# Cyber Security Flood Attacks and Risk Assessment for Internet of Things (IoT) Distributed Systems

Alunos:

- Artur Beerends Yamada
- Bruno Ribeiro Basílio
- Pedro Henrique Guimarães Gomes

# Introdução

- Sistemas distribuídos:
  - Potenciais alvos
  - Ferramentas de ataques
- *Distributed Denial of Service* (DDoS)
  - Variação do tipo de ataque *Denial of Service* (DoS) que usa sistemas distribuidos
  - Visa  exaurir a capacidade do sistema vítima
- *Botnets*
  - Grupo de computadores conectados à internet controlados pelo agressor que coordena o ataque
  - Máquinas de terceiros infectadas por *malware* que cede controle ao agressor

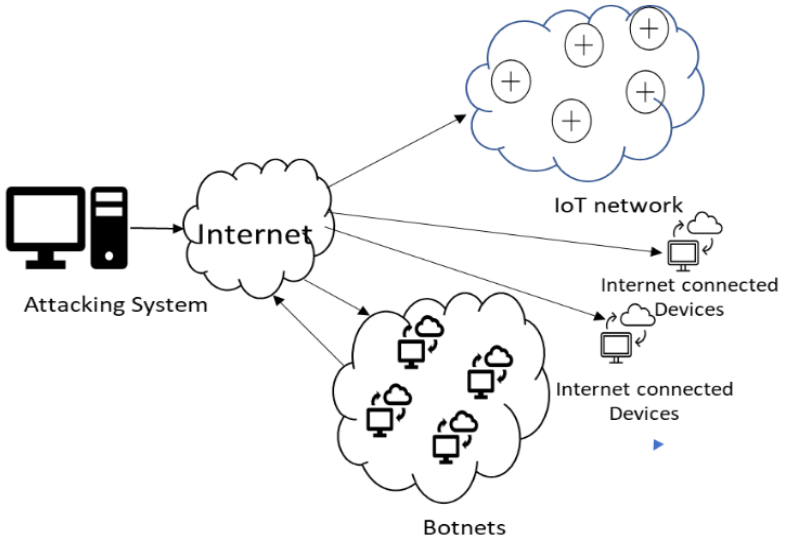
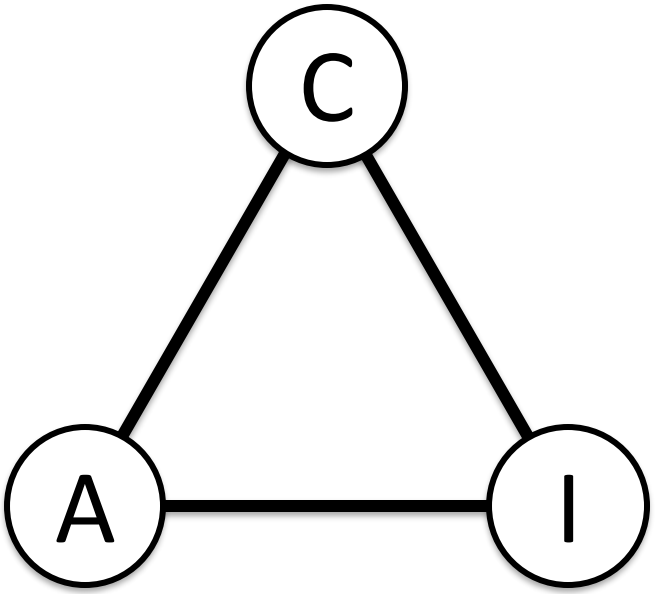



Figure 1: Cybersecurity risks for IoT networks

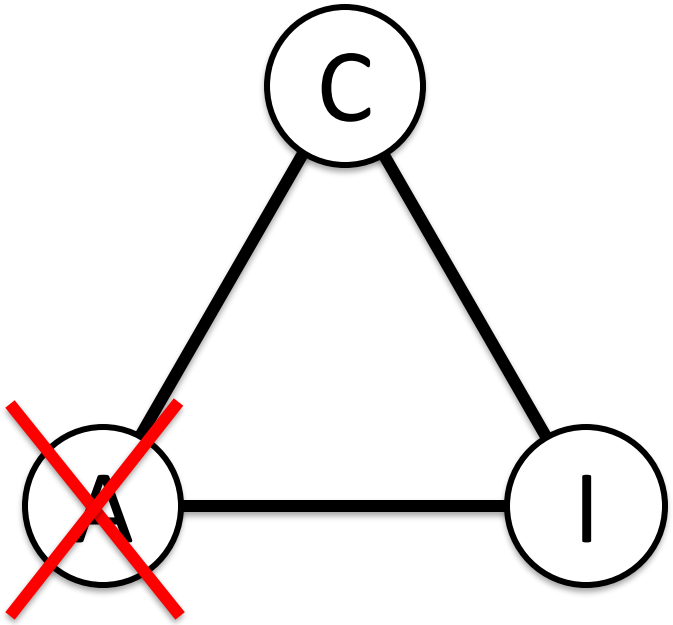
# Ataques DDoS Flood

- Tríade da Segurança CIA
  - Confidencialidade
  - Integridade
  - Disponibilidade (*Availability*)
- Ataques DDoS comprometem a disponibilidade dos sistemas sob ataque, previnindo que tratem de solicitações legítimas



# Ataques DDoS Flood

- Tríade da Segurança CIA
  - Confidencialidade
  - Integridade
  - Disponibilidade (*Availability*)
- Ataques DDoS comprometem a disponibilidade dos sistemas sob ataque, previnindo que tratem de solicitações legítimas



# Ataque ICMP Ping

- Ferramenta de diagnóstico de rede
  - Acessibilidade do sistema
  - Tamanhos de pacote
  - Disponibilidade do sistema
  - Integridade do canal
- RFC-792 exige que *Echo Requests* sejam respondidas com um *Echo Reply*

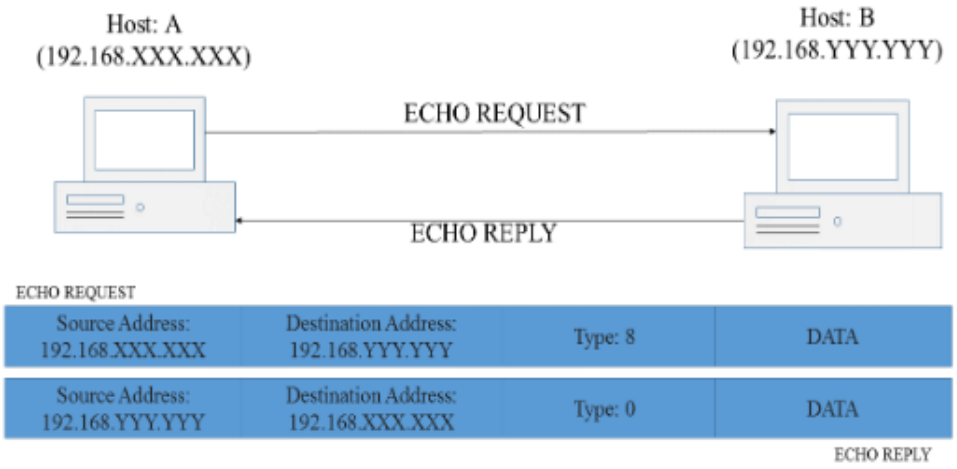



Figure 2: ICMP Echo Request/Reply Message Format

# Ataque TCP-SYN

- Mensagem de início do estabelecimento de uma conexão TCP
  - *three-way handshake*
- Além de prover resposta SYN-ACK, o sistema recebendo a mensagem TCP-SYN também é requirido pela RFC-793 a esperar a confirmação final com a conexão aberta
  - Os agressores nunca fornecem essa resposta, acumulando conexões desperdiçadas esperando *timeout*

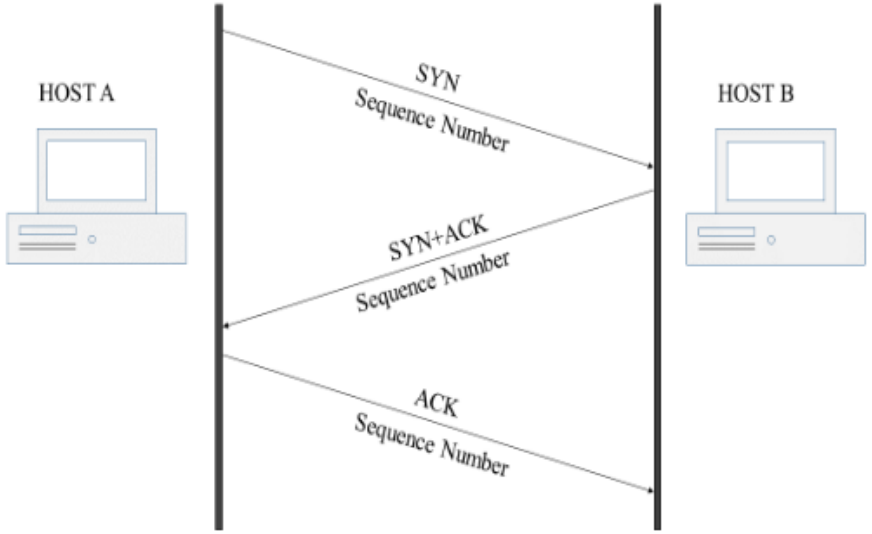



Figure 3: TCP Three-Way Handshake

# Propósito da Análise Experimental

• Avaliar o impacto de ataques DDoS por inundação em um sistema conectado.

• Comparar Ping Flood e TCP-SYN Flood quanto a

- Taxa de transações HTTP

- Uso de CPU e memória

• Determinar níveis de risco para cada tipo de tráfego.

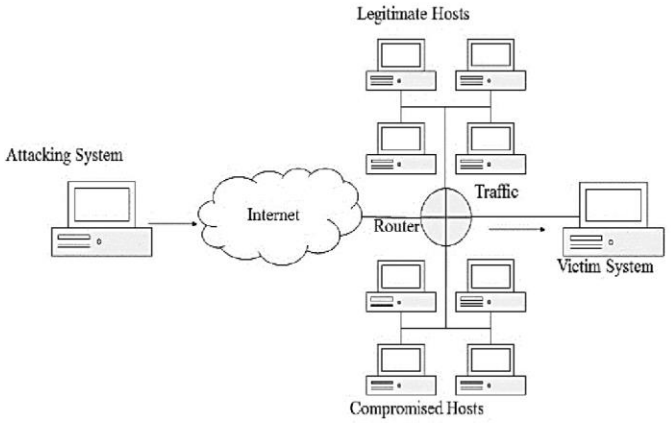



Figure 4: Experimental Setup [9]

# Ambiente e Parâmetros Utilizados

- • Experimento conduzido em rede fechada e controlada.
- • Sistema vítima: iMac (Windows 10 Pro, Intel i5 2.5 GHz, 8 GB RAM, 1 Gbps).
- • Botnet simulada: até 16 milhões de IPs (Class A).
- • Tráfego legítimo: 3000 transações HTTP/s (site hospedado localmente).
- • Ataques testados:
- - Escala baixa → até 20% da largura de banda.
- - Escala alta → até 100% (1 Gbps).

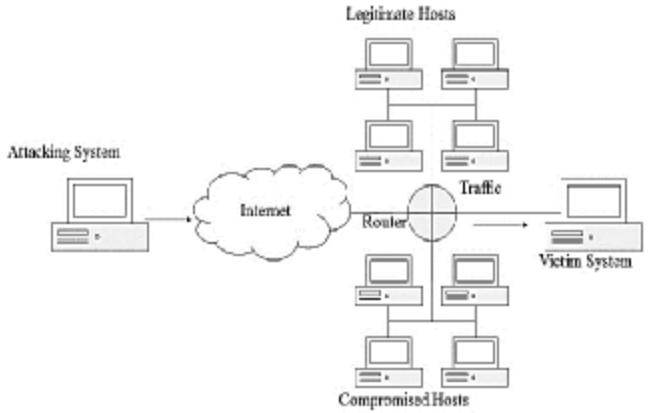


Figure 4: Experimental Setup [9]

# Efeitos dos Ataques nas Transações HTTP

- Ping Flood:

  - Ataques leves (< 20%) quase sem efeito.

  - Ataques fortes (> 70%) → bloqueio total de conexões HTTP.

- TCP-SYN Flood:

  - Mesmo com carga leve (< 20%) → queda total de transações.

- O processador foi o principal gargalo; a memória permaneceu estável.

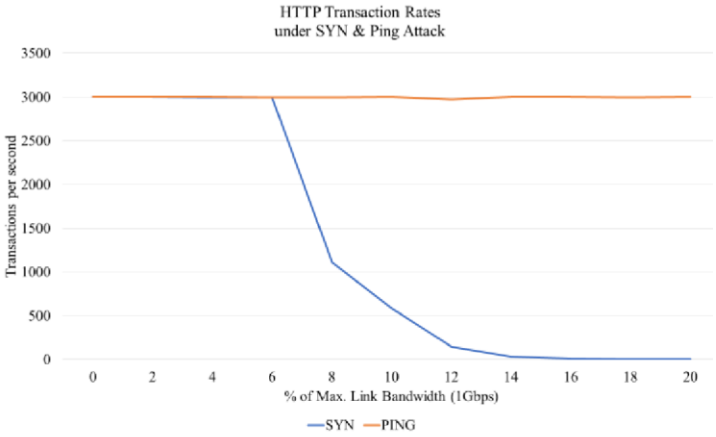



Figure 5: HTTP Transaction Rates measured under Ping and TCP-SYN flood attacks of small-scale load < 20% of link speed.

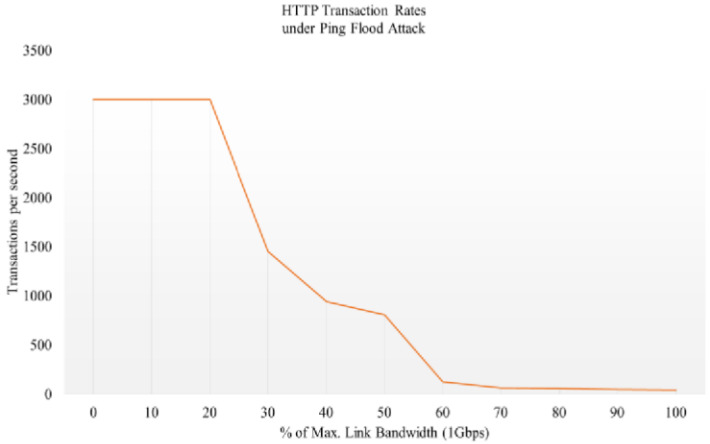



Figure 6: HTTP Transaction Rates measured under Ping flood attack with large-scale load up to 100% of link speed.

# Interpretação e Perfil de Risco

• Ataques diferem em intensidade de impacto:

- TCP-SYN Flood → alta exaustão da CPU, risco elevado.

- Ping Flood → afeta apenas sob carga intensa, risco moderado.

• Criação de perfil de risco baseada em comportamento medido.

• Fundamenta sistemas de defesa automáticos que detectam padrões de ataque.

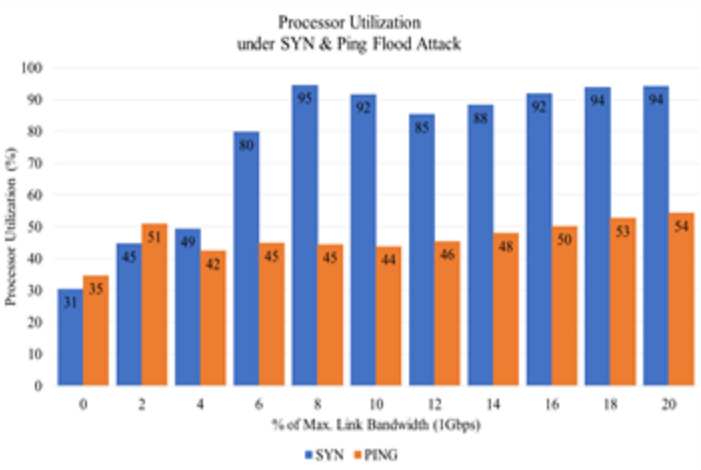



Figure 7: Total processor utilization for small-scale low intensity attacks under Ping floods and TCP-SYN floods.

# Conclusões: Anatomia do Risco

- **TCP-SYN → Eficiência**
  - Causa negação de serviço completa com baixo volume de tráfego (apenas 14% da capacidade da rede)
  - Prova que o volume do ataque não é a única métrica de perigo.

- **Ping Flood → Força Bruta**
  - Exige a saturação quase total da largura de banda (>70%) para ter o mesmo impacto.
  - Ineficaz em baixas intensidades.

- **Verdadeiro Gargalo → CPU**
  - A causa da falha foi a **exaustão do processador**, não da memória ou da rede.
  - O ataque TCP-SYN força o sistema a gerenciar milhares de conexões semiabertas.

# Conclusões: O Perfil de Risco

- **TCP-SYN -> Alto Risco:**
  - Um pequeno aumento neste tipo de tráfego é um indicador crítico.

- **Ping Flood -> Baixo Risco(em baixa intensidade):**
  - O sistema demonstra resiliência
  - Resposta menos agressiva (monitoramento ou alertas)

Table 1: Risk assessment for different traffic flows

| Traffic flows | Memory Intensive | Processor Intensive | Risk Assessment |
|---|---|---|---|
| Ping traffic flows | No, Memory consumption not impacted | Yes, low processor exhaustion at low traffic (< 20% of link speed) | Low risk |
| TCP SYN traffic flows | No, Memory consumption not impacted | Yes, high processor exhaustion at low traffic | High risk |

A defesa deve evoluir de uma análise baseada em **Volume** para uma análise baseada em **Impacto e Risco**

# Conclusões: IA com Consciência de Risco

- **Limitações dos sistemas Atuais:**
  - Baseiam-se apenas em volumes ou assinaturas
  - Geram muitos falsos positivos
  - Não conseguem detectar ataques novos (zero-day)
- **IA com Perfil de Risco:**
  - Sistema aprende a **Priorizar Ameaças**
- **Resultado:**
  - Defesas mais rápidas e precisas
  - Menos interrupções desnecessárias

Obrigado pela atenção