Uma Proposta Distribuída para Detecção de Intrusão, Hierárquica, Multiagente e Consciente de Situação

Ricardo B. Almeida[1], Roger S. Machado[1], Diórgenes Yuri L. Rosa[1], Lucas M. Donato[2], Adenauer C. Yamin[1], Ana M. Pernas[1]

[1]Programa de Pós-Graduação em Computação – Universidade Federal de Pelotas (UFPEL)
Caixa Postal 354 – 96.010-610 – Pelotas – RS – Brasil

[2]De Montfort University – Cyber Security Centre
Leicester, Reino Unido

{rbalmeida,rdsmachado,dyurirosa,adenauer,marilza}@inf.ufpel.edu.br,

lucas.donato@myemail.dmu.ac.uk

Resumo. *A necessidade do uso de Sistemas de Detecção de Intrusão (IDS) tem se potencializado devido à forma volátil, espontânea, heterogênea e invisível de como ocorre a comunicação nos modernos sistemas distribuídos. Assim sendo, este trabalho apresenta uma nova proposta de IDS distribuído baseado em sistemas multiagentes, com uma abordagem hierárquica que forneça a consciência de situação por meio do processamento de eventos complexos.*

1. Introdução

Com os avanços das tecnologias que permeiam os sistemas distribuídos, o acesso, a busca e o compartilhamento de informações tornaram-se tarefas naturais da vida cotidiana, provendo um dinamismo não antes visto na troca de dados. Infelizmente, todas as facilidades oferecidas por estes avanços acabam constituindo alvo para ataques. Logo, as soluções para detecção de atividades maliciosas, como os Sistemas de Detecção de Intrusão (IDS), se tornam uma necessidade potencializada nos ambientes distribuídos devido a forma volátil, espontânea, heterogênea e invisível de como ocorre a comunicação nestes ambientes [Langheinrich 2010].

Neste contexto, é possível destacar alguns desafios particulares à concepção de IDS's para ambientes distribuídos, como: o aumento da possibilidade de acesso não autorizado; o uso de recursos distribuídos; a variedade no formato dos dados; a velocidade em que os dados devem ser tratados, e; o grande volume de dados. Nesta perspectiva, para que se consiga um desempenho considerável na detecção de intrusão, uma abordagem distribuída e hierárquica para análise de eventos de segurança é uma possível estratégia para as modernas infraestruturas.

Tendo estes desafios em vista, surge a proposta deste trabalho, que é a concepção de um IDS distribuído baseado nos sistemas multiagentes, utilizando uma abordagem hierárquica que explore consciência de situação por meio do processamento de eventos complexos. O objetivo é proporcionar a melhoria da segurança em ambientes distribuídos, fornecendo: maior autonomia para os componentes da arquitetura do IDS, localizados nos diferentes nodos; flexibilidade para configuração, permitindo que módulos sejam habilitados ou desabilitados, de acordo com as necessidades e capacidades dos nodos envolvidos;

escalabilidade, e; visibilidade da situação dos ambientes monitorados quanto as atividades maliciosas.

2. Proposta

A proposta de IDS a ser concebida visa especialmente a distribuição de seus componentes no ambiente monitorado, sendo formada pelos seguintes componentes:

- Agente local: cada máquina monitorada possuirá um agente que será composto por funcionalidades de coleta e estratégias de IDS baseado em host e/ou em rede, podendo envolver métodos de detecção baseados em anomalia ou em conhecimento, fornecendo a possibilidade de escolha do administrador dos módulos e algoritmos a serem utilizados. Cada agente local poderá correlacionar e repassar seus eventos para o agente intermediário de sua escolha ou diretamente ao agente servidor. Caso algum dispositivo não possua capacidade de hospedar este componente, ele ainda poderá enviar seus eventos por protocolos como Syslog ou *Simple Network Management Protocol* para qualquer componente da arquitetura.
- Agente intermediário: visa filtrar e correlacionar os eventos recebidos de diversos agentes locais na procura por padrões de ataques. Ele poderá repassar seus eventos para outro agente intermediário de maior nível, ou ao agente servidor.
- Agente servidor: irá correlacionar os eventos de todo o ambiente, fornecendo uma visão aprimorada e apoiando a consciência de situação sobre o ambiente.

Todos os componentes permitem a realização de ações tanto no próprio agente, como de forma distribuída, como por exemplo, o envio de alertas, bloqueios no *firewall*, entre outras. A consciência de situação é alcançada por meio da correlação dos eventos nos diferentes níveis explorando hierarquia da arquitetura.

Por meio da análise dos trabalhos relacionados, que contemplam o desenvolvimento de um IDS distribuído com base no processamento de eventos complexos [Krügel et al. 2001], [Jun and Chi 2014], foi possível perceber que esta proposta se diferencia por apresentar uma abordagem distribuída e hierárquica, que considera além dos eventos de segurança comumente tratados, o uso dos recursos do sistema - que possui relação direta com os possíveis ataques à infraestrutura - e a utilização dos conceitos de consciência de situação para facilitar o entendimento do ambiente monitorado. Por fim, a quantidade de eventos comumente tratada em IDS's, especialmente considerando ambientes distribuídos, implica em outra característica a ser destacada desta proposta: o uso de um banco de dados não-relacional aliado a um banco relacional, explorando as diferentes vantagens de cada modelo.

Referências

Jun, C. and Chi, C. (2014). Design of complex event-processing ids in internet of things. In *Measuring Technology and Mechatronics Automation (ICMTMA), 2014 Sixth International Conference on*, pages 226–229.

Krügel, C., Toth, T., and Kerer, C. (2001). Decentralized event correlation for intrusion detection. In *in Proceedings of the International Conference on Information Security and Cryptology (ICISC)*, pages 114–131.

Langheinrich, M. (2010). *Privacy in Ubiquitous Computing*. J. Krumm, ed., CRC Press.