S3P

Gestão de Segurança em Cenários *Triple-Play*

Título:	**Versão:**
Análise de Vulnerabilidades em Ambientes *Triple-Play*	1.0

Data de Entrega: 2008-05-02	**Segurança:** Acesso Público

Autores:
Henrique Wallenstein, Thiago Leite

Resumo:

Ambiente do Provedor: Atender as necessidades do projecto de Segurança em Redes *Triple-Play* como um dos trabalhos iniciais. Será realizada a análise das vulnerabilidades da infra-estrutura envolvida no sistema sob a óptica do provedor de serviços. Obter resultados sobre a análise é importante para sustentação do projecto, que irá propor uma nova solução de segurança ao ambiente. Faz-se uma breve explicação do cenário anterior ao surgimento das redes *TriplePlay*, o mercado que resultou com o seu surgimento e os requisitos de segurança, analisando **vulnerabilidade**s, a topologia de exemplo que implementa parte das tecnologias hoje existentes e aqueles que possuem características *Triple-Play*.

Ambiente Home Security: Faz-se o levantamento de actuais riscos de segurança, na perspectiva do cliente, das redes domésticas, seguindo-se soluções fornecidas pelos operadores. A rede doméstica inclui LAN, VoIP e VoIP, focando as implicações de serviços *Triple Play* (*layout*, administração, segurança, privacidade, etc). Finalizam-se as diversas abordagens com propostas de sistemas de segurança para rede doméstica.

Palavras-chave:

DoS, QoS, Vulnerabilidade, Segurança, Privacidade, Controlo Parental, LAN doméstica, *Wi-Fi*, WMI, UPnP, DPWS, ISP, VoIP, H.323, SIP, SPIT, SEAL, *Lawful Interception*, IPTV, *Triple-Play*, Análise, Provedor, Internet.

Revisões

Análise de Vulnerabilidades na Rede dos Subscritores de Serviços *Triple-Play*

Revisão	Data	Descrição	Autores
v0.3	2008-04-8	- Criação do documento; - Abordagem da maioria dos riscos de segurança e algumas soluções.	Henrique de Oliveira Wallenstein
v0.5	2008-04-14	- Revisão de texto e maior associação ao serviço *Triple-Play* como solução a certas questões de segurança; - Correcção e aprofundamento de alguns conteúdos encontrados em inglês (*tutorial* de *firewall, email,* etc.); - Introdução de tabelas.	Henrique de Oliveira Wallenstein
v0.8	2008-04-17	- Adicionado comentário sobre a facilidade com que os utilizadores entregam a sua palavra-chave (novo artigo); - Segurança Remota: estudo sobre WMI; - Complemento sobre a implementação de Escuta Telefónica (*Law Interception, LI*) nos sistemas VoIP. Incluem-se novas figuras.	Henrique de Oliveira Wallenstein
v0.9	2008-04-19	- Introdução completada; - *Universal PnP* adicionado; - Revisão de texto no capítulo de IPTV e comentários à sua aproximação com o controlo de segurança nos outros serviços; - Criação de índice, lista de tabelas e figuras.	Henrique de Oliveira Wallenstein
V0.9b	2008-04-23	- Adicionado o tópico sobre "Controlo Parental"; - Adicionada uma conclusão para sintese das necessidades numa rede *Triple-Play*;	Henrique de Oliveira Wallenstein

Análise de Vulnerabilidades em Provedores de Serviços *TriplePlay*

Revisão	Data	Descrição	Autores
v0.5	2008-04-07	Criação do documento e primeira versão padronizada	Thiago Leite (DEI)
v0.6	2008-04-10	Aperfeiçoamento dos requisitos de segurança no provedor e adição do rascunho dos últimos capítulos.	Thiago Leite (DEI)
v0.7	2008-04-12	Complemento dos últimos capítulos e formatação da bibliografia.	Thiago Leite (DEI)
v0.8	2008-04-13	Complemento dos últimos capítulos e aperfeiçoamento dos requisitos de segurança no provedor.	Thiago Leite (DEI)
v0.8.1	2008-04-20	Correção nos requisitos de segurança no provedor (bancos de dados, resolução de nomes, serviço web).	Thiago Leite (DEI)
v0.8.2	2008-04-23	Adicionado requisitos de segurança no provedor (virtualização e sistema operativo) e finalização dos últimos capítulos.	Thiago Leite (DEI)
v0.9	2008-04-25	Finalizada versão preliminar do documento.	Thiago Leite (DEI)

Índice

Lista de Figuras

Lista de Tabelas

1. INTRODUCÃO

As principais conquistas tecnológicas do século XX surgiram na possibilidade das áreas de processamento e distribuição da informação, através de meios distintos. Esta distribuição foi possível graças ao desenvolvimento e popularização de tecnologias como o telefone, possibilitando as pessoas de se manterem em contacto umas as outras, mesmo em grandes distâncias. Depois, outros inventos como o rádio e, mais tarde, a televisão, fizeram nascer o fenómeno de multimédia em massa, já que o acesso tocava a milhões de pessoas simultaneamente, graças ao enorme sucesso que fez. Por último, e não menos importante, a Internet surgiu como um meio de agregar todas as informações numa grande rede de dados internacional, onde qualquer tipo de informação está disponível a qualquer um que tenha acesso em algum ponto da rede. A Internet, por sua vez, tornou possível inclusive que outros serviços de comunicações fossem agrupados sob o mesmo ambiente.

Com o resultado do rápido progresso tecnológico, a convergência destas áreas era uma questão de tempo para se tornar realidade. As diferenças entre estes meios de comunicação estão cada vez menores, e actualmente já é possível, numa residência, possuir acesso aos três mundos de telefone, televisão e Internet, através dos serviços das redes *TriplePlay*.

TriplePlay é um termo de marketing criado para definir provedores de serviço que oferecem, sob um mesmo canal de comunicação, os serviços de telefone, televisão e acesso à Internet em alta velocidade. É um modelo combinado de negócio que surgiu de maneira a atender as necessidades por um padrão comum de comunicação.

Do ponto de vista do cliente, as arquitecturas "*Home Broadband"* estão sobre uma variedade de ameaças que, comparando com uma ligação *dial-up*, são mais fáceis de explorar utilizando as actuais ligações *"allways on"* de banda larga xDSL ou cabo. A curta duração das ligações *dial-up* dificultava os atacantes na tarefa de comprometer os serviços correntes na rede fornecida pelo seu ISP e respectivos clientes. Tendo sido esta barreira ultrapassada, diversas organizações viram-se obrigadas a tomar medidas na fortificação das ruas redes, nomeadamente em *routers*, *gateways*, servidores e outros *hosts*. Contudo, tanto os utilizadores comuns (clientes ISP) como trabalhadores em telecomutação (acedem à rede interna da empresa através de VPN, partindo de sua casa), devem tomar diversas medidas de segurança na sua LAN doméstica.

Se um cliente possui uma rede LAN em casa e esta possui internet de banda larga, devem ser instalados e configurados dispositivos (hardware) *firewall* ou, como na maioria dos casos, em *software*. O uso de ambos facilitará a monitorização de um possível ataque, através de uma mais completa auditoria, mais importante para empresas com utilizadores em telecomutação. Outras importantes medidas que devem ser tomadas nos *hosts*, nomeadamente nos *WebBrowsers* que possuem: O código activo, processado do lado cliente, é o maior responsável pelas consecutivas *patches* e novas versões de *WebBrowsers*. Desactivar este código poderá oferecer uma maior segurança ao utilizador, limitando as vulnerabilidades de intrusão. No entanto, perder-se-á alguma qualidade em muitos *websites* que utilizam código activo. Também os *Cookies* devem ser removidos: Existe *software* de terceiros que analisam potenciais vulnerabilidades associadas aos *Cookies*, como palavras-passe não encriptadas e registadas no disco local, além de monitorizarem os hábitos dos utilizadores.

Os sistemas operativos, como Windows, Linux, FreeBSD, etc., oferecem diversas opções de segurança (SELinux, Windows *User Account Control*, etc.) que devem estar activadas e configuradas pelo seu utilizador ou responsável pela máquina. As configurações *standard* utilizadas são geralmente inadequadas à segurança desejada na maioria das empresas. Na visão de um utilizador comum, a existência destes sistemas acaba por contrariar as necessidades do primeiro, seja por desconhecimento da sua existência ou por dificuldades de configuração. Em muitos casos,

os ISPs não podem ajudar os seus clientes, na medida que o serviço teria de ser local, deslocando demasiados recursos humanos especializados para esta finalidade. Poderão os ISP utilizar ferramentas como o *nmap* para informar os seus clientes de possíveis *patches* e outras actualizações secundárias? Deverão fazer propaganda de software livre de *anti-spyware*, *anti-adware*, etc., e detectáveis por *nmap* para posterior análise? Pelo menos a actualização do sistema operativo e respectivas aplicações – factor crítico para a segurança do utilizador – estão, por defeito, em *schedule* automático.

Quando utilizando redes *wireless*, mais concretamente a 802.11, o utilizador comum não olha às configurações do seu *router* ou *access point*, ficando, por exemplo, a palavra-passe de acesso à configuração com o valor de fábrica, facilmente obtido nos manuais disponibilizados na Internet. Também o SSID da rede fica em *broadcast* com o nome padrão, facilitando ao atacante descobrir alvos fáceis. Estes e outros dados devem ser tomados em atenção para a garantir a segurança e *QoS* do cliente. Nos *routers,* devem-se definir o *range* de IPs possíveis, associá-los ao MAC-Address das suas placas *Ethernet* (ou outrem, quando usando *Gateways*), desactivar o DHCP, etc. Numa empresa, estas configurações são geralmente postas em prática, mas para um utilizador cliente de um ISP e com uma rede LAN doméstica, terá, na maioria dos casos, valores de fábrica, não ter qualquer encriptação *wireless* e os IPs serem oferecidos por DHCP sem limitação do seu *range* nem qualquer associação de MAC-Address. Uma posterior configuração da *firewall* pode tornar-se inconveniente ao cliente, podendo existir algum interesse na área de *Parental Control* (portos abertos/fechados a crianças que utilizem a internet para, por exemplo, partilha de ficheiros P2P ou jogos *on-line*).

À rede IP doméstica, pretende-se integrar múltiplos serviços:

- A integração de dispositivos na rede IP, sob a tecnologia *UPnP*, estão comprometidos pela sua falta de autenticação, sendo o seu futuro talvez assegurado pela tecnologia DPWS;

- A tecnologia VoIP vem em substituição da rede telefónica pela estrutura IP existente: É verdade que este meio já se provou ser barato e eficiente, e sendo assim, a sua maior vantagem será também a sua desvantagem, quando bombardeado por publicidade não solicitada. A encriptação pode ser a resposta para a integração de voz no ambiente de pacotes de dados, tantas vezes escutados por terceiros não autorizados. No entanto, é preciso garantir os serviços de escuta telefónica que a lei do país requer, tornando-se a implementação mais rígida;

- O uso da televisão na rede IP: IPTV, poderá ser muito agradável e fornecer diversos serviços de "cinema em casa" com a melhor das qualidades HD (até 15Mbit/s). É necessário aplicar-se algoritmos para detectar a origem de cópias piratas e garantir o não repúdio de quem o copiou (*Virtual Smartcards*, *Watermarks*, etc). Também a IPTV será extremamente vantajosa para integrar o cliente no controlo do seu ambiente de segurança: Da mesma forma que poderá receber avisos de uma chamada telefónica na televisão, poderá igualmente aceitar endereços MAC de visitantes autorizados ou rejeitar terceiros desconhecidos.

Em todos os casos onde se aplique a segurança do cliente, ter-se-á de planear a privacidade, qualidade de serviço e, para clientes domésticos sem telecomutação, liberdade de uso e controlo alargado. Analisar o surgimento das redes *TriplePlay* e as necessidades que a fizeram surgir pode ser um dos primeiros passos para percepção do ambiente e das vulnerabilidades que este pode estar inerentemente sujeito.

2. REDES TRIPLEPLAY

2.1. Surgimento

Apesar de o *TriplePlay* ser um novo termo, as maiores operadoras de televisão, presentes nalguns poucos países, já disponibilizam um serviço com as mesmas características base de IPTV há vários anos, como *VideoOnDemand*, distinguindo-se pela rede DVB. Apenas estas empresas, juntamente com as grandes entidades na área de telefonia fixa, móvel e outras do mercado de comunicações, discutem os possíveis caminhos a aplicar no serviço *TriplePlay*, pois existe uma forte inércia à participação de outras empresas, de menor porte, à oferta deste novo serviço, devido a distintos riscos comerciais.
A tabela abaixo demonstra, de maneira simples, como era a distribuição dos diferentes serviços oferecidos pelas companhias. [X]

Tabela 1 - Serviços Diferenciados

	Voz	**Dados**	**Vídeo**
Operadoras de telefonia fixa	Sim	Sim	Não
Operadoras de telefonia móvel	Sim	Não	Não
Operadoras de televisão por assinatura	Não	Não	Sim
Provedoras de acesso à Internet	Não	Sim	Não

A possibilidade de integração de todos estes serviços através de um único canal de comunicação, só é possível graças ao advento de um protocolo universalmente aceite: O *Internet Protocol* (IP), aliado à capacidade de prover qualidade aos serviços oferecidos (*Quality of Service* – QoS). Outra razão para o aproveitamento do canal para uso de diferentes tecnologias foi o avanço obtido no aumento da largura de banda, que garantiu o acesso às plataformas de telefonia e vídeo por pacotes. O advento de tecnologias de baixo custo, como a ADSL, representa uma evolução no desempenho para acesso à Internet, com ligações que suportam a largura de banda necessária para a transmissão, em simultâneo, de diferentes pacotes multimédia.

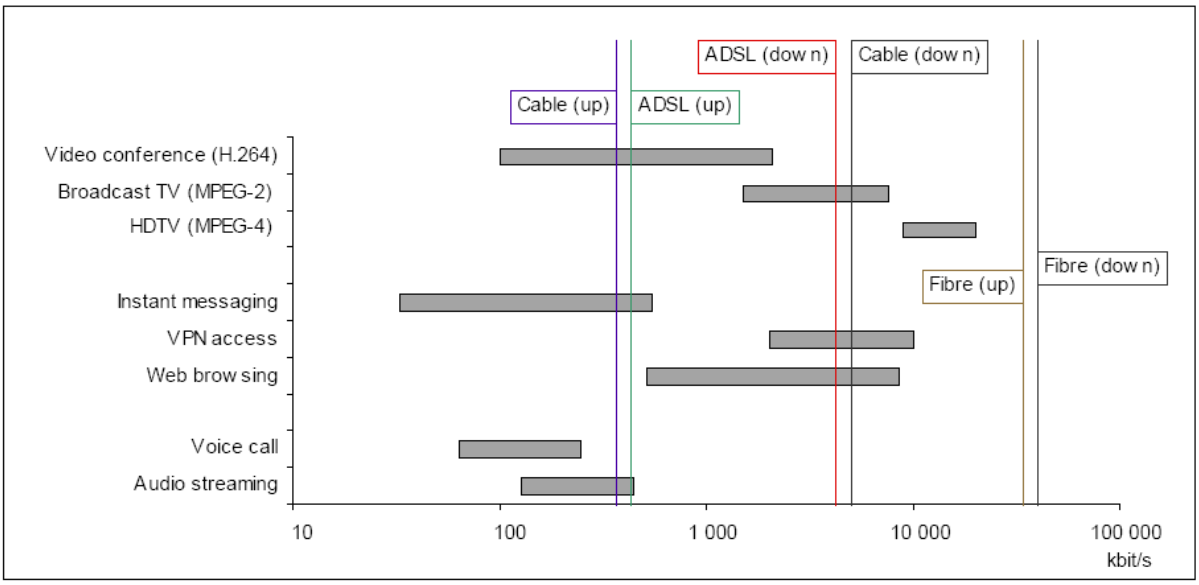


Fig. 1 - Tecnologias e velocidades de acesso necessária.
[in http://www.oecd.org/dataoecd/47/32/36546318.pdf]

2. PROVEDOR DE ACESSO À INTERNET

O Provedor de Acesso à Internet (*Internet Service Provider* – ISP) é o termo adequado para se referir as empresas que possuem a infra-estrutura necessária para ligar os seus clientes (indivíduos e empresas independentes) à Internet. Os requisitos de segurança necessários a um ISP estão separados nas seguintes categorias:

- Canais de Comunicação;
- Compartilhar Informações;
- Infra-estrutura de Rede;
- Infra-estrutura dos Sistemas.

2.2. Canais de Comunicação

Os canais de comunicação, estabelecidos pelos ISP, têm fundamental importância para os seus clientes, já que este o é o meio/serviço por onde ISP obtém proventos. Estes mesmos canais estão sujeitos a ameaças de diversas naturezas, seja por mal utilização dos serviços oferecidos pelos provedores ou por atacantes externos.

2.2.1. Nível de Serviço

Quando é realizada a contratação de um provedor de serviços, considera-se a disponibilidade de um canal durante o maior período de tempo possível, seja para manter os clientes satisfeitos ou simplesmente para cumprir cláusulas que foram anteriormente estabelecidas em acordos de nível de serviço (*Service Level Agreement* – SLA).

Todo o conteúdo que é transmitido aos clientes é transportado através das ligações que o ISP estabelece, isto é, o provedor é responsável pela criação de um canal que garanta a comunicação entre os diversos pontos.

Apesar de o ISP não ser o responsável pelo conteúdo que é transmitido, oferecer grande largura de banda aos clientes sem realizar distinção entre os tipos de fluxos existentes pode tornar impraticável a oferta de grande débito. A diferenciação do tráfego, por parte dos provedores de serviço, é chamada *Traffic Shaping* ou *Packet Shaping,* e tem um propósito louvável. Em certos momentos, chegam a ser utilizados de maneira até abusiva, desestimulantes ao uso de protocolos que requerem grande tráfego (como *P2P*). Porém, mesmo com tais imposições e a crescente dificuldade dos provedores em fornecer a largura de banda que vendem, o volume de dados na estrutura do ISP tem aumentado exponencialmente, aumentando as possibilidades de ataque ao ISP ou usá-lo como meio para a realização de ataques baseados em quantidade de tráfego.

2.2.2. Rede de Anonimato

Numa busca pela privacidade, é possível o uso da rede do ISP (pelos clientes) para a realização de actos ilegais em outras redes. Pode até ocorrer num cliente de forma involuntária, através de redes anónimas. Como exemplo, apresenta-se o TOR (*The Onion Router*), onde o tráfego da rede anónima utiliza vários pontos intermediários até ao destino, incluindo o ISP ao fluxo de dados que não tem origem nem destino na própria rede.

Os utilizadores da rede TOR tornam suas próprias máquinas em *proxies* da rede TOR. Uma vez dentro desta rede, o tráfego é enviado já encriptado pelas chaves públicas de cada intermediário que irá passar. Quando chega ao destino, os pacotes são desencriptados pela ordem de *hoppings* e as suas chaves. Desta maneira, o tráfego é recebido no destino como se tivesse sido enviado directamente pelo nó de origem e sem intermediários

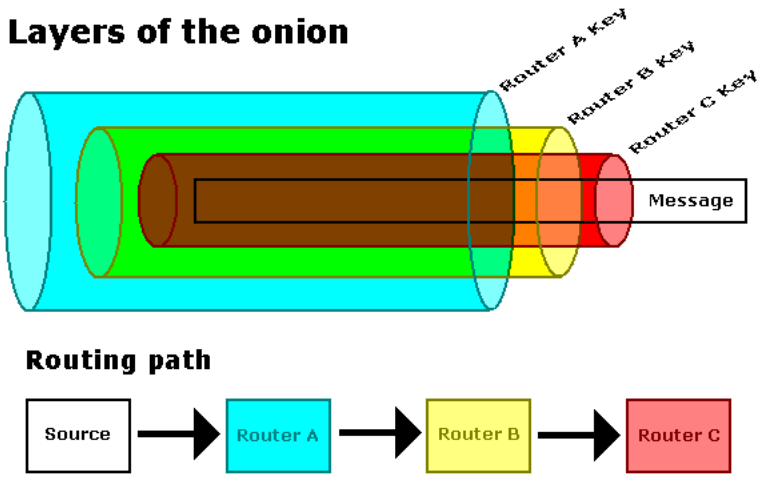


Fig. 2 - Representação do tráfego TOR.
[in http://en.wikipedia.org/wiki/Onion_routing]

A rede TOR é independente da aplicação, já que utiliza fluxos ao nível do TCP. À aplicações utilizando esta tecnologia TOR, como o IRC e outros tipos de IM ou *email* instantâneo. Normalmente, quando realizando o acesso à Web, o TOR é utilizado juntamente com o *software* "*Privoxy*" (de *private proxy*), que realiza uma filtragem ao servidor *proxy*, de maneira a adicionar uma camada extra de privacidade.

Nem todos os nós com TOR são iguais: Podem, por exemplo, auto-descrever-se e mostrar o seu *status*, de maneira a facilitar e melhorar a qualidade do caminho que os dados irão seguir, evitando nós sobrecarregados ou outros problemas. Para iniciar a transmissão, o TOR necessita entrar em contacto com os servidores de autoridade. Esses servidores fornecem uma lista dos nós existentes para que o cliente possa escolher, de maneira aleatória, o caminho para envio do fluxo de dados. O mesmo deve ser feito por todos os nós no caminho até o destino.

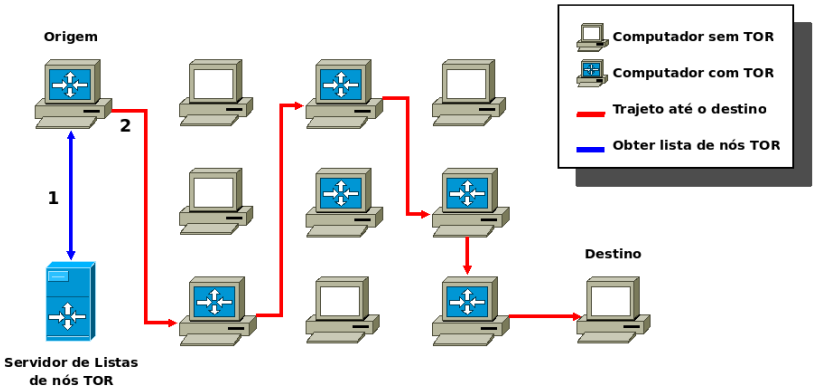


Fig. 3 - Rede TOR

O perigo do uso de redes TOR, do ponto de vista do provedor, surge no momento em que elas são utilizadas para ataques, sendo o provedor utilizado como intermediário para, como comentado anteriormente, o envio de dados ou estabelecimento de ligações entre pontos independentes da sua rede. Isto é, os ataques poderão ser realizados como se algum cliente do provedor fosse o real atacante, sem que o mesmo saiba do que está ocorrendo. A figura abaixo demonstra uma situação fictícia onde um determinado nó, usando TOR, realiza um ataque a um cliente fazendo com que a última origem dos dados seja de um computador noutro ISP, o que pode gerar problemas no momento de se apurar os culpados.

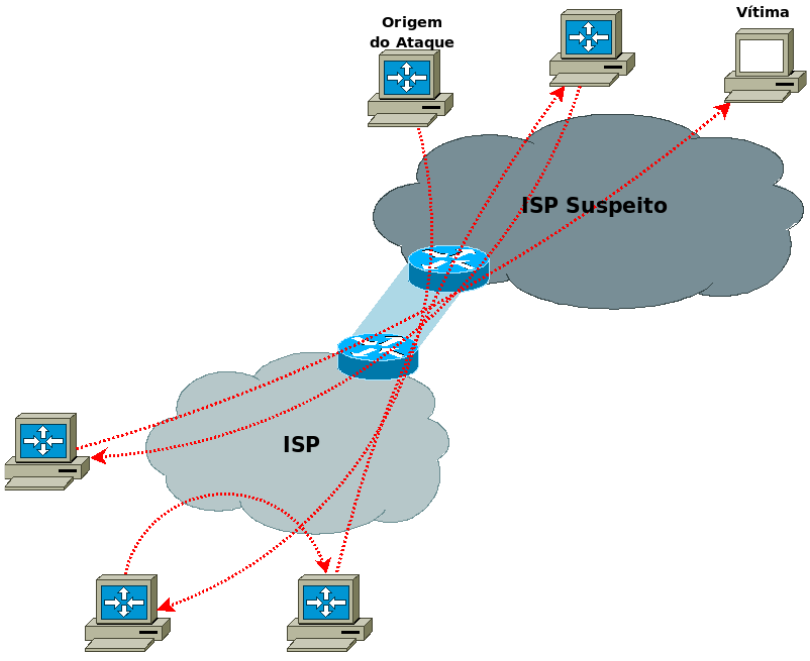


Fig. 4 - Ataque utilizando uma rede TOR

Apesar do tráfego gerado pelos clientes ser de interesse do próprio, os provedores devem possuir uma política de uso apropriado dos canais de comunicação (*Appropriate Use Policy* – AUP). Neste capítulo, tenta-se dar alguma orientação no tipo de fluxos permitidos no meio de comunicação fornecido pelo ISP e como poderá actuar contra possíveis infracções. A UAP deverá ser clara o suficiente para evitar ambiguidades e distorções. Um exemplo de restrição que pode ser imposta pelo UAP é a proibição de tráfego P2P, realização de *IP Spoofing* ou, por exemplo, o próprio ISP impor listas negras contra servidores de autoridade TOR.

2.3. Compartilhamento de Informações

Um provedor de serviços deve possuir um vasto número de procedimentos, criados de maneira a prover a disseminação do conhecimento e informação entre os membros internos e clientes. Todos os documentos devem ser colocados num meio de compartilha de informações, sendo que as mais importantes são as políticas de segurança e, mais especificamente, o comportamento e procedimentos de resposta a um possível ataque.

Independentemente do ambiente analisado, os principais itens a serem verificados são as políticas e procedimentos de segurança. Como qualquer documento desta categoria, tem de ser claro e objectivo, prevendo, inclusive, como será a sua disseminação durante e após um ataque.

2.3.1. Política de Segurança

As decisões sobre a segurança do ambiente devem estar registadas no documento intitulado de política de segurança [7], claro e objectivo, determinando quão segura ou insegura é a sua rede, quantas e quais as funcionalidades oferecidas e a facilidade de uso. É necessário determinar quais serão as metas de segurança e os seus objectivos devem ser definidos a partir dos seguintes pontos:

- **Serviços oferecidos e segurança fornecida**: Cada serviço oferecido acarreta os seus próprios riscos de segurança. Dependendo do ambiente do cliente, os benefícios de um determinado serviço podem não superar o risco associado. O administrador deverá optar por eliminar o serviço ao invés de tentar torná-lo mais seguro. Quanto mais serviços o provedor oferecer, maiores os riscos envolvidos (Imagine-se um provedor de *Triple-Play*!).
- **Facilidade de uso e segurança**: Por consequência, quanto maior a facilidade de uso, menor a segurança envolvida. Mecanismos de prevenção contra delitos irão sempre impor restrições ou limitações que devem, ou não, ser necessárias.
- **Custo da segurança e risco de perda**: Metrificar os riscos envolvidos na segurança vão além dos valores monetários: O custo pode ser através da performance inferiorizada, a perda da facilidade de uso, perda de privacidade, perda de dados e serviços, etc. O custo de perdas deve ser comparado ao custo para evitá-las.

Para a elaboração de políticas de uso, é necessário que todos os grupos, com representação no provedor, estejam presentes, já que as decisões na política estabelecida afectarão todo o modelo de negócio do ISP.

- Administração de segurança do provedor.
- Administração dos recursos computacionais.
- Representantes dos grupos de utilizadores, como o responsável por vendas e relacionamento com os clientes.
- Equipe de resposta a ataques.
- Conselho legal.

A participação e consenso de todos é importante já que a política aplicada será como linha de orientação às acções do provedor quando prestando os serviços.

2.3.2. Resposta a Ataques

O ambiente de partilha de informações possibilita aos clientes questionarem o provedor sobre o seu acesso aos serviços a que estão inscritos ou queira obter. No último caso, a requisição pode ter origem no próprio cliente ou através de autoridades públicas ou equipas de resposta a ataques (*Computer Security Incident Response Teams* – CSIRT) aquando de indícios de incidentes dentro da rede do ISP.

Os provedores de serviços também deverão ser proactivos, notificando os seus clientes sobre problemas de segurança nas suas redes, quando estes forem detectados. Os ISPs costumam impor aos utilizadores – através dos seus contratos – alguns requerimentos, visando a não actuação do segundo como causador de ataques. Infracções por parte do cliente serão punidas como previsto em contracto. Caso o ISP possua um CSIRT, deverá disponibilizar ao cliente informações sobre os problemas detectados antes que eles sejam explorados. Mais: os ISPs devem notificar os clientes quando o próprio provedor é afectado por algum incidente de segurança. Tal é necessário já que ele é o meio por onde os dados dos clientes são transmitidos. O ISP deverá então gerar um relatório aos clientes com as seguintes informações:

- Quem está coordenando as respostas aos incidentes: No caso de o ISP possuir um CSIRT, deve lá colocar a informação pública sobre os responsáveis pela investigação e resposta ao ocorrido.
- A vulnerabilidade explorada e, se possível, como ela foi explorada.
- Como os serviços foram afectados.
- O que está sendo feito para responder ao incidente.
- A atitude tomada para eliminar a vulnerabilidade existente.
- Que dados dos clientes podem ter sido comprometidos.
- O que esperar da resposta, considerando que esta está ganhando forma.

Para a notificação, pode ser criado pelos provedores alguns procedimentos, de maneira a agilizar o atendimento aos clientes e evitar maiores prejuízos quanto a imagem dos serviços prestados. Em todos os casos, o importante é manter os utilizadores o mais informados possível. O mesmo deve ser realizado quanto a incidentes de segurança que também tenham afetado outros provedores que estão conectados ao ISP.

2.4. Infra-estrutura da Rede

O ISP é responsável pela correcta gestão da rede visando melhor resposta dos seus serviços, tendo sempre em mente a resistência necessária contra conhecidas vulnerabilidades de segurança e, de modo algum, facilitar os meios que favorecem *hijacks* ou outros tipos de ataques.

2.4.1. Armazenamento de Dados da Rede

Normalmente, os ISPs são responsáveis por manter alguns dados de repositórios globais como os registos de *routing* da Internet (*Internet Routing Registry* – IRR), como APNIC, ARIN e RIPE. A actualização destes registos só é possível após um forte processo de autenticação, eliminando qualquer risco de *spoofing* dos dados armazenados.

O mesmo cuidado é necessário com as tabelas de *routing* presentes nos *routers* da rede interna do ISP, pois são os responsáveis em enviar os dados de um cliente para outro, ou para diferentes ISPs. Quando a autenticação não é possível, métodos restritivos devem ser adoptados.

Uma prática comum para prover anonimato a alguns ataques é a capacidade de alguns dos clientes, sejam do próprio ISP ou de outros, forjarem endereços falsos. O ISP pode e deve estar preparado para tais actos, realizando filtros nos endereços de origem dos seus clientes, somente aceitando – e permitindo o acesso à rede da Internet – a endereços verídicos. Ainda sim, o endereço precisa ser associado à origem exacta, não permitindo que um cliente use o endereço de um outro cliente do mesmo ISP. Torna-se, assim, mais difícil explorar relações de confiança baseadas em endereço. Em raras situações, quando não é possível aplicarem-se filtros, encoraja-se a realização de filtragem na própria rede do cliente.

Excessivas actualizações nas tabelas de *rooting*, propositadamente provocadas por um atacante, podem causar problemas com negação de serviço ou degradação do desempenho no *backbone* do ISP. Para tanto, o provedor deverá realizar filtragem dos anúncios, ignorando ou filtrando as mensagens que tenham origem em endereços de clientes.

2.4.2. Negação de Serviço

Um dos principais meios de preocupação dos provedores de serviços e utilizadores são os ataques de negação de serviço (*Denial of Service* – DoS). Apesar de ser um tipo de ataque comum e antigo, ainda é muito utilizado devido à dificuldade na sua prevenção e detecção.

Alguns dos ataques *DoS* são baseados na forma como o protocolo IP define os seus padrões de transmissão. A *RFC 919 – Broadcasting Internet Datagrams* define vários padrões para o endereçamento, incluindo a possibilidade de envio de endereçamento de *broadcast* a redes específicas. Potenciais atacantes podem aproveitar-se desta capacidade para gerar um número excessivo de tráfego em redes importantes, prejudicando, ou mesmo indisponibilizando, importantes segmentos de rede. De maneira a diminuir a probabilidade de serem detectados, os atacantes costumam introduzir uma quantidade considerável de tráfego endereçada ao *broadcast* de uma rede utilizando um endereço de origem falso. Ou seja, é possível utilizar uma rede que aceite *broadcasts* (ataque *smurf*) para gerar o tráfego que irá inundar a rede alvo do atacante.

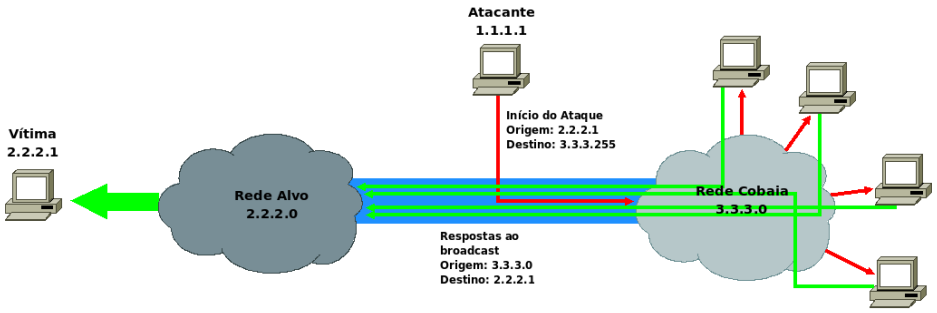


Fig. 5 - Ataque *Smurf*

Um ataque de negação de serviço distribuído (*Distributed Denial of Service* – DDoS) é outro tipo de ataque, utilizando a negação de serviço como base. Ocorre quando múltiplos sistemas, comprometidos ou não, realizam inundação de fluxos de dados a um mesmo alvo, que pode ser um ou mais sistemas. Os sistemas podem ser comprometidos de diversas maneiras pelo atacante, como uso de *malwares* (*trojans*, por exemplo) ou instalados através de invasões. São chamados computadores "*zumbis*". O conjunto de computadores *zumbis* irão formar uma *botnet*, que será utilizada para a realização do ataque.

O real perigo de ataques de negação de serviço em redes *Triple-Play* surge no instante que é disponibilizada, ao utilizador doméstico, uma largura de banda suficiente para que com poucos clientes, em simultâneo, seja possível realizar um ataque, sendo alvo o próprio provedor de serviço ou terceiros na rede da Internet. O problema é agravado pelas características dos utilizadores desse tipo de serviço: Dada a comodidade, os utilizadores com ligações de banda larga são encorajados a se manterem ligados a tempo inteiro, não aumentando os custos do serviço, como ocorria nas antigas ligações "*dial-up*". Porém, são poucos aqueles que levam a segurança até às suas redes, apontando o dedo ao pouco ou nenhum conhecimento que os mesmos possuem na área de segurança de redes. Esta atitude torna as suas redes em óptimas fontes de computadores *zumbis*, utilizados em ataques *DoS* distribuídos. De acordo com relatório publicado em *Channel Register (2005)* [11], em Inglaterra, qualquer computador doméstico sem protecção e ligado a um serviço de banda larga, será, sob a probabilidade de 50%, um possível infectado em menos de 12 minutos de uso.

Apesar dos riscos para as partes externas ao cliente serem mais evidentes, o facto de estarem sempre ligados e possuírem pouca segurança fazem deles o tipo de vítima mais procurado para ataques *D-DoS*. Estude-se a tabela seguinte, retirada do artigo *Inferring Internet Denial-of-Service Activity (2005)* [12]: A classificação foi realizada considerando a resolução inversa dos endereços das vítimas.

Tabela 2 - Destino dos ataques *DoS* em três ambientes distintos.

Kind	Trace-1				Trace-2				Trace-3			
	Attacks		Packets (k)		Attacks		Packets (k)		Attacks		Packets (k)	
Other	1,917	(46)	19,118	(38)	1,985	(51)	25,305	(32)	2,308	(49)	17,192	(28)
In-Addr Arpa	1,230	(29)	16,716	(33)	1,105	(28)	24,645	(32)	1,307	(27)	26,880	(43)
Broadband	394	(9.4)	9,869	(19)	275	(7.1)	13,054	(17)	375	(7.9)	8,513	(14)
Dial-Up	239	(5.7)	956	(1.9)	163	(4.2)	343	(0.44)	276	(5.8)	1,018	(1.6)
IRC Server	110	(2.6)	461	(0.91)	88	(2.3)	2,289	(2.9)	111	(2.3)	6,476	(10)
Nameserver	124	(3.0)	453	(0.89)	84	(2.2)	2,796	(3.6)	90	(1.9)	451	(0.72)
Router	58	(1.4)	2,698	(5.3)	76	(2.0)	4,055	(5.2)	125	(2.6)	682	(1.1)
Web Server	54	(1.3)	393	(0.77)	64	(1.7)	5,674	(7.3)	134	(2.8)	730	(1.2)
Mail Server	38	(0.91)	156	(0.31)	35	(0.90)	71	(0.09)	26	(0.55)	292	(0.47)
Firewall	9	(0.22)	7	(0.01)	3	(0.08)	3	(0.00)	2	(0.04)	1	(0.00)

[in http://www.cse.ucsd.edu/~savage/papers/UsenixSec01.pdf]

De maneira a minimizar os riscos com ataques de negação de serviço, algumas medidas e mecanismos de segurança devem ser adoptados pelos provedores, visando impossibilitar ou, pelo menos, diminuir os danos por um ataque. O primeiro passo para evitar ser-se vítima de grandes fluxos de *broadcasts* é a configuração dos activos de rede de maneira a não propagar *broadcasts* para determinadas redes e segmentos.

O uso de RPF (*Reverse Path Forwarding*) nos *routers* dos ISPs nas bordas é importante para desmascarar tentativas de falsificação do endereço de origem, como quando ocorre no ataque *Smurf*.

Quando um provedor se vê vítima de um corrente ataque, o processo de investigação deve iniciar-se imediatamente. Tal acção instantânea pode saltar grandes passos forenses, já que descobrir todas as possibilidades numa grande rede, como de um ISP, pode demorar várias horas.

O provedor de serviços deverá já ter definido todo o plano de intervenção, sabendo o que fazer durante e após um ataque: Um bom planeamento envolve realizar a separação dos endereços IP em blocos, de maneira a isolar redes e fazer com que serviços críticos estejam em ambientes protegidos. Os endereços dos clientes devem ser diferentes daqueles utilizados em outros segmentos de rede, já que o ataque pode partir tanto de redes externas (de outros ISPs), como nos clientes internos. A separação de endereços simplifica a criação de rotas separadas para as diversas redes, o que pode ser utilizado, inclusive, para o balanceamento de carga quando o ISP estiver sobre circunstâncias normais ou alteradas em caso de emergência, como quando sob ataque.

Normalmente, a filtragem de pacotes não é eficiente contra ataques de negação de serviço. Porém, com o uso de um filtro *statefull* – extremamente resistente – entre o ISP e os seus vizinhos, é possível fazer com que sejam descartados a maioria dos pacotes que não são necessários ou que façam parte de um possível ataque. Assim, as redes internas não serão atingidas e o ataque afectará apenas no exterior do ISP.

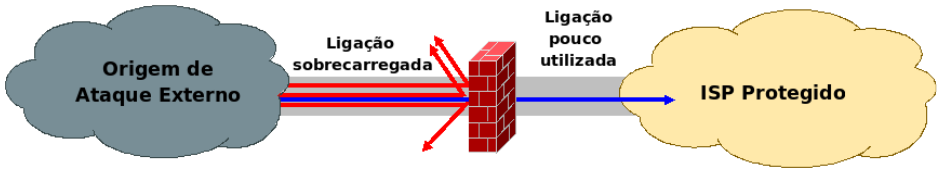


Fig. 6 - Filtro externo sob Ataque

Os ataques de negação de serviço representam um desafio para as actuais *firewalls*, já que o seu filtro é baseado apenas sobre os tipos de protocolos utilizados, portos ou endereços: Ataques baseados em regras legítimas, como por exemplo um ataque no porto 80 (serviço Web), não poderá ser evitado. Porém, as *firewalls* mais recentes, como os proprietários *Check Point FW1 NGX* e *Cisco PIX*, além do aberto *OpenBSD Packet Filter,* tem a capacidade de diferenciar o tráfego durante um ataque DoS. Tal é possível porque, antes de repassar uma ligação TCP, a *firewall* valida

o conteúdo por outros *routers* vizinhos. Outra estratégia de defesa é a possibilidade de configuração na *firewall* do valor máximo normal para o tráfego de chegada. Se o tráfego durante um período exceder o seu máximo, este entra num modo de emergência, bloqueando qualquer tentativa de novas ligações, apenas deixando entrar ou sair ligações TCP já activas.

Os *Switches* também podem trabalhar contra ataques de negação de serviço, desde que possuam capacidade para realizar limitação do tráfego, listas de acesso, *traffic shaping*, detectar ligações que sofreram quedas e análise profunda de pacotes, de maneira a detectar aberturas de ligações TCP que foram falsificadas. Os *routers* podem tratar DoS usando tais métodos, sendo que estes normalmente sofrem mais, já que realizam um maior processamento sobre cada pacote que é transmitido. Visando a diminuição este problema, algumas contagens existentes podem ser desactivadas durante o ataque, diminuindo o excesso de processamento necessário.

Por fim, um sistema de prevenção de intrusão (*Intrusion Prevention System* – IPS) pode atuar de maneira efetiva durante um ataque DoS, desde que ele possa monitorar constantemente o tráfego realizar uma análise de maneira a identificar padrões anormais. IPSs que apenas realizam reconhecimento do conteúdo do tráfego não podem bloquear um ataque baseado em DoS.

2.4.3. Sistema de Detecção e Prevenção de Intrusão

Devido o aumento nos riscos que a Internet proporciona aos provedores de serviços, os ISPs estão numa situação delicada, pois a sua infra-estrutura é baseada em padrões, sejam de mercado ou definidos, necessários para interligá-lo a diversas redes diferentes, sendo ele o canalizador de fluxos diferentes. O resultado é a necessária rapidez do ISP em apurar e detectar mudanças não autorizadas no ambiente, respondendo de acordo e minimizando os riscos ou possíveis tempos de queda (*downtimes*).

Os sistemas de detecção de intrusos (*Intrusion Detection Systems* – IDS) são relativamente novos, mas têm sido desenvolvidos a um ritmo notório. Basicamente, realizam análise em quatro diferentes categorias: detecção de intrusos na rede, verificação da integridade de sistemas, monitorização de ficheiros de registo (*logs*) e possíveis enganações que um sistema sofra.

- **Sistemas de detecção de intrusos na rede (*Network Intrusion Detection Systems* – NIDS)**: Monitorizam os pacotes que atravessam a rede, tentando descobrir possíveis anomalias que possam ocorrer, indicando quando um intruso está tentando afectar o sistema ou iniciar um ataque *DoS*.
- **Sistemas de Verificação da Integridade (*System Integrity Verifies* – SIV)**: Monitoriza o sistema de ficheiros, visando a detecção de alterações no sistema de ficheiros, de forma não autorizadas, como a instalação de *backdoors* ou *rootkits*. Ficheiros críticos, quando alterados, serão alertados em tempo-real pelo SIV.
- **Monitores de ficheiros de registo (*Log File Monitors* – LFM)**: Monitoriza os ficheiros de registo que são gerados em toda a rede. Os LFMs também procuram padrões de ataques e anomalias através da análise dos ficheiros.

Cada vez mais, os ISPs precisam destes sistemas para defender a rede contra ataques de negação de serviço (sejam estes distribuídos ou não) e outros métodos maliciosos. Se a linha de defesa não for construída quanto antes, o negócio pode ser explorado inclusive por *script kiddies* no futuro.

2.4.4. Customer-Provided Equipment

O CPE (*Customer-Provided Equipment* ou *Customer-Premises Equipment*) caracteriza-se por ser um dispositivo delimitador entre os clientes e os provedores de serviço. A sua função principal é fornecer, ao cliente, comunicação com o provedor de telecomunicações no ponto de demarcação (*demarcation point – demarc*), local onde se separam os equipamentos do cliente dos da companhia telefónica.

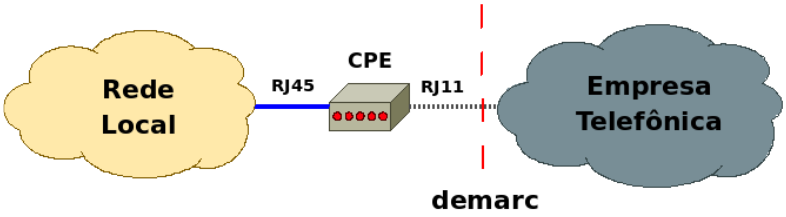


Fig. 7 - Exemplo de localização do *demarc*

Os CPEs geralmente referem-se aos telefones, modems DSL/Cabo ou *Set-top Boxes*, usados para a comunicação com os provedores de serviço(s), incluindo outros sistemas telefónicos como o PBX (*Private Branch Exchanges*).

Quanto ao provedor de serviços, um CPE será mais um risco no mundo da segurança, a partir do momento que o primeiro não é um equipamento de acesso padronizado pelo ISP: Um CPE desconhecido pode não prover diversos requisitos de segurança necessários para manter um bom relacionamento entre o provedor e os clientes: devem-se considerar as seguintes funcionalidades:

- **Possuir arquitectura modular e escalável a novos serviços**: um CPE modular possibilita, ao provedor, a introdução de novos serviços, oferecidos ao cliente sem a necessidade de troca do equipamento, diminuindo os custos e agilizando o processo de aquisição de novos produtos.

- **Integrar serviços de segurança no mesmo dispositivo**: o dispositivo pode agregar, às suas funcionalidades de ligação do cliente ao ISP, a capacidade de *firewall*, prevenção de intrusões, além de mecanismos de protecção ao ISP, impedindo ataques vindos da rede do cliente.

- **Capacidade para recuperação de falhas**: quanto menos intervenções forem necessárias no dispositivo, mais ágil é a recuperação de falhas e menor tempo de indisponibilidade do cliente.

- **Proteção *statefull***: análise das ligações e não de pacotes individuais, como acontece na maioria das *firewalls*. Poupa-se processamento e ganha-se tempo.

- **Flexibilidade na configuração dos serviços requeridos pelo provedor**: possibilidade de modificação dos serviços oferecidos ao cliente, possibilitando, ao provedor, capacidades de gestão remota do CPE, como aceitar especificações técnicas TR-069 para a gestão centralizada dos clientes.

Os CPEs que não estejam de acordo com os padrões estabelecidos pelo provedor de acesso, podem não só não atender aos requisitos acima, como facilitarão a incidência de ataques, seja através da má manipulação do tráfego ou podendo ser eles mesmos os agentes geradores de ataques, manipulados por clientes maliciosos, ou através de terceiros que tornarão o cliente no cúmplice do ataque.

2.5. Infra-estrutura dos Sistemas

A forma como o ISP gere os seus sistemas é essencial para a segurança e disponibilidade da rede: Uma brecha num dos sistemas pode degradar a performance de toda a rede, além de possíveis perdas de dados ou criar situações onde haverá um *man-in-the-middle*.

Inicialmente, é recomendado que todos os serviços sejam mantidos em sistemas separados, minimizando os danos no caso de algum destes blocos serem alvos de um ataque. Também não estarão localizados em redes onde haja trânsito de pacotes para outros destinos, como o *backbone* do ISP.

Todos os serviços, ditos críticos ou essenciais ao ISP, devem ser mantidos atrás de um forte mecanismo de protecção, permitindo que apenas utilizadores autorizados tenham acesso aos serviços, e que estes deverão oferecer apenas o direito às funcionalidades a ele necessárias. Todos os sistemas, onde existam serviços em execução, devem manter disponíveis para acesso público apenas os portos necessários. Devem-se manter actualizados os serviços do ISP com os mais recentes métodos e versões do *software* utilizado, prevenindo-se contra a maior parte das falhas de segurança conhecidas.

Quando gerindo os servidores de *e-mail*, é necessitaria especial atenção para que não sejam utilizados por *spammers*: Utilizadores mal intencionados com desejo de injectar mensagens não solicitadas para listas de *e-mails*, escondendo a identidade do remetente. O uso de relações de confiança entre *relays* SMTP deve ser adoptado mas com precaução, aceitando mensagens provenientes apenas de origem confiável.

A transferência das mensagens deverá ser utilizada apenas com autenticação e criptografia, de maneira a diminuir as chance de intercepção do conteúdo. Além disso, reforça a segurança existente num ambiente onde restrições são apenas baseadas no endereço, que pode ser forjado sem muitos problemas. Reforçando a política de segurança, recomenda-se vivamente que as mensagens sejam submetidas para envio através dos padrões definidos no *RFC 2476 – Message Submission*, ao invés do uso de SMTP normal. Assim, o SMTP no porto padrão é restrito apenas para entrega local.

2.5.1. Serviço Web

As aplicações baseadas na Web – mais conhecidas por *frameworks* –, como sistemas de gestão de conteúdo (*Content Management Systems* – CMS), Wiki, portais, plataformas de boletins e fóruns de discussão, são utilizadas por pequenas e grandes organizações. Muitas delas também desenvolvem e mantêm aplicações Web personalizadas, importantes aos seus negócios. Porém, a cada semana, milhares de vulnerabilidades são reportadas em sistemas comerciais ou abertos, fortemente exploradas quando descobertas por atacantes. As aplicações personalizadas também são alvo de ataques, mas o seu número não é reportado para listas externas, como @RISK, CVE ou *BugTraq*.

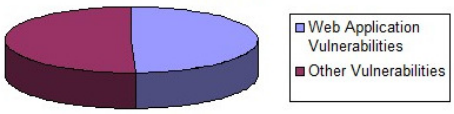


Fig. 8 - Total de vulnerabilidades reportadas para SANS @RISK em Novembro/2006 a Outubro/2007.
[in http://www.sans.org/top20/]

Todas as linguagens de programação aplicadas em *frameworks*, como PHP, .NET, J2EE, *Rub on Rails*, *Cold Fusion* e outros tipos de aplicações Web, estão vulneráveis a riscos de segurança. As explorações mais activas correm nas seguintes àreas:

- **Acesso a ficheiros pelo PHP** – PHP é uma das mais populares linguagens utilizadas para aplicações e *frameworks* na Web. Por defeito, o PHP permite o uso de funções para acesso a ficheiros remotos, activando-se pela variável *allow_url_fopen*. Através desta característica, alguns ataques são possíveis, como execução de código remoto, instalação de *rootkits*, comprometimento de sistemas *Microsoft Windows* através de *wrappers* de ficheiros SMB, etc.

- ***Cross-Site Scripting* (XSS)** – XSS permite que atacantes desfigurem páginas Web, inserindo código malicioso, conduzindo os utilizadores a ataques de *phising* que irão forçá-los a instalar *malwares* em *JavaScript*.

- ***Cross-Site Request Forgeries* (CSRF)** – CSRF faz com que utilizadores legítimos executem comandos sem o seu consentimento. Este tipo de ataque é extremamente difícil de prevenir.

- **Referência directa a objecto (*Direct Object Reference*)** – falha que ocorre quando um programador expõe referências de objectos internos, como um ficheiro, directório, registo em base de dados, chave ou URL. Um atacante pode manipular essas referências para aceder outros objectos sem autorização.

- **Informações soltas inadvertidamente** – aplicações Web podem, despropositadamente, revelar informações a atacantes, como sua configuração, serviços internos ou provocar a violação da privacidade de outras aplicações. Essas informações podem ser utilizadas para roubo ou conduzir ataques mais severos.

- **Quebra da autenticação e gestão de sessões** – se as credenciais da conta e sessão não forem adequadamente protegidas, atacantes podem comprometer senhas, chaves e *tokens* de autenticação, assumindo identidade de utilizadores legítimos.

- **Armazenamento inseguro dos dados** – As *frameworks* raramente utilizam a criptografia para o adequado e seguro armazenamento dados e credenciais. Os atacantes podem aproveitar-se desta fraqueza para roubo de dados sensíveis.

- **Comunicações inseguras** – As aplicações falham frequentemente quando realizando a criptografia dos dados a serem transmitidos na rede, quando necessário o estabelecimento de comunicações seguras.

- **Falha na protecção de páginas restritas** – frequentemente, uma aplicação apenas protege informações sensíveis prevenindo que os utilizadores vejam o *link* para áreas protegidas. Atacantes podem aproveitar-se desta fraqueza, bastando aceder directamente por um URL – numa de tentativa e erro – a estas informações sensíveis.

Diversas organizações, como a W3C (*World Wide Web Consortium*), procuram os requerimentos de segurança para melhor orientar a implementação de serviços sob plataformas Web, requerimentos estes designados por WSA (*Web Services Architecture*). Segue-se a apresentação de um conjunto de itens, padrões de segurança e interoperabilidade para referência em arquitecturas e desenvolvimento de soluções Web:

- **AC006**: Conjunto de requisitos de segurança para a *Framework* com serviços Web.
- **AC020**: Segurança a aplicar aos serviços Web para segurança dos seus clientes.

O objectivo das duas normas é respeitar as seguintes primitivas de segurança:

- **Autenticação**: a autenticação irá certificar que cada entidade envolvida num processo (requisitante e provedor) é quem realmente se espera que seja. Através da autenticação é realizado a validação das entidades perante uma autoridade maior.
- **Autorização**: a autorização determina as credenciais que garantem acesso ao serviço Web do provedor. Basicamente, são confirmadas as credenciais fornecidas ao requisitante, garantindo-lhe a possibilidade de receber respostas das operações realizadas ao serviço Web.
- **Protecção dos Dados**: a protecção aos dados irá garantir que o servidor Web possa responder as requisições através do meio de comunicação utilizado. Para tanto, é necessário que haja protecção à integridade e privacidade dos dados. No entanto, a sua protecção não garante a identidade do requisitante.
- **Não repúdio**: Garante que quem enviou uma mensagem é o mesmo que criou a mensagem.

Assim, o *framework* de um servidor Web, de acordo com o WSA, deverá possuir os seguintes requisitos de segurança para o ambiente:

Tabela 3 - Requisitos de Segurança em WSA

AR006.1	Mecanismos para tratar ameaças de ataques, como DoS, DDoS, DNS *Spoofing*, etc., através da *framework* de segurança.
AR006.2.1	Possibilidade de autenticação dos módulos no *framework* para a realização de trocas de informações importantes.
AR006.2.2	O *framework* do servidor Web deverá ser capaz de possuir autenticação persistente e/ou temporária dos utilizadores.
AR006.3	Capacidade de uso de mecanismos de autorização no *framework*.
AR006.4	O *framework* possibilitará a preservação da confidencialidade
AR006.5	*framework* com mecanismos para garantir a integridade dos dados e informações
AR006.6	mecanismos no *framework* para possibilitar a não-repudiação das partes envolvidas em uma transação
AR006.10.1	Meios para que as políticas de segurança da organização sejam expressadas.
AR006.10.2	Acesso às políticas de segurança da organização.
AR006.12	Possibilitar a auditoria do ambiente
AR006.13	Administração de todas as características de segurança para o serviço Web.

As medidas propostas pelo WSA visam proporcionar um ambiente seguro que seja simples de gerir por profissionais de desenvolvimento Web.

2.5.2. Base de Dados

As bases de dados, ou banco de dados, trouxeram muitas vantagens para as aplicações, porém, também criaram novos e mais maiores problemas no estudo da segurança em ambientes informáticos: Nas aplicações tradicionais, cada uma realiza a organização e manipulação dos próprios ficheiros. Agora, com as base de dados, uma grande quantidade de dados é compartilhada de modo flexível entre as aplicações, sendo que cada uma possui diferentes níveis de privilégios. O acesso aos dados deve ser controlado, garantindo que a confidencialidade (privacidade dos dados), integridade (alteração não solicitada) e disponibilidade (remoção acidental) sejam mantidas.

Um dos principais problemas – na segurança em bases de dados – é a capacidade de inferência, ocorrente quando um utilizador, com um determinado nível de privilégios, consegue obter dados de níveis mais sensíveis. Uma correcta implementação de níveis de segurança deve impossibilitar a obtenção de dados de níveis de segurança acima do atribuído ao utilizador: Um erro comum devido ao uso de chaves únicas para campos em comum entre vários níveis de segurança.

Actualmente, a maioria das base de dados são usados para registo de formulários em aplicações Web. Tal utilidade permite que utilizadores externos, bem ou mal intencionados, possam facilmente aceder, mesmo que indirectamente, ao base de dados. Se a segurança não for uma prioridade neste instante, a facilidade destes sistemas pode transformar-se numa possibilidade de injecção de códigos SQL, permitindo, a um atacante, executar código (*queries*) SQL no servidor, sob metodologias de *blackbox hacking* (tentativa e erro). Não só a base de dados deve possuir segurança, mas o código da aplicação Web deve estar preparado para tratar os dados fornecidos por utilizadores de enviá-los ao banco. O esquema que se segue deve ser respeitado:

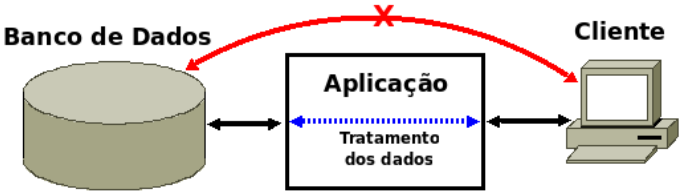


Fig. 9 - Modelo de acesso a uma base de dados

Para redução de riscos na injecção SQL, devem-se tomar as seguintes iniciativas:

- **Parâmetros** – todas as aplicações devem implementar a verificação dos parâmetros (tamanho, tipo, caracteres especiais) que são fornecidos por quem os introduz.
- **Permissões** – limitar as permissões da conta utilizada para acesso de consulta à base de dados. Sendo assim, o utilizador deverá possuir o mínimo de privilégios necessários para realizar a tarefa proposta, como apenas consulta, ou modificações de âmbito restrito.
- **Processos** – utilizar processos armazenados na base de dados para a realização das actividades do mesmo, limitando as *queries* apenas às que se encontram armazenadas.

Outra possibilidade de falhas quanto aos sistemas de base de dados é o lado humano. De acordo com o livro de *Chapple M.*: *A Fine Balance Between Roles and Rights*, 80% das brechas de segurança envolvem acessos internos, seja de funcionários ou organizações internas a uma empresa. Actualmente, o grande desafio é a criação de um balanceamento perfeito entre os acessos concedidos aos membros internos da organização e a protecção necessária aplicada às informações. Normalmente, os responsáveis pela criação de regras são os administradores dos sistemas de base de dados (*Database Administrator* – DBA). Não se tem considerado o facto de estes funcionários possuírem muitas atribuições, além de responderem por situações de emergência, o que poderá prejudicar a criação de regras adequadas para acesso às bases de dados. De maneira a garantir a segurança, integridade e privacidade das informações corporativas, algumas companhias têm adoptado políticas multi-factores (*multi-factored*), um esquema de segurança que envolve o uso de várias tecnologias para cobrir as necessidades de segurança na organização. Tal significa o estabelecimento de controlos, restrições e fronteiras ao acesso dos funcionários com a base de dados. Os mecanismos podem ser agrupados em quatro categorias:

- **Zonas (*realms*)** – são estabelecidas para encapsular acessos de uma aplicação existente a apenas um conjunto de objectos da base de dados. Pode ser realizado através da separação física dos dados ou, também, através da criação de base de dados privadas virtuais.

- **Regulamentos (*rules*)** – regras para restringir as operações de acordo com requisitos específicos, como os dados do ambiente do utilizador, endereço IP, hora do dia e modos de autenticação. Algumas situações, como quando os funcionários acedem aos dados remotamente, não poderão controlar os padrões de segurança do ambiente do utilizador. No entanto, poderão incluir algumas condicionantes, como acesso por endereços IP pré-aprovados.

- **Papéis (*roles*)** – para que todos os elementos de segurança sejam possíveis, cada empregado da organização deve possuir um papel definido: De acordo com o papel desempenhado pelo funcionário, os seus acessos deverão ser diferentes dos demais e as responsabilidades igualmente distribuídas.

- **Políticas (*policies*)** – as políticas de uma base de dados definem a estrutura e o tipo de conteúdo que cada elemento da estrutura deverá conter. Graças às novas tecnologias de segurança, podem-se aplicar restrições que, configuradas correctamente, podem proteger os dados contra acessos indevidos, além de permitir a separação dos dados. Estes e outros pontos são agora possíveis, apesar da sua necessidade e requerimento não ser novidade.

De maneira a exemplificar outras possíveis vulnerabilidades num ambiente de base de dados, a figura que se segue – retirada de *Data base Security Requirements (1980)* – mostra um esquema de possíveis pontos de falhas existentes nesta tecnologia.

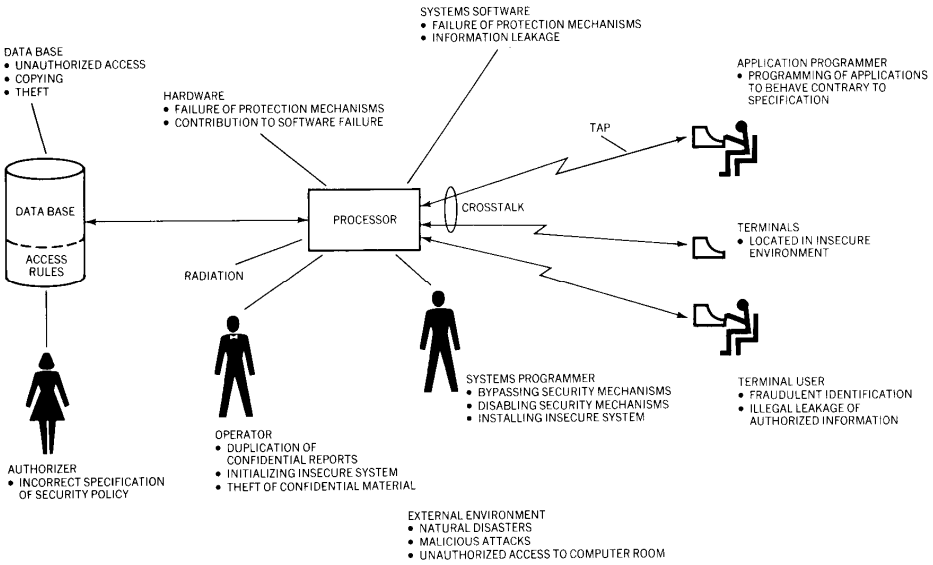


Fig. 10 - Ameaças a uma base de dados.
[in http://www.research.ibm.com/journal/sj/192/ibmsj1902F.pdf]

2.5.3. Sistema de Autenticação e Directório

O sistema de autenticação e directório de um provedor de serviços possui fundamental importância, já que irá realizar a autenticação para outros serviços de rede – como *web* e *e-mail* – além de fornecer acesso às bases de dados. É possível que, nalguns sistemas de directório, sejam armazenadas informações financeiras de clientes e parceiros, as quais não devem ter acesso público. Existem, nestes sistemas, ameaças que necessitam de cuidados específicos, nomeadamente:

- ***Eavesdropping*** – Intercepção da informação, sem alteração da origem/remetente. De tal acção, pode-se aceder às informações privadas do utilizador, descobrir as suas palavras-passe, etc. Devem-se implementar mecanismos que permitam o tráfego de informações de forma segura, através de um meio ou metodologia desconhecida por terceiros, como é a criptografia.

- **Acesso não autorizado** – Aceder a dados através de operações que levam o atacante a aceder o diretório pessoal do alvo. Podem obter tal acesso reutilizando informações de autenticação de um cliente que estejam monitorizando. As credenciais utilizadas por um utilizador durante uma sessão não devem ser válidas para reabertura da conta.

- **Tampering** – a informação em trânsito é modificada e recolocada para ser enviada ao destinatário. Há a possibilidade de alguém alterar a ordem dos bens ou modificar o nome de outra pessoa. Um atacante pode também cancelar uma requisição ou impedir requerimentos com destino ao servidor. Protocolos como SSL/TLS e similares podem resolver este problema.

- **Despersonalizar** – informações que são enviadas a alguém que falsifica a identidade. Pode ser realizado através de *spoofing* ou deturpação *(misrepresentation)* das suas informações pessoais. Deverá haver uma autenticação forte dos dois lados de maneira a impedir qualquer tipo de falsificação de identidade.

- **Negação de serviço** – um atacante pode utilizar e consumir todos os recursos do sistema alvo, impedindo-o de ser utilizado por utilizadores legítimos. Neste caso, o atacante irá impedir que o directório ou um sistema de autenticação de disponibilize serviço aos clientes. O sistema deve

possuir mecanismos para identificação (em tempo real) de ataques de negação, possibilitando--o de ignorar falsas requisições e não deixar de prestar os serviços de autenticação.

2.5.4. Sistema de Resolução de Nomes

Quando é dito segurança em sistemas de resolução de nomes de domínios (*Domain Names Server* – DNS) podem-se referir, igualmente, aspectos de segurança da implementação do protocolo ou da arquitectura do sistema (sistema operativo, serviços em uso, etc). Frequentemente, quando olhando aos ataques baseados no protocolo DNS, vêem-se três acções de destaque:

- ***DNS Spoofing*** – ocorre quando um atacante provoca o redireccionamento do requerimento DNS de um alvo, fazendo-se passar por servidor DNS "real" e reencaminhando a vítima para endereços IP falsos, isto é, não correspondentes à associação entre o nome de domínio e o seu endereço IP oficial. Pode ser realizado em comunicações entre servidores (um servidor DNS perguntando a outro, por um mapeamento) ou um diálogo entre cliente e servidor.

- ***DNS ID hacking*** – táctica utilizada para driblar um problema encontrado na técnica anterior: As respostas DNS recebem um número (ID) único relacionado com a requisição, além de que o atacante necessita fazer com que a resposta seja enviada pelo mesmo IP onde foi enviada a pergunta.

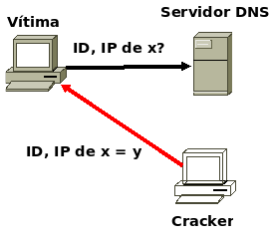


Fig. 11 - ***DNS ID Hacking***

- ***DNS cache poisonning*** – Fazer com que o servidor DNS forneça informações falsas, como um mapeamento "errado" para o endereço IP. Se a transação é realizada entre dois servidores DNS, o requisitante ainda poderá estar com uma *cache* infectada. Pode ser realizado através de dois métodos: Não-relacionados (*unrelated*) e relacionado (*related*). No primeiro caso, o servidor DNS é infectado com um *cache* sobre domínios não relacionados à consulta original. No segundo caso, a *cache* do servidor é infectada, porém, com informações relacionadas, como domínios MX, CNAME e NS. Este tipo de ataque não é eficiente nas versões mais recentes dos servidores DNS (por exemplo, o *Bind*).

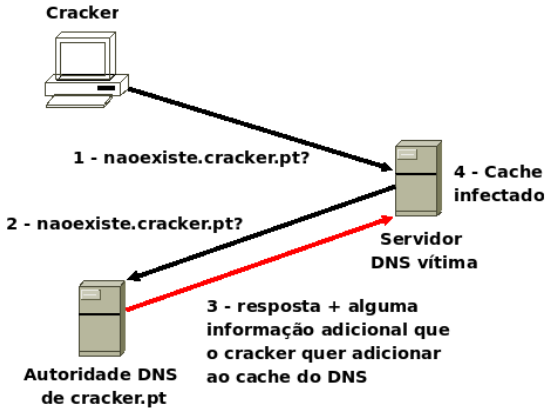


Fig. 12 - Ataque de DNS *cache Poisoning* não relacionado

- ***Client Misdirection*** – não é necessariamente um ataque, mas é utilizado para realizar o redireccionamento das requisições dos clientes para servidores não solicitados. Essa técnica é utilizada para iniciar os ataques anteriores.

Segundo o livro *Security Issues with DNS (SANS Institute, 2003)*, a ameaça de *spoofing* em ambientes DNS ainda é grande e real, representando sob percentagens no gráfico abaixo.

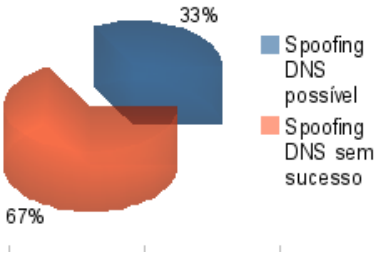


Fig. 13 - Possibilidade de *DNS Spoofing* na Internet
[*in Security Issues with DNS (SANS Institute, 2003)*]

2.5.5. Sistemas Operativos

Com sistemas de segurança sendo "*crackados*" todos os dias, os fornecedores de sistemas operativos têm disponibilizado um número recorde de *patches* e *hotfixes*, tornando-se uma frustração para os profissionais de segurança. Na pesquisa realizada em *The State of Server Operating System Security (2007),* é demonstrado que os profissionais têm gasto uma média de 32 horas mensais para responder a problemas de segurança.

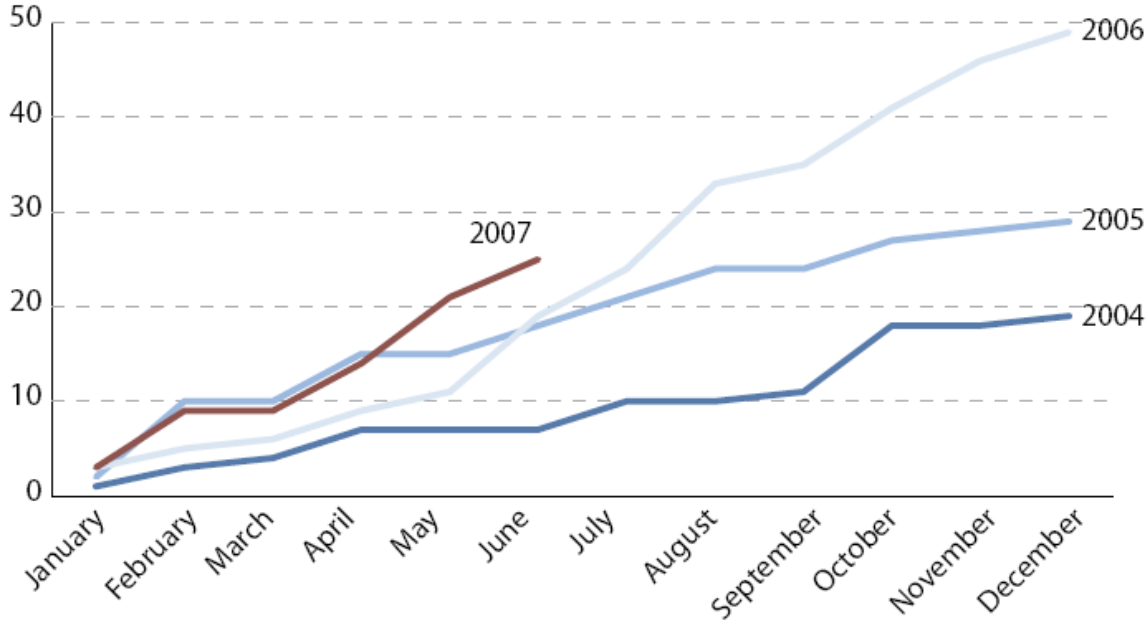


Fig. 14 - Número de *patches* de segurança da *Microsoft*.
[in http://ca.com/Files/IndustryAnalystReports/best_practices_server_operating.pdf]

Os maiores desafios para adequar os sistemas operativos às necessidades de segurança da organização podem ser listados abaixo, de acordo com pesquisa em *Best Practices: Server Operating System Security (2007)*:

1. Configuração adequada das permissões de acesso de cada utilizador.
2. Decisão para quais *patches* de segurança devem ser aplicadas.
3. Análise das *patches* e os níveis em que actuam.
4. Tempo de queda (*downtime*) dada a necessidade de actualizações de segurança.
5. Funcionários qualificados para a realização das actividades.
6. Falta de um sistema eficaz na aplicação de *patches*.
7. Tempos de queda por erros ou ataques.

Para melhor lidar com estes desafios, algumas recomendações podem ser adoptadas, tais como:

- **"Higiene" dos servidores** – verificar, repetidamente, se as opções de segurança adoptadas estão correctamente configuradas com ferramentas e metodologias padronizadas.
- **Aplicação de *patches*** – planear como e quando serão realizadas a triagem, aplicação e validação de novos *patches*.
- **Controle de acesso** – O mais claro e objectivo possível, definindo quem e o que será acedido.

Aos administradores de sistemas, os requerimentos de segurança para tornar o ambiente mais seguro são os abordados, porém, existem factores que estão além da gerência destes. Para que haja sistemas verdadeiramente seguros, é necessário que o código-fonte dos aplicativos e do próprio sistema também estejam devidamente protegidos contra as ameaças. Devido às diferentes arquitecturas e implementações, cada qual necessita de diferentes requisitos de segurança. Porém, quando é idealizada a segurança em sistemas operativos, é necessário focar todos os activos envolvidos nas redes do provedor, como os servidores, *routers* e *switches*.

Olhando o sistema operativo como um meio seguro, é necessário que este possua mecanismos que possibilitam a manutenção de seu domínio de execução, sendo capaz de se proteger contra códigos maliciosos em todos os níveis de execução. Normalmente, as vulnerabilidades existentes são resultantes de efeitos conhecidos de má programação, como *buffer overflows*, formatos de *strings*, *integer overflow* e injecção de código ou comandos. Estas vulnerabilidades são características de *software* desenvolvido em C ou C++. Linguagens mais recentes, como Java, são mais resistentes a estes problemas, mas ainda podem possuir alguns problemas quando má utilizada, ocorrendo possíveis injecções de código ou facilitismo na execução de aplicativos prejudiciais.

Recentemente, escrito em *New Hacking Technique Exploits Common Programming Error* (2007) da *SearchSecurity.com,* outra prática de má codificação foi descoberta: *dangling pointers*. O primeiro *exploit* para este particular problema foi apresentado em Julho de 2007. Antes, o problema era apenas conhecido e considerado pela comunidade académica como, na prática, "não explorável". Este alerta só vem reforçar a necessidade de codificação segura, já que outras alternativas não se mostram tão eficazes e que acabam por criar outros gargalos.

Codificação completamente segura é um objectivo que, em grandes e complexos sistemas, dificilmente se torna alcançável: o esforço necessário para prever todas as possibilidades de exploração possíveis é imenso! Foi perante estas situações, algo constrangedoras, que se desenvolveram e se apresentam, actualmente, algumas tecnologias para reforçar a segurança destes ambientes: protecção da memória de acesso, através do uso de aleatórias áreas de escrita e leitura da memória, separação de privilégios dos utilizadores, revogação dos privilégios – se necessário –, e aprisionamento de aplicações.

2.5.6. Sistemas Virtualizados

Actualmente, a virtualização de servidores é amplamente aceite, já que os fornecedores e utilizadores se sentem mais confortáveis para transferir diferentes tarefas – e não apenas suporte a legados – para aplicações e servidores virtualizados. As vantagens do uso da virtualização são inúmeras, como portabilidade, controlo de recursos físicos, etc. Porém este conceito introduz novos riscos de segurança para o ambiente.

Como *appliances* físicos (ou seja, "reais"), os clientes não se devem preocupar com a segurança do sistema operativo, já que o fornecedor da solução irá realizar os ajustes necessários. Toda a pilha de *software* existente é trabalhada e optimizada por um *appliance* virtual do fornecedor, e se houver a necessidade de alguma actualização, a imagem da máquina virtual é substituída por outra actualizada. Inadvertidamente, esta "facilidade" pode-se tornar uma das vulnerabilidades nestes ambientes.

A substituição completa da imagem para actualização do sistema operativo nem sempre é verdade, ainda mais quando se aplicam importantes *patches* de segurança: A substituição acarretaria alguma perda de características de segurança para optimização do ambiente físico. Sendo assim, a aplicação destes *patches* mais exigentes devem ser realizados pelo fornecedor da solução de virtualização. Antes de realizar a aplicação do *patch*, deve-se realizar homologação da imagem, não prejudicando o estado da máquina virtual. Só após alguns testes é possível a actualização segura das máquinas virtuais. O ciclo de actualizações torna-se claramente mais longo, podendo expor os sistemas operativos a explorações de falhas enquanto as mesmas ainda são testadas.

Um problema que pode resultar para empresas como a *VMWare*, que agem em conjunto com outras (como a Microsoft) é o licenciamento: A *Microsoft* possui uma forte EULA (*End-User Licensing Agreement*) para uso, incluindo as soluções virtualizadas. A qualquer instante, pode alterar a licença de uso, beneficiando sua própria solução de virtualização: *Windows Server Virtualization* (nome de código "*Viridian"*). Existe um esforço da mesma para o desenvolvimento de sua própria solução de virtualização, baseado num *Micro-kernel* chamado *VMkernel*. Algumas das vulnerabilidades que promete minimizar são:

- **Vulnerabilidades fundamentais dos sistemas operativos** – apesar da máquina virtual estar "separada" do *host*, problemas de segurança que afectem a última poderá acartar problemas para as virtuais.
- **Partilha de ficheiros entre a máquina convidada e a hospedeira** – algumas soluções de virtualização possibilitam a troca de ficheiros entre a máquina hospedeira e a virtualizada. Esta característica pode tornar-se um problema quando utilizada com propósitos inadequados.
- **Alocação de recursos** – as máquinas virtuais, em algumas soluções, são executadas como aplicativos comuns no espaço de memória do utilizador (*user-space*), o que pode prejudicar a performance e permitir acesso indevido do conteúdo ali armazenado.

Outros problemas que podem se tornar vulnerabilidades para a segurança do sistema são:

- **Delegação de acessos administrativos** – a distribuição de acessos necessários para a virtualização pode tornar-se algo complexo, pois a máquina virtual necessita de acesso ao nível de *kernel* no sistema operativo.
- **Interfaces de administração** – se não bem planejadas, podem provocar perda de dados, bem como outros vectores de ataques.
- **Visibilidade do tráfego** – o tráfego entre as máquinas virtuais – quando no mesmo *host* – não é visível por sistemas de detecção e prevenção de intrusos.

3. REDES DOMÉSTICAS ETHERNET

A rede *ethernet* é, actualmente, o sistema mais popular. O equipamento necessário pode ir desde um cenário simples, com apenas duas placas de rede (NICs) e um cabo até cenários complexos com múltiplos *routers*, *bridges* e *hubs*. Esta versatilidade torna-se muito útil para a telecomutação / criação de VPNs nas áreas de negócio, mas do ponto de vista do utilizador comum com uma LAN, somente lhe interessará o seu correcto funcionamento e partilha entre os seus *hosts*.

Possíveis velocidades na rede *Ethernet* (802.x):

- 10 Mbps, 100 Mbps (FastEthernet),1 Gbps e 10Gbps.

Actualmente, todas as NICs já suportam *FastEthernet*, contrastando com alguns *laptops* que ainda só suportam 10/100 (standard) pois a maioria dos *routers* no mercado comum não suportam *FastEthernet*. Assim, podem-se destacar algumas das vantagens no uso de redes 802.x.

- Tecnologia de rede mais rápida a se aplicar em casa (até 100 Mbps ou 1 e 10 Gbps);
- Relativamente barato (se os computadores se encontrarem no mesmo quarto ou se a casa já tiver um *backbone*).
- Fiável;
- Manutenção Fácil;
- Suporta um elevado número de dispositivos (SmartPhone, PocketPC, VoIP, etc.);
- Suporta a maioria dos computadores e respectivos Sistemas Operativos;
- Informações e Manuais disponível em grande escala.

A cablagem pode tornar-se num problema maior se a casa onde se monta a LAN não estiver preparada com um pequeno *backbone* com a cablagem espalhada pela casa com as respectivas tomadas *RJ-45*, optando-se por redes *Wireless* que requerem maior atenção. Quanto à Internet, embora muitos utilizadores estejam conscientes dos riscos associados ao seu uso, poucos têm consciência da magnitude deste risco, ainda mais com a actual largura de banda *allways on* oferecida aos mesmos.

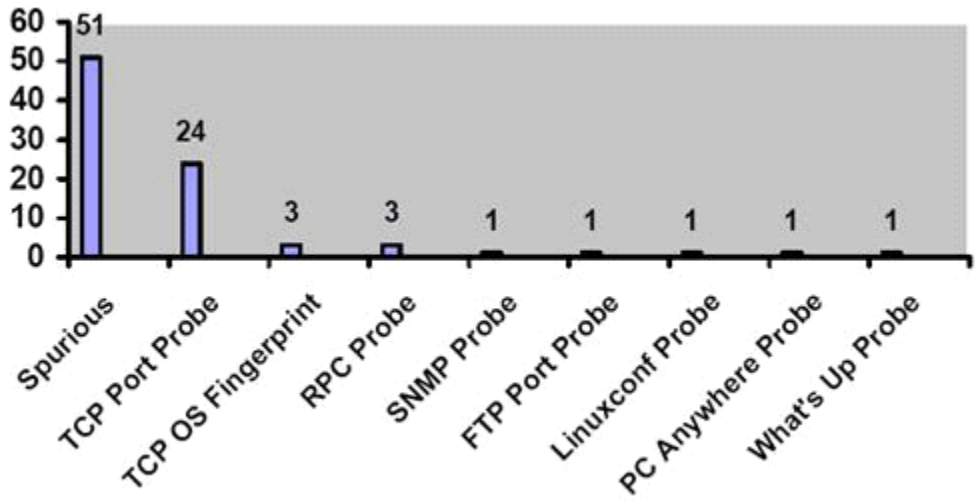


Fig. 15- Monitorização de ataques a um host num período de 10 dias

[***in NIST: Special Publication 800-46, page 17*** **]**

A figura acima mostra as tentativas de intrusão, registadas num período de 10 dias, a uma máquina ligada à internet. Este *log* foi gerado por uma *firewall* configurada com um nível de segurança considerado elevado. Segundo o *NIST*, a maioria dos ataques são falsos alarmes. Contudo, potenciais intrusões mais sérias chegaram a ocorrer mais de três por dia!

O atacante começa por investigar e identificar ("*Probing"*) as vulnerabilidades do sistema alvo: Procuram-se portos abertos, versões do software que as utilizam e possíveis vulnerabilidades que atordoam o correcto funcionamento do mesmo ou devolvam determinados valores desejados. Métodos que realizam *fingerprint* do sistema poderão identificar o sistema operativo ou *PreOS* instalado nos *routers* ou *hosts*, através da análise de reconhecimento do padrão de leitura dos últimos.

3.1. Segurança Local

São considerados, como pontos de vulnerabilidade na rede, quaisquer problemas ou situações que possa infringir alguma das três primitivas básicas da segurança de dados:

Confidencialidade: Refere-se à necessidade de manter a informação segura e privada. Para a maioria dos utilizadores, esta categoria inclui lembretes, informações financeiras e/ou de segurança (como *passwords*). Os computadores de casa contém informações pessoais (ou de uma empresa onde trabalhe) privadas, razão pela qual a segurança do dispositivo e a privacidade dos dados sejam de elevado interesse.

Integridade: Significa que a informação se mantém inalterada por utilizadores não autorizados. O interesse deste tipo de informação é de maior interesse de entidades que ofereçam serviços aos clientes e não queiram correr riscos, por exemplo, na troca - por terceiros não autorizados - de números de conta.

Disponibilidade: É a noção de que a informação está disponível quando necessária. Os ataques de *Denial of Service (DoS)* são assaltos à disponibilidade de um serviço (web, email, etc.). Aos utilizadores domésticos de xDSL ou Cabo, a preocupação será tanto a garantia de que o seu sistema

não é desactivado por terceiros, como a prevenção de intrusos sabotarem o sistema para seu próprio uso contra outros sistemas.

As vulnerabilidades podem surgir sobre diversas formas, apresentando-se desde a configuração padrão do Sistema Operativo utilizado, problemas de configurações de serviços, defeitos de software, erros do SO, etc. A curta duração das ligações *dial-up* dificultava os atacantes na tarefa de comprometer serviços em qualquer servidor. Agora com ligações a tempo inteiro e com grandes larguras de banda, devem-se tomar diversas medidas para garantir a segurança de dados privados.

Palavras-passe Robustas:

A maioria das tarefas no computador envolve autenticação por palavras-passe. É essencial que os utilizadores ganhem o hábito de criar fortes palavras-passe, com um mínimo de oito caracteres contendo letras maiúsculas, minúsculas e números. Esta necessidade de reforçar a palavra-passe deve-se ao facto de já existir uma larga oferta de *software*, na Internet, para obtenção de palavras-passe. Se este software utilizar dicionários de palavras-passe (+500.000 palavras), mais rápidos mas menos eficientes, muitas palavras comuns serão testadas, como nomes de pessoas, animais, junção destes com números comuns como o ano, etc. Uma possível solução para sessões *on-line*, seria o uso de um gerador de palavras-passe, dependente de um único *PIN* conhecido pelo utilizador. Aplicar-se-ia uma nova palavra-passe no inicio de cada sessão, impossibilitando o atacante de utilizar a palavra-passe obtida em futuras sessões.

Por curiosidade, recentemente saiu, no *TheInquirer* (http://www.theinquirer.net/), uma notícia sobre a facilidade com que um empregado de uma empresa dá a sua palavra-passe a um desconhecido. É dito que 45% das mulheres trocaria a sua palavra-passe por uma barra de chocolate. Aos homens, tal só ocorre a 10%. Como é questionado no artigo: “como responderiam os homens se se tratasse de uma caneca de cerveja?”

Artigo: http://www.theinquirer.net/gb/inquirer/news/2008/04/16/women-give-passwords-chocolate

3.1.1. Denial of Service (DoS)

A intenção de um ataque de bloqueio de serviços (*Denial of Service* - DoS) é bloquear o uso legítimo do recurso de uma rede, geralmente sobrecarregando serviços disponibilizados. Apesar dos esforços e recursos dispendidos para se criarem barreiras contra estas intrusões, todos os sistemas ligados à internet deparam-se com a consistente e real ameaça que são os DoS. Tal se deve a duas características básicas e fundamentais na rede Internet: A infra-estrutura que suporta a Internet, responsável por interligar todos os sistemas e redes, está limitada à largura de banda entre os infinitos *routers*, *gateways*, etc., e a capacidade de armazenamento destes dispositivos (cache), servidores ou outros *hosts*. Estes pontos são um alvo comum nos ataques DoS, desenhados para consumir suficientes recursos do alvo ao ponto de causar um certo nível de perturbação, chegando a impedi-lo de responder a outros *requests*.

Os primeiros ataques DoS eram pouco desenvolvidos, com pacotes enviados de uma única fonte a um só destino. Com o passar dos tempos, as ferramentas utilizadas para ataques DoS evoluíram com métodos de ataque para múltiplos alvos de uma ou várias fontes. Hoje em dia, existem ferramentas bastante eficientes, criadas com tal engenho à realização de ataques DoS de múltiplos pontos, que levam muitos domínios à saturação de recursos.

3.1.1.1. Ser Intermediário de Um Atacante

Um atacante, após a intrusão numa rede LAN doméstica, irá comprometer o computador como plataformas de lançamento a ataques para outros sistemas. Um exemplo disso será a forma como as ferramentas de DoS distribuído funcionam e são utilizadas: É instalado um "agente" (ou *trojan*) nas máquinas comprometidas, aguardando posteriores instruções. Depois, quando vários agentes já estão em execução (diferentes computadores), um simples *handler* pode instruir todos os *hosts* a lançar um ataque DoS. O alvo não será o computador afectado, mas um determinado servidor ou sistema acessível pela Internet, o qual possui alguma vulnerabilidade anteriormente detectada e explorada neste DDoS.

Pode-se olhar este tipo de ataque como uma hierarquia de *hosts:* Existe um computador "general", responsável por dar a ordem de ataque, um conjunto reduzido de "brigadeiros", encarregues de recrutar soltados, afectando computadores com a intrusão de agentes ou envio de *trojans*, geralmente em sistemas P2P por *Social Engineering* (atribuição de nomes apelativos). A defesa contra ataques DoS está longe de ser uma ciência exacta ou completa. Limitar a largura de banda e filtrar pacotes pode, em alguns casos, ajudar a reduzir o impacto dos ataques DoS distribuídos, consumindo-se parcialmente os recursos disponíveis.

3.1.1.2. Ataques e Defesa do ISP

A "caça ao atacante" é *sempre* mal sucedida, pois apresentam-se diversos entraves para quem procura responder-lhes. Assim, torna-se um desafio maior: poucos ou inexistentes *logs* de *firewalls* para partilha, o uso de técnicas de *spoofing* e outras mais ferramentas que criam diversas barreiras para o identificar.

Como já referido no capítulo anterior, o uso de *spoofing* é muito comum para cobrir o endereço original do atacante e, consequentemente, a origem do *stream* de pacotes. Pior ainda é quando o atacante aproveita este campo para indicar o endereço IP de outra vítima, não só bombardeando-o com *requests*, mas também obrigando-o a receber *replies* de outras vítimas (muito engenhoso, de facto)! Esta técnica é muito utilizada para "amplificação de pacotes", com o envio de pacotes a destinos de *broadcast*, ataques estes conhecidos por "*smurf*" ou "*fraggle*".

Ao longo dos tempos, utilizaram-se diversos tipos de pacotes para a criação de *flooding* ("inundação") no servidor alvo, mas existem uns poucos mais utilizados pela maioria das ferramentas de DoS:

- ***Floods TCP*** – São enviados, continuamente, ao endereço IP do alvo, vários pacotes TCP com diferentes *Flags* activas: SYN, ACK e RST são as mais comuns neste tipo de ataque.

- ***Floods UDP*** **–** O mesmo que em TCP, mas utilizando o protocolo UDP.

- ***Request*** **e** ***Reply*** **de pacotes ICMP –** Envio contínuo de pacotes de controlo de ligação – protocolo ICMP – como, por exemplo, pacotes de *Ping* (conhecido por "Ping of Death"). Neste e em outros casos, só se terá de fechar o porto que recebe para estes pacotes.

- **Portos de Origem e Destino:** Por vezes, as ferramentas de *flooding attack* de pacotes alteram o porto de origem e/ou destino, dificultando a filtragem de pacotes dos serviços implementados no *host* alvo.

- **Portos de Origem e Destino:** Por vezes, as ferramentas de *flooding attack* de pacotes alteram o porto de origem e/ou destino, dificultando a filtragem de pacotes dos serviços implementados no *host* alvo.

Como os ataques de "inundação" de pacotes procuram esgotar o processamento ou largura de banda disponível no alvo endereçado, o volume e continuidade de transmissão são parâmetros importantes na detecção destes ataques e o grau de sucesso. Numa outra vertente, é fácil, para um atacante, gerar e enviar por toda a rede, pacotes com atributos fabricados. O protocolo TCP/IP (v4) não está preparado com mecanismos para verificar a integridade destes atributos. Assim, um intruso no sistema só necessita privilégios suficientes para executar ferramentas de ataque capazes de fabricar atributos alterados maliciosamente e enviá-los pela rede vitimada.

3.1.2. Firewalls

A primeira linha de defesa numa rede LAN doméstica (ou empresarial) é uma boa *firewall*. Apesar da maioria dos utilizadores estarem conscientes da entrada de publicidade via Internet e ataques de DoS por *trojans*, *adware* ou *spyware*, poucos avaliam as vulnerabilidades da sua rede e sistemas contra tais ataques, pensando que um – ou pior, vários – "anti-virus" tratará de tudo, sem distinguirem as diferentes ameaças.

Segundo o NIST, utilizando o serviço de *scanning* http://www.DSLreports.com, 95% das máquinas que correram este *scan* mostraram uma ou mais falhas, nomeadamente a presença de *adware*, facilidade de obtenção de *usernames* e contas *guest*, *routers* com configurações de protecção fraca e impressoras visíveis a todos os utilizadores (não será um problema em redes domésticas, mas o controlo é necessário).

Tabela 4 - Distribuidores de Firewall de software
[in "NIST – Security for Telecommuting and Broadband Communications – Special Publication 800-46"]

Personal Firewall Product	Web Site	Free	Platform
BlackIce	http://www.networkice.com/		Windows
McAfee Personal Firewall	http://www.mcafee.com/		Windows
NeoWatch Personal Firewall	http://www.neoworx.com/		Windows
Norton Personal Firewall	http://www.symantec.com/		Windows
PC Viper	http://www.pcviper.com/		Windows
Securepoint	http://www.securepoint.cc/	✓	Windows
Sygate Personal Firewall	http://www.sygate.com/	✓[3]	Windows
Tiny Firewall	http://www.tinysoftware.com/	✓[4]	Windows
Winproxy	http://www.winproxy.com/		Windows
ZoneAlarm	http://www.zonelabs.com/	✓[5]	Windows
SmoothWall	http://www.smoothwall.org/	✓	Linux
T.Rex	http://www.opensourcefirewall.com/	✓	Linux
SINUS	http://www.ifi.unizh.ch/ikm/SINUS/	✓	Linux
Net Barrier	http://www.intego.com/netbarrier/		Mac OS

Juntamente com o *software* de *firewall* instalado directamente no *host*, poder-se-á utilizar dispositivos dedicados ao controlo de portos abertos/fechados, entre outros serviços da *firewall*, colocados entre o modem ADSL/Cabo e o *router* da LAN doméstica ou *host* único. Embora caros (entre os €60 e os €170), este *hardware* oferecem diversas vantagens sobre a *firewall* de *software*, sendo talvez os factores mais importantes o facto dos *hosts* estarem a partilhar a mesma *firewall* e processamento ser dedicado. Esta partilha é possível por *Network Address Translation* (NAT), responsável por traduzir o conteúdo de um IP público para os diferentes IPs da rede interna, aumentando a segurança, pois todas as chamadas à Internet têm de partir da rede interna. Tal possibilita a partilha de um único IP externo para um conjunto de *hosts* da rede interna e adiciona uma camada extra de segurança.

No mercado comum, estas funcionalidades já vêm incorporadas nos *routers*, que podem até incorporar *modem Cabo/ADSL*, *Firewall*&NAT, *Wireless*, Hub de 4 portos, etc. Inicio de tráfego fora da rede interna não será autorizado e o que é iniciado nesta rede interna poderá ou não ser autorizado, dependendo das regras da *firewall*.

De sublinhar que os *firewalls* dedicados são mais difíceis de se comprometerem, comparativamente às *firewalls* de *software*, estando estes dependentes da segurança do sistema operativo.

Com estes *packs* de serviços dedicados num único dispositivo, torna-se importante que a palavra-passe de autenticação no *router* seja imediatamente alterada para algo mais robusto, obedecendo às regras de letras maiúsculas, minúsculas e números, pois o acesso de terceiros poderá ser fatal à rede LAN doméstica alvo. As palavras-passe *default* dos fabricantes de *routers* são facilmente descobertas em manuais disponibilizados na internet, podendo ser tão óbvias que nem será necessário realizar esta busca. É igualmente importante actualizar o *firmware* dos dispositivos de rede, principalmente os que contêm autenticação por *password* guardada num espaço de memória dedicado. Vulnerabilidades de acesso a memória não são desejadas.

Quando é utilizada uma *firewall* de *software*, o utilizador deverá configurá-la, se tal já não vier como padrão, para que fique tudo bloqueado, seguindo-se o desbloqueio conforme necessário. A maioria dos *softwares*, após a sua instalação, obedece a este método: Após a instalação, nenhum porto está aberto, e somente se abrem os portos que forem aceites pelo utilizador (geralmente, associando-as às aplicações), num interface gráfico mais amigável.

Os utilizadores devem olhar bem às características existentes no *router* ou *software* que irá comprar ou fornecido pelo seu ISP. Abaixo apresentam-se algumas características importantes e a configuração ideal da *firewall*, dependendo do uso a dar na rede LAN doméstica ou empresarial.

3.1.2.1. Configuração

- ***Criação de Logs (Relatório):*** Certifique-se que são criados relatórios na *firewall*. Se terceiros não autorizados conseguirem aceder à rede ou máquina, o *log* poderá ajudar a identificar a fonte da vulnerabilidade e intrusão. Nos *logs* devem-se registar os endereços IP associados à data e hora de acesso (configuração geralmente padrão), para posterior comparação apreciados em esforços cooperativos com outras entidades para mais facilmente identificar o atacante, que certamente terá realizado *scan* (*nmap, traceroute,* etc.) a milhares de outros endereços IP, ficando o acto registado nos vários *logs*.

  Num ambiente com controlo remoto como é o *Triple-Play*, estes *logs* podem ser obtidos numa linha hierárquica superior (no seu domínio), sem ser necessário aceder o *gateway* do cliente. A maioria dos registos trará falsos alarmes à mistura, tornando-se o professo forense bastante moroso. Podem existir, por exemplos, alertas de infecções de *trojans* mesmo que o *host* alvo não esteja afectado, devido a uma leitura do pacote mal interpretada.

- **Esconder Portos (modo *stealth*):** Os *hosts* recebem pacotes para um número de porto específico, dedicado para algum serviço específico como *WebServer* (porta 80 ou 443 se encriptado), envio de correio electrónico (SMTP → 25 ou 465), etc. Quando um porto fechado recebe um pacote, é devolvida a mensagem RST como um aviso do seu estado. Um sistema no modo *stealth* não responderá a nenhum *request* de porto, escondendo a sua existência e, por

consequente, a máquina alvo. Este "corte" em respostas poderia afectar o correcto funcionamento de protocolos utilizados para oferecer serviços como HTTP, SMTP, FTP, etc., mas tal não acontece! Estes serviços não esperam uma resposta do cliente: apenas *requests*.

- ***Logout* automático:** Um dos problemas de segurança mais significativos advém da ligação a tempo inteiro à Internet. Certas *firewalls* disponibilizam uma opção onde se define um temporizador de inactividade. Quando este pára, o acesso do *host* ao router é desligado e só será restabelecido quando for novamente apresentado actividade. A própria ligação à rede externa (Internet) será cortada se nenhum *host* interno a aceder durante um período de tempo definido. Desligar a Internet fará com que serviços mal intencionados, correndo em *backdoor*, não possam actuar senão quando o alvo estiver a ser utilizado por alguém capaz de detectar o *malware*.

Mesmo trabalhando proactivamente para reforçar a segurança do sistema de diversas formas, deve-se assumir que "não existe segurança perfeita" para o sistema e dados pessoais durante uma ligação externa. Como tal, todos os outros pontos devem ser revistos.

Grupo de Regras Configuráveis: Certos dispositivos de *firewalls* são desenhados de forma a operar segundo um conjunto de regras que determinam o controlo de acesso. Estas regras examinarão os pacotes tanto nas camadas por que se responsabilizam, como em outras inferiores, analisando-se portos, tipo de serviço (FTP, http, SMTP, etc.), endereços IP de origem e destino, etc. Este grupo de regras limita o uso excessivo do utilizador aos diferentes serviços monitorizados, podendo criar-se/modificar-se particularidades para coincidir com as necessidades do administrador. Configurar estas regras requer um nível de conhecimento informático superior e na área das comunicações.

Configurando tais regras, devem-se excluir todos os pacotes de chegada de serviços não seguros (por exemplo, portos 135 a 139 que suportam o protocolo NetBIOS, utilizado para, por exemplo, partilha de ficheiros, e apresenta algumas vulnerabilidades). O acesso a portos aleatórios deve ser restringido, de forma a que uma tentativa de contacto com estes portos sejam vistos como "closed" pelos outros nós da rede (emula modo *stealth*).

Devem-se excluir, também, todos os pacotes enviados à excepção de serviços reconhecidos pelo utilizador (DNS, SMTP/POP/IMAP, HTTP, FTP, etc.) Apesar de diferentes formas de implementar estas regras – dependendo do fabricante –, o conceito das regras é generalizado para qualquer *firewall* do mercado. Há até algumas que são configuradas de forma a auto-configurar-se contra *trojans* conhecidos e outros tipos de *malware*. Quando presente, esta solução deve ser mantida.

Notificação de Ligação: A maioria das *firewall* de *software* envia notificações quando algum programa requer acesso à internet para envio de pacotes. A *firewall* interrompe o utilizador questionando o acesso a atribuir ao programa. Quando tal ocorre sem que o utilizador tenha realizado qualquer acção sobre o computador, provavelmente será um *spyware* ou um programa desconhecido a correr em *backdoor*, instalado sem conhecimento do utilizador.

- **Controlando o "nivel de Paranoia":** Se a *firewall* de *software* é configurada com um elevado nível de segurança, o risco de falsos alarmes aumenta exponencialmente! A maioria das *firewalls* permitem nivelar a segurança ao uso pretendido. Por exemplo, se um utilizador utiliza um programa para partilha de ficheiros, certos pacotes poderão "activar o alarme" desnecessariamente. Um nível moderado de segurança reduz tais alarmes, ao mesmo tempo que providencia a segurança básica necessária.

  O nível padrão de uma *firewall* não é necessariamente o ideal, sendo o acesso à configuração destes níveis pré-definidos é facilitado pelo fabricante.

- ***Virtual Private Network (VPN):*** Embora já hajam *firewalls* de *software* capazes de suportar VPN (http://www.fx.dk/firewall/), este método de criação de "túneis" pela Internet, encriptados para extensão da rede interna a outros *hosts* deslocados, são maioritariamente, criados a partir do *router*.

- **Configurações Protegidas:** Por último, mas não menos importante, é proteger toda a configuração efectuada com uma palavra-passe, impedindo terceiros mal intencionados (que consigam aceder à rede) de modificar os parâmetros definidos.

Dadas as dificuldades em configurar uma *firewall* – quando em ambientes *Triple-Play* –, será boa aposta oferecer-se serviços de configuração remota de *firewalls*. Claro está que os serviços de *CallCenter* serão um ponto importante para se compreender as necessidades dos utilizadores, se as politicas de segurança do ISP aceitam os requisitos do cliente e se o conforto de "ver as coisas funcionando" não é afectado.

3.1.2.2. Rastreio de Segurança On-line

Existem diversos *websites* que irão realizar - sem cobrar por isso - um rastreio (scanning) e gerar um relatório de segurança da rede doméstica por onde se está a aceder ao *website*. O rastreio decorre em tempo real, onde o servidor do *website* tenta ligar-se aos portos padrão de diversos serviços que estejam a correr na máquina alvo. Quando encontrado um porto aberto (*port scan*), tenta-se saber qual o serviço que a utiliza e a sua versão, explorando as possíveis vulnerabilidades (*vulnerability scan*). No final, é dado uma classificação à segurança da rede rastreada, apresentando-se um relatório completo. Espera-se que todo o processo se realize sob HTTPS (HTTP com SSL/TLS).

Tabela 5 - WebSites de Auditoria local
[in "NIST – Security for Telecommuting and Broadband Communications – Special Publication 800-46"]

Service	URL	Port Scan	Vulnerability Scan
DSL Reports	http://www.dslreports.com/tools/	✓	✓
GRC	http://grc.com/		✓
HackerWhacker	http://whacker2.hackerwhacker.com/	✓	✓
MS Baseline Security Analyzer	http://www.microsoft.com/technet/security/tools/Tools/mbsahome.asp		✓
Sygate	http://www.sygatetech.com/	✓	
Symantec	http://www.symantec.com/securitycheck/		✓

3.1.2.3. Recomendações

Todas redes LAN domésticas ligadas à internet deveriam ter um dispositivo ou *software* de *firewall*. O *software* protege o *host* que o corre, mas a melhor opção será em *hardware*, dispositivo que oferece uma camada extra de segurança na rede.

Operando com ambas as *firewalls* em *hardware* e *software* dá a oportunidade de monitorizar intrusões e identificar qualquer *software* responsável por transmitir mensagens do *host* para o exterior da rede. Para o utilizador comum com uma rede LAN doméstica, poder-se-á pensar que o computador está protegido "porque tem uma *firewall* instalada no computador" mas a solução está em usar dispositivos dedicados. Além da camada extra de segurança, o utilizador final ficará mais satisfeito, não tendo um *software* a sobrecarregar o computador nem a questionar-lhe associações entre portos e *software* instalado a requerer acesso.

Com os serviços *Triple-Play*, o próprio ISP poderá oferecer serviços de controlo do dispositivo de *firewall*. O incómodo será, provavelmente, o utilizador ter de telefonar para um *CallCenter* para explicar e requerer o porto de acesso desejado. Muitos nem saberão o que é "um porto", dizendo somente que *software* que precisa correr. Poder-se-ia até utilizar a ligação IPTV para explicar ao utilizador "o que é um porto e a sua necessidade", avisar o pedido de acesso de certos programas, etc. Infelizmente, também este meio ficaria sobrecarregado de informações, sendo preferencial, para o cliente, utilizar um *firewall* de *software,* voltando-se à estaca zero! A solução será deixar o utilizador aceder à *firewall* localmente (por IPTV?), aliviando os recursos humanos ("mão de obra") e *CallCenter* do ISP, sendo somente necessária a monitorização dos portos abertos e respectiva actividade, com eventos de alerta automático para anomalias – fora do padrão – na actividade do utilizador.

3.1.3. Segurança em WebBrowsers

Quando um utilizador acede a um *website*, estará a requerer a um servidor – que contém o *site* – o código HTML a ser lido, traduzido e apresentado pelo *webBrowser* local. O que o utilizador por vezes não sabe é que o seu IP é registado e, mesmo que este seja atribuído por DHCP – IP dinâmico, novo a cada reinício do de ligação à Internet (ISP) –, não deixará de ser possível identificar o utilizador na própria sessão. Mesmo que utilizando *NAT*, só não se saberá qual o computador da rede interna, mas da rede externa será fácil fazer *trace route* até à separação das redes. Assim, a solução para o "anonimato" do utilizador será utilizar um *proxy* no ISP que separe a sua rede de clientes da rede externa. Também possível será o próprio cliente, sabendo alguns conhecimentos de informática, utilizar *webProxies* de terceiros. De notar que o responsável deste *Proxy* pode identificar o utilizador que está a requerer o conteúdo da Internet.

Existem problemas de segurança mesmo no próprio conteúdo do ficheiro com o código HTML que é interpretado pelos *webBrowsers*. É possível explorar vulnerabilidades no *host* utilizando código activo, como JavaScript, XSS, etc., capazes de criar buracos de segurança no *host* que se ligou ao *webServer* (mal intencionado). Para se salvaguardar, ou o utilizador retira a opção de processamento do código activo no seu *webBrowser*, ou utiliza um *webProxy* com remoção de código activo. Além do anonimato, também é possível utilizar *Proxies* para remoção de conteúdo pouco seguro como código activo, *Cookies* com tempo de vida permanente, etc.

3.1.2.4. *Proxies* de Internet

Quando utilizando um *webProxy*, todo os requerimentos para e conteúdo de *websites* passam pelo respectivo servidor *proxy*. Primeiramente, este *proxy* irá reencaminhar os HTTP *requests* do utilizador ao *webserver* com o IP ou domínio requerido. Após receber por completo o *website* requerido, o *proxy* reencaminha o conteúdo para o cliente, com o código activo tratado numa ligação, por vezes, encriptada. Nesta perspectiva, os servidores que recebem os *requests* vêem o *proxy* como destino, não sendo possível identificar o *host* que se encontra atrás (destino real), impedindo qualquer "exploração" ao utilizador. O anonimato do cliente de um *webProxy* é limitado, na medida em que o segundo saberá identificar o primeiro e associá-lo aos *http Requests*: resta ao utilizador "fiar-se" no *webProxy* que está utilizando.

A análise de conteúdo realizada pelo *proxy* pode evitar diversos riscos de intrusão – por exemplo, embutir *spyware* sem que o utilizador se aperceba do que está a ser instalado –, modificando ou apagando alguns *cookies* sem tempo de duração e com informações como a palavra-passe do utilizador. A encriptação providenciará segurança contra intercepções (*sniffing*) na rede entre o *proxy* e o utilizador. Na maioria dos casos, a ligação entre um *webserver* e um *host* não é encriptada a não ser que o primeiro utilize *HTTP c/ SSL*. O envio de e-mails através destes *proxies* passará pela detecção de vírus. Tal não funcionará se a ligação entre o cliente e o *mailServer* já estiver encriptada.

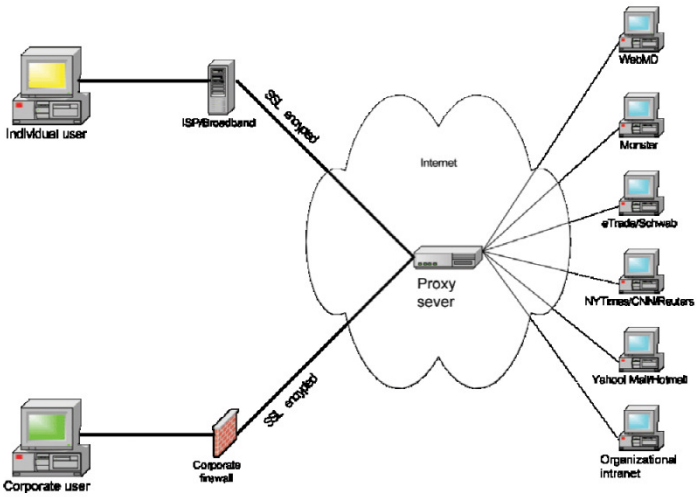


Fig. 16– Processo WebProxy
[in "NIST – Security for Telecommuting and Broadband Communications – Special Publication 800-46"]

É importante compreender os serviços de *webProxy* e as suas características, como a existência de encriptação, manuseamento de código activo e *cookies*, a compatibilidade com os *websites* que o utilizador frequenta, etc.

Apesar de útil, estes serviços podem ter certas limitações: A eficiência pode tornar-se um problema, pois a eventual sobrecarga deste *proxy* pode tornar o acesso bastante mais lento, além de que, se público, um ataque DoS dinâmico, com um elevado número de *hosts*, será muito fácil de se realizar. A degradação deve-se essencialmente à encriptação e ao desvio que o "roteamento" terá de realizar para passar por esse *proxy*. Mesmo que o acesso seja garantido, a incompatibilidade poderá ser incómodo ao utilizador, pois muitos *websites* necessitam de *JavaScript* ou *Flash* para o bom funcionamento, código este que será parcial ou totalmente eliminado pelo *proxy*. Por último, mas não menos importante, é o cuidado que se deve ter quando acedendo a, por exemplo, contas bancárias ou áreas de financiamento que necessitem de autenticação. Apesar de este tipo de acesso ser, na maioria das vezes, encriptado, passar por um *webProxy* pode não ser boa ideia.

Tabela 6 - Lista de WebProxies de entidades independentes do ISP: Os seus serviços e preços variam frequentemente
[in "NIST – Security for Telecommuting and Broadband Communications – Special Publication 800-46"]

Service	Web Site	Web Proxy	Encryption	Filters Cookies	Filters Active Code	Free
Anonymizer	http://www.anonymizer.com/	✓	Partial	✓	✓	✓
Anonymizer	http://www.anonymizer.com/	✓	✓	✓	✓	
HiddenSurf	http://www.hiddensurf.com/	✓	✓	✓	✓	
Ponoi[10]	http://www.ponoi.com/	✓	✓	✓		✓
PrivacyX	https://www.privacyx.com/		✓			✓
SafeWeb	https://www.safeweb.com/	✓	✓	✓	✓	

3.1.3. Redes Wireless 802.11

Quando utilizando redes *wireless* 802.11, o utilizador comum não olha às configurações do seu *router* ou *access point*, ficando muitos dos valores de configuração inalterados, com o padrão de fábrica. Se, por exemplo, o SSID da rede fica em *broadcast* com o nome padrão, facilitará ao atacante descobrir alvos fáceis com padrões de fábrica. Estes e outros dados devem ser tomados em atenção para a garantir a segurança e *QoS* do cliente. Abaixo seguem-se os passos a dar para garantir a melhor segurança numa WLAN.

1. Mudar a palavra-passe de administrador do dispositivo *wireless*

O núcleo da maioria das redes *Wi-Fi* são os pontos de acesso (APs) ou *routers*. Para configurar estes dispositivos, os fabricantes disponibilizam um interface gráfico *web* embutido, possibilitando ao administrador realizar a maior parte das informações necessárias ao correcto funcionamento da rede (endereços, partilhas, filtros, etc.). Este ambiente de configuração está protegido por uma palavra-passe – por vezes, também com nome de utilizador – a qual só o responsável pelo dispositivo ou rede deverá ter conhecimento. No entanto, a maioria destes equipamentos já vem com uma palavra-passe padrão, facilmente obtida dos manuais disponibilizados na Internet. É prioritário alterar esta palavra-passe ainda antes de qualquer configuração do dispositivo e difusão da rede *wireless*.

Infelizmente, muitos utilizadores não têm conhecimento deste interface (tão facilmente acedido), geralmente configurado, no acto da compra, por algum técnico de informática. Este pode introduzir uma palavra-passe comum em todos os seus "clientes" e ter posterior acesso não autorizado. O cliente terá a palavra-passe anotada num papelinho sem se dar conta da importância que seria mantê-lo ou até, mais recomendado, alterar o seu valor.

2. Activar encriptação WPA

Todas as redes *Wi-Fi* suportam encriptação. Esta tecnologia baralha as mensagens enviadas *over-the-air* para que não possam ser facilmente interceptadas (*sniffing*) por terceiros. Existem diferentes tecnologias de encriptação *wireless* aplicadas ao protocolo de rede 802.11. Naturalmente, o utilizador terá tendência a escolher o algoritmo mais forte. Infelizmente, muitos dispositivos NICs poderão não suportar encriptações mais recentes, tendo-se de escolher o algoritmo mais forte e comum entre o *access point* ou *router* e os seus *hosts*. Geralmente, todos utilizam WPA Pessoal/Enterprise, versão 1 ou 2.

A inconveniência de qualquer encriptação é a largura de banda que ocupará, dado que são mensagens maiores, e o tempo dedicado ao processo de encriptação e desencriptação, se bem que o último não será um problema, visto ser uma chave simétrica e a encriptação ocorrer em apenas um sinal de difusão.

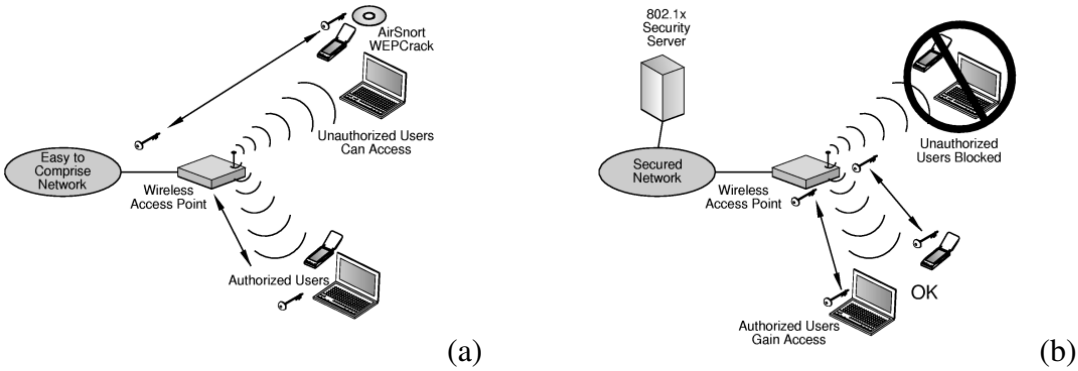


Fig. 17 - Uso de encriptação WEP (a) e WPA (b)
[in HP – *Tree Levels of Wireless Security*: http://docs.hp.com/en/T1428-90017/ch01s04.html]

O uso de encriptação nas redes *Wireless* começou com a tecnologia WEP, encriptação baseada num vector de iniciação (IV, do inglês *initialization vector*), acoplado no princípio do pacote WEP e com tamanho de 24bits, possibilitando 2^{24} chaves. Como é gerada um novo IV aleatoriamente a cada novo envio, não será necessário avaliar 2^{24} pacotes, bastando uns cinco a dez mil pacotes para realização de *sniffing*, reduzindo o tempo de espera nos *softwares* que realizam o *cracking* da chave WEP em "*brute force*". Além do tamanho pequeno do IV, também o uso de uma chave estática (síncrona) não ajuda na protecção dos conteúdos transmitidos por *wireless*.

Se levarmos a segurança a sério, confiar na encriptação WEP não é um bom passo. A alternativa – e correcta solução – é a tecnologia *Wi-Fi Protected Access*, ou WPA, a qual gera diferentes chaves assíncronas para cada cliente que se queira ligar ao *AccessPoint* ou *Wireless Router*. Os dados são encriptados usando a cifra contínua RC4, com chaves de 128bits (2^{128} possibilidades, muito mais extensa) e um vector de iniciação de 48bits. Juntamente com o IV, também é utilizado *Temporal Key Integrity Protocol* (TKIP) que muda a chave dinamicamente durante o uso do sistema baseando-se num conjunto de dados e a uma taxa temporal muito inferior à necessária para qualquer *sniffer* conseguir desencriptar a chave anterior. Todos os dispositivos de WLAN possibilitam o uso de WPA e WPA2.

3. Mudar o nome padrão do SSID

Os APs e os *routers* atribuem um nome à sua rede *Wi-Fi* conhecido por *Service Set Identifier* (SSID). Normalmente, os fabricantes destes dispositivos já atribuem um nome padrão. Esse, geralmente, é o nome da empresa e o modelo do dispositivo. Quando em difusão, por si só não apresenta perigo, no entanto será mais fácil para terceiros mal-intencionados escolher os seus alvos: O SSID padrão demonstra uma rede má configurada, e só por aí será mais fácil procurar e aplicar a palavra-passe padrão de acesso à configuração do dispositivo ou realizar *probing* a outras vulnerabilidades. É importante que o nome de rede *Wi-Fi* seja alterado para algo menos sugestivo.

4. Activar o filtro de MAC-Address

Cada dispositivo de rede possui um identificador único chamado *MAC-Address*. Os APs e *routers* mantêm um registo de actividade de cada MAC-Address, podendo os primeiros gerirem o acesso que lhes é dado, aceitando todos os MAC-Address registados, com ou sem atribuição de IP fixo na rede interna, restringindo o acesso a

qualquer outro dispositivo Wi-Fi NIC. É vantajoso utilizar-se esta opção, no entanto, terceiros poderão utilizar *software* que facilmente falsifica o *MAC-Address* da sua NIC (*Spoofing*).

Em redes domésticas, o controlo de MAC-Address poderá tornar-se incomodativo à maioria dos utilizadores. Primeiramente porque "ninguém" sabe o que é um MAC-Address, como obtê-lo e introduzi-lo no interface gráfico, etc. Num *gateway* ou *router* com fios e um número de dispositivos únicos, esta opção deve ser configurada, à partida, após a aquisição do equipamento (por exemplo, *Gateway Triple-Play*) ou até já vindo configurado de fábrica. No entanto, numa rede *Wireless*-LAN doméstica, o administrador da rede terá de ter conhecimentos de informática um tanto superiores à média da população para poder introduzir o MAC-Address de cada "visita autorizada" que recebe em casa.

Da mesma forma que, em *Triple-Play*, um utilizador é informado na televisão de uma chamada VoIP, será também possível informar a descoberta de um novo MAC-Address, perguntando se está autorizado a ligar-se à rede interna? Dever-se-á incluir um tempo limite do seu acesso? Classificá-lo como "Local" ou "Visitante"? Se tal fosse possível, dever-se-á manter a lista de MAC-Address aceites e bloqueados, pois ninguém quer ser constantemente questionado por um MAC-Address de terceiros não autorizados.

5. Desactivar a difusão do SSID

Os APs e *routers wireless* têm, por defeito, activada a difusão do seu SSID *over-the-air* num determinado período de tempo. Esta opção foi desenvolvida para *hot-spots* em locais públicos, não sendo ideal para ambientes privados como uma rede WLAN doméstica. Mantê-la activa aumenta a probabilidade de atacantes tentarem aceder ao dispositivo *wireless* e rede doméstica. É aconselhado desactivar esta opção e configurar os computadores com os parâmetros necessários para aceder à rede WLAN – nome de SSID, encriptação, etc. – mesmo que não esteja a difundir o seu SSID.

Numa rede *Wireless-LAN* doméstica, desactivar o SSID implicará configurar o acesso directamente no *host* que a deseja aceder. Mais uma vez, esta atitude tornar-se-á incómoda para o cliente. Imagine-se que este só tem conhecimentos básicos de informática: Nunca poderá configurar todos os computadores portáteis ou PDAs que queiram aceder à rede interna. Assim, sendo ou não num ambiente *Triple-Play*, o SSID deve ser mantido em emissão, pelo menos, nas redes domésticas, sacrificando algum nível de segurança pelo conforto do cliente.

Se num ambiente *Triple-Play* com o SSID em difusão, poder-se-iam seguir os passos indicados no ponto 4, perguntando ao utilizador, por IPTV, da autorização ou não de um novo MAC-Address.

6. Não utilizar a auto-ligação a redes *Wi-Fi* abertas

Ligar-se a redes Wi-Fi abertas, como *hotspots* gratuitos ou redes WLAN domésticas expostas, irá também expor o seu próprio computador a diversos riscos de segurança. Muitas vezes, os computadores ligam-se automaticamente a redes abertas sem antes questionar o utilizador. Esta opção só deverá estar activada quando necessário (redes encriptadas).

7. Atribuir endereços de IP fixos aos dispositivos e evitar DHCP

Por defeito, as WLAN estão configuradas com a tecnologia DHCP, oferecendo um endereço IP a cada *host* que liga ao nó da rede. Infelizmente, esta liberdade também favorece os atacantes, podendo facilmente obter um IP válido da oferta (*pool*) do DHCP. Deve-se desligar o DHCP, reduzir a oferta de IPs e defini-los como fixos e associando aos MAC-Address. Utilize-se um *range* de IPs privado, como 10.0.0.x, para prevenir o acesso aos computadores internos por fontes externas.

Seguindo o ambiente *Triple-Play* com a opção de filtragem de MAC-Address, poder-se-iam associar IPs fixos aos MAC-Address.

8. Se existir, activar a *firewall* no dispositivo *Wireless*

Actualmente, todos os *routers* vêm com *firewall* embutida, mesmo que desactivado (por defeito). Como explicado no tópico acima, extra protecção dependerá muito dos serviços e respectivos portos que o utilizador vá precisar.

9. Colocar o dispositivo *Wireless* num local seguro

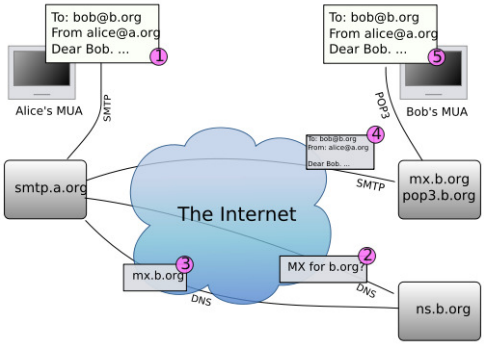
O sinal dos APs e *routers Wi-Fi* normalmente chegam ao exterior da casa. Quando o sinal é fraco nessas áreas limite, não será um problema mas, já com maior força, é fácil para terceiros não autorizados explorarem a rede WLAN. Muitas vezes, o sinal chega à casa de vizinhos até do outro lado da rua. O ideal será posicionar o AP no centro casa, ao invés de ao pé de janelas, minimizando as brechas do sinal.

Em apartamentos, o dispositivo poderá ficar centrado, mas em casas ou vivendas, poderá ser do interesse do cliente ter acesso à internet no exterior. Neste caso, a atenção aos outros pontos de segurança deve ser redobrada.

10. Desligar a rede *wireless* quando não utilizada por longos períodos de tempo.

Desligar a WLAN é o ultimato que impedirá qualquer *hacker* de entrar na rede LAN doméstica via *Wireless*. Claro que esta solução é impraticável, e tal só ocorrerá quando o utilizador autorizado não necessitar desta tecnologia por longos períodos de tempo.

3.1.4. E-mail



O surgimento do *email* ocorre aquando da criação da Internet, na segunda metade anos 60's, numa LAN onde se criou um protocolo responsável pela transmissão de mensagens entre os vários utilizadores da rede. Este sistema, protocolo SMTP, rápidamente se transformou na rede de "correio electrónico" dos actuais tempos.

3.1.4.1. Publicidade Não Solicitada (SPAM)

Sendo um protocolo tão antigo, e criado para facilitar a comunicação dentro de uma rede interna, não foram colocadas grandes questões de segurança nas áreas da privacidade e autenticação. Como meio de comunicação tão popularizado e barato, não demorou muito até que se tornasse um dos principais meios publicitários. Dada a actual massividade da publicidade não solicitada por correio electrónico, foram introduzidos diversos *add-ons* ao SMTP, desde anti-virus, detecção de publicidade SPAM, conteúdos impróprios, uso de listas negras, etc.

Numa rede doméstica, grande parte do problema publicitário foi resolvido, e muito se faz para se manter segura a rede – e domínio – das empresas. No entanto, e apesar de todo o *software* que, efectivamente, bloqueia *emails* não solicitados ou com conteúdo infectado (ficheiros *.exe, *.reg, etc.), não se pode fechar os olhos à realidade ocorrente na Internet: Utilizando programas de monitorização, é facil perceber a percentagem de largura de banda que o SPAM ocupa na actividade do correio electrónico. Cerca de 80% dos *emails* recebidos por um ISP ou empresa são SPAM, 99% deles originados em apenas 5 países, com a maior fatia proveniente da China (±73%).

3.1.4.2. Spoofing e Social Engineering

O "*spoofing*" pode ser um problema ainda mais grave para o utilizador comum. Enquanto o SPAM é um grande incómodo, receber correios electrónicos que aparente ter sido originado numa fonte e tendo veio de outra, poderá levar a grandes perdas! O objectivo mais comum é enganar o alvo e obter alguma informação confidencial, adoptando métodos de *Social Engineering*. Aos utilizadores menos atentos, nem será necessário realizar *spoofing* de correio electrónico se a técnica de *Social Engineering* for "fiável" (não olhando à origem do correio). Um utilizador menos consciente poderá responder com palavras-passe, números de contas bancárias, cartões de crédito, etc. Abaixo uns exemplos:

- Receber um correio electrónico, alegando ser de um administrador do sistema, requer ao utilizador a alteração da sua palavra-passe para uma *string* específica, ameaçando fechar a sua conta caso não actue.

- Receber um correio electrónico de uma autoridade, requerendo a cópia da autenticação necessária que acede a informações sensíveis.

Note-se que nenhum serviço legítimo irá requerer a um cliente ou trabalhador que envie informações privadas por tais meios. Também uma possível alteração à sua autenticação nunca seria para um valor conhecido! O que o alvo deve fazer é entrar em contacto com a entidade responsável pelo *e-mail* recebido (o contacto oficial).

A transmissão de dados por SMTP é em *cleartext* (desencriptado), pelo que para realização de "*sniffing*" se torna um alvo fácil. Felizmente, como em outros protocolos na camada de aplicação, pode-se adaptar o SMTP à encriptação por SSL/TLS, sendo reconhecido pelo MUA pelo porto que são recebidos os pacotes.

3.1.4.3. Vírus em Correio Electrónico

Encontram-se, a circular nos *emails*, diversos vírus e outros tipos de código malicioso, criados ou modificados para melhor se adaptarem a *Social Engineering* utilizado nos *emails* e *websites*. Assim, o utilizador deverá verificar primeiro o conteúdo (*attachments*) anexado ao *correio electrónico.* Não bastará reconhecer o correio electrónico, é preciso ter confiança no destino e saber que género de informação e conteúdos esperar, pois muitos vírus e *trojans* espalham-se precisamente por contactos familiarizados pelo utilizador.

3.1.4.4. Código HTML

Com a expansão do uso de correio electrónico, consequentemente foi necessário aplicarem-se protocolos capazes que dinamizar o conteúdo das mensagens, com conteúdos multimédia, desde imagens a vídeos embutidos por HTML. Com o tempo, esta junção de tecnologias facilitou a vida aos seus utilizadores mas também ao SPAM! Com a percentagem de largura de banda que este ocupa na Internet, ainda mais será quando enviando HTML com diversas imagens!

Utilizando código HTML, as mesmas preocupações aplicadas aos *WebBrowsers* são puxadas para o correio electrónico: Podem-se criar "buracos" de segurança num *host* utilizando código activo, tanto em *WebBrowsers* como em MUAs (*Mail User Agents*)!

3.1.4.5. Login Remoto:

O método mais comum para recepção de *e-mail* é com autenticação remota ao servidor que contém os *e-mails* enviados e recebidos. Este serviço requer, por parte da entidade responsável pela gerência de contas e palavras-passe, uma maior atenção. Um cliente facilmente perderá ou dirá a sua palavra-passe a terceiros, mesmo não intencionalmente (vitima de *Social Engineering*), dando acesso aos atacantes a servidores de *e-mail*. Note-se que a maioria das contas utiliza POP3 ou IMAP não encriptados, sendo a palavra-passe enviada em *cleartext* e facilitando a vida aos *sniffers*. Como para HTTP e SMTP, os protocolos POP3 e IMAP também podem correr sobre a camada de encriptação SSL/TLS.

3.1.4.6. Passo a Passo para a Segurança do Seu *email*

1º. Não abrir os ficheiros incluídos no *email* senão quando absolutamente necessário ou de alguma fonte de confiança: Os "pesos pesados" do correio electrónico na maioria das redes domésticas são conteúdos multimédia humorísticos, geralmente enviados entre amigos para grandes listas de endereços de correio electrónico! Esta atitude não só sobrecarrega a rede, como se torna um meio fácil de propagação de *malware*.

2º. Ficheiros .EXE, .BAT, .VBS ou SCR são vectores comuns para infecções *malware*. Por vezes, os provedores não bloqueiam este conteúdo e arriscam-se a infestar uma população de utilizadores. Nestes casos, devem-se manter actualizados os MUAs para que sejam bloqueados estes conteúdos.

3º. Realizar um *scan* ao conteúdo recebido. Geralmente, os *WebMail Servers* já indicam o resultado proveniente do anti-virus que lá utilizam, e o uso de *MUAs* não impede o anti-virus do utilizador de aceder ao conteúdo antes dele ser aberto, avisando caso sejam detectadas infecções.

4º. Abra os ficheiros, como DOC ou PDF, através do respectivo leitor e nunca clicando no próprio ficheiro: Evita que ocorram infecções de, por exemplo, *macro-virus* VisualBasic, embutido no documento e que arrancam logo após o duplo clique no ficheiro.

5º. Utilize um MUA que só lide com *plain text*, i. é, texto limpo sem conteúdos multimédia ou código activo como HTML. Não deixará de receber conteúdos multimédia e terá um sistema mais seguro.

6º. Não utilize serviços de *Webmail* quando acedendo a informações sensíveis. Por vezes, um utilizar mais distraído deixará a opção de "*Remember My Account*" (*cookies*), ficando o acesso livre à sua conta de correio no respectivo PC, sendo ainda mais grave se utilizando computadores de acesso público.

7. Por mais chato e irritante que seja, leia as licenças de acordo de serviço antes de clicar em "Concordo". Alguns servidores de *e-mail* passam a ser donos do conteúdo das suas mensagens de *email*.

3.1.4.7. Recomendações

A maioria dos trabalhadores precisa enviar e receber *emails* constantemente, seja do seu escritório ou de casa. Existem diferentes formas de manusear o envio de correio electrónico com diferentes vertentes na área de segurança. Algumas abordagens menos correctas podem gerar vulnerabilidades na rede do cliente e outras entidades presentes no mesmo ou outro ISP. Por outro lado, a segurança restrita poderá limitar demasiado o cliente. O uso de *mailProxies* poderá ser a opção ideal para controlo de *emails* por *backbone*.

3.1.5. Controlo Parental

Já à alguns anos que se disponibilizam *softwares* para filtragem, bloqueio e controlo parental: Uns livres e outros pagos, dependendo da qualidade do serviço desejado. Agora até as empresas de *hardware* querem embutir estes serviços no seu produto.

Existem *websites* que fazem o *review* a *software* de controlo parental. Um deles é http://parental-control-software.upickreviews.com/, e actualmente apresentam as três melhores escolhas: *Net Nanny*, *Cyber Patrol* e *Cyber Sitter*.

3.1.5.1. NetNanny

O *NetNanny* é um *software* de controlo parental que impede tanto protege menores de acederem a conteúdos inapropriados e limitar o tempo na Internet, como oferece funções de bloqueio de informação privada em ambientes de *Instant Messaging* (IM) ou *emails*.

A maior vantagem do controlo parental sob *software* sobre outros sistemas comuns de filtragem por *hardware* (portas, domínios ou IPs, etc.) é a maior flexibilidade. Neste *software*, é possível sistematizar até 12 filtragens diferentes, a aplicar a cada indivíduo, segundo o seu nível de maturidade e necessidades pessoais.

Até à data, poucos, como o *NetNanny*, ofereçem um serviço de *update* gratúito de novos *websites* com conteúdo inapropriado, presentes na sua base de dados *on-line*, sendo automaticamente bloqueados e ficando nas mãos do utilizador "facilitar" o acesso ao novo site.

O *NetNanny* garante que nenhuma informação privada será colocada na internet pelas mãos de menores ou outros familiares: Qualquer tentativa de envio de informações como cartões de crédito, endereços de e-mail, números de contacto telefónico, etc., via chatrooms, IM ou *e-mail*, *o software* irá transmitir tais informações substituindo os caractéres por X (tipo XXXXXXX…).

Cost:	$39.99
Software Features:	■■■■■
Filtering Effectiveness:	■■■■■
Userfriendly:	■■■■■
Customer Support:	■■■■■
Free:	14 Day Trial
Internet Filtering:	✓
Chat Blocking:	✓
Chat Filtering:	-
Email Filtering:	✓
Email Blocking:	✓
Newsgroup Blocking:	✓
Peer-to-Peer Blocking:	✓
IM Port Blocking:	✓
Personalized Profiles:	✓

Além do *NetNanny* conseguir bloquear os famosos e variados estilos de "*pop-ups*", também é bloqueado a partilha de ficheiros por programas *peer-to-peer* (P2P) como *eMule*, *Torrents, Kazaa, Napster,* etc., além de outros tantos por IM. Outra característica que dá realce ao *NetNanny* é uma tecnologia avançada que ajuda (o responsável pelo controle de conteúdos) a monitorizar e bloquear *websites* que contenham texto e imagens de potencial pedofilia em quaisquer actos indecentes. Este sistema é suportato pela SOC-UM, uma organização sem fins lucrativos que promove avisos públicos sobre este problema social.

Características gerais: Monitorizar URLs por comparação de palavras, bloquear *cookies* e *pop-ups,* submeter URLs suspeitos para posterior avaliação e integração na base de dados *on-line,* seguir listas-negras na actividade do *email,* limitar horas de uso de Internet, bloquear *Instant Messenger* e a troca de ficheiros P2P, relatório detalhado das actividades de cada utilizador, etc.

3.1.5.2. Cyber Patrol

O objectivo do *CyberPatrol* é proteger menores do uso indiscriminado da Internet, especialmente contra conteúdos que não deveriam aceder. Como qualquer outro *software* de controlo parental, o *CyberPatrol* também filtra o conteúdo da Internet, tornando a navegação de menores mais agradável e considerando uma segurança sem riscos de eventuais "precausos".

O *CyberPatrol* é muito *user-friendly*: Bloqueia todo o conteúdo dos *websites* que já tenham sido avaliados e colocados na sua lista *on-line "CyberNOT"*. Assim, se algum conteúdo impróprio, seja pornografia, violência ou material obsceno, nunca será acedido pelo utilizador com *CyberPatrol* instalado na máquina. O critério de classificação inclui factores como nudez parcial e completa, conteúdo sexual, intolerâncias religiosas, satanismo e outros cultos, apostas ilegais, drogas, etc., havendo também outros conteúdos com menor impacto.

Com base nas categorias atribuídas pelos desenvolvedores do *CyberPatrol*, os clientes são livres de escolher os tópicos que desejam bloquear. Pode-se também caracterizar diferentes opções a aplicar a cada membro, não havendo constrangimento a adultos que queiram/precisem aceder a conteúdos mais violentos. Em níveis de menor importância, poderá haver conteúdo livre para juvenis mas impróprio a crianças menores de 8 ou 12 anos. Neste sentido, o programa aceita a introdução de novos *websites* "inofensivos" à sua *blacklist* para criação de um filtro ainda mais rígido.

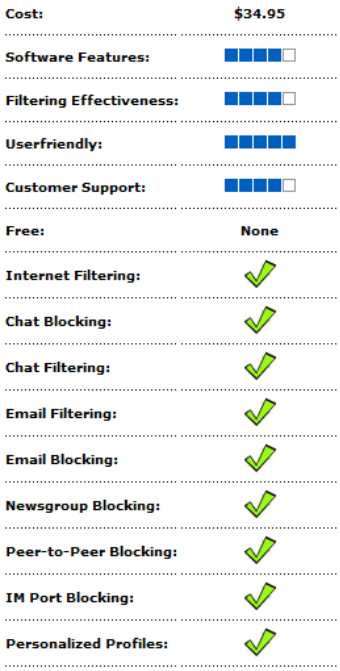
Cost:	$39.95
Software Features:	
Filtering Effectiveness:	
Userfriendly:	
Customer Support:	
Free:	14 Day Trial
Internet Filtering:	✓
Chat Blocking:	✓
Chat Filtering:	✓
Email Filtering:	-
Email Blocking:	-
Newsgroup Blocking:	-
Peer-to-Peer Blocking:	-
IM Port Blocking:	-
Personalized Profiles:	✓

Além do bloqueio de *websites*, o *CyberPatrol* também bloqueia outras aplicações como IM e outros meios onde informações privadas possam ser entregues por crianças (impedido por completo o uso destas aplicações, ao contrário do *NetNanny* que apenas faz a filtragem do conteúdo privado). Podem-se definir horários de navegação na Internet e bloquear pastas, como as que contêm jogos ou outros entretenimentos que consumam o tempo de uso dos menores lá de casa.

Características gerais: Gerar o tempo de uso da Internet, bloquear *downloads*, monitorizar os hábitos do utilizador, suporte *on-line* para controlar e configurar o sistema desejado, etc.

Desvantagens: Não há suporte técnico por telefone e falha em certos detalhes no relatório do uso de Internet. Muitos pontos não são monitorizados como é no *NetNanny* e a filtragem muitas vezes é substituída pelo bloqueio, tornando-se mais incómodo para o utilizador.

3.1.5.3. Cyber Sitter



O *CyberSitter* é a escolha ideal para uma filtragem de *websites* mais suave: Protege os menores de aceder a conteúdos impróprios de uma forma mais pacífica, bloqueando somente os *sites* mais notórios ou sem margem para dúvida. Aparecerá uma emulação de "404 Not Found", não dando a entender que o *website* foi bloqueado. Será confuso para o utilizador mas também para os menores, que tão rapidamente aprendem a saltar as barreiras que lhe são impostas. Nesta área, o *software* pode ser muito fraco, mas acaba por se estender a outras áreas como o rastreamento de materiais ofensivos no disco rígido do utilizador, localiza *spyware* instalados na máquina, etc. Pode também realizar filtragem no *email*, embora não tão eficiente como as opções dedicadas à filtragem de SPAM no mercado ou as soluções implementadas pelos *mailServers*.

3.1.5.4. Monitorização

Apesar dos três programas acima já mostragem algum potencial contra os menores, a realidade é que quanto mais barreiras lhes colocarmos, mais eles tentarão ultrapassá-las. Pode até criar na criança um espírito de *hacker*, algo não desejável. Se forem necessários meios mais fortes, talvez se deva considerar *software* de monitorização e relatório de actividade, não os impedindo de agirem como desejado.

Existem diversos programas de monitorização: *IamBigBrother*, *PC Tattletale*, *eBlaster* e *SpectorPro* são alguns. Cada um destes programas é capaz de capturar todas as teclas carregadas, aplicações abertas e fechadas, *websites* visitados, etc. Regista as conversas de *chats* como IM, ICQ ou IRC, assim como *emails* recebidos e enviados. No entanto, para bom aproveitamento destas ferramentas, é necessária alguma experiência do utilizador e infelizmente, na maioria dos casos, são os adultos a pedir ajuda aos menores, com maior capacidade de aprendizagem. Em termos de simplicidade, o *IamBigBrother* e o *PC Tattletale* são os mais intuitivos, mas tal advém da menor oferta de opções, como no *eBlaster* ou *SpectorPro*. Mais: ao contrário de outras aplicações, que deixam o utilizador criar diferentes *profiles* para múltiplos utilizadores, estes programas de monitorização só aceitam um perfil por computador.

Os menores devem sempre saber que estão sobre monitorização activa, de forma a se criar algum nível de confiança entre o primeiro e os seus parentes. No entanto, em casos mais drásticos, será necessária a monitorização num modo escondido, sem que a criança se aperceba de tal (*Stealth Mode*). Alguns programas de monitorização fazem-no melhor, outros não tanto. Muitos deles, e os próprios programas de *Parental Control*, são facilmente retirados do *Task Manager* do Windows, ou simplesmente se acede ao *Add/Remove Programs* para acabar de vez com o problema. Os programas *eBlaster* e *SpectorPro* são muito bons nisso, pois não deixam rasto da sua presença nem no *Windows Registry*! Aconselham-se os últimos dois programas para um maior detalhe de pacotes P2P, bloqueio de sessões de *chat*, acesso ao *email* ou qualquer outro *software* que exija a abertura de um porto para o exterior da rede.

Outra característica interessante é a captura de *printscreens* num período de tempo definido para tal, presente em todos os programas de monitorização referidos acima, à excepção do *eBlaster*, pois este é mais virado para a criação de *logs* para *email*.

3.1.5.5. Controlo Parental em Dispositivos Dedicados (*Hardware*)

O uso de mecanismos de controlo parental já existe há algum tempo nos *routers* domésticos, fazendo tarefas simples de bloqueio de uma lista de URL definida pelo administrador do sistema. Esta configuração, apesar de simples, não o é quando acedida pelo utilizador comum.

Os fabricantes de *routers* arranjaram uma solução muito simples e eficaz. A *Linksys* (modelo WRT54GS) e a *ZyXEL* (modelo HS-100W) formaram parceria com serviços de controlo parental *on-line* – *Netopia* e *Cerberian*, respectivamente – para oferecer um único ponto de protecção no seu *router*. Estes serviços são pagos numa taxa anual.

Ao invés de restringir o filtro de controlo parental a um único computador, o utilizador poderá fazer *login* em qualquer computador e ter as suas permissões individuais aplicadas e activas. Mesmo que múltiplos utilizadores partilhem a ligação num único PC, os *routers* saberão separar os filtros para cada conta. Em termos classificativos, pode-se definir diferentes perfis para os filtros, desde crianças, juvenis, jovens ou adultos. A administração é feita num ambiente gráfico acessível pelo *webBrowser* do utilizador, com todo o tipo de regras que serão controladas, pelo *router* segundo os dados nos servidores de controlo parental. Entre os *routers* da *ZyXEL* e o servidor da *Cerberian*, apenas a filtragem *web* requer ligação ao segundo, o que significa que a maioria dos serviços manter-se-á activa mesmo com o servidor da *Cerberian* em baixo. Os *routers* da Linksys requerem medidas adicionais mais robustas, desde a validação do utilizador, uso obrigatório de determinadas opções como restrições de tempo e aplicações, etc.

Ambas as entidades *Netopia* e *Cerberian* classificam milhões de *websites* mensalmente. Quando o utilizador navega na Internet, os *sites* a visitar são questiodados pelo *router* ao servidor de controlo parental e este retorna uma classificação. Segundo as regras de filtragem aplicadas ao utilizador, o *router* poderá ou não receber ou não o conteúdo requerido. Geralmente, esta interacção não é notória, mas os *routers* da *Linksys* não deixam passar a mensagem de rejeição e o motivo. Quanto ao controlo de programas de IM ou *input* de teclado, a situação já é diferente, e fica-se a desejar algo mais. A *Linksys* possibilita o uso de listas de contactos bloqueados e de confiança, seja para IM como para *e-mail*, além de detalhar mais os seus relatórios de actividade.

3.1.5.6. *Hardware* Dedicado ao Controlo Parental

Dada a importância do assunto, alguns fabricantes de *routers* separaram os serviços de controlo parental do dispositivo de *routing*. Por exemplo, a *D-Link* desenhou o *SecureSpot*, um dispositivo de segurança para a Internet que contém antivírus, anti-spam, anti-popup e controlo parental para todos *hosts*, situando-se entre o modem de internet e o *router*. Todo o controlo oferecido nos programas de controlo parental, seja nos *websites*, *emails*, IM, teclado, relatórios, etc. – características gerais do *NetNanny* –, é possível neste pequeno dispositivo.

Os dispositivos de segurança deste género não têm processador nem memória para se poderem implementar bons e rápidos sistemas de filtragem e antivírus, podendo proteger o computador contra uns milhares de *malwares* e nunca milhões, como em *softwares* de antivírus especializados. Contudo, antivírus no *SecureSpot* é da *McAfee*, assegurando alguma qualidade. Um ponto forte é a carga horária que se pode atribuir a cada programa para cada filtragem. Como "só poder navegar 2h / dia, até às 20h", ou "nunca ter acesso à rede P2P com o BitTorrent".

A instalação do *SecureSpot* é quase *Plug-and-play*, dependendo do nível de segurança a aplicar no ambiente em que é ligado. O nível por defeito é o médio, onde todos os *hosts* na rede necessitam correr um *software* específico para se ligarem à Internet. Num nível elevado, não é possível a ligação à Internet numa rede externa sem o *SecureSpot*, sendo necessária a palavra-passe de administrador. No nível baixo, um utilizador poderá ligar-se à internet com ou sem o *software* dedicado. Neste sentido, mesmo o dispositivo de *hardware* fica muito dependente da instalação e configuração de níveis num *software* dedicado, o que torna o produto algo decepcionante, além de que estes níveis de segurança podem ser muito incomodativos para um adulto – não administrador do *SecureSpot* – que leve o seu portátil para o emprego e seja questionado com a palavra-passe para aceder à Internet externa!

Outros dispositivos que não possibilitem a instalação do *software* da D-Link, como PDAs, SO Linux, consolas de jogos, etc., nunca poderão aceder à Internet. A solução para os menores é muito simples: desligar os cabos e fazer ligação directa entre o *modem* e o *router*! Nesta perspectiva, até se teriam de incluir barreiras físicas ao dispositivo.

3.1.5.7. A solução

As inúmeras opções e formas de bloquear conteúdo impróprio, filtrar informações privadas, classificar níveis para diferentes utilizadores e dificultar a desactivação do sistema, juntam-se os actuais "super sumos" nesta área: Têm tanto potencial como o *NetNanny* e o sistema é embutido em *hardware* como o *SecureSpot*, sem *software* que dificulte a tarefa de configuração: São os *iPhantom* e *iBoss,* fabricados pela *Phantom Technologies*. São *routers* com *wireless* e um muito completo sistema de controlo parental. Desligar este sistema implica a ligação directa de um *host* com o modem xDSL, tornando-se a melhor prática para quem leve a sério o controlo parental e, uma vez configurado, não esteja disposto a ter mais chatices.

3.1.6. Universal Plug and Play (UPnP)

O *UPnP* objectiva interligar quaisquer dispositivos, de uma forma dinâmica e directa, ligar-se com a rede LAN em que é aplicado, sem passar por qualquer configuração manual. Esta ideia advém da tecnologia *PnP*, utilizada para interligar dispositivos automaticamente com os computadores, sem necessidades de instalação, configuração ou autenticação. A utilidade do *UPnP* nos ambientes domésticos poderá ser a partilha de dados, comunicações, entretenimento, etc., quase como ligar um dispositivo USB ao computador.

Sendo uma tecnologia ainda recente, existe uma comunidade – constituída por uma larga gama de fornecedores de *hardware* de redes IP (*UPnP Forum* : http://www.upnp.org/) – que discute as vantagens/desvantagens desta tecnologia, novas soluções e métodos de segurança reforçados, aplicando-os em dispositivos de *hardware* já disponíveis no mercado.

A arquitectura do *UPnP* é constida por múltiplos protocolos que suportarão uma rede *zero-configuration*, i. é, sem a necessidade de se configurar quaisquer parâmetros de endereçamento e outros parâmetros de integração na rede. Um dispositivo compatível com *UPnP* poderá receber o endereço IP, anunciar o seu nome, informar as suas capacidades quando requerido e interagir com as capacidades de outros dispositivos *UPnP* na rede. O uso de serviços de DHCP e DNS são opcionais e só serão utilizados se activos na rede e, quando desligados da rede, os dispositivos *UPnP* não deixarão qualquer informação desnecessária.

Outras funcionalidades:

- **Independência dos Dispositivos:** Pode-se utilizar *UPnP* para estabelecer ligação por diferentes interfaces, como a própria rede eléctrica, *Ethernet*, Infra-vermelhos, radiofrequência *WiFi* ou *Bluetooth*, *FireWire*, etc. Não são necessários quaisquer controladores adicionais pois utilizam-se protocolos comuns.
- **Controlos *User Interface*:** Pode-se embutir, nos dispositivos com suporte *UPnP*, um ambiente gráfico acessível por *WebBrowsers*, da mesma forma como os *routers* comercializados o possibilitam.
- **Independência de Sistemas Operativos ou Linguagens de Programação:** Qualquer SO ou linguagem de programação pode ser utilizada para criar produtos de *software* com *UPnP*. Não há barreiras ao uso de APIs, desde que o SO o suporte.

Num ambiente com tais possibilidades, nunca se teria um serviço *Triple-Play* mas "*multi-play*", onde a mesma rede IP suportaria diversos elementos multimédia e respectivos serviços. No entanto, esta possibilidade sai do controlo do provedor, além de lhe criar grandes riscos, referidos e explicados nas páginas seguintes.

3.1.6.1. Ordem de Funcionamento e Protocolos no UPnP

***1. Discovery*:** Quando o dispositivo é adicionado à rede – após recepção do endereço IP – o protocolo *UPnP discovery* permite-lhe dar a conhecer os seus serviços a pontos de controlo na rede. De outra forma, quando um ponto de controlo é adicionado, o *UPnP discovery* permite que o primeiro busque serviços do seu interesse. O essencial, em ambos os casos, é a mensagem de *discovery*, baseada no protocolo *SSDP* (*Simple Service Discovery Protocol*), que contém algumas especificações sobre o serviço oferecido pelo dispositivo. Veja-se o ponto de controlo como um dispositivo com suporte *UPnP* e correndo sob a camada de aplicação.

***2. Description*:** Depois de recebido um SSDP, o ponto de controlo terá de requerer algumas informações extra para melhor definir as capacidades ou interagir com o dispositivo. Para tal, é enviado um *request* destinado ao URL anteriormente definido na mensagem *SSDP*. Este pedido é retribuído em formato XML, com as especificações do dispositivo, o fabricante, modelo, número de série, URLs, etc. Também é incluída uma lista de dispositivos ou serviços embebidos – no caso de um dispositivo modular – e respectivos URL de controlo, eventos e apresentações. Por cada serviço, é incluída na lista os comandos ou acções, que darão resposta do primeiro, e uma lista de variáveis, que definem o estado do serviço durante a sua actividade.

***3. Control*:** Após a assimilação da informação contida no XML, o ponto de controlo poderá enviar acções aos serviços do dispositivo. Estes comandos ou acções são enviados para o URL de controlo do serviço – anteriormente obtido no documento XML – sob o formato de SOAP (*Simple Object Access Protocol*). Como que emulando chamadas a funções, o serviço no dispositivo responderá com o valor especificado para a acção pretendida. Os efeitos das acções são modelados segundo as alterações efectuadas nas variáveis do estado de serviço.

***4. Event Notification*:** Segue-se a notificação de eventos: Se necessário, o ponto de controlo pode subscrever-se para recepção de notificações aquando da alteração de determinadas variáveis do serviço prestado pelo dispositivo *UPnP*. As mensagens de evento são expressas em XML e formatadas usando GENA (*General Event Notification Architecture*), contendo o nome de uma ou mais variáveis de estado e o seu respectivo valor.

Para possibilitar o ponto de controlo de seleccionar as variáveis, é primeiro enviada, do dispositivo, uma mensagem de evento que contém todos os nomes e valores das variáveis que aceitam a notificação. Quando perante cenários com múltiplos pontos de controlo, as mensagens de evento são enviadas com todas as variáveis inventariadas.

***5. Presentation*:** Se o dispositivo adverte um URL de apresentação na sua mensagem de *discovery*, o ponto de controlo pode facilmente carregar o *website* para o seu *browser*. Dependendo das capacidades da página, o utilizador poderá controlar o dispositivo e/ou o seu *status*.

***6. UPnP AV (Audio & Vídeo) standards*:** Existe, nos *standards UPnP*, um grupo constituído por fornecedores e fabricantes que trabalham na indústria do entretenimento doméstico, supervisionados – e seguem as linhas de orientação – pela DLNA (*Digital Living Network Alliance*). Partilham uma visão de "redes com e sem fios que interagem com os diversos aparelhos electrónicos domésticos, computadores, dispositivos móveis, etc., possibilitando um ambiente coordenado para a partilha e crescimento de novos serviços e conteúdos digitais". A DLNA está focada em disponibilizar linhas de orientação para a implementação de *frameworks* capazes da "interoperabilidade digital".

Em 2006, foi anunciado, no *UPnP Forum*, a primeira *release* (já 2ª versão) das especificações para áudio e vídeo (*Enhanced AV Specifications*).

3.1.6.2. Problemas no *UPnP*: Falta de Autenticação

Perante tantas regalias que a tecnologia *UPnP* pode proporcionar, era de duvidar se não vinham vulnerabilidades no pacote: Não está implementado qualquer metodologia para autenticação e só o é quando utilizando protocolos terceiros, como HTTP sobre SSL/TLS ou outros mecanismos embutidos nos dispositivos, ficando a *estandardização* neste ponto muito aquém da unificação desejada. Infelizmente, este cenário não acontece na maioria dos dispositivos, assumindo, por defeito, que o sistema ou utilizadores estão autorizados.

Routers e *firewalls*, sob controlo de um IGD (*Internet Gateway Device*) com UPnP activo, são vulneráveis a ataques pois os *framers* do protocolo estão omissos a aceitar qualquer método de autenticação *standard*. Por exemplo: programas criados com o *Adobe Flash* podem gerar *requests* HTTPU (*HTTP over UDP*, usados no *UPnP*), bastando que o *website* – onde este se encontra – seja acedido. Silenciosamente, poderão ocorrer algumas alterações sobre o *router* do utilizador, desde expor os computadores detrás de uma *firewall* ou rede interna, aceder à administração do *router* e modificar as suas credenciais, alterar as configurações de PPP, IP e *WiFi*, atacar um *host* – a partir do *router* – trocando as informações do servidor DNS e facilitando o manuseamento de *Social Engineering* ao tornar os dados mais credíveis (como aceder a bancos ou adquirir um *hotfix* para o seu *webBrowser* quando se trata de código malicioso), etc. Tudo isto com uma inicial e simples troca da *tag navigateToURL*, forgada e enviada após a recepção de um *requestURL* da vítima.

Os ataques acima descritos não ocorrerão se o IGD não suportar ou tiver o *UPnP* desactivado. Também nem todos os *routers* possuem configurações de DNS *server*, pelo que assim não se poderão associar domínios a endereços IP não correspondidos. Além disso, a modificação de tais parâmetros é opcional no *router* com *UPnP* activo, pelo que se deverá manter a modificação de DNS desactivada. Na verdade, são tantas as incógnitas e pouca confiança no *UPnP*, que por defeito, já vem desactivado nos dispositivos que o suportam.

Mais informações sobre o funcionamento dos ataques UPnP por Flash em:
http://www.gnucitizen.org/blog/flash-upnp-attack-faq/

3.1.6.3. Aplicações de Software com UPnP

As aplicações multimédia como o *Windows Media Player*, desde a versão 9 até à actual versão 11, possuem um sistema de partilha de ficheiros multimédia que pode ser, ou não, activado, possibilitando a qualquer utilizador aceder ao conteúdo. O problema está em que um "qualquer utilizador" pode ser um atacante que saiba explorar as vulnerabilidades da tecnologia UPnP, alargando o acesso a todo o sistema de ficheiros do utilizador.

Como se não fosse grave o suficiente, existem programas de partilha de ficheiros multimédia, ao estilo P2P, que utiliza a partilha UPnP do *Media Player* para este fim, estendendo a entrada do atacante até pela rede externa. Veja-se a aplicação P2P *on2Share*, em http://www.on2share.com/UPnP/.

Também é possível criar-se um *UPnP Media Server*, ou servidor multimédia UPnP, que possibilita a partilha de conteúdos áudio visuais, mas não parecem implementar qualquer tipo de segurança adicional. Vejam-se o *MediaTomb* ou GeeXboX, para Linux e BSD, ou *Allegro* para Windows e Mac OS, em http://mediatomb.cc/, http://ushare.geexbox.org/ e http://www.allegrosoft.com/ams.html, respectivamente.

Também as mais recentes consolas de videojogos, como a PlayStation3 e Xbox 360, possibilitam a exploração de ficheiros partilhados na rede interna por UPnP. Felizmente, esta partilha vem desligada e a sua activação não é tão simples quanto isso. No entanto, com o aparecimento dos *Firmwares* pirateados, que possibilitam o uso de *software* não classificado e aceite pelos fabricantes de consolas, os atacantes podem aproveitar-se destes dispositivos para tomar posse da configuração do *router* e respectivos *PCs.*

3.1.6.4. Devices Profile for Web Services (DPWS)

A tecnologia DPWS define um conjunto mínimo de regras a implementar para um sistema de *WebService* seguro para troca de mensagens de descobrimento, descrição e eventos sobre dispositivos ligados à rede IP. Os objectivos são similares aos de *UPnP*, mas totalmente alinhado à tecnologia de *WebServices* e inclui extensões de integração dos seus potenciais serviços a amplos e diversos cenários nas empresas. Até ao Windows XP, só se encontrava implementada a tecnologia de *UPnP*, mas com o seu fracasso dada a falha de autenticação, já o Windows Vista integra o DPWS como "WSDAPI".

Inicialmente publicadas em Maio de 2004, as especificações de DPWS definem uma arquitectura onde correm dois tipos de serviço:

- Serviços oferecidos (*hosting services*): Associados ao dispositivo e são importantes ao processo de *discovery*;

- Serviços hospedados (*hosted services*): São maioritariamente funcionais e dependem dos serviços oferecidos no *discovery* do dispositivo.

Em adição a estes serviços hospedados, o DPWS especifica um conjunto deles como base para o correcto funcionamento, como o *discovery*, para marcar presença como em *UPnP*, o *Metadada Exchange*, para proporcionar o acesso dinâmico aos seus serviços hospedados e meta data, e *Publish/Subscribe Eventing* para o envio de mensagens de evento assíncronas, anteriormente subscritas pelos pontos de controlo sob um dado serviço hospedado.

Os serviços *standard* do DPWS são: WSDL 1.1, XML *Schema*, SOAP 1.2 e múliplos serviços *Web* (*WS*) como *Addressing, MetadataExchange, Transfer, Policy, Security, Discovery* e *Eventing*. Note-se que nesta tecnologia já se encontram *webServices* para a segurança e aplicação de políticas.

Como o DPWS é um protocolo que suporta *discovery* dinâmico e uma visão de aplicações distribuídas com os *standard* de serviços *Web*, um ambiente automatizado é bastante claro. No *"2007 Consumer Electronics Show"* uma casa *nova-geração* era, conforme as circunstâncias, iluminada automaticamente! O seu sistema de iluminação era controlado pela comunicação com um sistema automatizado que usa DPWS. Mais: o sistema de distribuição de som e o próprio sistema de segurança, como alarme, cameras, etc., estavam igualmente por conta do automatismo do DPWS!

Desde simples controlo termóstato até sistemas de segurança, o DPWS veio para ficar: O espetáculo acima descrito mostrou grande entusiasmo dos clientes, trazendo todas as tarefas domésticas para um ambiente de entretenimento digital.

Já muito foi projectado e criado para as casas do futuro, e nunca tanto como agora, com resultados a olhos vistos. O projecto de investigação europeu SOCRATES, composto por grandes empresas como ABB, SAP, *Schneider Electric* e *Siemens*, estão focados em implementar e testar um protótipo para possibilitar dispositivos DPWS num domínio inteiro automatizado. Outros projectos estão presentes, como SODA (da europeia ITEA), SIRENA, etc. Mais informações em "*Web Services for Devices* - www.ws4d.org".

3.2. Segurança Remota

É possível gerir-se todo o *hardware* e *software* de um qualquer *host* por acesso remoto. Estes métodos, quando bem aplicados, são extremamente úteis à gestão de uma rede empresarial ou até, em serviços *Triple-Play*, em redes domésticas monitorizadas pelo ISP, considerando-se como uma nova "camada ubíqua" de manutenção. No entanto, também se abre um novo leque de possibilidades aos *hackers*!

3.2.1. Windows Management Instrumentation (WMI)

O WMI é a implementação da Microsoft dos projectos de estandardização *WebBased Enterprise Management* (WBEM) e *Common Information Model* (CIM) da DMTF (http://www.dmtf.org).

Nos Sistemas Operativos Windows (desde o *Windows NT 4.0*), existe uma componente de controlo remoto designada de WMI. É um conjunto de extensões para o modelo de controlo do Windows que oferece uma interface para aceder as informações e notificações presentes no SO de *hosts* remotos. Para tal, podem-se criar tarefas com linguagens de *script*, como VBScript ou *Windows PowerShell*, e agendá-las para eventuais registos de monitorização.

Desde a era do Windows NT 4.0, muitos comandos foram adicionados ao ambiente WMI, mais especificamente de apenas 15 para quase 100 (Windows Vista), com mais umas quantas adicionadas ao WindowsServer2008 para controlo de, por exemplo, o servidor Web ISS7, o uso de virtualização, etc. Com esta rápida expansão, os líderes no mercado de *software* de gestão distribuída suportam WMI aplicados em GUIs mais amigáveis, facilitando a vida aos administradores de sistema que não estejam tão ambientados às linhas de comando WMI.

3.2.1.1. Potencial do WMI

Capacidades Remotas com DCOM e SOAP: O sistema WMI utiliza, para comunicação entre aplicações, as tecnologias *Component Object Model* (COM), *Distributed COM* (DCOM) e um modelo mais standard: SOAP. O último estende o suporte de WMI a diferentes aplicações de *software* – e respectivos GUIs – que não sejam *.NET*.

Suporte a *Queries*: Utiliza-se uma linguagem de *queries* dedicada: *WMI Query Language* (WQL), que é o formato ANSI SQL mas com a semântica alterada (mas mantendo a linha standard) para aceitar técnicas de enumeração em resposta a comandos WMI.

Capacidade de Eventos: Podem-se criar/configurar eventos, ocorridos num ou mais *hosts*, do interesse do administrador. Para tal, utiliza-se uma *query* WQL e o tipo de notificação esperada. A gestão dos eventos definidos faz parte de interfaces *Automation* no WMI, não havendo qualquer custo ou notoriedade no *host* monitorizado.

Gerador de código padrão (*Template*): Para acelerar o processo de escrita de comandos WMI e interfaces COM/DCOM, foi desenvolvido o *WMI ATL Wizard*. Esta ferramenta

gera um padrão de códigos – introduzidos pelo administrador – e implementa novos comandos WMI.

Previsibilidade: Possibilita, a pessoal especializado em outras interfaces de gestão, aplicar as mesmas técnicas intuitivamente, sem ter de começar do zero e perder tempo a adaptar-se a novas heurísticas, aumentando o *Return of Investment* (RoI) do pessoal (COM / DCOM, *Automation*, *.NET*).

Modelos de Administração Lógicos Unificados: Como dito anteriormente, o modelo WMI baseia-se no standard CIM, definido pela DMTF. O *schema* das classes-base no CIM é definido por um consórcio de casas de *software development* (neste caso, IBM, MOM, SMS, etc) que respondem às necessidades da indústria.

3.2.2. Sistema Operativo Linux – Interpretação de Comandos WMI

Os Sistemas Operativos Linux não incluem embutido nenhum sistema de gestão que aceite WMI. No entanto, é possível instalar *software* que o faça, entre os quais estão dois da *ManageEngine* (http://www.manageengine.co.uk/):

- ***OpManager:*** Permite uma visão completa do que ocorre na rede com base no protocolo SNMP. Possibilita a monitoração de CPU, Memória, HD, Processos, Serviços. Suporte a MIBs (Management Information Base), etc. e a criação de relatórios de utilização e disponibilidade de recursos. É um *software* "100% web-based" e suporta SNMP, WMI, CLO, Telnet, SSH entre outros, por vezes, sendo necessário aplicar-se *patches* para diferentes protocolos de gestão.
- ***ServiceDesk Plus*:** *Software* "100% web-based" que permite services de *Help Desk* e gestão de *hosts*. Realiza rastreamento a *hosts*, pedidos de utilizadores, manutenção de licenças, uso de base de dados, etc. Enquadra-se num ambiente de TI com as boas práticas ITIL. Esta ferramenta é uma *Suite* que inclui, indirectamente, o *OpManager*.

3.2.3. Aplicando WMI ou Outros Protocolos de Gestão Remota

- No ambiente *Triple-Play*

Com a largura de banda atribuída aos clientes com pacotes *Triple-Play* (a rondar os 24Mbit), os protocolos de gestão remota terão de ser obrigatoriamente empregues, não só para defesa do ISP, como para oferta de serviços de segurança e manutenção!

3.2.3.1. Monitorização

A solução inicial para sistemas de monitorização e controlo remoto foi desenhada segundo normas OSI. Dada a sua complexidade (para variar…), foi implementado um protocolo simplificado: SNMP, protocolo com algum tempo e, actualmente, já embutido em todos os

dispositivos de *hardware* com camada de aplicação (dispositivos c/ SO*, gateways* ou *routers*), o que garante alguma monitorização para qualquer provedor, se se puder chamar, "mais cauteloso" com os dispositivos fornecidos aos seus clientes.

Infelizmente, a implementação do WMI não acontece como o SNMP, provavelmente devido à sua ainda pouca força de expressão. Não estando presente nos *hosts* do utilizador final, o provedor de serviços pode, distribuir o *Gateway CPE-Gateway* (principal) e respectivos CPEs de serviços (telefones, *routers*, *STB*s, etc.) com o WMI pré-instalado. Assim, poder-se-ão criar novos serviços de monitorização e segurança para os seus clientes, automatizando eventos de novas actualizações de *firmwares*, *drivers* ou até *software*, num nível de detalhe muito superior ao do SNMP!

Um cliente que adira aos serviços do WMI terá os seus computadores configurados para aceitarem esta leitura remota. Eventualmente, com auxílio/administração *on-line*, o provedor poderá disponibilizar *patches* que configurem automaticamente o serviço WMI a favor do primeiro.

Por último, o cliente terá de estar ciente das informações que entrega ao provedor, pois a nível de *software*, muito mais se vai saber para além de simples valores estatísticos! Sacrifica-se alguma privacidade para maior segurança.

3.2.3.2. Vulnerabilidades

Qualquer protocolo ou ferramenta de gestão remota tem as suas vulnerabilidades. Um *hacker* só terá de descobrir a falha antes que seja aplicada um *patch* que a cobra. Nem o SNMP, nem o WMI, são excepção. Inclusive as *Suites* de *Internet-Security* já rastreiam o código proveniente do WMI para assegurar que o código VB não é um potencial *trojan* ou outro tipo de *malware.* Houve até, no WMI do Windows XP, uma vulnerabilidade de *DoS* quando recebendo demasiados RPC, posteriormente corrigida por um *hotfix*. Pacotes mal formados e uso de ActiveX (VisualStudio) podem originar o *exploit* do sistema de monitorização se um utilizador mal intencionado conseguir compreender tais falhas. Mais informações em http://secwatch.org/.

Nota sobre os Próximos Capítulos: *Particularidades das Redes Triple-Play*

Apesar da rede *Triple-Play* ser como qualquer outro tipo de rede comutada em pacotes, onde existe também a entidade do ISP, esta possui algumas particularidades nos seus requisitos de segurança. O levantamento de requisitos é feito para os serviços seguintes serviços:

- **VoIP**: Voz sobre IP;
- **IPTV**: Televisão sobre IP.

Para transmissão de dados, os requisitos levantados nos capítulos anteriores são suficientes para tornar o ISP mais seguro e com garantia de satisfação do cliente.

4. VoIP

A implementação da tecnologia de voz sobre IP (VoIP), no esforço de reduzir o preço das comunicações, já deixou, à muito, de ser um "projecto científico", como era normalmente visto há seis ou sete anos atrás, sendo um grande passo para a qualidade de serviço no mundo das chamadas telefónicas. Como se utiliza a rede IP da Internet, a qualidade de serviço e os custos reduzidos são grandes vantagens e apresentam-se como os pontos que mais favorecem a "conversão" dos utilizadores da rede telefónica tradicional.

A tecnologia VoIP transporta o sinal de voz numa rede de dados (de pacotes comutados) via Internet. A voz é tratada como qualquer outro pacote de dados, com ênfase num algoritmo de compressão visando a optimização no uso da largura de banda disponível e, consequentemente, aumentar a quantidade de chamadas de voz numa dada largura de banda e até, como rede de dados que é, possibilitar serviços de comunicações unificadas (tipo *multicast*). Comparando com a rede tradicional de circuitos comutados, o VoIP tem, claramente, grandes vantagens. Nisto, muito se desenvolveu na oferta de diferentes serviços associados ao VoIP, mas, infelizmente, foi-se deixando a segurança para segundo plano, dado que primeiramente, estes serviços só rodavam em redes internas empresariais.

A segurança aplicada em VoIP era vista muito superficialmente até há pouco tempo, quando surgiu a ideia de expandir esta tecnologia como substituição às redes telefónicas tradicionais, tanto a nível empresarial (onde já existe há alguns anos) como em serviços públicos domésticos, para onde se está a expandir. No fundo, acaba por seguir os mesmos passos do correio electrónico e, como tal, as preocupações com a segurança e privacidade contra terceiros publicitários ou mal-intencionados foram colocadas para primeiro plano ainda antes da expansão do VoIP no mercado.

4.1. Segurança em VoIP

A junção do mundo das chamadas de voz com o de transmissão de dados levará a que o primeiro se envolva nos riscos de segurança já existentes no segundo: Segundo *David Krauthamer,* director de IT na empresa *Advanced Fibre Communications Inc.* (AFC), no artigo *ComputerWorld Executive Bulletin: IP Communications*, garantir a segurança no tráfego de voz na rede IP não é tão diferente da segurança garantida nos pacotes de dados comuns e a segurança que se lhe aplica deve ser manuseada no contexto geral da segurança aplicada à rede, com pouca ou nenhuma especificação dedicada. Para já, a AFC só utiliza comunicações VoIP na rede interna da empresa.

Como em qualquer comparativo de *hardware* e *software,* o uso de telefones VoIP sobre uma aplicação de *software* pode originar perigosas vulnerabilidades. Um utilizador mal intencionado poderá utilizar o *software* para, por exemplo, forçar uma *firewall* com o envio de pacotes para diferentes portos e provocar um *exploit*.

Mais uma vez, a melhor forma de se combater estas falhas será utilizando uma *Access list* e garantir que todo o tráfego VoIP da rede interna é enviada por um *gateway* VoIP, sem ter de passar directamente pela Internet. No caso das redes LAN domésticas, quando se realiza uma chamada nacional, a ligação do ISP ao *gateway* VoIP seria imediata, sem passar na Internet. No

entanto, em chamadas internacionais, o custo só será reduzido se, primeiramente, os pacotes forem enviados por IP até para à região pretendida e só depois ligar-se ao *gateway* VoIP. O ISP poderá disponibilizar uma ligação VPN a cada *gateway* para as chamadas internacionais, garantindo a segurança e privacidade do conteúdo corrente entre estes pontos e, mesmo com a largura de banda ocupada com maiores pacotes (dada a encriptação), o facto de não se realizarem muito deste tipo de chamada torna esta implementação numa mais-valia.

4.1.1. Ameaças de Segurança em VoIP

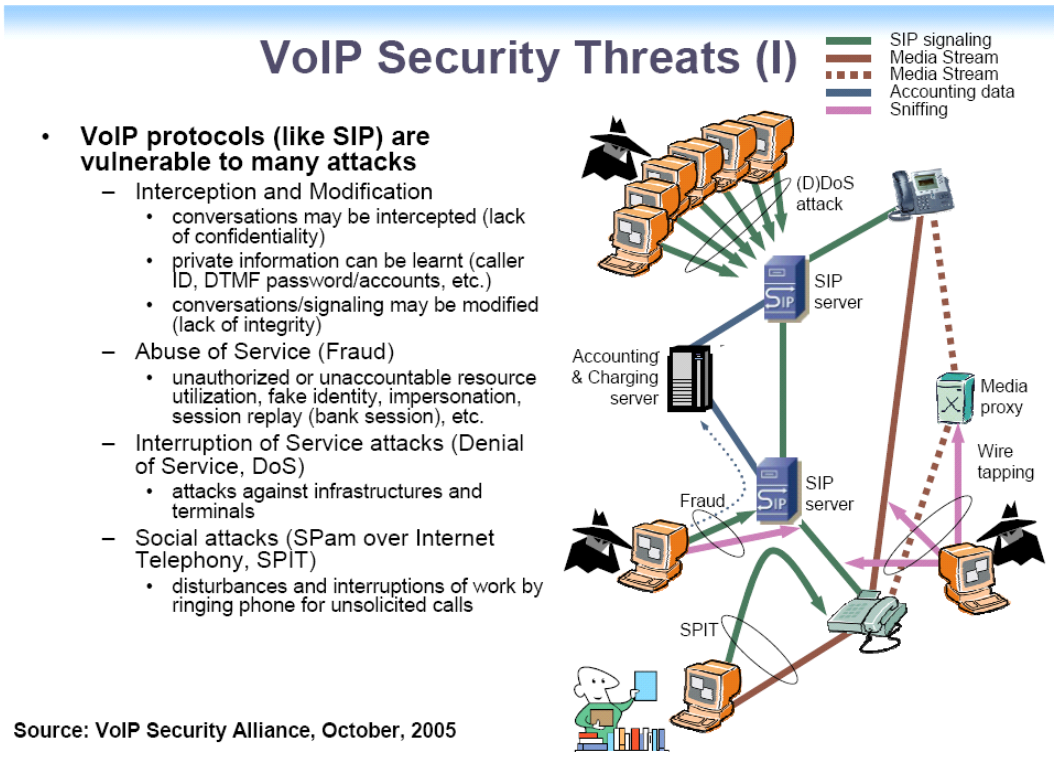


Fig. 18

Vectores de Ataque: (D)DoS ao servidor ou *gateway* VoIP, dispositivos finais (CPE), problemas na comunicação inter-procotolos, evasão de Contas (Pagamentos) e roubo de identidade, privacidade, etc.

Muitas das vulnerabilidades de segurança, já conhecidas da rede de dados, podem criar disturbação na rede VoIP. A procura pela solução tem de ser encontrada para vários casos, principalmente aos que se apontam abaixo:

- Ataques *Denial of Service* (DoS): Os telefones IP, *Gateways* VoIP (*proxies* SIP), servidores VoIP, etc., podem ser bombardeados com pacotes de sincronização (SYN) ou de controlo (ICMP) na tentativa de impedir terceiros autorizados de receberem os serviços provenientes da entidade alvo.
- Intercepção de Chamada: Monitorização de pacotes de voz ou RTP não autorizado.
- Adulteração do Protocolo: Dentro da categoria da intercepção de chamada, um atacante pode monitorizar e capturar os pacotes que preparam a chamada, processo que ocorre

depois da marcação e antes da chamada. Esta acção modifica os parâmetros necessários ao estabelecimento da comunicação, levando à ocorrência de chamadas internacionais, realizar chamadas sem utilizar o dispositivo VoIP, etc., levando o PBX-IP a acreditar que (e cobrar) a fonte tem origem num utilizador presente na sua lista.

- Roubo de Identidade: Quando um atacante altera o destino/origem e faz-se passar por outra pessoa.
- Fraude: Quando utilizadores maliciosos ou intrusos colocam chamadas fraudulentas na conta de outrem.
- Sistemas Operativos: O *software* que gere as várias chamadas de sistemas PBX-IP está assente e depende de Sistemas Operativos e/ou os seus componentes que poderão conter vulnerabilidades. Por exemplo, o uso de *Microsoft IIS* (ou Apache) como uma ferramenta de configuração de serviços *Web* para PBX-IP pode introduzir algumas vulnerabilidades ao ambiente VoIP.

Como é impossível eliminar todas as ameaças acima descritas, deve-se, pelo menos, seguir alguns passos que objectivam conter algumas destas falhas. Para isto, é imperativo que o responsável pelo equipamento busque por informação! Não falta documentação sobre como minimizar a exposição do *host* a diversos tipos de ataque em diferentes equipamentos e *software*. As comunidades de diversos *softwares* de serviços disponibilizam linhas de orientação específicas para contornar as vulnerabilidades favoráveis a DoS. Tomar conhecimento e aplicar estes "tutoriais" tornará a rede menos vulnerável aos diversos ataques. O Adultério de Protocolo, referido anteriormente, pode ser considerado um ataque DoS, dependendo da forma como é executado.

4.1.2. Ultrapassando as Ameaças

4.1.2.1. Passo a Passo para Configurar uma Rede VoIP

Escolher equipamento telefónico VoIP correctamente

Existem prós e contras em todos os protocolos VoIP e respectivos fornecedores do equipamento. Conforme as necessidades e especificidades da implementação VoIP do provedor, um cliente deverá informar-se do correcto equipamento a adquirir quando este não é já fornecido pelo ISP. Não tendo noção do que ocorre por detrás da rede, o cliente só deve comprar novos dispositivos VoIP pela loja do seu provedor, mesmo que existam outros com os mesmos protocolos.

Desligar protocolos desnecessários

Existem mais que suficientes vulnerabilidades desconhecidas associadas a cada protocolo VoIP que podem ser exploradas facilmente. O cliente VoIP não quererá aumentar o leque de possibilidades de um *hacker*, daí só dever ficar ligado o mínimo indispensável para o correcto funcionamento do protocolo escolhido e utilizado pelo ISP.

Elementos da infrastrutura VoIP podem ser acedidos e atacados

Podem parecer telefones normais ou terminais comuns, mas cada elemento é um serviço de *software* a correr num dispositivo com Sistema Operativo embutido e uso de protocolos de comunicação TCP e UDP sobre IP. Com a constante actualização dos serviços, muitos pontos estarão desactualizados e a rede nunca estará segura. Ao cliente, não lhe resta senão fiar-se na politica de actualizações do seu provedor.

"Dividir e Conquistar" nas redes VoIP

É recomendado separar a rede VoIP das redes de dados, mesmo que o aparecimento desta estrutura tenha sido para "poupar gastos de *hardware* e redes". É possivel, contudo, separá-las de uma forma lógica, configurando-se redes virtuais, com diferentes endereços e mantendo-se a estrutura física da rede.

Autenticar Operações Remotas

Os protocolos de VoIP, como o SIP, podem requerer várias camadas de autenticação, cada uma atribuída a um nó (*proxy*) responsável pela ligação de voz. Do ponto de vista do provedor, também estes terminais podem ser remotamente geridos e actualizados. Para tal, devem-se assegurar as politicas de segurança e encriptação para garantir que só pessoal autorizado terá acesso a tais parâmetros, baseando-se na identificação do IP, MAC-Address e *username* unicos. A última coisa que se quer é um atacante capaz de manusear os serviços VoIP remotamente.

Separar a rede VoIP da Rede Interna

Muitos dispositivos de segurança não compreendem ou não são compativeis com o correcto funcionamento de comandos de sinalização VoIP, como o abrir e fechar portos, utilizar diferentes protocolos, etc. O resultado serão portos abertos dinamicamente e, não estando o dispositivo preparado para os fechar após o seu uso, ficam estes "buracos" que facilitam a vida a atacantes (sem muita experiência) ou para uso de ferramentas maliciosas, possibilitando diversos tipos de ataque DoS nestes portos "esquecidos". Neste sentido, será bom separar a rede interna da rede VoIP. Em serviços *Triple-Play*, os clientes já terão as redes separadas por um *gateway* que distingue os serviços, além de que estará preparado para responder ao fecho de portos abertos dinamicamente pelo dispositivo VoIP. Contudo, o meio por onde é transmitido até ao ISP é único, e as redes virtuais serão benvindas para a separação virtual.

Sistema de Segurança VoIP Monitorizando os Portos de Comunicação

Fazer a leitura do pacote de sinal dá-nos a informação dos portos seleccionados para criar o *socket* para a comunicação entre dois ou mais pontos. É importante que o sistema compreenda a ordem de acontecimentos e operações dos protocolos VoIP, caso contrário um simples ataque DoS com pedidos de fecho de sessão irão desligar todas as chamadas que o servidor alvo assegura.

Utilizar *Network Address Translation* (NAT)

Em alguns casos, apesar de ser mais seguro o uso de NAT, são colocados problemas específicos na rede VoIP: O NAT converte endereços de uma rede interna num único endereço IP externo para o *routing* pela internet. O conteúdo dentro do empacotamento não é avaliado e, por consequente, as soluções de segurança não permitirão realizar a chamada senão estiverem preparadas para tal, impedindo um contacto externo de detectar outro numa rede interna com NAT.

Uso de Sistemas que Efectuem Verificações de Segurança Específicas para VoIP

O sistema deverá ser capaz de olhar o *stream* VoIP, analisar o estado da chamada e constar que o conteúdo nos parâmetros destes pacotes são consistentes e fazem sentido segundo as necessidades atribuídas ao cliente ou empresa.

4.1.2.2. Reforçando a Rede VoIP

Abaixo, algumas boas práticas para uma segurança reforçada no sistema VoIP:

LANs Virtuais

Mesmo usando a mesma rede, separar a voz dos dados, através de uma rede virtual, será boa ideia para aumentar a eficiência, oferecendo melhor qualidade de serviço (QoS) e segurança, adicionando-se outra camada de complexidade, dificultando a vida ao atacante que deseje escutar (*sniff*) ou capturar pacotes de voz a partir da rede de dados.

Uso de equipamentos não autorizados ou a acção de *spoofing* (personificação) podem ser mitigados se o *router* ou *switch* puder negar o encaminhamento de pacotes com *MAC-Address* e endereço *IP* que não coincidam com a lista de "dispositivos reconhecidos". No entanto, esta medida invalida para telefones virtuais (*soft phones*) a correrem num PC, visto que estes são dispositivos autorizados que residem na camada de dados (separados pela *Virtual LAN*).

É bom ler-se o RFC 1918 para a alocação de endereços em redes privadas, neste caso, associados aos telefones por IP, tornando a busca por dispositivos de voz muito difícil e garante que os pacotes nunca possam ser reencaminhados para fora da rede interna.

Sistemas Operativos e Servidores

No mundo VoIP, os PBX (*private branch exchanges*) tradicionais são substituídos por *PBXs IP* em servidores correndo o Windows NT ou outro OS proprietário, alvo susceptível a ataques de vírus e *hackers*, além de ataques DDoS. A intrusão nestes servidores resulta na perda ou comprometimento da máquina a dados sensíveis. Consequentemente, é importante que tais equipamentos estejam devidamente separados da rede externa, utilizando-se *firewalls* actualizadas e monitorização contínua usando sistemas de detecção de intrusão (IDS).

É aconselhável que nenhum outro serviço (como FTP e Telnet) seja instalado e disponibilizado nos servidores que gerem as chamadas VoIP. Contudo, é necessário ter a certeza que desactivar serviços não irá, inadvertidamente, desabilitar o sistema VoIP. Apesar de um administrador

pensar que o serviço de HTTP não é necessário e desactivá-lo, este poderá ser uma componente necessária para configurações remotas ou de administração da chamada, utilizado pelo SIP para trocar parâmetros de autenticação, abrir e fechar portos, etc. O ideal será, antes de se desactivarem todos os outros serviços independentes do VoIP, informar-se dos serviços a que o sistema VoIP assenta ou os tenha como componentes à comunicação ou configuração das chamadas.

Gateways PSTN-VoIP

Quando o VoIP é usado externamente, os *gateways* que convertem os pacotes de dados da rede IP para sinal de voz aceite nesta outra rede. Quando usando VoIP internamente, o *gateway* fará o roteamento da vos, empacotada e comprimida no formato de dados, para o destino IP. Neste processo, os *gateways VoIP* também têm potenciais pontos fracos. Por exemplo, se ocorrer uma intrusão de terceiros, com a finalidade de realizar chamadas telefónicas gratuitas. A protecção ao caso indicado baseia-se numa lista de controlo de acesso restrito, para que só pessoal desta lista estão autorizados a fazer e realizar chamadas VoIP. Equipara-se à lista negra utilizada em SMTP.

Como na telefonia tradicional, a escuta é uma preocupação para qualquer organização ou utilizador privado, com consequências ainda mais graves. Como a voz é enviada em pacotes de dados, atacantes poderão utilizar *software* de *sniffing* de dados ou outras ferramentas com a finalidade de identificar, modificar, guardar e permitir a terceiros escutar as conversas na rede. Mais ainda, um atacante que ganhe acesso a um *stream* VoIP poderá escutar muitas mais chamadas, comparando ao sinal de voz não comprimido da telefonia tradicional.

Encriptação

A encriptação do tráfego VoIP evita a intercepção do conteúdo dos pacotes. Antigamente era mais difícil aplicá-la, pois dependiam de uma maior e mais bem aproveitada largura de banda, desenvolver melhores algoritmos de compressão e processamento mais rápido na encriptação/desencriptação dos pacotes em tempo real. Felizmente, os rápidos avanços no processamento de sinal digital favorecem o uso de encriptação, juntamente com as novas capacidades presentes nos dois protocolos chave do VoIP: SIP e H.323.

Quando realizando chamadas para o exterior de um domínio ou LAN, encriptar os dados de voz e isolar o tráfego VoIP, transmitindo-o por VPN, seria um possível cenário para mitigar riscos de segurança. No caso de uma rede interna empresarial, a encriptação também deverá ser utilizada nas chamadas internas.

Voice Proxy Firewalls c/ MGCP

Se o tráfego VoIP atravessar uma *firewall,* esta deverá suportar os protocolos SIP ou H.323. Quando é necessário "abrir" manualmente um porto para algum destes protocolos, então esta *firewall* não suporta adequadamente o sistema VoIP.

O uso de *gateways* multimédia ou *proxies* revertidos, com suporte aos recentes protocolos *Media Gateway Control Protocol* (MGCP), *Signaling Connection Control Part* (SCCP) ou *Session Initiation Protocol* (SIP), facilita o manuseamento e segmentação de pacotes VoIP dos outros pacotes de dados. O uso destes dispositivos oferecem maior segurança, possibilitando, após uma autenticação reforçada, abrir e fechar portos conforme necessário e são desenhados para gerir e manusear o sistema VoIP de forma mais eficiente que outras *firewalls* tradicionais. É igualmente importante que as *firewalls* aceitem a configuração de fecho de portos quando

não utilizadas por algum período de tempo, possibilitando fechar os serviços de MGCP e SIP após, por exemplo, 5 minutos em *idle*.

Assegurar os Servidores que Encaminham Pacotes VoIP

Aos utilizadores mais experientes, podem realizar um *scanning,* com *software* comercial, para detectar os nós e servidores que manuseiam as sessões da sua chamada e identificar possíveis falhas. Se tal ocorrer, deve-se contactar de imediato o responsável pelo equipamento e exigir, se possível, a correcção da falha. Só devem ser detectadas portos abertos para serviços de VoIP ou componentes necessárias como o *http*.

Serviços de Monitorização

Completando a monitorização aos portos activos no sistema de VoIP, torna-se importante estabelecer-se metas de actividade diária, semanal e mensais. É uma boa actividade para o correcto funcionamento do sistema e rápida detecção de potenciais ataques.

Fraudes

Para imunizar a rede VoIP contra fraudes, é importante que os administradores do PBX-IP imponham as mesmas regras colocadas nos PBX-TDM (*Time Division Multiplexing*). Mesmo os números de chamadas internacionais (cerca de 900 de prefixo) devem ser colocados no PBX-IP. Deste modo, o sistema só será vulnerável a ataques populares "*phreaking*" (*phone freak*) ocorrentes nos sistemas TDM.

4.2. Protocolos VoIP: H.323 & SIP

4.2.1. H.323

O H.323 é uma especificação para comunicações de audio e vídeo através de uma rede de pacotes [33]. Sendo assim, o H.323 é um conjunto de padrões que envolve diversos protocolos, incluindo o H.225, H.245 e outros. A figura a seguir representa os elementos envolvidos em uma arquitetura H.323.

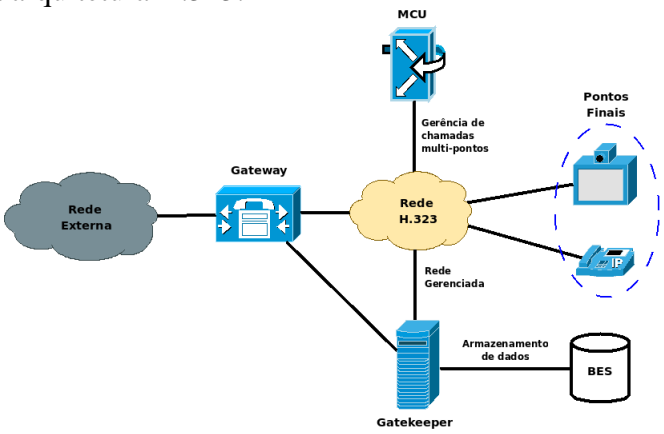


Fig. 19 - Arquitectura VoIP H.323

A arquitectura da rede H.323 é composta por diversos pontos finais, um *gateway*, possivelmente, um *Gatekeeper*, unidade de controlo de multi-pontos (*Multipoint Control Unit* - MCU) e um BES (*Back End Service*). O *Gatekeeper* é um dos principais componentes na arquitectura, pois processa a resolução de endereços e controlo de largura de banda, além de gerir os dados dos pontos finais através de BES, como permissões, serviços e configurações. O *gateway* oferece uma ponta entre a rede H.323 e outras redes "possivelmente não H.323", como uma rede SIP ou outra do sistema de telefonia pública (*Public Switched Telephone Network* – PSTN). Os elementos presentes na arquitectura são as MCU, um elemento opcional que facilita a realização de conferências entre dois ou mais pontos finais.

A cada nova versão do H.323, novos perfis de segurança são definidos. Tal é necessário já que o seu padrão, por si só, não define a segurança do ambiente. Os perfis de segurança oferecem diferentes níveis e descrevem diversas possibilidades, como criptografia do sinal digital (ou analógico) e autenticação entre os elementos da arquitectura com ou sem uso de certificados digitais.

O uso de alguns elementos de segurança de rede, como *firewalls*, que, como já referido, pode causar certos problemas no uso de redes VoIP utilizando H.323, pois a maior parte do tráfego é encaminhado através de portos dinâmicos. O problema surge quando há *firewalls stateless*, que não podem compreender o tráfego relacionado ou as respostas. A solução seria configurar "praticamente 10 mil portas UDP diferentes" no *firewall*, o que, com certeza, iria gerar sérios problemas de segurança. Na versão 5 do H.323 foram implementadas comunicações por túneis (VPN / comunicação encriptada) através do protocolo H.450.6.

As *firewalls statefull*: estas conseguem entender, sem grandes problemas, o tráfego VoIP do H.323. Este é codificado utilizando o formato binário ASN.1. Porém, não segue à risca este padrão, já que em diferentes instâncias da aplicação, podem ser negociadas diferentes opções. Sendo um protocolo binário, tal resultará num conjunto de bytes diferentes, mesmo quando informação a ser transmitida é de um mesmo tipo já existente em ASN.1. Este nível de complexidade não permite que simples ferramentas sejam utilizadas para descodificação do sinal, como filtros de pacotes ou *firewalls*. A existência de um analisador de tráfego no percurso do fluxo pode gerar atrasos num sistema tão sensível a tempos de espera, sendo a protecção contra possíveis atacantes, que tão rapidamente avançam à procura de vulnerabilidades, será atrasada neste ambiente.

O recurso de NAT, bem empregue por critérios económicos e de segurança, pode ajudar a esconder a topologia das redes. No entanto, é particularmente problemático para sistemas VoIP utilizando configurações de chamadas do H.323. Tal ocorre porque o endereço IP interno – e os portos especificados nos cabeçalhos H.323 – não serão os utilizados pelo terminal remoto para responder à mensagem. Para que este problema não impossibilite o uso do H.323, é necessário que o dispositivo NAT possa reconfigurar o endereço no fluxo de controlo, e não apenas lê-lo e enviá-lo para os pontos finais.

4.2.2. SIP: Session Initiation Protocol

O protocolo SIP foi especificado pelo IETF para gerir o início e fecho de sessões VoIP. É considerado mais simples que o H.323 – pois trabalha a nível da camada de aplicação – apesar de possuir uma das RFCs (*RFC 3261*) mais longas do IETF.

Para começar, o SIP é baseado em texto ASCII nas transmissões, ao contrário do que ocorre com o H.323, que utiliza o padrão binário ASN.1. Outra diferença entre os dois padrões surge quanto ao uso dos portos, já que o SIP apenas usa um porto para as comunicações. Como parte inerente da sua arquitectura de segurança, utiliza-se o protocolo S/MIME.

Na verdade, o SIP pode ser utilizado com uma infinidade de protocolos, pois comunicando-se pela camada de aplicação, é independente das tecnologias envolvidas nas camadas inferiores: Pode-se utilizar SIP com TCP, UDP ou SCTP, dependendo das necessidades de transmissão: UDP para transmissões mais sensíveis ao tempo de transmissão, TCP quando a encriptação SSL/TLS está incorporada nos serviços de segurança, ou o SCTP (*Stream Control Transmission Protocol*), desenvolvido especificamente para transporte de sinalização, com maior resistência a ataques de negação de serviço – através de ligações estabelecidas em quatro vias –, habilidade *multi-home* e a possibilidade de enviar vários pacotes num mesmo datagrama SCTP. De modo a incrementar a segurança, é possível o uso do SCTP também sob TLS ou *IPSec*.

A arquitectura da rede SIP é algo diferente da H.323. É antes constituída de pontos finais, um *proxy* e/ou um servidor para redireccionamento, um servidor de localização e o *"registrar"*. O utilizador dá inicio ao processo de estabelecimento de ligação, anunciando a sua localização para o *"registrar"*, que pode ser integrado com o *proxy* SIP ou o servidor de redireccionamento. Esta informação é então armazenada no servidor de localização externo. As mensagens entre os pontos finais são encaminhadas através de um *proxy* SIP ou outro comum. Estes reencaminham as mensagens dos pontos finais (ou outros serviços), verificando os campos de destino, comunicando-se com o servidor de localização para requerer o endereço do destinatário e, assim, repassar a mensagem para o ponto correcto ponto final ou outro *proxy*.

A diferença entre *proxies* SIP e os *proxies* comuns é a atribuição da responsabilidade de transmissão, onde o segundo deixa tal ordem com os pontos finais, já que estes obtêm o endereço do destino e os devolvem aos pontos finais de maneira que possam enviar directamente ao destinatário. A figura abaixo ilustra a relação existente entre as entidades SIP.

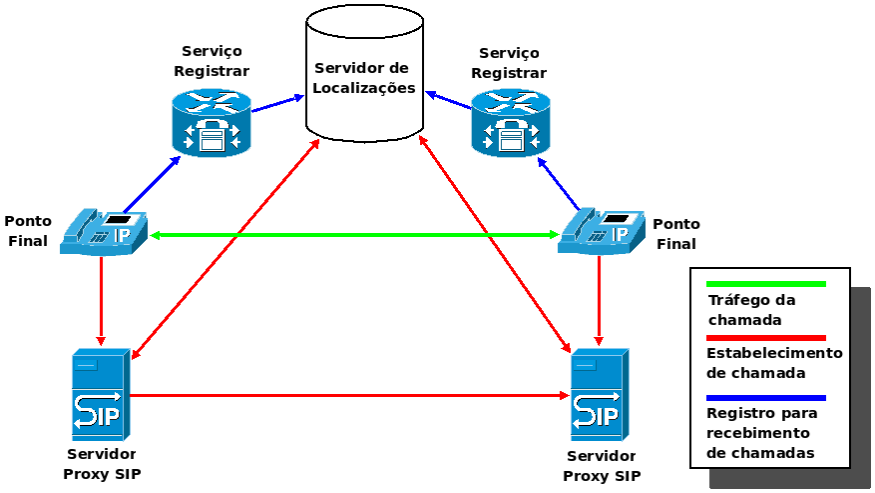


Fig. 20 - Arquitectura VoIP: SIP

Existem alguns mecanismos de segurança que são incorporados ao SIP original, como uso de PGP e autenticação *cleartext* sobre HTTP (RFC 2543), porém seu uso não é recomendado, já que existem melhores alternativas:

- **Autenticação dos dados de sinalização utilizando algoritmos *digest* sobre HTTP**: Mecanismo de autenticação baseado no desafio pela parte remota ao nó que se deseja autenticar. Esse desafio é baseado no envio do *checksum* e palavra-passe do utilizador através de um método HTTP, recomendado para substituição da autenticação por simples HTTP, onde as palavras-passe são enviadas em *cleartext*.

- **Uso de S/MIME com SIP**: O SIP carrega mensagens MIME. Como o próprio MIME já possui mecanismos de protecção para integridade e encriptação de conteúdo (S/MIME), não haverá problemas de maior na integração e uso desta tecnologia no SIP. O cabeçalho SIP é protegido num túnel que pode ser criado com o uso de pares de chaves, presentes em certificados mais comuns.

- **Confidencialidade do meio**: O SIP por si só não realiza criptografia do meio a transmitir os dados. Porém, com o uso da criptografia do RTP (*Real-time Transport Protocol*), a confidencialidade do meio se torna mais garantida. Outra possibilidade para criptografia do meio é através do uso do SRTP (*Secure Real-time Transport Protocol*).

- **TLS com SIP**: O uso de TLS é recomendado para os *proxies SIP*, servidores de redireccionamento e "registrars" para proteger a sinalização SIP. No entanto, só poderá ser aplicado quando sob TCP para transporte dos datagramas.

- ***IPSec* com SIP**: O *IPSec* pode ser utilizado com o SIP, garantindo a segurança na camada de rede. Este cenário é mais comum quando existe uma VPN interligando os nós envolvidos na comunicação, entre pontos finais, *proxies* ou domínios. O *IPSec* pode ser utilizado com UDP, TCP e SCTP nas comunicações SIP, oferecendo autenticação, integridade e confidencialidade dos dados transmitidos, de um telefone ao outro, "*hop-by-hop"*.

Além dos métodos descritos, existem outros que são (ou serão) padrões definidos pelo IETF, tais como o S/MIME com AES, gerir identidade e segurança *end-to-end*, *middle-to-middle* e *middle-a-end*. É importante compreender-se que assim que como o H.323, o SIP possui algumas particularidades que poderão acartar problemas sob alguns dos meios de segurança hoje implementados nas redes IP: Só as *firewalls statefull* conseguem monitorizar o tráfego SIP e determinar os portos a serem abertos após o estabelecimento de sessão, aquando da troca de pacotes RTP (*Real Time Protocol*).

Como em H.323, o grande problema do SIP ocorre perante o uso de NAT, já que este inibe os registos de endereços IP internos, necessários à comunicação VoIP. Só será possível quando o NAT não modifica os portos, liberando a troca de mensagens.

4.3. Spam over Internet Telephony (SPIT)

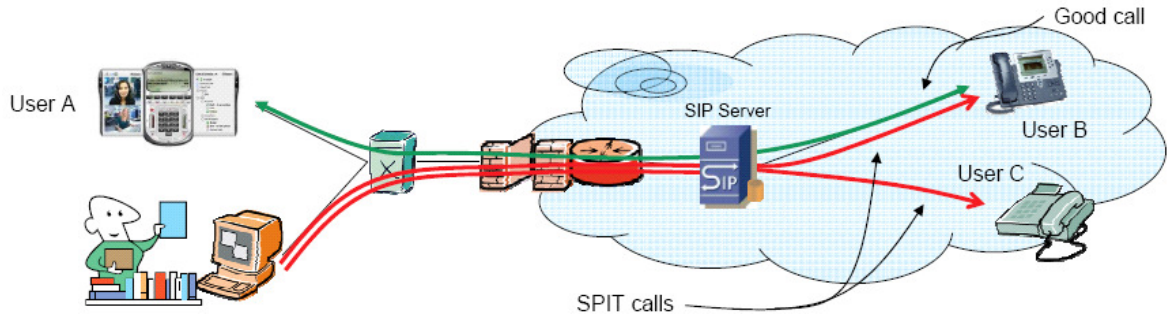


Fig. 21 - Apresentação NEC Corporation no Workshop VoIP Security

4.3.1. Publicidade Não Solicitada (SPAM over Internet Telephony - SPIT)

Tornou-se uma necessidade criar-se algoritmos capazes de compreender padrões de publicidade: identificá-la e bloqueá-la ainda antes do telefone VoIP alvo tocar. É imperativo combater estas tentativas criminais de "roubo de personalidade", através de tecnologias e fabrico de voz e técnicas de *Social Engineering* com a finalidade de enganar pessoas para obter dados das suas contas. Estes ataques são tão comuns e tão trabalhados, que as vítimas só darão conta quando as suas contas sofrerem alterações ou perdas.

Com a expansão de telefones VoIP *low-cost* (comparativamente à ocorrida nas redes PSTN) como novo método de comunicação no ambiente de *Next-Generation Network* (NGN) e as vantagens económicas do meio por onde é transmitido torna-se igualmente uma grande vantagem para actuação da publicidade, sendo os custos reduzidos – comparativamente à rede PSTN – a uma escala de 1000! O resultado já é conhecido nas infra-estruturas de correio electrónico e a grande "fatia" de largura de banda que é consumida para efeitos de publicidade não solicitada (usando *botnets* e outros meios automatizados). Infelizmente, estes inconvenientes são facilmente modificados para se adaptar ao mundo do VoIP, tornando-se a nova praga do séc. XXI se não forem tomadas medidas antes do "*boom*" da tecnologia VoIP.

4.3.2. VoIP SEAL (Solução da NEC)

A *NEC Corporation* apresentou um novo método, chamado VoIP SEAL, capaz de prevenir *SPIT* através de testes *Turing*, detectando chamadas geradas automaticamente para publicidade não solicitada. Torna-se importante o aparecimento destas tecnologias para combater tanto o SPIT, como o já antigo problema de SPAM nas nossas caixas de correio electrónico (por adaptação a diferentes padrões).

Muitos utilizadores são vítimas de chamadas gravadas, intitulando-se como o banco onde o alvo possui conta bancária, e com os métodos de *Social Engineering* obtêm os dados da conta

deste utilizador. Esta foi uma das principais causas que levou a *NEC Corporation* a desenvolver o *SEAL*. Esta solução já mostrou ter uma eficiência de 99% em várias apresentações no ano de 2007, ano da sua apresentação e lançamento em Barcelona, no Congresso Mundial de *3GSM*, sendo capaz de identificar máquinas comprometidas com *botnets* em milhões de números VoIP.

Principais características do VoIP SEAL são:

- Chamadas provenientes de *software* gerador de SPAM são separadas das chamadas de indivíduos através de testes *Turing*. Depois de se estabelecer uma ligação VoIP, o SEAL detecta e bloqueia o acesso não autorizado baseando-se em padrões observados durante a chamada. Ainda antes do telefone do alvo tocar, o SEAL bloqueia a chamada com sucesso!

- Adoptando uma estrutura modular, o SEAL é escalável e, como tal, possibilita uma resposta rápida a novos tipos de ataque SPIT sem ter de reajustar o núcleo do seu sistema.

- A estrutura modular também responde a uma grande variedade de aplicações, sendo flexível e configura-se facilmente em qualquer sistema. Qualquer *hardware* capaz de suportar VoIP, seja H.323 ou SIP, também suportará SEAL.

O sistema de VoIP SEAL protege e defende a rede contra ataques SPIT, e espera-se o contributo de todas as entidades, fornecedoras da rede VoIP, à realização de uma rede NGN mais segura. A NEC vai continuar a desenvolver esta tecnologia até à sua comercialização como solução VoIP. No entanto, na rede LAN doméstica, é preferível seguir-se alguns passos para garantir a segurança do utilizador mesmo com o SEAL.

4.4. Escutas Telefónicas (LI - Lawful Interception)

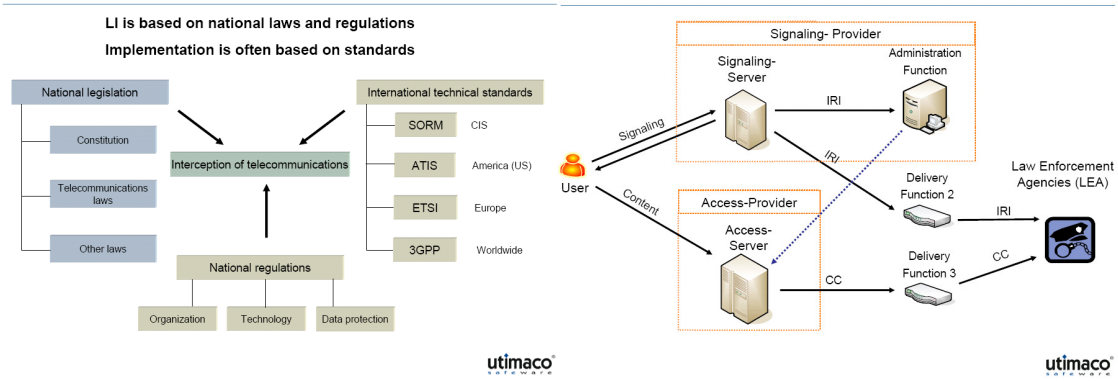


Fig. 22 - "utimaco software" VoIP Security
[in *utimaco software*, PDF de apresentação num Workshop sobre *VoIP Security*]

A escuta telefónica é um requisito essencial para que o ambiente VoIP seja aceite pelas autoridades governamentais como substituto das redes PSTN, onde as ferramentas nem têm de ser muito complexas para se conseguir escutar a linha. Contudo, a tecnologia VoIP permitiu a "mobilidade" do utilizador final. Desta forma, já não é possível garantir a intercepção de chamadas com base na escuta da linha física.

Enquanto os detalhes de LI possam divergir de uma jurisdição para outra, os requisitos gerais são os mesmos. O sistema LI só deve fornecer uma intercepção transparente do tráfego específico e o sujeito não deverá estar consciente/ciente dessa intercepção. O serviço fornecido a outros utilizadores não poderá ser afectado durante a intercepção.

Visão Geral da Arquitectura

Apesar dos detalhes do LI variarem de país para país, pode-se debruçar sobre os requisitos gerais lógicos e físicos, explicando, também, muita da terminologia utilizada. O principal propósito do ISP é o de permitir comunicações privadas entre indivíduos; qualquer funcionalidade LI inserida na rede não deverá afectar o serviço normal àqueles indivíduos. A arquitectura requer uma separação distinta entre a rede de telecomunicações publicas (*"Public Telecom Network"*, ou PTN) e redes privadas utilizadas para distribuição e processamento da informação LI. Os interfaces entre PTN e a estrutura de monitorização *Law Enforcement Monitoring Facility* (LEMF) são padronizados dentro de um território/região particular.

O LI lida com dois produtos: o conteúdo das comunicações (*Contents of Communications*, ou CC) e as informações relacionadas (*"Intercept Related Information"*, ou IRI). O conteúdo pode ser voz, vídeo ou diferentes tipos de mensagens a serem entregues. O IRI refere-se à informação sinalizada: à fonte e destino da chamada, etc.

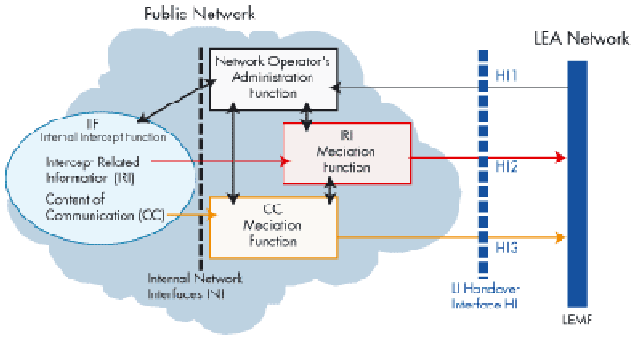


Fig. 23 - Esquema lógico do funcionamento entre a rede pública e a LEA
[in "*NewPort Networks" - Lawful Interception Overview for VoIP (White Paper)*]

A figura acima demonstra o funcionamento lógico do *Intercept Related Information* (IRI) e *Contents of Communications* (CC) desde a sua compilação na rede pública, passando pelo interface *handover*, até à *"Law Enforcement Monitoring Facility"* (LEMF), como definido pelo ETSI. Na América do Norte, a entidade que assegura as escutas telefónicas, CALEA (*Communications Assistance for Law Enforcement Act*), requer aos operadores a capacidade para fornecer LI. A arquitectura da rede e especificações de *handover* são baseadas no modelo de segurança *PacketCable*™, exibido na figura abaixo, onde podem ser vistas as semelhanças gerais de arquitectura:

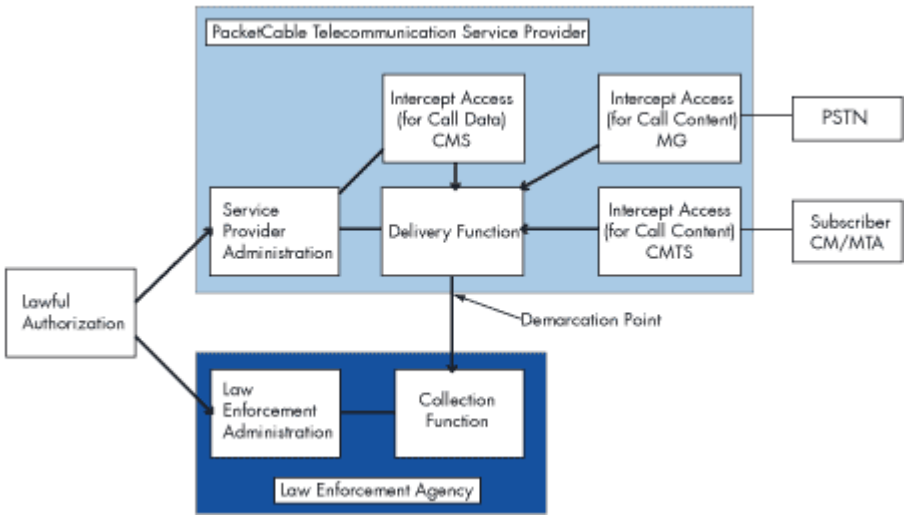


Fig. 24 - Esquema lógico da rede PacketCable utilizado na América do Norte.
[in "*NewPort Networks" - Lawful Interception Overview for VoIP (White Paper)*]

Elementos Básicos do LI na PTN

Funções de Intercepção Interna (IIF): Estas funções localizam-se dentro dos nós da rede e são responsáveis por gerarem o IRI e o CC.

Funções de Mediação (MF): Esta função claramente delineia as redes PTN e LEMF: Comunica com os IIFs utilizando interfaces de rede internos (INIs), que poderão ser patenteados/registados. O MF comunica com um ou mais LEMFs através de interfaces de *handover* localmente estandardizados.

Funções de Administração (ADMF): Esta função lida com o serviço de pedidos de intercepção e comunica com o *IIFs* e MF através de um interface de rede interno.

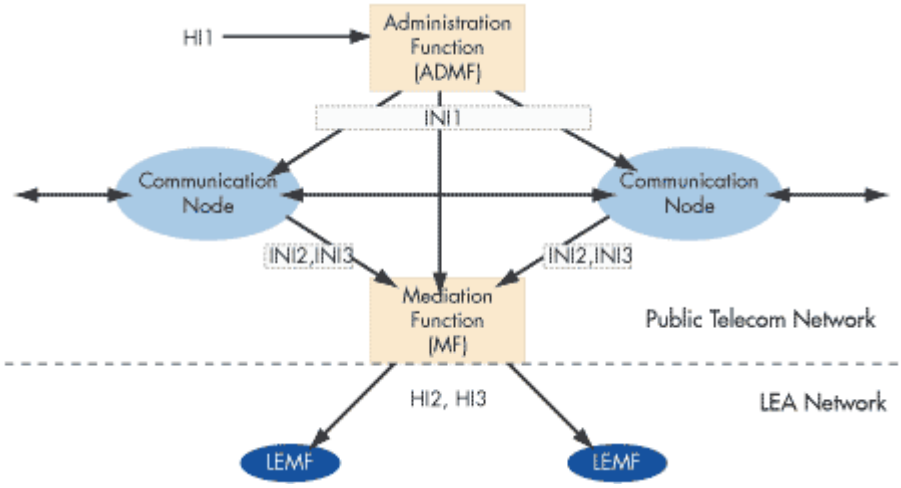


Fig. 25 - Elementos Básicos do LI na PTN
[in "*NewPort Networks" - Lawful Interception Overview for VoIP (White Paper)*]

Implementação de LI no ambiente VoIP

Um dos maiores problemas que o provedor VoIP enfrenta quando administra as chamadas VoIP e multimédia é a separação dos dados (voz, vídeo, etc) e da sinalização, isto já numa outra separação dos outros dados da Internet. Por outras palavras, é bem possível que duas correntes possam tomar caminhos completamente diferentes na rede. Mais: mesmo quando passam pelo mesmo aparelho, este poderá não estar ciente da relação entre as correntes. Contudo, alguns aparelhos dentro da rede são destinados à compreensão e administração das correntes de *media* e de sinalização separadas: As "*session border controllers*" (à direita, na nuvem azul da figura seguinte). Estas localizam-se na fronteira do provedor, local ideal para a implementação de IIF, pois recebem IRIs da corrente de sinalização e podem interceptar CCs directamente da rede de voz/video.

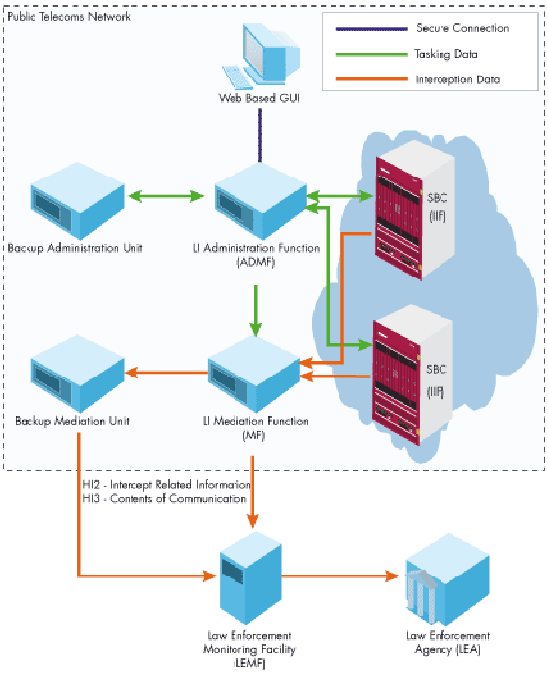


Fig. 26 - Elementos físicos do sistema LI, as suas funções lógicas e os interfaces ao LEMF.
[in "*NewPort Networks*" - *Lawful Interception Overview for VoIP (White Paper)*]

***LI Administration Function* (ADMF):** Normalmente implementada numa unidade de gestão reforçada (*firewalls, IDS*, etc). Fornece um método seguro que possibilita encontrar o tráfego alvo. O ADMF utiliza uma ligação segura a um ou mais dos IIFs e a uma ou mais Unidades de Mediação (MUs).

***LI Mediation Function* (MF):** Executa as funções de mediação e de entrega; é tipicamente implementada numa MU reforçada; recebe IRI genericamente formatado e dados CC de um ou mais IIFs, alterando-os para o formato específico do país e posteriormente, envia aos interfaces de *handover* no LEMF. O MF recebe detalhes sobre o alvo requerido pelo ADMF, seguindo-se a confirmação dos dados IRI e CC recebidos, assegurando, assim, que só dados autorizados são transmitidos ao LEMF. O MF suporta habitualmente o encaminhamento de tráfego interceptado a muitos interfaces LEMF em simultâneo. A MU é frequentemente auxiliada por uma unidade secundária que a substitui em caso de falha da unidade principal (no género de *Primary DNS / Secondary DNS*).

Internal Intercept Function (IIF): É mais eficaz quando implementada em hardware, dentro dos nós da rede, de forma a fornecer a mais eficaz e rápida detecção sem atrair processamento de software adicional e atrasos que podem permitir a que a presença do interceptor seja detectada. O IIF recolhe IRIs e CCs requeridos pelo ADMF, convertendo-os ao formato genérico que é transmitido ao MF.

Volatilidade da Informação

A informação-alvo essencial deve ser encriptada pela ADMF e qualquer informação armazenada no IFF em forma codificada, prevenindo-se, assim, um acesso desautorizado a informação susceptível a autorização. Qualquer informação armazenada dentro do IIF deve sê-lo em memória volátil, para que a informação seja eliminada se um componente do nó da rede for removido ou desligado. Somente a base de dados encriptada do ADMF deve ser mantida durante situações de reinício. Na eventualidade de uma falha de ligação entre o MF e o LEMF, os produtos interceptados poderão ser colocados em *buffer* de memória mas apenas por um curto período de tempo. Qualquer falha do interface a longo prazo resultará na perda de produtos interceptados – esta informação não poderá ser transferida para armazenamento permanente.

Do Ponto de Vista do Utilizador…

Do ponto de vista do utilizador surge a dúvida se é possível realizar a escuta em redes VoIP, seja por oficiais ou atacantes. Contudo, e com a "noticia" de que o VoIP é encriptado, pode-se pensar que com esta tecnologia, ninguém poderá receber o conteúdo desencriptado! Mesmo que as leis do seu país não exijam sistemas de escuta por parte do ISP, dever-se-á, pelo menos, construir o sistema com alguma escalabilidade para alterações futuras. Estes métodos devem ser tão seguros "quanto as transferências bancárias", visto se tratar da ligação entre uma rede pública – com o conteúdo alvo – e uma rede privada encriptada.

5. SERVIÇOS SET-TOP-BOXES (STB): IPTV

A tecnologia IPTV fornece programas de televisão agendados e *vídeo-on-demand* (VOD) através de técnicas de transmissão digital contínua (*digital streaming*) objectivando eficiência no rácio qualidade/recursos na rede IP. Para se receber e descodificar as imagens ou vídeos em tempo real, o utilizador necessita de um STB ou PC com o respectivo *software* baseado em *media player*.

A principal razão do atraso nos serviços de IPTV deve-se essencialmente à segurança que se aplica ao sistema: Até recentemente, os distribuidores têm-se deparado com dois grandes problemas: como proteger o *copyright* do conteúdo televisivo – um problema de à muitos anos – e como o proteger da rede IP, tão consumida por ataques externos. Os profissionais da área dizem ter o primeiro problema resolvido e que o segundo não está longe de se concluir com as tecnologias emergentes.

Segundo *Gary Southwell*, director da *Multiplay Solutions* na *JupiterNetworks,* em *darkREADING.com – Solving IPTV's Security Problem*, a solução ideal para os problemas de segurança do serviço IPTV seria "trancar" os seus servidores, mas infelizmente muitos não podem ser pois são necessários à interacção com o cliente. Poder-se-ia protegê-los com *firewalls* mas a entrega contínua de pacotes a 4Mbit/seg. (quando não usando HD: 15 a 19 Mbit/seg.) não é suportada pela maioria existente no mercado. Poder-se-iam colocar *firewalls* em cada codificador, mas os custos na empresa distribuidora iriam quadruplicar no *data center*. O elevado custo para garantir a segurança na rede IPTV foi a razão principal para impedir o modelo de negócio do serviço.

Os ataques DoS na rede IPTV podem até nem impedir a entrega de conteúdo, mas pode atrasá-la significativamente, podendo ser notado pelo cliente final. Por outro lado, num exemplo mais drástico, um servidor da Microsoft que gere a comutação de canais pode ser sobrecarregado por DoS, deixando o serviço inoperacional e sem capacidade de envio de conteúdo nos canais que gere. Para eliminar este problema, a *JupiterNetworks* adaptou o seu sistema de *integrated secure gateways* (ISG) para funcionar em conjunto com os servidores de IPTV da Microsoft. Essencialmente, o sistema irá criar um *buffer* de segurança entre o sistema do cliente (PC ou STB) e o servidor IPTV. São avaliados números anormais de *requests* e *responses* contidos neste *buffer*, podendo inclusive retirar utilizadores suspeitos para fora da rede. Assim, a compatibilidade do ISG com IPTV pode suportar tráfego de até 100 servidores IPTV, reduzindo significativamente os custos da distribuição de sistemas de segurança.

Segundo *Southwell*, com a maioria dos problemas de DRM resolvidos e uma infra-estrutura protegida no horizonte, não demorará até que os serviços de IPTV sejam largamente distribuídos. Ainda há muito trabalho a fazer para a oferta de serviços IPTV, havendo clientes a usarem PCs e PDAs para este fim, mas já muito se fez em segurança, ultrapassando obstáculos prioritários.

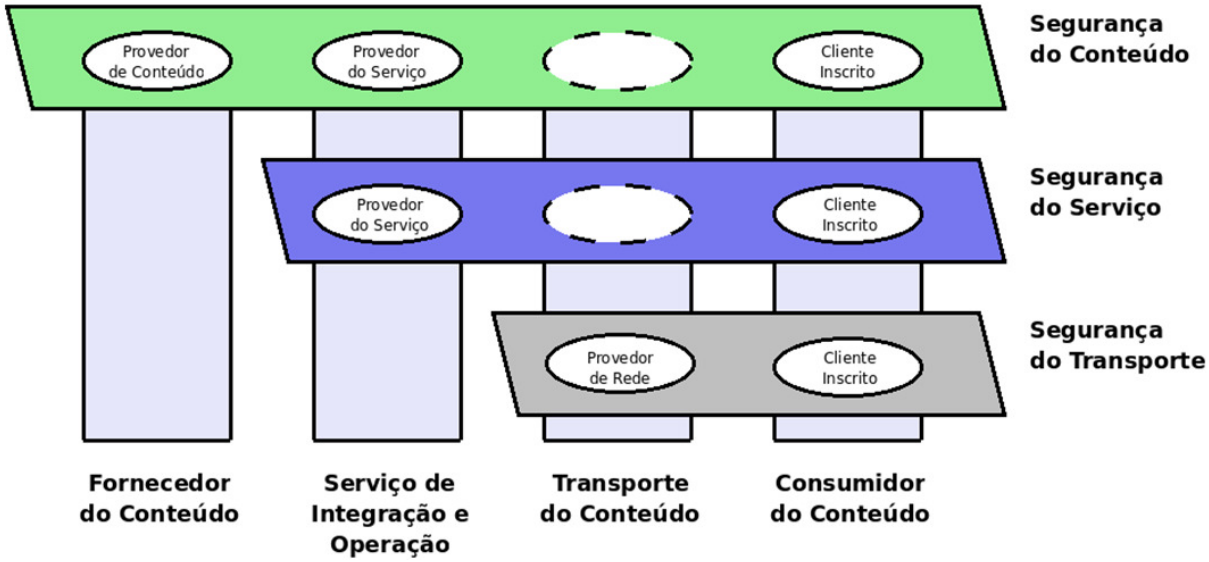


Fig. 27 - Camadas de Segurança em IPTV (Conteúdo e Privacidade)

5.1. Proteger o Conteúdo

Os provedores de IPTV têm-se esforçado para procurar uma forma de proteger a sua rede contra possíveis ataques de *hackers*, como os DoS que tantos problemas têm dado na rede VoIP ou roubo de conteúdo supostamente protegido. Resumidamente, o problema dos serviços de IPTV é a sua dependência de extensas redes de servidores e codificadores para distribuição de conteúdo a todos os seus clientes. Os provedores de IPTV estão criando camadas extras de segurança na esperança de proteger toda esta rede e deter a maioria dos roubos de conta e *sniffing* de conteúdo licenciado, aplicando diferentes tácticas, umas já conhecidas em DVDs e outras únicas no mundo da IPTV. Também se procura, a curto prazo, estandardizar as interfaces, sistemas de acesso condicional e outras ferramentas como *digital watermarking* que possibilitará à indústria uma melhor e mais fácil auditoria de conteúdos pirata.

Gerir os direitos digitais sobre conteúdos protegidos podem e devem ser restringidos apenas a clientes que tenham pago por tal. O problema é impedir a cópia e distribuição do conteúdo após a sua entrega ao cliente. Nos últimos anos, muitos distribuidores têm atacado este problema com sistemas de encriptação de sinal entre o servidor de conteúdos e a *set-top-box* (STB) do cliente. Esta encriptação garante que só os utilizadores que paguem o serviço poderão desencriptar o sinal na STB, mas nada o impede de fazer cópias ilegais!

O uso de *smartcards* já é obsoleto: os dispositivos necessários para clonar *smartcards* estão cada vez mais acessíveis. A única forma de os combater é redistribuir novos cartões aos clientes e eliminar todas as anteriores contas, tornando-se uma grande despesa para o provedor ou até para o cliente! A solução será, mais uma vez, a segurança baseada em *software*, oferecendo CAS/DRM renovável através do *download* na Internet, método agora designado de *Cypher Virtual Smartcard*, facilmente aplicado às novas *set-top boxes* com soluções de *hardware* dedicadas embutidas. Sistemas de segurança em *software*, capazes de gerar condições de acesso e manusear os direitos digitais, estão a surgir como componente chave para a distribuição serviços de IPTV, assegurando o conteúdo *Premium* e evitar pirataria de terceiros não autorizados.

Ainda que os novos métodos de *Cypher Virtual Smartcard* possam impedir o acesso não autorizado de terceiros, não impedirá o cliente de realizar a cópia após descodificar o conteúdo no STB, bastando, para isso, pegar no sinal analógico e reconvertendo-o para digital. A solução apresentada pela *Verimatrix* é o uso de *watermark* contido na imagem mas invisível ao olho humano. É constituído por um ID único, embutido no próprio *stream* de vídeo e que identificará a STB onde o conteúdo é utilizado e respectiva data de recepção, e um outro ID proveniente do sistema de controlo de conteúdos: Não resolve a pirataria mas identifica a origem da cópia! Como já não se utilizarão *SmartCards*, um utilizador que realize a cópia não se poderá defender com um possível roubo ou clonagem do cartão.

5.2. Transporte

Os requerimentos de segurança para o operador, no que tange ao transporte dos serviços de IPTV:

- **Autenticação e controle de acesso**: deverá ser implementado no acesso à, prevenindo o acesso não autorizado aos recursos disponíveis. Os dois recursos que deverão ser controlados no acesso são a rede e os serviços sobre ela. No acesso à rede, o terminal do cliente inscrito deverá ser identificado e autenticado.
- **Autenticidade das entidades de rede**: a rede IPTV deverá ter a habilidade de verificar a identidade cada entidade de rede que está participando do serviço IPTV, de maneira a estabelecer uma relação de confiança entre os vários nós.
- **Protecção da integridade dos dados e disponibilidade**: a rede IPTV deverá garantir a integridade e disponibilidade dos dados armazenados ou a entrega dos dados transmitidos na rede.
- **Contagem dos pacotes de dados**: de maneira a incentivar o bom uso dos recursos, comportamentos inadequados por uso irregular do serviço deverão ser punidos.
- **Segurança em *Multicasts***: são necessários mecanismos de protecção à camada de *multicast*, como a disponibilidade das chaves dos equipamentos, verificação da identidade da origem *multicast*, controlo dos membros do grupo *multicast*, etc.

Requerimentos de segurança sobre CDN: dois aspectos deverão ser considerados: a protecção dos nós CDN (*Content Delivery Network*) e a protecção dos fluxos distribuídos nas redes CDN.

5.3. Privacidade

A segurança e privacidade dos clientes de IPTV são os factores mais importantes para a expansão do negócio: proteger a privacidade e dados pessoais que possam ser inseridos quando acedendo diferentes canais televisivos. É preciso verificar os dados introduzidos, gerindo-os de forma responsável e garantindo a sua confidencialidade.

Um dos aspectos importantes na privacidade e segurança dos subscritores é a necessidade da sua rede LAN doméstica ser um espaço fechado e com segurança a limitar os seus utilizadores e dispositivos. Nesta perspectiva, a rede LAN é um ponto muito frágil, principalmente quando usando redes *Wireless* e partilha de diferentes tecnologias multimédia. Se for o caso, devem-se seguir os passos indicados nos temas abordados anteriormente deste

documento: estarão mais seguros de serem lidos por terceiros não autorizados.

Para encriptação do conteúdo em IPTV, utiliza-se uma camada de segurança para controlo de acesso condicional, a qual geralmente utiliza encriptação baseada em chaves simétricas partilhadas entre o *data center* e o cliente subscritor. A gama de opções para privacidade e segurança está a aumentar a um ritmo que dificulta aos provedores de IPTV seleccionar, com publicações em massa para de diversos resultados para cada algoritmo utilizado.

5.4. Utilidade da Tecnologia IPTV (em Segurança)

Olhando a tecnologia IPTV como uma ambiente de controlo da rede LAN, poder-se-ão aplicar diversas interfaces que possibilitem ao cliente, uma maior interacção e envolvência com o sistema que o rodeia. Desde notificar novos endereços MAC detectados pela rede WLAN, monitorizar portos da *firewall* e respectivo *software*, definir limites para eventuais serviços de *Parental Control*, etc.

O uso de ambientes simplificados na televisão pode trazer uma maior gama de serviços disponibilizados pelo provedor da rede. Resta realizarem-se os estudos necessários para o maior aproveitamento de ofertas/preço no mercado.

6. ANÁLISE DE VULNERABILIDADES DE TRIPLE-PLAY

Neste capítulo será realizado um levantamento das vulnerabilidades num ambiente de um ISP fictício, representando a generalidade das falhas de segurança encontradas. O objectivo aqui será apenas demonstrar alguns dos vectores utilizados para a exploração das falhas de segurança do ambiente.

6.1. Ambiente a ser Analisado

O ambiente elaborado tem, por base, uma pequena pesquisa realizada em topologias disponíveis na Internet com algumas considerações adicionais por se tratar de um provedor de serviços *Triple-Play*. O ISP exemplo fornecerá, além do serviço de ligação à Internet – através de uma ligação ADSL –, os serviços de VoIP (através da arquitectura VoIP) e IPTV através de uma solução proprietária genérica, possuindo alguns dos elementos que normalmente se apresentam neste tipo de arquitectura. A figura abaixo demonstra comunicação do provedor de serviços para com o cliente ADSL:

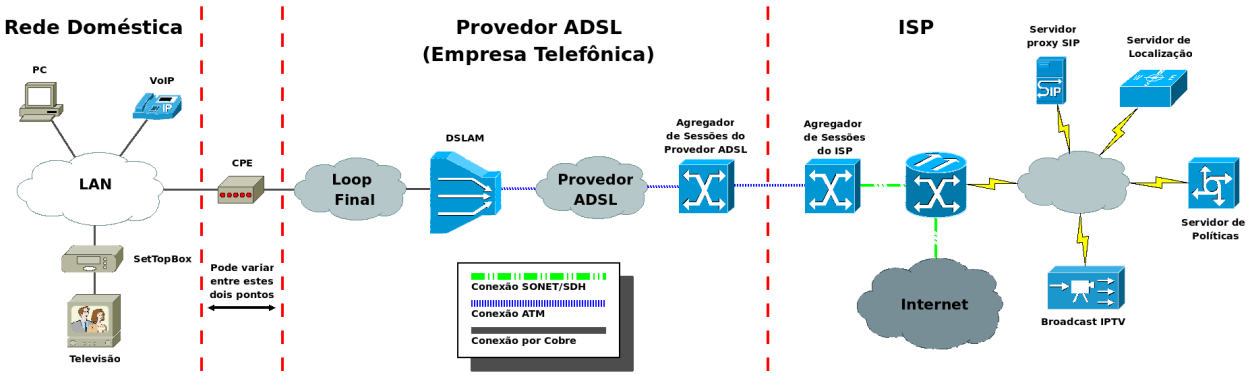


Fig. 28 - Exemplo da Topologia entre o Cliente e o ISP

6.2. Ameaças Existentes

O objectivo deste capítulo não será enumerar todas as ameaças possíveis no ambiente de um provedor de serviços *Triple-Play*, mas mostrar um modelo de prováveis ameaças. Analisar os ataques com notórias possibilidades de ocorrer é melhor do que verificar item a item numa lista interminável de ameaças existentes. Os ataques poderão vir dos seguintes ambientes:

- Ataque a partir da rede externa.
- Ataque a partir da rede local.
- Ataque a partir do sistema local.

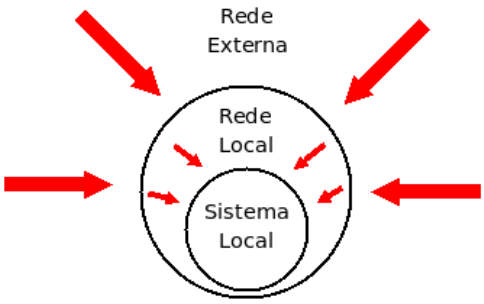


Fig. 29 - Ameaças ao Ambiente Triple-Play

Ao contrário do que possa parecer, ao se observar a figura acima, para a realização de ataques directamente ao núcleo, não é necessário que se tenha de quebrar a segurança dos níveis anteriores: A maior ameaça de ataques surge de dentro das empresas, sendo realizados por funcionários ou outros membros internos. Existem vectores de ameaças em todos os níveis organizacionais.

6.2.1. Ataque a partir da Rede Externa

O provedor de serviços pode ser afectado através da rede externa, pois, com tantos pontos de acesso oferecidos aos seus clientes, o provedor estará sob uma grande variedade de possíveis ataques vindos de ambos os flancos interno (clientes) ou externo (Internet).

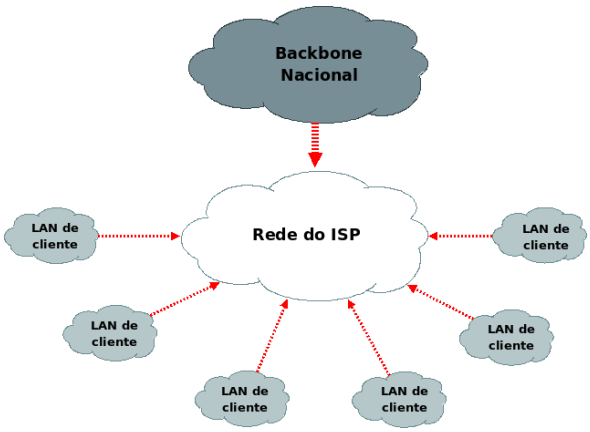


Fig. 30 - Vectores de Ataque ao ISP

As ameaças existentes nesta situação diversificam-se abaixo:

- **Uso das ligações entre clientes e rede do ISP**: com os serviços *TriplePlay*, vieram larguras de banda muito superiores às necessidades básicas para navegação na Internet, estando estas agora disponíveis para os clientes. Podem chegar a débitos elevados: algo como 24Mbit/s para cada cliente, considerando a partilha do meio com 2048Kbit/s para tráfego de saída (*upload*). Poucos clientes, quando sincronizados e em conjunto, podem inundar a ligação com tráfego, causando a negação de serviços no provedor por falta de recursos.~

- **Uso da ligação entre o *backbone* e a rede do ISP**: os provedores de serviço possuem largura de banda com os *backbones* dimensões estrondosas, suportando o tráfego de milhares de clientes simultaneamente. Considerando que não é possível confiar nos mecanismos de segurança de outras redes externas, é necessário adoptar medidas para protecção contra ataques de negação de serviço vindos do exterior.

- **Uso do provedor como meio de comunicação ao exterior**: tão provável quanto ser vítima é a possibilidade de se ser cúmplice de um ataque de negação de serviço, sendo que o tráfego foi gerado em clientes do ISP.

- **Ataque aos serviços do provedor**: A oferta de serviços do ISP correm diversos riscos, sejam eles específicos do protocolo em uso ou genéricos quanto ao sistema.

- **Infra-estrutura dos sistemas**: os sistemas críticos normalmente são desenvolvidos em linguagens de programação altamente flexíveis, como C e C++. Aplicações desenvolvidas sobre tais linguagens estão sujeitas, quando má programadas, à exploração das suas falhas: para citando os problemas mais conhecidos, tem-se *buffer over*, formatação de *strings* e *integer overflow*. Além destas ameaças, os sistemas de infra-estrutura estão também sujeitos a ataques de negação de serviço, já que todos possuem limites de clientes a servir. Outros ataques, específicos a plataformas, podem ser realizados:

- **Serviço Web** – exploração de falhas de configuração do servidor Web ou aplicações que dependam da sua execução (*AWStats*, MRTG, *Cacti*), XSS, CSRF, acesso a ficheiros para execução de código remotamente, falha no controlo de acesso no *framework* e a páginas restritas e, por último, sondagens, que não são necessariamente uma ameaça, mas precede.

- **Base de Dados** – injecção de código SQL, inferência através de um mau controlo de acesso e execução de código arbitrário.

- **Sistema de Autenticação e Directório** – e*avesdropping*, acesso a dados não autorizados, *tamperinge* e despersonalização.

- **Sistema de Resolução de Nomes** – s*poofing*, *ID hacking* e *cache poisoning.*

- **Sistemas Operativos** – aplicação incorrecta de *patches* de segurança (não é a causa, mas pode gerar instabilidade no sistema e daí favorecer ameaças), *dangling pointers*, vulnerabilidades em aplicações que podem resultar em comprometimento de todo o sistema, uso de força bruta contra serviços que requerem autenticação como FTP, SSH e Telnet, acesso a *logs* com informações sensíveis e sem necessidade de autenticação, exploração de falhas em módulos de maneira a obter acesso a nível administrativo em funções do sistema, etc. A maior parte das vulnerabilidades são específicas para um ambiente, já que cada um possui características e arquitectura própria.

- **Sistemas Virtualizados** – vulnerabilidades que afectem o sistema operativo da máquina hospedeira, poderão também afectar a máquina virtual e interfaces de administração com baixos requisitos de segurança.

- **Infra-estrutura de rede** – ataque a *routers*, *switches*, *firewalls*, *proxies*, *clusters* para balanço de carga, sistemas de detecção de intrusão, etc.

- **Armazenamento de dados na rede** – ataque às estruturas de armazenamento de dados na rede visando obter dados como registos de *routing*, faixa de endereços IP, *spoofing* para actualizações indevidas nas bases, etc.

- **Negação de serviço** – ataques *Smurfs* através de outros ISPs e ataques DDoS proveniente dos clientes internos ou de outros ISPs. Os ataques de negação de serviço são baseados em quantidade do fluxo de dados ou em dados específicos com o intuito de explorar alguma falha de segurança (como o envio de grande pacotes IPv4 mal formados) existentes em algum activo na rede.
- **Sistemas de Detecção e Prevenção de Intrusos** – ataques de negação de serviço, de maneira a impedir uma análise eficiente do tráfego da rede.

- **VoIP**: interceptação de chamadas VoIP, negação de serviço aos activos do sistema, como servidor *proxy* SIP, servidor de localização, ou apenas para degradação da qualidade das chamadas, *hijacking*, SPITs, *phreaking out* (acesso indevido ao sistema para a realização de chamadas de longa-distância), acesso indevido ao serviço de voz (*voicemail*) e indisponibilidade do serviço.
- **IPTV**: ataque de negação de serviço às estruturas de IPTV, causado através da inundação da estrutura com tráfego excessivo ou através de milhares de requisições simultâneas realizadas por clientes sincronizados, deteriorando a qualidade da transmissão. São ataques baseados em aplicação e cópia de conteúdo protegido.

Segue-se a figura da arquitectura *Triple-Play* com fluxos que indicam alguns dos tipos de ataques que o provedor está sujeito a sofrer:

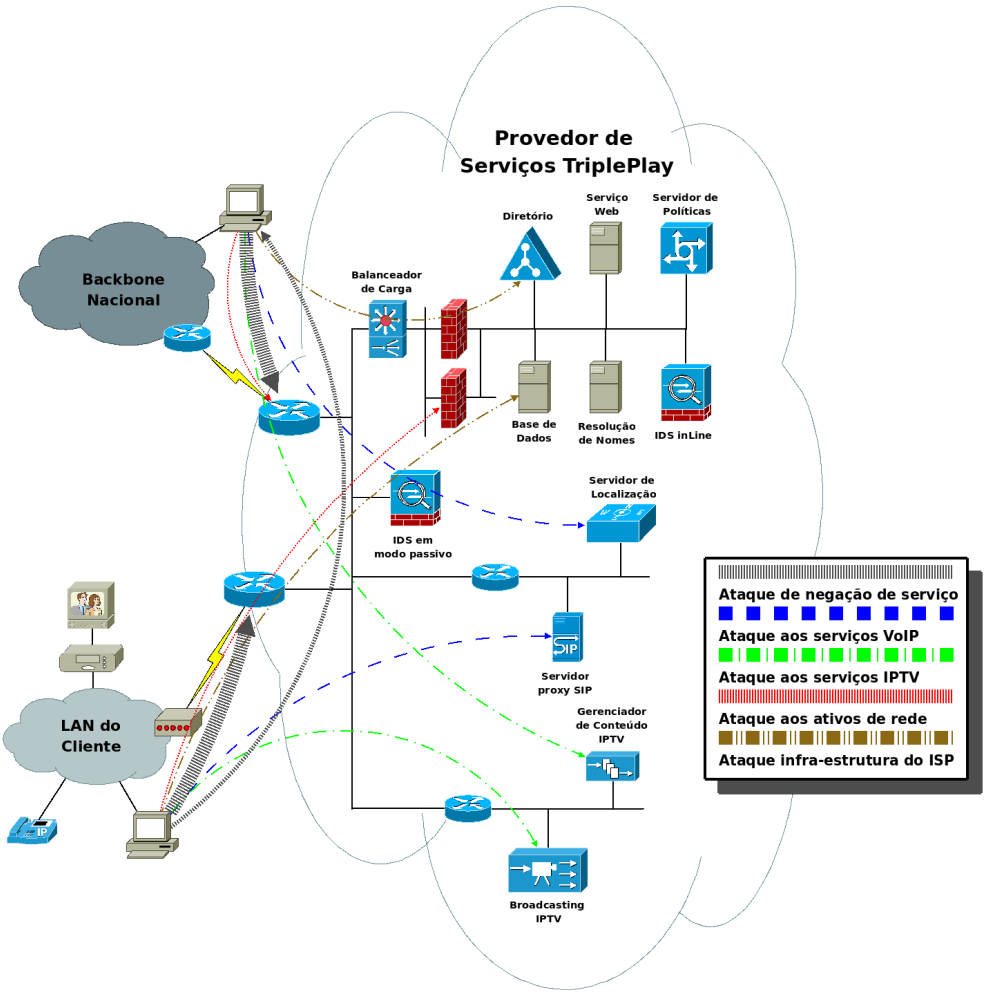


Fig. 31 - Tipos de Ataque no ISP pela Rede Interna

6.2.2. Ataque a partir da Rede Local

Após verificadas algumas possibilidades de ataque, entre outras ameaças existentes, com origem nas redes externas, será bom compreender as diferenças aquando de ataques realizados a partir da rede local. Estes têm muito maior proximidade dos serviços, já que é possível a partilha do mesmo barramento de rede: uma grande vantagem para o atacante.

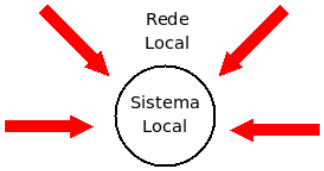


Fig. 32 - Ameaças à Rede Local

O vector de ataque no sistema, considerando-o com origem na rede local, pode ser algum dos subdomínios representados na figura:

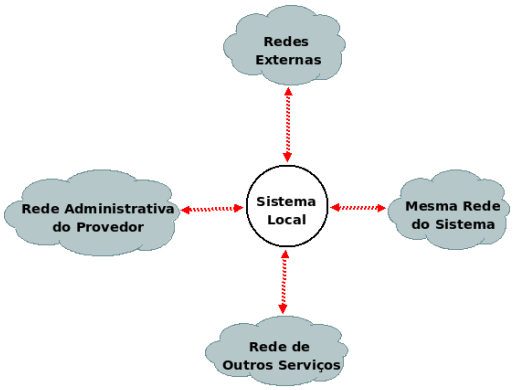


Fig. 33 - Vectores de ataque à Rede Local

Um sistema comprometido também representa uma ameaça para as redes vizinhas e outras, representadas na figura como redes externas. Abaixo, algumas das ameaças:

- **Uso das ligações entre clientes e rede do ISP**: se um ISP estiver com a sua rede infectada por algum *malware*, facilmente poderá espalhar o "vírus" para outros clientes, seja com a finalidade de criar processos de autenticação a dispositivos de controlo das redes domésticas ou simplesmente indisponibilizando os canais de comunicação.
- **Uso da ligação entre *backbone* e rede do ISP**: um ISP que esteja sobre uma crise de *malwares* é tudo o que os provedores vizinhos não querem. Dado o alto tráfego entre estas grandes redes, poucos mecanismos de segurança são implementados, resultando a vulnerabilidade e um ambiente de confiança "desconfiada": Um ISP infectado facilmente pode espalhar os seus sintomas para outras redes.
- **Uso do provedor como meio de comunicação externo**: qualquer tipo de ataque realizado para redes externas através do provedor poderá comprometer sua responsabilidade.

- **Ataque aos serviços do provedor**: a maioria das vulnerabilidades existentes são as mesmas quando o ataque é realizado de um ambiente externo, porém a facilidade com que é possível proceder com o ataque é maior, já que o acesso aos dados e a quantidade de defesas existentes podem fazer toda a diferença. Dependendo da proximidade com o alvo, o uso de *sniffing* torna-se mais prático.

A representação a seguir demonstra uma topologia com fluxos que indicam alguns dos tipos de ataques a que o provedor está sujeito:

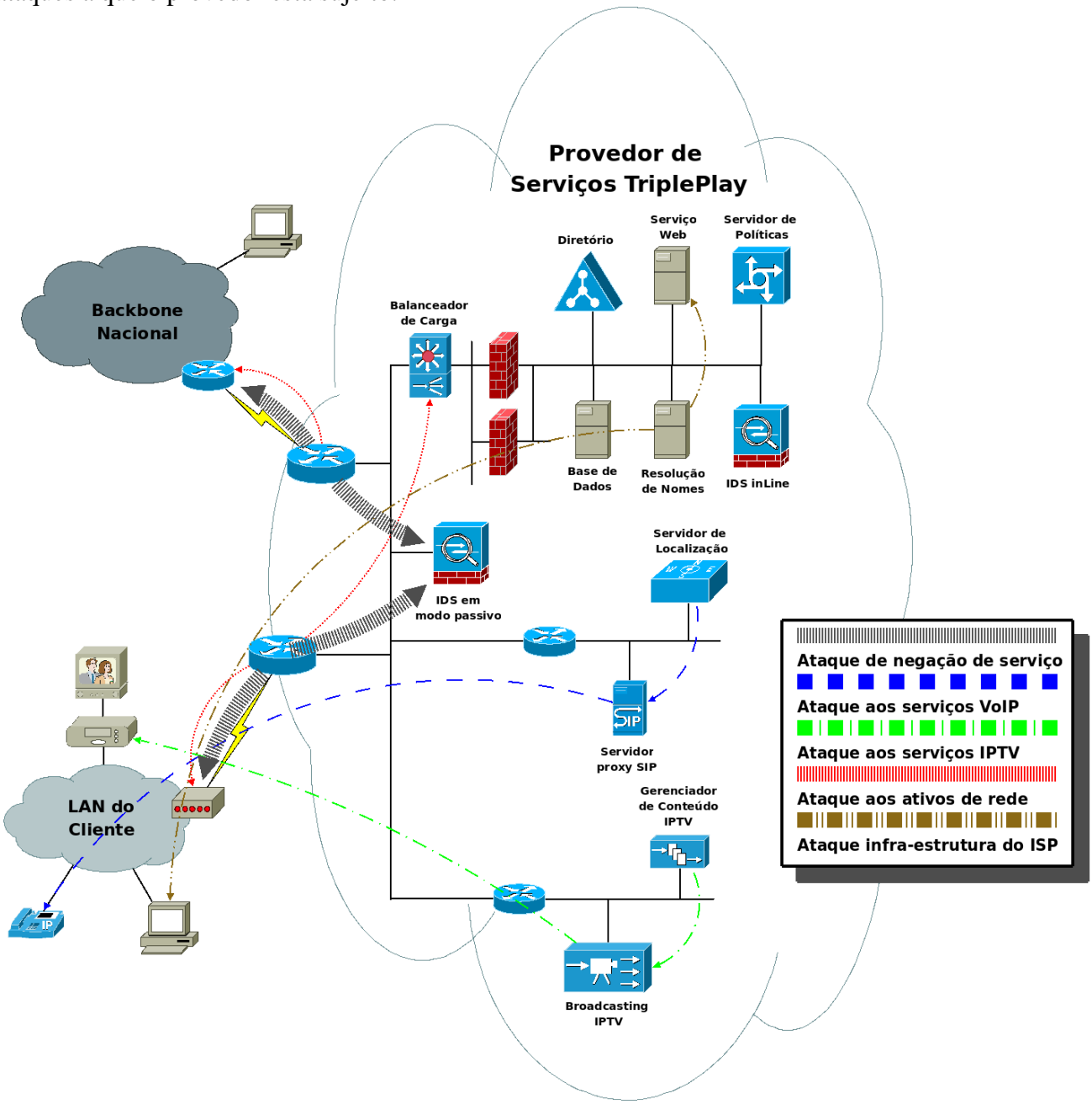


Fig. 34 - Ataque a partir da rede local

6.2.3. Ataque a partir do Sistema Local

A terceira vertente de ataque é possível quando um invasor possui acesso a algum recurso do sistema local. Este acesso caracteriza-se pela possibilidade do atacante utilizá-lo para ampliar as suas credenciais, permitindo que o utilizador comum se torne outro com os mesmos privilégios "superiores", necessários à realização do ataque a aplicação essencial a qual almeja.

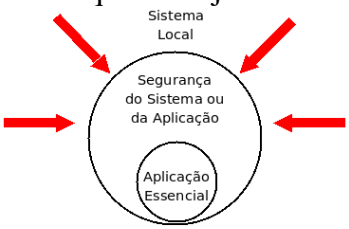


Fig. 35 - Ameaças ao Sistema Local

O uso de um sistema comprometido pode ser utilizado não apenas para afectar uma aplicação do mesmo, mas também como meio para a realização de ataques a outros sistemas. O esquema abaixo demonstra as vertentes de ameaças possíveis.

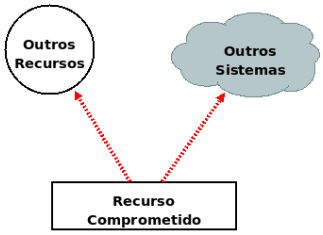


Fig. 36 - Vectores de Ataque ao Sistema Local

Abaixo descrição de algumas das ameaças no corrente ambiente:

- **Uso da ligação entre o sistema e a rede do ISP**: um ataque a um outro sistema do mesmo provedor possuirá maiores chances, já que pode existir uma relação de confiança entre as redes, caso estejam separados, ou acesso directo, se estiverem no mesmo barramento. As possibilidades aqui são as mesmas encontradas na situação anterior, onde se possui acesso à rede local do alvo, presumindo-se que possui acesso a algum sistema da mesma rede.

- **Uso do sistema local como meio de comunicação externo**: qualquer tipo de ataque realizado para redes externas, através de um sistema que encontro num provedor, poderá comprometer a sua responsabilidade. O ataque terá a vantagem na sua origem, numa rede de acesso menos complicada até ao alvo. O mesmo ocorre que na situação anterior, mas neste caso, já se presume o acesso a algum sistema na rede local para a realização da comunicação externa, existindo as mesmas ameaças.

- **Ataque aos serviços do sistema**: O sistema onde o atacante ganha acesso pode ter os seus serviços ameaçados. O principal meio para a realização de ataques num sistema onde já se tenha acesso básico é através do escalonamento de privilégios até se obter o necessário para a realização do ataque. Este terá como alvo, justamente, aqueles que compõem o objetivo do sistema, como o *software* de VoIP, IPTV ou de algum dos serviços de infra-estrutura, como DNS, directório ou serviço Web ou o próprio sistema operativo.

    - **Ataque ao sistema operativo** – Pode ser realizado a alguma das suas estruturas, como módulos, *drivers,* serviços ou quaisquer outras estruturas necessárias para seu correcto e

completo funcionamento. Normalmente, o ataque às estruturas fundamentais apenas é possível caso o atacante possua credenciais que lhe permitam realizar alterações profundas, como sedo um utilizador *root* em sistemas *Unix-like*. Através de exploração de vulnerabilidades anteriormente descritas, torna-se possível a realização destes ataques mesmo como utilizadores comuns. O uso de *rootkits* é bastante recorrente quando se trata de obter privilégios ou atacar o sistema operativo em si, fornecendo "óptimas" brechas de segurança ao atacante.

- **Ataque à aplicação** – É facilitado caso o sistema operativo esteja tomado pelo atacante. Uma aplicação apenas pode sofrer grandes interferências se as permissões utilizadas para executá-la, no modo de utilizador (*user-space*), assim o permitam.

Abaixo, a representação possíveis ameaças existentes, considerando que o atacante possui acesso a, pelo menos, uma linha de comandos, seja em modo simples – com poucos privilégios – ou em modo privilegiado.

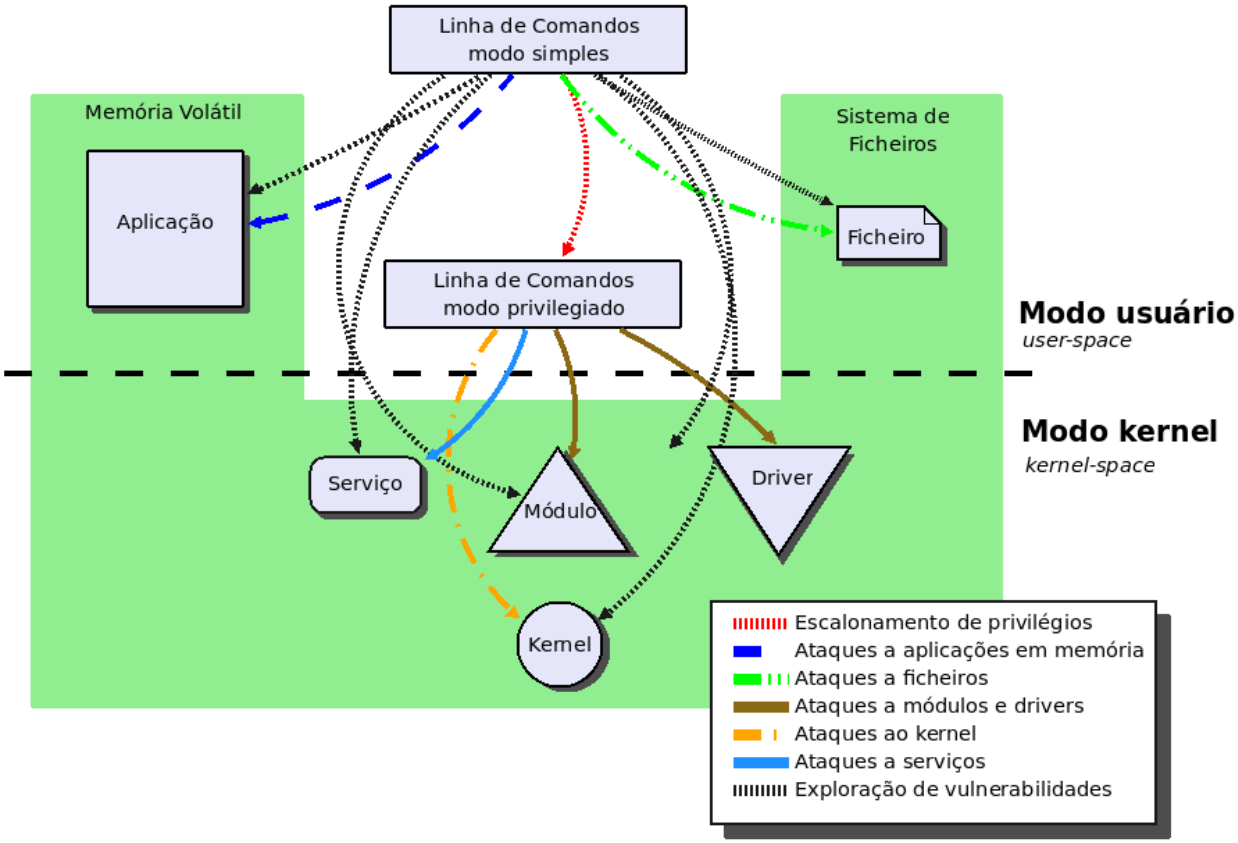


Fig. 37 - Ataques a partir do Sistema Local

7. SÍNTESE

São inúmeros os novos serviços que se desejaria oferecer ao cliente, e inúmeros os que este devería exigir do ISP. Num ambiente *Triple-Play*, as dificuldades em configurar um *firewall*, base para a maioria da segurança nas redes LAN, poderia ser facilitada pela manutenção remota que se tenta implementar com os novos métodos (veja-se http://www.workssys.com/). Maior segurança seria proporcionada, mas também seriam necessários mais recursos humandos para responder às diferentes necessidades. A melhor metodologia seria um serviço *on-line* com um *user interface* amigável e com ajuda suficiente para fazer entender o cliente do actual estado da sua *firewall*, as vantagens em configurá-la e o que o provedor pode fazer por ele. O uso de *firewalls* em *software* torna-se inútil em ambientes domésticos, pois a monitorização desejada ainda não requer níveis tão detalhados. Muito bom já seria se todos os utilizadores soubessem controlar a sua *firewall* e se o ISP ajudar nesta tarefa. A televisão por IP, integrada no serviço, poderá ser um ponto forte na aproximação do cliente a estas e outras configurações: "Introduzir o IP do *router* no seu *webBrowser"* não é uma conversa simples para o utilizador comum. Portanto a tecnologia IPTV poderá facilitar este acesso, sendo os endereços tratados pelo *CPE-Gateway*.

Quando à difusão do SSID nas redes *wireless*, retirar esta opção tornaria a configuração, em cada computador, algo mais complicado. O ideal será assegurar todos os outros pontos de segurança na rede *wireless*, aproveitando-se a comunicação do serviço *Triple-Play*. O acesso *wireless* é uma forma muito cómoda de qualquer terceiro não autorizado entrar numa rede doméstica. A segurança a aplicar-se nestes meios é prioritária e, infelizmente, a realidade é outra. Mais uma vez, podem-se apresentar questões de segurança pela televisão IP: Listas de endereços MAC aceites e bloqueados, mantendo-se o SSID activo e deixando que o utilizador autorizado apenas introduza a chave WPA2, provavelmente definida aleatoriamente pelo provedor, da mesma forma como se fazia nos serviços de Internet para os modems de 56k.

A oferta de serviços como a filtragem de conteúdos para controlo parental é outro ponto forte na exploração de negócios sobre os clientes. O uso de *routers* com serviço de *Parental Control* como o *iBoss* e *iPhantom* são a escolha ideal: Filtram-se os conteúdos, a configuração é acessível e, perante um ambiente *Triple-Play*, bastará, mais uma vez, redireccionar a sua configuração para a televisão IP através do *Gateway*.

Os provedores de *Triple-Play* podem e devem facilitar o acesso aos menus de configuração dos vários pontos de segurança, preferencialmente já com algumas definições padrão. O uso da tecnologia WMI poderá ser útil para avisar o utilizador de diversos *hotfixes* e actualizações necessárias nos seus computadores, e avisá-lo inclusive, através do envio de *scripts* que avisarão o utilizador. Coloca-se a questão do próprio *CPE-Gateway* gerar scripts para o envio de diversos avisos ao computador do administrador de rede, e não apenas à televisão IP. No entanto, o WMI possui algumas falhas de segurança que devem ser consideradas.

A segurança a aplicar-se aos *Mail User Agents* e *Web Browsers* podem ser revistas pelo WMI, não havendo outras opções senão o controle do ISP, já na sua nuvem de *proxies*, além de incentivar o cliente a seguir algumas normas de segurança no seu MUA ou *Browsers*, tanto para *cookies*, código activo, conteúdo multimédia, registos ou executáveis, etc.

Outra oportunidade de negócio é a tecnologia *UPnP* – se esta já obedecer às necessidades de autenticação – ou DPWS. Mesmo que não fazendo uso do seu futuro potencial, como a integração de múltiplos dispositivos e componentes de uma casa (segurança, iluminação, cortinados, cozinha, etc), deve-se, pelo menos, possibilitar futuras implementações deste tipo de serviços, claro está, sempre com a segurança em primeiro lugar, pois uma "Casa USB/Ethernet" não é coisa para facilitismos, principalmente nos IGD. O ideal será acompanhar o progresso dos projectos

SOCRADES, SODA e SIRENA e aguardar novos artigos pois para já, a associação desta tecnologia com os serviços de *Triple-Play* é nula e não será este o ponto de focagem mais evidente.

O serviço *Triple-Play* também se preocupa com os serviços de chamadas de telefone em VoIP. Além dos problemas de segurança que o protocolo SIP já trás, a mistura da rede de dados com a de voz será uma nova oportunidade para os *sniffers*. O que menos se espera é utilizarem-se *routers* ou *proxies* sem estarem com a *firewall* adaptada ao protocolo em uso, deixando portos abertos durante a sessão VoIP e não os controlando conforme o estado da chamada. Como foi dito, o uso de *gateways* multimédia ou *proxies* revertidos, com suporte aos recentes protocolos *Media Gateway Control Protocol* (MGCP), *Signaling Connection Control Part* (SCCP) ou *Session Initiation Protocol* (SIP), facilita o manuseamento e segmentação de pacotes VoIP dos outros pacotes de dados. Também o uso de redes virtuais será bem-vindo para salvaguardar a informação em ataques acima da camada de tratamento de dados. É preciso tomar atenção às exigências da lei aplicada no país referente às escutas telefónicas. É uma via privada que não se poderá perder no VoIP.

Sobre os casos de publicidade padronizada nos sistemas de VoIP, será bom seguir-se a metodologia da *NEC Corporation* e o seu sistema SEAL. Quanto às indesejadas chamadas a cobrar no destino, para já não há muito este controlo no mundo do VoIP.

Para o cliente, as preocupações da tecnologia IPTV é essencialmente a sua privacidade. Este bem não é um ponto de risco partindo do princípio que se estão a utilizar chaves simétricas partilhadas para encriptação do conteúdo.

A maior preocupação colocada do lado do fornecedor será a forma de identificar os que fazem cópias ilegais do conteúdo que lhes é mostrado. A resposta está em *watermarks* invisíveis ao olho humano e que identificam a hora e local onde foi realizada a cópia. O uso de *Cypher Virtual Smartcards* impedirá o cliente de negar que foi realizada a cópia pelo seu STB.

8. BIBLIOGRAFIA

[1] NIST: Security for Telecommuting and Broadband Communications, Special Publication 800-46, Agosto de 2002

[2] The Inquirer, "*Women give out Passwords for Chocolate*". Notícia de 16 de Abril de 2008

[3] *DSL Report* – Teste de Vulnerabilidade: http://www.dslreport.com

[4] Encriptação em redes sem fios:
http://www.wi-fiplanet.com/tutorials/article.php/3672711
http://www.wi-fiplanet.com/tutorials/article.php/2148721
http://www.esecurityplanet.com/best_practices/article.php/3740191

[5] 10 Passos para garantir segurança em *Wireless LANs*:
http://weblog.infoworld.com/smbit/archives/2006/04/10_steps_for_lo.html
http://h71028.www7.hp.com/hho/cache/387479-0-0-225-121.html

[6] SPAM no seu correio electrónico:
http://en.wikipedia.org/wiki/E-mail_spam
http://www.informationweek.com/blog/main/archives/2008/03/google_report_s.html
http://www.learningmovabletype.com/a/000246concerning_spam/ (em *Blogs*, não só *emails*)

[7] Universal PnP & DPWS:
http://www.upnp.org/
http://www.dlna.org/digital_living/how_it_works/
http://technet.microsoft.com/pt-br/library/bb457049(en-us).aspx
http://www.calsoftlabs.com/whitepapers/upnp-devices.html (inclui *Jini* e *Salutation*, menos conhecidos)

[8] DPWS - Projecto SOCRADES: http://www.socrades.eu/Home/default.html

[9] DPWS - Projecto SODA: http://www.soda-itea.org/Home/default.html

[10] *WebServices for Devices*: http://www.ws4d.org/

[11] Windows Management Instructions:
- *Background and Overview*: http://msdn2.microsoft.com/en-us/library/ms811553.aspx
- WMI *and* CIM: http://msdn2.microsoft.com/en-us/library/ms811552.aspx

[12] Workshop sobre Segurança em VoIP: http://www.iptel.org/voipsecurity/index.html

[13] Segurança VoIP - Opinião de *David Krauthamer*:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=74840&intsrc=article_pots_side

[14] Spam em VoIP – SPIT:
http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1020417,00.html
http://www.smallbusinesscomputing.com/news/article.php/3399011

[15] Solução da NEC contra SPIT: NEC *SEAL*:
http://www.securitypronews.com/insiderreports/insider/spn-49-20070129NECToSealOutVoIPSpit.html
http://www.voipcentral.org/entry/nec-to-develop-voip-seal-to-combat-ip-phone-spam/

[16] NewPort-Networks: "*Lawful Interception*" white-paper (2006)
http://www.newport-networks.com/cust-docs/87-Lawful-Intercept.pdf

[17] Segurança e Protecção de Conteúdos em IPTV:
Opinião de *Gary Southwell*: http://www.darkreading.com/document.asp?doc_id=121296

[18] Parental Control – *software review*: http://parental-control-software.upickreviews.com/

[19] D-link SecureSpot: http://www.dlink.com/products/securespot/info/

[20] SecureSpot *review*: http://blogs.pcmag.com/securitywatch/2007/11/dlink_securespot_cool_idea_com_1.php
iBoss & iPhantom – *website* oficial: http://www.iphantom.com/

[21] Tanenbaum AS. Redes de Computadores. Souza VD (Ed.). Elsevier, 2003.

[22] Wikipedia. Triple Play (telecommunications). Wikipedia (2008) p. 3.

[23] Leonel J, Paulino A & Bugbil O. Triple Play: Um fenômeno sem volta na indústria de Telecomunicações, 2007.

[24] RFC 3013 - Recommended Internet Service Provider Security Services and Procedures. 2000.

[25] Wikipedia. Traffic shaping . Wikipedia (2008) p. 5.

[26] Wikipedia. Tor (anonymity network). Wikipedia (2008) p. 4.

[27] RFC 2196 - Site Security Handbook. 1997.

[28] RFC 919 - Broadcasting Internet Datagrams. 1984.

[29] Wikipedia. Denial-of-service Attack. Wikipedia (2008) p. 7.

[30] Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks. 2007.

[31] Leyden J. Malware authors up the ante. Channel Register (2005) p. 1.

[32] Moore D, Voelker GM & Savage S. Inferring Internet Denial-of-Service Activity. (2005) p. 14.

[33] Product Documentation: NGX (R65). 2007.

[34] PF: Packet Filtering. 2007.

[35] Intrusion Detection Systems Directory. http://www.isp-planet.com/services/ids/.

[36] Wikipedia. Customer premises equipment. Wikipedia (2008) p. 1.

[37] RFC 2476 - Message Submission. 1998.

[38] Web Services Architecture Requirements. 2004.

[39] Wood C, Fernandez E & Summers R. Data base security requirements, polices and models. IBM Syst (1980) p. 24.

[40] Chapple M. Database Security Issues: Inference. About.com (2008) p. 2.

[41] Chapple M. SQL Injection Attacks on Databases. About.com (2008) p. 2.

[42] Chapple M. Database Security: A Fine Balance Between Roles and Rights. About.com (2008) p. 3.

[43] Carli F. Security Issues with DNS. SANS Institute (2003) p. 11.

[44] Mulligan J. The State of Server Operating System Security 2007. Forrester (2007) p. 7.

[45] Mulligan J. Best Practices: Server Operating System Security. Forrester (2007) p. 18.

[46] Fisher D. New Hacking Technique Exploits Common Programming Error. SearchSecurity.com (2007) p. 2.

[47] Security. http://www.openbsd.org/security.html.

[48] Perilli A. The hidden risk of virtual appliances. Virtualization.info (2007) p. 4.

[49] Leite T. Micro-Kernel ou Kernel Monolítico?. Localdomain (2007) p. 2.

[50] Wikipedia. Voice over IP. Wikipedia (2008) p. 9.

[51] Higdon J. The Top 5 VoIP Security Threats of 2008. VoIP-News (2008) p. 2.

[52] Voice Over Misconfigured Internet Telephones. http://vomit.xtdnet.nl/.

Análise de Vulnerabilidades em Provedores de Serviços TriplePlay

[53] Kuhn D, Walsh TJ & Fries S. Security Considerations for Voice Over IP Systems . NIST (2005) p. 99.

[54] RFC 3261 - Session Initiation Protocol. 2002.

[55] RFC 3436 - Transport Layer Security over Stream Control Transmission Protocol. 2002.

[56] RFC 3554 - On the Use of Stream Control Transmission Protocol (SCTP) with IPsec. 2003.

[57] Focus Group On IPTV. IPTV security requirements. ITU (2006) p. 4.

[58] Richardson R. CSI: Computer Crime and Security Survey 2007. Computer Security Institute (2007) p. 30.