UMA ABORDAGEM ONTOLÓGICA PARA CIÊNCIA DE SITUAÇÃO NO DOMÍNIO DE SEGURANÇA DA INFORMAÇÃO

DIÓRGENES YURI LEAL DA ROSA[1]; RICARDO BORGES ALMEIDA[1]; ROGER DA SILVA MACHADO[1], ADENAUER CORRÊA YAMIN[1]; ANA MARILZA PERNAS[1]

[1]*Universidade Federal de Pelotas – {diorgenes, rbalmeida, rdsmachado, adenauer, marilza}@inf.ufpel.edu.br*

1. INTRODUÇÃO

Tendo em vista o aumento de conectividade e de tráfego característico à computação ubíqua (UbiComp) e à Internet das Coisas (*Internet of things* - IoT), o sensoriamento necessário à Segurança da Informação (SI) por vezes não é acompanhado de forma adequada. Isto pode ser verificado principalmente quando não são exploradas técnicas voltadas a ciência de situação (CS) que desonerem o administrador de tarefas de inspeção rotineira. A relação existente entre SI e CS pode ser observada pelo conceito de *Network Security Situational Awareness* (NSSA), uma terminologia usada para descrever CS aplicada a segurança de redes de computadores que visa proporcionar conhecimento sobre situações de risco, otimizando o processo de tomada de decisões (ONWUBIKO, 2009).

Neste sentido, várias alternativas voltadas a CS têm sido exploradas no domínio de SI. Dentre estas, o uso de ontologias tem assumido destaque nas etapas de modelagem e processamento de dados de contexto, permitindo representação computacional do conhecimento, realização de inferências, aplicações de regras e correlações entre os dados. As ontologias podem propiciar visualização das situações em alto nível, auxiliando a etapa de compreensão e alinhando-se com o domínio em questão, observado o grande número de informações de interesse sensoriadas constantemente e a diversidade em seus formatos.

Diversos trabalhos exploram o uso de ontologias no domínio de SI, como o OntoSec (MARTIMIANO; MOREIRA, 2006); o sistema multiagente autonômico AutoCore (AZEVEDO et al., 2012) que tem ontologias voltadas a análise de risco e requisitos de SI; a abordagem para percepção de status de rede (BHANDARI, 2014) e o framework ontológico utilizado em (LASHERAS et. al., 2009) para fins de classificação.

O presente trabalho tem como objetivo principal a concepção de um módulo ontológico voltado a CS no domínio de SI, mais especificamente na fase de compreensão, que explore os recursos de expressividade das regras semânticas providas pelo emprego de ontologias, visando auxiliar no monitoramento de situações de SI possíveis em ambientes de UbiComp. Esta iniciativa visa uma contribuição para com a abordagem EXEHDA-USM (Execution Environment for Highly Distributed Applications - Unified Security Management) (ALMEIDA, 2016), em desenvolvimento pelo LUPS (*Laboratory of Ubiquitous and Parallel Systems*), no âmbito do Projeto SCALE (*Smart Context-Aware Social Environments*).

2. METODOLOGIA

A arquitetura EXEHDA-USM, base para o presente trabalho, é estabelecida por três componentes de software em Python, sendo denominados Collector, SmartLogger e Manager. Estes componentes são autônomos e respeitam uma

hierarquia, sendo o Collector ligado ao EXEHDAnodo e o SmartLogger e Manager ligados ao EXEHDAbase, ambos definidos no middleware que consolida o projeto, o EXEHDA (LOPES, J. L. et. al., 2014). Uma vez coletados os dados são encaminhados para o SmartLogger, onde ocorre processamento dos dados e armazenamento, entre outras funcionalidades.

Os eventos analisados pela abordagem EXEHDA-USM consistem de logs de serviços de rede ou de soluções de segurança e de estatísticas de uso dos recursos computacionais. Estes eventos possuem diferentes formatos e são utilizados como base para a identificação de situações de interesse utilizando uma estratégia de correlação de eventos baseada em regras na etapa de compreensão. Dentre as soluções de segurança responsáveis pela produção dos eventos analisados pela abordagem é possível destacar: Network-based Intrusion Detection System (NIDS), Host-based Intrusion Detection System (HIDS), Web Application Firewall (WAF) e/ou Network Performance Monitoring and Diagnostics (NPMD). Estes eventos são coletados na fase de Percepção passam para o módulo de pré-processamento para normalização, contextualização, priorização e categorização dos dados, iniciando a fase de Compreensão. Continuando a fase de Compreensão utiliza-se o Esper como técnica de CEP (Complex Event Processing) para analisar os dados recebidos por intermédio de regras pré-definidas. As situações que incorrem nas regras podem instanciar o módulo ontológico em desenvolvimento.

Na figura 1 identificam-se as 3 fases de CS (ENDSLEY, 2000) comuns a todos os componentes de software desenvolvidos: Percepção, Compreensão e Projeção. Também é demonstrado um fluxo dos eventos, já com a atuação do módulo ontológico na fase de Compreensão. O processamento que ocorre no Esper é o aspecto que oportuniza a contribuição deste trabalho, instanciando a ontologia com situações já tratadas e com maior contextualização. O módulo ontológico, por sua vez, pode proporcionar sugestões de contramedidas aos atuadores da fase de Projeção.

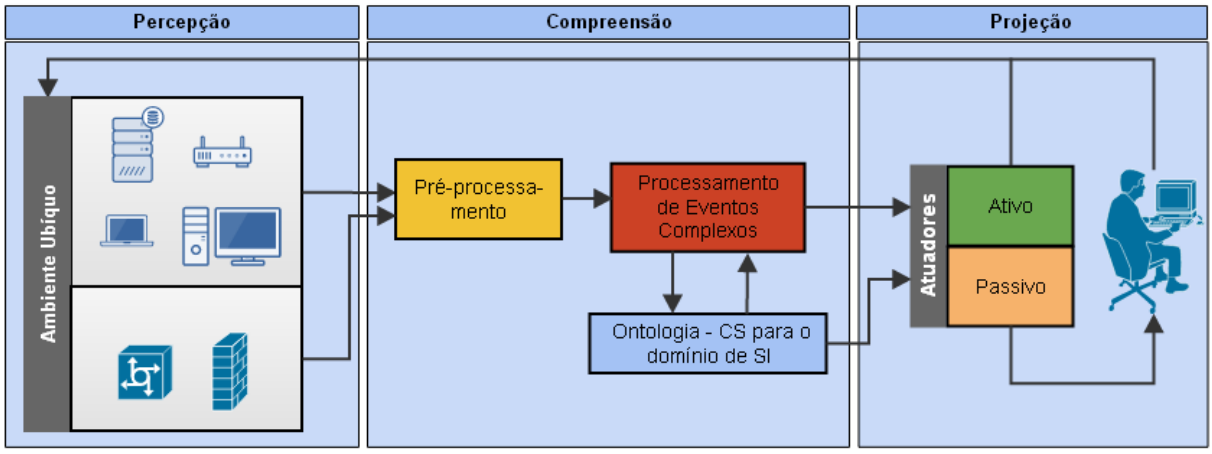

Figura 1 - Fases de CS no processo proposto

Para o desenvolvimento do módulo ontológico tem-se feito uso da ferramenta Protégé[1] e a formalização em OWL[2], recomendação da W3C[3], bem como consultas SparQL[4]. Para o estabelecimento dos conceitos, classes e

[1] Protégé - http://protege.stanford.edu
[2] OWL - Web Ontology Language
[3] W3C - World Wide Web Consortium
[4] SparQL – Linguagem de Consulta para RDF

relações desenvolvidas foram observados diversos trabalhos relacionados sempre adaptando o desenvolvimento às necessidades do projeto e à ISO 27002, que estabelece boas práticas para o gerenciamento de SI.

2. RESULTADOS E DISCUSSÃO

O módulo ontológico proposto neste trabalho atua a partir do SmartLogger, por ter um poder computacional maior e já dispor de dados contextuais mais ricos oriundos de diversos Collector's adjacentes. Em último momento, os dados dos n SmartLogger's são centralizados no Manager, onde é possível uma visão geral da SI do ambiente ubíquo.

Considera-se o uso de ontologias como ferramenta complementar ao módulo de compreensão da EXEHDA-USM para o processamento de eventos e situações, fornecendo uma abordagem híbrida de processamento de eventos, considerando que a abordagem já utiliza CEP baseada em regras. Desta forma propõe-se o ontológico compondo a fase de compreensão, atuando em conjunto com o Esper[5]. A medida busca solucionar a questão de processamento das ontologias para elevado número de eventos, sendo que as situações chegariam em menor quantidade, com filtros já aplicados. A figura 2 mostra o estágio atual de desenvolvimento do módulo ontológico onde pode-se ver as principais classes e relações entre as mesmas.

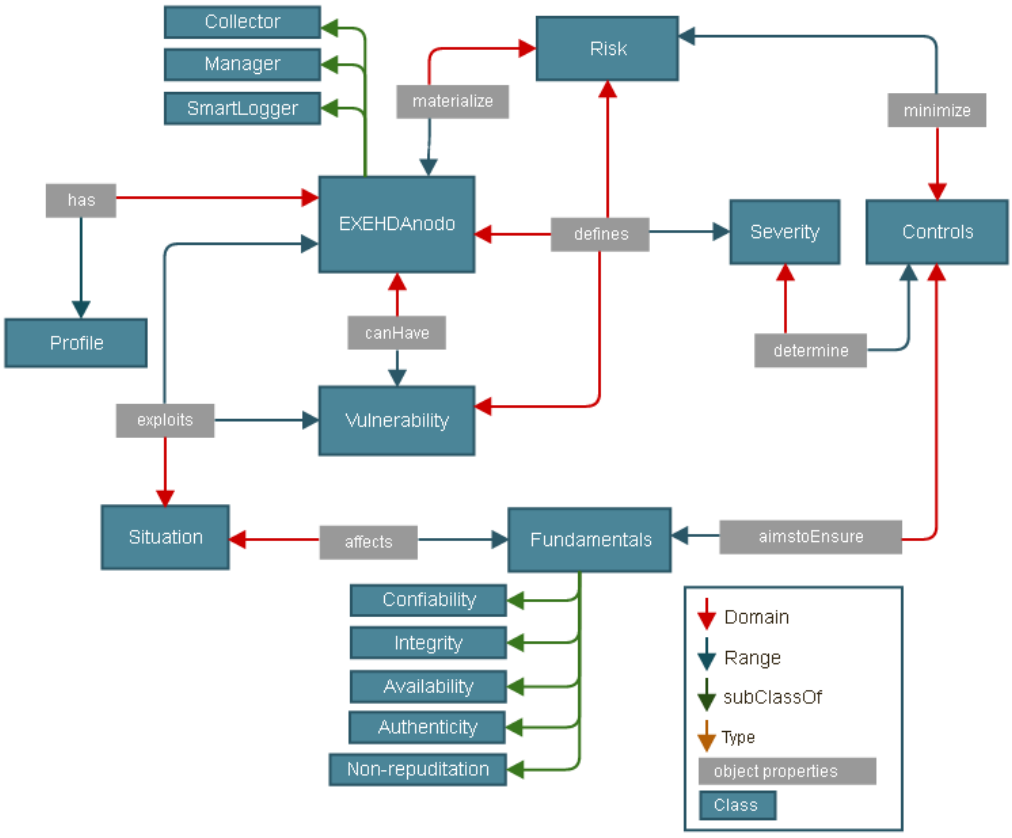

Figura 2 - Ontologia em desenvolvimento

4. CONCLUSÕES

A partir dos trabalhos relacionados percebe-se o aproveitamento das funcionalidades das ontologias na direção das demandas da CS em SI pela sua:

[5] ESPER - http://esper.codehaus.org

(i) capacidade de alcançar entendimento compartilhado da informação estruturada, que pode ser fundamentada e analisada automaticamente por seres humanos e agentes de software; (ii) habilidade de especificar várias relações semânticas entre diferentes conceitos; (iii) potencialidade em solucionar questões de interoperabilidade, visto a heterogeneidade tecnológica atual em termos de software e hardware; e (iv) reusabilidade e evolução ao longo do tempo.

A identificação deste alinhamento deixa clara a potencialidade das ontologias voltadas a CS em SI, sobretudo em sua fase de compreensão. Este trabalho apresentou um modelo ontológico para informações contextuais em desenvolvimento, e as adaptações necessárias para a integração deste na abordagem EXEHDA-USM visando proporcionar aos analistas de segurança sugestionamentos de contramedidas e uma visão alto nível de situações de interesse.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, R. B. **EXEHDA-USM: uma arquitetura hierárquica multinível consciente de situação aplicada a segurança da informação**. 2016. Dissertação (Mestrado em Computação). Programa de Pós-graduação em Computação. Universidade Federal de Pelotas.

AZEVEDO, R.; DIAS, G.; FREITAS, F.; VERAS, W.; RODRIGO, R. Um sistema autonomico baseado em ontologias e agentes inteligentes para uso em segurança da informação. **Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação**, [S.l.], v.17, n.35, p.167–184, 2012.

BHANDARI, P.; GUJRAL, M. Ontology based approach for perception of network security state. In: ENGINEERING AND COMPUTATIONAL SCIENCES (RAECS), 2014 RECENT ADVANCES IN, 2014. **Anais...** [S.l.: s.n.], 2014. p.1–6.

ENDSLEY, M. R. Theoretical underpinnings of situation awareness: a critical review. In: ENDSLEY, M. R.; GARLAND, D. J. (Ed.). **Situation Awareness Analysis and Measurement. Mahwah**, NJ, USA: Lawrence Erlbaum Associates, 2000.

LASHERAS J.; VALENCIA-GARCIA R.; FERNÁNDEZ-BREIS J. T.; TOVAL A. Modelling Reusable Security Requirements based on an Ontology Framework. Journal of Research and Practice in Information Technology

LOPES, J. L., de SOUZA, R. S., GEYER, C. F. R., da COSTA, C. A., BARBOSA, J. L., PERNAS, A. M., & YAMIN, A. C. (2014). A Middleware Architecture for Dynamic Adaptation in Ubiquitous Computing. J. UCS,20(9), 1327-1351

MARTIMIANO, L. A. F.; MOREIRA, E. The Evaluation Process of a Computer Security Incident Ontology. In: THE 2ND WORKSHOP ON ONTOLOGIES AND THEIR APPLICATIONS, RIBEIRAO PRETO, 2006. **Anais...** [S.l.: s.n.], 2006.

ONWUBIKO, C. **Functional requirements of situational awareness in computer network security.** In: INTELLIGENCE AND SECURITY INFORMATICS, 2009. ISI ’09. IEEE INTERNATIONAL CONFERENCE ON, 2009. **Anais...** [S.l.: s.n.], 2009. p.209–213.