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 [1] dos autores Michael Walfish, Mythili Vutukuru, Hari Balakrishnan, David Karger e Scott Shenker do MIT (Instituto de Tecnologia Massachusetts), apresenta a concepção, implementação, analise 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 computacioais (como ciclios CPU, disco, memória entre outros).

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

Com alguns exemplos pretendem esclarecer o principio 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 estimolo com volumes drasticamente elevados de tráfego fim a fim.

No corpo do artigo os autores com auxílio de calculos de desempenho demostram 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 premisa que os autores apresentão durante o artigo, sendo ela que sempre os maus clientes estaram cosumindo toda sua taxa de upload espurios, eles demostram dois modelos de sistemas de cobrança (Moeda de Troca). O primeiro utiliza um quebra-cabeça computacional como forma de pagamento, aquele que dicifrar obtém serviço, e o segundo modelo onde uma espécie de

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

Após os calculos os autores demostram em gráficos as condições de aplicabilidade sobre o speak-up, os mesmos afirmam que com diferentes, exigências defensivas, o speak-up não é apropriado para todas elas, e para se defender com essa tecnica tem que respeitar as sequintes 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 speak-up é explorar essa diferença.

Após alguns exemplos reais e verificações, encima do speak-up, os autores falam sobre as desvagatens 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 distribuida de forma desigual(por exemlo, alguns clientes têm uplinks mais rápidos do que outros). Outra cirtica dos sistemas de moeda é que eles dão aos atacanes alguns serviço assim poderia ser mais fraco do que os esquemas como o profiling que buscam enquadrar atacantes, porem alguns botnets inteligentes pode imitar um bom cliente, tendo sucesso em enganar o sistema de detecção, e novamente obter serviços.

Após uma análise verificamos que mesmo sob as condições que o speak-up e apliável, ainda podem levantar objeções, um exemplo de vários países onde 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 légitimos ou não legitimos comprar uma parcela, o mesmo estara consumindo serviço antes do pagamento, até que os clientes legitimos acabem os expulsando os não legitimos, em função do auto nível de upload utilizados pelos atacantes, com o teorema apresentado que sempre um atacante esta com sua taxa de upload sempre em uso, sendo assim abrindo brexas para sistemas de BootNet avançados como citado no artigo.

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

References

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