Segurança e QoS no Modelo DiffServ

Carlos Rabadão[1, 2], Edmundo Monteiro[2]

crab@estg.iplei.pt edmundo@dei.uc.pt

[1] **Escola Superior de Tecnologia e Gestão**
Instituto Politécnico de Leiria
Morro do Lena – Alto do Vieiro
2411-901 Leiria
http://www.estg.iplei.pt

[2] **Laboratório de Comunicações e Telemática**
CISUC / DEI
Universidade de Coimbra
Pólo II, Pinhal de Marrocos, 3030-290 Coimbra
http://lct.dei.uc.pt

Resumo

O principal objectivo do modelo 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 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 (Denial of QoS) – 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 do pacote IP. Esta abordagem apresenta algumas limitações discutidas mais adiante neste documento. De forma a minorar estas limitações de segurança, inerentes ao modelo DiffServ é, neste trabalho, proposto um sistema dinâmico de autenticação de clientes e autorização de fluxos, à entrada dos domínios DiffServ. A abordagem proposta recorre ao protocolo de autenticação Kerberos amplamente utilizado na autenticação de utilizadores em sistemas de comunicação.

Neste trabalho são abordados e discutidos os aspectos de segurança relativos ao modelo DiffServ. Os aspectos de segurança abordados restringem-se à autenticação dos clientes e a 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, concretamente, para os protocolos TLS e IPSec. Para resolver a questão da autenticação de fluxos é proposta e discutida neste trabalho uma abordagem que passa pela integração do protocolo Kerberos no modelo DiffServ num âmbito intra-domínio, pretendendo-se no futuro alargar a proposta a ambientes inter-domínio.

Palavras-chave

Qualidade de Serviço (QoS), Modelo DiffServ, Segurança, Roubo de QoS, Negação de QoS (DQoS), Kerberos

1. Introdução

Em sistemas de comunicação, a designação *"qualidade de serviço"* (QoS) é usada para caracterizar a capacidade de um sistema de comunicação em 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 no cabeçalho dos pacotes IP [2]. Na Secção 2 deste documento será realizada uma breve descrição do modelo DiffServ.

Nas infra-estruturas com suporte de QoS, o tratamento privilegiado dado a alguns fluxos de informação e o acesso privilegiado aos recursos de comunicação que este tratamento implica irá provocar irá originar uma apetência para a utilização não autorizada de recursos alheios fugindo os custos mais elevados que estão normalmente associados à utilização destes recursos. Para contrariar esta apetência é necessária a autenticação dos fluxos de informação. Actualmente a forma mais habitual de realizar esta autenticação é através da simples classificação, pacote a pacote, de um conjunto de campos do cabeçalho IP. Este método apresenta algumas vulnerabilidades discutidas na Secção 3.

O Kerberos [3] é um protocolo maduro, fiável, seguro e amplamente utilizado na autenticação em sistemas de comunicação de âmbito intra-domínio. Estão em curso alguns trabalhos, capazes de vir a tornar possível a utilização de infra-estruturas de chave pública (PKI) associadas ao protocolo Kerberos. Estas propostas poderão contribuir para a resolução das limitações da escalabilidade deste protocolo, viabilizando a sua utilização num âmbito inter-domínio. A Secção 4 fará uma descrição muito sucinta do funcionamento do Kerberos, incluindo as propostas em desenvolvimento com vista à extensão deste protocolo. As questões relacionadas com a confidencialidade e integridade da informação não tratadas, sendo relegadas para outros módulos do sistema de comunicações, concretamente, para o protocolo TLS [4] da camada de transporte ou o protocolo IPSec [5] na camada de rede.

Na Secção 5 será apresentada a proposta com vista à utilização do Kerberos na criação de um sistema de autenticação para o modelo DiffServ. A nossa proposta visa a criação de um sistema de autenticação e autorização mais eficiente e flexível comparativamente ao actualmente utilizado no modelo DiffServ. O sistema suporta a autenticação periódica dos clientes e permite uma fácil integração com mecanismos de contabilização e taxação de recursos.

Por fim, a Secção 6, será dedicada à avaliação do sistema proposto, sendo apresentadas algumas conclusões e indicações para trabalho futuro.

2. Modelo DiffServ

O modelo DiffServ tem por base um conjunto de mecanismos relativamente simples. À entrada de uma rede o tráfego é classificado, condicionado e integrado num de diferentes classes de tráfego [1], sendo cada classe caracterizada pelo respectivo *Differentiated Service Code Point* (DSCP) [2]. Nesta Secção será realizada uma breve abordagem ao modelo DiffServ, realçando os aspectos que se julgam mais necessários para a discussão da proposta. Para uma abordagem mais aprofundada deverão ser consultados os RFC 2474 [1] e RFC 2475 [2].

A Figura 1 representa uma infra-estrutura de comunicações DiffServ, com dois domínios diferentes (DS1 e DS2). Na figura são ilustrados os diversos elementos que compõem um domínio DiffServ, tais como: os *Edge Routers* (ER), os *Core Routers* (CR), os *Border Routers* (BR), os *End Devices* (ED) e os sistemas de gestão e de implementação de políticas (*Policy Server* – PS e *Policy Repository* – PR), os sistemas de controlo de admissão e gestão de recursos (*Bandwidth Broker* – BB) e os sistemas de autenticação, autorização e contabilização (*Authentication, Autorization and Accounting* – AAA).

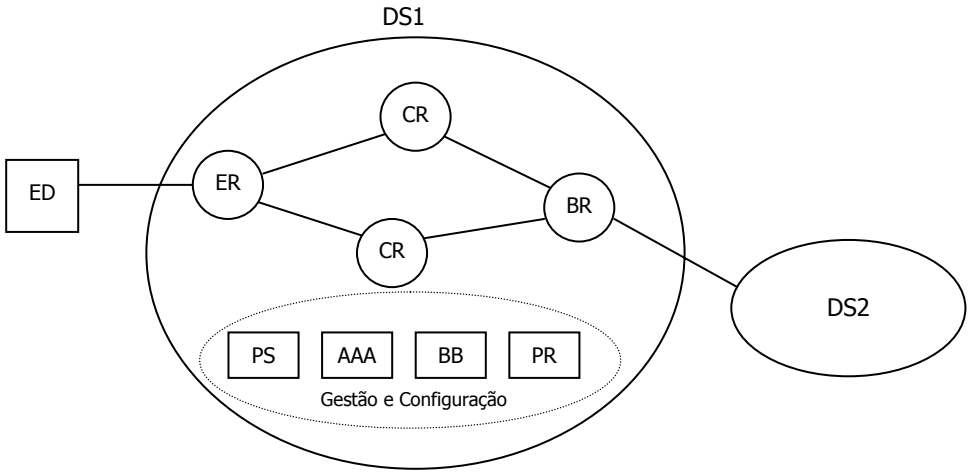

Figura 1. Elementos de uma infra-estrutura de comunicações DiffServ.

A Figura 2 esquematiza com maior detalhe o inter-funcionamento do sistema de gestão e configuração e da restante infra-estrutura do domínio DiffServ.

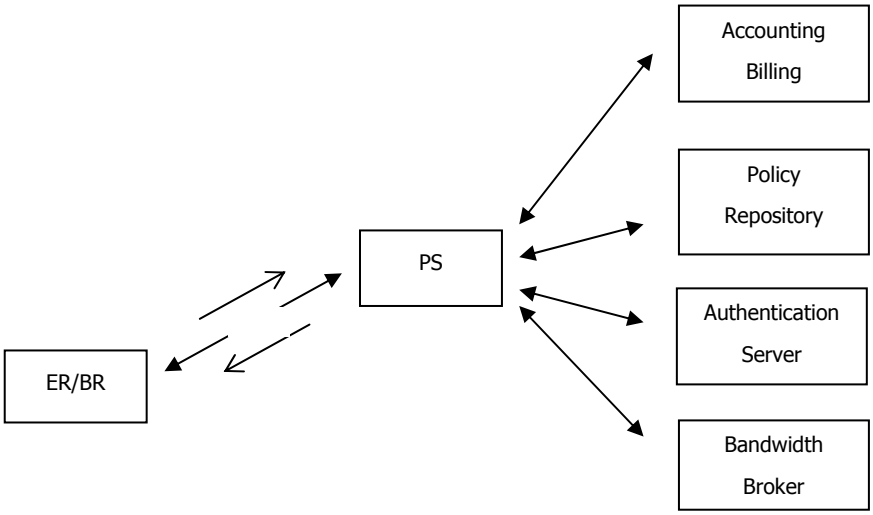

Figura 2. Elementos de um Sistema de Gestão e Configuração de um domínio DiffServ.

Os *routers* de fronteira do domínio DiffServ (ER e BR) são responsáveis por policiar todo o tráfego que entra no domínio e por fazer cumprir as políticas definidas. Para tal, analisam o campo DSCP ou diversos campos do cabeçalho do pacote IP (endereços IP origem e destino, portos TCP/UDP origem e destino e tipo de protocolo). Com base nesta informação é verificado se as características de QoS do fluxo em questão estão de acordo com o *Service Level Agreement*

(SLA) contratado pelo "dono" do pacote, através do recurso a informação, previamente disponibilizada pelo PR. Os ER e BR são também responsáveis por realizar medidas relativas à rede e ao tráfego de cada cliente e dá-las a conhecer aos sistemas de AAA [6].

O *Policy Server* (PS) é responsável pelas decisões baseadas nas políticas armazenadas no *Policy Repository* (PR) e na informação recebida dos ER/BR, relativa ao estado da rede, endereços IP origem e destino, portos TCP/UDP origem e destino e tipo de protocolo. Estas informações podem ser dadas em resposta a um pedido de um ER/BR, na sequência de actualizações das políticas ou em resposta a um pedido de uma entidade externa (ex. *Authentication Server* ou *Bandwidth Broker*). A troca de mensagens entre o PS e os ER/BR utiliza normalmente o protocolo COPS – *Common Police Open Service* [7].

As informações relativas a medidas de tráfego de cada cliente, recebidas dos ER/BR serão encaminhadas para os sistemas de contabilização e taxação (*Accounting and Billing)*. A autenticação de fluxos é tipicamente realizada através do recurso a informações contidas no cabeçalho dos pacotes IP, com algumas limitações de segurança à frente identificadas.

O *Bandwidth Broker* (BB) é responsável pela gestão de recursos e pela garantia de QoS extremo-a-extremo, através de um ou de múltiplos domínios DiffServ. No último caso, o BB contactará os BBs dos domínios adjacentes e negociará com eles os recursos necessários para garantir a QoS necessária ao suporte do fluxo de informação.

3. Segurança no modelo DiffServ.

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 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.

Nesta secção serão caracterizados, de forma genérica, os tipos de ataque a que as redes de comunicação de dados estão sujeitas. Esta análise será posteriormente particularizada para redes com diferenciação de serviços de acordo com o modelo DiffServ.

3.1 Ataques à segurança

Em termos gerais, os ataques a que os sistemas informáticos e os fluxos de informação estão sujeitos podem ser classificados em quatro categorias [8]:

- Interrupção – parte das infra-estruturas são inutilizadas ou bloqueadas. Exemplos desta situação são o corte do canal de comunicação, a inutilização de um servidor ou o bloqueio do sistema de gestão de ficheiros de um servidor. Nesta situação assiste-se a um ataque à disponibilidade da informação e dos recursos.

- Intercepção – "alguém" não autorizado ganha acesso a recursos da infra-estrutura, sem contudo poder alterar a informação. Este "alguém" pode ser uma pessoa, uma aplicação ou um computador. Exemplos desta categoria de ataques são a intercepção do canal de comunicação e posterior escuta dos dados que fluam na rede e a cópia ilícita de ficheiros e programas. Aqui assiste-se a um ataque à confidencialidade.

- Modificação – "alguém" não autorizado ganha acesso a recursos da infra-estrutura e altera a informação. Exemplos desta categoria de ataques são a alteração de um ficheiro de dados ou de uma aplicação, e a alteração do conteúdo das mensagens transmitidas na rede. Teremos neste caso um ataque à integridade da informação.

- Fabricação – "alguém" não autorizado tem acesso ao sistema usurpando a identidade de uma entidade autorizada ou quando no introduz "alguém" não autorizado introduz informação falsificada no sistema. Um exemplo desta categoria de ataque é a inserção de pacotes de informação na rede, contendo informação para configuração dos recursos da rede, usando uma identidade que tenha privilégios para tal e enganando desta forma o destinatário. Nesta situação teremos um ataque à autenticidade da informação ou das entidades intervenientes na comunicação.

Estas quatro categorias podem ser agrupadas em dois grupos de acordo com a metodologia utilizada no ataque: os ataques passivos e os ataques activos.

No primeiro grupo inserem-se unicamente a categoria de ataques por intercepção. Diz-se que são ataques passivos pelo facto de o atacante só aceder à informação sem contudo a alterar. Assim, o atacante poderá tomar conhecimento de informação confidencial. Recorrendo a técnicas de criptografia para codificação da informação, o atacante ficará impedido do acesso da informação, podendo contudo extrair os padrões de tráfego, a quantidade de informação transmitida e horas a que tais transmissões acontecem e à identidade e localização dos intervenientes na comunicação. Existem também algumas técnicas de segurança capazes de mascarar as características e proveniência do tráfego [8]. A solução genérica para evitar este tipo de ataques passa sobretudo pela prevenção pois eles não são facilmente detectáveis.

No segundo grupo, o grupo dos ataques activos, inserem-se as categorias de ataques por interrupção (ataque à disponibilidade), modificação (ataque à integridade) e fabricação (ataque à autenticidade). Neste grupo estão incluídos vários tipos de ataque concretos como o *masquerading*, o ataque por *replay* e a modificação de mensagens, de que poderão resultar o roubo de recursos, e a negação de serviço (DoS) [8].

3.2 Vulnerabilidades de segurança em DiffServ

As principais vulnerabilidades de segurança das infra-estruturas de comunicação DiffServ, são o roubo de recursos a negação da qualidade de serviço (*Denial of QoS* – DQoS) [1].

Os ataques referidos têm objectivos distintos. No caso do roubo de recursos, o atacante pretende unicamente usurpar recursos de comunicação para que os seus fluxos de informação sejam indevidamente tratados com QoS. Os recursos de comunicação podem ser usurpados a outros fluxos activos, a utilizadores inactivos ou ao sistema de comunicação em geral. No segundo caso (DQoS) as intenções do atacante são de provocar negação ou redução de QoS em fluxos de outros utilizadores sem ter como objectivo a usurpação de recursos de comunicação. Os objectivos do atacante poderão ser, por exemplo, visibilidade pelo ataque realizado, ou a perda de clientes por parte do fornecedor de serviço devido a descontentamento dos clientes, ou a perturbação de aplicações de utilizadores específicos.

Recuando à Figura 1 da Secção 2, podem ser identificados alguns pontos da infra-estrutura sobre os quais os ataques descritos podem ser lançados, tais como: os *routers* de fronteira de domínios (ER e BR), os *routers* de core (CR) e, os sistemas de gestão e de implementação de políticas (PS,

BB, AAA e PR). Podem ser consideradas duas abordagens distintas para lançar ataques sobre infra-estruturas DiffServ. São elas o ataque à informação de gestão e configuração e o ataque aos dados em trânsito.

Ataques aos sistemas de gestão

As vulnerabilidades dos sistemas de gestão de um domínio DiffServ dependem do método utilizado na sua configuração. Assim, se a configuração for manual, as únicas possibilidades de comprometer estas configurações são o acesso físico aos equipamentos e a "engenharia social". Se o processo de configuração for centralizado e automatizado, através do recurso a protocolos de sinalização (RSVP – *Resource Reservation Protocol*, de gestão (SNMP – *Simple Network Management Protocol*) ou de outros tipos (LDAP – *Lightweight Directory Access Protocol* ou COPS – *Common Open Policy Service*), o mais habitual em infra-estruturas de alguma dimensão, o leque de possibilidades para lançar ataques torna-se mais vasto.

Os resultados deste tipo de ataques aos pacotes de configuração de um sistema de comunicação DiffServ, qualquer que seja o método utilizado, são a configuração incorrecta dos diversos sistemas da infra-estrutura, podendo resultar em roubo de recursos e negação de QoS a clientes com recursos atribuídos.

Contudo, é possível minorar estes efeitos através da utilização de mecanismos de segurança que garantam a autenticidade, a integridade e privacidade das mensagens trocadas entre o sistema de gestão centralizado (ex. *Policy Server*) e os *routers* de fronteira. Desta forma os efeitos dos ataques por injecção, alteração e atraso de pacotes serão minimizados. Os ataques baseados no descarte de pacotes de forma selectiva serão também bastante dificultados através da utilização de técnicas de encriptação. A vulnerabilidade a ataques de descarte aleatório de pacotes continua a ser bastante elevada.

O protocolo COPS define um objecto denominado *Integrity Object* [7], que possibilita a utilização de técnicas que garantem a integridade e a autenticidade das mensagens trocadas. Para tal utiliza chaves secretas e negociação de números de sequência, e a subsequente geração de MD – *Messages Digest*. Assim, a utilização deste mecanismo na troca de mensagens COPS reduzirá substancialmente as vulnerabilidades a ataques aos sistemas de gestão.

Ataques aos dados em trânsito

Nas redes IP com DiffServ, a diferenciação da qualidade do serviço a prestar aos diversos clientes é baseada na codificação do DSCP [2] contida no campo TOS (*Type of Service*) do cabeçalho IP. Assim, um atacante que queira roubar ou negar QoS a fluxos de outros clientes, poderá gerar pacotes não autorizados com o campo ToS modificado, a partir de um equipamento terminal, ou alterar este campo nos pacotes que em trânsito no canal de comunicação.

O tipo de ataque vai depender de o atacante ter, ou não, acesso ao canal de comunicação. A situação mais vulgar é que os atacantes não tenham acesso ao canal de comunicação no *core* da rede, pois as tecnologias aí utilizados são bastante sofisticadas e os débitos de informação são tão elevados que os custos dos equipamentos necessários para interceptar e injectar pacotes poderão atingir valores demasiado elevados para os benefícios que se irão recolher. Contudo, o acesso ao meio não é impossível (sobretudo nas zonas de acesso ao *core* da rede) e poderá haver situações em que a relação custo/benefício seja vantajosa, podendo então ocorrer diversos tipos de ataque aos dados em trânsito, tais como injecção de pacotes com DSCP modificado ou inválido,

alteração não autorizada do cabeçalho dos pacotes, descarte selectivo de pacotes e atraso deliberado de pacotes [9].

A introdução do IPSec nos canais de comunicação poderá diminuir a vulnerabilidade destes sistemas, no que diz respeito ao descarte selectivo de pacotes, à custa da perda de algum desempenho originado pela utilização de operações de criptografia, sem contudo conseguir melhorar a segurança relativamente a descartes aleatórios. Contudo, a vulnerabilidade do DSCP mantém-se pois esta parte do cabeçalho não poderá ser encriptada nem autenticada, pois ele poderá ser alterado ao longo do caminho dos pacotes até este atinjam o seu destino. Provavelmente, a solução de segurança para a implementação de QoS em redes IP não passará unicamente pela introdução de técnicas de criptografia.

Os *routers* de *core* (CR) e routers de fronteira (BR) limitam-se a verificar agregados de fluxos e não fluxos individuais, caso contrário, a tecnologia DiffServ perderia a sua escalabilidade. Aliando a este facto a necessidade de soluções tecnológicas avançadas por parte do atacante, leva-nos a dar especial relevo aos *routers* de ingresso nos domínios (ER), pois estes são os responsáveis pela marcação dos pacotes relativamente à sua classe de serviço.

A proposta deste trabalho passa pela implementação de um método de autenticação obrigatório do cliente, baseado no Kerberos, sempre que este pretenda gerar um fluxo de tráfego com determinados parâmetros de QoS. O processo de autenticação irá originar a reconfiguração do *edge router*, que estabelece a fronteira entre o domínio DiffServ e a rede do cliente, para que os fluxos de informação estabelecidos possam usufruir das características de QoS solicitadas ou negociadas.

4. Kerberos

O protocolo Kerberos, descrito no RFC 1510 [3] e baseado nos trabalhos de Needham e Schroeder [10], fornece um mecanismo de autenticação para redes e serviços de comunicação. As propostas deste trabalho baseiam-se na versão 5 no Kerberos. A escolha recaiu sobre o Kerberos por este ser um protocolo versátil, maduro, fiável, seguro e amplamente utilizado na autenticação em redes e serviços de comunicação. Existem propostas em estudo para a ultrapassar as limitações de escalabilidade do Kerberos em ambientes alargados, multi-domínio administrativo. Estas propostas associam o Kerberos a infra-estruturas de chave pública (PKI) de certificados X.509 [13], permitindo a criação de soluções de autenticação leves e escaláveis, quando comparadas com soluções unicamente baseadas em infra-estruturas de chave pública e certificados X.509.

4.1 Funcionalidades básicas do Kerberos

Nesta secção será feita uma abordagem sucinta ao funcionamento do Kerberos para facilitar a apresentação da proposta objecto deste trabalho. Para um estudo mais aprofundado deste protocolo ficam as referências [11][12].

O funcionamento do Kerberos baseia-se no conceito de *realm.* Um *realm* é um domínio de autenticação que inclui um *Key Distribution Center* (KDC) primário, um ou mais KDCs redundantes, servidores de aplicações de comunicação e utilizadores. Um *realm* corresponde normalmente a uma infra-estrutura de comunicações com uma política de segurança única.

Um cliente que pretenda ganhar acesso a um servidor de aplicações deverá obter junto de um dos KDCs do *realm* um *Ticket-Granting Ticket* (TGT) que lhe dará acesso a um serviço centralizado, denominado por *Ticket-Granting Service* (TGS). Na posse do TGT o cliente poderá obter do TGS um *ticket* destinado a aceder a um determinado serviço de comunicações. A apresentação do *ticket* permitirá a autenticação no servidor que passará a partilhar com o cliente um chave de sessão secreta, distribuída de forma segura pelo KDC.

Quando o servidor de comunicações pertence a um *realm* distinto do cliente, é necessário que exista uma relação de confiança entre os dois *realms* para que a autenticação possa ter lugar. Esta relação será implementada através da partilha de chaves secretas entre os KDCs dos dois *realms*. Existindo está relação de confiança, o cliente necessitará de obter um *ticket* para acesso ao KDC do *realm* remoto o que deverá ser feiro por intermédio do KDC do *realm* local. Com este *ticket* o cliente receberá do TGS remoto um *ticket* de serviço para acesso ao servidor remoto.

4.2 Extensões ao Kerberos

Para redes de comunicação de grande dimensão e com muitos *realms*, a solução da relação de confiança baseada na partilha prévia de uma chave secreta entre cada par de KDCs, tem pouca escalabilidade. Têm sido apresentadas, pela comunidade científica internacional, diversas propostas para que o Kerberos passe a ser integrado com infra-estruturas de chave pública, e desta forma, permita que sistemas de autenticação baseados no Kerberos sejam mais facilmente escaláveis.

Duas dessas propostas, ainda sob a forma de Internet Drafts, são a *Public Key Cryptography for Inicial Authentication in Kerberos* (PKINIT) e a *Public Key Cryptography for Cross-Realm Authentication in Kerberos* (PKCROSS). A primeira propõe um conjunto de extensões à especificação do Kerberos contida no RFC 1510, para que esta possa passar a suportar criptografia de chave pública na autenticação inicial no KDC. A segunda propõe um conjunto de extensões à especificação inicial para que se possam utilizar infra-estruturas de chave pública (PKI) [13] na autenticação cruzada entre *realms*.

Com a integração do Kerberos e PKI consegue-se criar uma solução bastante escalável, pois a interacção entre os clientes de um *realm* e o AS poderá ser realizada com criptografia de chave pública, sendo a gestão local das chaves da responsabilidade do KDC local e não de uma PKI global. Sempre que se queira realizar autenticação cruzada entre *realms*, recorrendo-se nestas situações à PKI global, sendo o volume de chaves envolvidas na transacção muito menor.

4.3 Tickets renováveis

O Kerberos permite definir *tickets* renováveis, caracterizados por dois períodos de validade: o primeiro de duração mais curta que deverá ser renovado antes de caducar e, o segundo, de maior duração que quando expira já não pode ser renovado, tendo o cliente de solicitar novo *ticket* ao KDC. O cliente deverá periodicamente solicitar a renovação do *ticket* ao KDC e este por sua vez emitirá um novo *ticket* com uma nova chave de sessão e um novo período de duração. Quando o tempo máximo permitido para a duração do *ticket* for atingido, este caducará definitivamente.

O KDC poderá consultar uma lista de *tickets* caducados sempre que lhe seja solicitada uma renovação. Assim, se um *ticket* renovável for roubado tendo sido definido um tempo relativamente curto para a sua duração, o período de utilização de recursos de forma indevida por parte de clientes não autorizados será minimizado.

A informação relativa à quantidade de renovações e à duração de cada *ticket* renovável poderá ser utilizada para contabilizar a utilização de recursos da rede e consequentemente para a facturação de serviços ao cliente, por parte dos fornecedores de serviço.

5. Integração do Kerberos no modelo DiffServ

As vulnerabilidades com maior potência de ataque num sistema de comunicações, não serão as relacionadas com os *routers* e ligações do *core* da rede, mas sim as relativas à utilização indevida de endereços IP e aos campos de marcação de fluxos com QoS, conforme referido anteriormente. Assim, as questões de segurança abordadas nesta proposta são as relacionadas com a autenticação dos clientes e a autorização para utilização de recursos. Questões relacionadas com a confidencialidade e integridade da informação serão relegadas para outros módulos de segurança desenvolvidos para o efeito, nomeadamente os protocolos TLS [4] ou IPSec [5].

Assim, nesta proposta é definido que sempre que um utilizador pretenda usar recursos da rede com garantia de QoS, deva proceder à autenticação utilizando o protocolo de autenticação Kerberos. Se esta autenticação for realizada com sucesso, serão disponibilizadas credenciais para o cliente poder comunicar com o *Policy Server*. Este por sua vez irá disponibilizar ou não os recursos necessários a satisfação das necessidades do utilizador. Para evitar possíveis situações em que o endereço IP é "roubado" depois da autenticação e autorização, o utilizador dono do fluxo autorizado deverá periodicamente proceder à confirmação da sua autenticidade, junto do sistema.

No seguimento deste artigo irá ser descrito o funcionamento da proposta num âmbito intra-domínio e, posteriormente, será apresentada uma breve abordagem alargada a ambientes inter-domínio, que pretendemos desenvolver em trabalhos futuros.

5.1 Cenário intra-domínio

Na Figura 3 é apresentado de forma detalhada o cenário proposto. Este cenário é descrito em seguida passo-a-passo:

1 – Uma determinada aplicação cliente de um utilizador (utilizador A), necessita de estabelecer um fluxo de dados com uma aplicação de outro utilizador (utilizador B), pertencente a outro domínio DiffServ, com determinados parâmetros de QoS;

2 – Para que o fluxo possa ser correctamente classificado no *router* de fronteira e tratado com QoS no domínio DiffServ o utilizador A deverá começar por solicitar um *ticket* (TGT) junto do servidor de autenticação (KDC), para que se possa autenticar no TGS (*Ticket Grant Service*), utilizando para tal o *username* e *pwd*, ou criptografia de chave pública (PKINIT). Este pedido pode ser originado por dois tipos de clientes: pertencentes ao domínio de administrativo do fornecedor de serviço (ISP) ou pertencentes a um domínio administrativo próprio no caso de uma empresa, pró exemplo. No primeiro caso, o pedido é realizado ao KDC do ISP, enquanto no segundo caso este pedido será realizado ao KDC local, que por sua vez contactará o KDC do ISP. Este processo poderá ser desencadeado de forma automática com o início da aplicação que necessite de QoS;

3 – O KDC recebe o pedido, verifica a validade da conta e, caso esta seja válida e o utilizador disponha dos privilégios suficientes, ser-lhe-à atribuído então um TGT. Com o TGT o cliente irá solicitar ao TGS, credenciais para se poder autenticar no servidor de políticas do ISP;

4 – Com as credenciais obtidas, o cliente irá autenticar-se no servidor de políticas (PS), e posteriormente solicitar os parâmetros de QoS pretendidos;

5 – O PS deverá consultar o BB para se assegurar da disponibilidade de recursos capazes de garantir os parâmetros de QoS pretendidos para o fluxo em causa, fim-a-fim. Em caso afirmativo, o PS reconfigurará o *router* de entrada no domínio DiffServ, para que o fluxo em questão seja marcado com o DSCP de acordo com os parâmetros solicitados;

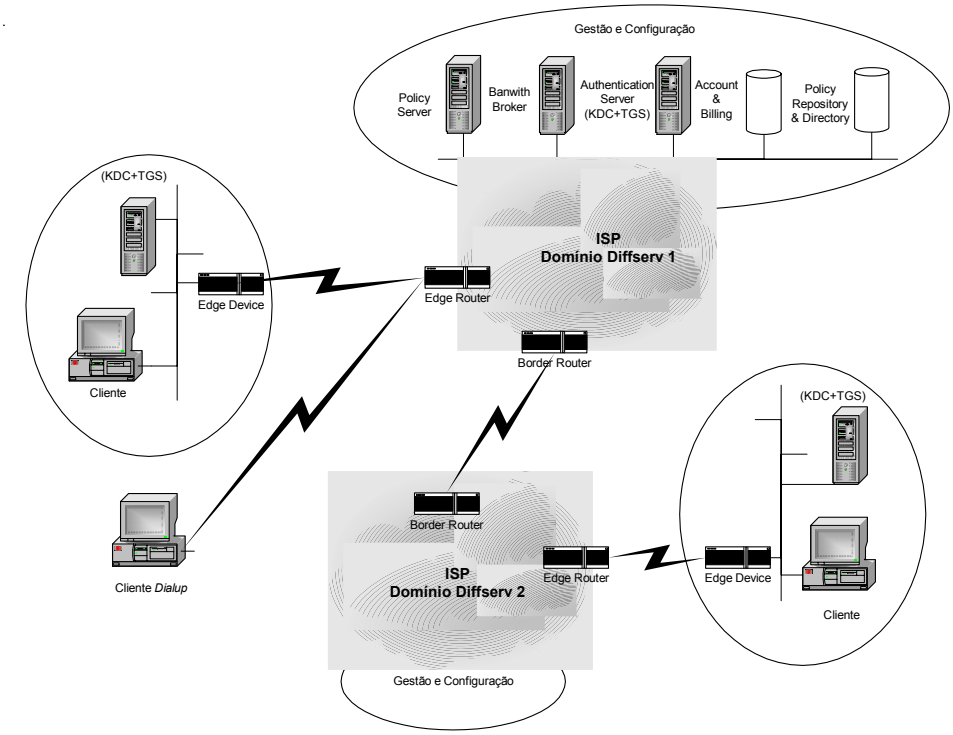

Figura 3. Cenário proposto

6 – Periodicamente, deve ser realizada uma reautenticação do fluxo em curso, junto do PS recorrendo ao Kerberos com *tickets* renováveis com dois períodos para expirar, um a longo prazo para definir a duração do *ticket*, e um outro a curto prazo destinado a renovar a autenticação do fluxo. Antes que o período mais curto expire, o cliente deverá revalidar o *ticket* por mais um determinado período, junto do servidor de autenticação (KDC). Expirado o período curto de validade do *ticket* sem que o utilizador o revalide, o *ticket* caducará e o utilizador deixará de se poder autenticar no PS. Na ausência de renovação da autenticação o PS reconfigurará o *router* do domínio para que passe a marcar o fluxo em questão como *best effort*.

O somatório da duração temporal de todos os *tickets* renováveis poderá ser disponibilizada ao sistema de *accounting* juntamente com as características de tráfego solicitadas para o fluxo em questão e posteriormente virem a ser utilizados para fins de taxação.

5.2 Cenário inter-domínio

Na figura 4 são identificadas as diferentes entidades envolvidas numa comunicação em ambiente inter-domínio.

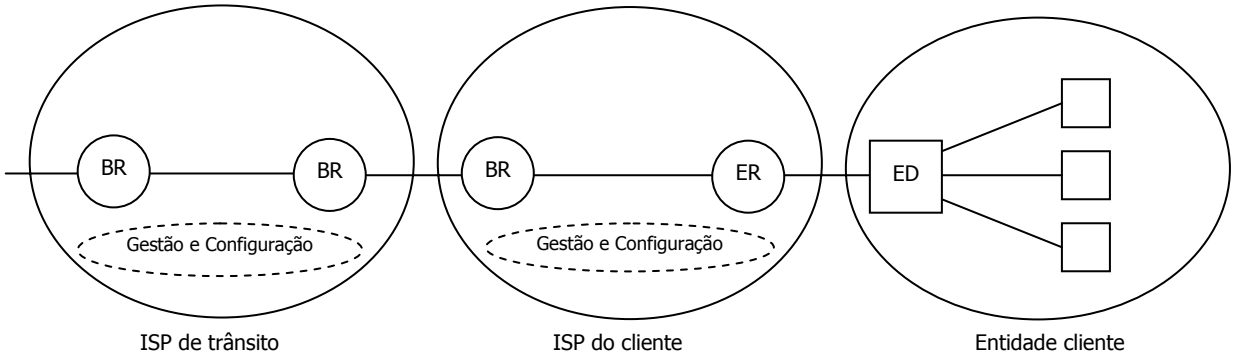

Figura 4. Entidades envolvidas numa comunicação inter-domínio com DiffServ

Passamos a apresentar uma breve abordagem à nossa proposta alargada a ambientes inter-domínio, que pretendemos vir a desenvolver em trabalhos futuros.

Inicialmente, quando a entidade cliente pretende iniciar uma comunicação com QoS com outra entidade, deverá autenticar-se junto do sistema de gestão e autenticação do seu domínio DiffServ. Este sistema, através do BB, deverá assegurar a disponibilidade de recursos fim-a-fim.

Caso a segunda entidade interveniente na comunicação pertença a um domínio DiffServ diferente, o BB do ISP original deverá solicitar recursos ao BB do domínio adjacente e este por sua vez deverá repetir o procedimento para o BB seguinte até que se atinja o BB do ISP do domínio a que pertence a entidade de destino. Haverá depois a necessidade de garantir QoS ao fluxo em sentido inverso, que deverá ser solicitado pela segunda entidade ao sistema de gestão e configuração do seu ISP.

6. Conclusão e trabalho futuro

O Kerberos é um protocolo versátil, maduro, fiável, seguro e amplamente utilizado na autenticação em redes de comunicação, sendo-lhe apontadas algumas limitações quanto à sua escalabilidade em ambiente inter-domínio. Existem, no entanto, diversas propostas actualmente em estudo na comunidade científica internacional para que o Kerberos passe a integrar com infra-estruturas de chave pública.

Com as extensões referidas será conseguida uma solução de autenticação bastante eficiente e escalável, sendo a gestão local de chaves da responsabilidade do KDC local e não de uma PKI global. Sempre que se queira realizar autenticação cruzada entre *realms*, aí recorre-se a uma PKI global, embora o volume de chaves envolvidas seja muito menor. Desta forma, as limitações de escalabilidade apresentadas pelas PKIs globais e pelo Kerberos unicamente com chaves privadas, poderão ser ultrapassadas e gerar-se uma solução bastante eficiente e escalável o que permitirá a sua utilização na autenticação de fluxos em ambiente DiffServ, proposto neste artigo.

A utilização de autenticação e autorização utilizando o protocolo Kerberos com as extensões discutidas, trará ao modelo DiffServ funcionalidades acrescidas de segurança contra ataques de roubo de recursos e de DQoS. Estas funcionalidades serão conseguidas através da autenticação periódica dos clientes e da configuração dinâmica dos recursos da rede, e poderão ainda suportar o funcionamento de mecanismos de contabilização e taxação.

Para validar as propostas contidas neste trabalho foi criado um *testbed* (ainda em fase de implementação), com máquinas Intel e Sistema Operativo Linux, com suporte de DiffServ e de Kerberos, onde serão realizadas implementações e testes em ambiente local.

Como trabalho futuro fica o estudo de integração da proposta com o protocolo *Diameter* [14], em discussão no grupo de AAA do IETF, a utilização dos *tickets* renováveis como fonte de informação para os sistemas de AAA, a passagem desta proposta do ambiente intra-domínio para um ambiente inter-domínio e a análise do impacto da gestão de tickets e da sua renovação em ambientes inter-domínio, caracterizados pelo elevado número de fluxos.

Agradecimentos

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. Black, D., Carlson, M., Davies, E., Wang, Z., Weiss, W., *An Architecture for Differentiated Services*, RFC 2475, Dezembro 1998.

[2] Nichols, K., Blake, S., Baker, F., Black, D., *Definition of the Differentiated Services Fields (DS Fields) in the IPv4 and IPv6 Headers*, RFC 2474, Dezembro 1998.

[3] Kohl, J., Neuman, C., *The Kerberos Network Authentication Service (V5)*, RFC 1510, Setembro 1993.

[4] Dierks, T., Allec, C., *The TLS Protocol*, RFC2246, Janeiro 1999.

[5] Kent, S., Atkinson, R., *Security Architecture for the Internet Protocol*, RFC2401, Novembro 1998.

[6] Mitton, D., St. Johns, M., Barkley, S., Nelson, D., Patil, B., Stevens, M., Wolff, B., *Authentication, Authorization, and Accounting: Protocol Evaluation*, RFC3127, Junho 2001.

[7] Durham, D., Boyle, J., Cohen, R., Herzog, S., Rajan, R. and Sastry, A., *The COPS (Common Open Policy Service) Protocol*, RFC 2748, Janeiro 2000.

[8] Stallings, W., *Cryptography and Network Security: Principles and Practices*, 2ª Edição, ISBN 0138690170, Prentice Hall, 1998.

[9] Fu, Zhi, Wu, S. Felix, Wu, T.S., Huang, He, *Security Issues for Differentiated Service Framework*, Internet Draft, Outubro 1999.

[10] Needham, R.M., Schroeder, M.D., *Using encryption for authentication in large networks of computers*, Communication of the ACM, p. 993-999, Dezembro 1978.

[11] Kaufman, C., Perlman, R., Speciner, M., *Network Security, Private Communication in a Public World*, 1995, Englewood Cliffs, New Jersey: PTR Prentice Hall.

[12] Schneier, B., *Applied Cryptography*, Second Edition, 2000, New York: John Wiley & Sons, Inc.

[13] ITU-T Information Technology – *Open Systems Interconnection – The Directory: Authentication Framework Recommendation X.509*, ISO/IEC 9594-8.

[14] Calhoun, P., Arkko, J., Guttman, E., Zorn, G., Loughney, J., *Diameter Base Protocol, Internet Draft*, Abril 2002.