ARQUITECTURAS DE QOS INTRA-DOMÍNIO

Carlos Rabadão[1, 2], Edmundo Monteiro[2]
[1] *Escola Superior de Tecnologia e Gestão*
Instituto Politécnico de Leiria
Morro do Lena – Alto do Vieiro, 2411-901 Leiria, Portugal
{crab}@estg.ipleiria.pt
[2] *Laboratório de Comunicações e Telemática, CISUC / DEI*
Universidade de Coimbra
Polo II, Pinhal de Marrocos, 3030-290 Coimbra Portugal
{crab, edmundo}@dei.uc.pt

RESUMO

O principal objectivo do modelo de Serviços Diferenciados da IETF (DiffServ) é permitir o suporte de diferentes níveis de serviço a diferentes fluxos de informação agregados em classes de serviço (CoS), sobre uma infra-estrutura de comunicações TCP/IP. Este tratamento diferenciado poderá levar a que alguns utilizadores tentem obter melhor Qualidade de Serviço (QoS) para os seus fluxos sem contudo assumirem os custos associados, levando ao roubo de recursos que, em situações extremas, poderá ter como consequência a negação da qualidade de serviço – Denial of QoS (DQoS) – contratada pelos utilizadores para os seus fluxos de informação. No modelo DiffServ a autenticação de fluxos é realizada, pacote a pacote, à entrada do domínio, com base na análise de um conjunto de campos do cabeçalho dos pacotes IP. Esta abordagem apresenta algumas limitações de segurança. Ora, sendo os routers de ingresso nos domínios (ER) os responsáveis pela admissão e marcação/remarcação dos pacotes relativamente à sua classe de serviço, são também os mais vulneráveis a ataques, podendo uma brecha de segurança neste ponto das redes repercutir-se por todo o domínio. De forma a minorar estas limitações, inerentes ao modelo DiffServ são, neste capítulo, avaliadas três arquitecturas para negociação e autenticação de QoS, destinado a autenticar clientes e a autorizar fluxos, de forma dinâmica, à entrada dos domínios DiffServ.

PALAVRAS-CHAVE

Negociação de QoS, Negação de QoS, Autenticação e Autorização de Fluxos DiffServ.

1. INTRODUÇÃO

Em sistemas de comunicação, a designação Qualidade de Serviço (QoS) é usada para caracterizar a capacidade de um sistema de comunicação suportar fluxos de dados com parâmetros de serviço (débito, atraso, *jitter*, perdas, etc.), garantidos de forma mais ou menos estrita. Os mecanismos de QoS impõem prioridades de acesso aos recursos disponíveis no sistema de comunicações. No caso particular do modelo DiffServ [1], esta prioritização de tráfego é suportada na identificação das Classes de Tráfego (grupos de múltiplos fluxos), efectuada com base no cabeçalho dos pacotes IP [2]. Esta abordagem apresenta algumas limitações de segurança conforme é discutido em [3, 4].

O grupo de trabalho DiffServ do IETF propôs alguns métodos destinados a minorar as limitações de segurança inerentes ao modelo DiffServ [4], tais como auditoria e IPSec [5,6], mas vulnerabilidades a ataques tais como *man-in-the-middle* e *Denial of QoS (*DQoS) permanecem por resolver [7].

Na secção 2 serão apresentados alguns trabalhos de investigação, relacionados com a melhoria da segurança e da gestão das redes com QoS. De forma a minorar as vulnerabilidades de segurança do modelo DiffServ, no que diz respeito a ataques de DQoS e de roubo de recursos, serão propostos na Secção 3, duas arquitecturas para autenticação, autorização, controlo de admissão e contabilização de recursos, destinado a autenticar clientes e a autorizar fluxos, de forma dinâmica, à entrada dos domínios DiffServ. Iremos focar-nos fundamentalmente em questões de negociação segura de QoS, em ambiente intra-domínio, mas concretamente nas questões associadas aos nós de admissão em domínios *DiffServ* e nos processos de autenticação dos clientes e de autorização de reserva de recursos. Os aspectos de segurança considerados restringem-se à autenticação dos clientes e à autorização de fluxos, para acesso aos recursos de comunicação. As questões relacionadas com a confidencialidade e integridade da informação são relegadas para outros módulos do sistema de comunicações. A secção 4 será destinada à avaliação das arquitecturas propostas. Finalmente, a Secção 5 será dedicada à apresentação de conclusões e indicações para trabalho futuro.

2. TRABALHOS RELACIONADAS

As infra-estruturas de comunicação de dados são vulgarmente alvo de um conjunto de ataques à confidencialidade, integridade e disponibilidade da informação em trânsito, e à autenticidade da origem e do destino dessa informação. Na infra-estruturas de comunicação baseados no modelo DiffServ [1] esta situação agrave-se pois, estas disponibilizam diferentes níveis de serviço a diferentes fluxos de informação, sobre uma infra-estrutura de comunicações TCP/IP, contribuindo para aumentar o potencial de ocorrência de alguns desses ataques.

No modelo DiffServ a autenticação e autorização de fluxos é realizada, pacote a pacote, à entrada do domínio, com base na análise de um conjunto de campos do cabeçalho do pacote IP [2]. Esta abordagem apresenta algumas limitações [3, 4], tais como a fragilidade da autenticidade de origem e destino da informação, que poderão ser exploradas por utilizadores menos escrupulosos, que tentem obter melhor qualidade de serviço para os seus fluxos sem contudo assumirem os custos associados, levando ao roubo de recursos que, em situações extremas, poderá ter como consequência a negação da qualidade de serviço (DQoS) nos fluxos activos. O grupo de trabalho *DiffServ* do IETF propôs alguns métodos destinados a minorar as limitações de segurança inerentes ao modelo DiffServ, tais como auditoria e IPSec [5, 6], mas vulnerabilidades a ataques tais como *man-in-the-middle* e *Denial of QoS* (DQoS) permanecem por resolver [7].

O projecto ARQoS [8] é uma das iniciativas no sentido de melhorar a segurança em redes com QoS, examinando as vulnerabilidades e soluções, para ataques de DQoS, ao nível da detecção e prevenção de ataques aos sistemas de gestão e aos pacotes em trânsito. O trabalho "Preventing Denial of Service Attacks on Quality of Service" [9], propõe a aplicação do paradigma do preço no processo de atribuição de recursos, isto é, os preços dos recursos aumentam com o aumento da ocupação dos recursos e vice-versa. A atribuição de recursos de rede a qualquer utilizador é sempre precedida de um processo de autenticação e autorização. Para tal, recorrem ao protocolo RSVP [10] e a extensão proposta na RFC2750 [11], que permite a utilização de PBNs (Policy Based Networks) [12] com RSVP. Sugerem também a utilização de um servidor de autorização, baseado no SIP (Session Initiator Protocol) [13], para emissão de objectos de políticas, assinados, que serão posteriormente apresentados ao router de entrada no domínio através do protocolo RSVP.

Uma abordagem semelhante é proposta pelo 3GPP (3rd Generation Partnership Project), na arquitectura de QoS *end-to-end* do UMTS [14], para interoperar com redes externas *IntServ*/RSVP. Quando a rede externa utiliza RSVP, as mensagens de sinalização devem conter um *authentication token*, quando disponível, e o identificador de fluxo, emitidos pelo protocolo SIP, num objecto *POLICY_DATA*.

O controlo de admissão do RSVP é frequentemente baseado na identidade do cliente ou aplicação [15]. A RFC3520 [16] especifica um novo objecto capaz de adicionar um novo mecanismo de admissão ao RSVP, baseado na sessão. Este novo objecto, denominado "*Session Authorization Policy Element*", contem a autorização para utilização de um conjunto de recursos, para uma sessão específica. Este objecto poderá conter informação referente aos recursos autorizados (ex. Parâmetros de QoS), à identificação dos fluxos e sessão a que pertencem, à duração das sessões e à identificação da entidade de autorização. Apesar da sua maturidade e versatilidade, introduzidas por diversas extensões ao protocolo inicial, o RSVP é um protocolo de estabelecimento de reservas, adequado para a sinalização de QoS fim-a-fim, originalmente concebido para suportar estabelecimento de reservas unicamente a partir do transmissor e para a sinalização de aplicações *multicasting*, que obriga a um elevado processamento de mensagens entre nós. Para além destes inconvenientes, existem um conjunto de outras aplicações que necessitam de serviços de sinalização distintos dos disponibilizados pelo RSVP.

O grupo de trabalho NSIS [17], do IETF, está a considerar uma solução baseada num modelo de sinalização em duas camadas, onde um protocolo de sinalização, genérico, ao nível da camada de transporte [18], NTLP - *NSIS Transport Layer Protocol*, servirá uma família de protocolos de camada superior, específicos para a sinalização de diversas aplicações, NSLP – *NSIS Signaling Layer Protocol* [19]. Este protocolo é semelhante ao RSVP, utilizando as mensagens de refrescamento como principal mecanismo de gestão de estados das reservas (*soft-state*). Contudo, permite que as reservas sejam iniciadas tanto pelo emissor como pelo receptor, entre nós arbitrários e não suporta multicasting IP, tornando-o num protocolo mais flexível e leve do que o RSVP.

Um conjunto de outros trabalhos [20, 21, 22, 23] abordam a problemática da segurança em infraestruturas com qualidade serviço, incidindo principalmente nas questões de controlo de admissão, propondo para tal a adopção de arquitectura PBN, e a securização da sinalização inter-domínio, entre BBs. Contudo, as questões relacionadas com a segurança na periferia das redes, tais como autenticação dos clientes e a autorização dinâmica de recursos, não são abordadas.

3. ARQUITECTURAS AAAA PARA QOS

3.1 Arquitectura com clientes activos – *Agent Sequence*

A arquitectura proposta nesta secção pretende colmatar as limitações da arquitectura apresentada anteriormente, relativamente às limitações na detecção de início e fim de fluxos UDP e à necessidade de utilização de IPSec. Para o efeito, será proposta a instalação de uma entidade em cada cliente, semelhante à instalada no router da arquitectura anterior, mas com funcionalidades estendidas, capaz de identificar todos os fluxos, TCP e UDP, e de comunicar com o Servidor de QoS para lhe solicitar a reserva dos recursos necessários. Contrariamente à arquitectura proposta na secção anterior, a arquitectura com clientes activos – *Agent Sequence* [24], assenta no pressuposto de serão realizadas alterações em todos os clientes para que estes possam interagir com o Servidor de QoS.

3.1.1 Descrição da arquitectura

Nesta arquitectura, sempre que uma aplicação origine um fluxo, este será interceptado por um *daemon* instalado no computador do cliente. Posteriormente, o módulo de autenticação deste *daemon* terá de se autenticar no Servidor de Autenticação e obter credenciais que lhe permitam contactar o Servidor de QoS.

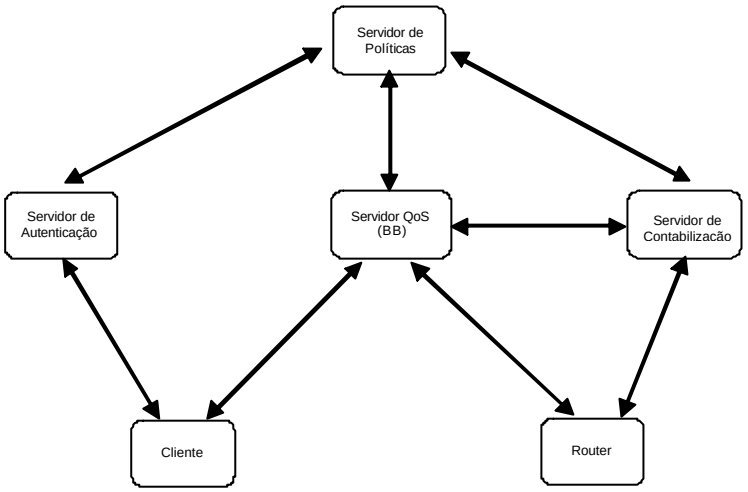

Figura 3. Arquitectura com clientes activos – Agent Sequence

Após a recepção das credenciais, o cliente solicitará ao BB a alocação de recursos de rede para o fluxo interceptado. A partir daqui, e com base nas políticas de utilização de recursos, armazenadas no Servidor de Políticas, e na disponibilidade de recursos na ligação ao ISP, o BB poderá autorizar ou rejeitar o novo fluxo, facto que se irá reflectir na configuração do *router* de entrada no domínio DiffServ (*Ingress Router*). Após expirar a validade da autorização, o *router* será reconfigurado e, desta forma, será barrado ao fluxo o acesso a recursos com QoS. A Figura 3 apresenta o cenário descrito.

3.1.2 Exemplo de funcionamento da arquitectura

Inicialmente, na sequência da detecção de um novo fluxo o cliente solicitará credenciais, junto do Servidor de Autenticação, que lhe permitirão comunicar com o Servidor de QoS. Após a recepção destas credenciais, o Cliente envia um pedido de reserva de recursos ao Servidor de QoS, contendo informações extraídas do cabeçalho do pacote IP, tais como endereço origem e destino, portos TCP/UDP origem e destino, protocolo da camada superior e requisitos de QoS pretendidos, sempre que a aplicação os especifique. Na resposta, o Servidor de QoS informará o cliente da aceitação ou não da reserva e, caso a resposta seja afirmativa, disponibilizará o valor do DSCP a utilizar na marcação dos pacotes do fluxo em causa. Após a recepção da autorização, o Cliente marcará todos os pacotes do fluxo autorizado, de acordo com o valor do DSCP fornecido.

A figura 4 apresenta o diagrama de fluxos simplificado do Servidor de QoS, para os processos de estabelecimento e finalização de reserva de recursos de um fluxo de dados. Na circunstância do estabelecimento de uma nova reserva, o Servidor de QoS recebe um pedido de reserva de recursos do Cliente de QoS (`reserveRequest`), contendo as informações que identificam o novo fluxo, tais como

IP origem e destino, portos TCP/UDP origem e destino, protocolo da camada superior e requisitos de QoS pretendidos, sempre que o cliente os especifique.

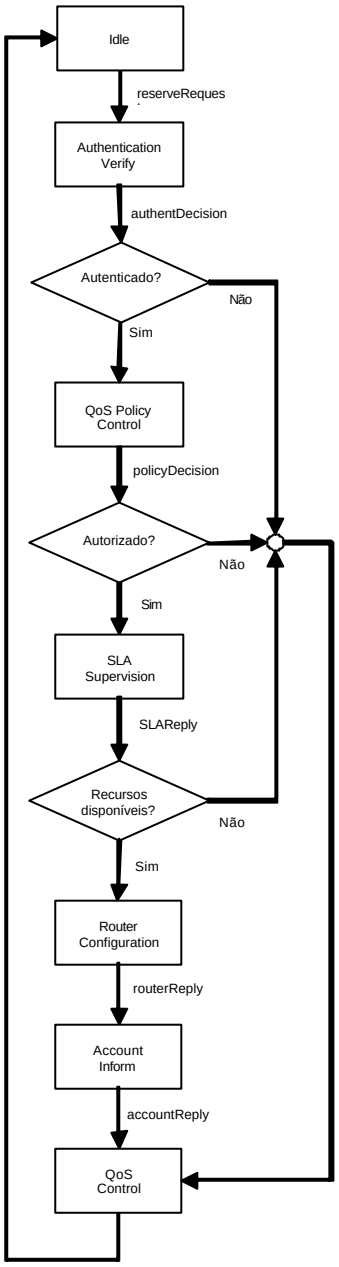

Figura 4 Diagrama de fluxos do Servidor de QoS – *Agent Sequence*

Se o cliente estiver devidamente autenticado (`authentDecision`), situação verificada pela entidade *Authentication Verify*, o Servidor de QoS aceitará o seu pedido e, através da entidade *QoS Policy Control*, consultará o repositório de políticas do domínio, para recolher informação sobre os critério de QoS a aplicar ao novo fluxo. Baseado nas políticas de QoS definidas para o utilizador/aplicação, (`policyDecision`) e na disponibilidade de recursos na ligação ao domínio Diffserv do ISP, será tomada uma decisão relativa ao pedido de reserva de recursos. Caso o pedido seja aceite, o Servidor de QoS dará instruções ao Router, através da entidade *Router Configuration*, para que este proceda à reconfiguração dos interfaces do router, de forma a que o novo fluxo receba o tratamento de QoS adequado. Após a recepção da resposta do router (`routerReply`), o Servidor de Contabilização de Recursos será informado sobre o estabelecimento de um novo fluxo, quais os parâmetros de tráfego associados e qual o seu dono, para que possa proceder à contabilização dos recursos utilizados. Finalmente, logo após a recepção da mensagem `accountReply`, proveniente dos Servidor de Contabilização de Recursos, o Servidor de QoS responderá ao Cliente, através da entidade *QoS Control*, comunicando-lhe a aceitação do pedido de reserva de recursos para o novo fluxo e o valor do campo

DSCP que deverá utilizar na marcação dos pacotes do fluxo. Na situação de rejeição do pedido, que pode ocorrer nas fases de autenticação ou autorização, o cliente será informado de que o seu pedido foi rejeitado, sendo identificado o motivo para tal rejeição.

3.2 Arquitectura com clientes activos – *Push Sequence*

Nesta arquitectura com clientes activos – *Push Sequence* [24], pretende-se propor uma solução algo diferente da arquitectura anterior, assente em dois sistemas: um sistema de autorização, que baseia as suas decisões nas políticas de QoS do domínio, e outro sistema de controlo de admissão, baseado na autorização do sistema anterior e na disponibilidade de recursos para ligação à rede do ISP. A autorização será feita na base da sessão ou do fluxo associado a uma sessão autorizada, contrariamente à arquitectura anterior, onde a autorização era realizada fluxo a fluxo, de forma independente.

3.2.1 Descrição da Arquitectura

Esta nova proposta baseia-se num *ticket*, contendo os recursos previamente autorizados por um sistema de autorização, que será utilizado pelo sistema de controlo de admissão, para proceder à reserva efectiva dos recursos para a sessão identificada no mesmo *ticket*. A figura 5 apresenta este cenário de forma geral.

Tal como na arquitectura anterior, o Cliente de QoS começará por ser autenticado pelo Servidor de Autenticação. Este servidor emitirá credenciais que possibilitarão ao cliente o contacto com o Servidor de Autorização. Posteriormente o cliente solicitará ao Servidor de Autenticação a atribuição de recursos de rede com as características necessárias para o estabelecimento da nova sessão ou fluxo. Na sequência deste pedido e de acordo com as políticas de QoS já definidas pelo administrador da rede, a entidade de Autenticação responderá a este pedido, através da emissão de um *ticket*. Este *ticket* conterá, entre outros parâmetros, os recursos autorizados e a identificação dos fluxos pertencentes à sessão.

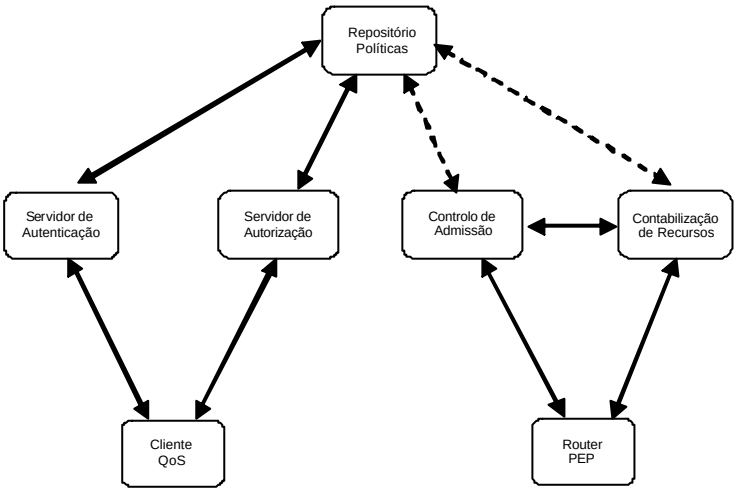

Figura 5. Arquitectura com clientes activos – Push Sequence

Neste ponto do processo, o cliente possuirá autorização para a utilização de determinados recursos, emitida pelo Servidor de Autorização. Contudo, os recursos não estarão ainda disponíveis. Para proceder à reserva efectiva dos recursos, o cliente necessitará de solicitar ao sistema de Controlo de Admissão, a entidade que controla os recursos de rede do domínio, a reserva dos recursos já autorizados por outra entidade, o Servidor de Autorização. Para tal, deverá enviar o *ticket*, contendo os recursos autorizados, para o sistema de Controlo de Admissão. Esta entidade, baseada na disponibilidade de recursos disponíveis no domínio e na informação contida no *ticket*, procederá à reserva dos recursos através da configuração do *router* de fronteira do domínio Diffserv e enviará ao cliente a sua decisão juntamente com os valores de DSCP que este deverá utilizar na marcação dos pacotes pertencentes aos diversos fluxos da sessão. Após a recepção desta informação, o cliente procederá à marcação dos pacotes e ao envio dos mesmos para o meio de comunicação. A autorização (*ticket*) é limitada no tempo, impondo-se a sua revalidação antes que expire, caso contrário serão interrompidos todos os fluxos da sessão.

3.2.2 Exemplo de funcionamento da arquitectura

Numa primeira fase o Cliente de QoS, deverá autenticar-se no Servidor de Autenticação e desta forma obter credenciais que lhe permitirão contactar o Servidor de Autorização. Posteriormente o cliente solicitará ao Servidor de Autenticação, a atribuição de recursos de rede com as características necessárias

para o estabelecimento da nova sessão ou fluxo. Na sequência deste pedido, o Cliente de QoS ficará a aguardar uma resposta. Na resposta estará contido um *ticket* que integrará, entre outros parâmetros, os recursos autorizados e a identificação dos fluxos pertencentes à sessão.

Neste ponto do processo, o cliente possuirá autorização para a utilização de determinados recursos, emitida pelo Servidor de Autorização, mas os recursos não estarão ainda disponíveis. Para proceder à reserva efectiva dos recursos, o cliente, solicitará ao sistema de Controlo de Admissão, a reserva dos recursos já autorizados pelo Servidor de Autorização, enviando para o efeito o *ticket* que contém os recursos autorizados.

A figura 6 apresenta o diagrama de fluxos simplificado do Servidor de QoS, para os processos de estabelecimento e finalização de reserva de recursos de um fluxo de dados. Em ambas as situações, estabelecimento e finalização, o sistema de Controlo de Admissão receberá do Cliente de QoS um pedido de reserva de recursos (`provisionRequest`).

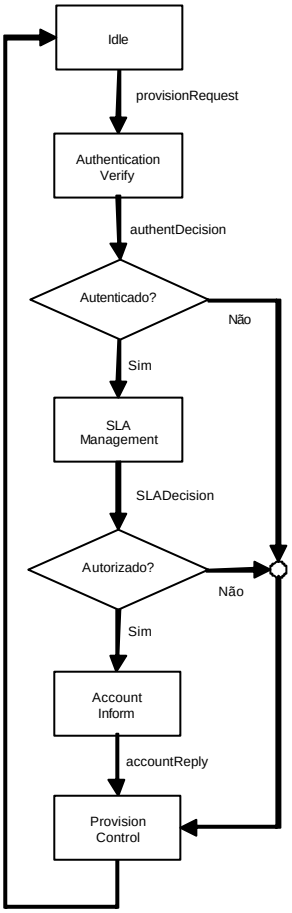

Figura 6. Diagrama de fluxos do Controlo de Admissão

Na circunstância do estabelecimento de uma nova reserva, o sistema de Controlo de Admissão receberá um pedido de reserva de recursos do Cliente de QoS, contendo as informações que identificam o novo fluxo, tais como IP origem e destino, portos TCP/UDP origem e destino, protocolo da camada superior e requisitos de QoS pretendidos, sempre que especificados pelo cliente. Após a validação da autenticidade do ticket (`authentDecision`), realizada pela entidade *Authentication Verify*, o Servidor de QoS verificará a disponibilidade de recursos na ligação ao domínio Diffserv do ISP, recorrendo para o efeito à entidade *SLA Management*. Após a recepção da mensagem `SLADecision` e no caso do pedido ter sido aceite, o sistema de Contabilização de Recursos será informado, pela entidade *Account Inform*, sobre o estabelecimento de um novo fluxo, quais os parâmetros de tráfego associados e qual o seu dono, para que possa proceder à contabilização dos recursos utilizados. Finalmente, logo após a recepção da mensagem `accountReply`, proveniente dos sistema de Contabilização de Recursos, a entidade *Provision Control* dará instruções ao Router PEP para que este proceda à configuração dos interfaces do router, de forma a que o novo fluxo receba o tratamento de QoS adequado, ficando a aguardar uma

resposta do router (`routerReply`). Na situação de rejeição do pedido, que pode ocorrer nas fases de autenticação ou autorização, o cliente será informado do motivo para tal rejeição.

Após a recepção da resposta ao seu pedido (`reserveDecision`), o cliente poderá tomar duas decisões distintas, condicionadas pelo tipo de resposta recebida. Em caso de resposta favorável ao pedido, o Cliente de QoS, utilizará os valores de DSCP fornecidos, para a marcação de todos os pacotes dos fluxos pertencentes à sessão autorizada. Em caso de resposta negativa, informará o Servidor de Autorização de tal decisão. Esta informação poderá servir para actualizar o estado de utilização dos recursos de rede por parte deste cliente ou para posterior análise, com a finalidade de optimizar as SLAs firmadas com os ISPs.

4. AVALIAÇÃO DOS CENÁRIOS PROPOSTOS

4.1 Avaliação Funcional

A arquitectura *Pull Sequence* apresenta uma solução para a autorização e disponibilização de recursos com qualidade de serviço, dinâmica, assente no pressuposto de que será instalada uma entidade em cada cliente, com responsabilidades de identificação de inicio e fim de fluxos, de autenticação do cliente junto do Servidor de Autenticação e de reserva de recursos junto do Servidor de QoS. Desta forma, não será necessária qualquer alteração nas aplicações instaladas nos clientes, permitindo-se a utilização de aplicações existentes, desenvolvidas sem suporte de QoS. Contudo, sendo uma solução orientada para a autorização fluxo a fluxo, realizada através da classificação de pacotes, também designada por classificação *stateless*, apresenta limitações no relacionamento entre os diversos fluxos duma mesma sessão, sempre que esta tenha necessidade de estabelecer diversos fluxos, utilizando diferentes portos TCP/UDP. Será pois desejável realizar a autorização e reserva de recursos na base da sessão ao invés do fluxo..

A arquitectura *Push Sequence* apresenta um sistema para a negociação de QoS, autenticação e controle da admissão de fluxos e contabilização de recursos, capaz de realizar a autorização e reserva de recursos na base da sessão ao invés do fluxo, através da autenticação de clientes e da autorização dinâmica de sessões/fluxos, à entrada do domínio DiffServ. Neste sistema, existirá uma entidade instalada em cada cliente, com as funcionalidades de identificação do fluxo e respectiva sessão associada, autenticação do cliente e pedido de autorização e de reserva de recursos com QoS. Os pedidos são autorizados por uma entidade de autorização, que emite um *ticket* de acordo com as políticas de QoS definidas para o cliente e/ou aplicação e, posteriormente, envia esse *ticket* à entidade de controlo da admissão. Desta forma, sempre que for solicitado o estabelecimento de um novo fluxo num porto habitualmente não autorizado a utilizar recursos de rede com QoS, este poderá ser autorizado se for parte integrante da sessão já autorizada

4.2 Avaliação de Segurança

Nas arquitecturas propostas existe uma interacção *peer-to-peer* entre o nó que origina a mensagem e o nó mais próximo, no caminho para o destino da mensagem. As ameaças à segurança, mais relevantes neste tipo de comunicação, são as relacionadas com ataques de MITM, perda de confidencialidade, DoS, violação de integridade e roubo de identidade, que poderão levar à fraude e ao roubo de recursos.

As questões de segurança focadas nestas arquitecturas restringem-se à negociação segura de QoS, em ambiente intra-domínio, mas concretamente às questões associadas aos nós de admissão em domínios DiffServ e aos processos de autenticação dos clientes e de autorização de reserva de recursos, por forma a minimizar as vulnerabilidades de roubo de identidade e consequente roubo de recursos e negação de QoS. As questões relacionadas com a confidencialidade e integridade da informação são comuns à maioria dos sistemas de comunicação, não tendo pois sido alvo de análise no nosso trabalho.

A arquitectura *Pull Sequence* propõe a identificação do cliente de origem do fluxo baseada em credenciais disponibilizadas ao cliente por um Servidor de Autenticação. Estas credenciais são posteriormente apresentadas ao Servidor de QoS, que procederá à autenticação do cliente e que, de acordo com as políticas de QoS definidas, procederá à disponibilização dos recursos adequados. Assim, os ataques de IP *spoofing*, e consequente roubo de identidade, ficarão bastante limitados sem que haja a necessidade de recorrer a qualquer técnica de encriptação, pois o estabelecimento de um novo fluxo só é autorizado a clientes cuja identidade tenha sido comprovada através de credenciais e não através do endereço IP origem das mensagens. De realçar também que a autorização para utilização de recursos de rede é dinâmica e explícita, realizada fluxo a fluxo, pois, sempre que o cliente pretenda estabelecer ou

finalizar um novo fluxo com garantias de QoS, este terá de o solicitar ao Servidor de QoS. Assim, caso seja proferido, com êxito, um ataque de IP *spoofing*, este será limitado aos fluxos autorizados, que têm destinos e aplicações bem definidas, e terá uma duração temporal bastante pequena. Isto porque, logo após a ocorrência de um ataque de IP *spoofing*, o *daemon* instalado no cliente aperceber-se-á do fim dos fluxos originados pelas aplicações locais e solicitará o fim da reserva junto do Servidor de QoS.

Na arquitectura *Push Sequence*, tal como na arquitectura *Pull Sequence*, a autorização para utilização de recursos de rede com QoS é dinâmica e explícita, realizada fluxo a fluxo. Contudo, a admissão de novos fluxos é realizada tendo em consideração o relacionamento entre os diversos fluxos duma mesma sessão, sempre que esta tenha necessidade de estabelecer diversos fluxos, utilizando diferentes portos TCP/UDP. Assim, sempre que o cliente pretenda estabelecer ou finalizar um novo fluxo com garantias de QoS, este terá de solicitar autorização ao servidor de autorização. O resultado deste pedido, será expresso por intermédio de um *ticket*, posteriormente enviado ao sistema de controlo de admissão, para solicitar a reserva de recursos pretendidos. A utilização de *tickets* permite ao sistema adicionar e remover novos fluxos de forma expedita, por sessão, e reduzir as vulnerabilidades aos ataques de roubo dos recursos e de DQoS, pois somente os clientes que adquiram um *ticket* poderão solicitar a reserva de recursos e somente clientes autenticados e com permissão, expressa pelas políticas de segurança, os poderão adquirir. Os ataques de IP *spoofing* serão pois limitados aos fluxos autorizados, que têm destinos e aplicações bem definidas, e têm uma duração temporal bastante limitada. Isto porque, logo após a ocorrência de um ataque de IP *spoofing*, o cliente de QoS aperceber-se-á do fim dos fluxos originados pelas aplicações locais e solicitará o fim das reservas, através da aquisição de um novo *ticket* e dos seu posterior envio para o sistema de controlo de admissão.

Como a segurança desta arquitectura se baseia fundamentalmente nos tickets, deverá ser dada especial atenção às características destes, de forma a reduzir as vulnerabilidades ao roubo ou à corrupção dos tickets. Assim, todos os tickets emitidos deverão possuir uma duração temporal limitada e informação de autenticação adicionada pela entidade emissora. Estes mecanismos permitiram reduzir as vulnerabilidades aos ataques de man-in-the-middle, lançados com o objectivo de adulterar o ticket e, consequentemente, negar a QoS aos fluxos.

5. CONCLUSÕES E TRABALHO FUTURO

Neste artigo, foram propostas duas arquitecturas para negociação, autenticação, controlo de admissão e contabilização de recursos com QoS, destinadas a autenticar clientes e a autorizar fluxos, de forma dinâmica, à entrada dos domínios DiffServ.

Estas propostas pretendem contribuir para minorar as limitações de segurança inerentes ao modelo DiffServ, e para permitir a admissão de fluxos, dinamicamente, de acordo com os perfis dos clientes e com a disponibilidade de recursos.

As propostas abordaram fundamentalmente nas questões de negociação segura de QoS, em ambiente intra-domínio, mas concretamente as questões associadas aos nós de admissão em domínios *DiffServ* e os processos de autenticação dos clientes e de autorização de reserva de recursos. Os aspectos de segurança considerados restringiram-se à autenticação dos clientes e à autorização de fluxos, para acesso aos recursos de comunicação.

Os trabalhos futuros focar-se-ão na experimentação e avaliação da escalabilidade e desempenho das arquitecturas propostas.

AGRADECIMENTO

Este trabalho foi parcialmente financiado pelo programa de PRODEP suportado pelo Estado Português e pela União Europeia no âmbito do Fundo Social Europeu.

REFERÊNCIAS

[1] Blake, S. et al, 1998, An Architecture for Differentiated Services, *RFC 2475*, IETF.

[2] Nichols, K. et al, 1998, Definition of the Differentiated Services Fields (DS Fields) in the IPv4 and IPv6 Headers, *RFC 2474*, IETF.

[3] Rabadão, C., Monteiro, E., 2002, Segurança e QoS no Modelo DiffServ, *CRC2002 – 5ª Conferência sobre Redes de Computadores*, Faro, Portugal.

[4] Fu, Z. et al, 1999, Security Issues for Differentiated Service Framework, *Internet Draft (expired)*, IETF.

[5] Kent, S. e Atkinson, R., 1998, IP Encapsulating Security Payload (ESP), *RFC 2406*, IETF.

[6] Atkinson, R., 1995, IP Authentication Header, *RFC 1826*, IETF.

[7] Striegel, A., 2002, Security Issues in a Differentiated Services Internet, *Proceedings of Trusted Internet Workshop - HiPC*, Bangalore, India.

[8] Maughan, D. et al, The ARQoS Project: Protection of Network Quality of Service Against Denial of Service Attacks, http://arqos.csc.ncsu.edu/, State University of North Carolina, University of California and MCNC.

[9] Fulp, E. et al, 2001, Preventing Denial of Service Attacks on Quality of Service, *Proceedings of DARPA Information Survivability Conference and Exposition (DISCEXII'01)*, IEEE Computer Society.

[10] Braden, R. et al, 1997, Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification, *RFC2205*, IETF, Sep.

[11] Herzog, S., 2000, RSVP extensions for policy control, *RFC2750*, IETF.

[12] Hahn, S. et al, Resource Allocation Protocol, IETF, http://www.ietf.org/html.charters/rap-charter.html.

[13] Rosenberg, J. et al, 2002, SIP: Session Initiation Protocol, *RFC 3261*, IETF.

[14] Access Security for IP-based Services, *Technical Specification 3GPP TS 33.203, Version 6.1.0*, 3rd Generation Partnership Project.

[15] Yadav, S. et al, 2001, Identity Representation for RSVP, *RFC 3182*, IETF.

[16] Hamer, L-N. et al, 2003, Session Authorization Policy Element, *RFC3520*, IETF.

[17] Loughney, J. et al, Next Steps in Signaling (NSIS), IETF, http://www.ietf.org/html.charters /nsis-charter.html.

[18] Hancock, R. et al, 2004, Next Steps in Signaling: Framework, *Internet Draft (work in progress)*, IETF.

[19] Van den Bosch, S., 2004, Karagiannis, G. and McDonald, A., NSLP for Quality-of-Service Signaling, *Internet Draft (work in progress)*, IETF.

[20] Pujolle, G. and Chaouchi, H., 2002, QoS, Security, and Mobility Management for Fixed and Wireless Networks under Policy-based Techniques, *IFIP World Computer Congress 2002*.

[21] Mykoniati, E. et al, 2003, Admission Control for Providing QoS in DiffServ IP Networks: The TEQUILA Approach, *IEEE Communications Magazine*, Jan. 2003, pp. 38-44.

[22] Ponnappan, A. et al, 2002, A Policy Based QoS Management System for the IntServ/DiffServ Based Internet , *Proceedings of 3rd International Workshop on Policies for Distributed Systems and Networks, POLICY'02*, Monterey, California.

[23] Sander, V. et al, 2001, End-to-End Provision of Policy Information for Networks QoS, *Proceedings of 10th IEEE International Symposium of High Performance Distributed Computing*, São Francisco, Califórnia.

[24] Vollbrecht, J. et al., 2000, AAA authorization Framework, RFC2904, IETF.