Introdução a Honeypots e Honeynets

Prof. Dr.-Ing. João Paulo C. Lustosa da Costa
Universidade de Brasília (UnB)
Departamento de Egenharia Elétrica (ENE)
Laboratório de Processamento de Sinais em Arranjos
Laboratório de Tecnologias da Tomada de Decisão (LATITUDE.UnB)

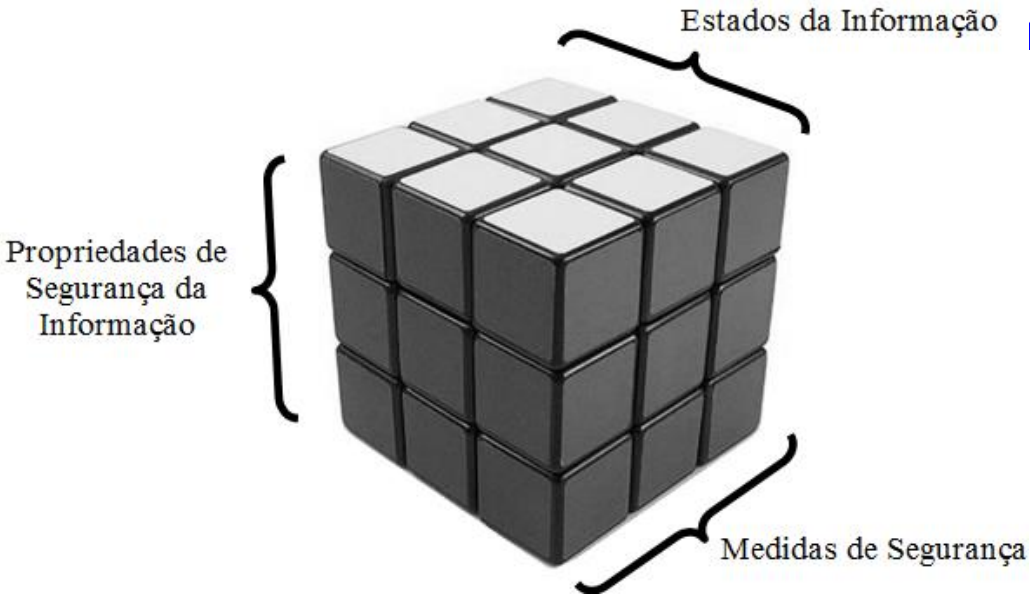
Roteiro

- Motivação
- Exemplos de Ataques: synflood, fraggle e portscan
- Modelagem dos Dados
- Testes Controlados
- Testes Não-Controlados com Honeypots
- Extensão para Honeynets

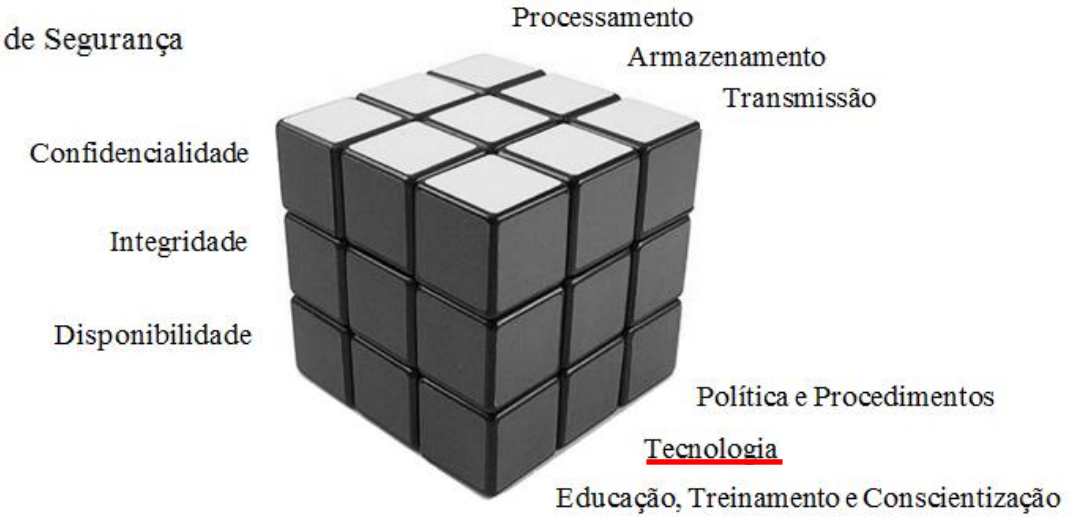
Roteiro

- Motivação
- Exemplos de Ataques: synflood, fraggle e portscan
- Modelagem dos Dados
- Testes Controlados
- Testes Não-Controlados com Honeypots
- Extensão para Honeynets

Motivação (1)



- Cenário atual
  - ⇒ Importância da informação
    - Big Data
  - ⇒ Vulnerabilidades nos pilares de segurança



Fonte: *National Training Standard for Information Systems Security Professionals* – NSTISSI 4011

Motivação (2)

- Métodos clássicos de mineração de dados [1]:
  ⇒ uso de grandes bases de dados.
- Análise regular de arquivos para identificação de padrões [2]:
  ⇒ necessidade de conhecimento prévio de dados.
- Uso de PCA para detecção de ataques [3]:
  ⇒ intervenção humana na análise de resultados.

[1] W. He, G. Hu, X. Yao, G. Kan, H. Wang, and H. Xiang, "Applying multiple time series data mining to large-scale network traffic analysis," in IEEE Conference on Cybernetics and Intelligent Systems, pp. 394-399, September 2008.

A. Ghourabi, T. Abbes, and A. Bouhoula, "Data analyzer based on data mining for honeypot router," in International Conference on Computer Systems and Applications (AICCSA), pp. 1-6, May 2010.

[2] F. Raynal, Y. Berthier, P. Biondi, and D. Kaminsky, "Honeypot forensics," in Proceedings from the Fifth Annual IEEE SMC on Information Assurance Workshop, pp. 22-29, June 2004.

[3] S. Almotairi, A. Clark, G. Mohay, and J. Zimmermann, "A Technique for Detecting New Attacks in Low-Interaction Honeypot Traffic," in Fourth International Conference on Internet Monitoring and Protection, pp. 7-13, May 2009.

Motivação (3)

- Técnicas de detecção cega e automática de tráfego malicioso em *honeypots* [4] [5], em redes de honeypots [6] e em quaisquer dispositivos [7]
- Esquemas de Seleção de Ordem do Modelo (MOS):

  $\Rightarrow$ detecção de componentes altamente correlacionadas em tráfego de rede
- Detecção de atividades maliciosas sem informação prévia ou assinatura de ataque [4, 5, 6, 7]

[4] B. M. David, J. P. C. L. da Costa, A. C. A. Nascimento, M. D. Holtz, D. Amaral, and R. T. Sousa Júnior. "Blind automatic malicious activity detection in honeypot data," pp. 02-04, in International Conference on Forensic Computer Science (ICoFCS), 2011

[5] J. P. C. L. da Costa, E. P. de Freitas, B. M. David, D. Amaral, and R. T. de Sousa Jr., "Improved Blind Automatic Malicious Activity Detection in Honeypot Data," The International Conference on Forensic Computer Science (ICoFCS) 2012, Brasília, Brazil, best paper award

[6] J. P. C. L. da Costa, E. P. de Freitas, A. M. R. Serrano, and R. T. de Sousa Jr. "Improved Parallel Approach to PCA Based Malicious Activity Detection in Distributed Honeypot Data," International Journal of Forensic Computer Science (IJoFCS), 2012

[7] D. F. Tenório, J. P. C. L. da Costa, and R. T. de Sousa Jr., "Greatest Eigenvalue Time Vector Approach for Blind Detection of Malicious Traffic," The International Conference on Forensic Computer Science (ICoFCS) 2013, Brasília, Brazil, best paper award

Motivação (4)

- Em caso de detecção de ataque, identificação no tempo (em milissegundos) e espaço (porta) [8]
- Proteção de dados confidenciais quando o cliente móvel não está conectado à nuvem corporativa [9]

[8] T. P. B. Vieira, D. F. Tenorio, J. P. C. L. da Costa, E. P. de Freitas, G. Del Galdo, and R. T. de Sousa Junior, "Model Order Selection and Eigen Similarity based Framework for Detection and Identication of Network Attacks," Journal of Networking and Computer Applications (JNCA), Vol 90, Jul 2017, Pages 26–41

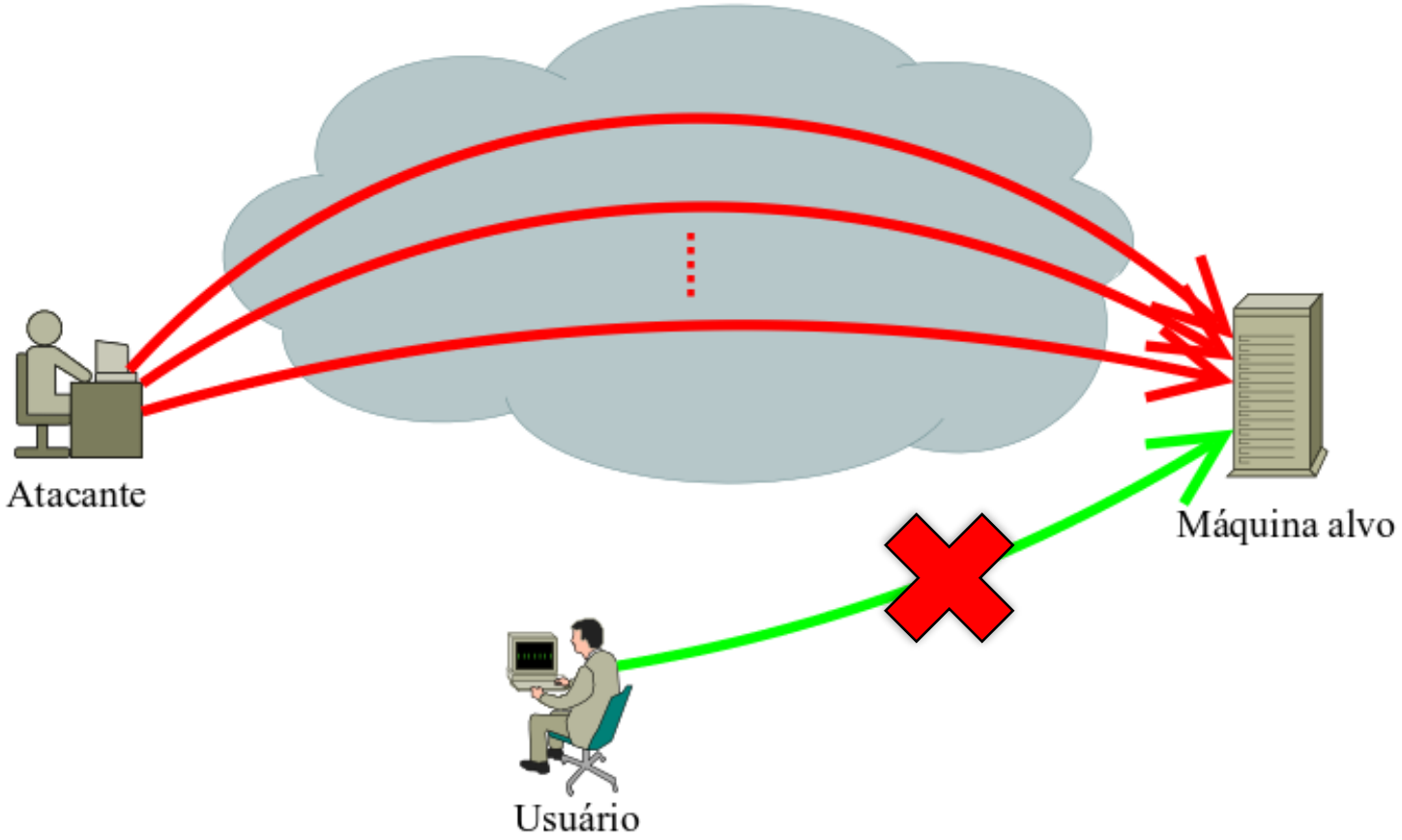
[9] T. Galibus, T. P. B. Vieira, E. P. de Freitas, R. Albuquerque, J. P. C. L. da Costa, R. T. de Sousa Jr, V. Krasnoproshin, A. Zaleski, H. Vissia, and G. del Galdo, "Offline Mode for Corporate Mobile Client Security Architecture", Mobile Networks and Applications, Springer, Mar 2017, Pages 1-17

Roteiro

- Motivação
- Exemplos de Ataques: synflood, fraggle e portscan
- Modelagem dos Dados
- Testes Controlados
- Testes Não-Controlados com Honeypots
- Extensão para Honeynets

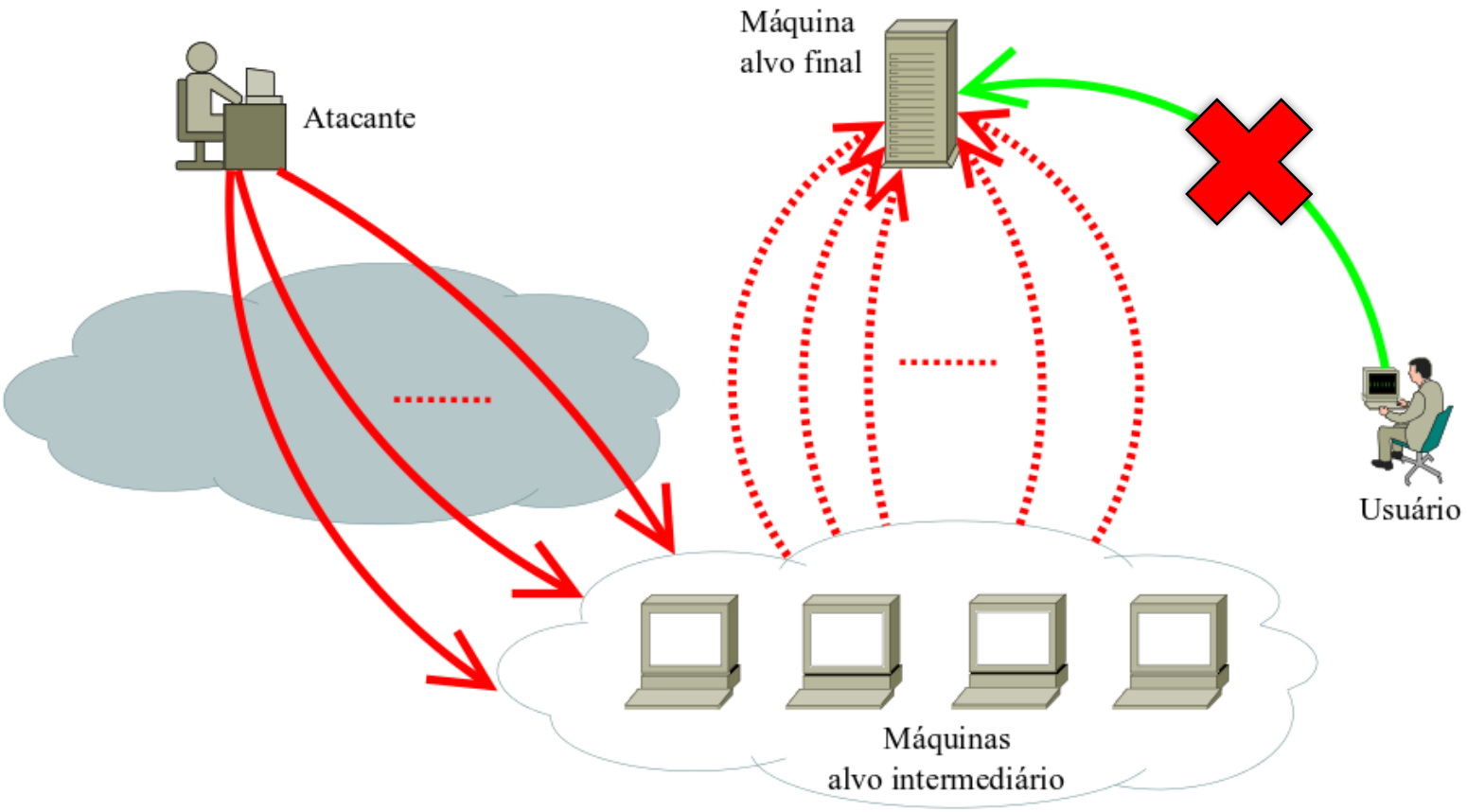
Exemplos de Ataques (1)

ATAQUE DE *SYNFLOOD*

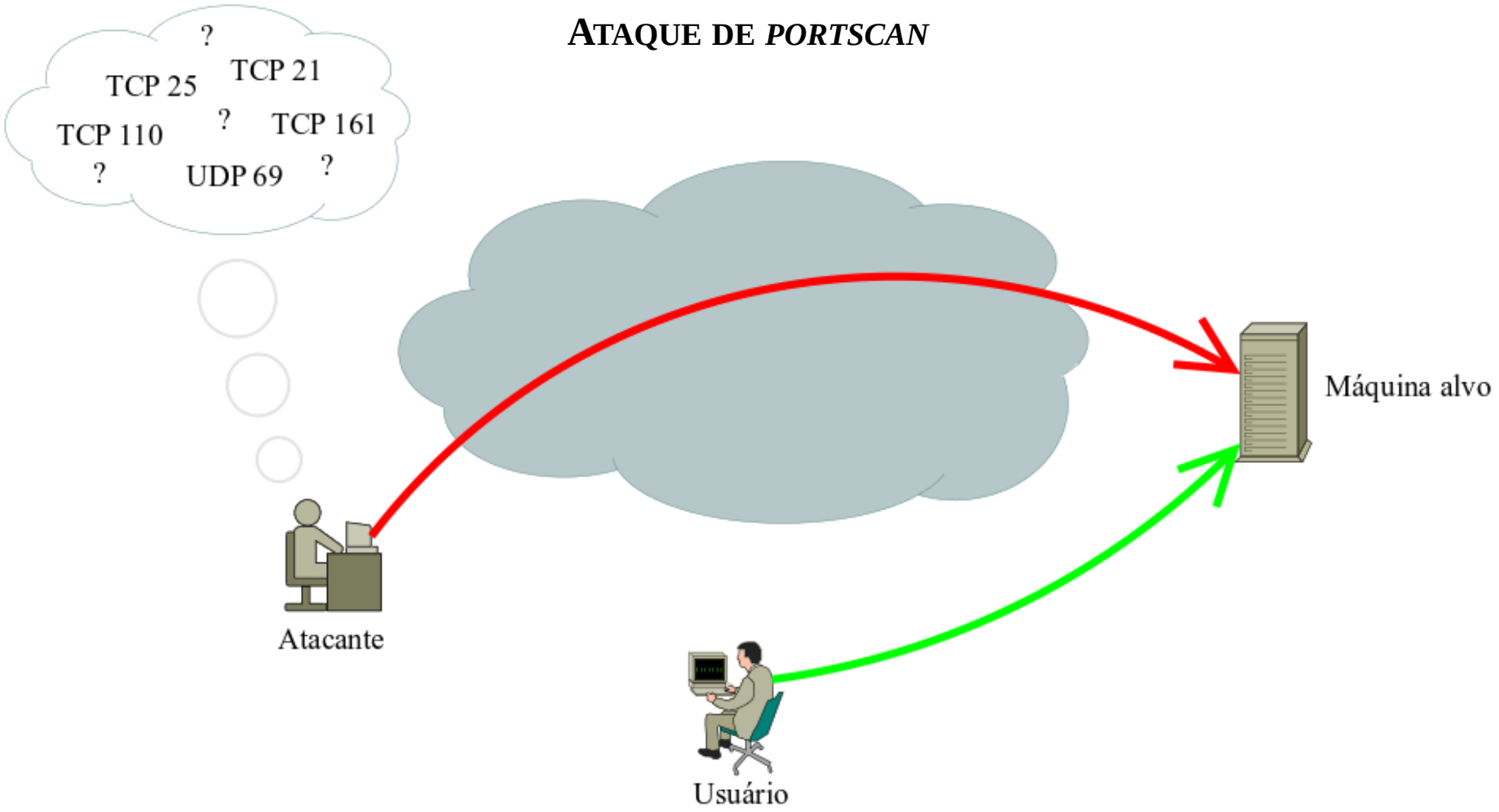


Exemplos de Ataques (2)

ATAQUE DE *FRAGGLE*



Exemplos de Ataques (3)



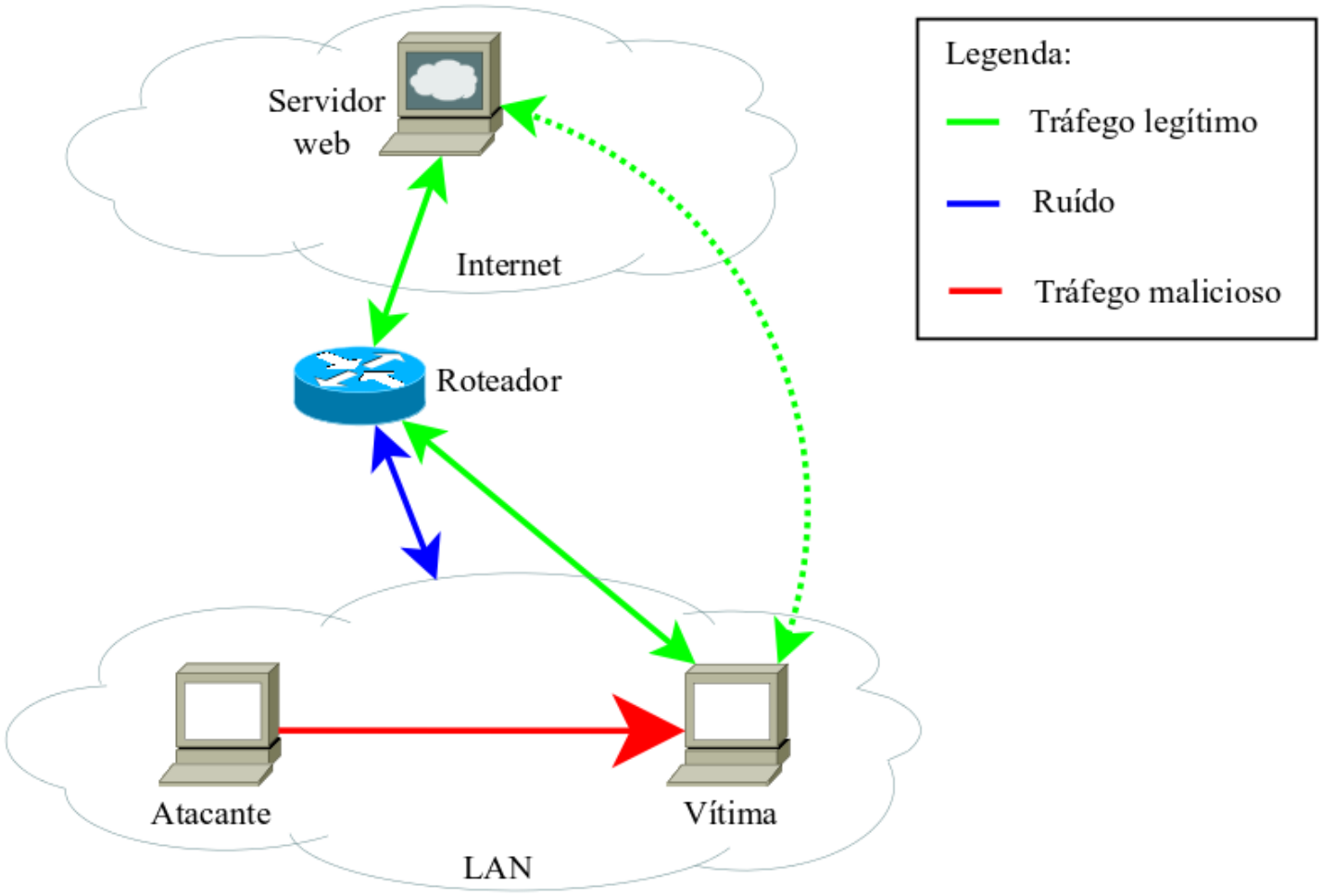
Roteiro

- Motivação
- Exemplos de Ataques: synflood, fraggle e portscan
- Modelagem dos Dados
- Testes Controlados
- Testes Não-Controlados com Honeypots
- Extensão para Honeynets

Modelagem dos Dados (1)

Modelo *Open System Interconnection* – OSI, criado pela *International Organization for Standardization* – ISO.

Modelagem dos Dados (2)



Modelagem dos Dados (3)

- Modelo de pré-processamento dos dados
  - ⇒ Os dados originais são divididos em *n* slots de tempo

```
2008-06-04-00:00:03.7586 tcp(6) S 56.37.74.42 4406 203.49.33.129 1080 [Windows XP SP1]
2008-06-04-00:00:03.7587 tcp(6) S 56.37.74.42 4406 203.49.33.129 1080 [Windows XP SP1]
2008-06-04-00:00:03.7667 tcp(6) S 56.37.74.42 4406 203.49.33.129 1080 [Windows XP SP1]
2008-06-04-00:00:04.0084 tcp(6) S 56.37.74.42 4406 203.49.33.129 1080 [Windows XP SP1]
2008-06-04-00:00:04.0156 tcp(6) S 56.37.74.42 4406 203.49.33.129 1080 [Windows XP SP1]
2008-06-04-00:00:04.2286 tcp(6) S 56.37.74.42 4406 203.49.33.129 1080 [Windows XP SP1]
2008-06-04-00:00:04.4568 tcp(6) S 56.37.74.42 4406 203.49.33.129 1080 [Windows XP SP1]
2008-06-04-00:00:04.5764 tcp(6) S 56.37.74.42 4406 203.49.33.129 1080 [Windows XP SP1]
2008-06-04-00:00:04.5857 tcp(6) S 56.37.74.42 4406 203.49.33.129 1080 [Windows XP SP1]
2008-06-04-00:00:04.6786 tcp(6) S 56.37.74.42 4406 203.49.33.129 1080 [Windows XP SP1]
2008-06-04-00:00:05.2346 tcp(6) S 56.37.74.42 4406 203.49.33.129 1080 [Windows XP SP1]
2008-06-04-00:00:05.4566 tcp(6) S 56.37.74.42 4406 203.49.33.129 1080 [Windows XP SP1]
2008-06-04-00:00:05.4577 tcp(6) S 56.37.74.42 4406 203.49.33.129 1080 [Windows XP SP1]
```

n = 1º slot de tempo

n = 2º slot de tempo

n = 3º slot de tempo

m = 1 indica a porta tcp(6) 1080

⇒ Portanto:

$$x_1(1) = 3$$

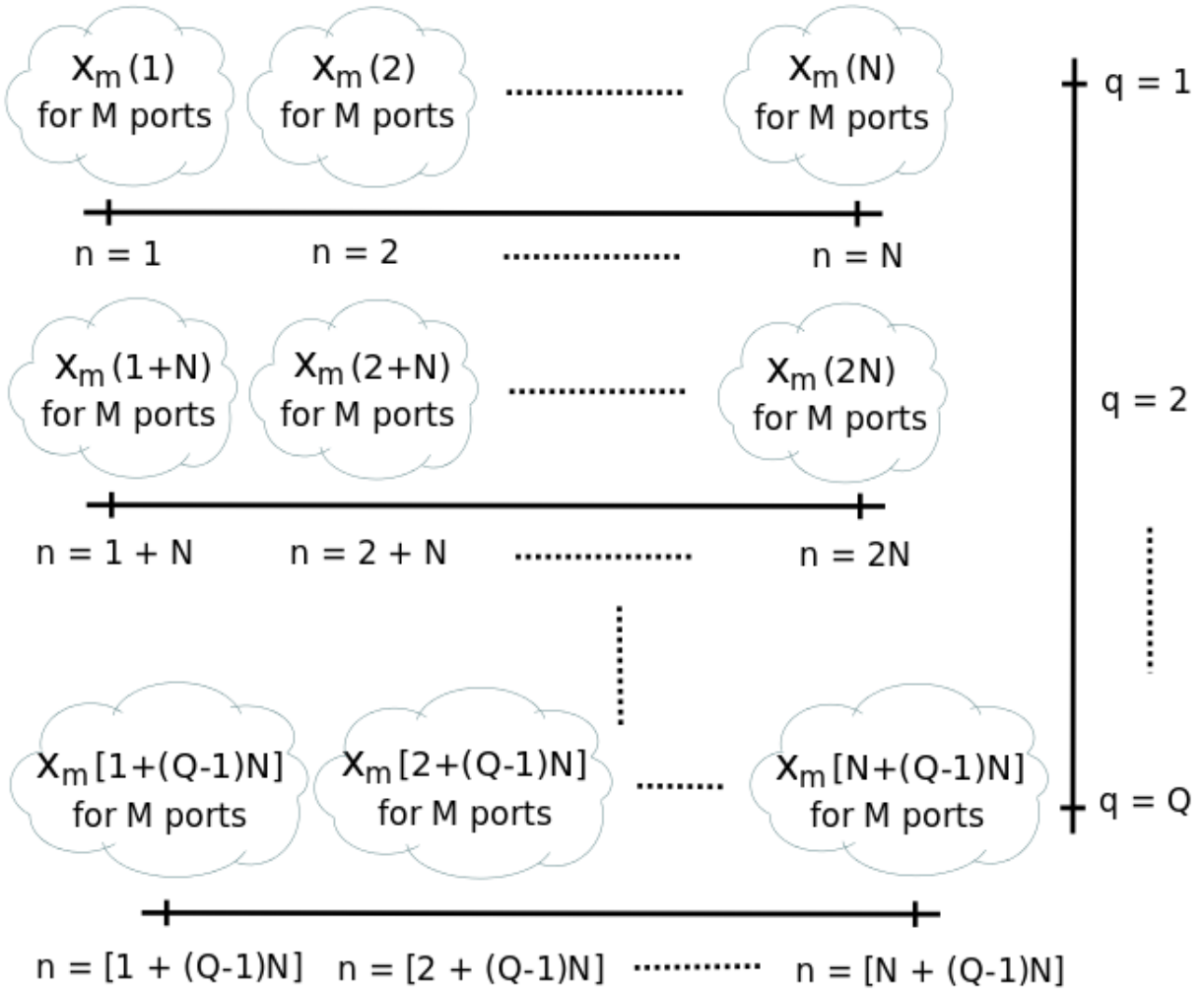
$$x_1(2) = 7$$

$$x_1(3) = 3$$

$$\mathbf{X}^{(q)} = \mathbf{S}^{(q)} + \mathbf{N}^{(q)} + \mathbf{A}^{(q)}$$

$\mathbf{X}^{(q)} \in \mathbb{R}^{M \times N}$: tráfego total
$\mathbf{S}^{(q)} \in \mathbb{R}^{M \times N}$: tráfego legítimo
$\mathbf{N}^{(q)} \in \mathbb{R}^{M \times N}$: tráfego de ruído
$\mathbf{A}^{(q)} \in \mathbb{R}^{M \times N}$: tráfego malicioso

Modelagem dos Dados (4)

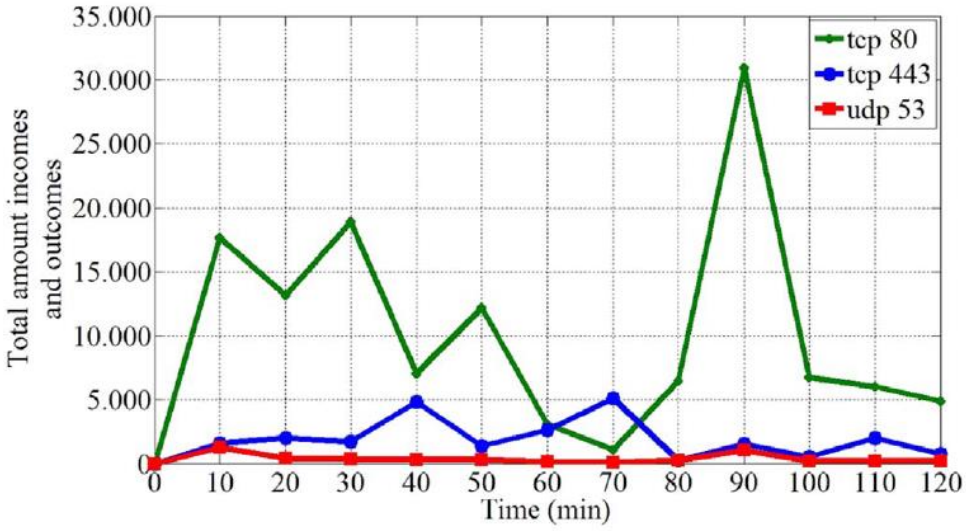


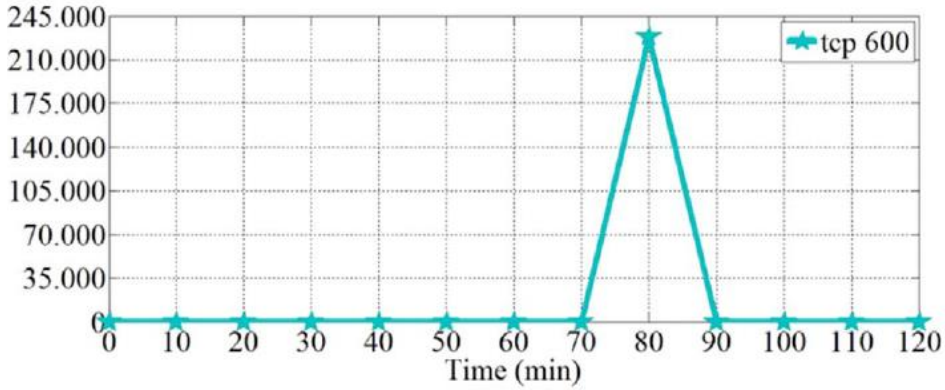
Roteiro

- Motivação
- Exemplos de Ataques: synflood, fraggle e portscan
- Modelagem dos Dados
- Testes Controlados
- Testes Não-Controlados com Honeypots
- Extensão para Honeynets

Testes Controlados (1)

- Objetivo:
  - ⇒ detecção de ataques massivos (flooding) e sutis (probe)
- Modelagem de tráfego de rede como:
  - ⇒ uma sobreposição de sinal, ruído e anomalias (ataques)
  - ⇒ Quantificada a quantidade de tráfego por porta e tempo
  - ⇒ Divisão em janelas de tempo





Testes Controlados (2)

- A análise de autovalores identifica as janelas em que ocorreram os ataques

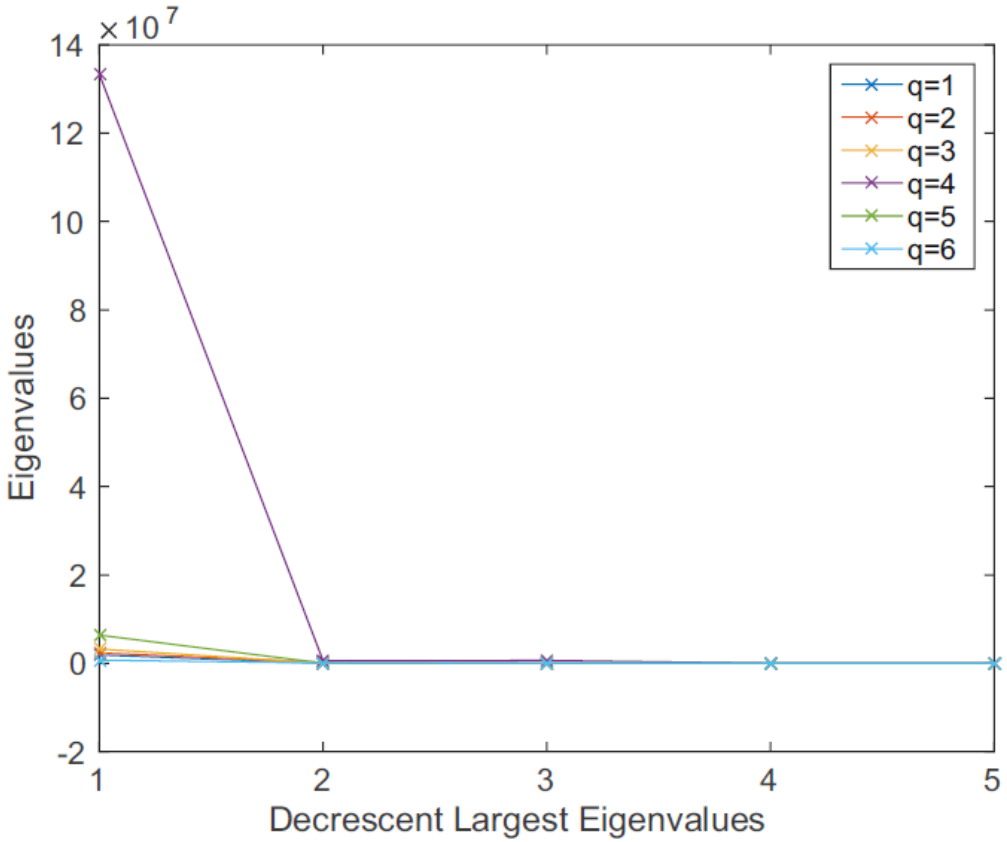
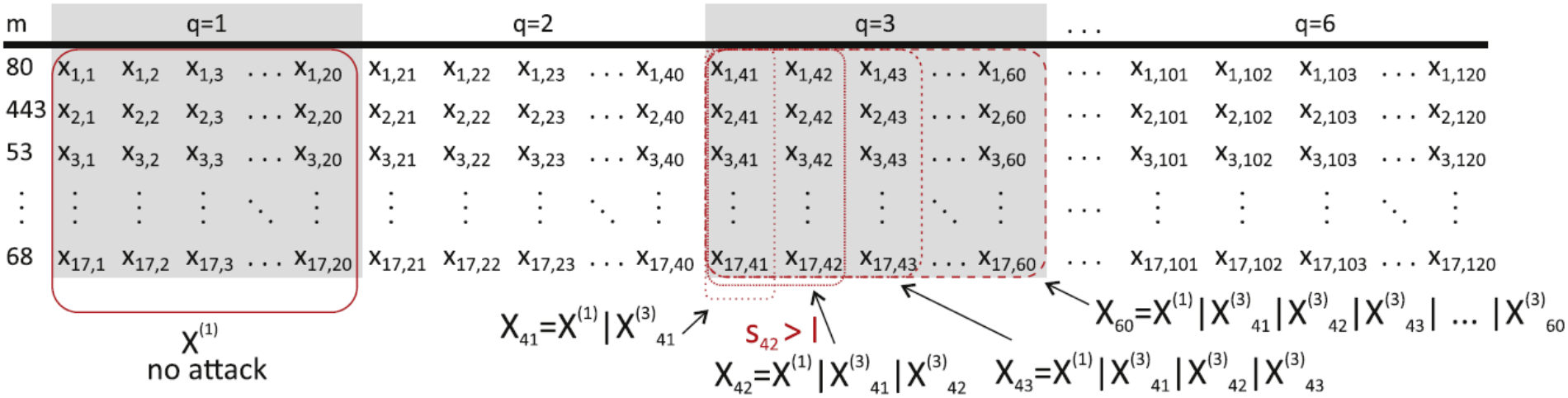


Fig. 11. Eigenvalues of the sample covariance matrix (synflood).

Testes Controlados (3)

- A análise de similaridade dos autovetores identifica o tempo e a porta em que os ataques ocorreram

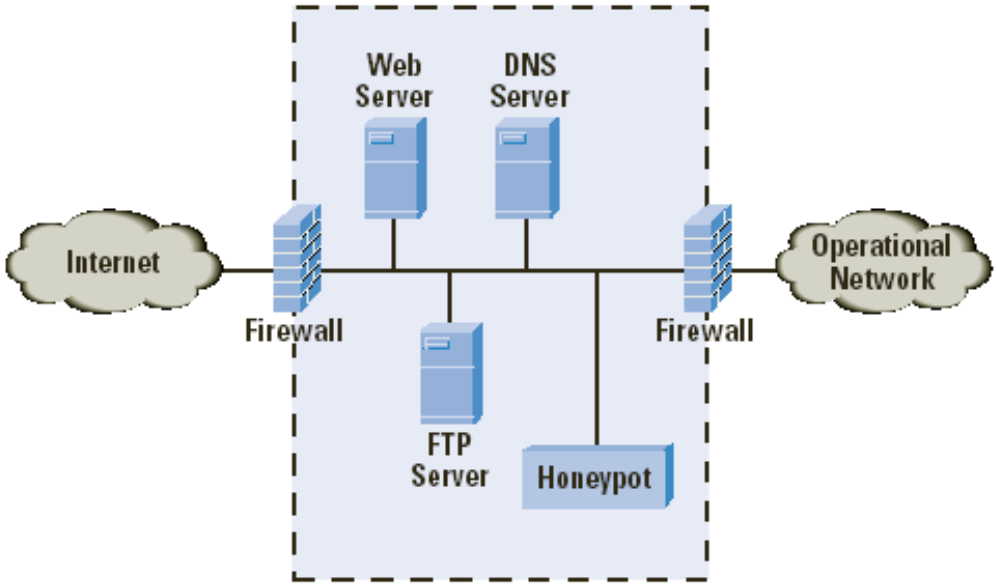


Roteiro

- Motivação
- Exemplos de Ataques: synflood, fraggle e portscan
- Modelagem dos Dados
- Testes Controlados
- Testes Não-Controlados com Honeypots
- Extensão para Honeynets

Testes Não-Controlados com Honeypots (1)

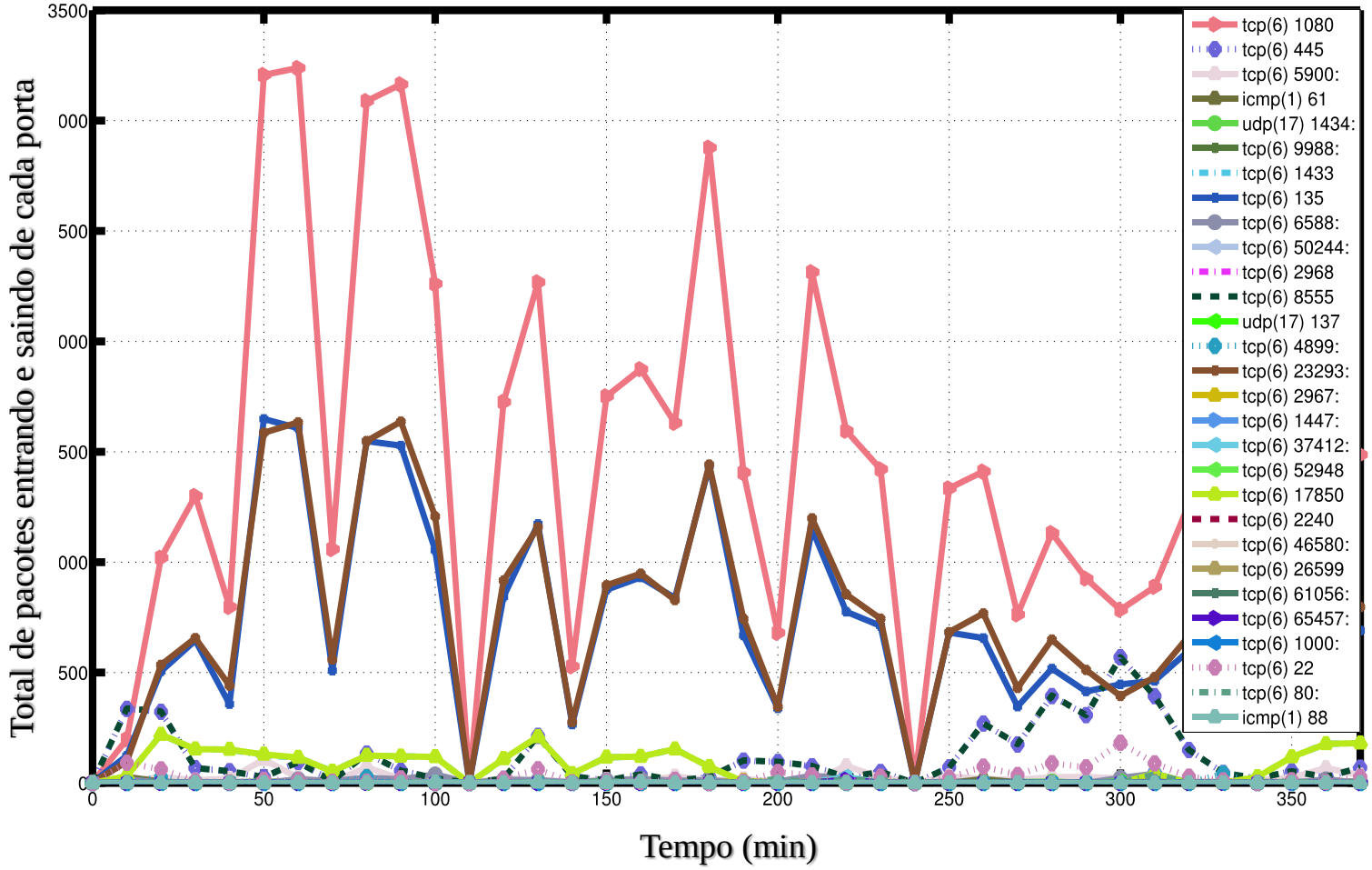
- Honeypot
  - ⇒Atrai ataques de usuários maliciosos
  - ⇒Redução da quantidade de dados analisados
  - ⇒Maior parte do tráfego é malicioso.



2008-06-04-00:00:03.7586 tcp(6) S 56.37.74.42 4406 203.49.33.129 1080 [Windows XP SP1]

Testes Não-Controlados com Honeypots (2)

- Pre-processamento do dados do Honeypot do Banco do Brasil

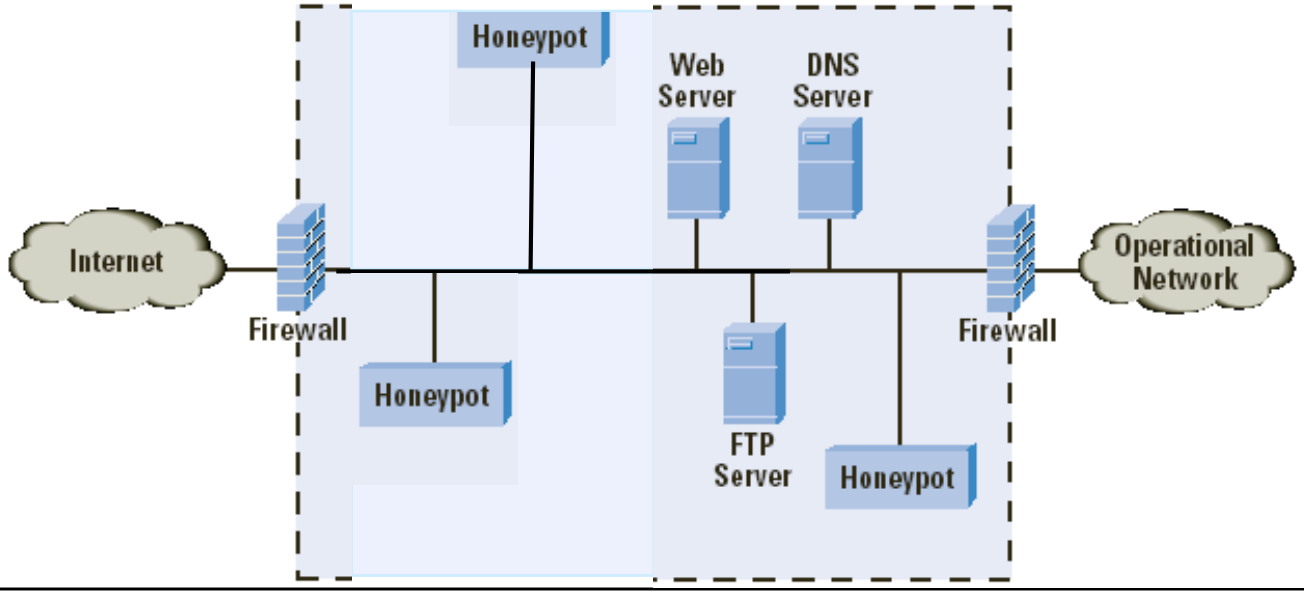


Roteiro

- Motivação
- Exemplos de Ataques: synflood, fraggle e portscan
- Modelagem dos Dados
- Testes Controlados
- Testes Não-Controlados com Honeypots
- Extensão para Honeynets

Extensão para Honeynets (1)

- Honeynet
  - ⇒Conjunto de honeypots
  - ⇒Logs de *H* honeypots para facilitar a detecção de ataques
  - ⇒Envio dos logs para um processador central para processamento
    - Limitação da grande massa de dados dependendo do ataque



Extensão para Honeynets (2)

- Honeynet
  - ⇒Proposta de envio de dados pre-processados [10]
    - Cálculo das matrizes com *Q* vetores de autovalores de tamanho *M* para cada *h* honeypot
    - Único vetor por meio do produto ponto a ponto dos *Q* *q*-ésimos vetores de autovalores das *H* matrizes da honeynet
    - Após a combinação dos vetores das *H* matrizes: matriz de combinação com os autovalores globais [11]
      - Estimação do ataque por meio de técnica multidimensionais de seleção da ordem do modelo

[10] B. M. David, J. P. C. L. da Costa, A. C. A. Nascimento, M. D. Holtz, D. Amaral, and R. T. de Sousa Jr., "A Parallel Approach to PCA Based Malicious Activity Detection in Distributed Honeypot Data," International Journal of Forensic Computer Science (IJoFCS), 2011

[11] J. P. C. L. da Costa, F. Roemer, M. Haardt, and R. T. de Sousa Jr., "Multi-Dimensional Model Order Selection," EURASIP Journal on Advances in Signal Processing 2011, Vol. 26, 20 July 2011, Springer publisher

Obrigado pela atenção!

Prof. Dr.-Ing. João Paulo C. Lustosa da Costa
Universidade de Brasília (UnB)
Departamento de Egenharia Elétrica (ENE)
Laboratório de Processamento de Sinais em Arranjos
Laboratório de Tecnologias da Tomada de Decisão (LATITUDE.UnB)