

ANÁLISE DE ASSINATURAS DE ATAQUE BASEADAS EM FLUXOS DE DADOS PARA DETECTORES DE INTRUSÃO ADAPTATIVOS. Jorge Luiz Corrêa, Adriano Mauro Cansian. - Ciência da Computação – Bacharelado em Ciência da Computação – Departamento de Ciências de Computação e Estatística – Instituto de Biociências, Letras e Ciências Exatas – Campus de São José do Rio Preto.

Introdução

A detecção de intrusão é o processo de identificação de atividades maliciosas ou não autorizadas em computadores ou redes de computadores. Trata-se de uma tarefa complexa quando analisada no âmbito das constantes mudanças nas tecnologias oferecidas na Internet. Alia-se a isto, a evolução das técnicas de ataques e o surgimento desenfreado de softwares de má qualidade, cujo quesito segurança é simplesmente ignorado. Assim, administradores convivem constantemente com a ocorrência de ataques e intrusões, não havendo uma maneira totalmente efetiva de bloqueá-las. Nesta situação, ferramentas que os auxiliem a evitar e detectar tais eventos tornam-se necessárias e de extrema valia.

É crescente o número de atividades importantes e críticas que passaram a ser realizadas por intermédio das redes de computadores, principalmente pela Internet, como por exemplo transações bancárias ou operações confidenciais e controle de processos críticos. Portanto, é de essencial importância que esta infra-estrutura opere de maneira correta. A segurança desses sistemas computacionais e redes de computadores tornou-se indispensável para a viabilidade destes processos. Além da criticidade dos processos e tarefas dependentes das redes de computadores, o crescimento tecnológico tem contribuído para uma demanda cada vez maior de processamento e velocidade.

Este trabalho apresenta uma proposta de análise de fluxos de dados em redes de computadores visando estabelecer uma metodologia de detecção de intrusos, utilizando para isto o padrão de fluxos de dados *Netflow* [Cis04][RFC-3954] em conjunto com uma rede neural artificial (RNA) [Hay01].

Sistemas de detecção de intrusão

Os IDSs (de *Intrusion Detection Systems*) são sistemas capazes de detectar um comportamento intrusivo em sistemas computacionais [Can07]. Esta detecção pode ocorrer em diversos perímetros de acordo com o tipo de IDS utilizado. Tanto pode ocorrer isoladamente em um computador (*host based*) quanto pode abranger toda uma estrutura de rede institucional, constituída de diversos computadores (*network based*). Ambos os tipos de IDSs estão em constante desenvolvimento. No entanto, os baseados em redes despontaram no contexto de escalabilidade e desempenho. As redes de alta velocidade inviabilizaram alguns modelos de detecção de intrusão utilizados anteriormente. Grandes taxas de dados e a alta demanda em seu manuseio tornaram algumas metodologias inviáveis.

Fluxos de dados

Uma nova tecnologia denominada fluxos de dados [RFC-3917][RFC-3955] está sendo empregada com sucesso na detecção de atividades anômalas que caracterizem ataques a sistemas computacionais. Esta tecnologia pode ser entendida como uma sumarização de informações referentes ao tráfego de borda. Roteadores exportam para máquinas especiais (denominadas coletores) informações sobre o andamento do ambiente de rede. Estas informações são encapsuladas em datagramas denominados registros de fluxos. Estes registros de fluxos carregam informações importantes que permitem uma variedade de análises. Algumas delas dizem respeito a quantidade de dados trafegada, quais os computadores envolvidos, os

tipos de serviços dentre várias outras. Estas informações são tomadas como matéria-prima para o novo modelo de detecção de intrusos.

A Inteligência artificial

A Inteligência Artificial (IA) é um ramo da Ciência da Computação que estuda problemas atualmente melhor realizados por seres humanos. Trata de processos nos quais esteja envolvido algum tipo de conhecimento, que possivelmente será absorvido pelo sistema. Dentre as diversas técnicas de resolução de problemas da IA estão as redes neurais artificiais (RNAs). As RNAs são sistemas compostos por entidades conectadas (denominadas neurônios) que utilizam modelos matemáticos para processamento de informações, utilizando uma metodologia conexionista da computação. As RNAs têm a capacidade de realizar classificações de padrões de forma bastante eficiente. O funcionamento básico ocorre em três etapas: concepção do modelo, treinamento e utilização. Na concepção a rede é modelada, de acordo com o número de neurônios e camadas utilizadas. O treinamento é o método pelo qual o conhecimento sobre determinado assunto é inserido no sistema. Na etapa final, correspondente ao seu funcionamento, a rede toma um padrão de entrada e produz uma saída classificatória, de acordo com o que já aprendeu.

Modelo adaptativo de análise de fluxos de dados

Reunindo as características das tecnologias anteriormente apresentadas, está em desenvolvimento e aprimoramento um sistema adaptativo de análise de fluxos de dados. Este sistema muito contribui no gerenciamento de ambientes de redes, pois reconhece de forma automática eventos que caracterizem comportamentos intrusivos. Além disso, como é inerente aos fluxos de dados, este modelo é facilmente adaptável à redes de alta velocidade, mantendo a escalabilidade do processo de detecção.

Pesquisa desenvolvida no projeto de iniciação científica

Um conceito bastante importante dentro dos IDSs são as assinaturas de ataque. Uma assinatura de ataque é um padrão procurado (dependendo do tipo de IDS) o qual representa intrinsecamente um ataque. Por exemplo, uma assinatura de um IDS baseado em redes pode levar em consideração a ocorrência de uma *string* no campo de dados de um datagrama UDP ou pacote TCP. Dessa forma, são estruturas que trazem características as quais descrevem um evento malicioso, utilizadas como parâmetros na busca por novas ocorrências em sistemas monitorados. Um conhecido exemplo de uma assinatura pode ser visto nos softwares antivírus, utilizado em qualquer computador que tenha o mínimo de segurança. Seu funcionamento é tal que, quando um arquivo é recebido o *software* procura dentro deste pela ocorrência de padrões conhecidos que descrevem vírus. Estes padrões são obtidos pela Internet, quando atualizamos o *software*.

Em sua grande maioria, tantos os IDS baseados em redes quanto os baseados em *host* utilizam uma técnica conhecida como *fingerprint*, que consiste em analisar registros de auditoria e procurar pelos dados dispostos nas assinaturas. Apesar de efetiva, tal metodologia pode inviabilizar o processo de detecção devido à demanda computacional, dependendo do ambiente em que é utilizada.

Diferentemente dos IDSs que utilizam *logs* e análise de pacotes como matéria-prima para a detecção de intrusão, este novo modelo decai sobre o conceito de comportamento do ambiente [Gee06]. A base para a detecção de intrusão é o tráfego em uma rede de computadores. Isso possibilita a detecção de eventos antes dificilmente detectados, como tentativas de prospecção (*scans*) e ataques de negação de serviço (DoS).

No contexto desta nova metodologia de detecção de intrusão, as assinaturas de ataque continuam com papel fundamental, pois são os parâmetros descritores das atividades maliciosas. No entanto, as assinaturas utilizadas em sistemas adaptativos possuem características próprias, podendo ser consideradas um novo conceito quando comparadas com as assinaturas dos IDS

comuns. Alguns dos fatores que levam a esta diferenciação estão os fluxos de dados e a inteligência acoplada ao sistema, a fim de torná-lo adaptativo ao ambiente.

Neste projeto de iniciação científica, estuda-se a modelagem de novas assinaturas de ataque, de forma a obter aquela que apresente melhor eficiência na tarefa de detecção de intrusão. Vários modelos estão sendo propostos e testados em um ambiente real de redes de computadores. Fatores como precisão de detecção, número de falsos positivos, facilidade de adaptação com a rede neural e quantidade de informações presentes na assinatura são utilizados como métrica para validação.

Referências bibliográficas

- [Can97] CANSIAN, A.M. **Desenvolvimento de um Sistema Adaptativo de Detecção de Intrusos em Redes de Computadores**. 1997. Tese (Doutorado em Física Computacional) - Instituto de Física, Universidade de São Paulo, São Carlos, 1997.
- [Cis04] CISCO SYSTEMS. **Netflow Overview**. Disponível em: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/switch_c/xcp3/xcovntfl.htm>. Acessado em: 17 ago. 2006.
- [Gee06] GEER, D. **Behavior-based network security goes mainstream**. In: IEEE Computer, v.39, n.3, pp. 14-17, 2006
- [Hay01] Haykin, S. **Redes Neurais Princípios e Prática**. Editora Bookman, 2ª edição, Porto Alegre – RS, 2001.
- [RFC-3917] QUITTEK, J. et al. **RFC 3917: Requirements for IP Flow Information Export: IPFIX**. 2004. Published by Internet Engineering Task Force (IETF). Internet Society (ISOC) RFC Editor, USA, oct. 2004. Disponível em: <<http://www.ietf.org/rfc/rfc3917.txt>>. Acessado em: 08 out. 2006.
- [RFC-3954] CLAISE, B. **RFC 3954: Cisco Systems NetFlow Services Export Version 9**. Published by Internet Engineering Task Force (IETF). Internet Society (ISOC) RFC Editor. USA. oct. 2004. Disponível em: <<http://www.ietf.org/rfc/rfc3954.txt>>. Acessado em: 08 out. 2006.
- [RFC-3955] LEINEN, S. et al. **RFC 3955: Evaluation of Candidate Protocols for IP Flow Information Export (IPFIX)**. Published by Internet Engineering Task Force (IETF). Internet Society (ISOC) RFC Editor, oct. 2004. Disponível em: <<http://www.ietf.org/rfc/rfc3955.txt>>. Acessado em: 08 out. 2006.

Bolsa: FAPESP.