

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 [Walfish et al. \(2006\)](#) dos autores Michael Walfish, Mythili Vutukuru, Hari Balakrishnan, David Karger e Scott Shenker do MIT (Instituto de Tecnologia Massachusetts), apresentam 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).

Nas duas primeiras páginas do artigo os autores propoem uma defesa para servidores contra nível de aplicação DDoS, o speak-up 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 o speak-up, 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. Bons clientes, no entanto, tem largura de banda de upload de reposição e vai reagir ao estímulo com volumes drasticamente mais elevados tráfego fim a fim.

Com auxilio de calculos de desempenho demostram a diferença entre sistemas tradicionais de defesa por Detecção e bloqueio que utilizam o IPs de roteadores ou dos atacantes para tentar cessar o ataque, em Currency Trading (Moeda de Troca), sistemas de defesa que utilizam a largura de banda como moeda de troca, um servidor atacado só aceita um serviço de cliente, somente depois que ele paga em alguma moeda. Exemplos ciclo de CPU ou memória (a comprovação do pagamento é a solução de um quebra-cabeça computacional)

Na página quatro os autores demostram os modelos e as condições de aplicabilidade sobre o speak-up, os mesmos afirmam que com diferentes exigências defensivas, o speak-up não e apropriado para todas elas, e para se defender com essa tecnica tem que respeitar as seguintes condições:

1. C1 Ligação de banda adequada.
2. C2 Ligação de banda cliente adequada.
3. C3 Clientela não pré-definida.
4. C4 Clientela não humana.

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

References

Walfish, M., Vutukuru, M., Balakrishnan, H., Karger, D., and Shenker, S. (2006). Ddos defense by offense. *SIGCOMM Comput. Commun. Rev.*, 36(4):303–314.