Proposta para Grupo de Trabalho

GT-Plainc: Plataforma de Análise de Incidentes

Bruno Bogaz Zarpelão

09/08/2013

1. Título

GT-Plainc: Plataforma de Análise de Incidentes

2. Coordenador

Prof. Dr. Bruno Bogaz Zarpelão
Professor Adjunto do Departamento de Computação
Universidade Estadual de Londrina (UEL), Londrina, PR

Currículo Lattes: http://lattes.cnpq.br/0260303520888425

Endereço:
Departamento de Computação/Universidade Estadual de Londrina
Rod. Celso Garcia Cid, S/N
CEP: 86.057-970
Cx. Postal: 10.011
Londrina, PR

Telefone: (43) 3371-5100/(43) 3371-4678

E-mail: brunozarpelao@uel.br

Dr. Rodrigo Sanches Miani
Pesquisador Colaborador do Departamendo de Comunicações/LaRCom
(Laboratório de Redes de Comunicações)

Universidade Estadual de Campinas (UNICAMP), Campinas, SP.

Currículo Lattes: http://lattes.cnpq.br/2992074747740327

Endereço:
Rua João Pandiá Calógeras
Cidade Universitária
13083870 - Campinas, SP - Brasil
Telefone: (19) 35218921 / (34) 98266270

E-mail: rsmiani@decom.fee.unicamp.br

3. Resumo

O crescimento da frequência e do impacto dos incidentes de segurança têm preocupado especialistas e autoridades em todo o mundo. Estes incidentes podem representar grandes prejuízos às organizações, já que soluções de TIC (Tecnologia da Informação e Comunicação) têm sido cada vez mais utilizadas para atender demandas e serviços importantes e estratégicos. A análise dos incidentes de segurança pode levar a melhoria na percepção do problema, facilitando a criação de soluções. Neste projeto, é proposto o desenvolvimento de uma plataforma de análise de incidentes, que emprega redes neurais conhecidas como Mapas Auto Organizáveis para extrair conhecimento de conjuntos de incidentes, de forma a apoiar a tomada de decisões dos administradores de redes. Os relatórios gerados pela análise dos incidentes são apresentados aos administradores de rede de maneira amigável, na forma de mapas e gráficos.

4. Abstract

With the increase in the number and diversity of security incidents, a critical concern for security professionals is to keep their network secure. Such computer security incidents have increased technical and financial consequences as demand for network accessibility and connectivity to ICT (Information and communication technology) resources continues to rise. Careful analysis of security incidents can be conducted to gather sufficient knowledge about the system and provide valuable insights into the overall security. In this project, the development of an incident analysis platform which uses neural networks techniques such as Self Organizing Maps is proposed. The main goal of the proposed platform is to support decision making by extracting knowledge from a security incident dataset. The platform is also able to generate reports for security administrators in a friendly way, with maps and charts.

5. Parcerias

Grupo de Pesquisa em Redes de Computadores e Comunicação de Dados Departamento de Computação - UEL

Este grupo desenvolve trabalhos de pesquisa em diversas áreas como: Gerência de Redes, Gestão de Segurança da Informação, Internet das Coisas e Qualidade de Serviço. Dois pesquisadores deste grupo farão parte do GTPlainc:

- Bruno Bogaz Zarpelão:
  - Doutor em Engenharia Elétrica pela FEEC/UNICAMP.
  - Professor Adjunto do DC/UEL.
  - Currículo Lattes: http://lattes.cnpq.br/0260303520888425.
  - Área de atuação: Serviços Web e Quantificação em Segurança da Informação.
- Mario Lemes Proença Jr.:
  - Doutor em Engenharia Elétrica pela FEEC/UNICAMP.
  - Professor Adjunto do DC/UEL. ○ Currículo Lattes: http://lattes.cnpq.br/9511234560141062.
  - Área de atuação: Gerência e Segurança de Redes de Computadores.
  - Bolsista de produtividade em pesquisa da Fundação Araucária (Fundação de Amparo à Pesquisa do Paraná). ○ Coordenador do Grupo de Pesquisa em Redes de Computadores e Comunicação de Dados do DC/UEL.

Grupo de Pesquisa em Mídia Digitais Departamento de Computação - UEL

Este grupo desenvolve trabalhos de pesquisa em Processamento Digital de Sinais (Imagens, Áudio e Vídeo), Computação Gráfica e Mineração de Texto.

Um pesquisador deste grupo fará parte do GT-Plainc:

- Sylvio Barbon Jr.:
  - Titulação: Doutor em Física Computacional pelo IFSC/USP. ○ Professor Adjunto do DC/UEL.
  - Currículo Lattes: http://lattes.cnpq.br/8086324432194233 ○ Área de atuação: Processamento de Sinais, Mineração de Dados e Inteligência Artificial.

- Um dos coordenadores do Grupo de Pesquisa em Mídias Digitais do DC/UEL.

Cybersecurity Quantification Lab (CyQL) University of Maryland at College Park (EUA)

Este grupo desenvolve trabalhos de pesquisas em quantificação de segurança e estudos empíricos usando dados coletados em diversas universidades e *honeypots* espalhados pelo mundo. Um pesquisador deste grupo fará parte do GT-Plainc:

- Michel Cukier:
  - Titulação: Doutor em Computer Science pelo National Polytechnic Institute of Toulouse.
  - Associate Professor of Reliability Engineering e Associate Director for Education no Maryland Cybersecurity Center at the University of Maryland, College Park.
  - Professor Associado do Departamento de Engenharia Mecânica e Diretor do ACES - Advanced Cybersecurity Experience for Students da University of Maryland, College Park.
  - Área de atuação: Confiabilidade e segurança e Quantificação em Segurança.

Laboratório de Redes de Comunicação (LaRCom) Faculdade de Engenharia Elétrica e Computação – Departamento de Comunicações - UNICAMP

Este grupo desenvolve trabalhos de pesquisa em sistemas de software e hardware para projeto e implantação de infovias municipais, desenvolvimento de software ERP (*Enterprise Resource Planning*) para prefeituras e gerência de redes. Um pesquisador deste grupo fará parte do GT-Plainc:

- Rodrigo Sanches Miani:
  - Doutor em Engenharia Elétrica pela FEEC/UNICAMP.
  - Pesquisador colaborador da FEEC/UNICAMP.
  - Currículo lattes: http://lattes.cnpq.br/2992074747740327.

- Área de atuação: Quantificação em Segurança da Informação, Segurança de Redes e Confiabilidade de Sistemas.

6. Duração do Projeto

Este projeto tem duração de 12 meses.

7. Sumário Executivo

Esta seção apresentará a motivação para o desenvolvimento do projeto, a solução proposta e as principais características da equipe que tornam a execução do projeto viável.

7.1 Motivação

Os recentes ataques de negação de serviço direcionados a instituições financeiras e governamentais realizados pelo grupo *Anonymous*, a descoberta de códigos maliciosos capazes de espionar e controlar sistemas industriais como o *Stuxnet* e o vazamento de informações sigilosas lideradas pelo grupo *Wikileaks* fazem com que haja uma preocupação crescente com as questões relacionadas à segurança da informação. Um relatório disponibilizado pelo departamento de segurança nacional (*Department of Homeland Security* - DHS) dos Estados Unidos [1], mostra que os ataques a computadores estão crescendo não somente em frequência, mas também em impacto.

Esta tendência é reforçada pela publicação de diversas estatísticas sobre incidentes de segurança. As principais fontes de dados de segurança do Brasil são o Centro de Atendimento a Incidentes de Segurança (CAIS), vinculado à Rede Nacional de Pesquisa (RNP) e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Dados de ambas as instituições mostram que, desde o fim dos anos 90, os incidentes de segurança apresentam uma forte tendência de crescimento.

Os desafios enfrentados pelas organizações com relação ao tratamento e prevenção de incidentes de segurança são grandes e exigem muitos cuidados. Algumas consequências relacionadas à ocorrência de incidentes incluem desperdício de tempo e recursos utilizados durante o processo de recuperação do sistema comprometido e roubo de informações confidenciais e prejuízos para

a reputação da empresa, afetando negativamente as ações comerciais ou até diminuindo a confiança do cliente na organização. Com o intuito de diminuir o impacto causado pelos incidentes, diversos meios para analisar e representar a segurança de uma organização são propostos [2]. O emprego da abordagem quantitativa em segurança, em particular, é objeto de discussões dos pesquisadores da área ao longo das últimas duas décadas [3].

A partir do uso de métricas bem definidas, a quantificação permite a descrição precisa e consistente de diferentes objetos de pesquisa. A ideia de quantificação aplicada à segurança da informação envolve desde o desenvolvimento de métricas de segurança até estudos sobre impactos econômicos, avaliação de risco e modelos para medir segurança [2].

Um exemplo simples de pesquisa sobre incidentes de segurança é realizado pelo CAIS/RNP, na forma de gráficos e estatísticas sobre os incidentes reportados em cada ano ou mês. Apesar de interessante, esse tipo de análise oferece apenas uma visão sobre as tendências envolvendo os ataques a computadores. Outros tipos de investigações sobre incidentes precisam ser realizadas a fim de melhorar a percepção do problema. Tópicos como modelagem e previsão de incidentes [4], [5], estudos de fatores que impactam a ocorrência de incidentes [6] e desenvolvimento de modelos para melhorar a detecção de incidentes [7], [8] são alguns exemplos de tópicos de pesquisa nessa área.

Um problema associado à análise quantitativa de incidentes é a ausência de dados acessíveis sobre o assunto. O compartilhamento desse tipo de informação ainda é visto com desconfiança pelos envolvidos [9]. Muitas organizações acreditam que a exposição de informações sobre segurança, mesmo anonimamente, pode eventualmente prejudicar os negócios [10]. Contudo, com o auxílio dos dados de incidentes reportados pelo CAIS/RNP, é possível desenvolver uma plataforma de análise de incidentes semelhante ao Serviço de monitoramento Ipê (MonIPÊ) já em operação na RNP. Nesta plataforma de análise de incidentes, um mapa traria a visão geral da rede com seus PoPs e relatórios sobre os incidentes de cada PoP poderiam ser facilmente acessados pelo usuário.

7.2 Solução Proposta

O objetivo principal deste projeto é propor uma plataforma de análise de incidentes. Com base nessa ideia, primeiramente, este projeto propõe a construção de um Serviço Web para análise de incidentes de segurança utilizando Mapas Auto Organizáveis de Kohonen (*SOM - Self Organizing Maps*) [11], denominado SOM-WS (*Self Organizing Maps Web Service*).

Os Mapas Auto Organizáveis de Kohonen são redes neurais capazes de realizar a classificação não supervisionada de um conjunto de dados de entrada. Estas redes neurais aplicam métodos de aprendizado competitivo que analisam as similaridades e correlações dos dados de entrada, oferecendo como saída a organização destes dados em diferentes classes (*clusters*). Ao aplicar os Mapas Auto Organizáveis de Kohonen sobre conjuntos de dados de incidentes de uma organização, podemos reconhecer padrões de comportamento e correlações entre os incidentes que não seriam facilmente descobertos sem o auxílio de uma ferramenta de mineração de dados. O projeto visa, portanto, construir um processo de extração de conhecimento que permita ao administrador de rede analisar profundamente os incidentes de segurança que ocorrem em sua organização.

Para desenvolvimento do SOM-WS será empregado o padrão arquitetural REST (*Representational State Transfer*) [12]. O REST é um padrão arquitetural que generaliza a arquitetura utilizada na Web. A arquitetura Web e, consequentemente, as arquiteturas construídas com base no REST proporcionam escalabilidade e baixo acoplamento, utilizando princípios simples como a modelagem de elementos do mundo real na forma de recursos, o emprego de URI (*Uniform Resource Identifier*) para identificar os recursos e a transferência de representações destes recursos utilizando protocolos como o HTTP (*Hypertext Transfer Protocol*). Com o REST, fundamentos utilizados com sucesso na Web passaram a ser também utilizados na integração de sistemas distribuídos corporativos. No SOM-WS, as mensagens serão escritas no formato JSON (*JavaScript Object Notation*) [13]. A união do padrão arquitetural REST e do formato JSON representa o estado da arte no desenvolvimento de serviços Web escaláveis e interoperáveis.

Além do SOM-WS, a plataforma de análise de incidentes incluirá um Portal Web que apresentará de maneira amigável os resultados das análises realizadas pelo

SOM-WS. O Portal Web será responsável por intermediar a interação entre o administrador de rede e o SOM-WS. Portanto, este Portal Web permitirá que o administrador de rede requisite relatórios e visualize-os de forma amigável na forma de mapas e gráficos. Além disso, o Portal Web será responsável por permitir que o administrador de rede faça análises baseadas na comparação de diferentes relatórios. Um exemplo seria a comparação de relatórios gerados em períodos diferentes. Em segurança da informação, as condições encontradas podem se modificar ao longo do tempo, de forma que uma análise de relatórios gerados em diferentes períodos pode mostrar mudanças importantes no comportamento das questões de segurança em uma organização.

A visão geral da plataforma de análise de incidentes de segurança é apresentada na Figura 1. A arquitetura da plataforma de análise de incidentes foi projetada para permitir que o Portal Web, o SOM-WS e o banco de dados sejam distribuídos em diferentes servidores, proporcionando maior flexibilidade na construção do ambiente.

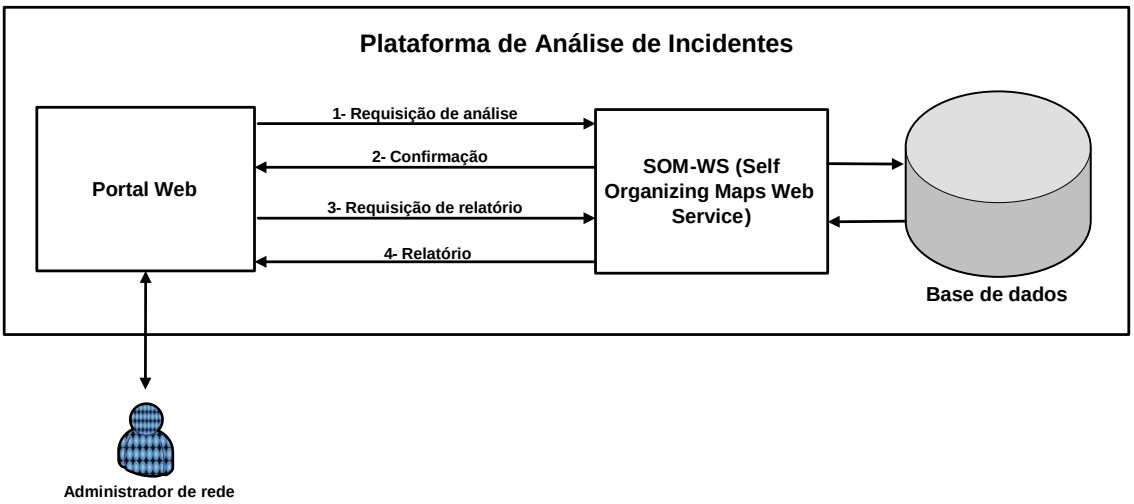

Figura 1 - Visão geral da plataforma de análise de incidentes de segurança.

Quando o administrador de rede requisitar a criação de um novo relatório ao Portal Web, este último enviará uma requisição de análise ao SOM-WS. Esta requisição de análise será enviada do Portal Web para o SOM-WS por meio do método HTTP POST. A requisição será formatada como um documento JSON contendo as seguintes informações:

- Parâmetros do Mapa Auto Organizável de Kohonen como mapa topológico da rede com a organização dos neurônios e taxa de aprendizagem.
- Liste de incidentes com as dimensões que deverão ser analisadas.

Após receber a requisição, o SOM-WS enviará uma confirmação ao portal Web contendo um URI (Uniform Resource Identifier) que deverá ser utilizado posteriormente para acessar os resultados da análise requisitada. Portanto, no SOM-WS, os relatórios das análises serão modelados na forma de recursos identificados por um URI, podendo ser manipulados por meio do HTTP.

Após confirmar o recebimento da requisição, o SOM-WS iniciará a análise dos incidentes com o Mapa Auto Organizável de Kohonen. Assim que a análise terminar, o resultado será armazenado no banco de dados junto com a requisição.

A segunda operação que pode ser executada pelo Portal Web é a recuperação do relatório de uma análise. Para tanto, o Portal Web enviará uma requisição ao SOM-WS utilizando o método HTTP GET e o URI que identifica o relatório.
O SOM-WS responderá a essa requisição com o envio do relatório em um documento JSON.

A fim de ilustrar a operação da plataforma, será apresentado um breve exemplo. Suponha que um administrador da Rede Ipê deseje um relatório sobre os incidentes de uma instituição (ou de um PoP) em um determinado período de tempo. O administrador requisitaria a criação do relatório usando o Portal Web e o SOW-WS realizaria a análise solicitada. Alguns exemplos de dimensões que poderiam ser utilizadas para a realização da análise:

- Tipo do incidente;
- Período de ocorrência do incidente. Exemplo: dias, semanas, meses;
- Volume de ocorrências de incidentes em determinado período;
- Tipo de incidente com o maior número de ocorrências no período;
- Tipo de incidente com o maior número de ocorrências em um período anterior ao período solicitado;
- Tipo de incidente com o maior número de ocorrências em um período posterior ao período solicitado;

Após realizar a análise, o SOM-WS classificaria os incidentes em diferentes classes (*clusters*) e retornaria a informação ao administrador no formato de um relatório. Neste relatório, o administrador poderia visualizar, por exemplo, quais são os tipos de incidentes mais representativos dentro do conjunto analisado e como eles se relacionam com os outros tipos de incidentes.

7.3 Análise de Viabilidade Técnica

Nesta seção, são apresentadas algumas características da equipe do projeto que reforçam a viabilidade de sua execução. A proposta de plataforma de análise de incidentes apresentada neste documento nasceu como desdobramento do trabalho de doutorado de Rodrigo Sanches Miani, coordenador adjunto do Grupo de Trabalho, que foi co-orientado pelo coordenador Bruno Bogaz Zarpelão. Michel Cukier, também presente na equipe do projeto aqui proposto, participou ativamente deste trabalho de doutorado, orientando Rodrigo S. Miani enquanto ele fazia um período sanduíche na University of Maryland, Estados Unidos, em 2011. O trabalho de doutorado de Rodrigo S. Miani, intitulado “Um Estudo sobre Métricas e Quantificação em Segurança da Informação”, inclui entre suas contribuições uma profunda análise de incidentes de segurança reportados pelo CAIS/RNP. Os coordenadores deste projeto trabalham na área de métricas e quantificação de segurança da informação desde 2008, quando publicaram seu primeiro artigo em conjunto intitulado “Metrics Application in Metropolitan Broadband
Access Network Security Analysis”. Portanto, os coordenadores têm reconhecida experiência no tema abordado por este Grupo de Trabalho.

O coordenador do projeto também tem experiência no desenvolvimento de sistemas distribuídos, adquirida em seu doutorado, quando desenvolveu um sistema de detecção de anomalias em redes de computadores, e na participação em projetos do LaRCom enquanto era pesquisador colaborador da FEEC/UNICAMP.

As demandas relacionadas ao desenvolvimento de soluções baseadas em redes neurais serão atendidas pelo Prof. Sylvio Barbon Jr., que tem atuado nesta área nos últimos anos com bons resultados, como pode ser atestado pelas publicações presentes em seu Currículo Lattes. O Prof. Mario Lemes Proença

Jr., por sua vez, tem larga experiência acadêmica na área de gerência e segurança de redes, tendo coordenado projetos de pesquisa com financiamentos aprovados pela Fundação Araucária e pelo CNPq.

8. Recursos Financeiros

8.1 Equipamentos e softwares

Descrição	Quantidade
Desktop na configuração padrão presente no anexo 2 do edital.	6
Notebook com a seguinte configuração: Processador: Intel Core i5 Tela de 14" 4GB RAM HD 320 GB DVD-RW Rede Ethernet 10/100/1000 Rede Wireless 802.11g/n Windows 7 Valor: R$ 3600,00	2

9. Ambiente para o Teste do Protótipo

O protótipo da plataforma será construído no laboratório do Grupo de Pesquisa em Redes de Computadores e Comunicação de Dados da UEL usando dados de incidentes de segurança previamente fornecidos pelo CAIS. Posteriormente, serão realizados os testes dentro do ambiente controlado disponibilizado pela RNP. Os mesmos equipamentos utilizados para desenvolvimento da proposta e adquiridos com recursos deste projeto serão utilizados no teste do protótipo.

10. Referências Bibliográficas

[1] Department of Homeland Security, “Cyber Security Research and Development,” 2011.

[2] V. Verendel, “Quantified security is a weak hypothesis,” in Proceedings of the 2009 workshop on New security paradigms workshop - NSPW ’09, 2009, pp. 37–49.

[3] W. Jansen, “Directions in security metrics research,” NIST Technical Report, 2010.

[4] E. Condon, A. He, e M. Cukier, “Analysis of Computer Security Incident Data Using Time Series Models,” em 2008 19th International Symposium on Software Reliability Engineering, 2008, pp. 77–86.
[5] E. Condon e M. Cukier, “Using Population Characteristics to Build Forecasting Models for Computer Security Incidents,” 2012 IEEE 23rd International Symposium on Software Reliability Engineering, pp. 71–80, Nov. 2012.
[6] J. Zhang, R. Berthier, W. Rhee, e M. Bailey, “Learning from early attempts to measure information security performance,” em Proceedings of the 5th USENIX conference on Cyber Security Experimentation and Test, 2012, pp. 1–10.
[7] R. S. Miani, M. Cukier, B. B. Zarpelão, e L. S. Mendes, “Relationships Between Information Security Metrics : An Empirical Study,” em Cyber Security and Information Intelligence Research Workshop, 2012.
[8] E. Condon, A. He, e M. Cukier, “Analysis of Computer Security Incident Data Using Time Series Models,” em 2008 19th International Symposium on Software Reliability Engineering, 2008, pp. 77–86.
[9] D. Geer, K. Hoo, and A. Jaquith, “Information security: Why the future belongs to the quants,” Security & Privacy, IEEE, vol. 1, no. 4, pp. 24–32, 2003.
[10] A. Jaquith, Security metrics: replacing fear, uncertainty, and doubt. Addison-Wesley Professional, 2007.
[11] Haykin, S. "Redes Neurais: Princípios e Prática", 2. Ed. Porto Alegre: Bookman, 2001.
[12] J. Webber, S. Parastatidis, I. Robinson. "REST in Practice", Ed. O'Reilly, 2010.
[13] JSON. Disponível na Web em: <http://www.json.org/>. Acessado em 07/08/2013.