Secure DNS-SD

Bruno dos Santos Duarte, Janaína Conceição Sutil Lemos, Rafael Bohrer Ávila
Universidade do Vale do Rio dos Sinos — UNISINOS
{brsants,janaina.lemos}@gmail.com
rbavila@unisinos.br

***Resumo*—A descoberta automática de serviços em redes é um mecanismo de extrema conveniência para compartilhar e acessar recursos, pois diminui o esforço de configuração e possibilita o uso transparente de tais serviços. Este trabalho traz uma proposta para incorporar mecanismos de segurança nos protocolos mDNS/DNS-Sd, os quais atuam na descoberta de serviços e estão presentes em diversos sistemas operacionais. A elaboração desta proposta se justifica pelo fato de que redes de computadores com gerenciamento distribuído e compartilhamento de serviços oferecem facilidades de acesso e utilização de recursos, entretanto cobram o risco de expor informações confidenciais.**

I. Introdução

Atualmente é de grande importância o uso de tecnologias para divulgar serviços disponíveis entre os integrantes de uma rede de computadores sem necessitar de configuração prévia e sem depender de uma entidade centralizadora para acessar estes recursos [1]. Isso se deve ao fato de a presença cotidiana das redes impulsionar a necessidade de soluções para a operação transparente nesses ambientes.

Um dos fatores que deve ser levado em conta no desenvolvimento de uma aplicação para descoberta de serviços é que uma rede de computadores auto-configurável contribui para a criação de um ambiente pervasivo, onde reinam o fácil acesso, a transparência operacional, e o anonimato dos usuários. Estes fatores tornam tais ambientes impróprios ao compartilhamento de recursos confidenciais, e por esse motivo, em aplicações dessa espécie é fundamental a aplicação de mecanismos que garantam confidencialidade e integridade de informações [2] [3].

Para que o processo de descoberta em ambientes pervasivos ocorra sem falhas de segurança ou quebra de confidencialidade, os protocolos de busca e anúncio de serviços devem prover os métodos de segurança cabíveis. Por exemplo, em uma sala de reuniões, em um saguão de aeroporto ou até mesmo em um café ou restaurante, pode haver uma ampla diversidade de dispositivos disseminando informações não solicitadas, críticas, ou mesmo nocivas, através dos mecanismos de descoberta de serviços [4]. A fim de evitar essa situação, a descoberta e o acesso a serviços confidenciais devem ocorrer sigilosamente através de credenciais válidas.

Esse trabalho tem como objetivo agregar mecanismos de segurança aos protocolos mDNS/DNS-SD, utilizados na descoberta de serviços. Para tal, faz-se uso do protocolo SEC-SD [5], que permite a descoberta de serviços exclusivamente em modo seguro e emprega uma arquitetura completamente distribuída. Nesse contexto, a adição de mecanismos de autenticação, confidencialidade e integridade aos protocolos mDNS/DNS-SD visa permitir o tratamento adequado da presença de serviços confidenciais em seu escopo de compartilhamento.

II. Trabalhos Relacionados

Existe um grande número de trabalhos e implementações que promovem descoberta de serviços, desenvolvidos tendo em conta diferentes critérios na escolha de suas características relacionadas aos aspectos e desafios inerentes a este tipo de aplicação.

O JINI [1] define regras para a criação uma rede ad hoc a fim de compartilhar serviços. Este sistema é uma extensão da linguagem java e faz uso de três entidades: provedores de serviços, serviços de consulta e clientes, permitindo que a descoberta de serviços seja feita com ou sem os serviços de consulta. A partir da segunda versão o JINI disponibiliza métodos de criptografia, autenticação e integridade. Porém, a autenticação é centralizada.

O UPnP [6] possibilita a auto configuração de dispositivos e descoberta de serviços. A arquitetura do UPnP baseia-se em duas entidades: os dispositivos controlados e os pontos de controle, onde os pontos de controle descobrem dispositivos controlados, porém não o contrário. O mecanismo de segurança implementado protege as mensagens de controle e as respectivas respostas, provendo identificação, integridade, autenticação, autorização e privacidade.

Em [7] é apresentado um protocolo desenvolvido para redes *mobile* e *peer-to-peer*, onde provedores e usuários de utilizam um sistema centralizado para registrar e buscar por serviços. Aqui é adotada a exposição gradual das identidades, a fim de estabelecer uma relação de confiança entre cliente e servidor. Este modelo não usa um número fixo de mensagens e apresenta baixa ocorrência de falsos positivos.

III. Secure DNS-SD

A. Zeroconf

Criado em 1999 pela IETF, o grupo *Zeroconf* define um conjunto de técnicas que possibilitam a criação automática de redes IP sem a necessidade de configurações prévias e servidores dedicados, como DHCP e DNS. Atualmente estas técnicas cobrem autoconfiguração de endereços IP, resolução de nomes via *multicast* e descoberta de serviços. Para a resolução de nomes é utilizado o protocolo mDNS

[1] www.jini.org

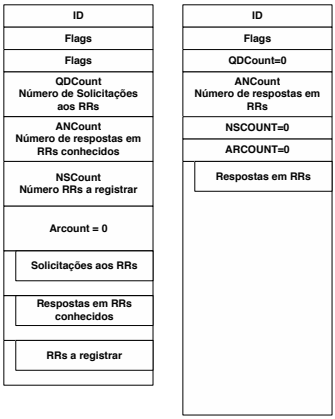

Figura 1. Pacotes de requisição e resposta mDNS

[8], já para a descoberta de serviços o protocolo adotado é o DNS-SD [1]. Um dos méritos dessa solução é o funcionamento completamente distribuído.

1) mDNS: A resolução de nomes sem servidores DHCP permite que um *host* na rede associe o seu *hostname* ao seu endereço IP auto atribuído [8]. Assim como ocorre na autoconfiguração de IPs, os conflitos de nomes devem ser resolvidos. Por isso, após ser criado o *address record* a exclusividade deste é colocada a prova e em caso de conflito, deve ser escolhido outro nome para o novo serviço. Para a diferenciação entre nomes locais de nomes de domínios existentes é utilizado o pseudo domínio de primeiro nível **.local**.

O processo responsável pelas respostas mDNS é o *mDNS Responder*, o qual efetua registros nos grupos *multicast*, publica estes registros e atualiza a cache mDNS. As requisições mDNS contém uma lista com as respostas possíveis às solicitações e o seu intervalo de envio tem crescimento exponencial, sendo uma hora o intervalo máximo. Outro detalhe importante é que cada novo membro da rede anuncia seus serviços automaticamente, enviando respostas sem que requisições tenham sido recebidas, e também o fato de o mDNS não apresentar nenhum mecanismo para prover segurança. A figura 1 mostra a estrutura dos pacotes mDNS.

2) DNS-SD: O protocolo DNS-SD define que um registro SRV deve carregar informações referentes a serviços, tais como nome do serviço, protocolo de transporte utilizado, *hostname* da máquina provedora, além de IP e porta [1] em uso, permitindo a identificação dos serviços pelos integrantes do grupo *multicast*. Já informações descritivas a respeito dos serviços podem estar contidas no registro TXT. Com isso tem-se que o protocolo DNS-SD é uma convenção para o uso de registros do DNS tradicional, não possuindo mecanismos adicionais de segurança, e por isso é um esquema vulnerável em ambientes pervasivos.

B. SEC-SD

O SEC-SD é um protocolo para a descoberta segura de serviços com funcionamento totalmente descentralizado, projetado para LANs, e que utiliza *four-way handshake* a fim de gerar uma chave criptográfica de renovação periódica que é utilizada para a busca de serviços oferecidos na rede [5]. Essas características tornam o SEC-SD um mecanismo interessante à proposta de integração com os protocolos MDNS/DNS-SD, que visa suprir a carência de técnicas de segurança nos mesmos.

As credenciais para a obtenção de chaves criptográficas via SEC-SD devem ser previamente distribuídas pelo proprietário do serviço aos seus clientes e dividem-se em identificador e senha, onde cada tupla diz respeito a apenas um serviço. Dessa forma é possível que um mesmo provedor de serviços os compartilhe serviços para vários grupos de usuários, cada qual com acesso limitado a determinados serviços, além de possibilitar que um mesmo dispositivo ofereça serviços pertencentes a diversos proprietários. Se for desejada pelo proprietário do serviços a identificação individual das entidades envolvidas na descoberta, ele e os seus clientes devem compartilhar as respectivas chaves públicas.

As credenciais do serviços são utilizadas pelos clientes e provedores juntamente com time-stamps para a obtenção de hashes dinâmicos que são enviados nas mensagens, a fim de evitar ataques do tipo *replay*. Os time-stamps também são enviados em claro nas mensagens. No SEC-SD não há anúncio de serviços, ao invés disso, quando um provedor ingressa na rede ele gera chaves criptográficas cada um de seus serviços, chamadas de *chaves de grupo* por serem distribuídas aos membros dos grupos que devem ter acesso ao serviço.

A descoberta de serviços com o SEC-SD se dá através das etapas de busca por serviços, autenticação, solicitação da chave criptográfica, envio da chave e solicitação das informações sobre o serviço. Detalhadamente, o processo inicia quando um cliente requisita um serviço enviando mensagens multicast e caso o provedor esteja disponível, ele verifica as credenciais enviadas pelo cliente e responde se as mesmas estiverem corretas. Nesse ponto, o cliente também verifica a autenticidade do provedor, e caso esta seja válida, ele solicita a chave criptográfica. Se as informações da solicitação estiverem corretas a chave é enviada. De posse da chave, o cliente pode então solicitar as informações referentes ao serviço e obter acesso ao mesmo. Assim, o SEC-SD fornece meios de legitimação de clientes que desejam acessar serviços protegidos, porém não oferece métodos de acesso aos serviços, assim como o conjunto mDNS/DNS-SD.

Na figura 2 é possível ver o formato dos pacotes SEC-SD.

C. Integração entre mDNS/DNS-SD e SEC-SD

Os protocolos mDNS/DNS-SD estão presentes em diversos sistemas operacionais e suas principais implemen-

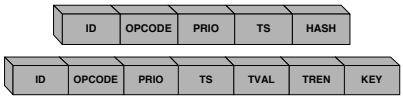

Figura 2. Pacotes SEC-SD de requisição/resposta e envio de chave de grupo

tações são o Bonjour[2], da Apple, e o Avahi[3] , uma implementação *open source*. Contudo, estes protocolos carecem de mecanismos de segurança. A seguir é descrito o SEC-SD, que provê técnicas de autenticação, confidencialidade e integridade e cuja integração com o mDNS/DNS-SD se dará com uso do Avahi.

A agregação dos mecanismos e políticas que garantem autenticação, autenticidade e confidencialidade presentes no protocolo SEC-SD ao processo de descoberta de serviços com os protocolos mDNS/DNS-SD visa permitir o acesso a serviços confidenciais apenas para usuários com permissão, reservando o anúncio de conteúdo para os demais recursos compartilhados, além de mantém a facilidade de uso e o funcionamento totalmente distribuído.

Apesar de os sistemas alvo para a integração serem soluções estáveis e com funcionamento comprovado, diversos desafios foram considerados antes de iniciar o processo de implementação do projeto, visto que na prática ambos podem apresentar sensibilidade em diversos pontos. Dentre as questões maid relevantes destacam-se a paralelização da descoberta de serviços confidenciais com o mecanismo de descoberta já implementado no Avahi, a disposição das informações utilizadas pelo SEC-SD no pacote DNS-SD, a vazão de dados resultante da integração e a política de interação entre estados dos protocolos, visto que o mDNS/DNS-SD utiliza uma política de *anúncio-requisição* enquanto o SEC-SD é *four-way handshake*.

Tendo em vista os desafios previstos para a implementação desse projeto, foram definidos os seguintes pontos de alteração para os protocolos mDNS/DNS-SD:

- As seções de descoberta serão iniciadas utilizando os protocolos mDNS/DNS-SD. A partir daí, caso a requisição seja por um serviço seguro, esta deverá ser repassada ao SEC-SD para receber tratamento adequado;
- O protocolo mDNS envia requisições e respostas em *multicast*. Para a descoberta segura de serviços é previsto o envio das respostas em *unicast*. Esse comportamento é próprio do protocolo SEC-SD e se ajusta a política de confidencialidade;
- O mDNS utiliza a porta 5353 UDP. A fim de simplificar o tratamento de requisições a serviços seguros e reduzir o impacto sobre o mecanismo de descoberta já implementado será adotada a porta UDP 5354;
- Para diferenciar localmente serviços públicos e confidenciais com um menor impacto, será adotado um novo diretório para armazenar as definições dos serviços confidenciais, visto que os serviços públicos ficam sob o diretório */etc/avahi/services*;
- Um pacote mDNS contém, além das múltiplas requisições, um conjunto de respostas conhecidas. Para operar de acordo com o protocolo SEC-SD em requisições por serviços confidenciais, o mDNS conterá apenas uma menção ao tipo genérico ***sec-services***. Além disso, não será enviada nenhuma resposta conhecida;
- O campo respostas conhecidas será utilizado para encapsular a requisição SEC-SD, contribuindo para que a adaptação do mDNS/DNS-SD seja tão pouco intrusiva quanto possível;

[2]http://developer.apple.com/mac/library/documentation /cocoa/Conceptual/NetServices/ Articles/about.html

[3]http://avahi.org

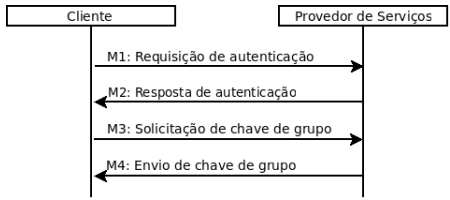

Figura 3. Sequência de mensagens do SEC-SD

D. Descoberta do serviço sec-services

A fim de permitir que a integração entre as tecnologias seja pouco intrusiva, as requisições e respostas de autenticação do SEC-SD serão encapsuladas no campo destinado as respostas conhecidas do mDNS.

Para atingir este objetivo, será enviada somente uma resposta nesse campo, contendo a requisição ou resposta do SEC-SD (50 bytes) no espaço que usualmente carrega a instância de um serviço conhecido (um exemplo comum de instância seria *anonymous-note.local*). Além disso, uma resposta conhecida contém normalmente o tipo de registro (IPv4 ou IPv6), o qual será mantido, o TTL, que deve assumir um valor alto para permitir o envio de respostas unicast, e o endereço IP (que com a adaptação será sempre o da placa de rede local).

Pelo fato de o mDNS prever nomes de até 255 bytes para as instâncias de serviços, o cabeçalho SEC-SD não incidirá aumento significativo no tamanho das mensagens mDNS. Além disso, os campos do DNS-SD serão mantidos, com alterações somente nos valores dos parâmetros.

A sequência de mensagens do SEC-SD para obtenção da chave criptográfica é mostrada na figura 3.

Para as duas primeiras mensagens desta sequência será utilizado o mDNS/DNS-SD, conforme descrito acima. Para a solicitação e envio da chave será utilizado o protocolo SEC-SD em seu formato original, com mensagens unicast.

IV. Validação

Nesta seção é apresentada a avaliação do tráfego gerado pelo Secure DNS-SD com base na quantidade de mensagens enviadas durante a autenticação e obtenção da chave

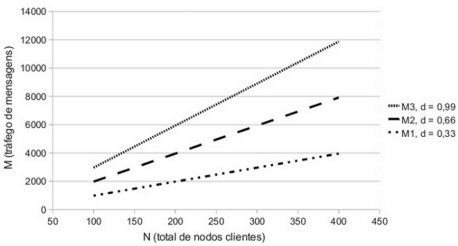

Figura 4. Tráfego de mensagens da integração SEC-SD e mDNS/DNS-SD

de grupo do SEC-SD, considerando o seu cabeçalho de 50 bytes encapsulado na mensagem mDNS/DNS-SD.

Objetivando verificar a adequação da proposta a ambientes com grande quantidade de máquinas e serviços, foi avaliado o impacto do tráfego causado pelas respostas de autenticação enviadas em unicast pelos provedores. Estas mensagens são enviadas no momento em que os dispositivos ingressam na rede e iniciam o processo para obtenção das chaves de grupo, e seu volume cresce proporcionalmente a disponibilidade de serviços na rede.

O tráfego de respostas de autenticação unicast em um determinado instante é dado por

$$M = N * S * d$$

onde N é a quantidade de nodos clientes rede e S é a quantidade média de serviços que cada nodo pode descobrir (possui credenciais válidas). Os dispositivos denotados por N são máquinas que executam o Sec-SD e atuam ao menos como clientes, podendo ou não disponibilizar serviços, e d compreende a disponibilidade média de serviços exclusivos na rede em um dado momento.

Para análise, são considerados os seguintes cenários:

$100 <= N <= 400$
$S = 30$
$d = 0.33, d = 0.66, d = 0.99$

Estes valores foram escolhidos a fim de representar redes de tamanho variável no que diz respeito a quantidade de nodos e a disponibilidade de serviços, e o impacto do uso do Secure DNS-SD em tais redes, avaliando assim a adequação do mesmo a ambientes com grande número de máquinas. O gráfico correspondente a estes cenários é mostrado na figura 4

Considera-se que as mensagens mostradas no gráfico representam uma situação onde a entrada dos clientes ocorre em um intervalo de 30 minutos. Esse comportamento poderia ocorrer por exemplo em um ambiente educacional, na chegada de alunos em um laboratório. Considerando este intervalo, é possível obter uma estimativa do tráfego de pacotes por minuto em situações onde o volume de mensagens enviadas tende a apresentar picos.

Observou-se que o cenário 1 (gráfico M1), com 100 nodos ativos descobrindo um total de 30 serviços a média de respostas unicast de autenticação é de 4.6 KB por minuto. Com 400 nodos ativos (pior caso), este número sobe para 18.6 KB a cada minuto. Já no cenário 2 (M2), com 300 nodos clientes na rede, a média de respostas de autenticação é de 28 KB por minuto. Com 400 nodos ativos, são enviados 37.3 KB a cada minuto. Por último, tem-se no cenário 3 (M3) uma rede onde 99% dos serviços estão disponíveis. Neste caso, são enviadas em média 56 KB por minuto quando se tem 400 clientes ingressando na rede em um intervalo de 30 minutos.

V. Conclusões e Trabalhos Futuros

Este trabalho contribui agregando as técnicas de autenticação, confidencialidade e integridade trazidas no protocolo SEC-SD às tecnologias mDNS/DNS-SD, já amplamente difundidas. Esta integração é feita visando obter uma solução econômica, completamente distribuída e destinada a redes locais. Além disso, esse novo sistema utiliza-se de implementações open source a fim de estimular a sua adesão e possibilitar a sua evolução. Como trabalho futuro, está prevista a implementação do Secure DNS-SD com o uso Avahi e do protótipo do SEC-SD.

Referências

[1] S. Cheshire and M. Krochmal, "DNS-Based Service Discovery," feb 2011, Internet Draft, Internet Engineering Task Force (IETF). http://tools.ietf.org/html/draft-cheshire-dnsext-dns-sd-10.

[2] J. Golbeck, "Trust on the World Wide Web: A Survey," *Foundations and Trends in Web Science*, vol. 1, no. 2, pp. 131–197, 2008.

[3] G. Ververids, C.; Polizos, "Service discovery for mobile ad hoc networks: A survey of issues and techniques," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 3, pp. 30–45, 2008.

[4] F. Zhu, M. Mutka, and L. Ni, "A private, secure, and user-centric information exposure model for service discovery protocols," in *IEEE Transactions on Mobile Computing*, vol. 5, no. 4, Piscataway, NJ, USA, 2006.

[5] J. Lemos, "Sec-sd: Um modelo distribuído para descoberta segura de serviços em redes locais," Dissertação de Mestrado, Universidade do Vale do Rio dos Sinos, São Leopoldo, RS, Brasil, 2011.

[6] A. Presser, L. Farrell, D. Kemp, W. Lupton, S.Tsuruyama, and S.Albright, "UPnP device architeture 1.1," 2008, uPnP Forum. www.upnp.cn/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf.

[7] S. L. M. Muthyapu, S.; Madria, "Preservd - privacy ensured service discovery in mobile peer-to-peer networks," in *Reliable Distributed Systems*, 2010, pp. 1–10.

[8] S. Cheshire and M. Krochmal, "Multicast DNS," feb 2011, Internet Draft, Internet Engineering Task Force (IETF). http://tools.ietf.org/html/draft-cheshire-dnsext-multicastdns-14.