Uma arquitetura para monitoramento e detecção de anomalias de segurança para nuvens computacionais

Anderson Soares Ferreira[1], **Paulo Lício de Geus**[1]

[1]Instituto de Computação – Universidade Estadual de Campinas (Unicamp)

Abstract. *An important aspect to security management is the continuous monitoring of the environment where we want to ensure security. However, there are still very few results in the field of security monitoring in cloud computing, which happens mainly because of the environment characteristics like virtualization, multilayer and multitenancy service. Aiming to improve security on cloud computing, this article presents an architecture for security monitoring based on SLA for IaaS services and proposes a model for security anomaly detection that uses performance signatures from the monitoring system.*

Resumo. *Um importante aspecto do gerenciamento da segurança é o monitoramento contínuo do ambiente onde se quer garantir segurança. Apesar disso, ainda há poucos resultados no campo do monitoramento da segurança em nuvens, o que se deve principalmente às características do ambiente, como virtualização, serviço multi-camada e multi-locado. Visando a melhoria da segurança em ambientes de nuvens, este trabalho apresenta uma arquitetura de monitoramento baseada em SLA para serviços IaaS e propõe um modelo de detecção de anomalias de segurança baseado em assinaturas de desempenho originárias do sistema de monitoramento.*

1. Introdução

A computação em nuvens é uma tecnologia amplamente utilizada nos dias atuais, que oferece grande flexibilidade e capacidade computacional. Está disponível em um modelo de serviço utilitário, garantindo aos usuários acesso a recursos computacionais, os quais dificilmente poderiam ser utilizados em infraestruturas computacionais tradicionais, devido a seus altos custos [Krutz and Vines 2010].

Apesar dos benefícios desta tecnologia, é crescente a preocupação com a segurança de aplicações e informações nestes ambientes, o que faz com que as questões relativas a segurança sejam o principal obstáculo para a adoção da computação em nuvens [Foster et al. 2008].

Diante desse cenário, este trabalho apresenta uma solução de monitoramento voltada ao acompanhamento de acordos de nível de serviço de segurança *Security-SLA* e discute também a utilização de dados de desempenho, coletados durante a execução de máquinas virtuais (VM), para a detecção de anomalias de segurança.

2. Trabalhos Relacionados

O monitoramento de nuvens fornecido por provedores e também por soluções de código aberto baseia-se apenas em informações de desempenho e não fornece suporte ao acompanhamento de acordos (*Security-SLA*). Na área acadêmica, o monitoramento de nuvens

computacionais também apresenta poucos resultados concretos [Shao et al. 2010]. Os sistemas de monitoramento existentes são voltados ao monitoramento aplicações específicas, e não estão associados ao acompanhamento de acordos *Security-SLA*.

A detecção de anomalias de segurança está fortemente associada a sistemas de detecção de intrusão (IDS). De modo geral, existem poucos trabalhos que tratam da detecção de anomalias ou intrusões para ambientes de nuvens.

Modi et al. [Modi et al. 2012] fazem um levantamento dos diferentes tipos de IDS disponíveis para nuvem; observa-se que a grande maioria dos trabalhos nesta área aborda soluções de IDS de rede, sendo que os trabalhos que propõem soluções de máquina são voltados para a proteção do nó. Soluções de IDS para VMs tipicamente consideram a instalação de agentes na própria VM.

3. Solução de Monitoramento

A solução de monitoramento proposta tem o objetivo de acompanhar o cumprimento de acordos *Security-SLA* em nuvens IaaS. A mesma integra-se à infraestrutura da nuvem e utiliza uma arquitetura distribuída para fazer a coleta segura das informações. Nesta arquitetura, agentes de coleta de dados utilizam técnicas como o monitoramento caixa-preta ou a introspecção de VM, que permitem a coleta de informações sem a necessidade de instalação de ferramentas no sistema operacional da VM, o qual é controlada pelo usuário do serviço.

A solução também trata a representação dos acordos através de uma linguagem XML que permite especificar os níveis de serviço e políticas que podem ser utilizadas por controles de segurança no nó.

Apesar de sua arquitetura ser voltada ao controle de acordos *Security-SLA*, a solução é flexível o suficiente para permitir o monitoramento de outros tipos de parâmetros, como por exemplo, dados de desempenho.

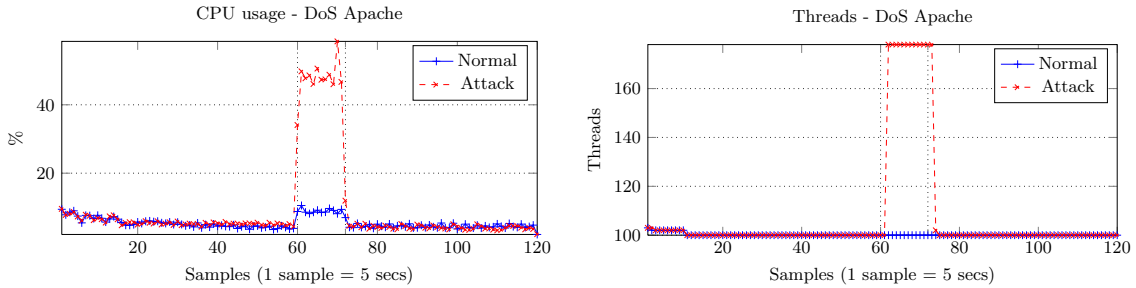
4. Detecção de Anomalias de Segurança

A detecção de anomalias baseia-se no estudo conduzido por Avritzer et al. [Avritzer et al. 2010], onde são utilizadas assinaturas de desempenho para a detecção de anomalias de segurança. Diferentemente do trabalho original, baseado em máquinas reais, nosso estudo monitorou VMs com sistema operacional Linux. Com o uso da solução de monitoramento proposta, evita-se a necessidade de qualquer conhecimento prévio sobre processos em execução na VM.

Os testes foram divididos em duas fases: a fase de *baseline*, onde foram coletadas informações de desempenho em condições de execução normais (sem ataque) e a fase de ataque propriamente dita. Cada teste teve duração de 20 minutos, com coletas de dados a cada 5 segundos.

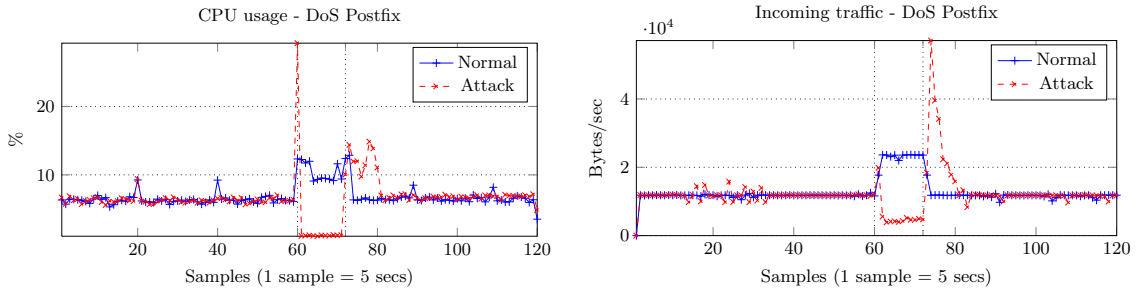
4.1. Análise dos Resultados Obtidos

A partir dos testes realizados foi possível comprovar que as perturbações causadas pelos ataques à VM puderam ser detectadas de forma semelhante aos resultados encontrados na análise em máquinas reais.



(a) Uso de CPU (b) Threads em execução

Figura 1. Assinatura do ataque DoS ao servidor Apache HTTP



(a) Uso de CPU (b) Tráfego de entrada

Figura 2. Assinatura do ataque DoS ao servidor Postfix

A Figura 1 mostra parâmetros coletados durante o ataque DoS a um servidor HTTP Apache. Nos gráficos apresentados, pode-se observar elevação no uso de CPU, memória e número de threads em execução, durante todo o período de ataque (amostras 60 até 72). Diferentemente do comportamento apresentado pelo Apache, o ataque ao servidor de correio eletrônico Postfix fez com que certos recursos tivessem seu uso reduzido durante o ataque (ver Figura 2).

Também foram testados os efeitos causados por alterações nos parâmetros de configuração de serviços e diferentes implementações do mesmo serviço, na geração das assinaturas de desempenho. Os resultados obtidos nestes testes mostraram que, apesar da efetividade na identificação de ataques através de assinaturas de desempenho, um sistema para detecção de anomalias não poderia utilizar uma base de dados única. Tanto as assinaturas obtidas se mostraram dependentes da implementação do serviço utilizado, como da configuração da máquina onde os dados de desempenho foram coletados.

A partir dos resultados obtidos, novos experimentos foram realizados com o objetivo de avaliar a utilização de mecanismos de aprendizado de máquina baseados em *Support Vector Machines* (SVM) em um sistema de detecção de anomalias. Foram realizados novos ataques de negação de serviço em diferentes servidores HTTP. Para cada servidor foram gerados 2 conjuntos de dados, o primeiro utilizado para treinamento, com dados coletados por 20 minutos, e o segundo aquele a ser avaliado, com duração de 24 horas.

Como forma de aumentar a precisão do sistema de classificação foi utilizado um seletor de parâmetros baseado em algoritmo genético, que permitiu eliminar parâmetros

desnecessários ao processo de classificação e também reduzir o custo de processamento do modelo de classificação.

A Tabela 1 apresenta os resultados obtidos pelo modelo. Vemos que o uso do seletor de parâmetros elevou fortemente a precisão da classificação do conjunto de dados do Apache e do Nginx, chegando a valores acima de 99%, ao passo que levou a perda insignificante no caso do Lighttpd. Pode-se observar também o aumento geral de acurácia e F-Measure, levando quase todos os casos a valores acima de 99%.

Tabela 1. Métricas de Avaliação da Classificação

	Precisão		**Recuperação**		**F-Measure**		**Acurácia**	
	Todos	Seletor	Todos	Seletor	Todos	Seletor	Todos	Seletor
Apache	0,5761	0,9923	1,0000	0,9979	0,7310	0,9951	0,9397	0,9992
Nginx	0,8316	0,9959	0,9938	0,9954	0,9050	0,9957	0,9832	0,9993
Lighttpd	0,9552	0,9512	0,9974	0,9989	0,9759	0,9745	0,9973	0,9972

5. Conclusões

Neste trabalho apresentamos uma arquitetura voltada ao monitoramento de serviços de nuvens de infraestrutura (IaaS) baseadas em monitoramento caixa-preta e introspecção de VM, eliminando a necessidade de instalação de ferramentas de monitoramento no sistema operacional da mesma, controlada pelo usuário.

Utilizando esta arquitetura, realizamos um estudo onde mostramos que é possível utilizar assinaturas de desempenho na detecção de anomalias de segurança em máquinas virtuais. Tal estudo permitiu a formulação de um modelo de arquitetura de detecção que utiliza um seletor de parâmetros baseado em algoritmo genético e classificação baseada em Support Vector Machines.

Referências

Avritzer, A., Tanikella, R., James, K., Cole, R. G., and Weyuker, E. (2010). Monitoring for security intrusion using performance signatures. In *Proceedings of the first joint WOSP/SIPEW international conference on Performance engineering*, pages 93–104. ACM.

Foster, I., Zhao, Y., Raicu, I., and Lu, S. (2008). Cloud computing and grid computing 360-degree compared. In *Grid Computing Environments Workshop, 2008*, GCE '08, pages 1–10.

Krutz, R. and Vines, R. (2010). *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. John Wiley & Sons.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., and Rajarajan, M. (2012). A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications*, 36:42 – 57.

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