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, 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).

Nas duas primeiras páginas do artigo os autores propoem uma defesa para servidores contra nivel de aplicação DDoS, o speak-up 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

Os autores apresentão um sistema de defesa denominado 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. Bons clientes, no entanto, tem largura de banda de upload de reposição e vai reagir ao estimolo com volumes drasticamente mais elevados de tráfego fim a fim.

No corpo do artigo os autores 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 sistemas de 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)

Após os calculos 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 sequintes 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.

Os autores assumem que maus clientes esgotar toda a sua largura de banda disponível em solicitações espúrias. Em contraste, os bons clientes, que gastam tempo substancial de não estam considerando ataques de link. Eles assumem que os links de acesso do repouso, utilizam provavelmente uma única parcela pequena de sua largura de banda do servidor. A ideia-chave de speak-up é explorar essa diferença.

Com a premisa que os autores apresentão durante o artigo, que sempre os maus clientes estaram cosumindo sua taxa de upload, eles demostram dois metodos de sistemas de cobrança (Moeda de Troca), o primeiro utiliza um um quebra-cabeça computacional, onde quem tiver melhor o dezempenho obtém serviço, e o segundo onde uma especie de leilão e implementado quem conseguir ter a maior largura de banda de uplod obtem serviço.

Apos alguns exemplos de taxometria e verificações encima do speak-up e dos dois modelos, 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.

Mesmo sob as condições que o speak-up e apliável, ainda podem levantar objeções como e o exemplo de alguns clientes de paises 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 demostrado e que o esquema de moeda ainda fornece serviço no começo para clientes maus e bons até que os clientes legitimos acabem os expulsando pelo auto nível de uplod utilizado pelos os mesmos.

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.