Nome: Davi Jorge Leite Santos - Matricula: 614017

MÉTRICAS PARA A DETECÇÃO DE ATAQUES DDOS

Nícolas Rocha e Silva* e Ronaldo Moreira Salles

Sobre o DDoS

“A Internet atual é vulnerável a ataques de negação de serviço distribuídos (DDoS). Ataques desse tipo têm como objetivo fazer com que uma rede ou serviço oferecido por ela fique inacessível a usuários legítimos, o que geralmente é alcançado quando um atacante envia pacotes a uma taxa maior do que a vítima pode processar (Castelúcio, 2009). Este é um dos diversos tipos de ataque que se aproveita das falhas de programação da pilha TCP/IP, que possibilita ao invasor explorar a enorme assimetria de recursos que existe entre a Internet e a vítima” PAG 2

“Na maioria das vezes, o intuito desses ataques não é realizar uma invasão, mas impedir que usuários legítimos utilizem um determinado serviço de um computador ou rede.” PAG 6

Metodos de detecção

“De maneira geral, combater ataques DDoS requer a execução de 3 etapas: (i) identificar a ocorrência de um ataque; (ii) rastrear a origem dos pacotes maliciosos; e (iii) acionar contramedidas que contribuam para a mitigação ou eliminação dos danos causados pelo ataque, tais como filtragem e bloqueio de pacotes (Castelucio, 2009)” PAG 9

“Atualmente, os métodos de detecção de ataques DDoS podem ser agrupadas em duas classes principais, cujas métricas se baseiam ou na assinatura de ataques ou na presença de anomalias no tráfego (Xiang, 2011)” PAG 9

Detecção via assinatura

“Na primeira classe, deve-se conhecer um conjunto de assinaturas, tais como padrões ou conjuntos de caracteres, presentes em pacotes maliciosos. Neste caso, além de ser necessário conhecer a assinatura do ataque, o custo computacional para identificar os ataques é bem elevado, e o seu emprego em tráfegos backbone torna-se inviável, a não ser que sejam empregados métodos estatísticos para reduzir o número de pacotes inspecionados.” PAG 9

Detecção via anomalias

“Nas métricas baseadas em anomalias, o comportamento do tráfego de rede em condições normais serve de base para a determinação de limites que são ultrapassados na presença de ataques. Nesse caso, a principal vantagem reside na capacidade de detectar ataques desconhecidos. Podem ser baseados em limiares fixos (threshold) ou limites que são atualizados em tempo de execução a partir de estatísticas geradas durante o período em que ataques não são detectados.” PAG 9

Entropia

“Em trabalhos anteriores percebeu-se que os valores de Entropia podem representar a dispersão de valores presentes numa dada distribuição, e apresentam boa sensibilidade na identificação de ataques DDoS, quando a entropia dos endereços de origem e destino observados num determinado intervalo sofrem alterações expressivas em seus valores” PAG 10

Divergencia

“Quando ocorre um ataque DDoS, espera-se que o número de pacotes destinados a um determinado endereço cresça repentinamente, alterando significativamente sua distribuição de probabilidade.”PAG 10