Proposta para Grupo de Trabalho

GT-EWS: Mecanismos para um Sistema de Alerta Antecipado

Daniel Macˆedo Batista

18 de Agosto de 2014

1 T´ıtulo

- GT-EWS: Mecanismos para um Sistema de Alerta Antecipado

2 Coordenador

- Daniel Macˆedo Batista
- Departamento de Ciˆencia da Computac¸˜ao – Instituto de Matema´tica e Estat´ıstica – Universidade de S˜ao Paulo (USP)
- http://lattes.cnpq.br/2934786440085983

3 Resumo

Este projeto prop˜oe o desenvolvimento de uma ferramenta para monitorar atividade maliciosa e detectar antecipadamente eventos e incidentes de seguran¸ca, atrav´es da correla¸c˜ao e an´alise de dados providos por sensores de redes tradicionais e outras fontes, como redes sociais, f´oruns e registros de redes virtuais. Esta ferramenta ser´a utilizada tamb´em para monitorar o uso de nomes de institui¸c˜oes em f´oruns e redes sociais, alertando poss´ıveis atividades maliciosas. Como contribuic¸˜ao para a RNP, espera-se que esta ferramenta auxilie nos processos de seguran¸ca da informa¸c˜ao, em especial detec¸c˜ao e resposta a incidentes de seguran¸ca. Esta ferramenta tamb´em poder´a ser oferecida como um servic¸o de detec¸c˜ao de atividade maliciosa e monitoramento de padr˜oes para as suas institui¸c˜oes usu´arias. E importante destacar tamb´em a contribuic¸˜ao cient´ıfica´ deste trabalho, que ´e a avalia¸c˜ao de novos sensores e o fornecimento de evidˆencias emp´ıricas do uso de t´ecnicas de recuperac¸˜ao de informa¸c˜ao para suportar novas arquiteturas de EWS (*Early Warning Systems* – Sistemas de Alerta Antecipado).

4 Abstract

This project proposes the development of a tool to monitor malicious activities and to detect, in advance, events and security incidents by correlating and analyzing traditional network sensors and other sources of information, such as social networks, forums and logs of virtual networks. This tool will also be used to monitor the citation of names of institutions in forums and social networks, warning the administrators about malicious activities. As contributions to RNP, we expect that this tool will help in the processes of information security, in special, in detection and response to security incidents. This tool can also be offered as a malicious activities detection and pattern monitoring to the users institutions of RNP. It's important to highlight the scientific contribution of the project, which is the evaluation of new network sensors and the empirical evidence about the use of techniques of information retrieval to support the new Early Warning Systems (EWS) architectures.

5 Parcerias

- **USP**: Al´em do Professor Daniel Macˆedo Batista, que ser´a o coordenador do projeto, um estagi´ario tamb´em ser´a contratado.
- **Universidade Tecnol´ogica Federal do Paran´a (UTFPR)**: Os professores Luiz Arthur Feitosa dos Santos e Rodrigo Campiolo, que sa˜o doutorandos no programa de p´os-graduac¸˜ao do IME-USP, orientados pelo Professor Daniel Batista, atuara˜o no projeto. Dois estagi´arios tamb´em ser˜ao contratados.
- **Ponto de Presen¸ca da RNP na Bahia (PoP-BA/RNP)**: Italo Valcy da Silva Brito, funciona´rio do PoP-BA atuara´ diretamente no projeto.
- **Superintendˆencia de Tecnologia da Informa¸c˜ao da Universidade Federal da Bahia (STI/UFBA)**: Rafael Brito Gomes, funciona´rio da STI/UFBA atuara´ diretamente no projeto.

6 Dura¸c˜ao do projeto

12 meses

7 Sum´ario executivo

Caracteriza¸c˜ao do Problema

Atualmente a economia de boa parte das empresas ao redor do mundo depende da disponibilidade e da normalidade de operac¸˜ao da infraestrutura de rede, tanto local quanto na Internet. Ataques a integridade e operac¸˜ao da infraestrutura de rede implicam em preju´ızos financeiros. Apesar dos investimentos para prevenc¸˜ao e prote¸c˜ao a ataques, nem sempre eles sa˜o suficientes para evitar os danos causados por uma invas˜ao ou uma tentativa de invas˜ao. Ataques compostos por diversas etapas, que vistas isoladamente n˜ao aparentam ser amea¸cas, e ataques que necessitam de alto poder computacional para serem detectados antes do atacante ter sucesso, sa˜o exemplos de problemas que ainda afligem as organizac¸˜oes. Em casos como estes, as medidas reativas, quando aplicadas, sa˜o tardias. Outro problema cr´ıtico ´e a falta de comunicac¸˜ao entre as organizac¸˜oes no sentido de compartilhar as informa¸c˜oes sobre ataques sofridos. A existˆencia de modelos para compartilhar esse tipo de informa¸c˜ao evitaria que atacantes ampliassem os sucessos dos seus ataques. Algumas propostas para esse compartilhamento existem mas n˜ao sa˜o implantadas na pr´atica.

Apesar da sofistica¸c˜ao dos ataques dificultar o trabalho de detec¸c˜ao por parte das empresas, novas tecnologias e novos servic¸os da Internet podem ser utilizados com o objetivo de auxiliar na detec¸c˜ao desses ataques, e de forma antecipada.

Os Sistemas de Alerta Antecipado, em inglˆes, *Early Warning Systems* (EWS), visam detectar e prever poss´ıveis amea¸cas de ataques baseados no comportamento dos sistemas, gerando alertas de situa¸c˜oes que apresentam

padr˜oes de risco, com o intuito de desencadear mecanismos reativos antecipadamente, evitando ou diminuindo os danos causados por um ataque. Em s´ıntese, os Sistemas de Alerta Antecipado permitem estabelecer hipo´teses e predi¸c˜oes correlacionando informa¸c˜oes incertas e incompletas providas por sensores em uma rede [2].

As limitac¸˜oes em detectar previamente ataques apenas confiando em an´alises de dados coletados de sensores na rede local, como registros de *firewall*, fluxos de rede e alertas de IDS, nem sempre permitem concluir ou detectar uma amea¸ca de ataque real ou reagir a tempo de evitar maiores danos. Tamb´em n˜ao permitem notificar a possibilidade real de ataque a outras organizac¸˜oes antes que realmente o ataque tenha sido identificado, pois gerariam muitos falsos positivos. Uma das formas de resolver esses problemas ´e projetar arquiteturas de EWS que sejam baseadas na cooperac¸˜ao [5] [1] [6]. Utilizar informa¸c˜oes vindas de fontes ignoradas, ou inexistentes, a alguns anos atr´as como redes sociais (e.g. Twitter – `https://twitter.com`) e registros de plataformas de virtualizac¸˜ao de redes (e.g. OpenFlow – `https://www.opennetworking.org/`) tamb´em tem mostrado resultados promissores [4] [7] [8] [3].

Neste projeto ser´a desenvolvida uma ferramenta para monitorar atividade maliciosa e detectar antecipadamente eventos e incidentes de seguran¸ca. A entrada para a ferramenta vir´a da correla¸c˜ao e an´alise de dados providos por sensores de redes tradicionais juntamente com outras fontes de informa¸c˜oes, como por exemplo, redes sociais, f´oruns e registros de redes virtuais. Mecanismos de redes virtuais tamb´em ser˜ao utilizados como forma de reagir `as amea¸cas. A ferramenta ser´a utilizada tamb´em para monitorar o uso de nomes de institui¸c˜oes em f´oruns e redes sociais, alertando poss´ıveis atividades maliciosas.

Contribui¸c˜oes e Potencial para se Tornar um Produto/Servi¸co da RNP

Como contribuic¸˜ao para a RNP, espera-se que esta ferramenta auxilie nos processos de seguran¸ca da informa¸c˜ao, em especial detec¸c˜ao e resposta a incidentes de seguran¸ca. A ferramenta tamb´em poder´a ser oferecida como um servic¸o de detec¸c˜ao de atividade maliciosa e monitoramento de padr˜oes para as institui¸c˜oes usu´arias da RNP. Como contribuic¸˜oes cient´ıficas espera-se prover a avalia¸c˜ao de novos sensores de rede para obter maior precisa˜o na detec¸c˜ao de novas amea¸cas, e prover evidˆencias emp´ıricas do uso de t´ecnicas de recuperac¸˜ao de informa¸c˜ao para suportar as novas arquiteturas de EWS. Propostas para permitir a cooperac¸˜ao entre institui¸c˜oes tamb´em ser˜ao fornecidas.

Estudos preliminares

Em estudos preliminares realizados pelos participantes da USP nos u´ltimos dois anos foi confirmado que fontes de informa¸c˜oes abertas, como redes sociais, proveem informa¸c˜oes relevantes de seguran¸ca [4] [8] [3]. Estudos preliminares tamb´em confirmaram a utilidade de redes virtuais tanto como sensores quanto como atuadores para EWS [7]. No esta´gio atual, h´a necessidade da investiga¸c˜ao de t´ecnicas de correla¸c˜ao de eventos para aplicac¸˜ao dos mecanismos preliminares em fluxos reais de redes. Al´em disso, precisa-se compreender e sistematizar as principais formas de ataques e explora¸c˜ao de vulnerabilidades e avaliar a escalabilidade dos mecanismos propostos. Por fim, pretende-se investigar o uso de t´ecnicas de aprendizagem de m´aquinas para

investigar e gerar alertas. Alguns dos c´odigos preliminares desenvolvidos nos u´ltimos dois anos esta˜o dispon´ıveis em https://github.com/luizsantos/Of-IDPS.

Estudos preliminares tamb´em foram realizados em 2010 quando o coordenador deste projeto foi instrutor do curso "Construindo um Sistema de Alerta Antecipado contra Ataques Cibern´eticos" no XVI Semin´ario RNP de Capacitac¸˜ao e Inovac¸˜ao (http://www.rnp.br/capacitacao/sci/2010/programa.php?apresentacao=536). Integrantes do PoP-BA/RNP foram alunos do curso.

Objetivos e metas

Neste projeto objetiva-se o desenvolvimento de mecanismos que permitam uma abordagem distribu´ıda e colaborativa para a detec¸c˜ao antecipada de incidentes de seguran¸ca em redes de computadores.

Como objetivos espec´ıficos tˆem-se:

- analisar e sistematizar os ataques e vulnerabilidades mais comuns em redes de computadores;
- investigar as limitac¸˜oes das soluc¸˜oes tradicionais de seguran¸ca, tais como IDS, honeypots e firewalls;
- avaliar e selecionar as t´ecnicas de minera¸c˜ao de dados mais efetivas para correla¸c˜ao de eventos gerados por sensores de redes;
- construir novos sensores para obter informa¸c˜oes de seguran¸ca a partir de fluxos de redes, tais como OpenFlow, redes sociais e f´oruns;
- prover um mecanismo para distribui¸c˜ao de dados de sensores de redes e de alertas sem comprometer a qualidade das informa¸c˜oes e a privacidade das entidades;
- desenvolver e analisar proto´tipos de software para os mecanismos de detec¸c˜ao antecipada de incidentes de seguran¸ca.

Os objetivos listados anteriormente j´a se encontram parcialmente desenvolvidos pelos integrantes conforme explicado na subse¸c˜ao **Estudos preliminares**. Entretanto, as implementac¸˜oes e os experimentos realizados at´e o momento possuem limitac¸˜oes que seriam vencidas caso o projeto fosse aceito pois passar´ıamos a contar com medidas reais de uma rede de larga escala por meio do servic¸o Monipˆe (http://www.monipe.rnp.br) al´em de termos acesso `a rede do PlanetLab para mais experimentos em casos onde a rede da RNP n˜ao pudesse ser utilizada por questo˜es operacionais. Al´em do projeto utilizar o servic¸o de monitoramento j´a existente na RNP, ele tamb´em visar´a a criac¸˜ao de um servic¸o de EWS que poderia ser do interesse do Centro de Atendimento a Incidentes de Seguranc¸a da RNP (CAIS – http://www.rnp.br/cais/). Novos sensores, novos mecanismos para correlacionar as informa¸c˜oes desses sensores e novos atuadores poderiam ser de utilidade de va´rios usu´arios da RNP e permitiriam a detec¸c˜ao antecipada de atividade maliciosa no backbone acadˆemico, a partir

de sensores internos distribu´ıdos por diversos pontos da Rede Ipˆe, al´em dos sensores de outras fontes de informa¸c˜ao na web.

O projeto proposto ´e inovador por explorar novos fluxos de informa¸c˜oes, providos pela grande quantidade de informa¸c˜oes dispon´ıveis e compartilhadas na Internet, em especial, em redes sociais, f´oruns e s´ıtios Web. Tamb´em inova ao buscar novas formas de correla¸c˜ao de eventos de seguran¸ca e investigar e avaliar mecanismos para gerac¸˜ao antecipada de alertas.

Tarefas dos parceiros

A fun¸c˜ao dos professores Daniel, Luiz e Rodrigo no projeto ser´a a de (1) propor novos algoritmos e mecanismos para correla¸c˜ao de eventos de sensores tradicionais de redes e de novos sensores que coletara˜o informa¸c˜oes, por exemplo, de redes sociais e f´oruns relevantes; (2) propor novos mecanismos para tomada de decis˜oes autonˆomicas em redes virtuais com o objetivo de reagir antecipadamente a ataques; (3) coordenar a implantac¸˜ao dos mecanismos em experimentos no PlanetLab e em m´aquinas do PoP/BA.

A fun¸c˜ao dos estagi´arios ser´a implementar proto´tipos dos mecanismos propostos pelos professores ou, nos casos em que proto´tipos j´a esta˜o implementados, como a vers˜ao preliminar do controlador OpenFlow que toma ac¸˜oes autonˆomicas, e do c´odigo que faz a classifica¸c˜ao de mensagens no Twitter, realizar testes de escalabilidade nesses softwares. Os estagi´arios ser˜ao coordenados diretamente pelos professores.

A fun¸c˜ao do ´Italo e do Rafael ser´a portar os mecanismos implementados pelos estagi´arios em novos sensores que atuara˜o com as informa¸c˜oes de monitoramento da rede Ipˆe (MonIPE) a fim de avaliar o seu correto funci-ˆ onamento em m´aquinas do PoP/BA e da UFBA. Experimentos realistas tamb´em ser˜ao projetados e realizados pelos dois.

8 Ambiente para testes do prot´otipo

Os equipamentos solicitados ser˜ao utilizados exclusivamente para o projeto. Os softwares ser˜ao desenvolvidos nesses computadores e redes virtuais ser˜ao criadas para realiza¸c˜ao de experimentos com o objetivo de correlacionar dados de diversos sensores. Bases de dados ser˜ao construi´das nos servidores com coletas de tweets e sites de forma regular. Al´em disso ser´a necess´ario acesso ao servic¸o do Monipˆe a fim de alimentar as ferramentas que correlacionar˜ao os eventos da rede da RNP juntamente com informa¸c˜oes vindas de outras fontes de informa¸c˜ao. Finalmente, o acesso ao PlanetLab tamb´em ser´a necess´ario nos u´ltimos 6 meses do projeto a fim de serem avaliadas as ac¸˜oes dos atuadores em uma rede de larga escala.

9 Referˆencias

[1] M. e. a. APEL. Towards Early Warning Systems - Challenges, Technologies and Architecture. *Lecture Notes in Computer Science*, 6027:151—-164, 2009.

[2] J. e. a. BISKUP. 08102 working group - early warning systems. In *Perspectives Workshop: Network Attack Detection and Defense – Dagstuhl Seminar Proceedings*, 2008.

[3] R. CAMPIOLO, L. A. F. SANTOS, D. M. BATISTA, and M. A. GEROSA. An´alise de Mensagens de Seguranc¸a Postadas no Twitter. In *Anais do Simpo´sio Brasileiro de Sistemas Colaborativos (SBSC)*, pages 1–8. SBC, 2012.

[4] R. CAMPIOLO, L. A. F. SANTOS, D. M. BATISTA, and M. A. GEROSA. Evaluating the Utilization of Twitter Messages As a Source of Security Alerts. In *Proceedings of the 28th Annual ACM Symposium on Applied Computing*, SAC '13, pages 942–943. ACM, 2013.

[5] B. GROBAUER, J. I. MEHLAU, and J. SANDER. Carmentis: A Co-Operative Approach Towards Situation Awareness and Early Warning for the Internet. In *Proceedings of the IT-Incidents Management & ITForensics (IMF)*, pages 55–66, 2006.

[6] U. Meissen and A. Voisard. Towards a Reference Architecture for Early Warning Systems. In *Proceedings of the 2nd International Conference on Intelligent Networking and Collaborative Systems (INCOS)*, pages 513–518, 2010.

[7] L. A. F. SANTOS, R. CAMPIOLO, and D. M. BATISTA. Uma Arquitetura Autonˆomica para Detecc¸˜ao e Reac¸˜ao a Amea¸cas de Seguranc¸a em Redes de Computadores. In *Anais do III Workshop em Sistemas Distribu´ıdos Autoˆnomicos (WoSiDA) – Workshops do Simpo´sio Brasileiro de Redes de Computadores e Sistemas Distribu´ıdos*, pages 1–4. SBC, 2014.

[8] L. A. F. SANTOS, R. CAMPIOLO, M. A. GEROSA, and D. M. BATISTA. Extrac¸˜ao de Alertas de Seguranc¸a Postados em Mensagens de Redes Sociais. In *Anais do XXXI Simpo´sio Brasileiro de Redes de Computadores e Sistemas Distribu´ıdos (SBRC)*, pages 791–804. SBC, 2013.