UMA ABORDAGEM COMPOSICIONAL PARA CORRELACIONAR INFORMAÇÕES CONTEXTUAIS PRESENTES EM DIFERENTES MODELOS

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

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

1. INTRODUÇÃO

Ao se construir e executar aplicações ubíquas cientes de contexto há uma série de funcionalidades que devem ser providas, envolvendo desde a aquisição de informações contextuais a partir de fontes heterogêneas e distribuídas, até a representação dessas informações, seu processamento, armazenamento e a realização de inferências para seu uso em tomadas de decisão (BELLAVISTA et al., 2012).

A construção de sistemas cientes de contexto exige, inicialmente, a definição do que considerar como contexto, onde este se aplica e que informações são necessárias para descrevê-lo. Considerando a escalabilidade das infraestruturas computacionais modernas, é preciso viabilizar a aquisição de contexto da forma mais automática possível. Após a coleta de dados brutos a partir do sensoriamento, tornam-se necessários mecanismos de processamento de contexto que tratem as informações coletadas, produzindo informações contextualizadas (BAUER et al., 2014).

Atualmente, as aplicações cientes de contexto tendem a tratar com dados de diferentes naturezas, onde os mesmos podem ser modelados utilizando diversas abordagens. Nesta perspectiva, se observa uma tendência na utilização de repositórios com diferentes modelos de armazenamento, chamados de modelos híbridos (PERERA et al., 2013), (YU et al., 2014), pois muitas vezes a utilização de somente um modelo para armazenamento das informações contextuais pode ter impactos negativos em aspectos ligados a desempenho, utilização de disco, expressividade na representação dos dados contextuais, entre outros (CARVALHO, 2014), (KOTENKO et al., 2013).

Os modelos híbridos trazem consigo desafios de pesquisa relacionados a forma com que é realizada a manipulação dos dados contextuais, tendo em vista a necessidade de acesso e processamento de dados provenientes de diferentes modelos.

Com esta motivação, foi concebida uma estratégia de processamento composicional de contexto, a qual possui como diferencial a capacidade de correlacionar as informações presentes em diferentes modelos de contexto. A abordagem proposta tem como premissa sua integração ao middleware EXEHDA (LOPES et al., 2014), contribuindo com o seu Subsistema de Adaptação e Reconhecimento de Contexto.

2. METODOLOGIA

A estratégia de processamento composicional foi concebida tendo por base o emprego de tags de marcação, as quais são utilizadas na criação das regras que manipulam diferentes modelos contextuais. As *tags* são identificadas pelo símbolo “#” seguido de um número que representa a consulta responsável por

buscar as informações desejadas no RHIC (Repositório Híbrido de Informações Contextuais).

Quando do procedimento de composição, as *tags* são substítuidas pelo conteúdo do atributo especificado na consulta. Também é facultada a verificação se uma determinada consulta possui retorno, empregando o método que devolve o boleano "*true*", caso positivo, e "*false*", caso contrário.

A camada de processamento realiza a execução da regra composicional seguindo um fluxo específico de processamento, conforme pode ser visualizado na Figura 1. Primeiramente é buscada a regra desejada no RHIC, após, são identificadas as consultas auxiliares que devem ser realizadas, tendo como intuito buscar os dados necessários no RHIC para substituição das tags de marcação presentes na regra que está sendo processada.

Posteriormente, com o retorno das consultas auxiliares, a regra é composta pelos valores necessários e sua avaliação é realizada, tendo como retorno o comando a ser executado, e cujo identificador encontra-se na própria regra. Com isso, é necessário buscar o comando desejado no RHIC e, então, executar o comando retornado.

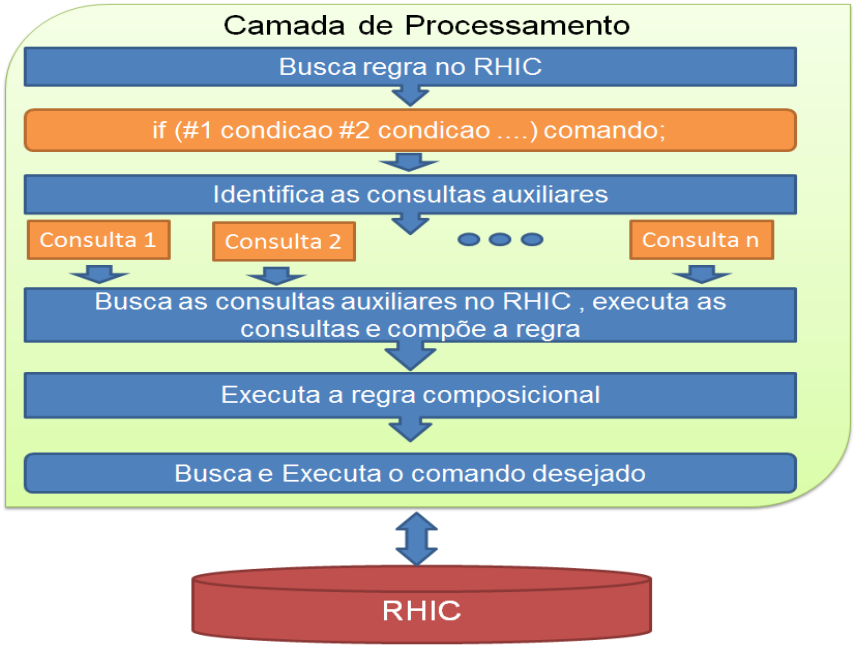

Figura 1: Fluxo de execução da regra composicional

Destaca-se que as regras composicionais podem ser compostas de dados armazenados nos diferentes modelos, tornando a consulta mais expressiva e, em consequência, facilitando à aplicação identificar situações de interesse. Caracteriza-se ainda a melhora na atualização e manutenção das regras criadas, pois, caso mais de uma aplicação utilize as mesmas regras só é necessário atualizar seu conteúdo em um determinado campo e todas estarão atualizadas. Além disso, os comandos que determinam as ações decorrentes das situações não são definidos nas regras, mas em uma tabela no RHIC, o que facilita a reutilização e manutenção dos mesmos.

3. RESULTADOS E DISCUSSÃO

Visando avaliar a abordagem de processamento composicinal, foi proposta a sua utilização em um cenário de segurança da informação, de forma mais precisa,

no reforço de políticas de segurança. Sabe-se que um dos desafios relacionado as politicas de segurança é a sua implementação e, mais especificamente, a verificação da sua conformidade. Por exemplo, como verificar se os usuários estão em conformidade com a política de senhas.

Desta forma, este estudo de caso explora a ISO 27002 que apresenta um código de prática para a gestão da segurança da informação. Com isso foi empregada uma ontologia baseada em (ALCÁZAR; FENZ, 2012), a qual é responsável por mapear a estrutura da ISO 27002, incluindo seus controles, ativos, ameaças e vulnerabilidades. A ontologia foi armazenada no modelo de triplas presente no RHIC, com o intuito de facilitar o acesso a estas informações.

Como fonte para a aquisição de contexto, foi explorado o monitoramento dos logs de um *Web Application Firewall* que foi devidamente configurado para identificar quebras na política de senhas de aplicações web. Após o tratamento do log é realizada a identificação da situação de interesse caracterizada pela mensagem "*password does meet complexity requirements*", e por último, a situação identificada é armazenada no modelo não relacional do RHIC, já que as situações possuem um formato semiestruturado.

Com a situação já identificada e armazenada no RHIC, pode ser utilizada a estratégia de processamento composicional com a execução da regra *if(#3 && #4) "b"*. A *tag #3* é substituída pela consulta que busca no modelo não relacional as situações com o atributo "*subcategory*" igual a "*ComplexityRequirements*". A *tag #4* representa a consulta SPARQL (*SPARQL Protocol and RDF Query Language*) que busca os controles a serem sugeridos que estão relacionados a ComplexityRequirements de acordo com a ontologia da ISO 27002 e as propriedades *controlStatement*, *implementationGuidance*, *otherInformation* onde estão inseridas as informações a respeito de cada controle que foi sugerido.

Como condição a ser executada na regra composicional, foi utilizado o método que verifica se foi retornado algum resultado na consulta. O comando previamente configurado para ser executado, caso seja detectada a situação, é representado por "b", sendo este referente ao envio de e-mail para os analistas de segurança da informação. Este e-mail é composto de uma mensagem de notificação de incidente, junto aos controles que constam na ontologia da ISO 27002 que servirão como sugestões de melhorias a serem empregadas, sendo os analistas responsáveis por avaliar a necessidade de tomada de ações para reforçar a política de senhas.

4. CONCLUSÕES

Neste trabalho foram tratados os desafios enfrentados pelas aplicações cientes de contexto com o emprego de modelos híbridos, onde destaca-se a ausência de uma estratégia que permita utilizar os contextos presentes nos diferentes modelos utilizados. Com estes desafios em vista, as seguintes contribuições foram alcançadas com o desenvolvimento deste trabalho: (i) a concepção de uma abordagem com suporte a modelagem híbrida de contexto; (ii) o desenvolvimento de uma estratégia de processamento composicional de contexto, a qual possui como diferencial a possibilidade de correlacionar os dados presentes nos diferentes modelos de armazenamento utilizados.

Com a utilização da abordagem de processamento composicional aumenta-se a flexibilidade e a expressividade da aplicação, permitindo que sejam utilizados em uma mesma regra dados armazenados nos diferentes modelos, melhorando a identificação de situações de interesse.

O estudo de caso explorou a aplicação da abordagem de processamento em um escopo de atual relevância devido ao aumento das preocupações com segurança da informação nas instituições. Com o emprego da abordagem proposta foi possibilitada a correlação das situações armazenadas no modelo não-relacional com as informações presentes na ontologia da ISO 27002, tendo como resultado a indicação de controles de segurança aos analistas.

Dentre os aspectos levantados para continuidade do trabalho, podem ser citados: (i) realizar estudos de ferramentas para processamento de eventos complexos e suas respectivas sintaxes, tendo como intuito avaliar alternativas às regras utilizadas que seguem o padrão do condicional if; (ii) aplicar a abordagem proposta em diferentes cenários de utilização, por exemplo, em ambientes educacionais, os quais costumam utilizar tanto os modelos baseados em ontologias quanto os modelos relacionais.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ALCÁZAR, F.; FENZ, S. **Mapping ISO 27002 into Security Ontology**. Treball final de grau – Universitat Politècnica de Catalunya. Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels. Departament de Teoria del Senyal i Comunicacions, 2012.

BAUER, J. S., NEWMAN, M. W., AND KIENTZ, J. A. (2014). Thinking about context: Design practices for information architecture with context-aware systems. In **iConference 2014 Proceedings**, pages 398–411.

BELLAVISTA, P.; CORRADI, A.; FANELLI, M.; FOSCHINI, L. A survey of context data distribution for mobile ubiquitous systems. **ACM COMPUTING SURVEYS**, New York, NY, USA, v.44, n.4, p.24:1–24:45, Sept. 2012.

CARVALHO, A. G. **Interface NoSQL integrada a banco relacional para gerenciamento de dados em nuvem privada**. 2014. Monografia Bacharelado em Engenharia da Computação — Centro Universitário de Brasília Faculdade de Tecnologia e Ciências Sociais Aplicadas.

KOTENKO, I.; POLUBELOVA, O.; SAENKO, I. The Ontological Approach for SIEM Data Repository Implementation. **In: IEEE INTERNATIONAL CONFERENCE ON GREEN COMPUTING AND COMMUNICATIONS (GREENCOM '12)**, 2012.

LOPES, J.; SOUZA, R.; GEYER, C.; COSTA, C.; BARBOSA, J.; PERNAS, A.; YAMIN, A. A Middleware Architecture for Dynamic Adaptation in Ubiquitous Computing. **JOURNAL OF UNIVERSAL COMPUTER SCIENCE**, 2014.

PERERA, C.; ZASLAVSKY, A.; CHRISTEN, P.; GEORGAKOPOULOS, D. Context Aware Computing for The Internet of Things: A Survey. **Communications Surveys Tutorials, IEEE**, v.16, n.1, p.414–454, First 2014.

YU, H. Q.; ZHAO, X.; ZHEN, X.; DONG, F.; LIU, E.; CLAPWORTHY, G. (2014). Healthcare-Event driven semantic knowledge extraction with hybrid data repository. In **INNOVATIVE COMPUTING TECHNOLOGY (INTECH)**, 2014 Fourth International Conference.