18º WRNP
Workshop RNP

15 | 16 MAIO
Belém | PA

GT-BIS
Mecanismos para análise de Big Data em segurança da informação

EQUIPE

Coordenador
Daniel Macêdo Batista
Instituto de Matemática e Estatística (IME)
Universidade de São Paulo (USP)

Coordenadores-adjuntos
Luiz Arthur F. dos Santos
Rodrigo Campiolo
Diego Bertolini Gonçalves
Universidade Tecnológica Federal do Paraná (UTFPR-CM)

Gerência de projeto e infraestrutura
Wagner A. Monteverde (UTFPR)

Pesquisa e Desenvolvimento
- Universidade de São Paulo
- Universidade Tecnológica Federal do Paraná

ESTAGIÁRIOS
- Universidade de São Paulo
- Universidade Tecnológica Federal do Paraná

PARCEIROS
- Universidade de São Paulo
- Universidade Tecnológica Federal do Paraná
- CAIS/RNP (a firmar)

SITE
gtbis.ime.usp.br

CONTATO
batista@ime.usp.br

Descrição

Com a obtenção de quantidades massivas de dados de tráfego de rede, vem a necessidade de métodos mais "inteligentes" para identificar incidentes de segurança, principalmente porque passa a ser possível encontrar informações novas por meio da correlação das informações e também porque uma análise de força bruta levaria muito tempo para ser finalizada.

Neste Grupo de Trabalho, é proposto o desenvolvimento de um sistema para análise de quantidades massivas de dados heterogêneos capturados em redes de computadores, no escopo da infraestrutura de rede da RNP, a fim de possibilitar a detecção, imediata ou antecipada, de ataques que não seriam detectados com sistemas existentes e o aprendizado automático do sistema com o histórico do tráfego.

Os objetivos a serem alcançados são:

- Definição de uma arquitetura capaz de escalar horizontal e verticalmente de forma automática, que realize análise de quantidades massivas de dados coletados por sensores distribuídos heterogêneos (pacotes e *logs* de aplicações e sistemas operacionais) em busca de ataques.
- Análise de desempenho, e de falsos positivos e falsos negativos, de diversas técnicas de correlação de dados a fim de avaliar a melhor para antecipação de ataques.
- Implementação de um protótipo de mecanismo de aprendizado de ataques simples para avaliar a viabilidade de um mecanismo mais robusto para ataques compostos por diversas etapas.
- Desenvolvimento de uma interface *web* para configuração do sistema e para visualização dos resultados das análises, possibilitando pelo menos: diferenciação de ataques por nível de criticidade, criação de linhas do tempo para ataques de duração prolongada, como ataques de DDoS, e criação de gráficos de índice de risco.
- Análise da viabilidade da utilização do sistema desenvolvido no CAIS da RNP. É possível ainda que apenas alguns mecanismos desenvolvidos sejam integrados a sistemas e procedimentos já existentes no CAIS da RNP, já que todos serão desenvolvidos pensando em serem facilmente integrados a padrões e protocolos bem definidos de envio de dados relacionados com segurança da informação.

Como inovações tecnológicas, destacam-se: (i) mecanismo capaz de correlacionar grandes quantidades de dados de diferentes fontes heterogêneas de modo a detectar ataques que não seriam possíveis de serem detectados com dados de uma única fonte, (ii) mecanismo capaz de antecipar ataques com base nos dados coletados de vários sensores e (iii) o protótipo de mecanismo de aprendizado de ataques.

O protótipo, ao término da Fase 1, deve ser capaz de realizar a análise de dados massivos que suporte a inclusão de diversas fontes e de gerar visualizações de incidentes de segurança, e a antecipação dos mesmos, utilizando a correlação de dados provenientes de diversos pontos de uma rede de computadores bem como de fontes heterogêneas, por exemplo, cabeçalhos de pacotes e *logs* de aplicações.

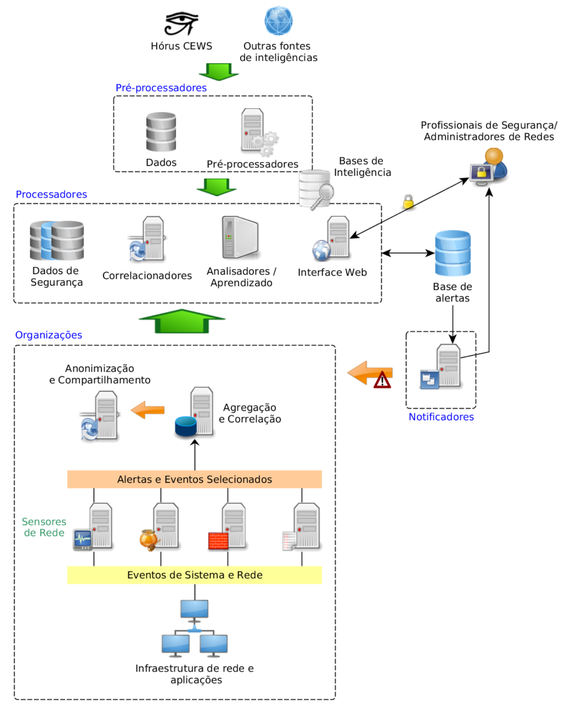

Figura 1: Visão geral do processamento de quantidades massivas de dados de segurança de fontes heterogêneas.