IPT

Instituto de Pesquisas Tecnológicas
de São Paulo

Análise de Tendências Futuras para Eventos de Segurança da Informação em IDS

Elvis Pontes	elvis@pontes.inf.br	IPT
Dr. Adilson Guelf	guelfi@lsi.usp.br	IPT, EPUSP, LSI - USP
Dr. Edson Alonso	edson@lsi.usp.br	EPUSP, LSI - USP

03 de setembro de 2008

Objetivo / Motivação

IPT
Instituto de pesquisas Tecnológicas

- **Objetivo:**
  - Previsão de incidentes em um IDS.
- **Motivação:**
  - Pouco (ou nenhum) estudo de previsão incidentes em IDS e Internet;
  - **Descoberta da presença de razões da seqüência de Fibonacci (φ) na série histórica de incidentes do DARPA.**

Trabalhos Relacionados

IPT
Instituto de pesquisas Tecnológicas

- **Meteorologia;**
- **Sismologia;**
- **Vulcanismo;**
- **Bolsa de Valores;**
  - Ralph Nelson Elliot – psicologia social.

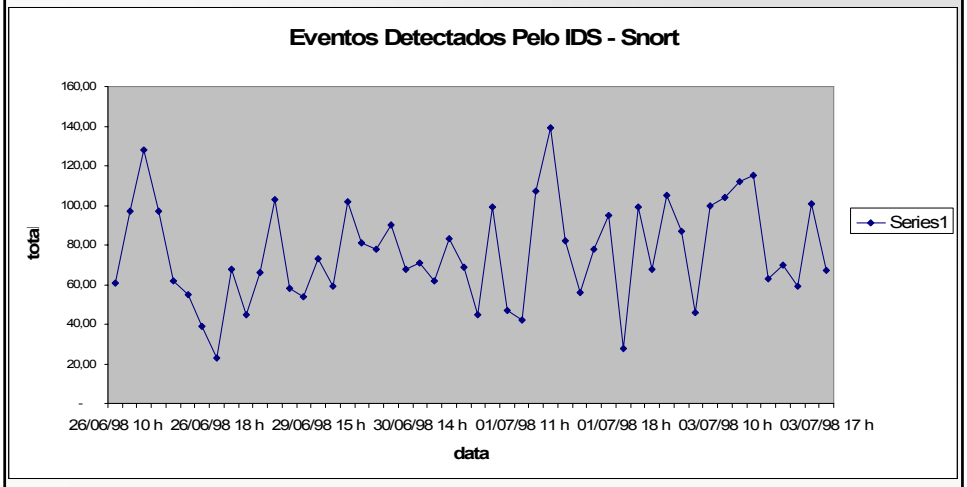
Metodologia

IPT
Instituto de pesquisas Tecnológicas

Análise Gráfica de Tendências Futuras

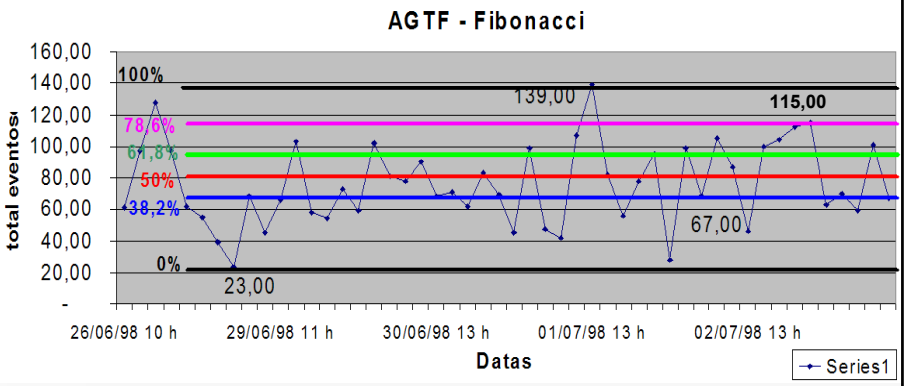
Resultados

IPT
Instituto de pesquisas Tecnológicas



Resultados

IPT
Instituto de pesquisas Tecnológicas



Metodologia / Fionacci

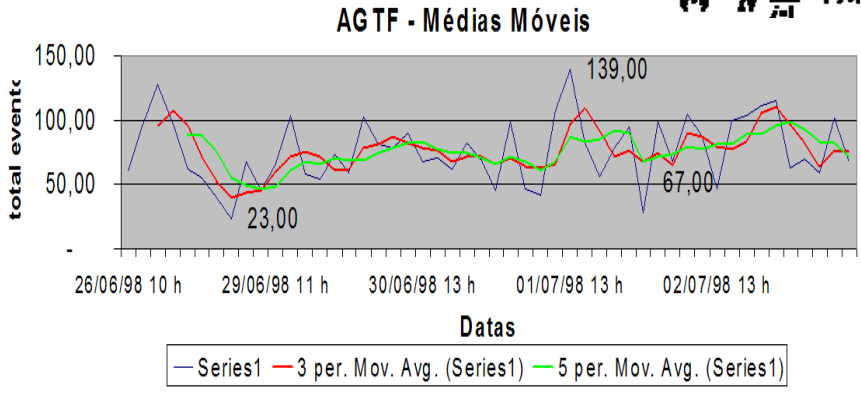
IPT
Instituto de pesquisas Tecnológicas

- •100% quantidade máxima dos ataques;
- •78,60% obtido por φ;
- **•61,80% φ;**
- •50% razão entre o quinto e o quarto elementos da seqüência de Fibonacci (3/2);
- **•38,20% complemento de φ;**
- •23,60% razão entre o complemento de φ e o próprio φ;
- •0% menor quantidade dos ataques.

Resultados

IPT
Instituto de pesquisas Tecnológicas

$$F_{(\cdot)} = \frac{1}{N}\sum_{i=1}^{N} A_{i-j+1}$$



Conclusões

IPT
Instituto de pesquisas Tecnológicas

- Nos datasets DARPA foi possível encontrar φ e razões da seqüência de Fibonacci;
- Aparentemente existem padrões nos incidentes do identificados pelo IDS;
- Os resultados são positivos e favoráveis a aplicação das técnicas previsão de incidentes.

Trabalhos Futuros

IPT
Instituto de pesquisas Tecnológicas

1. Agregar outros métodos de previsão de incidentes de SI em IDS;
2. Agregar a AGTF a outras técnicas de detecção de anomalias e incidentes:
   - Análise de tráfego;
   - Antivírus;
   - Firewall.
3. Agregar a previsão de eventos de SI à ANÁLISE DE RISCO;
4. Agregar a previsão de eventos de SI ao estudo do ROSI.

Referências Bibliográficas

IPT
Instituto de pesquisas Tecnológicas

- DARPA, Defense Advanced Research Projects Agency (1998, 1999, 2000) “Intrusion Detection Evaluation”, MIT – Massachusetts Institute of Technology
- Elliot, Ralph Nelson (1982) “Reconstruction of the Elliott Wave Principle (New Expanded Edition)”, Amer Classical
- SNORT, VRT Certified rules (2008), http://www.snort.org
- Wei, Huaqiang, Frinke, Deb, Carter, Olivia and Ritter, Chris (2001) “Cost-Benefit Analysis for Network IDS” CSI 28th Annual Computer Security Conference.

IPT
Instituto de pesquisas Tecnológicas

- Dúvidas
- Sugestões

Obrigado!

Elvis Pontes	elvis@pontes.inf.br	IPT
Dr. Adilson Guelf	guelfi@lsi.usp.br	IPT, EPUSP, LSI - USP
Dr. Edson Alonso	edson@lsi.usp.br	EPUSP, LSI - USP