Arquitetura de monitoramento para Security-SLA em Nuvem Computacional do tipo SaaS

Carlos Alberto da Silva[1], **Paulo Lício de Geus**[1]

[1] Instituto de Computação – Universidade Estadual de Campinas (Unicamp)
{ beto, paulo}@lasca.ic.unicamp.br

Abstract. *Cloud Computing has introduced new technology and architectures that changed enterprise computing. In particular, when hiring a service in the cloud, an important aspect is how security policies will be applied in this environment characterized by both virtualization and large-scale multi-tenancy service. Security metrics can be seen as tools to provide information about the status of the environment. Aimed at improving security in cloud, this paper presents an architecture for security monitoring based on Security-SLA for SaaS services.*

Resumo. *Nuvem Computacional introduziu novas tecnologias e arquiteturas que modificaram a computação empresarial. Em particular, ao contratar um serviço na nuvem, um aspecto importante é a forma como as políticas de segurança serão aplicadas neste ambiente caracterizado pela virtualização e serviço de multilocação em grande escala. Métricas de segurança podem ser vistas como ferramentas para fornecer informações sobre o estado deste ambiente. Visando a melhoria da segurança em nuvens, este artigo apresenta uma arquitetura para monitoramento de segurança baseado em Security-SLA para serviços SaaS.*

Palavras chaves: Métricas de Segurança, Security-SLA, Segurança em Nuvem.

1. Introdução

Nuvem Computacional define-se como um modelo para permitir acesso fácil, a rede sob demanda para um conjunto compartilhado de recursos configuráveis de computação como: redes, servidores, armazenamento, aplicações e serviços, que podem ser rapidamente provisionados e liberados com um esforço mínimo de gerenciamento ou interação com o provedor destes serviços. Os três tipos principais de serviços oferecidos por provedores de nuvem computacional são: Infraestrutura-como-um-serviço (IaaS), Plataforma-como-um-Serviço (PaaS) e Software-como-um-Serviço (SaaS).

Os potenciais clientes de nuvem percebem uma ausência de transparência e uma relativa falta de controles, quando comparado com os modelos tradicionais [Pearson 2013].

As qualidades especificadas em um Security-SLA podem ser classificadas em mensurável e não mensurável. As qualidades mensuráveis são medidas automaticamente por meio de métricas, e as qualidades não mensuráveis não permitem uma medição automática, ou através de um método que resulta em um valor único. As qualidades encontradas em serviços de TI são: (a) Mensuráveis: precisão, disponibilidade, capacidade, custo,

latência, tempo de provisionamento, confiabilidade e escalabilidade; (b) Não mensurável: interoperabilidade, modificabilidade e segurança.

Diante deste cenário, este trabalho apresenta uma solução de monitoramento que acompanha os acordos de nível de serviço de segurança, Security-SLA, utilizando um sistema de monitoramento de segurança que baseia-se em uma hierarquia de métricas de seguranças para Infraestrutura e Serviço contratado, e discute também a utilização de escala de valores para tratar o problema de aferir qualidades não mensuráveis.

2. Trabalhos Relacionados

Atualmente, as soluções comerciais de monitoramento permitem apenas o monitoramento de informações básicas como carga de CPU, uso de espaço de armazenamento e tráfego de rede, tais como: (i) plataforma AWS da *Amazon* oferece o *CloudWatch*, um sistema de monitoramento oferecido como um serviço para o controle de recursos; (ii) *Microsoft Windows Azure* possui o *Azure Fabric Controller* que monitora e gerencia os recursos e serviços dos servidores; (iii) *Google App Engine* oferece um conjunto de APIs que permitem a utilização de soluções de monitoramento como o *CloudStatus*; (iv) assim como as soluções de nuvens de código aberto como: *Eucalyptus*, *OpenNebula* e *OpenStack*.

Na área acadêmica, o monitoramento da nuvem computacional apresenta poucos resultados concretos [Shao et al. 2010], e os sistemas de monitoramento são voltados para o monitoramento de aplicações específicas, e não estão associados ao acompanhamento dos acordos de Security-SLA.

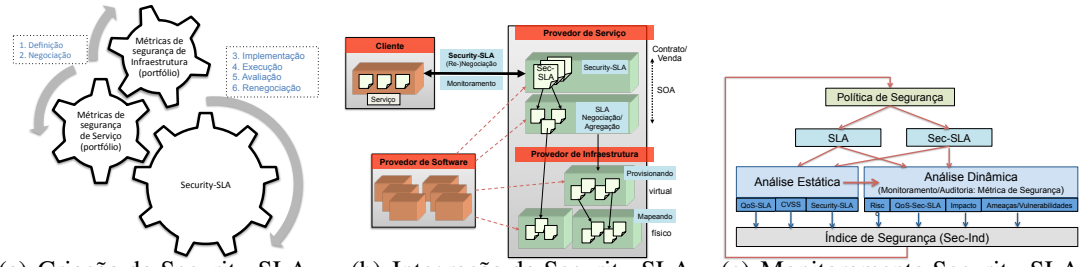
Em Emeakaroha et al. [Emeakaroha et al. 2010] apresentam a solução de monitoramento baseada no protocolo SNMP e métricas de desempenho, que são posteriormente utilizadas por um módulo de detecção de violação do acordo de SLA.

3. Solução de Monitoramento

A solução de monitoramento proposta tem o objetivo de acompanhar o cumprimento de acordos de Security-SLA para nuvem SaaS, e é dividida em: [1a parte] o monitoramento ocorre nos dispositivos de infraestrutura da nuvem, como: *firewalls*, roteadores, comutadores, *proxies*, etc.; [2a parte] o monitoramento ocorre sobre o serviço contratado utilizando técnicas de monitoramento de caixa-preta ou a introspecção da Maquina Virtual (VM), que permitem a coleta de informações sem a necessidade de instalação de ferramentas no sistema operacional da VM. O mecanismo de Introspecção da VM da biblioteca LibVMI permite o acesso aos aspectos da VM no *hypervisor* como: memória, utilização do processador, entradas e saídas de dados [VMITools 2013].

Esta solução apresenta o acordo de Security-SLA através de uma linguagem XML que permite especificar os serviços e as políticas de segurança que serão monitoradas através de métricas. Apesar de sua arquitetura ser voltada ao controle de acordos de Security-SLA, a solução é flexível o suficiente para permitir o monitoramento de outros tipos de requesitos, como por exemplo, qualidade do serviço (QoS), risco e impacto.

A Figura 1 apresenta a arquitetura de monitoramento do Security-SLA. Na figura 1(a) descreve a criação do Security-SLA a partir dos portfólios de métricas de segurança, onde cada métrica está associada a um Objetivo de Nível de Serviço (SLO). A Figura 1(b) descreve como o Security-SLA irá interagir com a infraestrutura física e virtual da



(a) Criação do Security-SLA (b) Integração do Security-SLA (c) Monitoramento Security-SLA

Figura 1. Arquitetura de monitoramento do Security-SLA

nuvem. E a Figura 1(c) representa o processo de monitoramento, onde a política de segurança define o SLA e Security-SLA. Na sequência, o processo de monitoramento das métricas é dividido em duas etapas: (1) Análise Estática: especifica como as métricas serão aferidas e os valores de comparação para: (i) SLA e Security-SLA; (ii) as qualidades do serviço do SLA (QoS-SLA); (iii) as vulnerabilidades registradas no *National Vulnerability Database* (NVD) para o tipo de serviço, identificando o valor de risco e impacto; (2) Análise Dinâmica: é executado o processo de aferir as métricas definidas na fase anterior, comparando valores de SLOs com valores aferidos (MA). Neste modelo, cada cláusula do acordo (SLO) está associado a uma métrica de segurança, e assume valores no intervalo de [0-4], e este intervalo representa os níveis de segurança permitidos [Crítico, Alto, Médio, Baixo, Zero]. Resultando ao final do processo um índice de segurança (Sec-Ind).

O processo de monitoramento depende do tipo de serviço sendo contratado, onde as ameaças e vulnerabilidades são identificadas para este perfil de serviço, e calcula-se o risco e impacto das operações executadas sobre o serviço usando como referência no NVD do *Common Vulnerability Scoring System* (CVSS).

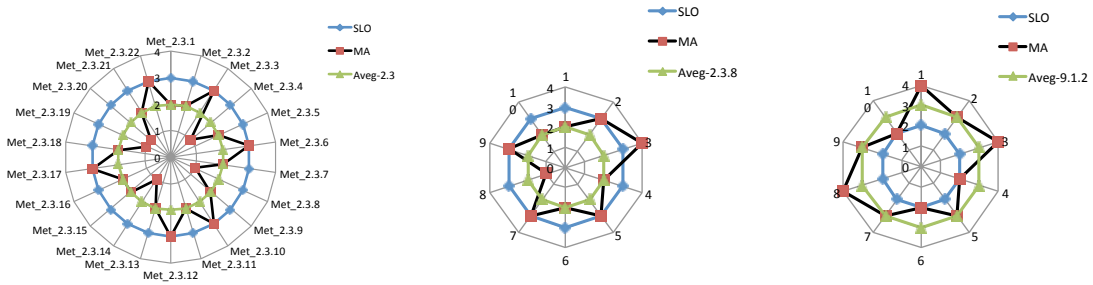
Para validar as métricas de segurança coletadas, a arquitetura de monitoramento realiza duas etapas: (1) Os valores aferidos por métricas de segurança entre [0-4] são classificados como: verdadeiros-positivo (VP), falsos-positivo (FP), verdadeiros-negativo (VN) e falsos-negativo (FN); (2) Indicadores de validação são calculados para o modelo: (i) *Precision*: $P = \frac{VP}{VP+FP}$, indica o percentual de eventos corretamente classificados como incidente entre aqueles que foram classificados como incidentes; (ii) *Recall*: $R = \frac{VP}{VP+FN}$, indica a percentual de eventos corretamente classificados como incidentes entre todos os eventos que são efetivamente incidentes; (iii) *F-measure*: $F = \frac{2 \times P \times R}{P+R}$, é a média harmônica entre Precisão e Recall; (iv) *Accuracy*: $A = \frac{VP+VN}{VP+VN+FP+FN}$, indica o percentual de eventos corretamente classificados.

Analisando os valores dos Indicadores de validação, é determinado o grau de confiabilidade dos valores coletados pelas métricas de segurança.

3.1. Estudo de Caso

Um estudo de caso foi desenvolvido e testado em um ambiente de nuvem computacional com base no *OpenNebula*, em uma máquina com *Gentoo Linux*, *hypervisor* KVM e banco de dados *PostgreSQL*. O sistema em teste é responsável pela gestão de recursos humanos em uma universidade e possui cerca de 400 tabelas, 200 usuários e 5 administradores.

A Figura 2 apresenta o resultado do monitoramento do Security-SLA, onde a Figura 2(a)



(a) Métrica *Firewall* (b) Sub-métrica *Packet filtering* (c) *Insecure user account*

Figura 2. Resultado do monitoramento do Security-SLA

é a métrica *Firewall* ($Met_{2.3}$), a Figura 2(b) é a sub-métrica *Packet filtering* ($Met_{2.3.8}$) e a Figura 2(c) é a sub-métrica *Insecure user account* ($Met_{9.1.2}$) do *PostgreSQL*. E os parametros: SLO é o valor acordado no Security-SLA, MA é o valor aferido da métrica e *Aveg* é a média de MA nas 10 amostras coletadas das figuras 2(b) e 2(c). As Figuras 2(b) e 2(c) apresentam valores aferidos menores que o contratado (violação de acordo).

4. Conclusão e Trabalhos Futuro

Nós apresentamos contribuições substanciais para uma arquitetura de monitoramento de Security-SLA através de métricas de segurança. O intervalo de valores de [0-4] para cada SLO ou métricas de segurança apresenta-se como uma nova abordagem para tratar os valores não mensuráveis ou intangíveis do ambiente de nuvem computacional.

Como trabalho futuro, consideramos o desenvolvimento de mapeamentos dinâmicos dos SLOs entre Security-SLA e os modelos de serviços existentes através de uma pré-análise de *sockets* (número IP + porta). E automatizar o processo de contramedidas para minimizar as violações dos Security-SLA e maximizar o nível de segurança do ambiente de nuvem computacional.

Agradecimentos

Os autores agradecem o apoio financeiro da CAPES e Fundect (Processo #23/200.308/2009).

Referências

Emeakaroha, V. C., Calheiros, R. N., Netto, M. A. S., Brandic, I., and Rose, C. A. F. D. R. A. F. D. (2010). Desvi: An architecture for detecting sla violations in cloud computing infrastructures. In *2nd International ICST Conference on Cloud Computing*, CloudComp 2010.

Pearson, S. (2013). Toward accountability in the cloud. *Jornal IEEE Cloud Computing - Especial Edition: Securing the Cloud*, 1(1):6–10.

Shao, J., Wei, H., and Mei, H. (2010). A runtime model based monitoring approach for cloud. *IEEE 3rd International Conference on Cloud Computing - CLOUD'10*, page 313–320.

VMITools (2013). Virtual machine introspection tools. Technical report, Available in `https://code.google.com/p/vmitools/`. Acessado em 5 julho de 2014.

