# Análise de segurança em infraestruturas de rede de provedores de nuvens computacionais OpenStack

**Nicolas Peter Lane, Charles Christian Miers**

[1] Departamento de Ciência da Computação (DCC)
Centro de Ciências Tecnológicas (CCT) – Universidade do Estado de Santa Catarina (UDESC)

nicolas@colmeia.udesc.br, charles.miers@udesc.br

***Resumo.*** *O presente trabalho propõe uma solução de segurança intitulada Honeypot as a Nova Node (Haa2N). A solução viabiliza a análise de infraestruturas de rede de provedores em nuvens computacionais OpenStack tradicionais e de alto desempenho. É apresentada a sua arquitetura genérica, aplicabilidade e um exemplo de caso de uso em nuvens computacionais OpenStack Newton, que atualmente encontra-se sob experimentação.*

## 1. Introdução

A computação em nuvem é uma forma de computação bem estabelecida, que é impactada pelo exercício de diversas áreas, dentre elas destaca-se a segurança. Por sua vez, a segurança em nuvens computacionais abrange a infraestrutura de nuvem do cliente e do provedor [5, 7]. A infraestrutura de um cliente corresponde aos recursos computacionais contratados de um provedor de nuvem computacional (*e.g.*, OpenStack, CloudStack, OpenNebula, Amazon AWS, *etc.*). Enquanto a infraestrutura do provedor corresponde aos demais recursos de computação que não estão presentes na infraestrutura do cliente (*e.g.,* domínio público, domínio de controle e domínio de convidados). O que é crítico, uma vez que a forma como o serviço é ofertado ao cliente, implica sob a responsabilidade com segurança atribuída às partes [1, 2]. Responsável por tornar ora o cliente, ou o provedor, o ator que desempenha função predominante quanto a segurança na infraestrutura. Nesse sentido, nuvens *Infrastructure-as-a-Service* (IaaS) atribuem ao cliente maior liberdade com sua infraestrutura, o que torna a sua contribuição para a execução de medidas de segurança na nuvem mais significativa do que para nuvens *Software-as-a-Service* (SaaS), cenário onde o provedor possui tal atribuição. Especificamente, nuvens computacionais IaaS compreendem uma forma de oferta de serviços genérica da qual as demais podem ser reproduzidas. Sendo pertinente pois mesmo para infraestruturas de nuvens SaaS, o que existe e carece de métricas de segurança afeta a nuvem holísticamente [1, 7].

De modo que faz-se relevante o que ocorre nas infraestruturas tanto de clientes quanto de provedores. Contudo, foi identificada na literatura uma carência de estudos voltados à segurança da infraestrutura de provedores de uma nuvem computacional (*e.g.,* domínio de controle, orquestração dos recursos físicos, *etc.*) [6, 7]. Tal fato implica em uma maior probabilidade das infraestruturas dos provedores de nuvens computacionais serem comprometidas, o que se deve a carência de ferramentas que auxiliem na investigação de padrões maliciosos, podendo afetar diretamente na qualidade dos serviço providos aos seus clientes [3]. Portanto, o presente trabalho prima viabilizar aos provedores de nuvens computacionais abertas OpenStack, uma solução que capacite-os à realização de análises de segurança sob o tráfego de controle, dentro de sua infraestrutura

de nuvem. Isso é feito com o intuito de possibilitar ao provedor o aperfeiçoamento de sua infraestrutura de rede e do serviço provido aos seus clientes.

## 2. Definições

### 2.1. Domínio de controle

O domínio de controle faz-se presente na infraestrutura do provedor de uma nuvem computacional e compreende as redes de controle e de armazenamento [5, 7]. Sob condições ideais a natureza do tráfego de uma rede de controle deve ser correspondente aos serviços, suas comunicações e as requisições dos diferentes usuários da nuvem (*e.g.,* cliente, administrador). Contudo, a relatada carência de estudos de segurança na infraestrutura do provedor, implica que de dois, um ou o outro ocorre, a inexistência de risco tangente, ou a sua existência. Nesse contexto, levando a existência de nuvens computacionais sujeitas às atividades maliciosas e que podem prejudicar o serviço provido ao cliente [3]. Neste contexto a motivacão do foco da investigação científica se dá pela carência de meios de mensuração, a respeito do que ocorre nesse domínio de rede.

### 2.2. *Honeypots* de baixa interatividade

Os *honeypots* são ferramentas de segurança passivas, imunes contra falsos positivos, negativos e incapazes de proteger infraestruturas de redes contra ataques, mas que oferecem meios para a realização de análises de segurança [4, 8]. Seu *modus operandi* consiste da oferta de serviços e sistemas operacionais (SOs) (*e.g.,* emulados, reais), que convidam intencionalmente atacantes a comprometê-lo, a fim de coletar dados a respeito do ataque e do próprio, sendo capazes de descrevem a interação do atacante com a ferramenta durante o ataque e a sua intenção. Adicionalmente, o tráfego capturado por *honeypots* é sempre de natureza maliciosa em função da forma como o mesmo é implantado. Nesse sentido, existe uma relação qualitativa entre coleção de dados, o nível de interação e o risco atrelado a infraestrutura de rede onde a solução é implantada, sendo atreladas às classes (*e.g.,* baixa, média e alta interatividade) [8]. Das quais, dentre essas classes, o presente trabalho utiliza-se de uma solução de *honeypot* de baixa interatividade (HBI). Similarmente, a solução pode ser implantada em redes de pesquisa para identificar novas ameaças cibernéticas e em redes de produção para o aperfeiçoamento da infraestrutura de rede de organizações.

Os HBI consistem de soluções com menor complexidade de uso, administração e baixo risco à infraestrutura de rede onde são implantados por não oferecerem serviços genuinos à interação do atacante. Essa limitação restringe o serviço que é provido ao atacante à emulação e capacidade de coleção de dados às circunstâncias do ataque e não ao ataque em si (*e.g.,* IP da máquina emissora, IP da máquina receptora, horário do ataque, *Time to Live* (TTL) do SO utilizado, *etc.*). O que torna HBI interessantes para ambientes computacionais complexos por não serem intrusivos (*e.g.,* contêineres, nuvens computacionais tradicionais e de alto desempenho) [4]. Enquanto proveem meios suficientes para obter conhecimento da origem dos ataques, tornando possível em específico, caso seja interno à infraestrutura da nuvem, a sua identificação e correlação aos atacantes via análises de segurança sob os dados obtidos.

## 3. Arquitetura do Haa2N

A arquitetura do *Honeypot as a Nova Node* (Haa2N) consiste de uma máquina física com SO, na qual reside um HBI responsável por prover o serviço de criação de instâncias de máquinas virtuais (MVs), semelhantemente a um nó de computação Nova. Tendo a oferta de seu serviço realizada pela mesma porta TCP/IP do serviço de computação Nova, TCP/IP 8774 [5]. No entanto, o atacante pode unicamente interagir com o serviço emulado. O nó de Haa2N é conectado fisicamente à rede de controle por meio de uma interface de rede, tornando-o acessível a partir dessa rede. Não obstante, esse nó não oferta um serviço genuino de computação Nova, de modo que o nó de controle Nova não o agrega à base de dados *Structured Query Language* (SQL), que é usada durante a execução do escalonador-Nova para determinar qual o nó de computação vai armazenar e computar a nova instância. Nesse sentido, o nó de Haa2N é ignorado pelo escalonador-Nova, o que faz com que seu serviço seja unicamente interagido por meio de técnicas inconvencionais de acesso à rede com a nuvem computacional, que não utilizem-se da *web dashboard* do OpenStack. De modo que o *modus operandi* do nó de Haa2N e as condições para a interação com o seu serviço, tornam todo tráfego recebido de natureza maliciosa. O serviço provido pelo nó de Haa2N é configurável, o que permite a sua modificação ou a simulação de outros serviços específicos aos propósitos da equipe de segurança do provedor (*e.g.,* identificação, resposta, monitoramento, coleção de malware, identificação de motivações, *etc.*).

## 4. Projeto de implementação

O projeto de implementação consiste das tecnologias que se fazem necessárias para a implementação e aplicação da solução de Haa2N dentro do ambiente de experimentação, são elas:

- Nuvem computacional/*release*: OpenStack/Newton.
- Sistema operacional: OpenBSD.
- Solução de HBI: Honeyd.
  - *Listener script*: serviço de criação de máquinas virtuais (MVs).

O escolha da *release* Newton do OpenStack é motivada pela forma de desenvolvimento do OpenStack focar-se em criar e consolidar os serviços básicos, enquanto adiciona novos. O que não inviabiliza a implantação da solução de Haa2N em *releases* posteriores do OpenStack. O OpenBSD 6.1 é o SO cuja escolha justifica-se por ser robusto e fazer uso ativo de boas práticas de segurança. Adicionalmente, o OpenBSD residirá no hardware de uma máquina física e sobre este SO será instalada uma solução de HBI.

Por fim, o Honeyd é a solução de HBI a ser instalada no OpenBSD, escolhido por ser uma solução com arquitetura aberta, o que permite a implementação de serviços específicos e adicionais aos objetivos dos times de segurança de uma organização. Essa liberdade é implementada por meio de um *listener* que corresponde a um *script* no Honeyd. No caso específico da solução deste presente trabalho, o *listener* implementado dispõe do serviço de criação de MVs do Nova, na qual envia uma mensagem de erro ao atacante, enquanto faz a coleção dos dados.

## 5. Ambiente de testes

A fim de obter dados estatísticos da correlação, a experimentação decorre em dois ambientes: a experimentação em uma nuvem de testes, e na nuvem de produção. O primeiro

teste tem por objetivo verificar se a implantação está correta, além de mitigar o máximo possível das vulnerablidades da arquitetura, antes de tê-la no segundo ambiente.

## 6. Considerações & Trabalhos futuros

A partir da teoria de HBI e do serviço implementado no nó de Haa2N é possível contribuir com a identificação de ataques internos e externos, enquanto a correlação resume-se aos ataques internos à rede de controle. De modo que a correlação é condicionada a uma razão inversamente proporcional ao tamanho da infraestrutura do provedor da nuvem computacional, na qual quanto menor for, mais precisão existe. O aspecto da correlação é probabilístico por depender de aspectos da organização (*e.g.,* quantidade de funcionários, regime de trabalho, *etc.*) e o entendimento obtido pela equipe de segurança por meio da análise, que aumenta de complexidade de acordo com o tamanho da infraestrutura do provedor.

A experimentação inicialmente é conduzida em uma pequena infraestrutura de nuvem privada de alto desempenho OpenStack, presente no Laboratório de Processamento Paralelo e Distribuído (LabP2D). Posteriormente é a intenção dos autores, a implantação dessa implementação em uma infraestrutura de nuvem computacional de grande porte, como a disposta pela Yellow Circle, onde os mesmos testes serão aplicados e um estudo comparativo dos resultados vai ser conduzido.

## 7. Agradecimentos

Os autores agradecem o apoio do Laboratório de Processamento Paralelo e Distribuído (LabP2D) no CCT da Universidade do Estado de Santa Catarina (UDESC). As opiniões expressas no presente artigo são de responsabilidade dos autores e não refletem a oficial política da UDESC.

## Referências

[1] CSA. Security Guidance For Critical Areas of Focus in Cloud Computing v4.0. 2017.

[2] Ryan Ko et al., editor. *The cloud security ecosystem: technical, legal, business and management issues*. Syngress is an imprint of Elsevier, Waltham, MA, USA, 2015. OCLC: 900028079.

[3] Ronald L. Krutz et al. *Cloud security: a comprehensive guide to secure cloud computing*. Wiley, Indianapolis, Ind, 2010. OCLC: 699803939.

[4] Mohssen Mohammed et al. *Honeypots and Routers: Collecting Internet Attacks*. CRC Press, 1st edition, 2015.

[5] OpenStackPike. OpenStack Docs: Pike, 2017.

[6] Y. Qiu et al. A Secure Virtual Machine Deployment Strategy to Reduce Co-residency in Cloud. In *2017 IEEE Trustcom/BigDataSE/ICESS*, pages 347–354, 2017.

[7] Tiago Rosado et al. An Overview of Openstack Architecture. In *Proceedings of the 18th International Database Engineering & Applications Symposium*, IDEAS '14, pages 366–367, New York, USA, 2014. ACM.

[8] L Spitzner. *Honeypots: tracking hackers*. Addison-Wesley, Boston, 1st edition, 2003.