Um IDS Cooperativo para Redes de Acesso de Banda Larga

Tiago Cruz[1] , Thiago Leite[1], Patrício Batista[1], Rui Vilão[1],
Paulo Simões[1], Fernando Bastos[2], Edmundo Monteiro[1]

[1] CISUC – DEI, Universidade de Coimbra,
Dep. Eng. Informática, Polo II da Universidade de Coimbra,
3030-290 Coimbra, Portugal
[2] PT Inovação SA,
Rua Eng. José Ferreira Pinto Basto, 3810-106 Aveiro, Portugal
tjcruz@dei.uc.pt, {thiago, pmbento, rpvilao}@student.dei.uc.pt,
psimoes@dei.uc.pt, fbastos@ptinovacao.pt, edmundo@dei.uc.pt

Resumo. O crescimento do número de clientes servidos por redes de acesso de banda larga (cabo, xDSL) acarreta um novo conjunto de preocupações ao nível da segurança, com potenciais consequências para os operadores de telecomunicações, para os seus clientes e para terceiros. O elevado número de clientes domésticos e tecnicamente impreparados que são actualmente servidos por conexões de elevado débito e natureza permanente constitui um cenário de risco para o qual o modelo tradicional de segurança dos operadores, centrado na sua infra-estrutura interna, é incapaz de dar resposta. Como alternativa a este cenário, propõe-se um modelo baseado no conceito de *segurança partilhada*, envolvendo a estreita cooperação entre os recursos de rede do operador e dos próprios clientes, procurando tirar partido do posicionamento que as *gateways* domésticas possuem no contexto das infra-estruturas de banda larga – como mediadores de fronteira entre as redes do operador e do cliente – para implementar um IDS/IPS (*Intrusion Detection System/Intrusion Protection System*) distribuído e escalável.

Palavras-chave: arquitecturas de segurança para serviços de banda larga, IDS distribuídos, redes domésticas.

1 Introdução

As redes de acesso de banda larga, na sua forma actual, representam um risco de segurança significativo para o *Internet Service Provider* (ISP) devido a quatro factores distintos: os elevados débitos disponíveis para cada um dos clientes; a massificação generalizada deste tipo de acesso, resultando num elevado número de clientes servidos por cada ISP; o carácter tendencialmente permanente das ligações (xDSL, Cabo, fibra óptica); e o facto de grande parte destes clientes não terem conhecimentos técnicos suficientes para garantir a segurança da sua rede doméstica. Ainda que parte dos riscos actuais existisse já anteriormente, o carácter intermitente das ligações *dial-up* clássicas e os reduzidos débitos disponíveis tornavam mais

simples aos ISP a tarefa de detectar e controlar situações de risco para as suas redes, para os seus clientes ou para terceiros.

A recente convergência dos serviços de voz, dados e televisão num mesmo canal de acesso (serviços *triple play*), aliada à profusão de serviços e aplicações com implicações nos modelos de uso tradicionais (aplicações P2P, *instant messaging*, etc.) veio agravar ainda mais o problema da segurança em ambientes de banda larga, com repercussões a vários níveis. Em primeiro lugar, os clientes, por falta de sensibilidade tecnológica têm uma crescente dificuldade para lidar com o problema de segurança ao nível das suas próprias redes domésticas, ficando estas mais vulneráveis a ataques externos que poderão posteriormente comprometer a segurança da própria rede do operador. Adicionalmente, a sucessiva adição de serviços e aplicações torna cada vez mais difícil a detecção e resolução de ataques de segurança, principalmente quando esta tarefa é confiada a sistemas centralizados na rede do operador, de limitada escalabilidade. Por último, o impacto de quebras ou limitações de serviço de conectividade IP é cada vez maior, pois os clientes esperam que os serviços tradicionais agora suportados sobre o canal de banda larga mantenham parâmetros de qualidade e fiabilidade não inferiores às experiências anteriores com meios convencionais de acesso a telefone e televisão.

A atitude tradicional dos ISP tem sido considerar que a segurança da rede do cliente está fora da sua esfera de influência, devendo ser administrada autonomamente pelo cliente. Em geral, os operadores consideram que a sua esfera de influência termina no seu equipamento de fronteira (tais como, por exemplo, os DSLAM em infra-estruturas xDSL), sendo exclusiva responsabilidade do cliente a gestão dos seus equipamentos de fronteira – que designaremos por *home gateways* – e de tudo o que esteja para lá desses equipamentos. Esta atitude está aliás alinhada com a perspectiva cultural da maioria dos utilizadores, uma vez que estes não aceitariam de bom grado a interferência do operador – implícita ou explícita – na sua rede doméstica.

As redes *triple play* começam a alterar parcialmente esta perspectiva, passando a ser necessárias e aceites algumas intervenções do operador no interior da rede do cliente, nomeadamente para administrar remotamente s*et-top boxes* (STB) de TV e *gateways* de serviço telefónico. Mesmo para além desse contexto específico, a profusão de novos dispositivos nas redes domésticas, a oferta de novos serviços (IPTV, VoD, telefone, televigilância, *online backup*…) e a mudança dos modelos de tráfego (com um peso cada vez maior de tráfego P2P) tornam necessário reavaliar estes pressupostos.

Actualmente, o modelo de segurança adoptado pelos ISPs é baseado num número relativamente reduzido de barreiras de tráfego (*firewalls*, analisadores de tráfego e outros mecanismos de IDS/IPS) posicionadas em locais estratégicos da sua rede. Como consequência do aumento de clientes, do débito das ligações de cada cliente e de novas aplicações *bandwidth intensive* essas barreiras necessitam de lidar com volumes de tráfego cada vez mais elevados e com mecanismos de análise de tráfego cada vez mais complexos, com sérias implicações ao nível da escalabilidade e dos custos destas barreiras.

Em alternativa a esse modelo, propõe-se o aproveitamento do posicionamento específico que as *gateways* domésticas possuem no contexto das infra-estruturas de banda larga – como mecanismos que fazem a mediação entre as fronteiras da rede do operador e dos clientes – para implementar um IDS/IPS (*Intrusion Detection*

System/Intrusion Protection System) largamente distribuído. Caso o operador possa usar essas *gateways* domésticas como primeiro ponto de defesa da sua própria rede, poderá implementar mecanismos de segurança mais sofisticados, mais baratos, mais escaláveis e mais granulares. Em paralelo, os tradicionais utilizadores domésticos (com reduzidos conhecimentos técnicos) beneficiarão também com esta gestão partilhada das suas *gateways*, passando a ter as suas redes domésticas potencialmente mais protegidas.

O projecto S3P (Segurança em Ambientes *Triple-Play* [1]) – conduzido pelo Grupo de Comunicações e Telemática do Centro de Informática e Sistemas da Universidade de Coimbra e pela PT Inovação – tem precisamente por objectivo a definição, implementação e avaliação de uma arquitectura de segurança baseada nesse pressuposto de melhor articulação entre as redes domésticas e a infra-estrutura do operador, enquadrando a *gateway* doméstica como um dispositivo útil, simultaneamente, ao ISP e ao cliente. Nesta comunicação são apresentados os principais aspectos da arquitectura definida no S3P, de acordo com a seguinte organização: a Secção 2 discute em maior detalhe o contexto do projecto (ambientes *Triple Play* e tendências da indústria), a Secção 3 analisa as implicações ao nível ético da solução proposta. A Secção 4 debruça-se sobre os principais aspectos da solução proposta. As Secções 5 e 6 apresentam a arquitectura da plataforma S3P em detalhe (na perspectiva da *gateway* doméstica e do operador, respectivamente). A Secção 7 constitui um sumário do trabalho prévio realizado em projectos similares. A Secção 8 apresenta as conclusões e algumas perspectivas de futuros desenvolvimentos do projecto.

2 Motivação

Tal como foi já mencionado na secção anterior, nos ambientes de banda larga a segurança da rede doméstica do cliente é tradicionalmente da sua inteira responsabilidade. Ainda que isto seja aceitável para clientes tecnicamente qualificados, coloca riscos consideráveis no caso da esmagadora maioria dos clientes domésticos, cuja capacidade para instalar e gerir mecanismos de segurança é nula ou bastante reduzida. Esta situação afecta em primeiro lugar o próprio cliente, mas acarreta também consequências para o operador. Por um lado tem um cliente potencialmente menos satisfeito (degradação de serviços prestados a esse cliente, incidentes graves de segurança na esfera do cliente). Por outro lado, caso a rede do cliente seja comprometida poderá ser usada para atacar outros clientes do ISP, o próprio operador ou terceiros. Nesse cenário, os elevados débitos oferecidos pelas actuais redes de acesso, a profusão de aplicações P2P e a convergência para cenários totalmente suportados sobre IP aumentam substancialmente os riscos, tanto para o cliente (numa perspectiva de intrusão na sua rede e acesso a dados confidenciais) como para o operador, que passa a estar muito mais vulnerável a ataques concertados de DoS e a situações de uso abusivo da sua infra-estrutura de rede.

Esta tendência tem-se reflectido na indústria, com a entrada na rede doméstica de equipamentos do operador (em especial *set-top boxes*) e com a presente tendência de normalização e convergência. Seja por iniciativas como a HGI [2] e o *Broadband*

Forum [3] seja por produtos como o *Windows Home Server* [4], passará a ser possível contar na rede de cada cliente com um conjunto homogéneo de serviços de segurança e administração remota, capazes de monitorizar a rede interna do cliente (se este assim o desejar), bem como a ligação entre a rede doméstica e a rede do operador. Diversas propostas técnicas produzidas pelo *Broadband Forum* e pela HGI apontam neste sentido, com a proposta de interfaces normalizados para configurações de serviços de segurança e operações de manutenção remota [2][5][6] em dispositivos localizados na rede do cliente.

Em conjunto, estas tendências abrem caminho para uma revisão da segurança das redes domésticas e das redes de acesso subjacentes, sendo que por um lado é necessário identificar e caracterizar as novas ameaças de segurança associadas a este cenário e por outro é necessário investigar e avaliar novas abordagens à forma de lidar com a rede doméstica do cliente.

3. Modelos de Segurança e Questões Éticas

Apesar de concebidas para proteger o ISP e/ou o cliente, praticamente todas as medidas de segurança têm efeitos secundários adversos, afectando um ou ambos os lados – a limitação de largura de banda e o *traffic shaping* por exemplo, têm sido alvo de polémica devido às suas implicações ao nível ético e legal. Estes efeitos colaterais tornam difícil alcançar o equilíbrio adequado entre a segurança e a privacidade em ambientes de banda larga.

No modelo tradicional, o ISP possui um raio de acção limitado (estando o seu perímetro de influência limitado ao nível da rede de acesso), recorrendo a barreiras de tráfego e sensores colocados em posições estratégicas para detectar e conter potenciais ataques. Uma análise simples a este modelo demonstra que este se baseia em dois pressupostos base:

- os clientes não abdicam da sua privacidade e não toleram interferências externas com os seus equipamentos e redes – sendo portanto responsáveis pela sua própria infra-estrutura

- os ISPs devem assegurar níveis adequados de segurança nas suas próprias infra-estruturas, ao mesmo tempo que restringem o seu raio de acção ao perímetro das redes de acesso

No cenário moderno das redes de banda larga, estes dois pressupostos são em larga medida incompatíveis entre si, uma vez que a maioria das ameaças é proveniente de equipamentos e redes de clientes que se encontram comprometidos. A título de exemplo, é frequente os ataques DDoS (*Distributed Denial of Service*) serem provenientes de *botnets* constituídas por aglomerados de computadores domésticos comprometidos por software malicioso, que atacam de modo concertado e coordenado – os próprios *spammers* utilizam técnicas similares para inundar os servidores de correio electrónico. No passado, estes ataques podiam ser mitigados com o recurso a medidas de contenção de tráfego activadas ao nível das barreiras

colocadas no interior da rede do ISP. Contudo, estas medidas são em parte ineficazes devido à mudança que se registou na natureza dos ataques: em vez de recorrer a um número relativamente limitado de hospedeiros comprometidos que geram fluxos de elevado débito no sentido de inundar um alvo, actualmente o número de equipamentos envolvidos é significativamente maior (envolvendo as redes de vários ISPs em vários países), caracterizando-se os fluxos de ataque pelo seu reduzido - quase insignificante - débito, em termos de tráfego gerado individualmente por cada maquina comprometida. No sentido de dar resposta a estes cenários, torna-se inevitável permitir aos ISPs que alarguem o seu raio de acção para além das restrições actualmente impostas.

A visão tradicional dos serviços de acesso de banda larga – nos quais o fornecedor apenas oferece serviços de conectividade, dando completa autonomia ao utilizador na forma de organizar a sua rede doméstica – perde algum sentido com *Triple Play* e outros serviços de valor acrescentado que dependem directamente de equipamento a colocar em casa do cliente. Na maior parte dos casos estes serviços exigem a instalação de equipamentos fornecidos especificamente pelo operador (*set-top boxes*, telefones IP, centrais de alarme…), quer por questões de compatibilidade técnica quer por estratégias comerciais (por exemplo capacidade de garantir níveis de *Digital Rights Management* apropriados para conteúdos multimédia). A crescente aceitação desses dispositivos abre caminho para uma redefinição da fronteira entre cliente e operador que permita uma melhor articulação entre a rede de acesso e a rede doméstica, sem com isso deixar de garantir a autonomia, liberdade de escolha e privacidade do cliente.

3.1 Um Novo Modelo de Segurança num Novo Cenário

Com os clientes a aceitarem voluntariamente a interferência, até certo grau, por parte dos ISPs nas suas próprias redes e equipamentos, um dos pressupostos base do modelo tradicional perde a sua relevância. Simultaneamente, as limitações do modelo de segurança tradicional tornam-no incapaz de beneficiar adequadamente do acréscimo de tolerância por parte dos subscritores dos serviços. Estas circunstâncias obrigam à adopção de uma abordagem diferente para as questões da segurança nos ambientes de banda larga.

No sentido de tirar partido da oportunidade da tolerância acrescida por parte dos utilizadores em relação à intervenção externa do ISP, propõe-se a introdução do conceito de *segurança assistida pelo operador*, baseado num modelo de gestão partilhada onde é permitido ao operador que alargue a sua influência até ao nível da *gateway* do cliente (denominada CPE – *Customer Premises Equipment*, no contexto deste projecto, ainda que o termo possua um significado mais amplo) podendo opcionalmente ir mais longe (ao nível da rede do cliente) se tal for autorizado:

- a possibilidade por parte do ISP de aceder ao CPE cria as condições necessárias para a implementação de um novo modelo de segurança baseado numa abordagem distribuída onde é possível posicionar mecanismos "inteligentes" de monitorização e segurança ao nível do CPE (na fronteira estratégica entre as redes do ISP e do cliente, em vez de centralizados ao

nível da infra-estrutura do ISP, com benefícios em termos de escalabilidade) sem interferir com a rede do cliente. Adicionalmente, nos casos em que sejam usadas exclusivamente para monitorizar o tráfego entre o ISP e o cliente, não reduzem a privacidade do cliente: o ISP poderia sempre proceder a uma monitorização semelhante dentro da sua rede, ainda que com custos substancialmente mais elevados.

- se o cliente assim o permitir, o CPE pode estender o raio de acção ao nível da sua rede interna, procurando localizar e identificar um amplo leque de vulnerabilidades, podendo mesmo recorrer a mecanismos nativos dos sistemas operativos para aceder a informações sobre as actualizações e parametrizações locais de segurança.

De certo modo, esta proposta constitui uma mudança de paradigma no que diz respeito aos modelos de segurança nas redes de banda larga, passando-se de uma arquitectura centralizada e pouco escalável para um solução distribuída, baseada num modelo de *gestão partilhada* (Tabela 1).

Tabela 1: Abordagem Tradicional vs. Gestão Partilhada.

Abordagem Tradicional	**Abordagem Proposta: Gestão partilhada**
ISP restrito à sua própria rede.	Utilizadores definem o grau de influência do ISP. Alcance mínimo conseguido pelo ISP estendido até à fronteira do CPE. Rede interna do cliente poderá ser monitorizada pelo CPE, se o cliente assim desejar e autorizar.
Barreiras estáticas dentro da infra-estrutura do ISP, actuando como limitadores de tráfego/largura de banda.	Mecanismos a nível do CPE permitem um controlo de tráfego granular.
Equipamento do CPE incorpora capacidades limitadas e a sua eficiência em termos de segurança depende largamente dos (hipotéticos) conhecimentos técnicos do cliente.	Integração do CPE na infra-estrutura de segurança, gestão partilhada entre o ISP e o cliente.
Monitorização de tráfego é exequível na infra-estrutura do ISP, ainda que com limitações em termos de escalabilidade, granularidade e custo.	Monitorização de tráfego ao nível do CPE.
Mecanismos de detecção e contenção disponíveis em caso de um ataque distribuído são limitados, lentos e ineficazes.	Capacidade de detecção de ataques em execução antes de se espalharem, através de pedidos locais ao CPE. Capacidades embebidas no CPE permitem a activação de contra-medidas rápidas e de uma forma efectiva.

4. Abordagem Proposta

4.1 Modelo de Gestão

Como resposta à crescente dificuldade em escalar soluções de segurança clássicas do lado do operador, o Projecto S3P propõe um modelo de segurança distribuído, aproveitando as capacidades de processamento e gestão remota das *home gateways,* transferindo parte das funções de segurança para o equipamento do cliente. As *home gateways* são actualmente dispositivos com capacidade computacional bastante razoável, já estão disponíveis sem custos adicionais e estão posicionadas num ponto privilegiado da rede (mediação da rede de um único cliente com a rede de acesso do operador). Podem assim ser usadas para filtrar o tráfego de rede (em ambos os sentidos), enviar informação relevante para o operador e/ou para o cliente (alarmes de segurança, padrões de utilização, etc.) e implementar medidas de protecção (por exemplo bloqueio selectivo de tráfego em resposta a eventuais ataques).

O Projecto S3P propõe assim a criação de uma estrutura descentralizada em que as *gateways* domésticas actuam na linha da frente da protecção das redes internas, de modo a conter os efeitos de um eventual ataque a uma rede doméstica ou à rede do operador, ou mesmo evitá-lo de todo. A Figura 1 ilustra esta abordagem.

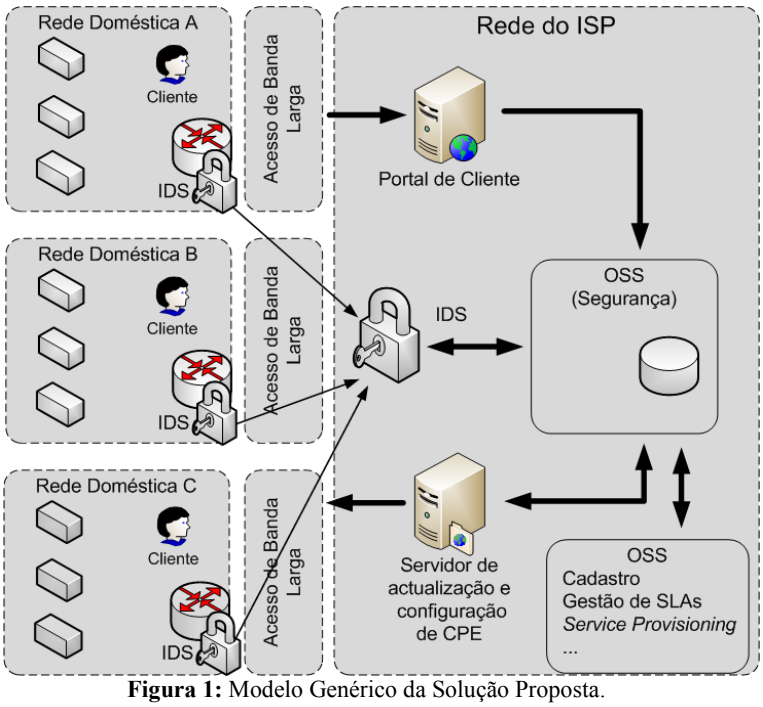

Figura 1: Modelo Genérico da Solução Proposta.

Na arquitectura S3P as *gateways* domésticas passam a funcionar de forma coordenada. Para além de realizarem funções de monitorização e prevenção de ataques através de meios próprios (com base em configurações previamente definidas pelo operador), podem também notificar o IDS do operador de determinados eventos e exercer acções de controlo de tráfego com base em instruções do IDS central.

Continuarão obviamente a existir clientes cujas *gateways* não colaborem com o IDS do ISP e que existe o risco de ter *gateways* comprometidas dentro da estrutura, pelo que o grau de confiança depositado pelo ISP em cada *gateway* doméstica nunca pode ser absoluto. A plataforma do operador terá pois de ter flexibilidade suficiente para suportar simultaneamente clientes com *gateways* cooperantes, clientes com *gateways* comprometidas e clientes sem *gateways* integradas. Apesar disso, do ponto de vista global, os potenciais ganhos de granularidade e de escala são consideráveis.

A arquitectura proposta não corresponde apenas ao "aproveitamento" da *gateway* doméstica pelo IDS do operador, tentando também aumentar efectivamente a articulação entre a rede do cliente e o ISP. Para o efeito as políticas de segurança adoptadas pelo IDS distribuído tomam em consideração o perfil do utilizador (cadastro, serviços contratados, etc.) e também permitem ao utilizador algum grau de personalização, por meio de um portal de cliente onde este pode por exemplo solicitar suporte explícito para algumas aplicações ou especificar perfis de uso mais detalhados que possam ser repercutidos no funcionamento do sistema (por exemplo controlo parental de conteúdos Web, bloqueio de acesso a servidores SMTP não previamente discriminados, etc.).

A arquitectura prevê o uso de entidades (agentes) presentes ao nível do ISP e CPE (Figura 2). Estas entidades actuarão sobre a análise do tráfego de dados transmitido, além de outros dados que possam ser obtidos a partir das bases de dados do ISP.

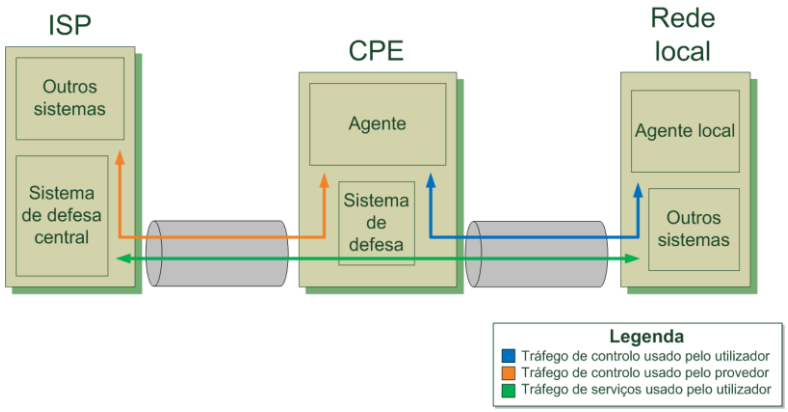

Figura 2: Âmbitos de influência no Projecto S3P

Conforme transparece da Figura 1, o modelo proposto não é completamente descentralizado, visto continuar a existir uma infra-estrutura de gestão do lado do operador que coordena os vários intervenientes neste processo, orquestrando a sua operação com base na correlação das informações recolhidas na rede do próprio operador e nos diversos CPEs.

A existência de um modelo de gestão de perfis de utilizadores permite que seja relativamente simples ao operador disseminar novas regras ou configurações para grupos alargados de utilizadores, em função dos seus perfis específicos e dos equipamentos instalados. A gestão de configurações (Figura 3) é realizada recorrendo ao servidor de auto-configuração (ACS, ou *Auto-configuration Server*), que realiza a distribuição de actualizações de software dos CPEs e a adição de novos serviços. A comunicação entre o ACS e os CPEs é assegurada por uma pilha protocolar especialmente desenvolvida para o efeito, que implementa a especificação TR-069 do *BroadBand Forum* (ou CWMP – *CPE WAN Management Protocol*), com o intuito de permitir transacções seguras entre o operador e os CPEs geridos.

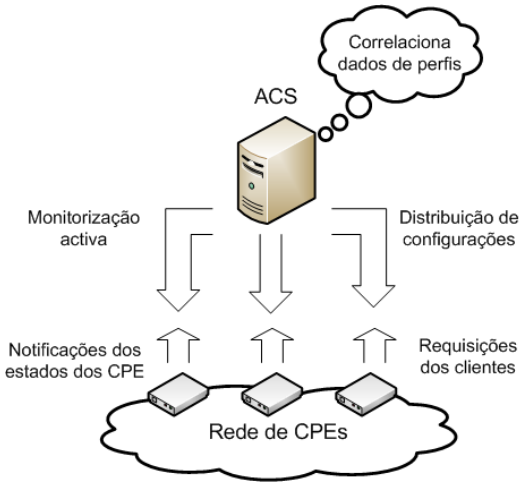

Figura 3: Relação entre ACS e CPEs

4.2 Mecanismos de Segurança e Tratamento de Eventos na Arquitectura S3P

A ideia de proporcionar um papel mais activo às *gateways* domésticas não é propriamente novidade. Ferramentas como *firewalls* e mecanismos de gestão de *QoS* fazem hoje parte da maioria desses equipamentos, podendo ser configurados pelos utilizadores por meio de interfaces *Web*. No entanto, esta abordagem à questão é limitada por um conjunto de factores:

- A responsabilidade de configurar estas ferramentas é do utilizador, que frequentemente não tem a preparação técnica adequada para o efeito.

- A *gateway* funciona de forma isolada, não havendo por exemplo correlação de ataques com outros utilizadores do mesmo ISP ou com serviços específicos do operador ou da rede local. Um ataque realizado de modo

distribuído, como é característico das *botnets,* não é detectável através da análise de uma rede isolada.

- A capacidade destas ferramentas é relativamente limitada, podendo não ser suficiente para os ataques cada vez mais sofisticados a que hoje se assiste. Uma ferramenta, por mais flexível e poderosa que seja, não é efectiva se não for acompanhada por um conjunto de regras e mecanismos adaptáveis à altura das necessidades.

Estes três factores são minimizados no projecto S3P dos seguintes modos:

- Pela maior sofisticação dos mecanismos locais de segurança, incluindo filtros de pacotes, *proxies*, detecção e prevenção de intrusos, detecção de *portscans* e vários outros mecanismos habitualmente reservados para redes de maior dimensão.

- Pela capacidade que o operador tem de correlacionar incidentes ocorridos em clientes distintos e activar mecanismos de resposta coordenados ao nível da sua rede e de todos os seus clientes.

- E pelo facto de as configurações de segurança de cada CPE serem geridas pelo operador, ainda que tendo em conta as preferências do cliente.

A detecção e o correcto tratamento de incidentes de segurança (que designaremos genericamente por *eventos*) é uma peça fundamental da arquitectura proposta. A geração e o tratamento de eventos ocorrem a dois níveis distintos:

- Ao nível do ISP. Os eventos recebidos dos diversos CPEs são correlacionados pelo motor de eventos do ISP, permitindo assim detectar, por exemplo ataques concertados a/de vários clientes do ISP. O ISP pode reagir a esses eventos tomando medidas preventivas na sua própria rede ou alterando as configurações dos CPEs (Figura 4).

- Ao nível local (CPE). Por razões de eficiência e escalabilidade, e de modo a permitir uma elevada granularidade no processo de monitorização, o CPE está dotado de um motor local de correlação de eventos (eventos esses captados pelas ferramentas de análise de tráfego, nomeadamente o sistema de detecção de intrusão, *portscans* e registos da actuação de outras ferramentas, tais como os bloqueios realizados pelo *firewall*, *proxy* e sistema de prevenção de intrusões). Todos os eventos são processados pelo motor local de correlação, podendo despoletar contra-medidas de natureza local, baseadas na aplicação de regras e procedimentos ao nível dos mecanismos de segurança do próprio CPE e/ou notificações de eventos para o ISP.

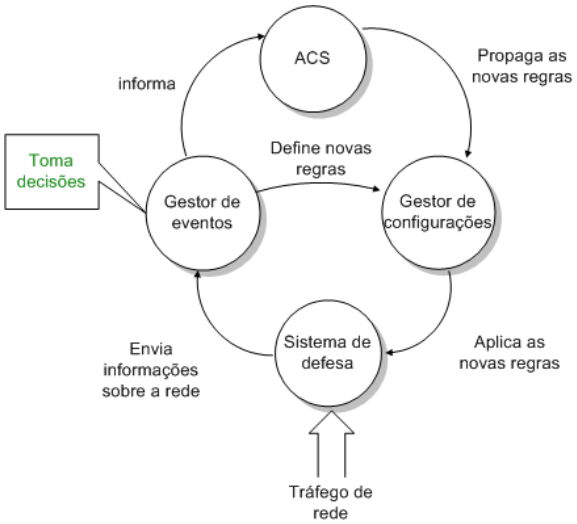

Figura 4: Modelo operacional do processo de tomada de decisões ao nível do ISP

Em termos gerais a plataforma proposta funciona como um sistema de detecção e prevenção de intrusões distribuído, abrangendo a rede do operador e os pontos de entrada/saída da rede dos clientes, sendo capaz de lidar com dois níveis de operação: CPE/microscópico e ISP/macroscópico. A título de exemplo, consideremos um conjunto de redes cliente que acabam de ser atacadas por um *trojan* e estão a cooperar num ataque DDoS (*Distributed Denial of Service*) sincronizado. Cada CPE poderá, ao detectar actividades anómalas, alertar o operador através de um evento. Do lado do operador o mecanismo de correlação, ao detectar um padrão global, efectua a distribuição de novas regras de segurança (por exemplo, restringindo o uso de um determinado conjunto de portos TCP/IP ao nível do CPE) de modo a prevenir este ataque nos restantes clientes. É nesta óptica que se destaca a importância da gestão de eventos distribuída no projecto S3P.

5. Arquitectura S3P ao Nível do CPE

A Figura 5 apresenta a arquitectura da plataforma S3P na perspectiva do CPE. Os três módulos nucleares do CPE correspondem ao sistema de defesa (*Defense System*), ao motor de gestão de eventos (*Event Management*) e à gestão de configuração (*Configuration Management*). Entre os módulos de suporte inclui-se o gestor de falhas (*Failure Management*), destinado a gerir o funcionamento do próprio CPE (avarias de hardware, perdas de configurações, etc.) e o monitor da rede do cliente (*Customer Network Monitoring*), um módulo que poderá mais tarde ser usado para monitorizar a rede doméstica do utilizador.

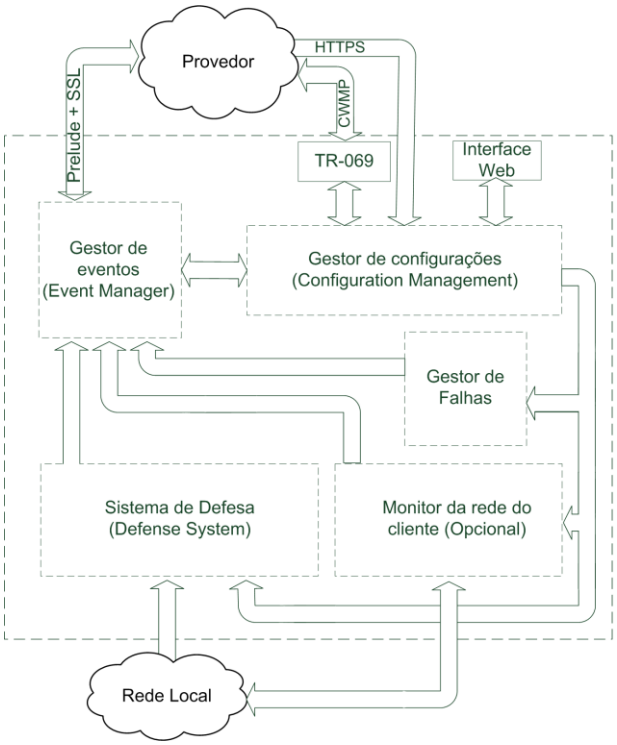

Figura 5: Arquitectura do S3P (vertente CPE)

O *Defense System* agrega os mecanismos activos de protecção do ambiente e análise passiva do tráfego que circula pelo CPE. A sua configuração (regras, listas de acesso, etc.) é controlada pelo ISP com recurso aos mecanismos anteriormente apresentados. O *Defense System* inclui os seguintes componentes: *firewall*, filtragem *Web* (*proxy* e controlo parental), sistema de detecção e prevenção de intrusão (IDS/IPS), detector de *portscans*, entre outros. Alguns destes componentes terão funções passivas (detectores de *portscans*, IDS), limitando-se a gerar eventos para tratamento pelo motor local. Outros terão também funções activas, podendo a sua configuração ser alterada dinamicamente, por decisão local ou do operador, em reacção a incidentes de segurança.

O gestor de eventos do CPE assenta na plataforma *Prelude IDS* [7], que inclui sofisticados mecanismos programáveis para processamento e correlação de eventos [8]. Nesta ferramenta os eventos são provenientes de sensores (agentes simples) que recolhem informação proveniente de diversas fontes e a partir daí constroem mensagens IDMEF *Intrusion Detection Message Exchange Format*) [9] que posteriormente são enviadas para o módulo de gestão de eventos através de uma ligação segura e mantidas numa base de dados local.

O Gestor de Configurações assegura a gestão das configurações do CPE (serviços instalados, configurações activas). As actualizações podem ser despoletadas remotamente pelo ISP ou pelo próprio CPE (alteração de configuração decidida localmente para reacção a incidente de segurança).

6. Arquitectura S3P do Ponto de Vista do ISP

A Figura 6 apresenta a arquitectura da plataforma, do lado da infra-estrutura do operador. Os principais componentes correspondem ao gestor de perfis (*Profile Management*), ao gestor de eventos de segurança (*Security Event Management*) e ao gestor dos CPEs (*CPE Management*).

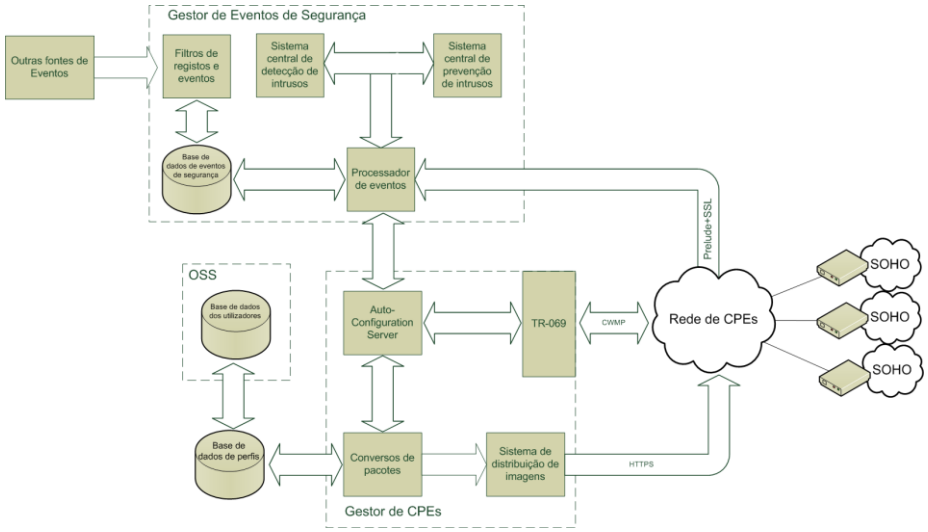

Figura 6: Arquitectura S3P (componentes do lado do ISP)

O gestor de eventos de segurança corresponde a um sistema correlacionador de eventos de segurança – alimentado pelos gestores de eventos de cada CPE e também por eventos detectados por sensores instalados na própria rede do operador – que permite correlacionar acontecimentos ocorridos em pontos distintos da rede e accionar respostas orquestradas a esses acontecimentos – por exemplo bloqueio de tráfego ao nível da rede do operador e/ou reconfigurações de *firewalls* dos CPEs.

A gestão dos CPE lida essencialmente com a configuração remota dos CPE (distribuição das aplicações e das configurações que devem aplicadas por cada CPE) e na monitorização do funcionamento do CPE (detectando e reagindo a falhas de funcionamento). Estas ferramentas servem para gestão de configuração, numa perspectiva genérica (inventário, *updates*, etc.) e são também o mecanismo de actuação remota que o ISP usa para alterar dinamicamente a forma de funcionamento dos CPE em resposta a incidentes de segurança.

A gestão de perfis assegura a manutenção de uma base de dados com perfis de equipamentos (fabricantes das CPE, modelos e versões instalados em cada cliente) e de utilizadores (serviços contratados ao ISP, preferências definidas no portal de cliente, etc.). Estes perfis são essenciais para definir que configurações devem ser enviadas para cada CPE.

7. Trabalho Relacionado

Apesar da relevância que assume actualmente a protecção de redes de acesso de banda larga, e da profusão de propostas de plataformas de IDS distribuídas, não existem, tanto quanto é do nosso conhecimento, outras propostas de integração de dispositivos domésticos em plataformas de segurança geridas de modo concertado por ISPs. Deste modo, os trabalhos mencionados nesta secção são distintos da plataforma S3P, ainda que com alguns pontos de contacto.

Koutepas [10] e Wan [11] [12] apresentaram um conjunto de propostas para lidar com ataques DDoS, baseadas em sistemas de detecção locais, posicionados estrategicamente ao longo da Internet, constituindo um sistema distribuído de detecção de ataques. Ao nível interno deste DIDS, os alertas são comunicados com recurso a mensagens IDMEF – uma vez detectado um ataque, são activados um conjunto de mecanismos de limitação de débito de tráfego no sentido de conter a ameaça.

Ioannidis et al [13], propõem uma solução para o problema dos ataques DDoS, utilizando *routers* quer para a detecção quer para a resposta aos ataques. Uma vez detectado um ataque DDoS, o sistema utiliza filtros específicos para bloquear o tráfego ao nível dos *routers.* Entre *routers* cooperantes, os eventos são comunicados com recurso ao protocolo *Pushback* desenvolvido para o efeito – deste modo, as fontes dos ataques vão sendo alvo de um cerco progressivo, ao mesmo tempo que são subjugadas ao uso controlado da largura de banda disponível.

8. Conclusão

Esta arquitectura distingue-se por aproveitar activamente a gateway doméstica – enquanto dispositivo de fronteira entre a rede de acesso e a rede doméstica – para criar uma plataforma distribuída de segurança, com ganhos para o operador (maior escalabilidade e granularidade, menores custos com sistemas centralizados na sua própria rede) e para o cliente. Ainda que esta abordagem pareça ir contra a visão tradicional do serviço Internet – com a fronteira na rede de acesso do ISP – ela ajusta-se bem aos recentes desenvolvimentos com a introdução de redes *Triple Play* e com a crescente adopção pelos fabricantes de normas como o TR-069 para gestão remota de CPEs.

Está actualmente em curso a validação deste protótipo numa rede piloto da PT Inovação, de modo a que se possam recolher dados para um trabalho mais extenso de validação da escalabilidade da plataforma, por meio de medições experimentais e de métodos analíticos.

Agradecimentos. Este trabalho de investigação é parcialmente financiado pela Fundação para a Ciência e Tecnologia, através do projecto DOMUS (POSC/EIA/61076/2004) e pela PT Inovação, através do projecto S3P.

Referências

1. Projecto S3P, http://s3p.dei.uc.pt
2. HGI (2006), "Home Gateway Technical Requirements: Release 1, Version 1.0", Home Gateway Initiative (online), http://www.homegatewayinitiative.org/publis/HGI_V1.0.pdf, Julho de 2006.
3. Broadband-forum, http://www.broadband-forum.org
4. WHS (2007), "Windows Home Server" (online), Microsoft Corporation, http://www.microsoft .com/windows/products/winfamily/windowshomeserver
5. Broadband-forum (2006), "Functional Requirements for Broadband Residential Gateway Devices (TR-124) issue 1.0" (online), Broadband Forum, http://www.broadband-forum.org/technical/ download/TR-124.pdf, Dezembro de 2006.
6. Broadband-forum (2007), "CPE WAN Management Protocol (TR-069) specification v1.1", http://www.broadband-forum.org/technical/download/TR-069Amendment2.pdf, Dezembro de 2007.
7. Vandoorselaere, Yoann (2008), "Prelude Universal SIM: State of the Art" (online), *Libre Software Meeting* 2008, http://www.prelude-ids.com/fileadmin/templates/pdf/ RMLL_2008.pdf, Mont-de-Marsan , France, July 2008
8. Chifflier, Pierre and Tricaud, Sébastien (2008), "Intrusion Detection Systems Correlation: a Weapon of Mass Investigation" (online), CanSecWest 2008, http://www.prelude-ids.com/fileadmin/templates/pdf/ correlation-womi-cansec2008.pdf, Vancouver, Canada, March 2008
9. Debar, H. et al (2007), "The Intrusion Detection Message Exchange Format (IDMEF)", RFC 4765, March 2007
10. Koutepas, G., Stamatelopoulos. F. ,Maglaris, B., "Distributed Management Architecture for Cooperative Detection and Reaction to DDoS Attacks", Journal of Network and Systems Management, Vol. 12, No. 1, March 2004
11. Wan, K. and Chang R., "Engineering of a global defense infrastructure for DDoS attacks", Proc. of IEEE International Conference on Networking, August 2002.
12. Wan, K., "An infrastructure to defend against distributed denial-of-service attack", M.Sc. Thesis, Hong Kong Polytechnic University, June 2001.
13. Ioannidis, J. and Bellovin S., "Implementing pushback: Router-based defense against DDoS attacks", Network and Distributed System Security Symposium 2002, San Diego, California, February 2002.