Análise de Tendências Futuras para Eventos de Segurança da Informação em Sistemas de Detecção de Intrusão

Elvis Pontes[1], Adilson E. Guelfi[1 e 2], Edson E. Alonso[2]

[1]Instituto de Pesquisas Tecnológicas de São Paulo (IPT)
Av. Prof. Almeida Prado, 532 – Cidade Universitária – Butantã – São Paulo - SP

[2]Escola Politécnica da Universidade de São Paulo (EPUSP)
CEP: 05508-900 – São Paulo – SP – Brasil

elvis.ipt@gmail.com.br, (guelfi,ealonso)@lsi.usp.br

1. Introdução

Atualmente, análise gráfica de tendências futuras (AGTF) é utilizada no mercado acionário para auxiliar na tomada de decisão de investimentos. Assim como no mercado acionário, a meteorologia, por exemplo, estuda a previsão do tempo para dar suporte à tomada de decisões: se uma tendência mostrar possibilidade de chuva na semana seguinte, isto auxilia a decidir se é prudente carregar ou não um guarda-chuva – carregar um guarda-chuva em uma tendência de dia ensolarado pode ser inútil. Ciências como a sismologia e o vulcanismo também estudam a previsão de eventos e incidentes de suas áreas de interesse, antecipando a tomada de decisões.

Nos dias de hoje, pouca, ou nenhuma pesquisa é realizada sobre tendências futuras de eventos de segurança em SDI. Analogamente ao mercado financeiro, à meteorologia, sismologia e vulcanismo, por exemplo, o resultado de análise de tendências futuras em um SDI pode mostrar a necessidade e o momento de investimentos em controles de segurança da informação. Considerando um cenário futuro de aumento de incidentes, a AGTF pode viabilizar decisões sobre o uso de dispositivos de segurança antes da ocorrência de incidentes e conforme necessário. Incrementar controles pode significar processar mais, gastar mais, consumir mais energia, ter redundância de servidores, etc. Corroborando essa idéia existe o trabalho de [Wei, Huaqiang et al 2001] que, com sua a análise de custo-benefício em SDI, conclui sobre a aplicação de controles de segurança somente quando necessário.

O objetivo deste resumo estendido é mostrar a AGTF aplicada a eventos gerados por um sistema de detecção de intrusão (SDI), por duas técnicas de identificação de tendências: seqüência Fibonacci e médias móveis.

2. Metodologia

Assim como apresentado na Figura 1, na etapa atual deste trabalho foram estudadas as tendências de eventos de segurança de curto prazo (período de horas). Na Figura 1 se exibe o modelo AGTF que gera dois gráficos com as duas técnicas consideradas de identificação de tendências (seqüência de Fibonacci e médias móveis). Utiliza-se uma base de dados de tráfego do [DARPA, 1998, 1999, 2000] e o SDI [Snort 2008] é a ferramenta para verificar os eventos de segurança (intrusões) presentes na base de dados. As intrusões são posteriormente armazenadas em uma base MySQL. A AGTF coleta os dados gravados no banco de dados MySQL, analisa as informações e gera os gráficos de tendência, segundo as técnicas da seqüência de Fibonacci e médias móveis.

Conforme mostrado no gráfico superior da Figura 1, a AGTF empregando a seqüência de Fibonacci, aponta a tendência (esta AGTF é derivada das teorias de [Elliot, Ralph Nelson 1982]). As razões da série são 61,8% e seu complemento 38,2%. Para as expansões, usam-se os extremos 23,6% e 78,6%. Entre 26/06/98 e 03/07/98, os incidentes têm um mínimo de 23, atingem o topo de 139 e recuam a 67, que representa 38,2% de correção do movimento anterior. Mas, nos momentos da queda para 61,8% e 50%, há a retomada de aumento de incidentes, ambos próximos aos 78,6%. Percebe-se, também, que o movimento de queda se encerra próximo ao percentual de 61,8%.

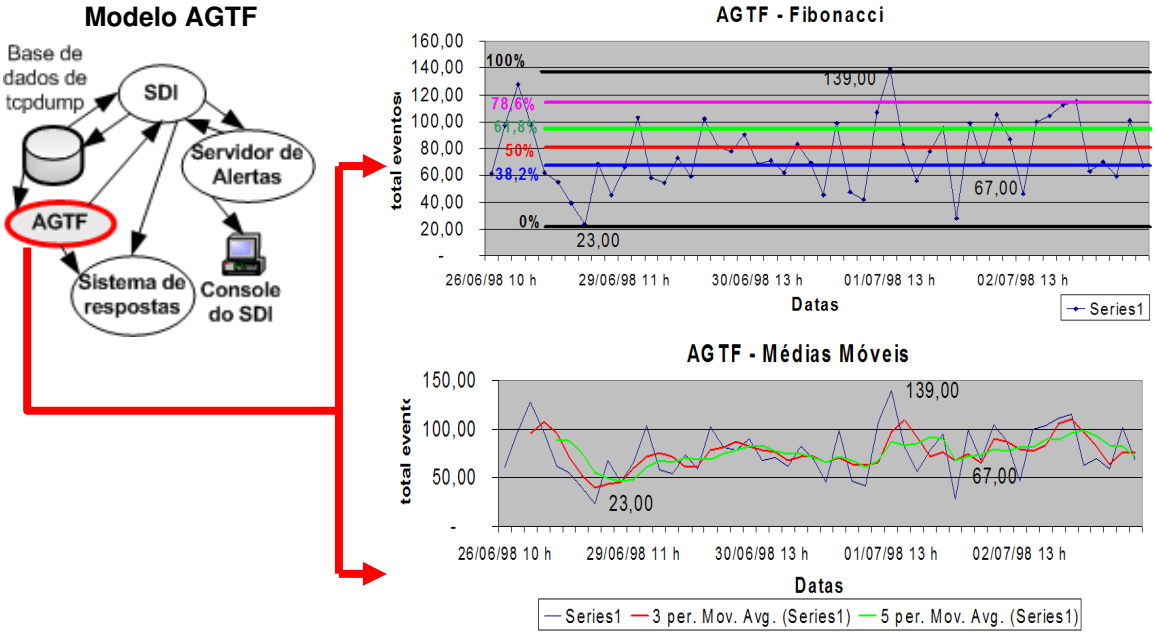

Figura 1: Metodologia AGTF e Gráficos AGTF

De acordo com o exibido no gráfico inferior da Figura 1, a AGTF Médias Móveis confirma tendência. Usando duas médias móveis, de 3 horas (curta) e de 5 horas (longa), tem-se a tendência de alta quando a média curta cruza a média longa para cima e, quando a média curta cruza a média longa para baixo, tem-se a tendência de baixa.

Os resultados obtidos, até o estágio atual deste trabalho, são positivos e favoráveis a aplicação das técnicas de identificação de tendências de eventos de segurança da informação em SDI. Em próxima etapa, para se analisar períodos mensais e trimestrais, pretende-se aplicar as mesmas técnicas definidoras de tendências (seqüência de Fibonacci e médias móveis) em outras bases de dados tráfego.

Referências

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.