Metodologia para Avaliação de Uso de SNMP e Web Services em Gerência de Redes Através de Medições de Tráfego

Giovane C. M. Moura, Ewerton M. Salvador

[1]Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brasil

{gcmmoura, emsalvador}@inf.ufrgs.br

Resumo. *O protocolo SNMP tem como objetivo prover funcionalidades de gerenciamento de redes. Porém, não se sabe exatamente como o SNMP é utilizado no dia-a-dia das redes de produção. Recentemente, o IRTF propôs uma metodologia para se descobrir o uso real desse protocolo. Uma outra tecnologia tem sido grande alvo de estudos no gerenciamento de redes: Web Services. Neste artigo propõe-se uma extensão à metodologia do IRTF, a fim de possibilitar uma avaliação do uso de Web Services em gerenciamento de redes.*

1. Introdução

Proposto há mais de 15 anos, o *Simple Network Management Protocol* (SNMP) [Harrington et al. 2002] tem como objetivo prover funcionalidades de gerenciamento de redes. Ele encontra-se disponível em diversos dispositivos de rede, como roteadores, *switches* e modems ADSL. Duas versões do protocolo foram propostas após a versão original, sendo elas o SNMPv2 e SNMPv3.

Apesar de amplamente conhecido, não se tem uma idéia de como SNMP é usado no dia-a-dia e quais de suas funcionalidades são efetivamente aproveitadas. A partir dessa constatação, o *Network Management Research Group* (NMRG) [NMRG 2006] do *Internet Research Task Force* (IRTF) propôs uma metodologia [Schoenwaelder 2006] para determinar como o SNMP é utilizado nas redes de computadores.

Recentemente outra tecnologia tem sido grande alvo de estudos no gerenciamento de redes: Web Services [Pavlou et al. 2004]. Como vantagens, Web Services utiliza-se de padrões abertos da Internet, como *Extensible Markup Language* (XML), SOAP [SOAP 2003], *Universal Description, Discovery, and Integration* (UDDI) [UDDI 2005], que facilitam a integração entre diversos sistemas, independente de linguagem de programação e sistema operacional.

Web Services ainda não são utilizados em gerenciamento de redes, porém a indústria estuda o seu uso, como se pode constatar com os padrões *Management Using Web Services* (MUWS) [MUWS 2005] e *Web Services Management* (WS-M) [WS-M 2005]. Desta forma, existe a tendência de que ele seja utilizado em gerenciamento. A proposta do IRTF não contempla o uso de quaisquer outros protocolos de gerenciamento senão o SNMP. O objetivo deste artigo é promover a extensão da metodologia do IRTF para o suporte aos Web Services em gerenciamento de redes.

Este artigo se organiza da seguinte forma: na Seção 2 é apresentada a metodologia proposta pelo IRTF. Na Seção 3 é mostrada a extensão da metodologia do IRTF para análise de Web Services em gerenciamento de redes. Na Seção 4, são apresentadas

questões iniciais para conduzir as análises. Por fim, na Seção 5, o artigo é finalizado com conclusões e trabalhos futuros são encorajados.

2. Metodologia para Estudo de Uso do SNMP

Em março de 2006, o NMRG lançou o *draft* intitulado "*SNMP Traffic Measurements*"[Schoenwaelder 2006], contendo a metodologia para estudo de uso do SNMP. Esta metodologia é composta de 5 passos básicos:

1. Captura do tráfego SNMP com algum *sniffer* de rede, como Ethereal, e gravação no formato pcap [Jacobson et al. 2006].
2. Conversão dos arquivos pcap em outro formato, como XML. Um XML *schema* foi desenvolvido para capturar todos os detalhes das mensagens SNMP. Outro formato mais compacto seria o *comma separated values* (CSV) para armazenar apenas as informações chave dos arquivos pcap.
3. Filtragem do tráfego para que seja possível remover informações confidenciais dos pacotes SNMP, tais como *strings* de comunidade. A filtragem é um passo separado, porém pode ser implementado junto com conversão dos dados para um melhor desempenho.
4. Armazenamento dos dados filtrados em um repositório onde possam ser acessados de forma pública ou sobre controle de operadores de redes ou grupo de pesquisa.
5. Análise dos arquivos obtidos com ferramentas automatizadas para extrair e agregar informações.

A partir dessa metodologia, será possível determinar várias características de uso de SNMP nas atividades de gerência de redes.

3. Proposta de uma metodologia para análise de uso de Web Services em gerenciamento de redes

São apresentadas, nessa Seção, as extensões da proposta do IRTF para análise do tráfego de gerenciamento de redes com Web Services.

3.1. Captura dos Dados

A metodologia do IRTF recomenda o uso de algum *sniffer* de rede, como Ethereal e tcpdump [Jacobson et al. 2006], que possibilite usar filtros para separar o tráfego SNMP que, tipicamente, é feito nas portas 161 ou 162 com protocolo UDP.

Para Web Services, a abordagem é mais complicada, pois o conteúdo é encapsulado em envelopes SOAP que, por sua vez, é encapsulado no HTTP. Além disso, deve-se distinguir o tráfego de gerenciamento daquele gerado por outras aplicações que também usam Web Services.

Para lidar com este problema, deve-se capturar todo tráfego HTTP e posteriormente realizar uma análise, observando se o conteúdo dos envelopes SOAP contém algum dos padrões de gerenciamento com Web Services. Como exemplo, poderíamos ter uma aplicação qualquer utilizando Web Services e um roteador utilizando Web Services para gerenciamento. Ao observar o conteúdo SOAP, pode-se descobrir através de *tags* XML se é usado um padrão de gerenciamento, conseguindo assim distinguir a aplicação do roteador.

Caso o conteúdo esteja compactado, deve-se capturar o tráfego e posteriormente descompactar a partir do fluxo. Caso esteja criptografado não será possível, *a priori*, decodificar o conteúdo dos pacotes capturados.

3.2. Conversão dos Arquivos Capturados

O IRTF propõe a conversão do tráfego representado no formato pcap para um formato que seja facilmente legível por humanos, para identificação de dados confidenciais a serem retirados; e por máquinas, para tornar os programas que realizarão as análises mais eficientes e fáceis de serem desenvolvidos. A escolha natural para se atender a esses requisitos é a representação XML. Ela pode ser facilmente lida pelas pessoas e para máquinas, devido à abundância de bibliotecas para linguagens de programação de alto nível que suportam a manipulação de arquivos XML. Entretanto, como XML utiliza-se muito de tags, pode ser necessário a escolha de um padrão que gere menos sobrecarga no processamento desses arquivos. Para isso, pode-se utilizar a representação CSV, que consiste em registros sendo armazenados em linhas de arquivos de texto puro (ASCII), com informações separadas por vírgulas, o que o torna mais compacto.

Para gerenciamento com Web Services, a idéia de se converter os dados que estão em formato pcap para as representações XML/CSV permanece válida. Dessa forma, pode-se analisar o tráfego gerado pelos Web Services com a mesma eficiência da metodologia original proposta pelo IRTF para tráfego SNMP.

A proposta do IRTF apresenta a ferramenta SNMPDUMP para conversão do formato pcap com conteúdo de SNMP para formato XML e CSV. Por isso, identifica-se a necessidade do desenvolvimento de uma ferramenta para que, a partir de tráfego de Web Services em formato pcap, se obtenha representações XML e CSV.

3.3. Filtragem dos Arquivos

O tráfego SNMP possui informações confidenciais tais como endereço IP dos roteadores e *strings* de comunidade. Para evitar que essas informações sejam divulgadas sem nenhum controle, deve-se realizar um processo de anonimização dos dados obtidos da etapa anterior da metodologia do IRTF.

O mesmo problema ocorre quando se captura tráfego de gerenciamento utilizando-se Web Services em redes de produção: informações confidenciais poderão ser obtidas, e deve-se filtrá-las para análise. Por isso, o mesmo processo de anonimização apresentado pelo IRTF deve ser aplicado aos arquivos XML/CSV originados a partir da conversão das informações de tráfego de Web Services que se encontravam no formato pcap.

A ferramenta SNMPDUMP fornece suporte para anonimização de dados confidenciais do SNMP. Analogamente, deve-se desenvolver uma ferramenta de anonimização para tráfego Web Services.

3.4. Armazenamento das Informações

A proposta inicial sugere que tanto os arquivos pcap quanto os arquivos XML/CSV devem ser armazenados e mantidos por um grupo de pesquisa ou operadores de rede. O armazenamento seguro desses arquivos é de fundamental importância para projetos futuros e validações de pesquisas. A proposta ainda afirma que o acesso aos dados deve ser público ou restrito a pessoas que assinem algum tipo de “acordo de não-divulgação”.

É proposto um modelo modificado: acesso público e livre a todos os arquivos XML/CSV filtrados. Desta forma, fornecem-se informações e ferramentas para pesquisadores/estudantes desprovidos de acesso a tal conteúdo sem, com isso, divulgar informações confidenciais. Quanto aos arquivos pcap (não filtrados), estes sim devem seguir a abordagem sugerida de acesso restrito. É encorajado que os arquivos XML/CSV obtidos sejam disponibilizados para cópia na Internet.

3.5. Análise dos Arquivos

A partir dos arquivos filtrados, deve-se analisar os dados do tráfego de gerenciamento, a fim de se obter as respostas para as questões pertinentes ao estudo realizado. Para isso, o mesmo processo de análise descrito na metodologia original do IRTF deve ser utilizado para o processamento dos tráfegos de Web Services aplicados na área de gerenciamento de rede.

A sugestão dada pela metodologia do IRTF, e por conseqüência a mesma oferecida pela metodologia apresentada neste artigo, seria a utilização da linguagem Perl para a análise dos arquivos filtrados. Dessa forma, o código-fonte desses *scripts* podem ser facilmente legíveis pelos componentes do grupo de pesquisa e pelos operadores da rede que serviu de fontes para os dados a serem analisados.

Um resumo de todo processo pode ser visto na Figura 1, onde os números entre parênteses marcam a fase do processo da metodologia.

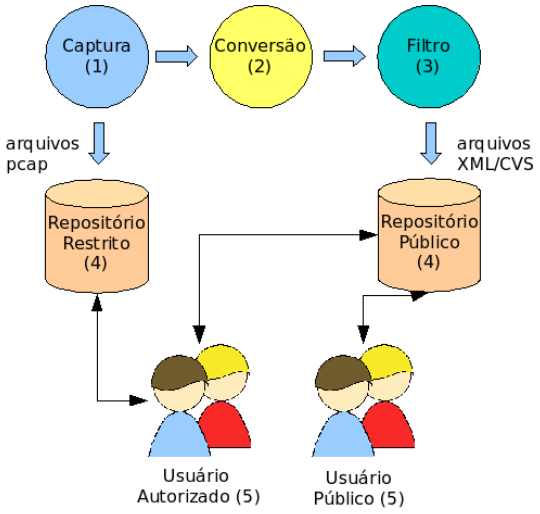

Figura 1. Etapas da Metodologia descrita na Seção 3

4. Análise dos Arquivos Filtrados

Este seção apresenta e discute um conjunto de questões que constituirão a proposta inicial apresentada por este artigo para a análise do tráfego de gerenciamento coletado. Outras questões podem ser propostas pelo grupo que está promovendo a pesquisa de uso do protocolo SNMP, a fim de enriquecer a análise realizada com resultados mais completos.

4.1. Estatísticas Básicas

As estatísticas básicas representam informações mais gerais sobre a monitoração realizada. Nessas estatísticas foi incluído um levantamento das ocorrências dos padrões de

Web Services utilizados para o gerenciamento, assim como as operações de gerenciamento realizadas que foram identificadas no tráfego SNMP monitorado. A partir desses dados, poderá se identificar a predominância de um ou outro padrão de Web Service na rede, como os padrões MUWS e WS-M. Do mesmo modo, será possível se determinar as operações (por exemplo, leitura/escrita de informações de gerenciamento) que estão sendo mais utilizadas, assim como aquelas que não foram colocadas em uso.

4.2. Tráfego Periódico e Tráfego Aperiódico

Em gerenciamento de redes existem basicamente dois tipos de tráfego: periódico e aperiódico. O tráfego periódico é caracterizado pela repetição de alguma operação realizada automaticamente, de maneira periódica. Como exemplo disso, cita-se o caso de uma aplicação de gerenciamento que verifica a cada 30 minutos a temperatura de um roteador. Já o tráfego aperiódico se caracteriza por aquelas operações que não se repetem de maneira periódica, ou seja, tem uma característica mais eventual. Por exemplo, pode-se citar a operação de alteração de uma rota em uma tabela de roteamento. É interessante se entender a relação existente entre tráfego periódico e aperiódico nos padrões de gerenciamento com Web Services, além de se pesquisar em quais situações existem vários níveis de periodicidade em diferentes escalas de tempo.

4.3. Tamanho da mensagem e distribuição da latência

Uma informação interessante a ser obtida com a análise do tráfego SNMP é a determinação da distribuição dos tamanhos das mensagens. Isso é especialmente importante em relação aos Web Services, tendo em vista que basicamente são enviados nas mensagens documentos XML: arquivos de textos com muitas marcações especiais, gerando um maior uso da rede.

Outro ponto a ser observado é a distribuição da latência nas transmissões de mensagens de gerenciamento, dando-se atenção especialmente ao tempo de processamento dessas mensagens pelos agentes que as receberem. Dessa forma, poderão ser utilizadas abordagens para se inferir atrasos na rede através da observação do tempo compreendido entre o envio de uma requisição e o recebimento da respectiva resposta, levando-se em consideração o tempo aproximado que essa requisição precisou para ser processada.

4.4. Níveis de concorrência

O uso de Web Services nas tarefas de gerenciamento deve permitir a aquisição de informações de múltiplos agentes concorrentemente. Por exemplo, pode-se solicitar a temperatura de todos os roteadores presentes em um domínio administrativo num mesmo instante, de forma que essas requisições, por serem simultâneas, concorrem entre si. É interessante identificar quais são os níveis de concorrência típicos que podem ser observados nas redes de produção, ou quais os casos em que as aplicações de gerenciamento dão preferência à soluções seqüenciais de recuperação de dados.

4.5. Distribuição da quantidade de objetos retornados por requisição

Em comparações de desempenho entre o protocolo SNMP e Web Services utilizados para gerenciamento de redes, pode-se observar que o SNMP pode ser mais eficiente do que Web Services quando um único objeto é retornado em uma requisição. Por exemplo, quando se solicita o nome de um dispositivo, apenas um objeto é retornado. Entretanto,

geralmente Web Services apresentam uma maior eficiência quando mais de um objeto é retornado [Pras et al. 2004]. Um exemplo em que uma requisição retorna múltiplos objetos é a solicitação de quais rotas estão cadastradas na tabela de roteamento de um determinado roteador. Devido a isso, é interessante identificar-se qual desses dois casos é mais comumente utilizado no dia-a-dia dos gerentes de rede, a fim de tornar mais justas as comparações apresentadas nessas análises comparativas já existentes.

5. Conclusões e Trabalhos Futuros

A partir da metodologia apresentada pelo IRTF, que lida apenas com o SNMP, foi proposta uma extensão para que as abordagens que utilizam Web Services também possam ser avaliadas, assim que elas forem aplicadas em gerenciamento de redes de produção.

Além disso, também foi apresentado um modelo de armazenamento de informações, em que qualquer pessoa possa ter acesso às informações filtradas para fins de pesquisa, e foram mantidas restrições quanto ao acesso aos arquivos pcap, uma vez que estes possuem informações confidenciais. Como maior benefício de um repositório de consulta aberta, tem-se a inclusão de diversos estudantes/pesquisadores, que não possuem acesso a este tipo de dados.

Como trabalho futuro, pretende-se implementar uma ferramenta que auxilie no processo de conversão dos dados que estão armazenados no formato pcap (com traços de *Web Services)* para o formato XML ou CSV. Também deverá ser tarefa dessa ferramenta automatizar o processo de filtragem dos dados, a fim de se remover as informações consideradas confidenciais.

Referências

Harrington, D., Presuhn, R., and Wijnen, B. (2002). An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. Internet Engineering Task Force (IETF), RFC 3411, STD 62. http://tools.ietf.org/html/3411.

Jacobson, V., Leres, C., and McCanne, S. (2006). tcpdump. http://www.tcpdump.org/.

MUWS (2005). Web Services Distributed Management: Management Using Web Services (MUWS). http://docs.oasis-open.org/wsdm/2004/12/wsdm-muws-part1-1.0.pdf.

NMRG (2006). Network Management Research Group. http://www.irtf.org/charter?gtype=rg&group=nmrg.

Pavlou, G., Flegkas, P., Gouveris, S., and Liotta, A. (2004). On management technologies and the potential of Web services. *Communications Magazine, IEEE*, 42(7):58–66.

Pras, A., Drevers, T., van de Meent, T. R., and Quartel, D. (2004). Comparing the performance of SNMP and web services based management. *eTransactions on Network and Services Management, IEEE*.

Schoenwaelder, J. (2006). SNMP Traffic Measurements. http://www.ietf.org/internet-drafts/draft-irtf-nmrg-snmp-measure-00.txt.

SOAP (2003). SOAP version 1.2 part 0: Primer. http://www.w3.org/TR/soap12-part0/.

UDDI (2005). UDDI.org. http://uddi.org/.

WS-M (2005). WS-Management. http://www.dmtf.org/newsroom/releases/2006_04_25a/.