LEVANTAMENTO E MAPEAMENTO DA DISTRIBUIÇÃO DE *MIDDLEBOXES* PRESENTES NA *WORLD WIDE WEB*

SURVEY AND MAPPING OF MIDDLEBOX DISTRIBUTION IN THE WORLD WIDE WEB

Autores: Bruno Borsatti CHAGAS [1], Adenes Sabino SCHWANTZ[2].
Identificação autores: [1]Aluno do Curso Superior de Engenharia Elétrica do Instituto Federal Catarinense – Campus Videira. [2]Professor Orientador do Instituto Federal Catarinense – Campus Videira

RESUMO

Este trabalho visou investigar a ação de dispositivos, presentes em redes de computadores de forma geral, chamados *middleboxes*. Além disso a pesquisa visa trazer à luz, em forma de resultados, o impacto e a frequência de atuação desses dispositivos. A pesquisa se deu de forma ampla e global, avaliando diferentes modos de conexão, bem como testando a interação desses dispositivos com diversas características dos dados que trafegam na rede mundial de computadores.
Palavras-chave: Topologia de rede; Descoberta de rede; Middleboxes.

ABSTRACT

This work aimed to investigate the action of devices, present in computer networks, called middleboxes. In addition, the research aims to bring to light, in the form of results, the impact of these devices. This research was conducted in a broad and global way, evaluating different modes of connection, as well as testing the interaction of these devices with several characteristics of the data flowing through the internet.
Keywords: Network topology; Network Discovery; Middleboxes.

INTRODUÇÃO E JUSTIFICATIVA

A internet é baseada em roteadores e *hosts*. Conforme Sherry et al. (2012, p. 2) evidenciam, “com o crescimento da rede, surgiram alguns problemas, tais como vírus, segurança de dados, falta de endereços IPv4, entre outros”. Para contornar esses problemas, antivírus, *firewalls*, NATs (Tradudores de Endereço de Rede), etc., são usados. Entretanto, a rede mundial de computadores não foi projetada originalmente para lidar com tais dispositivos.

Outros dispositivos, que não roteadores e *hosts*, executando qualquer função são denominados *middleboxes*, nome proposto por Lixia Zhang e formalizado na RFC 3234. De acordo com Medina et. al. (2007, p. 4) “uma *middlebox* pode modificar a informação contida nos campos dos cabeçalhos do protocolo TCP/IP”.

Os autores Detal et al. (2012) apresentam Tracebox, uma ferramenta que permite a detecção de *middleboxes* em qualquer caminho de rede, ou seja, entre um *host* fonte e um *host*/endereço IP de destino. Todos os campos do datagrama TCP/IP são passiveis de sofrerem modificações resultantes de uma operação efetuada por uma *middlebox*, e Tracebox pode detectar tais modificações.

Dessa forma, com este trabalho objetivou-se detectar as modificações ocasionadas pelas *middleboxes* nos dados que estas processam. Além disso teve-se como objetivo compreender sua atuação e impactos no tráfego de dados na rede.

METODOLOGIA

Esse estudo envolveu uma amostra 1152 endereços IP, a partir dos quais foram levantadas as *middleboxes* presentes no caminho de rede e as modificações que estas causaram. Os testes foram realizados de quatro maneiras, identificadas de 0 a 3, afim de tentar localizar *middleboxes* que atuam e reagem com determinados tipos específicos de pacotes de dados.

Ainda, foram utilizados três modos de conexão, sendo estes Ethernet (802.3), Wi-Fi (802.11) e 3G (HSDPA) para todos os endereços IP e utilizando quatro configurações de argumento nos pacotes enviados. Ademais, os modos de conexão foram comparados para verificar uma possível prioridade, devido ao fato de que o caminho percorrido é, quase em sua totalidade, o mesmo.

A *probe* (pacote-teste) 0 faz parte do grupo controle, com ela foi possível observar modificações que as *middleboxes* normalmente provocam. Já as *probes* de 1 a 3 possuem parâmetros para detectar modificações diferentes do grupo controle. As *probes* 1 e 2 testaram argumentos do cabeçalho TCP do pacote. Argumentos estes tais como MSS, que define o tamanho do *payload* e WSCALE. Ainda se testou MPCAPABLE, que verifica a capacidade da rede de executar uma tarefa em múltiplos caminhos, como definido na RFC 6824. Se averiguou TS, que auxilia na performance do protocolo TCP como exemplifica Silbersack (2005) em seu estudo. O parâmetro NOP, que é usado para preencher a lista de opções, bem como SACKPermitted, que altera o comportamento de confirmação do TCP, também foram intensamente testados. A *probe* 3 testou única e exclusivamente o argumento MPCAPABLE, afim de verificar a adaptabilidade da rede à esta recente opção adicional do protocolo.

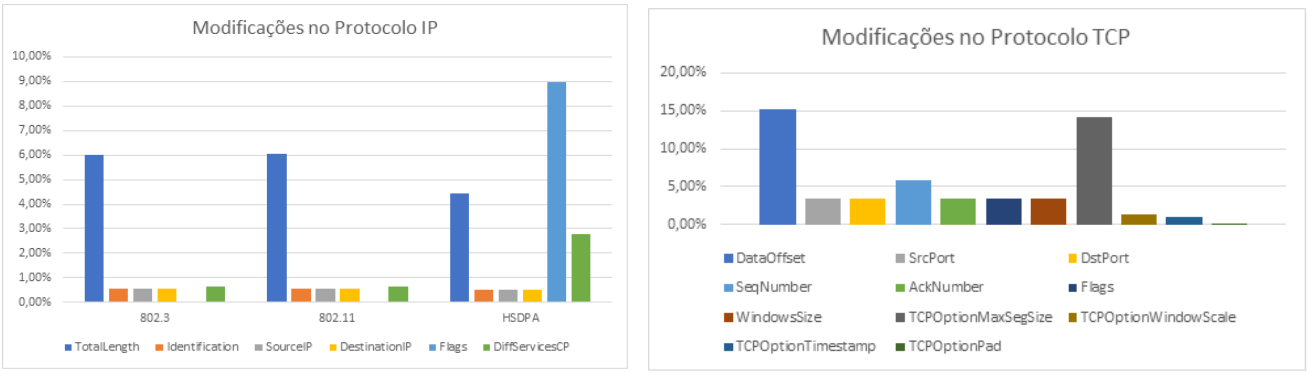
Para a realização dos testes, foi composta uma lista com os endereços IP que serviram de alvo. Todos os endereços foram analisados com quatro diferentes configurações de argumentos e em três modos de conexão, já citados no começo da sessão.

Após a execução de todos os testes, as mudanças detectadas são contabilizadas. As comparações foram feitas entre *probes* 0 e 3, buscando diferenças nas *middleboxes* que são acionadas com a função MPCAPABLE. Isso também é feito entre as *probes* 1 e 2, identificando diferenças principalmente no protocolo TCP.

RESULTADOS E DISCUSSÕES

Os dados levantados pelos testes mostraram que o protocolo IP apresentou um comportamento anômalo em vista do padrão esperado. Esperava-se uma porcentagem menor que 0,1% das modificações no campo *Flags* nas conexões em geral (HONDA et al., 2011). Em especial na conexão HSDPA, porém, encontrou-se valores bem superiores nos testes realizados, vide figura 1. O campo *Flags* indicou 9,04% do total de modificações, sendo que 8,95% foram apenas com a conexão HSDPA, assim como o campo *DiffServicesCP*, que apresentou um total de 4,05% das modificações, sendo 2,76% relacionadas a conexão HSDPA.

Figura 1. Panorama geral de alterações relacionadas aos cabeçalhos IP e TCP.



Fonte: Autores.

Logo, analisando o percentual de modificação dos campos *Flags* e *DiffServicesCP* nas três conexões e o tempo total de execução dos testes, verifica-se que a conexão HSDPA

obteve um pior desempenho em relação as conexões 802.3 e 802.11 devido à alta taxa de alteração no campo *Flags*.

Esse fator impacta diretamente na velocidade de comunicação e transmissão da informação (DETAL et al., 2012). Percebemos assim que outros pacotes estavam sendo priorizados de forma constante. Nesse sentido nota-se uma maior presença de *middleboxes* nesse modo de conexão, desrespeitando, portanto, o princípio *end-to-end* das redes de computadores.

Analisando o tempo total de execução dos testes, o tempo médio para que uma modificação no campo *Flags* com as conexões 802.3 e 802.11 ocorra é de aproximadamente 247 segundos, já na conexão HSDPA uma modificação ocorre aproximadamente a cada 3 segundos.

Nas *probes* 0 e 3 foi identificado o mesmo padrão na maioria dos campos, com a exceção da alteração "Removidos" que apresentou uma taxa de 1,70% na execução da *probe* 3. Isso aponta para que alguns endereços IP que foram testados pela *probe* não possuírem múltiplos caminhos a serem percorridos pelos pacotes. Com isso reforça-se a hipótese de lenta adaptabilidade da rede a inovações (HONDA et al., 2011).

CONSIDERAÇÕES FINAIS

Foi possível identificar padrões e casos específicos que vem sendo executados pelas mais diversas *middleboxes* presentes na grande rede. A presença destas, ainda que conhecida, mostrou-se forte, bem como sua atuação, atendendo seus requisitos. Requisitos estes que obedecem às mais diversas especificações, determinadas por aqueles (provedores, empresas, usuários) que as instalaram.

Os resultados desta pesquisa nos mostraram a forte presença de *middleboxes* nos caminhos testados e por consequência na internet como um todo. Idealmente teríamos uma rede sem quaisquer dispositivos alterando o conteúdo da informação que esta transporta (SALTZER; REED; CLARK, 1984). Porém, os resultados apontam para taxas exorbitantes de modificações, alcançando, em alguns casos, níveis de 6% até 9% do total de endereços.

A livre implantação de *middleboxes*, especialmente à critério de administradores de

rede não é novidade. Diversos estudos apontam para o crescente número de dispositivos e, principalmente sua interação com as diferentes camadas de rede (MEDINA; ALLMAN; FLOYD, 2004) (JUSTINE et al., 2012). Ao comparar-se os resultados obtidos nesse estudo com pesquisas datadas de alguns anos atrás, acima mencionadas, percebemos o forte crescimento das *middleboxes* na rede, bem como suas ações, prioridades e impactos. Alguns padrões de atuação e prioridades de execução puderam ser observados. Ainda, pode-se averiguar quais protocolos de rede vem sofrendo maiores e menores modificações de seus campos, quando submetidos a ação destes dispositivos.

REFERÊNCIAS

DETAL, G.; HESMANS, B.; BONAVENTURE, O.; VANAUBEL, Y.; DONNET, B. **Revealing Middlebox Interference with Tracebox**. In: Proc. ACM SIGCOMM Conference, v. 18 n. 85 p. 1-8, 2012.

HONDA, M.; NISHIDA, Y.; RAICIU, C.; GREENHALGH, A.; HANDLEY, M.; TOKUDA, H. **Is It Still Possible to Extend TCP** In: Proc. ACM SIGCOMM Conference, v. 17 n. 13 p. 181-194, 2011.

JUSTINE, S.; HASAN, S.; SCOTT, C.; KRISHNAMURTHY, A.; RATNASANY, S.; SEKAR, V. **Making Middleboxes Someone Else's Problem: Network Processing as a Cloud Service**. University of Washington, UC Berkeley, Interl Labs. Proceeding of the ACM SIGCOMM 2012. Outubro, 2012.

MEDINA, A.; ALLMAN, M.; FLOYD, S. **Measuring Interactions Between Transport Protocols and Middleboxes**. ICSI Center for Internet Research. Proceedings of the ACM SIGCOMM 2004. 10-2004.

RFC 3234, **Middleboxes: Taxonomy and Issues**. Disponível em: http://tools.ietf.org/html/rfc3234.txt Acesso em: 03-07-2018.
SALTZER, J.; REED, D.; CLARK, D. **End-to-End Arguments in System Design**. ACMTransactions on Computer Systems, v. 2 n. 4, Novembro 1984.

SHERRY, J.; HASAN, S.; SCOTT, C.; KRISHNAMURTHY, A.; RATNASAMY, S.; SEKAR, V. **Making Middleboxes Someone Else's Problem: Network Processing as a Cloud Service** University of Washington, UC Berkeley, Intel Labs. Proceedings of the ACM SIGCOMM 2012. 10-2012

SILBERSACK, M. J. *Improving TCP/IP security through randomization without sacrificing interoperability*.2005. 230 f. Tese – University of Wisconsin, Milwaukee, 2005.