Segurança em Redes de Acesso *Triple-Play*

T. Cruz[1], T. Leite[1], P. Baptista[1], R. Vilão[1], P. Simões[1], F. Bastos[2], E. Monteiro[1]

[1] CISUC - DEI, Universidade de Coimbra
[2] PT Inovação - Aveiro

tjcruz@dei.uc.pt

Resumo

O S3P é um projecto de investigação levado a cabo pelo grupo de Comunicações e Telemática do Centro de Informática e Sistemas da Universidade de Coimbra e pela PT Inovação. Este projecto tem por objectivo a identificação de novos riscos de segurança, introduzidos pela crescente disseminação de redes domésticas ligadas à Internet por banda larga (ADSL, cabo, fibra, 3G), e a investigação de soluções para neutralizar esses riscos. Apresenta-se aqui a arquitectura de gestão distribuída para ambientes "triple-play" que foi desenvolvida no âmbito deste projecto. Esta arquitectura, especificamente orientada para as questões da segurança nestes ambientes, caracteriza-se pelo seu carácter fortemente distribuído (melhorando assim a escalabilidade do sistema) e pela forma como integra nas soluções de segurança do operador dispositivos presentes nas redes dos clientes e na fronteira entre as redes dos clientes e a rede de acesso do operador.

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), pela associação entre quatro factores: os elevados débitos disponíveis para cada um dos clientes; a massificação generalizada deste tipo de acesso, resultando num número de clientes servidos por cada ISP; o carácter tendencialmente permanente das ligações (xDSL, Cabo); 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 (*triple play*), aliada à profusão de serviços e 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 é cada vez maior, pois os clientes esperam que os serviços agora suportados sobre o canal de banda 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 pára no seu equipamento de fronteira (e.g. DSLAMs), sendo responsabilidade do cliente a gestão dos seus equipamentos de fronteira – *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, que veria com maus olhos 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 *set-top-boxes* (STB) 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 premente repensar estes pressupostos.

Mesmo sem colocar em causa a autonomia e privacidade dos utilizadores domésticos, existe actualmente uma janela de oportunidade para questionar o actual modelo de segurança, tentando articular melhor os mecanismos de segurança ao nível do ISP com os mecanismos de segurança disponíveis em cada rede doméstica. No modelo actual os operadores tentam controlar o tráfego montagem "barragens" num conjunto relativamente reduzido de pontos da sua própria rede. Essas "barragens" necessitam por conseguinte de lidar com volumes de tráfego substancialmente elevados, com as consequentes implicações ao nível de custos, escalabilidade e granularidade.

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 escaláveis e mais granulares. Em paralelo, os próprios utilizadores sem conhecimentos técnicos beneficiarão com esta gestão partilha das suas *gateways*, passando a ter redes domésticas mais protegidas.

O Projecto S3P – um trabalho de investigação levado a cabo pelo grupo de Comunicações e Telemática do Centro de Informática e Sistemas da Universidade de Coimbra e pela PT Inovação – tem por principais objectivos a definição, implementação e avaliação de uma arquitectura de segurança baseada nesse pressuposto de melhor articulação entre redes domésticas e rede do operador, passando a encarar a *gateway* doméstica como um dispositivo útil ao ISP e ao cliente. Nesta comunicação são apresentados os principais aspectos da arquitectura do 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 apresenta os traços gerais da solução proposta, e as Secções 4 e 5 apresentam a arquitectura da plataforma S3P (na perspectiva da *gateway* doméstica e do operador, respectivamente). A Secção 6 apresenta as conclusões e discute trabalho futuro.

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 aumenta 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.

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 DRM 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.

Esta tendência tem-se reflectido na indústria, com a entrada na rede doméstica de equipamentos do operador (em especial set-topboxes) e com a presente tendência de normalização e convergência. Seja por iniciativas como a HGI [1] e o Broadband Forum (ex-DSL Forum) [2] seja por produtos como o *Windows Home Server* [3], 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) e a ligação entre a rede doméstica e a rede do operador. Diversas propostas técnicas produzidos 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 [4-6] em dispositivos localizados na rede do cliente (CPE, *Customer Premise Equipment*).

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

3. Abordagem Proposta

3.1 Modelo de gestão e integração na infra-estrutura do operador

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*. Transferem-se assim parte das funções de segurança para o equipamento do cliente. As *home gateways* são actualmente dispositivos com capacidade computacional bastante razoável (processadores entre 200 e 400 MHz, memória RAM adequada, versões reduzidas de Linux), já estão disponíveis sem custos adicionais e estão 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). 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.

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.

Essas *gateways* (designadas por CPE no âmbito do S3P, ainda que habitualmente o termo CPE tenha um âmbito mais alargado) 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.

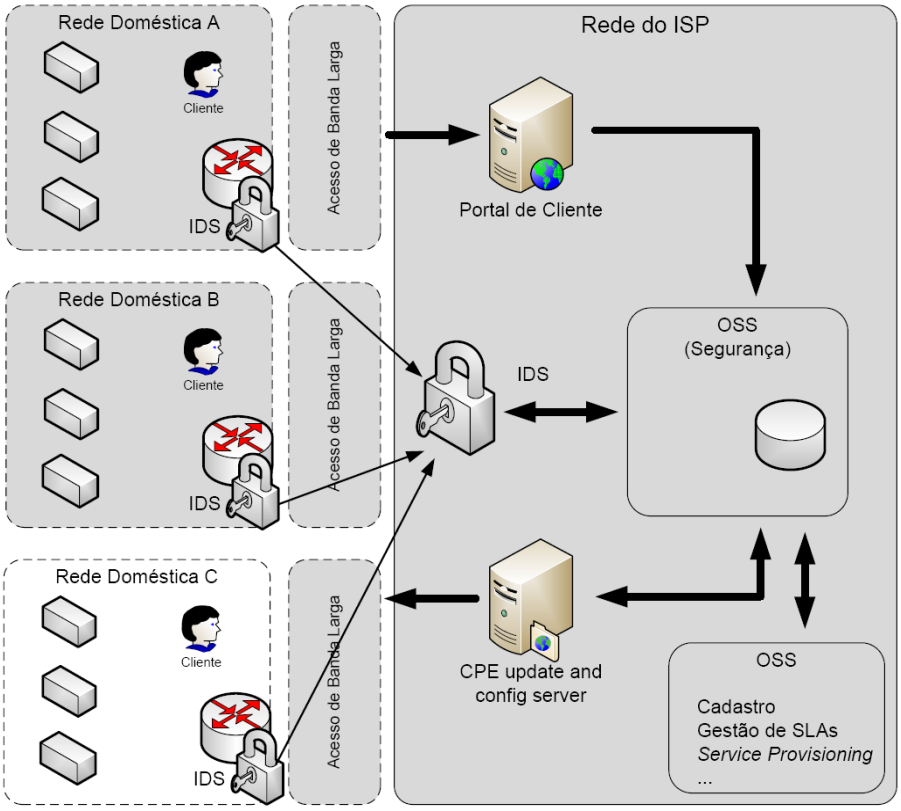

Figura 1. Modelo Genérico da Solução Proposta.

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.). Este cruzamento de informação é útil para o ISP e para o próprio cliente.

No seu essencial, a solução proposta pelo projecto S3P vai de encontro à noção de IDS distribuído. Este modelo conceptual é suportado por várias estações colectoras de dados e uma ou várias estações centrais que realizam a correlação dos dados obtidos. Independentemente de aspectos como as topologias adoptadas [7] [8] ou mesmo a disposição das estações colectoras [9] a ideia base tem-se vindo a manter relativamente inalterada desde a sua concepção. O projecto S3P procura integrar esta noção num contexto mais específico, com recurso às tecnologias existentes e especificamente desenvolvidas para os ambientes de banda larga.

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. Para que haja coordenação entre os CPE dos diversos clientes, será adicionalmente necessário o suporte por aplicações centrais ao nível do operador. Estas aplicações fornecerão actualizações e outras rotinas de verificação, monitorização e configuração.

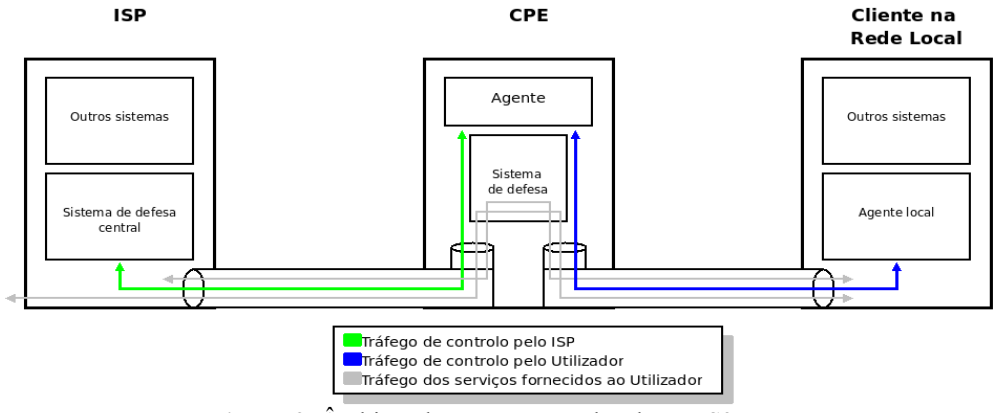

Figura 2. Âmbitos de actuação na abordagem S3P.

Conforme transparece da Figura 1, o modelo proposto não é totalmente 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.

Para a comunicação entre as aplicações do operador e os CPEs optou-se pela norma TR-069 ou CWMP (*CPE WAN Management Protocol* [5]), desenvolvida pelo *Broadband Forum* para a gestão remota de equipamentos da rede doméstica. O TR-069 pertence ao âmbito das *Broadband Suites* do referido *forum*, fazendo assim parte de uma família mais de normas e protocolos extensíveis e orientados para a gestão em ambientes de banda larga. Esta norma tem vindo a conhecer crescente aceitação, sendo de esperar que seja gradualmente integrada por todas as aplicações de administração, do lado dos operadores, e por todos os equipamentos, pelo lado dos fabricantes de CPEs (em especial routers/modems ADSL e *set top boxes*).

A adopção do TR-069, complementado pelo já referido 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.

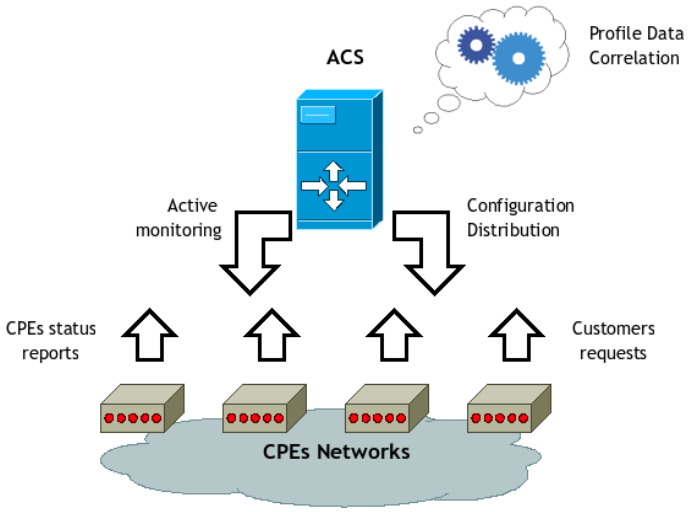

Figura 3. Operação com recurso ao protocolo TR-069.

A gestão de configurações é realizada recorrendo ao servidor de auto-configuração (ACS, ou *Auto-configuration Server*, segundo a terminologia TR-069), que realiza a distribuição de actualizações de software dos CPEs, a adição de novos serviços e a gestão dos perfis do ambiente. A maior parte das transacções realizadas entre o ACS e os CPEs são já normalizadas pelo *Broadband Forum*, tendo as restantes transacções

sido implementadas como extensões da norma TR-069, de acordo com o modelo de extensões *vendor-specific* previstas na norma. A Figura 3 ilustra o relacionamento entre os CPE e o ACS.

3.2 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* (inicialmente do tipo *stateless* e, mais recentemente, *stateful*) e mecanismos de gestão de *QoS* fazem hoje parte da maior parte 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 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 nas necessidades.

Estes três factores são minimizados, no projecto S3P, de vários 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 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 do tráfego, nomeadamente o sistema de detecção de intrusão e *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. Um potencial ataque que seja detectado através dos registos do IDS será enviado ao correlacionador de eventos que por sua vez deverá acionar a(s) medida(s) adequada(s) quando determinar que exista ameaça ao ambiente. Os eventos poderão ser enviados para o ISP se a gravidade da ocorrência assim o exigir e/ou ser utilizados localmente para geração de regras de modo automático.
- 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). Um exemplo deste modelo seria por exemplo a detecção de um

ataque concertado por meio de uma *botnet*, com diversos clientes infectados, e a distribuição pelos CPEs de regras de bloqueio das portas usadas por essa *botnet*.

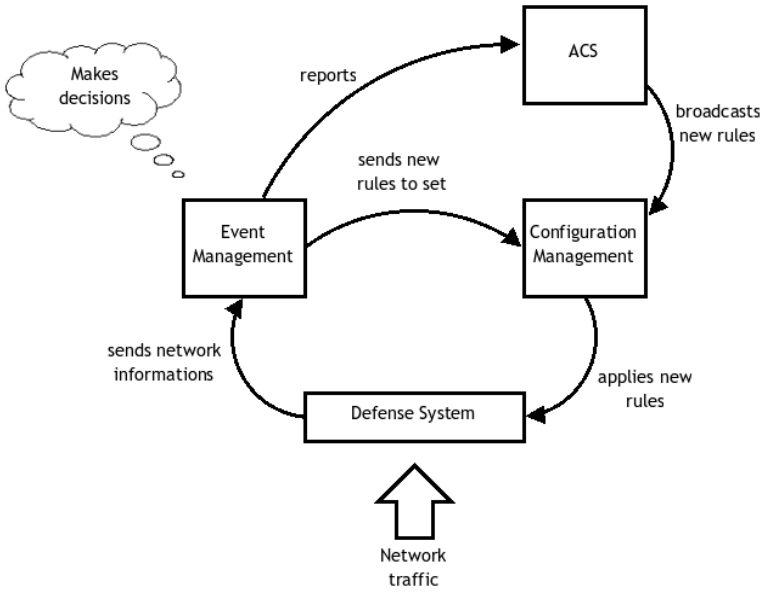

Figura 4. Modelo operacional de tomada de decisão na arquitectura S3P.

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. 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. Os CPEs poderão, ao detectar actividade anómala, 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 de modo a prevenir este ataque nos restantes clientes. O mecanismo de correlação actua de acordo com os perfis associados ao ambiente em questão. Padrões de tráfego que não estejam de acordo com as premissas do perfil poderão ser considerados como eventos passíveis de activar contramedidas por parte deste mecanismo. É nesta óptica que se destaca a importância da gestão de eventos distribuída no projecto S3P.

Em termo de tecnologias, optou-se por uma solução capaz de suportar em simultâneo os dois níveis de funcionamento (CPE, ou microscópico, e operador, ou macroscópico) e com bons mecanismos de comunicação entre os dois níveis. Essa solução assenta na ferramenta *Prelude IDS* [10], ao nível de ambos os motores de correlação, e em IDMEF (*Intrusion Detection Message Exchange Format* [11]), ao nível da comunicação de eventos entre os CPEs e o operador. O IDMEF é um protocolo recentemente proposto pelo IETF para troca de informação relacionada com eventos de segurança, esperando-se que seja gradualmente aceite pela indústria como norma aberta para troca de informações de segurança. Esta solução será discutida em maior pormenor nas Secções 4 e 5.

4. Arquitectura da Plataforma S3P (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[1].

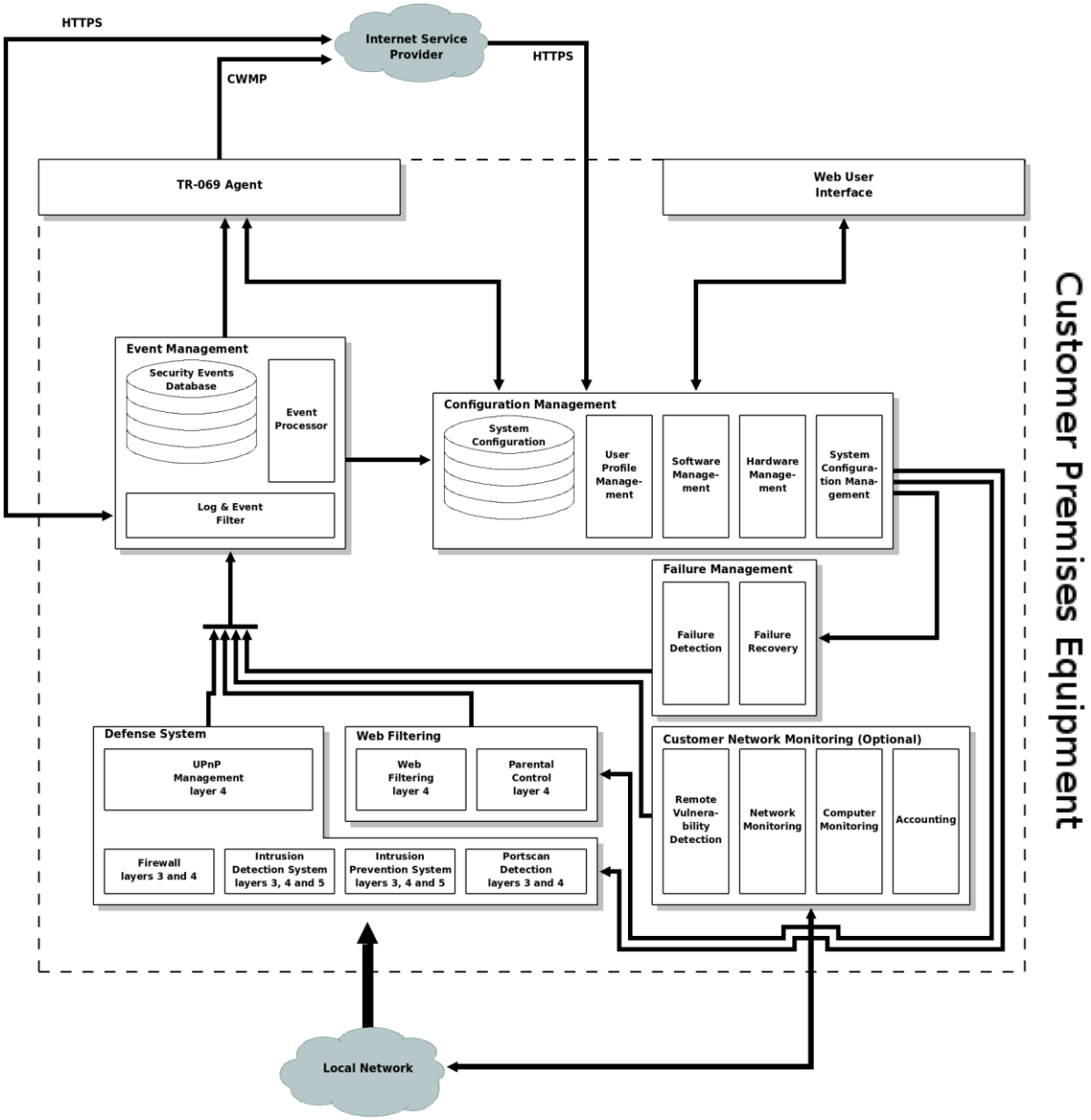

Figura 5. Arquitectura da Plataforma S3P (CPE)

Do ponto de vista de hardware, optou-se por uma plataforma de referência ligeiramente acima da capacidade dos *routers* de banda larga correntes. Em vez dessa capacidade corrente (tipicamente com CPUs entre 200 e

[1] Este módulo não foi até agora objecto de trabalho no projecto S3P e poderá suscitar algumas questões éticas, já que permitirá ao operador monitorizar proactivamente a própria rede local do seu cliente, detectando e/ou colmatando falhas de segurança (por exemplo PCs locais com fragilidades de segurança). No entanto, do ponto de vista arquitectural é importante inclui-lo pelos serviços adicionais de segurança que oferece e que poderão interessar a determinados clientes.

400 MHz e cerca de 256 Mbyte de RAM) optou-se por tomar como referência uma configuração que será previsivelmente atingida dentro de 2 a 3 anos: CPUs com velocidades na ordem dos 900 MHz, 512 Mbyte a 1 Gbyte de RAM, 2 a 4 Gbyte de capacidade de armazenamento não volátil. Espera-se que esta configuração se torne vulgar dentro de pouco tempo – em especial por via da disseminação da plataforma Atom, da Intel, que reduzirá significativamente os custos deste tipo de dispositivos – e com ela torna-se mais simples integrar um grande número de ferramentas *opensource* disponíveis para Linux.

4.1 *Defense System*

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 sistema de gestão de configurações que pode actuar em consonância com regras criadas pelo correlacionador de eventos ou através de comandos enviados pelo operador.. Para que isto seja possível, os componentes de software serão geridos através da distribuição de pacotes personalizados. 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* e um gestor de dispositivos *UPnP* (*Universal Plug and Play* [12]).

Alguns destes componentes terão funções passivas (detectores de *portscans*, IDS e e gestor uPnP), 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.

Do ponto de vista de implementação do protótipo, todos estes componentes foram integrados a partir de ferramentas *opensource* já disponíveis (*GD UPnP*, *squid*, com *plug-in SquidGuard*, *scanlogd*, *Iptables*, *Snort* e *Snort inLine*), o que facilita a futura actualização da plataforma. A justificação para o uso das referidas ferramentas deve-se á sua popularidade, facilidade de manutenção, suporte e disseminação.

4.2 Gestão de Eventos

Tal como foi já mencionado, o gestor de eventos do CPE assenta no *Prelude IDS*. Nesta ferramenta os eventos são provenientes de sensores (agentes simples que analisam fontes de informação e a partir daí constroem mensagens IDMEF que posteriormente são enviadas para o módulo de gestão de eventos através de uma ligação segura) e mantidas numa base de dados local. Para além de existirem já sensores parametrizáveis para as ferramentas de segurança mais comuns (incluindo parte das ferramentas usadas pelo *CPE Defense System*) e para os serviços de rede mais habituais, é simples construir novos sensores, expandindo assim o sistema.

O processador de eventos inclui mecanismos sofisticados de correlação e de tratamento de eventos, usando para o efeito a linguagem LUA [13]. Esta é uma inovação que desataca o *Prelude IDS* dos outros HIDS existentes no mercado. Segue-se um exemplo para detecção de um ataque por força bruta a um sistema de autenticação interactivo, descrito na linguagem LUA:

```
function brute_force(INPUT)

local is_failed_auth = INPUT:match("alert.classification.text",
 "[Ll]ogin|[Aa]uthentication","alert.assessment.impact.completion",
 "failed")

local userid = INPUT:get("alert.target(*).user.user_id(*).name");

if is_failed_auth and userid then
 for i, user in ipairs(userid) do
    local ctx = Context.update("BRUTE_U_" .. user, { expire =
     120,threshold = 2 })
    ctx:set("alert.source(>>)", INPUT:getraw("alert.source"))
    ctx:set("alert.target(>>)", INPUT:getraw("alert.target"))
    ctx:set("alert.correlation_alert.alertident(>>).alertident",
```

```
    INPUT:getraw("alert.messageid"))
    ctx:set("alert.correlation_alert.alertident(-1).analyzerid",
    INPUT:getAnalyzerid())

    if ctx:CheckAndDecThreshold() then
     ctx:set("alert.classification.text", "Brute force attack")
     ctx:set("alert.correlation_alert.name", "Multiple failed login")
     ctx:alert()
     ctx:del()
    end
 end
end

end -- function brute_force(INPUT)
```

O motor de correlação é um mecanismo de natureza não-reactiva, dotado de memória. Os eventos, ao serem enviados para o motor de correlação, irão despoletar o processamento de todos os *scripts* registados no respectivo módulo. Assim, cabe ao programador fazer as verificações necessárias de modo a que sejam capturados os eventos correctos para correlação, sendo esta a primeira acção a ser efectuada - no exemplo acima mencionado existe uma verificação para confirmar se o texto capturado é proveniente de uma autenticação que não tenha sido bem-sucedida.

De seguida é extraído o utilizador ao qual o login foi negado. A partir daqui é iterado um ciclo para cada utilizador envolvido no evento (note-se que é possível ter vários utilizadores associados a um login falhado, pois poderão ser provenientes de uma anterior correlação), onde é verificado se este é reincidente recorrendo para o efeito à memória do correlador de eventos (Context.update). Caso não exista um contexto associado áquela chave, então irá ser criado uma nova instância com uma expiração de 120 minutos e um limite de duas ocorrências, i.e., para o um novo evento ser despoletado (ctx:alert()), terão de ocorrer duas falhas no espaço de dois minutos.

Estes mecanismos são bastante flexíveis, permitindo definir os vários tipos de comportamento previstos para a plataforma S3P: descarte de eventos; registo local de eventos, para histórico (por exemplo correlação com eventos futuros); tomada de decisões locais, com execução de medidas autónomas de resposta a incidentes de segurança; envio para o ISP de eventos locais (sejam eles os eventos originais ou eventos agregados), usando IDMEF, para que possam ser correlacionados com eventos de outros clientes e dar origem a respostas concertadas ao nível do operador.

Neste contexto, a correlação de eventos é importante na medida em que permite reduzir o número de alertas recebidos ao nível do operador, visto existirem eventos cujo processamento e tratamento será feito localmente a nível do CPE. Além disso, é necessário ter em conta que nem todos os eventos deverão gerar alertas, pois nem todos apresentam a mesma severidade. A título de exemplo: caso exista uma tentativa de autenticação no CPE com um conjunto de credenciais inválidas, será gerado um evento mas à partida este evento *per se* não deverá ser considerado um ataque. No entanto, se a mesma situação se repetir várias vezes no espaço de um minuto, podemos considerar que se trata de um ataque por força bruta. Caberá então ao mecanismo de correlação fazer a distinção entre as duas situações e, caso se verifique um ataque, gerar um alarme para o sistema tomar alguma medida de segurança que poderá passar, por exemplo, pelo bloqueio do endereço IP de onde provém o ataque na *firewall* local (Figura 6).

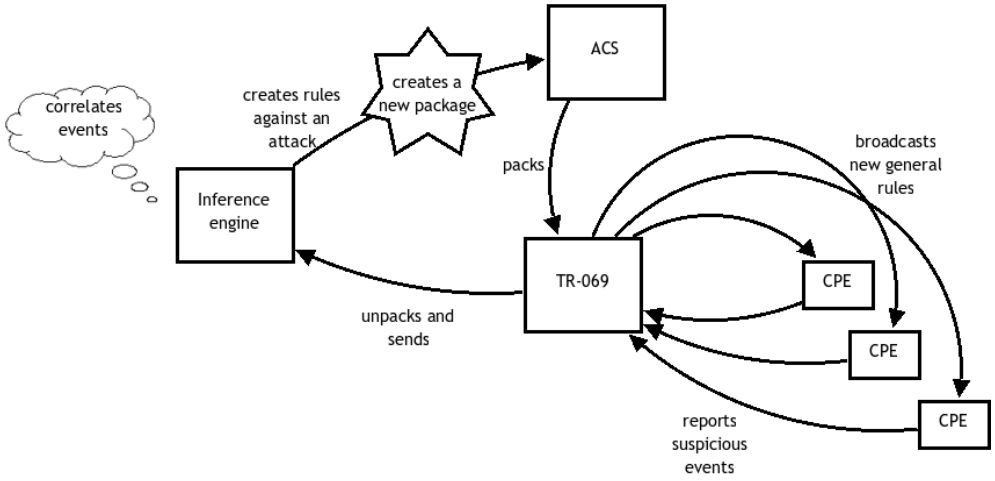

Figura 6. O mecanismo de correlação de eventos na perspectiva macroscópica

4.3 Gestão de Configurações

O Gestor de Configurações assegura a gestão das configurações do CPE (serviços instalados, configurações activas). As actualizações podem ser despoletadas remotamente pelo ISP (envio de um novo serviço ou de versão actualizada de um serviço já existente; envio de novas configurações para *firewall*, etc.) ou pelo próprio CPE (recuperação de configurações em caso de falha do *file system*, alteração de configuração decidida localmente para reacção a incidente de segurança…). Através do gestor de configurações é garantido que todas as alterações, sejam elas ao nível dos serviços ou regras de segurança, sejam aplicadas nos CPEs com o uso de pacotes que podem ser enviados pelo ISP, como actualização, ou gerados localmente.

5. Arquitectura da Plataforma S3P (na óptica do Operador)

A Figura 7 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*). Entre os módulos complementares, incluem-se o Gestor de Falhas (*Failure Management*) e o monitor da rede do cliente (*Customer Network Monitoring*), assim como os componentes de integração com os sistemas OSS (*Operations and Support Systems*) e AAA (*Authentication, Authorization, and Accounting*) do operador.

5.1 Gestão de Eventos de Segurança

O gestor de eventos de segurança corresponde a um concentrador 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.

Ao nível de tratamento de eventos é mais uma vez usado o *Prelude IDS*, num formato semelhante ao já descrito para os CPE. Relativamente às ferramentas de IDS e IPS que actuam na rede do operador, a plataforma S3P é neutra, podendo à partida ser integrada com as ferramentas que os operadores tenham já em exploração.

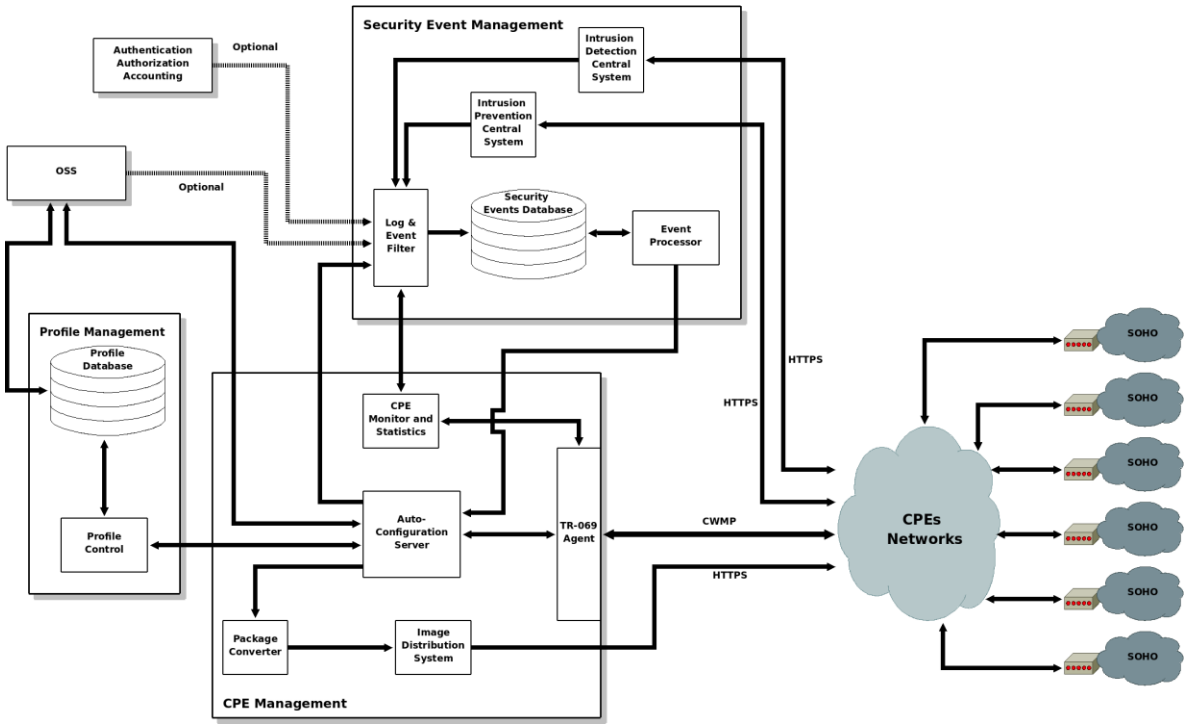

Figura 7. Arquitectura S3P (do lado da infra-estrutura do operador).

5.2 Gestão de CPE

A gestão dos CPE consiste essencialmente na 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 monitorização e troca de informação entre o ISP e os CPE usa canais seguros e a já referida norma TR-069, e a distribuição de aplicações e configurações segue um modelo de distribuição de imagens (pacotes).

5.3 Gestão de Perfis

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.).

Do ponto de vista da plataforma S3P estes perfis são essenciais para definir que configurações devem ser enviadas para cada CPE. Estes perfis também determinam os padrões de tráfego aceitáveis para cada ambiente, de modo a que eventuais desvios possam ser detectados e eventualmente interpretados como passíveis de despoletar reacções por parte do IDS distribuído.

6. Conclusão

Nesta comunicação foram apresentados os aspectos mais relevantes da arquitectura proposta pelo Projecto S3P. 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.

O protótipo desenvolvido mostrou que é possível implementar esta plataforma distribuída com base em ferramentas *open source* – resultando em menores custos de desenvolvimento e manutenção – e normas já adoptadas pela indústria. Esse protótipo usa para os CPE uma plataforma de *hardware* com capacidades superiores às das *gateways domésticas* actualmente comercializadas pelos ISP, mas espera-se que num prazo de 2 a 3 anos as gateways domésticas atinjam essas capacidades sem acréscimos de custo, tornando possível a massificação de plataformas como o S3P.

O próximo passo será a validação deste protótipo com utilizadores reais, numa rede piloto, de modo a que se possa depois avançar com um trabalho mais extenso de validação da escalabilidade da plataforma, por meio de medições experimentais e de métodos analíticos.

7. Agradecimentos

O trabalho de investigação subjacente a esta comunicação foi parcialmente financiado pela Fundação para a Ciência e Tecnologia, por meio do Projecto DOMUS (referência POSC/EIA/61076/2004) e pela PT Inovação, por meio do Projecto S3P.

Referências

[1] *Home Gateway Initiative*, http://www.homegatewayinitiative.org/

[2] *Broadband Forum* (ex-*DSL Forum*), http://www.dslforum.org

[3] Windows Home Server, www.microsoft.com/windows/products/winfamily/windowshomeserver

[4] HGI, Home Gateway Technical Requirements: Release 1, Version 1.0, July 2006.

[5] DSL Forum TR-069, Amendment 1, CPE WAN Management Protocol, November 2006.

[6] DSL Forum TR-124, Functional Requirements for Broadband Residential Gateway Devices, December 2006.

[7] R. Puttini, J.-M. Percher, L. Me, R. de Sousa, A fully distributed IDS for MANET, Proceedings of the Ninth International Symposium on Computers and Communications 2004 Volume 2 (ISCC"04) - Volume 02, pp. 331-338, 2004

[8] Luo Guangchun, Lu Xianliang, Li Jiong, Zhang Jun, MADIDS: a novel distributed IDS based on mobile agent, ACM SIGOPS Operating Systems Review Volume 37, Issue 1, pp. 46-53, January 2003

[9] Jing Wang, Naoya Nitta, Hiroyuki Seki, An Efficient Method for Optimal Probe Deployment of Distributed IDS, IEICE - Transactions on Information and Systems Volume E88-D Issue 8, pp. 1948-1957, August 2005

[10] PreludeIDS Technologies, http://www.prelude-ids.com

[11] H. Debar, et al, The Intrusion Detection Message Exchange Format (IDMEF), RFC 4765, March 2007

[12] Universal Plug and Play Forum, http://www.upnp.org/

[13] PUC-Rio, http://www.lua.org