Projeto da disciplina de Gerência de Redes

Cinara, Fernando Cezar, Fernando Gielow, Nadine

1 Proposta inicial

Um ataque DDoS consiste, genericamente, da tentativa de tornar indisponíveis os recursos oferecidos por alguma entidade [ref]. Na internet, este tipo de ataque tem se tornado cada vez mais comum, visando *websites* de grandes empresas. Recentemente, houveram ataques aos *websites* da Amazon, do Paypal e da bandeira de cartões de crédito Visa [ref], que acarretaram em grandes prejuízos à estas empresas.

Diversas dificuldades são encontradas ao se tentar mitigar os efeitos destes ataques. Em servidores de hospedagem tradicionais, os recursos são limitados e, assim, quando o número de requisições ultrapassa um patamar máximo, não há como continuar respondendo efetivamente as requisições. Em abordagens mais avançadas, como é o caso de hospedagem em *clouds* [ref], tais ataques acarretam na alocação de uma quantidade imensa de recursos, a afim de tratar todas as requisições que chegam ao servidor, independente de serem clientes legítimos ou atacantes. Embora esta abordagem consiga tratar ataques DDoS até dados limites, é uma abordagem custosa, pois todos os recursos utilizados nesta tentativa de mitigação serão cobrados [2].

O trabalho [1] tenta tratar estes ataques através da criação de uma nova instância da aplicação. Uma vez que um ataque DDoS é detectado, ele tenta detectar os atacantes através de um PING - caso o possível atacante não responda o PING, ele é considerado como um atacante. Desta maneira, apenas os clientes que responderem o PING serão redirecionados para a nova instância da aplicação. Entretanto, tal abordagem depende da premissa que atacantes jamais responderão a PINGs e que clientes genuínos sempre responderão, o que nem sempre condiz com a realidade.

O objetivo deste trabalho é apresentar uma proposta de um esquema de mitigação de ataques DDoS para aplicações hospedadas em *clouds*. Este esquema será composto pelos seguintes módulos: (i) detecção de comportamento similar a ataques DDoS; (ii) redirecionador de tráfego; (iii) gerenciador de *blacklist*. O módulo (i) observará proativamente o padrão de tráfego de entrada, visando detectar um ataque DDoS. Caso um ataque seja detectado, será criada uma nova instância da aplicação em uma outra instância de servidor *cloud*, consequentemente com um endereço IP diferente. Desta forma, o módulo (ii) será responsável por tratar todo o tráfego de entrada, informando o endereço do novo servidor, e inserindo o IP origem da requisição à uma *blacklist*, através do módulo (iii). Desta maneira, o atacante não afetará a nova instância da aplicação, pois ele não interpretará as respostas que informam o IP da nova instância.

Estamos estudando a implementação de tal mecanismo, sendo que ele possivelmente será implementado e testado nos serviços *cloud* disponibilizados pela Amazon [ref]. Serão apresentados resultados que demonstram a eficiência do mecanismo em tratar ataques DDoS de pequenos portes.

Referências

[1] A Bakshi and B Yogesh. Securing cloud from ddos attacks using intrusion detection system in virtual machine. *Communication Software and Networks, 2010. ICCSN '10. Second International Conference on*, pages 260 – 264, 2010.

[2] SH Khor and Akihiro Nakao. spow: On-demand cloud-based eddos mitigation mechanism. *Fifth Workshop on Hot Topics in System Dependability*, Jan 2009.