Um Estudo de Caso em Avaliação de Riscos de Segurança da Informação Utilizando ACO e Redes Bayesianas

Elias P. Silva, Daniel G. e Silva

Departamento de Engenharia Elétrica
Universidade de Brasília (UnB) – Brasília, DF – Brazil

eps.elias@gmail.com, danielgs@ene.unb.br

Abstract. *This work describes the proposal of implementing a Security Risk Analysis Model based on a Bayesian Network built via Ant Colony Optimization. The main advantages of this approach involve the possibilities of relationship analysis between the vulnerabilities, the continuous learning capability through a training database and the possibility of risks re-evaluation when facing new evidences, collected in real time.*

1. Introdução

Independentemente do método adotado para Gestão de Riscos de Segurança da Informação (GRSI), três grandes etapas compõe este processo: Identificação dos Riscos (mapeamento de ameaças, vulnerabilidades, probabilidade de materialização, estimativa de impacto); Mitigação dos Riscos (escolha de estratégias para eliminação ou minimização dos riscos encontrados, considerando que os recursos empregados não podem ser maiores que o possível impacto da ocorrência do risco); Monitoramento do risco (os riscos devem ser continuamente analisados, visto que as ameaças, vulnerabilidades e os próprios ativos alteram-se com o passar do tempo) (Oliveira, 2006).

Neste contexto, existe a necessidade de avaliar o relacionamento dos riscos individuais, pois, embora as vulnerabilidades ocorram separadamente em diferentes áreas e diferentes ativos, uma manifestação conjunta delas pode levar a riscos não considerados sob uma perspectiva isolada. Nas soluções atuais, esse relacionamento não é integrado a fim de gerar uma medida de risco global de determinado sistema computacional, o qual irá depender dos riscos individuais dos *hardwares* e *softwares* que o sustentam.

2. Solução Proposta

Com o objetivo de medir os riscos aos quais estão sujeitos os sistemas computacionais e de fornecer uma forma proativa de tratá-los, foram verificados trabalhos recentes ligados ao Monitoramento Contínuo do Risco. Dentre tais pesquisas, destaca-se o modelo Security Risk Analysis Model (SRAM) proposto por N. Feng, H. Wang e M. Li (2014).

Este modelo propõe uma abordagem para avaliação contínua do risco, considerando um banco de dados histórico de casos, as definições de especialistas sobre diferentes áreas de vulnerabilidades e o recebimento de novos dados, em tempo real. A partir destas fontes de dados constrói-se uma rede Bayesiana que define os fatores de risco e seus relacionamentos causais. Um algoritmo de otimização por colônia de

formigas é utilizado para inferir o modelo da rede e para realizar a análise de propagação das vulnerabilidades encontradas, determinando os caminhos com maior probabilidade de ocorrência e com maior risco estimado. A Figura 1, adaptada de (Feng et al., 2014), representa as diferentes etapas do modelo SRAM.

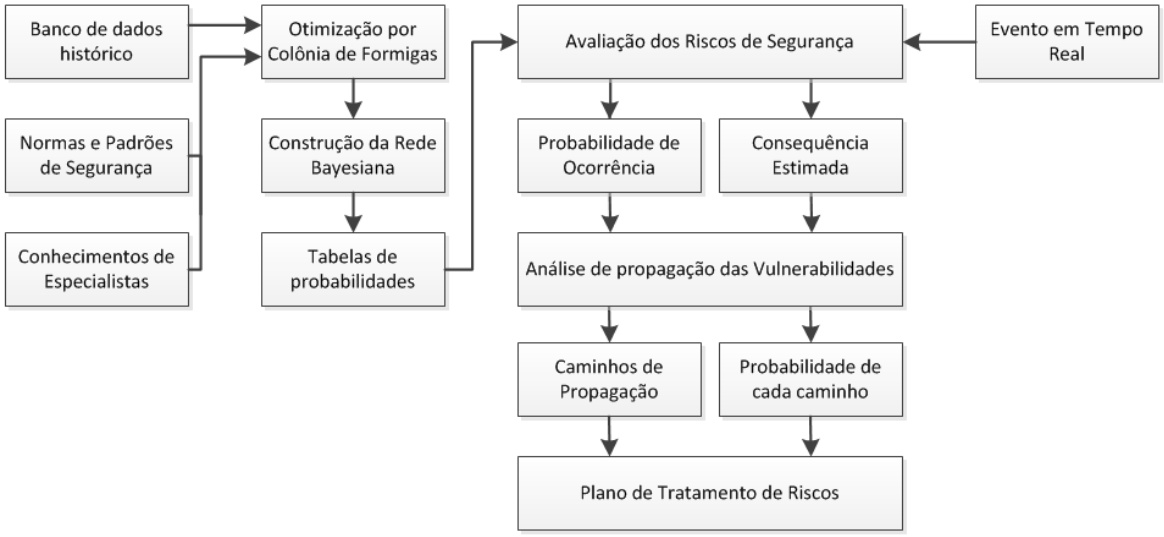

Figura 1. Modelo SRAM (adaptada de (Feng et al, 2014))

Inicialmente, são criados dois bancos de dados (BD1 e BD2), o primeiro armazena um conjunto de controles de segurança definidos por normas e conhecimentos de especialistas. Já o segundo banco contém um registro histórico dos controles definidos no primeiro banco de dados. Em uma adaptação ao modelo apresentado em (Feng et al, 2014), são considerados na proposta deste trabalho os controles de segurança derivados da norma NBR ISO/IEC 27002 (ABNT, 2006).

Após a construção das duas bases de dados, deve ser utilizada a técnica proposta por (Campos et al., 2002), a qual consiste na inferência de redes Bayesianas a partir de otimização baseada em colônia de formigas. Neste caso, determina-se por meio de um esquema de pontuação a rede Bayesiana que melhor dispõe seus nós aos dados históricos (cada nó corresponde a um controle de segurança). Em seguida, são calculadas as tabelas de probabilidade condicional dos nós com dependências.

Construída a rede, um terceiro banco de dados (BD3) entra em cena, o qual armazena os eventos em tempo real relacionados com cada controle de segurança. Quando um evento ocorre, calcula-se o risco gerado em relação à probabilidade de ocorrência e suas consequências. Caso esse valor ultrapasse o limite definido pelos especialistas, o sistema inicia uma análise de propagação desta vulnerabilidade.

Esta análise também utiliza otimização por colônia de formigas e possui o objetivo de determinar o caminho pela rede com maior probabilidade de ocorrência e maior exposição ao risco. Assim, baseando-se no resultado da análise de propagação, é possível desenvolver um plano para tratamento dos riscos encontrados e priorizados pela técnica.

3. Considerações Finais

No contexto apresentado, propõe-se a aplicação do modelo SRAM, utilizando como fonte de dados o monitoramento de sistemas computacionais em produção na Polícia Federal, a fim de analisar e validar a efetividade deste modelo em comparação com outras ferramentas bem estabelecidas (ex.: AlienVault Unified Security Management, McAfee Enterprise Security Manager, HP ArcSight SIEM) e, não obstante, verificar se a análise de propagação dos riscos proposta proporciona benefícios relevantes em termos da gestão de segurança dos sistemas de informação, atuando como uma ferramenta de suporte à tomada de decisão.

Face à importância da utilização de dados reais frente à publicação de novas abordagens para análise de risco de segurança da informação, propõe-se a escolha de alguns sistemas computacionais utilizados pela Polícia Federal e a avaliação do modelo SRAM para cada sistema escolhido. Desta forma, os eventos isolados de diferentes *hardwares* e *softwares,* que constituem cada sistema escolhido, são avaliados de modo a fornecer uma medida conjunta da possibilidade de sua ocorrência e mensurar os impactos ao serviço de TI.

Referências

ABNT (2005) NBR ISO/IEC 27002. Tecnologia da informação – Técnicas de segurança – Código de prática para gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

ABNT (2006) NBR ISO/IEC 27001. Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2006.

Campos, L., Fernández-Luna, J. Gaméz, J. Puerta, J. (2002) “Ant colony optimization for learning Bayesian networks”. International Journal of Approximate Reasoning. 31, 291-311, 2002.

Feng, N., Wang, H. J., Li, M. (2014) “A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis”. *Information Sciences*. v. 256, p. 57–73, jan. 2014.

Kavanagh, K., Rochford, O. (2015). “Magic Quadrant for Security Information and Event Management”. Gartner database, ID G00267505, jul. 2015.

Oliveira, V. L. (2006) “Uma análise comparativa das metodologias de gerenciamento de risco FIRM, NIST SP 800-30 e OCTAVE”. Dissertação de Mestrado, UNICAMP, Campinas, Brasil, 2006.