IPTV: Uma abordagem sobre segurança

Uma das mais importantes tecnologias para distribuição de conteúdo é o conceito de Internet Protocol Television (IPTV) que é, em grande parte, resultado da viabilizado pela difusão do Internet Protocol (IP) e da evolução das plataformas que permitem a oferta de serviços de transmissão de vídeo, valendo-se de uma infra-estrutura IP convergente. O serviço IPTV permite o uso de uma rede banda larga para entregar conteúdo de TV, com garantia de qualidade de serviço e, potencialmente, acrescido de serviços interativos.

A combinação IP mais TV é a expressão do conceito da convergência multimídia: voz, vídeo e dados. O IPTV abre novas oportunidades de negócio às operadoras de telecomunicações, pequenos provedores e tem elementos para colocar em prática uma oferta chamada Triple Play (voz + acesso à Internet banda larga + TV) ou até Quadruple Play (Triple Play + celular). O acesso banda larga se torna veículo não apenas de acesso a Internet, mas passa a realizar chamadas utilizando Voice Over IP (VoIP).

O IPTV ganha força no Brasil com a aprovação da Resolução número 581 de 26 de março de 2012. Essa resolução define o SeAC (Serviço de Acesso Condicionado), que é destinado à distribuição de conteúdos audiovisuais na forma de pacotes, de canais de programação nas modalidades avulsa de programação e avulsa de conteúdo programado e de Canais de Programação de Distribuição Obrigatória, por meio de **tecnologias, processos, meios eletrônicos e protocolos de comunicação quaisquer (aqui destaca-se a utilização do IPTV)** (Resolução 578, 2012).

Apresentamos neste tutorial a tecnologia IPTV, abordando tanto aspectos de infraestrutura quanto aspectos de segurança.

Luciano Henrique Duque

Engenheiro Eletricista, com Ênfase em Eletrônica e Telecomunicações, pelo Instituto Nacional de Telecomunicações (INATEL, 1994) e Mestre em Engenharia Elétrica pela Universidade de Brasília (UnB, 2008). É Professor Mestre do UniCEUB (Centro Universitário de Brasília) no curso de Graduação em Engenharia Elétrica e Pós-Graduação em Redes Com ênfase em Segurança. Atuou como Engenheiro consultor em Redes na Oi/BrasilTelecom por 15 anos. Atualmente é Engenheiro Consultor de Telecomunicações em sua empresa LHD Engenharia. Tem vasta experiência na área de Engenharia Elétrica, com ênfase em Telecomunicações e eletrônica, atuando principalmente nos seguintes temas: projetos para regularização de serviços junto a Anatel (SCM e SeAC), e Consultorias na área de Avaliação da qualidade de Rede de Banda Largas, TV Digital, IPTV.

Email: luciano.duque@brturbo.com.br

IPTV: I - Serviços do IPTV

Os serviços que compõem uma oferta de IPTV são definidos nas seguintes categorias: vídeo, áudio, comunicação, entretenimento, comércio e utilitários. O IPTV representa a transmissão de sinais multimídia, tais como: áudio, vídeo, gráficos, textos e TV, sempre transportando em rede IP com garantias de qualidade, segurança, integridade e confiabilidade.

Os serviços de vídeo englobam duas grandes categorias – broadcast e vídeo armazenado. O serviço de broadcast é o tradicional existente na TV aberta ou TV paga, baseado em canais e grades de programação. Esse serviço constitui a base de um serviço de TV e oferece aos usuários a possibilidade de controlar o conteúdo armazenado incluindo funções como play, stop, rewind, fast forward. Exemplos de modalidades de serviços nesta categoria incluem:

***Video on Demand* (VOD)**: usuário pode selecionar o conteúdo que deseja assistir de uma lista que inclui filmes, documentários, entre outros programas. Existem diversas variações de modalidades do serviço como, por exemplo: near VOD (NVOD) em que existem horários pré-definidos (ex.: meia em meia hora) para início da exibição de um determinado conteúdo; subscription VOD (SVOD) em que o usuário paga uma assinatura que lhe dá direito a consumir uma quantidade de títulos determinada; free VOD (FVOD) em que o usuário possui acesso gratuito a conteúdo sob demanda; e o VOD propriamente dito em que, tradicionalmente, o usuário paga por transação.

Virtual Channels: é uma variação dos serviços NVOD em que a operadora cria canais virtuais para exibir conteúdos selecionados. Por exemplo, é possível criar canais virtuais temáticos onde são exibidos filmes de um determinado gênero sequencialmente.

Time-shifted TV: enquanto o usuário assiste um conteúdo broadcast, possui a facilidade de retroceder no tempo como se tivesse utilizando um vídeo cassete e depois continua a seguir o conteúdo de acordo com a transmissão original.Personal Video Recorder (PVR) ou Digital Video Recorder (DVR): facilidade que permite ao usuário armazenar um conteúdo desejado de acordo com regras pré-estabelecidas de Digital Rights Management (DRM). A facilidade é análoga a de um vídeo-cassete. O conteúdo pode ficar armazenado localmente no *Customer Premises Equipment* (CPE) do usuário, ou então em unidades de armazenamento distribuídas na rede da operadora sendo denominado então de network PVR (NPVR).

Áudio

Os serviços de áudio incluem:

Broadcast de música: serviços de transmissão de estações de rádio tradicionais ou de canais de música criados pela operadora, e que podem ser personalizados e já são oferecidos pelas operadoras de TV a cabo e satélite.

Música sob demanda: serviço análogo ao VOD aplicado no contexto de música, permitindo ao usuário selecionar as músicas que deseja ouvir e até criar coleções personalizadas.

Comunicação

Os serviços de comunicação integrados permitem às operadoras adicionarem funcionalidades avançadas aos serviços tradicionais de telefonia e acesso à Internet, além de oferecerem aos usuários um novo meio de comunicação, a TV. Os serviços e novas funcionalidades de comunicação podem ser agrupados em duas categorias:

Telefonia: permite aos usuários estenderem as funcionalidades de seus serviços de telefonia utilizando a TV. Exemplo: vídeo telefonia e vídeo conferência.

Internet: serviços que trazem as facilidades da Internet para a tela da TV. Exemplo: navegação web via TV em portais desenvolvidos de forma específica.

Entretenimento

Na categoria de entretenimento incluem-se os serviços de jogos que variam em complexidade e sofisticação, desde os jogos mais simples – single player – até jogos mais sofisticados – multiplayer com recursos tridimensionais, também conhecidos como Massively Multiplayer Online Games (MMOG). Além dos jogos, incluem-se aqui outros serviços de entretenimento como, por exemplo, apostas ou até karaokê.

Comércio

Essa categoria inclui o comércio de bens e serviços utilizando a interface da TV, também denominado como telecommerce. Essa aplicação é similar ao conceito de e-commerce, mas possui interface adaptada para interatividade via TV. Além do serviço de comércio, se incluem aqui os serviços de propaganda interativa e direcionada.

Utilitários

Além dos serviços listados, existe uma variedade de serviços utilitários que se prestam tanto ao público corporativo quanto ao residencial. Alguns exemplos nesta categoria são: vigilância, automação residencial, e-learning, aplicações para mercados verticais específicos (ex.: setor hoteleiro).

IPTV: II - Infraestrutura de Rede

A infraestrutura de rede é constituída pelas diversas redes que suportam o serviço IPTV. Em essência, essa camada oferece o serviço IP de maneira fim-a-fim valendo-se de uma rede conhecida como multisserviços. Sua missão é oferecer conectividade de alto desempenho à camada de serviço e os principais requisitos relacionados à rede são:

Largura de banda adequada para suportar os canais de vídeo. Deve-se notar que apesar da grande necessidade de largura de banda, o tráfego é assimétrico com volume significativamente maior na direção de downstream.

Inteligência de QoS para garantir os requisitos de QoE desejados;

Arquitetura de multicast robusta para suportar a distribuição de vídeo com a otimização de recursos.

Uma arquitetura de rede típica IP multisserviço apresenta os seguintes elementos: núcleo; borda / agregação; acesso e residência.

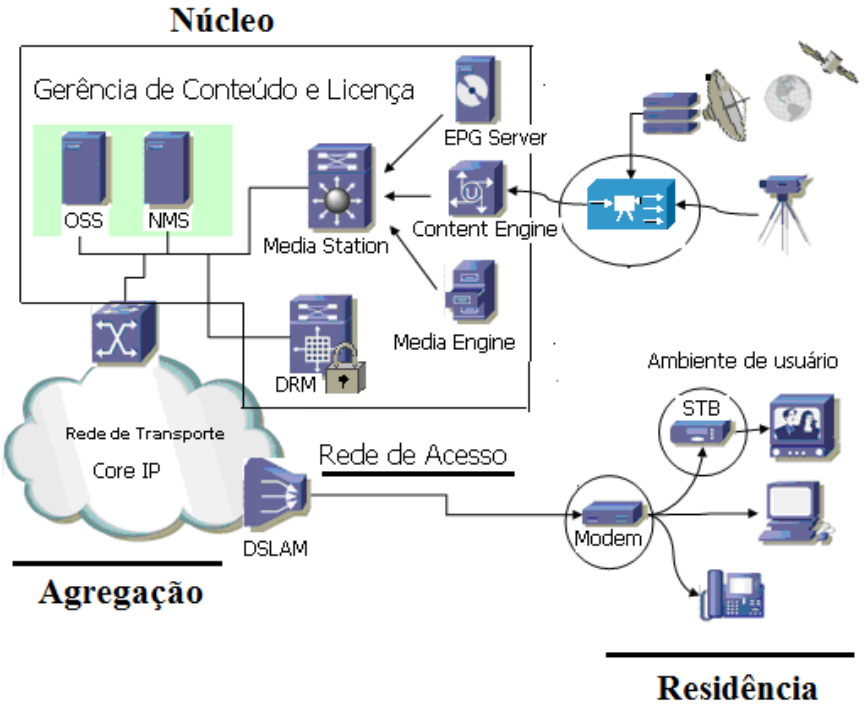

Figura 1: Modelo de referência de serviços IPTV
Fonte: (DUQUE, 2008)

Núcleo da rede IP

É responsável por transportar o elevado volume de tráfego das diversas redes de agregação, utiliza tecnologia das redes IP e a sua função, na essência, é o transporte e roteamento combinando tecnologias em duas camadas principais. IP e MPLS

Roteamento/comutação de pacotes

Utiliza a dupla Internet Protocol (IP) e *Multiprotocol Label Switching* (MPLS) . O MPLS no núcleo da rede é responsável pela criação de uma rede estável e escalável, aumenta a velocidade de transmissão e garante o desempenho da rede

Transmissão sobre redes ópticas

São utilizadas para o transporte de dados de longa distância entre os diversos PoPs de núcleo sobre fibra óptica, consegue maximizar a utilização dessas redes com a multiplexação de diversos comprimentos de ondas em uma única fibra.

Agregação

A agregação é responsável pelas camadas de roteamento, comutação e transmissão, onde ocorre o escoamento do tráfego entre o acesso e o núcleo da rede. Dessa forma essas redes são delimitadas tanto pelos roteadores da borda próximos ao núcleo quanto roteadores/switches de agregação próximos do acesso.

Acesso

Redes de acesso atendem às necessidades de largura de banda exigidas pelos serviços de vídeo, pode-se utilizar para o IPTV várias implementações de rede de acesso, tais como : xDSL, PON e GPON. A rede de acesso interliga o ambiente do prestador de serviço até o usuário. A figura 2 apresenta as várias formas de distribuição do sinal IPTV, com utilização da tecnologia de banda larga fixa.

A tecnologia xDSLque são redes adaptadas para prestação de serviços de Internet Banda Larga valendo-se da Digital tecnologia *Digital Subscrider Line* (DSL). O padrão mais difundido é o *Asymetric DSL* (ADSL2plus).

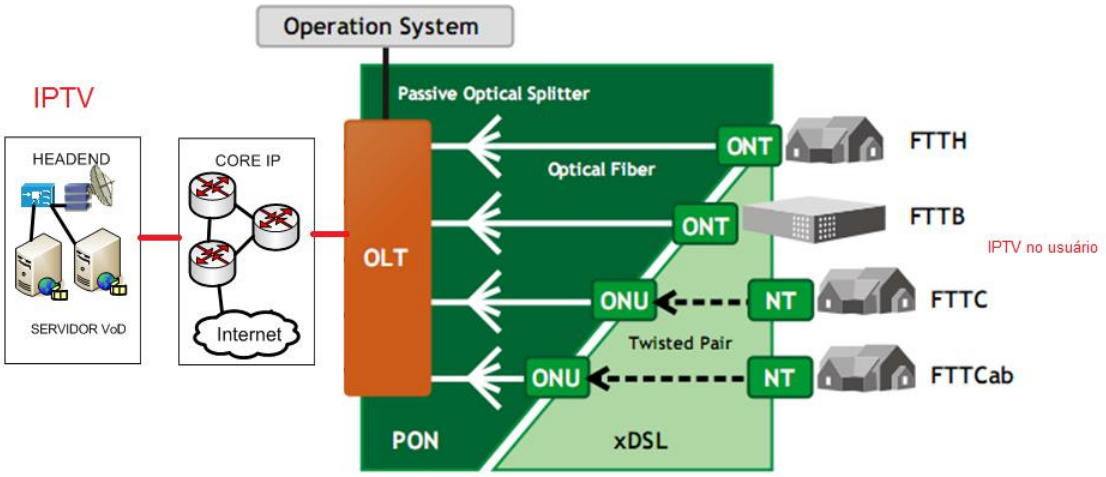

Figura 2: Rede de acesso para distribuição de IPTV
Fonte: (DUQUE, 2012)

As variantes que empregam fibra óptica incluem :

Fiber to the Cabinet (FTTCab): a fibra-óptica chega até o armário de distribuição;

Fiber to the Home / Building (FTTH / FTTB): a rede é implementada em fibra óptica em toda sua extensão.

Modalidades de implementação:

Tecnologia óptica ativa utiliza tecnologia Ethernet, enquanto que tecnologia óptica passiva não necessita de equipamentos eletrônicos ativos para transmissão.

***Passive Optical Network* (PON):**

Uilizam o conceito de compartilhamento da fibra na rede primária. Na tecnologia óptica passiva existe um nó central chamado *Optical Line Terminal* (OLT) realiza a conexão com a rede de agregação, os diversos tipos de dispositivos de assinantes, denominados *Optical Network Termination* (ONT), os *Optical Network Unit* (ONU), as redes de fibras ópticas e o conjunto de splitters que a compõe *Optical Distribution Network* (ODN).

Em geral, os termos OLT e ONT/ONU também são usados para referenciar os elementos que estão no nó de acesso e terminais de assinante para as arquiteturas também baseadas em Ethernet.

***Fiber to the Home*:**

As principais topologias de redes puramente ópticas são:

- Redes PON utilizam *splitters* passivos que dividem o sinal em direção ao assinante a uma determinada taxa de compartilhamento;
- *Ethernet* estrela ativa: implementam o conceito análogo ao da PON, substituindo os *splitters* por elementos ativos que são *switches Ethernet* e também compartilhando a fibra da rede primária;
- *Ethernet* ponto-a-ponto (P2P): implementam o conceito de rede ponto-a-ponto e não existe compartilhamento de fibra entre assinantes.

Protocolos utilizados no tráfego de IPTV

Em uma rede IPTV, os pacotes de vídeo são carregados em geral utilizando-se protocolos de tempo real, de maneira a privilegiar a característica do tráfego multimídia de fluxo contínuo. Um exemplo de protocolo utilizado em IPTV é o *Internet Group Management Protocol* (IGMP) que será analisado nos tipos de endereçamento mais a frente.

Protocolos de tempo real:

Após a codificação do vídeo utilizando, por exemplo, o padrão MPEG-2[1], os pacotes resultantes da codificação são transportados em geral utilizando *User Datagram Protocol* (UDP) sobre IP.

A razão para a utilização do UDP em detrimento do *Transmission Control Protocol* (TCP) é que ele não prevê retransmissão de pacotes perdidos, o que poderia prejudicar o sincronismo que é de fundamental importância no tráfego de vídeo.

O encapsulamento dos pacotes UDP é realizado utilizando *Real Time Protocol* (RTP) que suporta transmissão de conteúdo em tempo real, valendo-se de mecanismos de controle, para sincronizar diversos *streams*[2] com características temporais. O protocolo RTP pode vir associado de seu protocolo de controle *Real Time Control Protocol* (RTCP), que oferece funções de *feedback* de Qualidade de Serviço (QoS), sincronização, identificação de participantes e informações de controle de sessão.

Adicionalmente, no caso de serviços de *Video on Demand* (VOD), pode-se utilizar o protocolo de controle de sessão *Real Time Streaming Protocol* (RTSP) que associado ao RTP pode oferecer funcionalidades análogas ao DVD – funções como: *play, pause, rewind* para serviços baseados em *streaming*.

Tipos de endereçamento

Dependendo do tipo de tráfego, existem três tipos de endereçamento capazes de levar pacotes IP ou *frames Ethernet* de sua origem ao destino.

Unicast:

O endereçamento *unicast* é utilizado para a comunicação entre dois *hosts* e apenas uma cópia do conteúdo é envio da origem ao seu destino.

---

[1] MPEG-2 - *Moving Picture Experts Group* – evolução do MPEG-1 com a associação de imagens em movimento e áudio a uma taxa de 10 Mbps.

[2] Refere-se a fluxo de dados linha a linha até o carregamento total de um arquivo.

Quando o conteúdo transmitido no serviço IPTV é de natureza VOD, utiliza-se o endereçamento *unicast* para sua transmissão, pois o *stream* de vídeo está sendo enviado do servidor para apenas um usuário.

***Broadcast*:**

O endereçamento *broadcast* é utilizado quando um *host* deseja enviar a mesma informação simultaneamente para os outros *hosts.*

***Multicast:*:**

O endereçamento *multicast* é um caso específico do *broadcast* onde um *host* deseja enviar a mesma informação simultaneamente para um subconjunto de *hosts* conectados à rede. A transmissão dos canais de programação utiliza o endereçamento multicast, dessa forma, um stream é enviado simultaneamente para um grupo limitado de usuários que estejam assistindo o conteúdo naquele momento.

O mecanismo de *multicast* evita que exista tráfego de vídeo redundante na rede, otimizando a utilização destes recursos e baseia-se no conceito da criação grupos nos quais um usuário precisa se integrar a um determinado grupo para poder receber seu conteúdo. Quando o usuário não deseja mais receber aquele conteúdo ele deixa um grupo e se autentica a outro, passando a receber outro tipo de conteúdo como, por exemplo, outro canal de programação.

O protocolo IGMP controla desde o anúncio e manutenção dos grupos *multicast* até o registro (*join*/*leave*) dos receptores aos grupos até a sinalização do mecanismo *multicast* entre *hosts* e a rede,

Quando assinantes selecionam um mesmo canal para exibição, para evitar a duplicação desnecessária de pacotes na rede, são empregados os conceitos de árvore de distribuição *multicast*, especificando um caminho único entre a origem e o grupo de usuários que requisitaram esse conteúdo. O objetivo principal das árvores de distribuição é garantir que apenas uma cópia de cada pacote seja encaminhada em cada ramificação da árvore, sendo que as folhas são representadas pelos assinantes e a origem pela fonte de conteúdo.

IPTV: III - Infraestrutura de conteúdo

A infraestrutura de serviço caracteriza-se disponibilização dos serviços de IPTV para o cliente. Tal infraestrutura é composta por:

Sistema de Head-End

O *head-end* de video é uma das peças centrais da infraestrutura de um serviço IPTV. Seu papel é capturar conteúdo de diversas fontes seja: terrestre, *offline,* sob demanda, etc., para processar e codificar de acordo com padrões de compressão preestabelecidos (MPEG-2, MPEG-4, WM9, etc.), encapsular sobre IP e, por fim, disponibilizar para ser distribuído pela rede (DUQUE, 2008). A figura 3 abaixo represeta uma estrutura de Head-end.

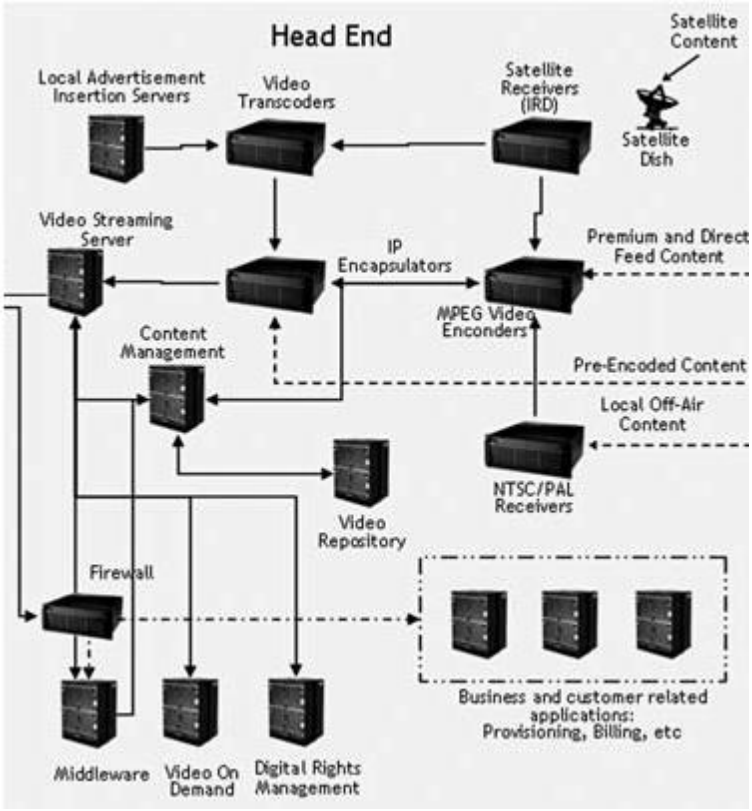

Figura 3: Headend IPTV

Fonte : (RAMIREZ, 2008)

- Elementos críticos do Head End
  Receptores Satélite
  Integrado receptor decodificador (IRD).
- Repositório Vídeo
  Isto inclui:
  • videoteca;
  • biblioteca de mídia;
  • Biblioteca de servidores;
  • rede de área de armazenamento;
  • Vídeo-on-demand banco de dados de cinema;
  • Servidor de filme (vídeo e arquivos de áudio).
- Gestão de Conteúdos
  Isto inclui:
  • centro de comando;
  • Sistema de gestão de ativos;
  • gerenciamento de direitos digitais.
- Mestre Streaming de Video / Game Server
  Isto inclui:
  • propagação de serviço;
  • serviço de streaming.
- Ingest Gateway (Video Capture)
  Isto inclui:
  • Sistema de gravação;
  • Gestor de gravação;
  • capturar / servidor de distribuição.
- Server Cache Video Streaming
  Isto inclui:
  • cache do servidor;
- ligados às empresas de Sistemas
  • Contabilidade;
  • provisionamento;
  • informações do cliente.

Os sistemas de head-end podem ser divididos em duas partes: recepção e processamento de sinais.

Sistemas de recepção:

Podem ser divididos de acordo com o meio e, em geral, incluem um elemento de captação de sinal e um elemento receptor

Recepção via satélite:

Inclui o conjunto de antenas de satélite dedicadas a capturar os sinais vindos do satélite, conversores *Low Noise Block* (LNB) e *splitters* cuja distribuição de sinal recebido estende-se até os receptores denominados de *Integrated Receivers Decoders* (IRDs).

Recepção via terrestre("*off air*"):

Abrange um conjunto de antenas VHF/UHF e *splitters* para efetivar sua distribuição até os receptores, que são os demoduladores de VHF/UHF. A recepção de canais *off air* está vinculada a conteúdos locais e regionais, podendo ocorrer tanto no SHE, quanto nos VHO.

Recepção via conexão dedicada:

Utiliza fibra óptica com a possível utilização de receptores específicos para este fim.

Processamento de sinais:

Depois de recebidos, os sinais eles são processados e codificados para serem transmitidos via *broadcast* ou armazenados (VOD). Os sinais são amplificados e distribuídos para os codificadores (*encoders*), que são os principais elementos deste bloco. Por sua vez, esses são responsáveis por codificar e comprimir o conteúdo recebido, segundo padrões de compressão definidos pela operadora.

Normalmente, o padrão de codificação definido é pelo grupo *Moving Picture Experts Group* (MPEG) da *International Standardization Organization* (ISO).

É mister esclarecer que os padrões mais utilizados são MPEG-2, MPEG-4 e, mais recentemente, o MPEG-4 *Advanced Video Coding* (MPEG-4 AVC) ou H.264 (versão padronizada pelo ITU-T) pelo fato de eles oferece melhor compressão que os demais.

O Servidor *Middleware*

Pode ser considerado como o sistema operacional da solução. Dito de outra forma,o servidor *middleware* é o componente responsável pela inteligência do serviço, além de interpor-se no âmbito da entrega do serviço fim-a-fim, sendo, por isso, responsável pela interligação das diversas partes do sistema: servidores de vídeo, *set top box*, *head-end*, DRM, elementos de rede.

Nesta mesma linha de raciocínio, pode-se dizer que o *middleware* é o viabilizador da solução de IPTV. Portanto é ele o responsável por: experiência do serviço do usuário; definições de serviços, pacotes e preços; interface com outros blocos da solução; gerenciamento de transações, conteúdo de ativos de mídia, dispositivos e assinantes.

O middleware é, portanto, um conjunto de aplicações que suportam as quatro áreas mencionadas.

Funções do middleware

Dentre as funções sustentadas pelo middleware, podemos destacar duas:

Funções para o assinante:

Eletronic Program Guide (EPG), apresentação e interatividade dos serviços (VOD, PVR, etc.); apresentação e interatividade de serviços integrados (vídeo, telefonia, identificador de chamadas, etc.); informação de programação; parental controle e informações da conta do assinante.

Funções para a operadora:

Representada por atividades como: *Application Programing Interface* (API); kit de desenvolvimento de software (SDK); gestão do serviço; gestão de clientes; gestão de transações; gestão de conteúdo e estratégia de distribuição; controle remoto dos dispositivos de usuário – *set top box*; interface com *billing*; interface com aprovisionamento/ativação; integração com sistemas de segurança e elaboração de relatórios.

O Digital Rights Management (DRM)

A segurança do conteúdo é um requisito fundamental para viabilizar a oferta de IPTV.

Os tradicionais sistemas de acesso condicional ou *Conditional Access Systems* (CAS), são projetados essencialmente para os serviços de *broadcast/pay-per-view*. Tais sistemas legados focalizam principalmente o conteúdo em trânsito, e não o conteúdo armazenado. Esses sistemas legados criptografam o conteúdo no head-end e depois decriptografam na residência do assinante, utilizando autenticação baseada geralmente em smart cards localizados no set top box (VILLEGAS, 2007).

A segurança no contexto de IPTV abrange também a proteção do conteúdo de vídeo armazenado ao longo da infraestrutura, seja nos servidores da operadora ou nas dependências do assinante. A necessidade de soluções mais abrangentes nos levam a uma nova categoria de soluções denominadas como *Digital Rights Management* (DRM).

O DRM tem como propósito, gerenciar o conteúdo digital. Ele é utilizado baseado em condições específicas definidas pelos direitos de utilização do usuário e visa garantir controle de acesso (autenticação e autorização), contabilização de utilização (gestão dos direitos de uso), controle de replicação (cópia), autenticidade da fonte, confidencialidade, integridade e disponibilidade do conteúdo protegido.

Vale registrar que são os sistemas de DRM que oferecem a infraestrutura de segurança, necessária, para prevenir a pirataria do conteúdo de vídeo independente de ele estar armazenado ou sendo transmitido.

O funcionamento do DRM é baseado na criptografia do conteúdo no *head-end* e a sua decriptografia é baseada no *set top box* utilizando certificados digitais. Nessa perspectiva, o conteúdo fica criptografado onde quer que esteja e só é decriptografado na sua exibição.

O DRM possui, ainda, inúmeros pontos de contato ao longo do sistema e, portanto, necessita de integração fim-a-fim com os diversos componentes da solução para garantir a proteção do conteúdo.

Os Servidores de Vídeo

Os servidores de vídeo são responsáveis por armazenar e disponibilizar conteúdos que são oferecidos sob demanda para os assinantes. Assim, eles armazenam, o conteúdo destinado a VOD e também o conteúdo *broadcast* selecionado para habilitar funcionalidades de PVR ao usuário final. Essa modalidade de PVR é conhecida como *Network* PVR (NPVR) em que o conteúdo não está armazenado nas dependências do usuário, mas sim nos sistemas da operadora (WEBER,2006).

Os servidores possuem, portanto, uma alta capacidade de armazenamento, bem como uma alta disponibilidade, permitindo suportar um elevado número de streams de vídeo simultâneos. Nessa conjuntura, quando se necessita de soluções mais complexas e de maior escalabilidade, os servidores possuem inteligência para formar *Content Delivery Networks* (CDNs), capazes de gerenciar a distribuição de conteúdo entre diversos

servidores colocados na rede mais próximos do assinante (por exemplo, nos VHOs e VSOs).

Vale lembrar que, as arquiteturas distribuídas de armazenamento de vídeo mantêm cópias do conteúdo mais acessado mais próximas do usuário final.

O Set top box

Componente da camada de serviço que realiza a interface entre o sistema de IPTV com o usuário e os aparelhos de exibição de conteúdo (televisores, telas de plasma, etc.).

Hospedam os componentes do *middleware*, DRM, *browser* de navegação, decodificador, possuindo, assim, capacidade de armazenamento de conteúdo local e realizando a função de um PVR.

IPTV: IV – Os Mecanismos de Criptografia

A *Internet Streaming Media Alliance* (ISMA) foi responsável pelo desenvolvimento da criptografia ISMA e sua especificação de autenticação. O padrão que abrange a criptografia e autenticação de conteúdo que é transmitido sobre protocolo Internet é independente dos players, sistemas de DRM, esquemas de gerenciamento de chaves, etc.

O algoritmo de criptografia é o de criptografia avançada (AES).

O *Ismacryp* suporta links bidirecionais criptografando o *stream*. Nesses parâmetros, os pacotes podem ser armazenados e colocados à disposição por meio de outros mecanismos.

Assim, o acesso às seções criptografadas é feito por intermédio de RTP. A partir daí, o conteúdo é criptografado na origem e pode ser armazenado ou transmitido, dependendo das necessidades específicas.

Vale salientar que, prestadores de serviços de IPTV podem tanto descriptografar o conteúdo *head-end* e proteger o conteúdo com o seu DRM próprio, ou podem adicionar uma segunda camada de criptografia. Esta abordagem é compatível com diferentes sistemas de gerenciamento de chaves (KMSs), adicionando flexibilidade à solução (RAMIREZ,2008)

É importante dizer, também, que nas DSLAMs existe um agente de retransmissão de DHCP que insere o identificador de linha física (opção 82) sobre o pedido de endereço. Tal ato legitima o fato de que as mensagens provenientes do *set top box* estão ligadas a um determinado local físico, reduzindo as chances de falsificação e fraude.

O processo de autenticação depende da opção 82 para validar os usuários, uma vez que, ao utilizar o serviço RADIUS, é possível pedir a aplicação de negócio e que tipo de acesso deve ser concedido para o assinante (ou qual o endereço de IP/VLAN).

Há também o serviço de autenticação dos *set top box*, que é transmitido pelo DSLAM e pelos roteadores até o servidor DHCP. Sua solicitação inclui informações de linha física, na opção 82 do pedido DHCP. A partir daí, o DHCP verifica com o servidor *RADIUS* ou com o servidor *middleware,* se a linha física e o assinante devem receber um endereço IP válido. Uma vez, confirmado é obtido o acesso.

DSLAMs participam do processo de *multicast* utilizando tanto *snooping* ou *proxy* para pedidos IGMP. O tráfego de IGMP será marcado para a VLAN para assegurar segregação de tráfego na rede de agregação.

Para fornecer *antispoofing* e segurança, o DSLAM irá verificar o endereço IP de origem de cada assinante cadastrado. Um mapeamento do endereço IP e sua porta física correspondente é armazenado no DSLAM. O endereço IP de origem de cada pacote irá entrar no DSLAM por meio da porta de assinante.

IPTV: V – Ameaças no ambiente de IPTV

Conforme estudo de caso realizado por Ramirez, constatou-se grande número de vulnerabilidades em uma arquitetura IPTV. O número de informações contido em uma oferta específica de serviço de IPTV pode variar, pois o serviço de diferentes prestadores terão arquiteturas de rede diferentes como o tipo de acesso à rede, xDSL, cabo, fibra. Estas vulnerabilidades encontram-se nas camadas de aplicações, serviços, e infraestrutura, conforme é ilustrado na figura 4.

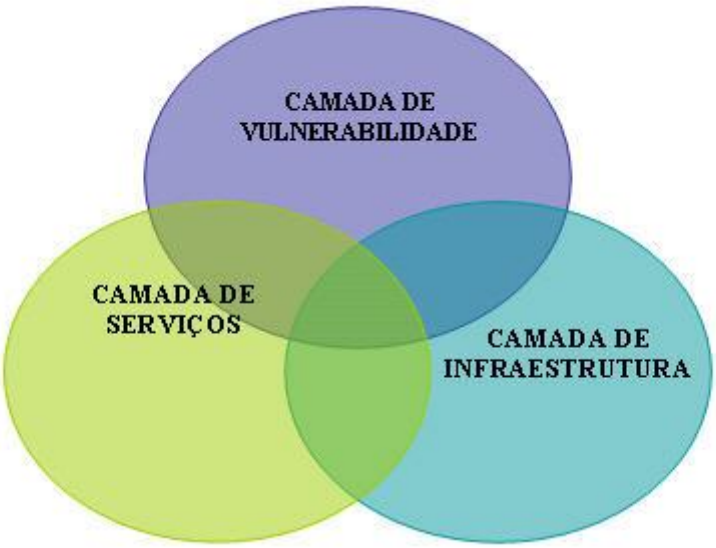

Figura 4: Pontos de ameaças em uma arquitetura IPTV

Fonte: (Adaptado de RAMIREZ, 2008)

Dentre as ameaças ao IPTV, podemos citar:

- Acesso não autorizado aos elementos do ambiente;
- Negação de serviço (DOS);
- Vulnerabilidades do sistema operacional e ataques de aplicação;
- Sistema operacional sem implementação de patches de segurança;
- Presença de aplicativos e serviços desnecessários;
- Existência de contas de usuário desnecessárias;
- Política de restrição de senha;
- Falta de arquivos de log;
- Auditoria desativada;

- Implementação de controles de acesso deficiente;
- Lista de aplicações autorizadas;
- Arquivo padrão e falta de controle de permissões de pastas.

Autenticação

O acesso a conteúdos e serviços deve ser fornecido somente para usuários autorizados. Prestadores de serviços de IPTV podem validar cada um dos set top boxes e verificar se esses elementos particulares representam assinantes autorizados ou não autorizados.

O DRM não é a única linha de defesa. Ambientes de IPTV tem na autenticação de rede e na autorização a primeira linha de defesa. Isto é feito no nível DSLAM, e a segunda linha é fornecida pelo *middleware* por meio da autenticação nesse servidor, contando com o DRM para fornecer o terceiro nível de proteção (RAMIREZ, 2008).

Detecção e Prevenção de Intrusão (IDS/IPS)

Todo sistema de segurança tem como princípio básico o monitoramento. Desse modo, todo o tráfego de dentro do ambiente de IPTV, deve ser monitorado para detectar possíveis ataques conhecidos e/ou tentativas de intrusões.

Embora *firewalls* e *Access Control Lists* (ACLs) são implantados em todo o ambiente de IPTV, a redução dos tipos de protocolos e das sessões permitidas são importantes para manter as regras sobre o IDS/IPS, responsáveis pela detecção de sessões em portas e serviços que foram bloqueados pelo *firewall*.

A partir do IDS/IPS existem diferentes sistemas críticos que devem ser protegidos. São eles:

- O repositório de vídeo que contém os ativos mais valiosos e qualquer intrusão pode causar perdas significativas para os prestadores de serviços de IPTV;
- O Servidor DRM que é responsável por disponibilizar as chaves de criptografia para todos os conteúdos. Intrusos estarão interessados em roubar as chaves ou abrir conteúdo criptografado ou, até mesmo, para falsificar comunicações para *set top boxes*;
- O Servidor de middleware, identificado como o elemento central na operação da plataforma sendo um dos primeiros alvos dos atacantes, uma vez que permite a comunicação de todos os decodificadores;
- O servidor de streaming de vídeo e VOD que, também, aceitará comunicações de set top boxes, contudo, apenas em portas limitadas. Os atacantes podem planejar enviar negação de serviço.

Como alvos secundários, com menos exposição e com acesso mais difícil por intrusos, os seguintes sistemas também poderiam ter um *host-based intrusion detection system* (HIDS). Desse modo temos:

- O Encapsulator MPEG;
- O transcoder;
- O servidor de gerenciamento de conteúdo;
- Os servidores de negócios.

Do ponto de vista da rede, os switches podem ser configurados para espelhar todo o tráfego na interface ligada ao IDS/IPS. Isto irá facilitar a detecção e contenção de ataques.

Firewalls de Rede

Devem ser utilizados para controlar o tráfego dentro do *head-end*.

O fluxo de tráfego entre os servidores dentro de uma VLAN é conhecido e, portanto, um firewall de rede ou um mecanismo equivalente, podem ser implantados para garantir que apenas os pedidos válidos serão transmitidos.

Prevenção de Fraudes

Qualquer serviço de IPTV deve ter recursos de prevenção de fraude, capazes de impedir o abuso do ambiente por assinantes ou fraudadores privilegiados.

Nesse sentido, existem elementos diferentes que podem participar na prevenção e detecção de fraudes. São, portanto:

- O *middleware* que pode relatar atividades de assinantes e detectar quando o mesmo assinante está solicitando conteúdo usando dois endereços IP separados;
- O servidor de *middleware* capaz de detectar quando um *set top box* está solicitando um número muito elevado de títulos de VOD;
- O servidor *RADIUS* que pode detectar quando o assinante está solicitando acesso a partir de dois diferentes endereços IP, sinalizando que esses tais IPs estão em DSLAMs separados. Este mecanismo pode sugerir a clonagem *set top box.*
- O DSLAM responsável por detectar quando o mesmo assinante solicita o acesso a partir de duas diferentes linhas físicas (somente se ambos estão na mesma DSLAM);
- Os servidores de negócios e o servidor *RADIUS,* que podem executar a validação de usuários, estabelecendo se existem assinantes no sistema *RADIUS* que não tenham sido criados nos servidores (de cobrança, provisionamento, etc);
- Vale lembrar que, em geral, auditorias devem ser realizadas para confirmar se todos os elementos de IPTV têm o mesmo número de assinantes e se qualquer anomalia deve ser investigada. Uma fraude interna pode ser detectada para comparar registros e encontrar novas contas que foram criadas;
- Os servidores de negócios e o servidor de *middleware* capazes de executar validações de usuários, estabelecendo se existem quaisquer assinantes de comunicação com o servidor de *middleware* que não tenham sido criados no servidor de negócios;
- É mister salientar que, servidores DSLAM podem relatar para os servidores de negócios títulos *unicast* recebidos por assinantes. Esta informação pode ser combinada com os registros de faturamento para determinar se houve manipulação do sistema.

Encapsulador IP

Uma VLAN deve ser configurada com lista de controle de acesso, filtrando a origem e o destino para permitir que o encapsulador IP receba dados a partir do MPEG e se comunique com o servidor de DRM, gestão de conteúdo e repositório de vídeo. Todo o acesso administrativo deve ser feito usando canais de comunicação seguros (como SSH,

TLS, SSL e SNMPv3), além de possuir meio de inclusão de identificação, autenticação e autorização de usuários e sistemas que têm acesso para o encapsulador IP (RAMIREZ, 2008).

Em geral a maioria dos servidores dentro do *head-end* são protegidos por seis camadas de segurança, formadas principalmente por mecanismos independentes. É essa estrutura que aumentam os controles e reduzem as chances de fraude.

A primeira camada, mais externa, é formada pelos *firewalls* e IDS/IPS. Estes proporcionarão os controles de acesso entre as funções principais e de intercâmbio, bem como proteção contra ataques conhecidos, tais como vírus e *worms.*

A segunda camada compreende a VLAN estabelecida nos *switches,* que permitem somente *hosts* pré-aprovados para ingressar na rede. Desse modo, os servidores terão uma placa de rede destinada para a VLAN administrativa e placas de rede para várias outras VLAN's de acordo com as necessidades essenciais de comunicação. Assim, o acesso à VLAN é controlado no endereço MAC da placa de rede ou no endereço IP da máquina.

A terceira camada é formada pela lista de controle de acesso no comutador. Na maioria dos casos, a comunicação será iniciada por um *host* e aceita pelo *host* de destino. Por exemplo: o servidor de encapsulamento IP, não será capaz de enviar pacotes para o *Simple Mail Transfer Protocol* (SMTP) da porta do servidor de gerenciamento de conteúdo. Nesta perspectiva, os consoles administrativos terão acesso mais flexível com os servidores, mas será validado pelo *firewall*.

A quarta camada é formada pela encapsulação fornecida dos protocolos seguros. Dito de outra forma é basicamente um túnel estabelecido entre *hosts* usando SSL, TLS, SSH, SNMPv3 ou canais de comunicação seguros que vão proteger a sessão de interceptação e modificação, bem como reduzir as chances de um ataque *man-in-the-middle*.

A quinta camada é constituída por os mecanismos de segurança específicos executados pelo software fornecedor que criou a aplicação em particular. Na maioria dos casos, as aplicações irão solicitar credenciais antes de permitir acesso como usuário ou administrador e atribuirão diferentes perfis de usuários.

A sexta camada é constituída pelo *hardening* da plataforma, o que inclui os patches e configurações do sistema operacional, seguindo as recomendações do fabricante.

Diante disso, por esta abordagem em camadas, torna-se muito difícil tomar o controle de elementos dentro do *head end*.

O Firewall de Aplicação Web

Os blocos de firewall de aplicação web de acesso a todas as páginas não autorizadas estão dentro do sítio do servidor do DRM e bloqueiam também as solicitações que não estejam em conformidade com os valores pré-aprovados ou estruturados. Nesse sentido, respostas serão também pré-validadas e qualquer resposta anormal será bloqueada.

Um exemplo: seriam intrusos enviando um ataque de injeção SQL contra o servidor. Esta seria uma solicitação usando personagens que não fazem parte da estrutura pré-aprovado. O firewall de aplicação web irá bloquear o pedido e nenhum pacote será encaminhado para o servidor DRM. Mesmo que um ataque passe a resposta de uma injeção SQL, não estaria em conformidade com a resposta do DRM padrão, e, portanto, seria bloqueada (DUQUE, 2012).

O DRM vai ter uma placa de rede dedicada para se comunicar com o firewall de aplicação web *firewall*, permitindo que as seis camadas de proteção sejam aplicadas.

O Servidor Streaming de vídeo

O servidor de *streaming* de vídeo recebe o conteúdo criptografado a partir de qualquer repositório ou o vídeo diretamente do DRM de forma criptografada. Uma VLAN dedicada pode ser configurada para estes elementos se comunicarem. Com esta abordagem, a VLAN irá proporcionar um ambiente seguro onde apenas os sistemas esperados estarão trocando informações.

É importante, pois, seguir as seguintes recomendações:

- Desativar FTP anônimo log-ins;
- SFTP (ou seja, FTP seguro) deve ser usado em vez de FTP;
- Configurar ACLs nas interfaces do firewall para bloquear pacotes SFTP provenientes de interfaces ou com endereços IP desconhecidos.

O IGMPv2/v3

O tráfego *multicast* proveniente do *head-end* encapsulados no interior de VLANs deve ser protegido contra modificação não autorizada. Uma alternativa, é o uso de um cabeçalho de autenticação IPsec. Após sua implantação a IPSec fornecerá autenticação e proteção de integridade.

O IPSec *authentication header* (AH) é usado para fornecer integridade sem conexão e autenticação de origem dos pacotes, reduzindo a exposição a ataques de repetição. Ainda, o IPsec AH podem ser usados em conjunto com IP *encapsulating security payload* (ESP) fornecendo proteção do *payload*.

Os *firewalls* podem ser configurados para bloquear qualquer tráfego que não é IGMPv2/v3 proveniente de endereços de transmissão autorizados. Para evitar ataques DOS, recomenda-se que IGMPv3 seja utilizado. Todos os gateways residenciais e set top boxes que recebem pacotes IGMP devem ser verificados e descartados, se o endereço MAC Ethernet não é um endereço *multicast* válido.

O RTP

Para reduzir a exposição aos pacotes falsos ou modificados do *real time protocol* (RTP),o *secure real-time transport protocol* (SRTP), deve ser usado no lugar do protocolo RTP, uma vez que fornece proteção de integridade e autenticação na forma de um HMAC-SHA-1, para os pacotes RTP e RTCP(GILBERT, 2007).

A especificação do *secure real-time transport protocol* (SRTP) fornece confidencialidade através de criptografia de autenticação de mensagens e proteção *replay* para RTP e RTCP.

Recomenda-se, portanto, que ACLs sejam configuradas em interfaces de *firewall* para bloquear pacotes RTP/SRTP originários de interfaces impróprios ou com endereços IP impróprias *fonte*. Além disso, para evitar a possibilidade de captura de pacotes RTP em trânsito, o SRTP deve ser usado, uma vez que fornece a criptografia na forma de AES para pacotes RTP e RTCP.

Os Pacotes RTSP

Para evitar ataques por meio de pacotes não autorizados de RTSP, adota-se a autenticação RTSP (*shared secret*) ou autenticação Digest (MD5) habilitada em servidores VOD e interfaces STB. Além disso, é importante proteger os pacotes RTSP com Ismacryp (i.e. ISMA 1.1).

O *Ismacryp* usa SRTP para fornecer tráfego com autenticação, integridade e criptografia. Para uma proteção adicional contra o acesso não autorizado DOS é importante configurar ACLs nas interfaces de firewall para bloquear mensagens RTSP transportando pacotes RTSP originários de interfaces desconhecidas ou com endereços IP de origem duvidosa.

IPTV : VI – Conclusão

Sendo o conceito de *Internet Protocol Television* (IPTV), uma das mais recentes tecnologias de distribuição de conteúdo, podemos observar que, por mais sofisticada e moderna que esta área seja, há, ainda, muita coisa a ser descoberta.

Por ser uma área em ritmo acelerado de desenvolvimento, a tecnologia de um modo geral, oferece um vasto campo para pesquisas, além de um rico e farto acervo, para legitimar os diversos trabalhos que surgem a todo o momento.

Não obstante o arcabouço teórico existente no mercado para embasamento de pesquisas, observamos, por meio deste trabalho, que a área de segurança de redes é, ainda, completamente deficitária, no que tange a conceitos que legitimem os trabalhos acadêmicos referentes aos diversos meios de segurança de redes.

Diante de todas essas perspectivas, consideramos este tutorial um pequeno item de cunho esclarecedor para alguns conceitos concernentes à segurança de redes. Nesse certame, temos consciência de que o tema: segurança de redes para IPTV é um campo em grande expansão. Por ser assim, o serviço IPTV, que permite o uso de uma rede banda larga para entregar conteúdo de TV, com garantia de qualidade de serviço e, potencialmente, acrescido de serviços interativos, só pode ser legitimado, mediante a um bom sistema de segurança de redes.

Bibliografia

DUQUE, Luciano Henrique. Avaliação de Qualidade de Vídeo em Redes IPTV com Acesso Baseado em ADSL, Dissertação de Mestrado- Universidade de Brasília, 2008.

DUQUE, Luciano Henrique. Apostila: Segurança em Redes IPTV, LANCORE NETWORK, 2012.

RAMIREZ, David. IPTV Security Protecting High-Value Digital Contents, Editor: John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, 2008.

RESOLUÇÃO 578, ANATEL 2012.

GILBERT HELT, Understanding-IPTV-Informa-Telecoms-Media, Auerbach Publications

Taylor & Francis Group, 2007.

VILLEGAS, A. *DRM Convergence Analysis of Products and Standards*. Alcatel-Lucent, 2007.

WEBER, J., Newberry, T., “IPTV Crash Course”, McGraw –Hill, Chicago San Francisco, jun. 2006.