Um Panorama das Técnicas de Segurança em Cloud Computing

Pedro Paulo Vezzá Campos

3 de novembro de 2010

Resumo

A Computação em Nuvem, ou cloud computing vem avançando tanto no mercado empresarial quanto para usuários finais como uma forma de reduzir custos e facilitar a manutenção ao delegá-los a empresas especializadas. Porém, ao mesmo tempo surgem diversos questionamentos quanto à segurança dos dados confiados a terceiros. Neste artigo em formato de *survey* será abordado o estado da arte nas técnicas de proteção produzidas para cloud computing.

1 Motivação

Cloud computing é um novo nicho de mercado que tornou-se mais atrativo com o barateamento de insumos necessários à computação como energia, poder de processamento, armazenamento e transmissão de dados, permitindo uma economia de escala. [1] Através da computação em nuvem, surgiu a noção de computação como um serviço, elástico, virtualmente ilimitado e pago apenas pela porção realmente utilizada, muito similar ao sistema de distribuição elétrica.

Diante desse cenário, *players* como Amazon, Google, Microsoft, HP, IBM, dentre outros, adentraram essa área oferecendo diversas modalidades de cloud computing, desde a mais abstrata, SaaS ou Software como Serviço, na qual é fornecido um software pronto para ser utilizado utilizando recursos da nuvem, até a mais básica, IaaS ou Infraestrutura como Serviço, que permitem uma personalização da computação desde o nível de *kernel* até camadas superiores.

Por outro lado, críticas e dúvidas são levantadas por opositores dessa tecnologia. Um exemplo é Richard Stallman, evangelista do software livre, que afirma em uma tradução livre:

> "É estupidez. É pior que estupidez: É uma campanha de marketing. Alguém está dizendo que isso é inevitável — e sempre que você ouvir alguém falando isso, é muito provável que seja um conjunto de empresas realizando campanha para torná-lo verdade." [2]

Paralelamente às oportunidades possibliltadas através do uso de cloud computing há um aumento das preocupações com a segurança dos dados armazenados na núvem. Frente a isso diversas pesquisas abordaram técnicas tradicionais e inovadoras para solucionar esse problema. Neste trabalho serão apresentadas as mais importantes dessas propostas apresentadas.

Este artigo está organizado da seguinte maneira: A seção 2 deste artigo trata dos objetivos visados na elaboração desse texto. Na parte 3 há um estudo dos principais trabalhos correlatos na área de cloud computing. Já na seção 4 são apresentadosa os principais conceitos relacionados à area, necessários para a compreenção dos assuntos seguintes. Posteriormente, na seção 5 são apresentadas as principais preocupações de usuários da nuvem relativos à sua segurança. Continuando, a parte 6 aborda as principais técnicas tradicionais de segurança, aplicáveis à cloud. Ainda, a parte 7 explora as novas possibilidades de ataques e defesas originados do uso (e abuso) da computação em nuvem. Por fim, a parte 8 apresenta as conclusões mais importantes desse trabalho.

2 Objetivos

O principal objetivo deste *survey* é apresentar um panorama geral das técnicas de segurança em cloud computing, apresentando tanto ataques possíveis a um usuário ou gerente da nuvem quanto maneiras de proteger-se de tais invasões. Para isso, serão apresentados inicialmente os conceitos principais da área de cloud computing como forma de fundamentação. Posteriormente, serão apresentados os mais importantes tópicos de preocupação de usuários e administradores de sistemas a respeito da computação nas nuvens. Por fim, será apresentado um paralelo entre técnicas de ataque e defesa existentes.

3 Trabalhos Correlatos

Em [3] são apresentados diversas preocupações com cloud computing, categorizadas segundo três macro áreas, como apresentado abaixo. Ao longo desse trabalho serão apresentados e discutidos os itens contidos em cada uma dessas categorias.

- Segurança tradicional
- Disponibilidade
- Controle de dados por terceiros

Em [4], Chen et. al. fazem um paralelo entre os desafios tradicionais enfrentados pelos provedores de cloud computing e novas possibilidades ataques. O trabalho é permeado por exemplos de técnicas de proteção em sistemas históricos, como o Multics, comprometimento de sistemas e suas consequências, dentre outros.

Ristenpart et. al. apresentam em [5] um exemplo prático de uma tentativa de invasão em um serviço de computação em nuvem, tomando como exemplo o Amazon EC2. No trabalho os autores apresentam detalhadamente as técnicas empregadas para mapear a rede que compõe a nuvem da empresa, heurísticas adotadas para conseguir que uma máquina virtual invasora seja instalada na mesma máquina física que a máquina virtual alvo e, por fim, explorando vulnerabilidades da ferramenta de virtualização conseguir gerar um canal lateral entre máquinas virtuais, burlando o isolamento imposto pelo *hipervisor*.

4 Conceitos básicos

O significado de cloud computing ainda é motivo de discussão na indústria e academia, uma vez que seu significado é amplo. Uma das tentativas de sistematizar a definição desse termo pode ser encontrada em [1]. Ainda, segundo o *National Institute of Standards and Technology*, algumas das características essenciais do cloud computing incluem [6]:

- Serviço sob demanda
- Acesso em banda larga
- *Pooling* de recursos

- Elasticidade rápida
- Consumo medido, similar ao do sistema de distribuição elétrica, por exemplo.

4.1 Modelos de serviços

Atualmente há três modelos de serviços reconhecidos como cloud computing, cada um variando no nível de configurabilidade e abstração, como é possível ver abaixo:

SaaS - Software-as-a-Service SaaS, ou Software como um Serviço, é a modalidade de cloud computing mais abstrata de todas. O usuário possui apenas a capacidade de configurar a aplicação utilizada. Nesta faixa encontram-se serviços tais como o Gmail, Google Apps, Evernote, etc.

PaaS - Platform-as-a-Service PaaS, ou Plataforma como um Serviço, é a versão intermediária de computação em núvem. Nesta, o usuário possui o poder configurar certas varáveis do ambiente de hospedagem. Aqui encontram-se serviços tais como o Google App Engine.

IaaS - Infrastructure-as-a-Service IaaS, ou Infraestrutura como um Serviço, é a versão mais básica de computação em núvem. Neste ponto o usuário tem total controle do ambiente desde o kernel até camadas mais superires. Um exemplo de IaaS é o Amazon EC2.

Ainda, há variadas maneiras de implementar uma núvem, variando no compartilhamento de recursos entre diferentes clientes:

Cloud Pública Nesse modelo qualquer pessoa ou empresa pode contratar o serviço de cloud computing.

Cloud Comunitáira Aqui o serviço é fornecido a apenas algumas organizações.

Cloud Privada A núvem passa a ser exclusiva de uma organização.

Cloud Híbrida Uma mistura dos modelos anteriores.

5 Principais preocupações

A natureza da nuvem, uma estrutura normalmente externa ao *firewall* da organização e possívelmente gerenciada por terceiros, gera a necessidade de estudos detalhados de análise de riscos antes de adotar uma solução de cloud computing. Algumas das preocupações apresentadas por [3] estão descritas abaixo:

5.1 Segurança tradicional

Ataque à virtualização Os hipervisores de virtualização são pontos sensíveis a um ataque direcionado, uma vez que eles são responsáveis por garantir o isolamento entre máquinas virtuais. Vulnerabilidades importantes já foram encontradas em diversas ferramentas, como apresenta [3].

Maior superfície de ataque Com a cloud encontrando-se possivelmente fora do firewall da empresa há a necessidade de haver uma proteção da infraestrutura, principalmente a rede que os conectam.

Vulnerabilidades do provedor de cloud Outra possibilidade é a invasão ser dirigida ao provedor de cloud computing. Um ataque pode comprometer a infraestrutura de autenticação do sistema e assim permitir o invasor o acesso irrestrito a dados sensíveis do usuário.

5.2 Disponibilidade

Controle da integridade computacional Ao contratar um serviço de cloud computing o cliente espera que o fornecedor da cloud aja de boa-fé, fornecendo valores de computação corretos. Dependendo do nível de criticidade de um serviço localizado na nuvem, apenas essa promessa é insuficiente. Para resolver esse problema pode-se adotar a redundância, por exemplo. O projeto Folding@Home envia tarefas idênticas para computadores diferentes no intuito de atingir um consenso nos resultados obtidos. A Google, por outro lado, armazena cópias de dados em diversas máquinas diferentes como forma de tolerância a falhas.

5.3 Controle de dados por terceiros

Aprisionamento de dados Uma das grandes preocupações com o cloud computing é que um cliente passe a ser dependente de um fornecedor único (ou um

pequeno grupo) de forma que o primeiro passe a ser um refém do segundo. Esse problema pode surgir através da imposição do uso de formatos ou APIs proprietárias. O Google App Engine, por exemplo, impõe o uso de tecnologias internas à Google, como o BigTable, GFS, dentre outros. Claramente uma solução a esse problema é a adoção de padrões livres. Uma amostra dessa tentativa é a API GoGrid.

6 Técnicas tradicionais

Na área de técnicas tradicionais de segurança, pode-se incluir a criptografia como forma de controlar o acesso a informações privilegiadas armazenadas na nuvem. Ainda, o fator humano continua sendo crucial, ataques de engenharia social continuam sendo bastante efetivos em conseguir comprometer um sistema.

Um exemplo dessa última afirmação foi apresentada na conferência BlackHat USA 2009. Invasores tiveram acesso a máquinas virtuais instaladas no Amazon EC2 apenas fornecendo imagens de sistemas operacionais infectadas de maneira aparentemente oficial, utilizando nomes como "fedora_core".

Por outro lado, as organizações devem estar preparadas para a recuperação de disastres, dessa forma, backups são essenciais. A ausência de um cuidado simples pode levar a sérias consequências como é possível encontrar na bibliografia.

No Brasil um caso recente foi o do migre.me: Uma falha catastrófica no servidor que mantinha o serviço causou não só a perda de todos o banco de redirecionamentos quanto os backups do site. Como agravante, o administrador não mantinha backups próprios dos dados do site, apenas do código. A consequência disso é que milhares de URLs do migre.me tornaram-se irrecuperáveis, causando diversos transtornos e possivelmente prejuízos aos usuários do serviço.

7 As novas possibilidades

Uma prova da importância da área de segurança voltada para o cloud computing é a criação de eventos importantes na área tais como: ACM Cloud Computing Security Workshop e a ACM Conference on Computer and Communications Security. Nelas são discutidas diferentes abordagens para aprimorar as defesas dos serviços contra ataques cada vez mais sofisticados.

Nesta seção serão apresentados dois tópicos um mostrando as últimas técnicas de ataques ao cloud computing e outro apresentando o estado da arte das técnicas

de defesa na área.

7.1 Novos ataques

No contexto de cloud computing, uma possibilidade pouco explorada anteriormente é a de captura do tráfego gerado e a transmissão ativa de dados por um agente malicioso. Isso é possível graças ao compartilhamento de recursos realizado pela nuvem. Outra possiblidade é a de um invasor conseguir recuperar informações sobrescritas ou apagadas por um cliente.

Ainda, com a concentração de vários clientes diferentes em somente um local, um ataque massivo pode afetar diversos usuários ao mesmo tempo. Um caso exemplificável foi o *blacklisting* de uma grande faixa de endereços IP do Amazon EC2 para o envio de emails depois que spammers conseguiram subverter as proteções levantadas pela empresa para evitar abusos do serviço. Vários usuários sofreram interrupção na entrega normal de seus emails. Como medida para corrigir o problema, agora os clientes devem preencher um formulário junto à Amazon informando a necessidade de envio de grandes quantidades de emails para que seja requisitado o *whitelisting* da faixa de IPs correspondente àquele usuário específico.

7.2 Novas defesas

Uma crescente vantagem da computação em núvem é a concentração de expertise em segurança. Um único provedor de cloud computing pode diluir os custos para manter políticas de segurança e uma equipe de segurança responsável por controlar possíveis falhas e repará-las.

Isso leva a uma modalidade de serviços conhecida como *Security-as-a-Service* na qual um provedor fornece soluções prontas de segurança tais como frameworks, criptografia, antivírus, etc.

8 Conclusão

Como foi possível perceber ao longo do artigo a área de segurança em cloud computing alia tanto conceitos tradicionais de segurança de redes, quanto novas técnicas de proteção. Ela ainda permanece em constante evolução à medida que novas técnicas de ataques surgem e novas soluções a essas invasões são implementadas.

Através de diferentes exemplos práticos envolvendo diversas empresas fornecedoras de serviços de computação em nuvem foi possível ver as consequências severas que podem surgir a partir de vulnerabilidades e descuidos tanto dos administradores da cloud quanto dos usuários dos serviços. Isso corrobora a importância das pesquisas na área visando o aprimoramento das técnicas de proteção vistas nesse trabalho e outras mais.

Referências

[1] ARMBRUST, M. et al. *Above the Clouds: A Berkeley View of Cloud Computing*. Feb 2009. Disponível em: <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html>.

[2] JOHNSON, B. *Cloud computing is a trap, warns GNU founder Richard Stallman*. setembro 2009. Disponível em: <http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman>.

[3] CHOW, R. et al. Controlling data in the cloud: outsourcing computation without outsourcing control. In: *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security*. New York, NY, USA: ACM, 2009. p. 85–90. ISBN 978-1-60558-784-4.

[4] CHEN, Y.; PAXSON, V.; KATZ, R. H. *What's New About Cloud Computing Security?* [S.l.], 2010.

[5] RISTENPART, T. et al. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: *Proceedings of the 16th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2009. (CCS '09), p. 199–212. ISBN 978-1-60558-894-0. Disponível em: <http://doi.acm.org/10.1145/1653662.1653687>.

[6] MELL, P.; GRANCE, T. *The NIST Definition of Cloud Computing*. 2009.

[7] JENSEN, M. et al. On technical security issues in cloud computing. In: *CLOUD '09: Proceedings of the 2009 IEEE International Conference on Cloud Computing*. Washington, DC, USA: IEEE Computer Society, 2009. p. 109–116. ISBN 978-0-7695-3840-2.

[8] NURMI, D. et al. The eucalyptus open-source cloud-computing system. In: *CCGRID '09: Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid*. Washington, DC, USA: IEEE Computer Society, 2009. p. 124–131. ISBN 978-0-7695-3622-4.

[9] VAQUERO, L. M. et al. A break in the clouds: towards a cloud definition. *SIGCOMM Comput. Commun. Rev.*, ACM, New York, NY, USA, v. 39, n. 1, p. 50–55, 2009. ISSN 0146-4833.

[10] FOSTER, I. et al. *Cloud Computing and Grid Computing 360-Degree Compared*. nov. 2008. 1 -10 p.

[11] VOUK, M. Cloud computing - issues, research and implementations. In: *Information Technology Interfaces, 2008. ITI 2008. 30th International Conference on*. [S.l.: s.n.], 2008. p. 31 –40. ISSN 1330-1012.

[12] GROSSMAN, R. The case for cloud computing. *IT Professional*, v. 11, n. 2, p. 23 –27, mar. 2009. ISSN 1520-9202.

[13] BUYYA, R.; YEO, C. S.; VENUGOPAL, S. Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In: *High Performance Computing and Communications, 2008. HPCC '08. 10th IEEE International Conference on*. [S.l.: s.n.], 2008. p. 5 –13.

[14] WANG, C. et al. Ensuring data storage security in cloud computing. In: *Quality of Service, 2009. IWQoS. 17th International Workshop on*. [S.l.: s.n.], 2009. p. 1 –9. ISSN 1548-615X.

[15] HUANG, W.; YANG, J. New network security based on cloud computing. In: *Education Technology and Computer Science (ETCS), 2010 Second International Workshop on*. [S.l.: s.n.], 2010. v. 3, p. 604 –609.