

# Proposta para Grupo de Trabalho

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

Daniel Macêdo Batista

18 de Agosto de 2014

# 1 Título

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

# 2 Coordenador

- Daniel Macêdo Batista
- Departamento de Ciência da Computação – Instituto de Matemática e Estatística – Universidade de São Paulo (USP)
- <http://lattes.cnpq.br/2934786440085983>
- E-mail: [batista@ime.usp.br](mailto:batista@ime.usp.br)
- Telefone: (11) 3091-0749

# 3 Resumo

Este projeto propõe o desenvolvimento de uma ferramenta para monitorar atividade maliciosa e detectar antecipadamente eventos e incidentes de segurança, através da correlação e análise de dados providos por sensores de redes tradicionais e outras fontes, como redes sociais, fóruns e registros de redes virtuais. Esta ferramenta será utilizada também para monitorar o uso de nomes de instituições em fóruns e redes sociais, alertando possíveis atividades maliciosas. Como contribuição para a RNP, espera-se que esta ferramenta auxilie nos processos de segurança da informação, em especial detecção e resposta a incidentes de segurança. Esta ferramenta também poderá ser oferecida como um serviço de detecção de atividade maliciosa e monitoramento de padrões para as suas instituições usuárias. É importante destacar também a contribuição científica deste trabalho, que é a avaliação de novos sensores e o fornecimento de evidências empíricas do uso de técnicas de recuperação de informação 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:** Além do Professor Daniel Macêdo Batista, que será o coordenador do projeto, um estagiário também será contratado.
- **Universidade Tecnológica Federal do Paraná (UTFPR):** Os professores Luiz Arthur Feitosa dos Santos e Rodrigo Campiolo, que são doutorandos no programa de pós-graduação do IME-USP, orientados pelo Professor Daniel Batista, atuarão no projeto. Dois estagiários também serão contratados.
- **Ponto de Presença da RNP na Bahia (PoP-BA/RNP):** Italo Valcy da Silva Brito, funcionário do PoP-BA atuará diretamente no projeto.
- **Superintendência de Tecnologia da Informação da Universidade Federal da Bahia (STI/UFBA):** Rafael Brito Gomes, funcionário da STI/UFBA atuará diretamente no projeto.

## 6 Duração do projeto

12 meses

## 7 Sumário executivo

### Caracterização do Problema

Atualmente a economia de boa parte das empresas ao redor do mundo depende da disponibilidade e da normalidade de operação da infraestrutura de rede, tanto local quanto na Internet. Ataques a integridade e operação da infraestrutura de rede implicam em prejuízos financeiros. Apesar dos investimentos para prevenção e proteção a ataques, nem sempre eles são suficientes para evitar os danos causados por uma invasão ou uma tentativa de invasão. Ataques compostos por diversas etapas, que vistas isoladamente não aparentam ser ameaças, e ataques que necessitam de alto poder computacional para serem detectados antes do atacante ter sucesso, são exemplos de problemas que ainda afligem as organizações. Em casos como estes, as medidas reativas, quando aplicadas, são tardias. Outro problema crítico é a falta de comunicação entre as organizações no sentido de compartilhar as informações sobre ataques sofridos. A existência de modelos para compartilhar esse tipo de informação evitaria que atacantes ampliassem os sucessos dos seus ataques. Algumas propostas para esse compartilhamento existem mas não são implantadas na prática.

Apesar da sofisticação dos ataques dificultar o trabalho de detecção por parte das empresas, novas tecnologias e novos serviços da Internet podem ser utilizados com o objetivo de auxiliar na detecção desses ataques, e de forma antecipada.

Os Sistemas de Alerta Antecipado, em inglês, *Early Warning Systems (EWS)*, visam detectar e prever possíveis ameaças de ataques baseados no comportamento dos sistemas, gerando alertas de situações que apresentam padrões de risco, com o intuito de desencadear mecanismos reativos antecipadamente, evitando ou diminuindo os danos causados por um ataque. Em síntese, os Sistemas de Alerta Antecipado permitem estabelecer hipóteses e previsões correlacionando informações incertas e incompletas providas por sensores em uma rede [2].

As limitações em detectar previamente ataques apenas confiando em análises 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 ameaça de ataque real ou reagir a tempo de evitar maiores danos. Também não permitem notificar a possibilidade real de ataque a outras organizações antes que realmente o ataque tenha sido identificado, pois gerariam muitos falsos positivos. Uma das formas de resolver esses problemas é projetar arquiteturas de EWS que sejam baseadas na cooperação [5] [1] [6]. Utilizar informações vindas de fontes ignoradas, ou inexistentes, a alguns anos atrás como redes sociais (e.g. Twitter – <https://twitter.com>) e registros de plataformas de virtualização de redes (e.g. OpenFlow – <https://www.opennetworking.org/>) também tem mostrado resultados promissores [4] [7] [8] [3].

Neste projeto será desenvolvida uma ferramenta para monitorar atividade maliciosa e detectar antecipadamente eventos e incidentes de segurança. A entrada para a ferramenta virá da correlação e análise de dados providos por sensores de redes tradicionais juntamente com outras fontes de informações, como por exemplo, redes sociais, fóruns e registros de redes virtuais. Mecanismos de redes virtuais também serão utilizados como forma de reagir às ameaças. A ferramenta será utilizada também para monitorar o uso de nomes de instituições em fóruns e redes sociais, alertando possíveis atividades maliciosas.

### **Contribuições e Potencial para se Tornar um Produto/Serviço da RNP**

Como contribuição para a RNP, espera-se que esta ferramenta auxilie nos processos de segurança da informação, em especial detecção e resposta a incidentes de segurança. A ferramenta também poderá ser oferecida como um serviço de detecção de atividade maliciosa e monitoramento de padrões para as instituições usuárias da RNP. Como contribuições científicas espera-se prover a avaliação de novos sensores de rede para obter maior precisão na detecção de novas ameaças, e prover evidências empíricas do uso de técnicas de recuperação de informação para suportar as novas arquiteturas de EWS. Propostas para permitir a cooperação entre instituições também serão fornecidas.

### **Estudos preliminares**

Em estudos preliminares realizados pelos participantes da USP nos últimos dois anos foi confirmado que fontes de informações abertas, como redes sociais, proveem informações relevantes de segurança [4] [8] [3]. Estudos preliminares também confirmaram a utilidade de redes virtuais tanto como sensores quanto como atuadores para EWS [7]. No estágio atual, há necessidade da investigação de técnicas de correlação de eventos para aplicação dos mecanismos preliminares em fluxos reais de redes. Além disso, precisa-se compreender e sistematizar as principais formas de ataques e exploração de vulnerabilidades e avaliar a escalabilidade dos

mecanismos propostos. Por fim, pretende-se investigar o uso de técnicas de aprendizagem de máquinas para investigar e gerar alertas. Alguns dos códigos preliminares desenvolvidos nos últimos dois anos estão disponíveis em <https://github.com/luizsantos/Of-IDPS>.

Estudos preliminares também foram realizados em 2010 quando o coordenador deste projeto foi instrutor do curso “Construindo um Sistema de Alerta Antecipado contra Ataques Cibernéticos” no XVI Seminário RNP de Capacitação e Inovação (<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 distribuída e colaborativa para a detecção antecipada de incidentes de segurança em redes de computadores.

Como objetivos específicos têm-se:

- analisar e sistematizar os ataques e vulnerabilidades mais comuns em redes de computadores;
- investigar as limitações das soluções tradicionais de segurança, tais como IDS, honeypots e firewalls;
- avaliar e selecionar as técnicas de mineração de dados mais efetivas para correlação de eventos gerados por sensores de redes;
- construir novos sensores para obter informações de segurança a partir de fluxos de redes, tais como OpenFlow, redes sociais e fóruns;
- prover um mecanismo para distribuição de dados de sensores de redes e de alertas sem comprometer a qualidade das informações e a privacidade das entidades;
- desenvolver e analisar protótipos de software para os mecanismos de detecção antecipada de incidentes de segurança.

Os objetivos listados anteriormente já se encontram parcialmente desenvolvidos pelos integrantes conforme explicado na subseção **Estudos preliminares**. Entretanto, as implementações e os experimentos realizados até o momento possuem limitações que seriam vencidas caso o projeto fosse aceito pois passaríamos a contar com medidas reais de uma rede de larga escala por meio do serviço Monipê (<http://www.monipe.rnp.br>) além de termos acesso à rede do PlanetLab para mais experimentos em casos onde a rede da RNP não pudesse ser utilizada por questões operacionais. Além do projeto utilizar o serviço de monitoramento já existente na RNP, ele também visará a criação de um serviço de EWS que poderia ser do interesse do Centro de Atendimento a Incidentes de Segurança da RNP (CAIS – <http://www.rnp.br/cais/>). Novos sensores, novos mecanismos para correlacionar as informações desses sensores e novos atuadores poderiam ser de utilidade de vários usuários da RNP e permitiriam a detecção antecipada de atividade maliciosa no backbone acadêmico, a partir de sensores internos distribuídos por diversos pontos da Rede Ipê, além dos sensores de outras fontes de informação na web.

O projeto proposto é inovador por explorar novos fluxos de informações, providos pela grande quantidade de informações disponíveis e compartilhadas na Internet, em especial, em redes sociais, fóruns e sítios Web.

Também inova ao buscar novas formas de correlação de eventos de segurança e investigar e avaliar mecanismos para geração antecipada de alertas.

### **Tarefas dos parceiros**

A função dos professores Daniel, Luiz e Rodrigo no projeto será a de (1) propor novos algoritmos e mecanismos para correlação de eventos de sensores tradicionais de redes e de novos sensores que coletarão informações, por exemplo, de redes sociais e fóruns relevantes; (2) propor novos mecanismos para tomada de decisões autônomicas em redes virtuais com o objetivo de reagir antecipadamente a ataques; (3) coordenar a implantação dos mecanismos em experimentos no PlanetLab e em máquinas do PoP/BA.

A função dos estagiários será implementar protótipos dos mecanismos propostos pelos professores ou, nos casos em que protótipos já estão implementados, como a versão preliminar do controlador OpenFlow que toma ações autônomicas, e do código que faz a classificação de mensagens no Twitter, realizar testes de escalabilidade nesses softwares. Os estagiários serão coordenados diretamente pelos professores.

A função do Ítalo e do Rafael será portar os mecanismos implementados pelos estagiários em novos sensores que atuarão com as informações de monitoramento da rede Ipê (MonIPÊ) a fim de avaliar o seu correto funcionamento em máquinas do PoP/BA e da UFBA. Experimentos realistas também serão projetados e realizados pelos dois.

## **8 Ambiente para testes do protótipo**

Os equipamentos solicitados serão utilizados exclusivamente para o projeto. Os softwares serão desenvolvidos nesses computadores e redes virtuais serão criadas para realização de experimentos com o objetivo de correlacionar dados de diversos sensores. Bases de dados serão construídas nos servidores com coletas de tweets e sites de forma regular. Além disso será necessário acesso ao serviço do Monipê a fim de alimentar as ferramentas que correlacionarão os eventos da rede da RNP juntamente com informações vindas de outras fontes de informação. Finalmente, o acesso ao PlanetLab também será necessário nos últimos 6 meses do projeto a fim de serem avaliadas as ações dos atuadores em uma rede de larga escala.

## **9 Referências**

- [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. Análise de Mensagens de Segurança Postadas no Twitter. In *Anais do Simpósio 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 & IT-Forensics (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 Autônoma para Detecção e Reação a Ameaças de Segurança em Redes de Computadores. In *Anais do III Workshop em Sistemas Distribuídos Autônomicos (WoSiDA) – Workshops do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 1–4. SBC, 2014.
- [8] L. A. F. SANTOS, R. CAMPIOLO, M. A. GEROSA, and D. M. BATISTA. Extração de Alertas de Segurança Postados em Mensagens de Redes Sociais. In *Anais do XXXI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pages 791–804. SBC, 2013.