Framework para detecção de ataques DDoS

Autor Bruno Riccelli dos Santos Silva [1,2]

[1]Universidade Federal do Ceará

[2]Laboratório de Engenharia de Sistemas de Computação - LESC

25 de agosto de 2017

Sumário

Introdução
Motivação

Ataques DDoS

Tentativa de tornar os recursos de um sistema indisponíveis aos utilizadores.

Tipos

- Ataque de vulnerabilidade.
- Inundação na largura de banda.
- Inundação na conexão.

Exemplos

- SIDDOS, UDP Flood, Smurf ...

Introdução
Motivação

Ataques DDoS

Tentativa de tornar os recursos de um sistema indisponíveis aos utilizadores.

Tipos

- Ataque de vulnerabilidade.
- Inundação na largura de banda.
- Inundação na conexão.

Exemplos

- SIDDOS, UDP Flood, Smurf ...

Introdução
Motivação

Ataques DDoS

Tentativa de tornar os recursos de um sistema indisponíveis aos utilizadores.

Tipos

- Ataque de vulnerabilidade.
- Inundação na largura de banda.
- Inundação na conexão.

Exemplos

- SIDDOS, UDP Flood, Smurf ...

Objetivos

- Desenvolver um framework para detecção de ataques DDoS baseado em uma medida de correlação encontrada na literatura;
- Filtrar e selecionar conjuntos de dados para análise e realizar medições estatísticas;
- Implementar em software o framework proposto;
- Avaliar o framework em termos de taxa de acerto com um caso real de ataque.

Objetivos

- Desenvolver um framework para detecção de ataques DDoS baseado em uma medida de correlação encontrada na literatura;
- Filtrar e selecionar conjuntos de dados para análise e realizar medições estatísticas;
- Implementar em software o framework proposto;
- Avaliar o framework em termos de taxa de acerto com um caso real de ataque.

Objetivos

- Desenvolver um framework para detecção de ataques DDoS baseado em uma medida de correlação encontrada na literatura;
- Filtrar e selecionar conjuntos de dados para análise e realizar medições estatísticas;
- Implementar em software o framework proposto;
- Avaliar o framework em termos de taxa de acerto com um caso real de ataque.

Objetivos

- Desenvolver um framework para detecção de ataques DDoS baseado em uma medida de correlação encontrada na literatura;
- Filtrar e selecionar conjuntos de dados para análise e realizar medições estatísticas;
- Implementar em software o framework proposto;
- Avaliar o framework em termos de taxa de acerto com um caso real de ataque.

Framework de Detecção

Componentes do framework

- Pré - processamento.
- Módulo de detecção em hardware.
- Gerenciador de segurança.

Medida de correlação NaHiD

$$NaHiD(X,Y) = 1 - \frac{1}{n}\sum_{i=1}^{n}\frac{|X(i) - Y(i)|}{||meanX - SDX| - X(i)| + ||meanY - SDY| - Y(i)|} \quad (1)$$

onde X e Y são objetos de tráfego e n é a dimensão deles.

Sumário

Framework de Detecção

Métricas utilizadas

- Entropia de IPs origem;
- Variação de IPs origem;
- Packet Rate

Framework de Detecção

Métricas utilizadas

- Entropia de IPs origem;
- Variação de IPs origem;
- Packet Rate

Framework de Detecção

Métricas utilizadas

- Entropia de IPs origem;
- Variação de IPs origem;
- Packet Rate

Entropia de IPs origem

$$H(X) = -\sum_{i}^{n} p(x_i) log2 p(x_i); \quad (2)$$

Onde X é uma variável aleatória e n é o número total de valores possíveis para IPs origem.

Variação de IPs origem

Variação de IPs origem

$$V(x) = \frac{\delta}{N} \tag{3}$$

onde δ é o número de mudanças de IPs origem em uma dada janela de tempo e N é o número de IPs origem nessa janela.

Tabela de validação

Tabela: Objetos de tráfego de rede

Objeto	F1	F2	F3
O_1	365	2.52	0.9533
O_2	379	2.55	0.9709
O_3	345574	12.98	0.94
O_4	166453	12.7	0.9866
O_5	357663	12.79	0.94

Onde cada objeto representa uma instância de tráfego e F1, F2 e F3 representam, o Packet Rate, Variação de IPs origem e Entropia de IPs origem, respectivamente.

Tabela de validação

Tabela: Objetos de tráfego de rede

Objeto	NaHiD
O_1, O_2	0.9917
O_2, O_3	0.5600
O_3, O_1	0.5600
O_3, O_5	0.9924
O_5, O_1	0.5600

Onde O_5 e O_3 são instâncias de tráfego normais e O_1, O_2 e O_4 são padrões de ataques.

Sumário

Dataset avaliado pelo framework

Número da variável	Descrição
1	SRC ADD
2	DES ADD
3	PKT ID
4	FROM NODE
5	TO NODE
6	PKT TYPE
7	PKT SIZE
8	FLAGS
9	FID
10	SEQ NUMBER
11	NUMBER OF PKT
12	NUMBER OF BYTE
13	NODE NAME FROM
14	NODE NAME TO
15	PKT IN
16	PKTOUT
17	PKTR
18	PKT DELAY NODE
19	PKTRATE
20	BYTE RATE
21	PKT AVG SIZE
22	UTILIZATION
23	PKT DELAY
24	PKT SEND TIME
25	PKT RESEVED TIME
26	FIRST PKT SENT
27	LAST PKT RESEVED

Dataset avaliado pelo framework

Considerações

- Filtragem por IP destino.
- Janela contendo 1 segundo de tráfego.
- Média do Packet Rate.
- Variação de IPs origem como mudança sem "memória".
- Escolha do limiar de correlação.
- Tráfego normal "estático".

Sumário

Próximos passos

- Abrir e tratar datasets MIT - DARPA e outros.
- Terminar gerenciador de segurança.
- Criar arquivo para comunicação com FPGA **?**.
- Validar os resultados.