

Resenha Crítica do Artigo DDoS Defense by Offense

ACM SIGCOMM Computer Communication Review - Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications, Pages 303-314.

O artigo DDoS Defense by Offense [3] dos autores Michael Walfish, Mythili Vutukuru, Hari Balakrishnan, David Karger e Scott Shenker do MIT (Instituto de Tecnologia Massachusetts), apresenta a concepção, implementação, análise e avaliação experimental de *speak-up*, uma defesa contra ataques distribuídos de negação de serviço (DDoS) em que os atacantes paralisam um servidor enviando solicitações aparentemente legítimas que consomem o recursos computacionais (como ciclos CPU, disco, memória entre outros).

Logo nas primeiras páginas do artigo, os autores propõe um sistema de defesa para servidores contra nível de aplicação DDoS, onde os clientes (legítimos e não legítimos) são incentivados a enviar mais tráfego para um servidor atacado, esse conceito foi analisado ao decorrer do artigo.

Com alguns exemplos pretendem esclarecer o princípio eo funcionamento do *speak-up*, onde um servidor vitimado incentiva todos os clientes, a enviar automaticamente maiores volumes de tráfego, supondo que os atacantes já estão usando a maior parte de sua banda de upload por isso não pode reagir ao estímulo. Já os bons clientes, no entanto, tem largura de banda de upload de reposição e vai reagir ao estímulo com volumes drasticamente elevados de tráfego fim a fim.

No meio do artigo os autores com auxílio de calculos de desempenho demonstram a diferença entre sistemas tradicionais de defesa por Detecção e Bloqueio que utilizam o datagrama IP, vindo de roteadores(no núcleo da rede) ou dos atacantes para tentar cessar o ataque, porem em sistemas de Currency Trading (Moeda de Troca), esses sistemas utilizam a largura de banda como moeda de troca, criando assim um sistema de defesa, por exemplo um servidor atacado só aceita um serviço de cliente, somente depois que ele pagar em alguma moeda(recursos), um exemplo de moeda seria ciclos de CPU e/ou memória.

Com a premissa que os autores apresentam durante o artigo, sendo ela que sempre os maus clientes estaram consumindo toda sua taxa de upload espurios, eles demonstram dois modelos de sistemas de cobrança (Moeda de Troca). O primeiro utiliza um quebra-cabeça computacional como forma de pagamento, aquele que decifrar obtém serviço, e o segundo modelo onde uma espécie de

leilão e implementado quem conseguir ter a maior largura de banda ofertada pelo servidor obtém serviço.

Após os cálculos os autores demonstram em gráficos as condições de aplicabilidade sobre o *peak-up*, os mesmos afirmam que com diferentes exigências defensivas, o *peak-up* não é apropriado para todas elas, e para se defender com essa técnica tem que respeitar as seguintes condições:

1. C1 Ligação de banda do servidor/cliente adequada.
2. C2 Clientela não pré-definida.
3. C3 Clientela não humana.

Após sua aplicabilidade e resultados levantados os autores mostram como os maus clientes esgotar toda a sua largura de banda disponível em solicitações espúrias. Em contraste, os bons clientes, que gastam tempo substancial em repouso, utilizam provavelmente uma parcela pequena de sua largura de banda do servidor. A ideia-chave de *peak-up* é explorar essa diferença.

Os autores mostram alguns exemplos reais e verificações, encima do *peak-up*, os autores falam sobre as desvantagens de esquemas baseados em moedas, eles percebem que em primeiro lugar os clientes bons deve ter dinheiro (Largura de banda) suficiente e segundo que a moeda poder ser distribuída de forma desigual (por exemplo, alguns clientes têm uplinks mais rápidos do que outros). Outra crítica dos sistemas de moeda é que eles dão aos atacantes alguns serviços assim poderia ser mais fraco do que os esquemas como o profiling que buscam enquadrar atacantes, assim alguns botnets inteligentes pode imitar um bom cliente, tendo sucesso em enganar o sistema de detecção, e novamente obter serviços.

Embora sob as condições que o *peak-up* é aplicável, ainda podem levantar objeções, uma problemática seria que vários países, possuem conexões ISPs de baixa largura de banda, fazendo com que atacantes que tem um recurso melhor de banda se passe por clientes bons, outra objeção seria referente ao esquema de moeda, antes de um cliente legítimos ou não legítimos comprar uma parcela os mesmos estarão disputando recursos e consumindo serviços antes do pagamento, até que os clientes legítimos acabem expulsando os não legítimos, em função do alto nível de upload utilizados pelos atacantes, com o teorema apresentado neste artigo que sempre um atacante está com sua taxa de upload elevada, pode-se assim abrir brechas para sistemas de BootNets sofisticados que

tentam se passar por clientes normais, cada agente da rede de bootnet envia em uma taxa de largura de banda controlada, como citado no artigo [1].

Assim concluímos que o *speak-up*, seria funcional sendo utilizado em conjunto com outras técnicas existentes, algumas citadas em [2], sendo assim o melhor método para se defender de ataques DDoS e sempre utilizar um conjunto de verificações tanto na infraestrutura de rede quanto nas ferramentas de segurança utilizadas em camada de aplicação, assim combinando suas características visando criar uma resistência (escudo), contra ataques de negação de serviço.

**Rafael Gonçalves de Oliveira Viana
Ramon da Silva Varjão dos Santos
Graduandos de Sistemas de Informação.**

References

- [1] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita. Botnet in ddos attacks: Trends and challenges. *IEEE Communications Surveys Tutorials*, 17(4):2242–2270, Fourthquarter 2015.
- [2] S. R. Talpur and T. Kechadi. A survey on ddos attacks: Router-based threats and defense mechanism in real-world data centers. In *2016 Future Technologies Conference (FTC)*, pages 978–984, Dec 2016.
- [3] Michael Walfish, Mythili Vutukuru, Hari Balakrishnan, David Karger, and Scott Shenker. Ddos defense by offense. *SIGCOMM Comput. Commun. Rev.*, 36(4):303–314, August 2006.