυλλομετρητής (browser) μέσα στο STB επικοινωνεί με τον middleware server ζητώντας τις απαιτούμενες πληροφορίες. Αυτό το επίπεδο πρόσβασης των STBs στον middleware server, μειώνει την προστασία που παρουσιάσαμε στα έξι επίπεδα ασφαλείας. Για να αποτρέψουμε περιστατικά παραβίασης ασφαλείας και μη εξουσιοδοτημένης πρόσβασης στον middleware server, πρέπει να εφαρμόσουμε τους μηχανισμούς ασφαλείας των web υπηρεσιών που περιγράψαμε στην ενότητα του DRM. Τα αντίμετρα που προσφέρουν αυτοί οι μηχανισμοί θα αντικρούσουν τις απειλές που μπορεί να δεχτεί ο middleware server.

3.3 Ασφάλεια στο δίκτυο του πάροχου της υπηρεσίας IPTV

3.3.1 DSLAM

Τα STB παρόλο που κατασκευάζονται και εγκαθίστανται από τον πάροχο της υπηρεσίας IPTV, δεν βρίσκονται υπό την φυσική προστασία του κατασκευαστή. Η περιφερειακή θύρα εισόδου (*residential gateway*) βρίσκεται επίσης εκτός της φυσικής προστασίας του πάροχου της υπηρεσίας. Υπάρχουν αρκετές περιπτώσεις όπου καλωδιακά μόντεμ και STB, αποσυναρμολογούνται για την απόκτηση πληροφοριών και στην συνέχεια συναρμολογούνται ξανά, έχοντας τροποποιημένες παραμέτρους. Τέτοιες ενέργειες χρησιμοποιούν συνήθως οι hackers για να αναιρέσουν τους περιορισμούς της λειτουργίας του STB και για να επιχειρήσουν την κλοπή της υπηρεσίας IPTV.

Η ευθύνη της προστασίας ενάντια σε τέτοιους κακόβουλους και μη εξουσιοδοτημένους χρήστες, ανήκει στους μηχανισμούς ασφαλείας του δικτύου του πάροχου της υπηρεσίας IPTV. Ο κόμβος πρόσβασης στο δίκτυο, είναι το μοναδικό σημείο στο οποίο η ταυτότητα του συνδρομητή μπορεί να συνδεθεί (linked) με ένα πρωτόκολλο αυθεντικοποίησης του δικτύου, όπου θα είναι διαθέσιμη για μελλοντική χρήση από την υποδομή.

Το DSLAM βρίσκεται μέσα σε ένα προστατευμένο φυσικό περιβάλλον, όπου μπορούμε να εξασφαλίσουμε και να προστατεύσουμε τις ρυθμίσεις του. Αυτή είναι η βασική γραμμή άμυνας του πάροχου της υπηρεσίας IPTV. Τα πιο βασικά χαρακτηριστικά ασφαλείας του DSLAM είναι τα παρακάτω :

I. Έλεγχος πρόσβασης και συνεδρίας (session)
II. Δρομολόγηση (routing)
III. Διαχωρισμός χρηστών
IV. Ποιότητα της υπηρεσίας (QoS)
V. Εικονικά δίκτυα και εικονικές υπηρεσίες (VPN, VLAN)
VI. 802.1X αυθεντικοποίηση

Επιπλέον, το DSLAM διαθέτει τους παρακάτω μηχανισμούς ασφαλείας. Στο επίπεδο 2 (*L2*), υπάρχουν μηχανισμοί όπως το MAC antispoofing και στο επίπεδο 3 (*L3*), υπάρχουν μηχανισμοί όπως το IP antispoofing.

Με το MAC antispoofing προστατεύουμε το δίκτυο από κακόβουλους χρήστες οι οποίοι τροποποιούν και χρησιμοποιούν τις MAC διευθύνσεις άλλων συνδρομητών (*spoofing*). Το MAC antispoofing εμποδίζει κάθε χρήστη να χρησιμοποιεί μια ήδη γνωστή MAC διεύθυνση. Οι MAC διευθύνσεις συνδέονται με τις φυσικές τοποθεσίες των συνδρομητών και τους συνδρομητές. Για να προστεθεί μια MAC διεύθυνση, απαιτείται πρώτα αυθεντικοποίηση από τον συνδρομητή.

Σε ένα broadband δίκτυο με ενεργοποιημένο το DHCP, κάποιος κακόβουλος χρήστης μπορεί να συνδεθεί από ένα PC αντί από το STB του και να ρυθμίσει χειροκίνητα οποιαδήποτε στατική IP διεύθυνση, όπως για παράδειγμα την στατική IP διεύθυνση κάποιου άλλου συνδρομητή. Με την χρήση του IP antisnooping ο κόμβος πρόσβασης μπλοκάρει όλη την κίνηση από τον συνδρομητή (*downstream, upstream*), μέχρι να σταλεί ένα αίτημα DHCP και μια έμπιστη DHCP απάντηση, από τον DHCP server. Με αυτόν τον τρόπο ένας συνδρομητής που δεν έχει αυθεντικοποιηθεί από το DHCP, δεν μπορεί να έχει πρόσβαση σε καμία υπηρεσία και δεν μπορεί να επηρεάσει κανέναν άλλο συνδρομητή. Όταν πραγματοποιηθεί η αυθεντικοποίηση, η διεύθυνση IP του συνδρομητή συνδέεται με μια DSL φυσική γραμμή και επιτρέπεται μόνο η κίνηση που σχετίζεται με τις ασφαλές διευθύνσεις, των αυθεντικοποιημένων χρηστών.

Μία επιπλέον λειτουργία προστασίας που προσφέρει το DSLAM είναι να εμποδίζει την επικοινωνία μεταξύ των χρηστών (user-to-user). Στο επίπεδο του κόμβου πρόσβασης, αυτή η λειτουργία αποτρέπει οποιαδήποτε ανταλλαγή κίνησης δευτέρου επιπέδου (π.χ. Ethernet) μεταξύ των χρηστών. Με αυτόν τον τρόπο καταφέρνουμε έναν αυστηρό διαχωρισμό μεταξύ των οικιακών δικτύων των συνδρομητών και αποτρέπουμε επιθέσεις μέσω low level δικτύων, στον εξοπλισμό του συνδρομητή. Άλλοι μηχανισμοί ασφαλείας είναι η χρήση virtual MAC διεύθυνσης, δηλαδή η μετάφραση της MAC διεύθυνσης από το DSLAM και το φιλτράρισμα, δηλαδή μια πολιτική ασφαλείας που στηρίζεται σε κανόνες που ελέγχουν την κίνηση από και προς τους συνδρομητές DSL.

Με αυτούς τους μηχανισμούς ασφαλείας του DSLAM, μπορούμε να διασφαλίσουμε ότι οποιαδήποτε επικοινωνία η οποία γίνεται δεκτή, προέρχεται από εξουσιοδοτημένους φυσικούς κόμβους και οι χρήστες δεν έχουν την επιλογή για απευθείας επικοινωνία μεταξύ τους. Οι hackers, τα worms και οι ιοί μπορούν να επιτεθούν μόνο σε έγκυρους κόμβους upstream, οι οποίοι είναι προστατευμένοι.

3.3.1.1 Έλεγχος πρόσβασης και συνεδρίας (ACL)

Το DSLAM, όπως περιγράψαμε προηγουμένως, περιλαμβάνει μηχανισμούς αυθεντικοποίησης του χρήστη και δυνατότητες ανίχνευσης (tracking) των συνεδριών, που είναι πολύ κρίσιμα στοιχεία για την επικύρωση των set top box μέσα στο περιβάλλον της IPTV. Οι συνδρομητές, με την χρήση των διαπιστευτηρίων τα οποία είναι αποθηκευμένα μέσα στα STB τους, μπορούνε να αυθεντικοποιηθούν σε έναν εξωτερικό RADIUS server ή σε μια τοπική βάση δεδομένων χρηστών η οποία είναι αποθηκευμένη στο DSLAM. Το DSLAM μπορεί να ανταλλάξει τα δεδομένα αυθεντικοποίησης με τον RADIUS server ή με τον middleware server. Μόνο οι αυθεντικοποιημένες φυσικές θύρες επιτρέπεται να ανταλλάξουν πληροφορίες με το δίκτυο μεταφοράς και το head end. Αυτός ο μηχανισμός μειώνει σε μεγάλο βαθμό τις πιθανότητες μη εξουσιοδοτημένης πρόσβασης στο δίκτυο. Κάθε φυσική θύρα αντιστοιχίζεται με κάθε συνδρομητή. Επομένως, ο επιτιθέμενος πρέπει να αυθεντικοποιηθεί και να χρησιμοποιήσει μια έγκυρη φυσική θύρα. Το DSLAM μπορεί να επικυρώσει και να εξουσιοδοτήσει χρήστες, βάσει της MAC διεύθυνσης η οποία χρησιμοποιείται, ή με την χρήση άλλων κοινών μηχανισμών αυθεντικοποίησης, όπως το challenge handshake authentication protocol (CHAP), η αυθεντικοποίηση της IP διεύθυνσης και το πρωτόκολλο αυθεντικοποίησης PPP. Επειδή οι θύρες είναι συνδεδεμένες με τις MAC διευθύνσεις των συνδρομητών, είναι αδύνατο ένας συνδρομητής να προσποιηθεί κάποιον άλλο συνδρομητή.

Συνήθως ένα περιβάλλον IPTV συμπεριλαμβάνει χιλιάδες συνδρομητές. Ο μόνος πρακτικός τρόπος για να διαχειριστούμε τις IP διευθύνσεις είναι η χρήση του DHCP (dynamic host configuration protocol). Όταν χρησιμοποιούμε το DHCP για να αναθέσουμε διευθύνσεις IP, το DSLAM μπορεί να χρησιμοποιήσει την επιλογή 82

του DHCP για να εισάγει στοιχεία που σχετίζονται με την φυσική σύνδεση του συνδρομητή. Η αυθεντικοποίηση των STB στηρίζεται κυρίως στην επιλογή 82 του DHCP. Η λειτουργία της επιλογής 82 είναι να ελέγχει τα αιτήματα DCHP που προέρχονται από το δίκτυο του συνδρομητή και να εισάγει στο πεδίο της, τις πληροφορίες ταυτοποίησης της φυσικής γραμμής. Αυτές οι πληροφορίες περιλαμβάνουν το ID του κόμβου πρόσβασης, το shelf ID, το slot ID και το ID της γραμμής. Επιπλέον, η επιλογή 82 χρησιμοποιείται για να αναγνωρίσει την ταυτότητα του συνδρομητή και να του αναθέσει μια έγκυρη IP διεύθυνση για τις υπηρεσίες που περιλαμβάνει η συνδρομή του.

Αν κάποιος συνδρομητής προσπαθήσει να παρακάμψει την αυθεντικοποίηση που παρέχει το DSLAM, το σύστημα αναγνωρίζει ότι ο συγκεκριμένος συνδρομητής έχει τροποποιημένες παραμέτρους. Για παράδειγμα, ο συνδρομητής Α τροποποιεί την MAC διεύθυνσή του και την αντικαταστεί με τη έγκυρη MAC διεύθυνση του συνδρομητή Β. Σε αυτήν την περίπτωση ο DHCP server θα αναγνωρίσει ότι η MAC διεύθυνση που έχει υποβάλλει ο συνδρομητής Α, κατά την διαδικασία του αρχικού DCHP αιτήματος, αντιστοιχεί σε μια MAC διεύθυνση η οποία έχει ήδη καταχωρηθεί έχοντας μια διαφορετική φυσική τοποθεσία, αυτήν του συνδρομητή Β. Με αυτήν την διαδικασία οι πληροφορίες της φυσικής γραμμής συνδέονται με την MAC διεύθυνση του συνδρομητή και αποτρέπεται το spoofing και το hijacking.
Με την χρήση της επιλογής 82 του DHCP, θα εξαλειφθούν οι περισσότερες ευκαιρίες για MAC και IP spoofing. Επιπλέον θα αυξηθεί το επίπεδο εμπιστοσύνης σε σχέση με τις πληροφορίες συστήματος και θα μειωθούν τα περιστατικά, η συχνότητα και η επίδραση της μη εξουσιοδοτημένης πρόσβασης σε περιεχόμενο.

Το DSLAM μπορεί επίσης να παρέχει λίστες ελέγχου πρόσβασης (ACL) και περιορισμούς χρήσης για να ελέγξει τον τύπο και την ποσότητα των δεδομένων που στέλνουν οι συνδρομητές. Το DSLAM μπορεί να ελέγχει τον τύπο των αιτημάτων που στέλνονται από τα STB μέσω των VLANs. Για παράδειγμα, το DSLAM μπορεί να ρυθμιστεί έτσι ώστε να επιτρέπει μόνο τα HTTP, HTTPS, DHCP, DNS και RTSP να ρέουν upstream. Το DSLAM προστατεύει την υποδομή από επιθέσεις τύπου διακοπής της υπηρεσίας που προέρχονται από τα STB.

- **Δρομολόγηση**

Η δρομολόγηση μπορεί να παρέχει μηχανισμούς οι οποίοι προστατεύουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα. Οι πάροχοι της υπηρεσίας μπορούν να χρησιμοποιήσουν στατική, δυναμική και policy-based δρομολόγηση, η οποία στηρίζεται στην χρήση των VRD (virtual routing domain). Κάθε VRD χρησιμοποιείται για να παρέχει την απόφαση δρομολόγησης για τα πακέτα των συνδρομητών. Τα πακέτα μπορούν να διαχωριστούν ξεχωρίζοντας αυτά που έχουν έγκυρες domains και να διασφαλίσουμε ότι μόνο εξουσιοδοτημένα στοιχεία του δικτύου μεταδίδονται στο VRD. Τα μη εξουσιοδοτημένα STB δεν θα έχουν την δυνατότητα να στείλουν πακέτα στο δίκτυο της IPTV. Έτσι αποτρέπονται επιθέσεις, όπου ο εισβολέας προσπαθεί να εισβάλει στο δίκτυο μέσω ενός φυσικού συνδέσμου.

- **Διαχωρισμός Χρηστών**

Ο διαχωρισμός των χρηστών διασφαλίζει ότι οι συνδρομητές δεν έχουν την δυνατότητα πρόσβασης στα STB άλλων συνδρομητών, μειώνοντας έτσι τις επιπτώσεις από τους ιούς και τα worms. Αν ένας εισβολέας αποκτήσει τον έλεγχο ενός STB, δεν θα επιτρέπεται η ανταλλαγή πακέτων με τα γειτονικά STB. Αυτό είναι πολύ χρήσιμο για να μειώσουμε τις επιπτώσεις των ιών και των worms που χρησιμοποιούν αλγορίθμους για να μαντέψουν την IP διεύθυνση γειτονικών STB. Επιπλέον, οι χρήστες επιτρέπεται να έχουν πρόσβαση μόνο στο head end για τις υπηρεσίες της IPTV.

3.3.1.2 Ποιότητα της Υπηρεσίας (Qos)

Το DSLAM έχει την δυνατότητα να ταξινομεί την κίνηση έτσι ώστε να διασφαλίσει ότι η ποιότητα της υπηρεσίας διατηρείται συνεχώς. Το DSLAM ενεργοποιεί κανόνες ώστε να εγγυηθεί ότι οι κρίσιμες υπηρεσίες είναι πάντα διαθέσιμες. Με αυτόν τον τρόπο παρέχεται επιπλέον προστασία ενάντια σε επιθέσεις τύπου διακοπής της

υπηρεσίας, από συνδρομητές που προσπαθούν να χρησιμοποιήσουν όλο το διαθέσιμο bandwidth για HTTP πρόσβαση στο head end. Οι συνεδρίες ελέγχονται για να διασφαλιστεί ότι υπάρχει διαθέσιμο bandwidth για τις κρίσιμες υπηρεσίες. Κατά τον σχεδιασμό του DSLAM και των απαιτήσεων για το upstream bandwidth, πρέπει να προσδιοριστεί το μέγιστο bandwidth που θα επιτρέπεται να έχει το κάθε STB. Οποιαδήποτε προσπάθεια γίνει για να ξεπεραστεί το προκαθορισμένο bandwidth, θα έχει ως αποτέλεσμα την απόρριψη της επιπρόσθετης κίνησης από τον μηχανισμό QoS.

Είναι πολύ κρίσιμο να διασφαλίσουμε ότι οι συνδρομητές δεν έχουν την δυνατότητα να προκαλέσουν υπερχείλιση στην πλατφόρμα, στέλνοντας υπερβολικό αριθμό αιτήσεων στο head end. Πρέπει ένα ελάχιστο bandwidth να είναι εγγυημένο ώστε να εξασφαλίσουμε ότι οι συνδρομητές θα μπορούν οποιαδήποτε στιγμή να συνδεθούν στο head end για να αιτηθούν υπηρεσίες.

3.3.1.3 Εικονικά δίκτυα και εικονικές υπηρεσίες (VPN, VLAN)

Όταν χρησιμοποιούμε VPN και VLAN για την μετάδοση πληροφοριών σε ένα δημόσιο δίκτυο, τα δεδομένα προστατεύονται από την μη εξουσιοδοτημένη πρόσβαση.

Στο VPN, μια ομάδα από εξουσιοδοτημένα στοιχεία δικτύου έχουν την δυνατότητα πρόσβασης στο περιεχόμενο. Εικονικά δίκτυα και εικονικά κυκλώματα (virtual circuits) μπορούν να χρησιμοποιηθούν για να διαχωρίσουν την κίνηση της IPTV από την υπόλοιπη κίνηση που ρέει μέσω του DSLAM. Με την ποιότητα της υπηρεσίας που περιγράψαμε προηγουμένως και με τα VLAN, η κίνηση μπορεί να ελεγχθεί με τέτοιον τρόπο έτσι ώστε να εξασφαλίσουμε ότι το VLAN της IPTV θα έχει εγγυημένο bandwidth και ότι η υπηρεσία θα διατηρηθεί ακόμα και σε απόπειρες επιθέσεων τύπου διακοπής της υπηρεσίας.

Τα VLAN και τα VPN μπορούν να χρησιμοποιηθούν για να διαχωρίσουμε την κίνηση μεταξύ συγκεκριμένων κυκλωμάτων που ανήκουν αποκλειστικά σε υπηρεσίες όπως η IPTV, το voice over IP (VoIP), η πρόσβαση στο Internet κτλ. Σε κάθε κύκλωμα, μπορούν να εφαρμοστούν διαφορετικοί κανόνες και μηχανισμοί ασφαλείας, συγκεκριμένη κίνηση μπορεί να εμποδίζεται και το ποσό του θορύβου

στο δίκτυο μπορεί να μειωθεί σημαντικά. Για παράδειγμα, το VLAN που ανήκει αποκλειστικά στην IPTV, μπορούν να εφαρμοστούν μηχανισμοί ασφαλείας που να εξασφαλίζουν ότι μόνο HTTPS αιτήματα στέλνονται μεταξύ του STB και του head end.

Τον πίνακα 3.7 βλέπουμε πώς οι μηχανισμοί ασφαλείας που περιγράψαμε εξασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα της υπηρεσίας IPTV.

ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΤΟΥ DSLAM			
	ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ	**ΑΚΕΡΑΙΟΤΗΤΑ**	**ΔΙΑΘΕΣΙΜΟΤΗΤΑ**
ACL	Η επιλογή 82 του DHCP μειώνει τις πιθανότητες του MAC και IP spoofing.	Οι επιτιθέμενοι δεν έχουν την δυνατότητα να κάνουν spoof μια έγκυρη διεύθυνση, για να επιτεθούν στο head end και να τροποποιήσουν πληροφορίες.	Οι επιτιθέμενοι δεν έχουν την δυνατότητα να κάνουν spoof μια έγκυρη διεύθυνση, για να προκαλέσουν διακοπή της υπηρεσίας.
Δρομολόγηση	Με την χρήση των VRD μειώνεται ο κίνδυνος μη εξουσιοδοτημένης πρόσβαση σε πληροφορίες.	Μέσα στα VRD η πληροφορία διατηρείται χωρίς να μπορεί να υποστεί τροποποιήσεις.	Σε κάθε VRD ανατίθενται χαρακτηριστικά ποιότητας της υπηρεσίας.
Διαχωρισμός Χρηστών	Το STB του κάθε συνδρομητή προστατεύεται από τη πρόσβαση κάποιου άλλου συνδρομητή σε αυτό.	Δεν υπάρχει επικοινωνία μεταξύ των STB και ένας επιτιθέμενος που έχει καταλάβει ένα STB, δεν μπορεί να το χρησιμοποιήσει	Οι επιτιθέμενοι δεν μπορούν να κάνουν spoof και να προκαλέσουν διακοπή της υπηρεσίας στα STB.

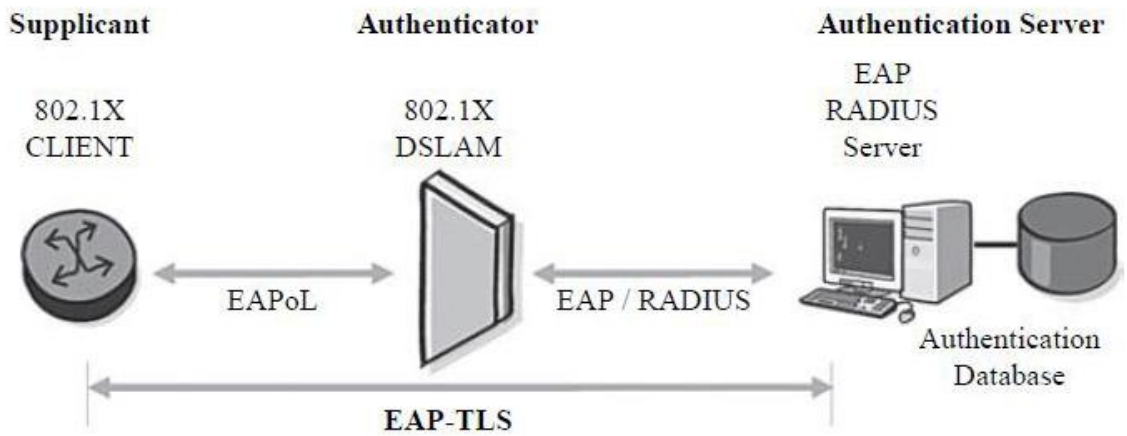
		για να προσβάλλει κάποιο άλλο.	
QoS	-	-	Οι επιτιθέμενοι δεν έχουν την δυνατότητα να καταναλώσουν όλο το bandwidth και να προκαλέσουν διακοπή της υπηρεσίας.
VPN & VLAN	Η πληροφορία διαχωρίζεται, δίνοντας την δυνατότητα για καλύτερη προστασία της εμπιστευτικότητας της πληροφορίας.	Είναι ξεκάθαροι οι περιορισμοί στον τύπο της κίνησης που επιτρέπεται, μειώνοντας έτσι τον τύπο των επιθέσεων που επηρεάζουν την ακεραιότητα των δεδομένων και τν συστημάτων.	Η κίνηση διαχωρίζεται, μειώνοντας τις πιθανότητες υπερχείλισης.

Πίνακας 3.7 Εξασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας

3.3.1.4 802.1X Αυθεντικοποίηση

Το IEEE έχει αναπτύξει ένα πρότυπο για τα τοπικά και τα αστικά δίκτυα, το οποίο καλύπτει τον έλεγχο πρόσβασης σε port-based δίκτυα. Αρκετά έχουν έναν μεγάλο αριθμό φυσικών θυρών που είναι εκτεθειμένες σε μη εξουσιοδοτημένη πρόσβαση. Σε αυτές τις φυσικές θύρες πρέπει να εφαρμοστούν μηχανισμοί ελέγχου για να αποφευχθούν περιστατικά παραβίασης ασφαλείας. Όσον αφορά την IPTV, αυτή η προηγούμενη περίπτωση αντιστοιχεί στα STB και στην σύνδεσή τους με το DSLAM, μέσω της περιφερειακής θύρας.

Ο σκοπός του προτύπου είναι να επιτρέπει πολύ περιορισμένη επικοινωνία μεταξύ ενός πρόσφατα συνδεδεμένου host και ενός host που προσφέρει επικύρωση, μέχρι να επαληθευτεί η ταυτότητά του και να του δοθεί η πρόσβαση. Το DSLAM αναλαμβάνει τον ρόλο του αυθεντικοποιητή (authenticator) και τον ρόλο του server αυθεντικοποίησης αναλαμβάνει ο RADIUS server, με την χρήση EAP. Η συνδεδεμένη συσκευή ξεκινάει ένα αίτημα 802.1X με τη χρήση EAPoL. Αυτό λαμβάνεται από τον αυθεντικοποιητή και προωθείται στον server αυθεντικοποίησης. Όταν ο server αυθεντικοποίησης επαληθεύσει τη συνδεδεμένη συσκευή και την εξουσιοδοτήσει, η ρύθμιση της θύρας θα τροποποιηθεί και οι περιορισμοί θα αναιρεθούν. Στην εικόνα 3.2 παρουσιάζεται η λειτουργία του 802.1X.



Εικόνα 3.2 802.1X Αυθεντικοποίηση

Πιο συγκεκριμένα η ανταλλαγή πληροφοριών μεταξύ του DSLAM και του αυθεντικοποίησης είναι η εξής :

I. Ένα αρχικό πακέτο EAPoL στέλνεται από την συνδεδεμένη συσκευή για να ξεκινήσει η διαδικασία.
II. Το DSLAM ανταποκρίνεται στέλνοντας ένα πακέτο EAP, ζητώντας την ταυτότητα της συνδεδεμένης συσκευής.
III. Η συνδεδεμένη συσκευή στέλνει τις πληροφορίες τη ταυτότητας, οι οποίες θα χρησιμοποιηθούν από το DSLAM, για να λάβει επιβεβαίωση από τον

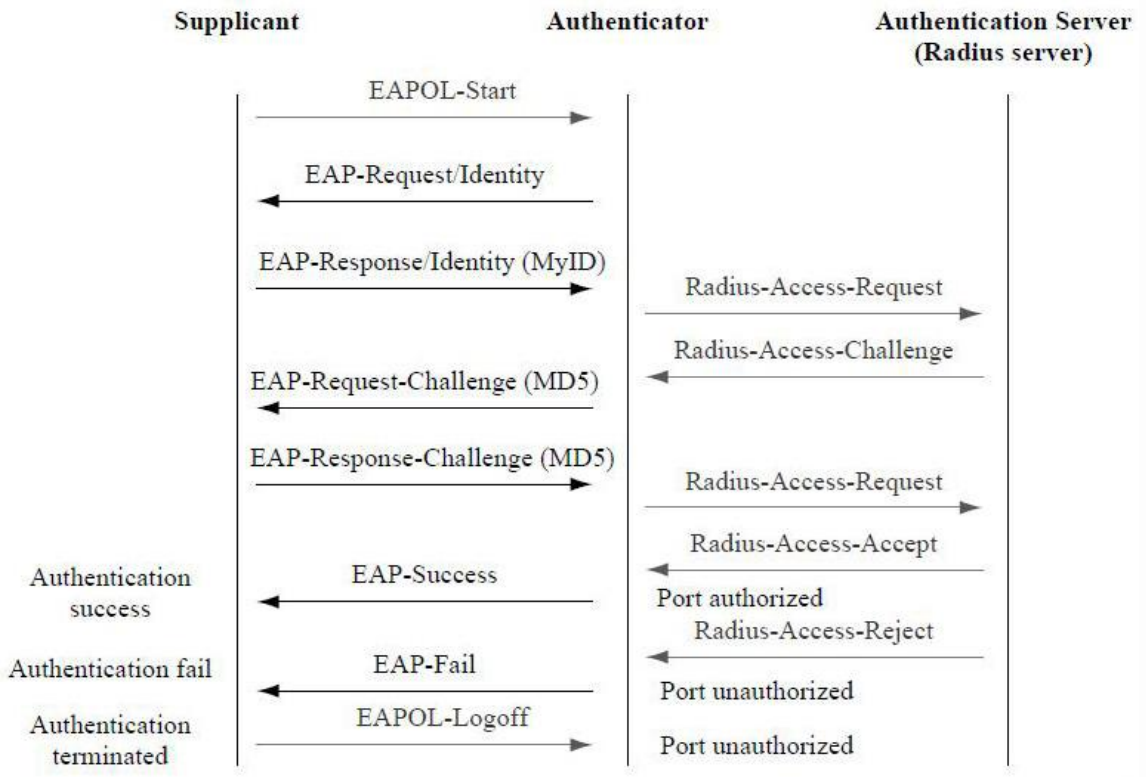
RADIUS server, για το επίπεδο πρόσβασης που πρέπει να έχει η συνδεδεμένη συσκευή.

IV. Μία κλήση (challenge) εκδίδεται από τον RADIUS server και προωθείται από το DSLAM στην συνδεδεμένη συσκευή.

V. Μια απάντηση κλήσης (challenge response) εκδίδεται από την συνδεδεμένη συσκευή, και προωθείται από το DSLAM στον server αυθεντικοποίησης, μαζί με ένα αίτημα πρόσβασης. Αν είναι ικανοποιητική η επικύρωση, ο server αυθεντικοποίησης θα εκδώσει ένα πακέτο που θα περιλαμβάνει την εξουσιοδότηση πρόσβασης στην θύρα. Αν η αυθεντικοποίηση αποτύχει, δεν θα δοθεί εξουσιοδότηση.

VI. Η απάντηση θα προωθηθεί στη συνδεδεμένη συσκευή και οι απαραίτητες διαδικασίες θα πραγματοποιηθούν στην θύρα.

Στην εικόνα 3.3 παρουσιάζεται η κίνηση των πακέτων κατά την 802.1X αυθεντικοποίηση.



Εικόνα 3.3 Ανταλλαγή πακέτων κατά την 802.1X Αυθεντικοποίηση

3.3.2 Τοίχος προστασίας

Για την προστασία της upstream κίνησης, που στέλνεται από το DSLAM στον middleware server, απαιτείται η εφαρμογή τοίχους προστασίας. Παρόλο που η περιφερειακή θύρα και το DSLAM εμποδίζουν τα αιτήματα σε μη εξουσιοδοτημένες θύρες, υπάρχει το ρίσκο οι επιτιθέμενοι να καταφέρουν να παρακάμψουν αυτούς τους μηχανισμούς ασφαλείας.

Ένα τοίχος προστασίας δικτύου πρέπει να εφαρμοστεί, πριν το home end, το οποίο θα φιλτράρει όλα τα αιτήματα και θα επιτρέπει μόνο τα έγκυρα αιτήματα στον middleware server.

3.4 Ασφάλεια στο Home End

Στο home end τα συστατικά βρίσκονται έξω από τον έλεγχο του πάροχου της υπηρεσίας IPTV και το hardware είναι εκτεθειμένο σε τροποποιήσεις από τους επιτιθέμενους. Τα αντίμετρα που μπορούμε να εφαρμόσουμε στο home end έχουν σκοπό να καθυστερήσουν τους επιτιθέμενους και να εμποδίσουν τις περισσότερες συνηθισμένες επιθέσεις.

Πρέπει να έχουμε κατά νου, ότι τα STB έχουν εικονική (virtual) πρόσβαση στην αποθήκη του video μέσω έγκυρων αιτημάτων. Αν οι επιτιθέμενοι αποκτήσουν τον έλεγχο του STB μέσω του internet, θα έχουν την δυνατότητα να εξάγουν ψηφιακό περιεχόμενο από το STB.

3.4.1 Ασφάλεια στην οικιακή πύλη πολυμεσικής επικοινωνίας

Η οικιακή πύλη πολυμεσικής επικοινωνίας συγκεντρώνει όλες τις υπηρεσίες που παρέχονται στον συνδρομητή. Επιπλέον, μοιράζεται διάφορες τοπικές συνδέσεις συμπεριλαμβανομένων των VoIP τηλεφώνων, της πρόσβασης σε internet υψηλών ταχυτήτων και των υπηρεσιών της IPTV. Η οικιακή πύλη πολυμεσικής επικοινωνίας (residential gateway) διαθέτει κάποιους βασικούς μηχανισμούς ασφαλείας, όπως οι λειτουργίες φιλτραρίσματος και δυνατότητες ποιότητας της υπηρεσίας (QoS).

i. **Φιλτράρισμα :** Η οικιακή πύλη πολυμεσικής επικοινωνίας μπορεί να ρυθμιστεί έτσι ώστε να φιλτράρει πακέτα και να επιτρέπει μόνο έγκυρα αιτήματα από το home end προς το head end. Συγκεκριμένα, τα φίλτρα μπορούν να εμποδίσουν οποιαδήποτε upstream κίνηση δεν συμμορφώνεται με τον αναμενόμενο τύπο κίνησης (80, 443, RTSP). Με αυτόν τον τρόπο θα μειωθούν οι πιθανότητες οι ιοί και τα worms να προσβάλλουν μεγάλο αριθμό των STB, ώστε να προκαλέσουν διακοπή υπηρεσίας στο head end. Επιπλέον, τα φίλτρα μπορούν να εμποδίσουν προσπάθειες μη εξουσιοδοτημένης πρόσβασης από το head end προς το STB. Έτσι θα

αποφύγουμε σάρωση θυρών (port scans) και παρόμοιες επιθέσεις στον οικιακό εξοπλισμό.

ii. **Ποιότητα της υπηρεσίας (Qos) :** Στην οικιακή πύλη πολυμεσικής επικοινωνίας μπορούν να ενεργοποιηθούν λειτουργίες της ποιότητας της υπηρεσίας, έτσι ώστε να ενδυναμώσουμε τους περιορισμούς της ποιότητας της υπηρεσίας. Η upstream κίνηση θα πρέπει να απαιτεί σχετικά χαμηλό bandwidth. Αν το STB προσβληθεί από κάποιο worm και προσπαθήσει να στείλει μεγάλα ποσά δεδομένων σε έγκυρες θύρες (80, 443, RSTP), τότε η ποιότητα της υπηρεσίας θα περιορίσει το bandwidth και θα ελαχιστοποιήσει την επίδραση της επίθεσης.

3.4.2 Ασφάλεια στο Set top Box

Τα STB συνήθως περιλαμβάνουν όλες τις λειτουργίες τους σε τσιπάκια. Ελάχιστες είναι οι περιπτώσεις χρήσης PC-based STB. Οι επιτιθέμενοι θα προσπαθήσουν να αφαιρέσουν το hardware, με σκοπό να καταλάβουν πως λειτουργεί το STB και σε ορισμένες περιπτώσεις να προγραμματίσουν ξανά τα τσιπάκια, με σκοπό να εισάγουν επιπρόσθετο λογισμικό στο σύστημα. Τα PC επιτρέπουν πιο εύκολη πρόσβαση σε πληροφορίες και σε κλειδιά, επειδή ο επιτιθέμενος έχει ήδη πλήρη έλεγχο του λειτουργικού συστήματος. Συγκεκριμένα, οι μόνες επιπλέον δραστηριότητες που απαιτούνται είναι η σύλληψη των κλειδιών όταν βρίσκονται στην μνήμη ή η σύλληψη του περιεχομένου μετά την αποκρυπτογράφησή του.

Τα STB σχεδιάζονται έτσι ώστε να αποθηκεύουν το λειτουργικό σύστημα και τους clients, με την χρήση hardware. Αυτά τα στοιχεία χρησιμοποιούνται για να αποθηκεύσουν κώδικα λογισμικού και κλειδιά. Ένα από τα πιο βασικά στοιχεία της λειτουργίας των STB είναι η flash memory. Η flash memory είναι αμετάβλητη μνήμη η οποία μπορεί να διαγραφτεί ηλεκτρικά και να προγραμματιστεί ξανά.

Όταν σχεδιάζουμε ένα περιβάλλον IPTV, πρέπει να εξασφαλίσουμε ότι τα STB που επιλέγουμε έχει κατάλληλα χαρακτηριστικά ασφαλείας, ώστε να μπορεί να προστατευτεί από επιθέσεις. Όταν συγκρίνουμε διαφορετικά μοντέλα STB πρέπει

να ερευνήσουμε τα χαρακτηριστικά ασφαλείας του κάθε μοντέλου και να διαπιστώσουμε πόσο καλά θα ανταποκριθεί το κάθε μοντέλο σε επιθέσεις εισβολής.

Το λειτουργικό σύστημα των STB πρέπει να προστατευτεί σύμφωνα με τους τρόπους που περιγράψαμε στην αρχή του κεφαλαίου. Οι θύρες και οι υπηρεσίες που δεν είναι χρήσιμες πρέπει να αφαιρεθούν, για να αποφύγουμε μη εξουσιοδοτημένη πρόσβαση στο σύστημα. Στην συνέχεια περιγράφονται τρείς βασικοί μηχανισμοί ασφαλείας του STB, το secure processor, το DRM και το output protection.

i. Secure processor :

Κάποιοι κατασκευαστές συμπεριλαμβάνουν τσιπάκια με μηχανισμούς στο STB, για να προστατέψουν τα προγράμματα που βρίσκονται εντός του εξοπλισμού. Έτσι οι επιτιθέμενοι δεν θα μπορούν να συλλάβουν τις πληροφορίες που είναι αποθηκευμένες στη μνήμη. Σε κάποια μοντέλα, τα οποία είναι ήδη διαθέσιμα, κάθε κομμάτι μιας flash συσκευής μπορεί να προστατευτεί ξεχωριστά ενάντια σε παράνομα προγράμματα και λειτουργίες διαγραφής. Επιπλέον τα κομμάτια αυτά, μπορούν να κλειδωθούν έτσι ώστε να μην επιτρέπεται περαιτέρω τροποποίησή τους. Μπλοκάροντας τομείς της flash μνήμης, εξασφαλίζουμε ότι οι επιτιθέμενοι δεν θα έχουν την δυνατότητα να προγραμματίσουν ξανά τις εφαρμογές. Έτσι θα προστατεύσουμε το STB από την εισαγωγή backdoors και από την αφαίρεση μηχανισμών ασφαλείας. Γενικά, θα διασφαλίσουμε ότι οι εφαρμογές θα λειτουργούν σύμφωνα με τον αρχικό σχεδιασμό τους.

Άλλοι διαθέσιμοι μηχανισμοί ασφαλείας, συμπεριλαμβάνουν αυθεντικοποίηση μεταξύ των στοιχείων της flash μνήμης και της CPU. Κάθε στοιχείο μπορεί να επικυρώσει το στοιχείο με το οποίο αντιστοιχίζεται και να παρέχει διαπιστευτήρια για την επιβεβαίωσή του. Με αυτόν τον τύπο αυθεντικοποίησης, αποτρέπονται οι παράνομες λειτουργίες μέσω μη εξουσιοδοτημένων επεξεργαστών ή flash μνήμης που έχουν συνδεθεί με παράλληλη σύνδεση. Οι επιτιθέμενοι προσπαθούν να αντικαταστήσουν τα στοιχεία που παρέχουν φραγμούς ασφαλείας(security barriers). Στην περίπτωση της flash μνήμης που έχει προστατευμένους τομείς, οι

επιτιθέμενοι θα προσπαθήσουν να την αντικαταστήσουν με ένα άλλο τσιπάκι το οποίο δεν θα έχει περιορισμούς.

Υπάρχουν μηχανισμοί ασφαλείας που εμποδίζουν τη μη εξουσιοδοτημένη ανάγνωση (reading) της μνήμης ή την δημιουργία διπλότυπων δεδομένων σε ιδιωτικές συσκευές, προστατεύοντας έτσι την πνευματική ιδιοκτησία και τον αποθηκευμένο κώδικα των προγραμμάτων. Οι επιτιθέμενοι θα έχουν μόνο την δυνατότητα πρόσβασης σε κρυπτογραφημένες καταχωρήσεις μνήμης (memory entries). Αυτό δεν θα συμβάλλει στη διαδικασία σύλληψης κλειδιών αποκρυπτογράφησης και περιεχομένου.

Γενικά, τα στοιχεία αυτού του τύπου αναφέρονται ως επεξεργαστές ασφαλείας system-on-chip και προσφέρουν προστασία ενάντια σε εισβολή και αλλοίωση. Έχουν τη δυνατότητα να εκτελούν κρυπτογραφημένα προγράμματα και να προστατεύουν δεδομένα και κώδικα από τους επιτιθέμενους. Οι επεξεργαστές ασφαλείας περιλαμβάνουν :

- Επεξεργαστές
- Σύστημα ανίχνευσης αλλοίωσης
- Τομέα αποθήκευσης κλειδιών
- Προστασία εκκίνησης
- Έλεγχο πρόσβασης
- Μηχανές κρυπτογράφησης
- Ασφαλή κανάλια

Το σύστημα ανίχνευσης αλλοίωσης, είναι ο πρωταρχικός μηχανισμός, ο οποίος ανιχνεύει κάθε προσπάθεια τροποποίησης του hardware. Αν το τσιπάκι αφαιρεθεί από την πλακέτα ή υπάρξει σε κάποιο στοιχείο απόπειρα μη εξουσιοδοτημένης πρόσβασης, το στοιχείο θα υποστεί βλάβη και η διαδικασία δεν θα μπορεί να ολοκληρωθεί.

Τα ασφαλή κανάλια χρησιμοποιούνται για την επικοινωνία εντός και εκτός του επεξεργαστή ασφαλείας.

Τα κλειδιά αποκρυπτογράφησης και τα ιδιωτικά κλειδιά, αποθηκεύονται και χρησιμοποιούνται μόνο εντός των στοιχείων του επεξεργαστή ασφαλείας. Αν ο DRM ή ο middleware server στείλει ένα συμμετρικό κλειδί, κρυπτογραφημένο με το

δημόσιο κλειδί του STB, το πακέτο αυτό θα ληφθεί από το STB σε κρυπτογραφημένη μορφή και θα προωθηθεί στον επεξεργαστή ασφαλείας όπου θα αποκρυπτογραφηθεί και θα αποθηκευτεί για μελλοντική χρήση.

Οι μηχανές κρυπτογράφησης χρησιμοποιούνται για να επιταχύνουν την διαδικασία κρυπτογράφησης και να εξασφαλίσουν ένα ασφαλές περιβάλλον για την επαναφορά (recovery) των πληροφοριών. Το κρυπτογραφημένο περιεχόμενο αποστέλλεται στον επεξεργαστή ασφαλείας μέσω των ασφαλών καναλιών και αποκρυπτογραφείται με την χρήση των διαθέσιμων συμμετρικών κλειδιών.

Ο βασικός σκοπός του επεξεργαστή ασφαλείας είναι να προστατεύσει τα κρίσιμα δεδομένα. Κρυπτογραφημένος κώδικας λαμβάνεται, αποκρυπτογραφείται και εκτελείται από τον επεξεργαστή ασφαλείας. Οι καταχωρήσεις μνήμης είναι κρυπτογραφημένες, όπως και τα δεδομένα τα οποία διαχειρίζεται ο επεξεργαστής ασφαλείας. Επειδή όλα τα δεδομένα είναι κρυπτογραφημένα, οι επιτιθέμενοι δεν έχουν καμία ευκαιρία να συλλάβουν δεδομένα σε διαμόρφωση ανοιχτού κειμένου (open text form).

ii. DRM :

Οι DRM clients είναι υπεύθυνοι για την διαπραγμάτευση και την επικύρωση των κλειδιών. Επιπλέον συμμετέχουν στην PKI ανταλλαγή επικύρωσης, η οποία περιλαμβάνει την παρουσίαση των ψηφιακών πιστοποιητικών των STB, την κρυπτογράφηση των πληροφοριών επικύρωσης μέσω του επεξεργαστή ασφαλείας και την επικύρωση των διαπιστευτηρίων από τον DRM server και τον middleware server.

Ο DRM client πρέπει να ρυθμιστεί κατάλληλα, έτσι ώστε να μπορεί να επικυρώσει τα δεδομένα που σχετίζονται με την PKI. Το σύστημα πρέπει να διαθέτει και να ελέγχει συχνά την λίστα ανάκλησης πιστοποιητικού. Είναι σημαντικό να εξασφαλίσουμε ότι η αρχή πιστοποίησης (CA και subCA) δεν έχει ανακληθεί και ότι οι DRM, οι middleware και οι VOD hosts έχουν έγκυρα πιστοποιητικά. Η λίστα ανάκλησης πιστοποιητικού πρέπει να υπογραφεί ψηφιακά από έναν έγκυρο CA. Τα root CA πιστοποιητικά, πρέπει να είναι αποθηκευμένα σε μια ασφαλή τοποθεσία μέσα στο STB και πρέπει να απαγορεύεται η τροποποίηση αυτών των καταχωρήσεων. Οι επιτιθέμενοι μπορεί να προσπαθήσουν να εισάγουν ψευδή

πιστοποιητικά CA, έτσι ώστε να ξεγελάσουν το STB ώστε να δεχτεί ψευδή DRM και middleware πιστοποιητικά.

Το ψηφιακό πιστοποιητικό του STB και τα ιδιωτικά κλειδιά, πρέπει να αποθηκευτούν σε μια ασφαλή τοποθεσία στο STB, έτσι ώστε να εμποδίσουμε την αλλοίωσή τους. Ένα αντίγραφο των πιστοποιητικών μπορεί να διατηρείται σε μια έξυπνη κάρτα, μέσα στο STB. Με αυτόν τον τρόπο προσθέτουμε ένα επιπλέον επίπεδο ασφαλείας.

iii. Output protection :

Οι επιτιθέμενοι μπορεί να προσπαθήσουν να πάρουν τον έλεγχο του STB και να εξάγουν πολύτιμες ροές περιεχομένου. Η εξαγωγή του STB μπορεί να υποκλαπεί, έτσι ώστε οι επιτιθέμενοι να διανείμουν αντίγραφα των ψηφιακών αγαθών. Είναι σημαντικό να προστατεύσουμε την εξαγωγή των STB, σύμφωνα με διεθνή πρότυπα όπως το HDCP (*high bandwidth digital content protection*) και το DTCP (*digital transmission content protection*).

Το HDCP χρησιμοποιείται για να προστατεύσει τα ψηφιακά αγαθά από μη εξουσιοδοτημένη αντιγραφή-αναπαραγωγή. Το πρότυπο αυτό καλύπτει την εξαγωγή από το DVI (*digital visual interface*) και από το HDMI (*high definition multimedia interface*). Το HDCP παρέχει τους απαραίτητους μηχανισμούς αυθεντικοποίησης, ώστε να εμποδίσει οποιαδήποτε εξαγωγή υψηλής ευκρίνειας σε μη εξουσιοδοτημένες συσκευές. Μόνο εξουσιοδοτημένες συσκευές, οι οποίες δεν δημιουργούν διπλότυπα του περιεχομένου, επιτρέπεται να λάβουν το περιεχόμενο. Με την κρυπτογράφηση του περιεχομένου, εμποδίζεται η υποκλοπή και η τροποποίησή του κατά την μετάδοση. Αν γνωρίζουμε ότι κάποιο μοντέλο έχει καταληφθεί από κάποιον hacker, μπορούν να ανακληθούν τα κλειδιά του έτσι ώστε να μην μπορεί να λάβει HD περιεχόμενο. Το HDCP παρέχει ένα σετ 40 μοναδικών κλειδιών σε κάθε συσκευή. Τα κλειδιά έχουν μήκος 56 bits. Επιπλέον, στην συσκευή ανατίθεται και ένα KSV (*key selection vector*), το οποίο χρησιμοποιείται από τον αποδέκτη και το STB για να ανταλλάξει πληροφορίες επικύρωσης και να επιλέξει τα HDCP κλειδιά κρυπτογράφησης.

Το DTCP χρησιμοποιείται για να επιτρέψει στα STB, στα PC, στις κονσόλες πολυμέσων και σε άλλες συσκευές του home end να συνδεθούν με την χρήση USB,

PCI, Bluetooth, Firewire και IP. Η εξαγωγή του STB θα περιοριστεί στις συσκευές που έχουν αυθεντικοποιηθεί, εμποδίζοντας έτσι την αντιγραφή του ψηφιακού περιεχομένου.

3.5 Ασφάλεια κατά ITU-T X.805

Το ITU-T X.805 παρέχει ένα πλαίσιο για μια πλήρη ανασκόπηση όλων των ζητημάτων ασφαλείας σε ένα IPTV περιβάλλον. Υπάρχουν οκτώ διαστάσεις ασφαλείας οι οποίες εφαρμόζονται στα παρακάτω τρία πεδία :

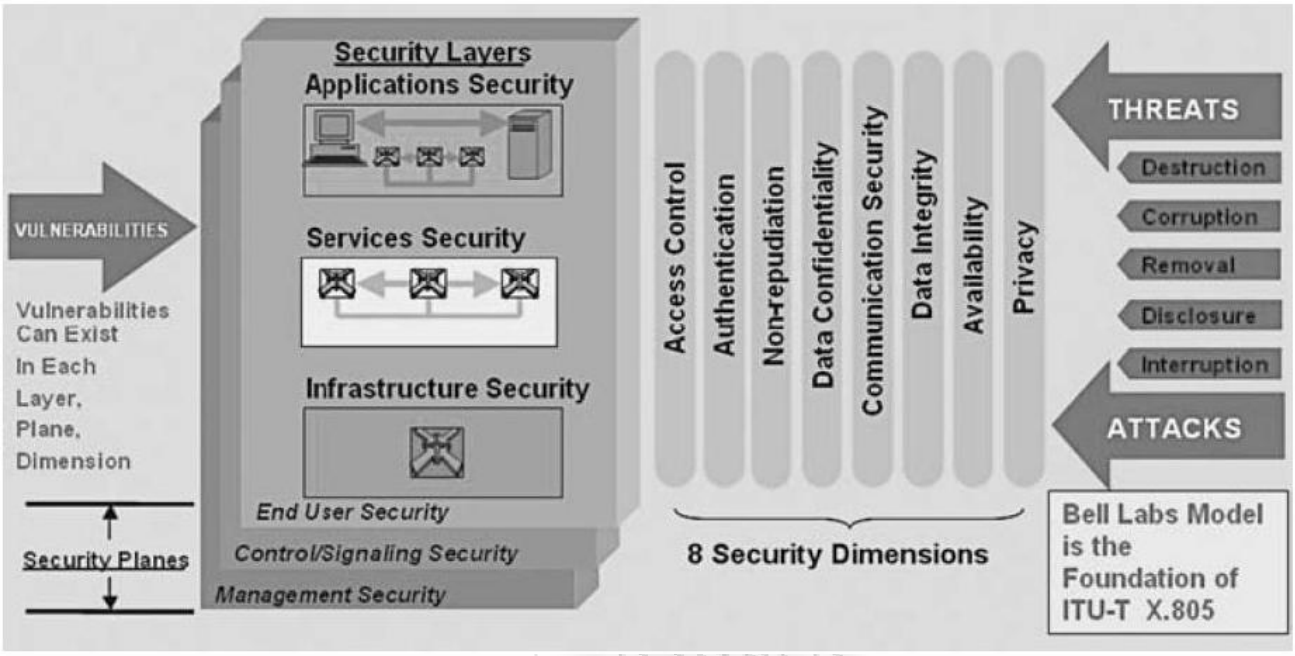
- Ασφάλεια της διαχείρισης (*management security*)
- Ασφάλεια ελέγχου (*control security*)
- Ασφάλεια χρήστη (*end user security*)

Το κάθε πεδίο περιλαμβάνει τρία επίπεδα, (i) των εφαρμογών, (ii) των υπηρεσιών και (iii) της υποδομής. Οι οκτώ διαστάσεις ασφαλείας είναι οι εξής :

- Έλεγχος πρόσβασης
- Αυθεντικοποίηση
- Μη άρνηση αναγνώρισης (*nonrepudiation* : ένα πρόσωπο που στέλνει ένα μήνυμα δεν μπορεί να αρνηθεί ότι το έστειλε και αντίστροφα)
- Εμπιστευτικότητα δεδομένων
- Ασφάλεια επικοινωνίας
- Ακεραιότητα δεδομένων
- Διαθεσιμότητα
- Ιδιωτικότητα

Η διασταύρωση της κάθε διάστασης ασφαλείας με το κάθε πεδίο ασφαλείας δηλώνει που πρέπει να εφαρμοστούν αντίμετρα και μηχανισμοί ασφαλείας, για να

αντιμετωπιστούν οι απειλές. Στην εικόνα 3.4 παρουσιάζονται τα πεδία, οι διαστάσεις και οι απειλές ασφαλείας κατά το ITU-T X.805.



Εικόνα 3.4 Ασφάλεια κατά ITU-T X.805

Στην συνέχεια θα περιγράψουμε τα επίπεδα των πεδίων ασφαλείας και την επίδραση των διαστάσεων ασφαλείας στο καθένα από αυτά.

i. Ασφάλεια στο επίπεδο εφαρμογών, στο πεδίο της διαχείρισης

1) **Έλεγχος Πρόσβασης** : Διασφαλίζει ότι επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό να εφαρμόσει δραστηριότητες διαχείρισης στις εφαρμογές, όπως η διαχείριση των αιτημάτων για VOD και η πρόσβαση στις λίστες και στις περιγραφές περιεχομένου. Μόνο εξουσιοδοτημένοι χρήστες πρέπει να έχουν την δυνατότητα απομακρυσμένης διαχείρισης του STB, του εξοπλισμού του δικτύου broadcast και όσων στοιχείων σχετίζονται με head end broadcast. Η έλλειψη κατάλληλων μηχανισμών ελέγχου πρόσβασης, θα οδηγήσει σε επιθέσεις διακοπής υπηρεσίας, εξαπάτησης πρόσβασης (*access fraud*) και επιθέσεις τύπου man in the middle.

2) **Αυθεντικοποίηση** : Επικυρώνει την ταυτότητα του προσώπου ή της συσκευής, που προσπαθεί να εκτελέσει δραστηριότητες διαχείρισης σε εφαρμογές δικτύου. Έτσι θα μειωθεί ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης σε περιεχόμενο. Ο έλεγχος πρόσβασης είναι συνδεδεμένος με την αυθεντικοποίηση των χρηστών. Όλοι οι χρήστες πρέπει να έχουν επικυρωμένη ταυτότητα.

3) **Μη άρνηση αναγνώρισης :** Καταγράφει όλα τα άτομα τα οποία εκτελούν δραστηριότητες διαχείρισης σε εφαρμογές δικτύου. Επιπλέον, με αυτήν την διάσταση ασφαλείας, μειώνονται οι πιθανότητες απάτης του συνδρομητή (*subscriber fraud*), για παράδειγμα η παροχή της υπηρεσίας σε λογαριασμούς "φαντάσματα" (*ghost-accounts*).

4) **Εμπιστευτικότητα δεδομένων :** Προστατεύει όλα τα αρχεία που χρησιμοποιούνται για την δημιουργία και την διαχείριση μιας εφαρμογής. Όλες οι πληροφορίες πελατών πρέπει να προστατεύονται από την πρόσβαση τρίτων, οι οποίες συμπεριλαμβάνουν ηλεκτρονικές καταγραφές των πελατών και πληροφορίες ρυθμίσεων. Πρέπει να κρυπτογραφούνται για να αποφύγουμε την μη εξουσιοδοτημένη πρόσβαση σε αυτές.

5) **Ασφάλεια επικοινωνίας :** Εξασφαλίζει ότι οι πληροφορίες διαχείρισης ρέουν μόνο μεταξύ της εφαρμογής και της εξουσιοδοτημένης ομάδας.

6) **Ακεραιότητα δεδομένων :** Όλες οι πληροφορίες ρύθμισης και διαχείρισης και τα δεδομένα των εφαρμογών πρέπει να προστατεύονται από μη εξουσιοδοτημένη τροποποίηση. Έτσι οι επιτιθέμενοι δεν έχουν την δυνατότητα να τροποποιήσουν δεδομένα και να προκαλέσουν κατάρρευση του συστήματος (*system failure*).

7) **Διαθεσιμότητα :** Διασφαλίζει ότι η δυνατότητα διαχείρισης μια εφαρμογής, δεν επηρεάζεται ή παρεμποδίζεται.

8) **Ιδιωτικότητα :** Διασφαλίζει ότι οι πληροφορίες που μπορούν να χρησιμοποιηθούν για την αναγνώριση network-based εφαρμογών, δεν είναι εκτεθειμένες σε μη εξουσιοδοτημένες ομάδες.

ii. Ασφάλεια στο επίπεδο εφαρμογών, στο πεδίο του ελέγχου

1) **Έλεγχος Πρόσβασης** : Διασφαλίζει ότι οι πληροφορίες ελέγχου των εφαρμογών που λαμβάνονται από μια συσκευή δικτύου, η οποία συμμετέχει σε μια εφαρμογή δικτύου, προέρχονται από εξουσιοδοτημένη πηγή. Οι διάφορες παράμετροι που λαμβάνονται πρέπει να προστατεύονται, για να μην έχουν την δυνατότητα οι επιτιθέμενοι να χειριστούν την διαδικασία ελέγχου. Είναι πολύ σημαντικό να εφαρμοστούν μηχανισμοί ελέγχου πρόσβασης έτσι ώστε μόνο έγκυρα στοιχεία χρησιμοποιούνται για υπηρεσίες όπως το DHCP και το DNS.

2) **Αυθεντικοποίηση :** Επικυρώνει την ταυτότητα της πηγής των πληροφοριών ελέγχου των εφαρμογών που στέλνονται στις συσκευές δικτύου που συμμετέχουν στις εφαρμογές.

3) **Μη άρνηση αναγνώρισης :** Παρέχει μια καταγραφή (record) αναγνώρισης της οντότητας, από την οποία προέρχονται οι πληροφορίες ελέγχου των εφαρμογών. Όλες οι πληροφορίες ελέγχου πρέπει να περιλαμβάνουν δεδομένα μη άρνησης αναγνώρισης. Τέτοια είναι οι ψηφιακές υπογραφές ή log details του συστήματος και του λογαριασμού που χρησιμοποιήθηκε για την αποστολή των πληροφοριών.

4) **Εμπιστευτικότητα δεδομένων :** Προστατεύει τις πληροφορίες ελέγχου των εφαρμογών που βρίσκονται σε μια συσκευή δικτύου και μεταδίδονται στο δίκτυο. Τα δεδομένα εφαρμογών πρέπει να προστατεύονται από τους επιτιθέμενους, οι οποίοι θα προσπαθήσουν να συλλάβουν πληροφορίες ελέγχου, session keys κτλ.

5) **Ασφάλεια επικοινωνίας :** Διασφαλίζει ότι οι πληροφορίες ελέγχου των εφαρμογών που μεταφέρονται, ρέουν μόνο μεταξύ εξουσιοδοτημένων κόμβων. Έτσι παρέχεται προστασία ενάντια σε επιθέσεις man in the middle.

iii. Ασφάλεια στο επίπεδο εφαρμογών, στο πεδίο του τελικού χρήστη

1) **Έλεγχος πρόσβασης :** Διασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες επιτρέπεται να χρησιμοποιούν τις εφαρμογές δικτύου.

2) **Αυθεντικοποίηση :** Επικυρώνει την ταυτότητα του χρήστη που προσπαθεί να χρησιμοποιήσει την εφαρμογή.

3) **Μη άρνηση αναγνώρισης :** Παρέχει καταγραφή (record) που αναγνωρίζει κάθε χρήστη που έχει πρόσβαση στην εγαρμογή.

4) **Εμπιστευτικότητα δεδομένων :** Προστατεύει τα δεδομένα του τελικού χρήστη τα οποία μεταφέρονται ή αποθηκεύονται από την εφαρμογή του δικτύου.

5) **Ασφάλεια επικοινωνίας :** Διασφαλίζει ότι τα δεδομένα του τελικού χρήστη δεν εκτρέπονται ή συλλαμβάνονται από μη εξουσιοδοτημένες οντότητες.

6) **Ακεραιότητα δεδομένων :** Προστατεύει τα δεδομένα του τελικού χρήστη που μεταφέρονται από μια εφαρμογή δικτύου, από την τροποποίηση, την διαγραφή και την αντιγραφή.

7) **Διαθεσιμότητα :** Διασφαλίζει ότι δεν θα επιτρέπεται η πρόσβαση από μη εξουσιοδοτημένους τελικούς χρήστες σε μια εφαρμογή δικτύου.

8) **Ιδιωτικότητα :** Διασφαλίζει ότι μια εφαρμογή δικτύου δεν αποκαλύπτει πληροφορίες που αφορούν τον τελικό χρήστη.

iv. Ασφάλεια στο επίπεδο υπηρεσιών, στο πεδίο της διαχείρισης

1) **Έλεγχος Πρόσβασης :** Διασφαλίζει ότι μόνο εξουσιοδοτημένο προσωπικό και εξουσιοδοτημένες συσκευές επιτρέπεται να εκτελέσουν δραστηριότητες διαχείρισης των υπηρεσιών δικτύου. Για παράδειγμα, να παρέχει σε έναν χρήστη πρόσβαση στην υπηρεσία.

2) **Αυθεντικοποίηση :** Η ταυτότητα κάποιας οντότητας πρέπει να επιβεβαιώνεται πριν του επιτραπεί πρόσβαση σε λειτουργίες διαχείρισης στο επίπεδο υπηρεσιών.

3) **Μη άρνηση αναγνώρισης :** Παρέχει καταγραφή (record) όλων των οντοτήτων που εκτελούν ενέργειες διαχείρισης στις υπηρεσίες δικτύου.

4) **Εμπιστευτικότητα Δεδομένων :** Παρέχει προστασία στις πληροφορίες διαχείρισης των υπηρεσιών δικτύου, από μη εξουσιοδοτημένη πρόσβαση. Συμπεριλαμβάνει κωδικούς ασφαλείας, ρυθμίσεις και παραμέτρους.

5) **Ακεραιότητα δεδομένων :** Παρέχει προστασία στις πληροφορίες διαχείρισης των υπηρεσιών δικτύου, από μη εξουσιοδοτημένη τροποποίηση, διαγραφή ή αντιγραφή.

6) **Διαθεσιμότητα :** Διασφαλίζει οι διαχειριστές να έχουν την δυνατότητα διαχείρισης των υπηρεσιών του δικτύου, κάθε στιγμή.

7) **Ιδιωτικότητα :** Διασφαλίζει ότι οι πληροφορίες που μπορούν να αναγνωρίσουν τα συστήματα διαχείρισης δεν είναι διαθέσιμες σε μη εξουσιοδοτημένο προσωπικό.

v. Ασφάλεια στο επίπεδο υπηρεσιών, στο πεδίο του ελέγχου

1) **Έλεγχος πρόσβασης :** Διασφαλίζει ότι όλες οι πληροφορίες ελέγχου που λαμβάνονται από τα διάφορα στοιχεία, έχουν σταλεί από εξουσιοδοτημένες πηγές.

2) **Αυθεντικοποίηση :** Παρέχει επιβεβαίωση της ταυτότητας κάθε στοιχείου που στέλνει πληροφορίες ελέγχου.

3) **Μη άρνηση αναγνώρισης :** Παρέχει καταγραφή (record) που αναγνωρίζει όλα τα στοιχεία που στέλνουν πληροφορίες ελέγχου.

4) **Εμπιστευτικότητα δεδομένων :** Παρέχει προστασία σε όλες τις πληροφορίες ελέγχου που αποθηκεύονται ή αποστέλλονται μέσω του δικτύου, από μη εξουσιοδοτημένη πρόσβαση.

5) **Ασφάλεια επικοινωνίας :** Όλες οι πληροφορίες ελέγχου πρέπει να ρέουν μόνο μεταξύ της καθορισμένης πηγής και προορισμού.

6) **Ακεραιότητα δεδομένων :** Παρέχει προστασία στις πληροφορίες ελέγχου των υπηρεσιών που βρίσκονται σε συσκευές δικτύου ή σε servers, από μη εξουσιοδοτημένη πρόσβαση.

vi. Ασφάλεια στο επίπεδο υποδομής, στο πεδίο διαχείρισης

1) **Έλεγχος πρόσβασης :** Διασφαλίζει ότι μόνο εξουσιοδοτημένο προσωπικό επιτρέπεται να εκτελεί δραστηριότητες διαχείρισης σε συσκευές δικτύου ή σε συνδέσμους επικοινωνίας. Αυτός ο μηχανισμός μπορεί να εφαρμοστεί σε όλα τα στοιχεία που σχετίζονται με την επικοινωνία. Χωρίς τους κατάλληλους μηχανισμούς ελέγχου πρόσβασης, οι επιτιθέμενοι μπορούν να τροποποιήσουν τις ρυθμίσεις των στοιχείων επικοινωνίας και να προκαλέσουν διακοπή στην υπηρεσία, να κλέψουν την υπηρεσία ή να εφαρμόσουν μια επίθεση τύπου man in the middle.

2) **Αυθεντικοποίηση :** Επιβεβαιώνει την ταυτότητα της οντότητας ή της συσκευής που εκτελεί δραστηριότητες διαχείρισης σε στοιχεία δικτύου. Οι κατάλληλοι μηχανισμοί αυθεντικοποίησης των συσκευών μειώνουν την επίδραση των επιθέσεων τύπου man in the middle και εξασφαλίζουν ότι τα downstream στοιχεία, δέχονται πληροφορίες μόνο από αυθεντικοποιημένες πηγές. Τα worms στηρίζονται σε μη αυθεντικοποιημένες επικοινωνίες για να μολύνουν και άλλα στοιχεία.

3) **Μη άρνηση αναγνώρισης :** Παρέχει καταγραφή (record) όλων των οντοτήτων και των συσκευών που εκτελούν δραστηριότητες διαχείρισης στα στοιχεία του δικτύου. Οποιαδήποτε αλλαγή στο σύστημα πρέπει να

αντιστοιχίζεται με μια ξεχωριστή οντότητα ή με μια συσκευή. Έτσι ενισχύονται οι δυνατότητες ελέγχου.

4) **Εμπιστευτικότητα δεδομένων :** Προστατεύει τις επικοινωνίες του δικτύου από μη εξουσιοδοτημένη πρόσβαση και παρακολούθηση. Περιλαμβάνει όλα τα δεδομένα που σχετίζονται με το επίπεδο της υποδομής, όπως τις πληροφορίες ρυθμίσεων, τα δεδομένα αυθεντικοποίησης και τα δεδομένα backup.

5) **Ασφάλεια επικοινωνίας :** Προστατεύει την ροή των δεδομένων κατά την απομακρυσμένη διαχείριση. Διασφαλίζει ότι οι επικοινωνίες δεν εκτρέπονται, ούτε διακόπτονται.

6) **Ακεραιότητα δεδομένων :** Προστατεύει τις πληροφορίες διαχείρισης, από τροποποίηση. Έτσι οι επιτιθέμενοι δεν μπορούν να τροποποιήσουν οδηγίες (instructions) και δεδομένα ρυθμίσεων.

7) **Διαθεσιμότητα :** Προστατεύει την δυνατότητα διαχείρισης των συσκευών του δικτύου και των συνδέσμων επικοινωνίας. Οι πληροφορίες για τις ρυθμίσεις στα διάφορα συστήματα πρέπει να είναι διαρκώς διαθέσιμες.

8) **Ιδιωτικότητα :** Οι πληροφορίες που μπορούν να χρησιμοποιηθούν για να αναγνωρίσουν συσκευές δικτύου δεν πρέπει να είναι διαθέσιμες σε μη εξουσιοδοτημένες ομάδες. Έτσι μειώνεται ο κίνδυνος χαρτογράφησης του δικτύου από τους επιτιθέμενους.

vii. Ασφάλεια στο επίπεδο υποδομής, στο πεδίο του ελέγχου

1) **Έλεγχος πρόσβασης :** Οι συσκευές του δικτύου πρέπει να δέχονται μηνύματα με πληροφορίες ελέγχου μόνο από εξουσιοδοτημένες συσκευές δικτύου. Έτσι μειώνεται η απειλή μη εξουσιοδοτημένων τροποποιήσεων. Επιπλέον, εμποδίζει τα worms να χρησιμοποιήσουν πληροφορίες ελέγχου για να κάνει νέες ρυθμίσεις στην υποδομή και να προκαλέσει διακοπή της υπηρεσίας.

2) **Αυθεντικοποίηση :** Επιβεβαιώνει την ταυτότητα της συσκευής που αποστέλλει πληροφορίες ελέγχου.

3) **Μη άρνηση αναγνώρισης :** Διατηρεί καταγραφές (records) που αναγνωρίζουν συσκευές που στέλνουν πληροφορίες ελέγχου. Κάθε τροποποίηση πρέπει να καταγράφεται μαζί με την ταυτότητα της οντότητας που την προκάλεσε και να εξασφαλίζεται η ευθύνη για οποιαδήποτε αλλαγή στην υποδομή.

4) **Εμπιστευτικότητα δεδομένων :** Οι πληροφορίες ελέγχου, συμπεριλαμβάνουν εμπιστευτικά δεδομένα, όπως οι κωδικοί πρόσβασης και λεπτομέρειες για τις ρυθμίσεις ασφαλείας. Τα δεδομένα πρέπει να προστατεύονται για να αποφύγουμε την πρόσβαση των επιτιθέμενων σε πληροφορίες ελέγχου.

5) **Ασφάλεια επικοινωνίας :** Διασφαλίζει ότι οι πληροφορίες ελέγχου ρέουν μόνο από την καθορισμένη πηγή προς τον συγκεκριμένο προορισμό.

6) **Ακεραιότητα δεδομένων :** Προστατεύει τις πληροφορίες ελέγχου που είναι αποθηκευμένες στις συσκευές δικτύου ή στους servers.

7) **Διαθεσιμότητα :** Διασφαλίζει ότι τα στοιχεία του δικτύου έχουν πάντα την δυνατότητα να λάβουν πληροφορίες ελέγχου.

8) **Ιδιωτικότητα :** Οι πληροφορίες που μπορούν να χρησιμοποιηθούν για να αναγνωρίσουν ένα συγκεκριμένο στοιχείο δικτύου, πρέπει να παραμένουν εμπιστευτικές.

4. Συμπέρασμα

Η ασφάλεια της IPTV πρέπει να είναι προσανατολισμένη στην προστασία του κάθε σημείου της υπηρεσίας (*point to point approach*). Οι χάκερς θα εκμεταλλευτούν οποιοδήποτε ευάλωτο σημείο υπάρχει και θα επιτεθούν στην υποδομή της IPTV, για να αποκτήσουν πρόσβαση σε περιεχόμενο ή σε προσωπικές πληροφορίες των συνδρομητών. Το head end κληρονομεί τις ευπάθειες του λειτουργικού συστήματος που χρησιμοποιεί για τις εφαρμογές της IPTV και για τον εξοπλισμό επικοινωνίας. Η κίνηση στο head end πρέπει να περιοριστεί σε συγκεκριμένα VLAN και όλα τα στοιχεία του πρέπει να αναβαθμίζονται με τα τελευταία patch ασφαλείας. Η IPTV επιτρέπει σε ένα μεγάλο βαθμό την αλληλεπίδραση των χρηστών με τις εφαρμογές της IPTV. Κάποιοι χρήστες χρησιμοποιούν υπηρεσίες HTTP και TFTP, όπου υπάρχουν γνωστές ευπάθειες σε αυτά τα πρωτοκόλλα και τις υπηρεσίες. Οι χακερς μπορούν να εκμεταλλευτούν αυτές τις ευπάθειες ώστε να αποκτήσουν των έλεγχο των server και των εφαρμογών. Το home end είναι επίσης ευάλωτο σε επιθέσεις των χακερ στα PC και στα STB. Από την πλευρά του πάροχου της υπηρεσίας, το STB δεν πρέπει να θεωρείται ως ασφαλές στοιχείο. Είναι πολύ σημαντικό να εφαρμοστούν μηχανισμοί ελέγχου, που θα ανιχνεύουν την προσπάθεια πρόσβασης σε περιεχόμενο και πρέπει να λαμβάνονται μέτρα διακοπής της υπηρεσίας στους συνδρομητές που έχουν τροποποιήσει το σύστημά τους. Όλες οι συνδέσεις πρέπει να ελέγχονται έτσι ώστε να εξασφαλίσουμε ότι οι συνδρομητές δεν αναδιανείμουν το περιεχόμενο που λάβανε.

Η βάση για ένα ασφαλές περιβάλλον IPTV, είναι η λεπτομερή γνώση όλων των στοιχείων του περιβάλλοντος καθώς και οι τεχνολογίες και οι επικοινωνίες που σχετίζονται με αυτά. Πρέπει να γνωρίζουμε τις απειλές που υπάρχουν στο σύστημά μας και να αναλογιστούμε, κάθε φορά , την επίδραση που θα έχει η αφαίρεση ή η πρόσθεση ενός μηχανισμού ασφαλείας.

Βιβλιογραφία

1. Held Gilbert. *UNDERSTANDING IPTV.* New York : Auerbach Publications, 2007.

2. Venkata N. Padmanabhan, Helen J. Wang, Philip A. Chou. *Distributing streaming media content using cooperative networking.* Microsoft Research, 2002.

3. Δημήτρης Ζεϊναλιπούρ, Στέλλα Αριστείδου, Σοφία Καζέλη. *Internet Protocol Quality of Services.* Department of Computer Science – University of Cyprus, 1999.

4. ITU-T. *Security in Telecommunications and Information Technology.* ITU-T, 2003.

5. ITU-T FG IPTV-ID-0051. *IPTV security requirements.* FG IPTV, 2006 .

6. Hong Joo Lee. *A Review of IPTV Threats Based on the Value Chain.* College of Business Administration, Seoul National University,2006.

7. Zachary Zeltsan. *ITU-T Recommendation X.805 and its application to NGN.* Lucent Technologies, 2005.

8. Arnaud Robert. *July 18th CPTWG Meeting - Securing IPTV.* NagraVision – Kudelski group, 2002.

9. Jongyoul Park. *Security Issues for IPTV services.* Electronics and Telecommunications Research Institute, 2007.

10. ITU-T FG IPTV-DOC-0155. *Working Document: IPTV Security Aspects.* FG IPTV, 2006.

11. ITU-T FG IPTV-C-0217. *End-to-End IPTV Security: Assets, Risks and Threat.* FG IPTV, 2006.

12. Ramirez David. *Protecting High-value Digital Contents*. John Wiley & Sons Ltd, 2008.