MO447 – Análise Forense de Documentos Digitais – Fichamento do Seminário

Technical Issues of Forensic Investigation in Cloud Computing Environments

por dominik Birk e Christoph Wegener

27 de Outubro de 2011

Autores: André Guaraldo - RA 101487, Giuliano R Pinheiro - RA 108579
e Oscar Esgalha - RA 108231

1 Visão global

O artigo expõe a organização básica da computação em nuvem, arquiteturas básicas, modelos de serviço, e cita alguns softwares conhecidos de virtualização. Em seguida, são listados problemas consequentes da própria computação em nuvem e discorre-se sobre algumas técnicas de computação forense empregadas e suas limitações nesse ambiente. São, então, discutidas algumas possíveis soluções para os problemas citados, buscando a eliminação de outras possíveis falhas e a construção de um padrão único.

2 Resumo

A segurança na nuvem é uma preocupação da qual provém muitas pesquisas, muitas relacionadas à prevenção de incidentes no ambiente. Mas poucos são os que abordam o tratamento desses incidentes e menos os que propõem tópicos relevantes para pesquisa. É isso que os autores apresentam neste trabalho, que contém tres seções de importância: a introdução, sobre o funcionamento da computação em nuvem, o tratamento de incidentes, que elabora um quadro geral de detecção, análise, contenção, erradicação e recuperação do ambiente, e as implicações das falhas discutidas e dos métodos atuais de computação forense quando aplicados na nuvem.

Como explicitado pelos autores diversas vezes no artigo, a computação em nuvem tem sido negligenciada pela comunidade forense. Os serviços em nuvem crecem rápido e a tendência é de que muito, no futuro, seja feito na nuvem. Segundo os autores, o problema centra no fato de os desenvolvedores dessa tecnologia estarem desenvolvendo-na com padrões muito variáveis entre as plataformas disponíveis.

Atualmente, essas plataformas diferem em arquitetura de tal maneira que, se um algoritmo forense é desenvolvido para uma delas, ele pode não ser efetivo nas outras. Isso ocorre, dentre outras razões, por diferenças nos sistemas de arquivos, protocolos internos e processos de virtualização.

Os autores abordam processos cotidianos como *logging* de dados e eventos detecção e análise de recursos. Para eles, os provedores de serviço de nuvem, ou CSPs (*Cloud Service Provider*) ainda não dispõem, para o

usuário ou investigador, de funções forenses satisfatórias.

Uma dessas formas é o *data provenance*, a genealogia dos dados. São metadados mantidos para possível investigação de histórico. Atualmente, como apontado, esses dados são insuficientes ou, a depender do dado requisitado, inexistentes.

Outro destaque é a *virtual machine introspection*, uma técnica de observação de uma instancia de máquina virtual que visa observá-la de fora dela mesma, por outra máquina, ou pelo *hypervisor*, o gerenciador das VMs da nuvem.

São analisados os casos de incidente nos três tipos básicos de serviço, SaaS, PaaS e IaaS (*Software as a Service*, *Platform as a Service* e *Infrastructure as a Service*, respectivamente), e os autores mostram que o único desses modelos que atualmente suporta o emprego das técnicas atuais, com exceções, é o IaaS, por dar muito mais acesso ao cliente e ao investigador a dados como *logs* e dados de execução de processos, já que pertencem ao cliente.

O trabalho é encerrado um *recap* das soluções discutidas, apontando a necessidade da criação de padrões homgêneos das tecnologias de virtualização e uma maior atenção da comunidade de pesquisa forense ao ambiente da nuvem.

3 Contribuições

A principal contribuição do artigo é a forma com que os autores abordam o assunto. O trabalho foca a análise forense em nuvem da forma mais aberta possível no campo, analisando cada um dos três tipos de serviço e colocando como os ataques e as vulnerabilidades mais comuns afetam a coleta de evidências em cada modelo.

Para cada caso, é proposto um caminho a ser seguido pela pesquisa, notando que as abordagens existem, mas que seu modelo atual não se encaixa no modelo da computação em nuvem. Os autores frizam constantemente a falta de padronização como uma, senão a principal, das causas de a análise forense não evoluir muito nessa área.

4 Defeitos/Desvantagens

O artigo é teórico e, apesar de rico, um tanto superficial em relação a cada tema. Por um lado, os autores conseguem ser suscintos ao descreverem cada problema e aprensentam as soluções de maneira elegante, com ferramentas conhecidas que, de acordo com eles, basta sofrerem adaptações para aumentarem a blindagem da nuvem, que conta com poucos recursos forenses atualmente.

Não são dados detalhes de nenhuma técnica apresentada, apesar de explicarem-nas de forma satisfatória, o que pode obrigar o leitor a buscar mais referências a essas técnicas com frequência.

Além disso, o artigo trata sobre tudo o mais suscintamente possível, provavelmente por uma questão de volume de leitura. Talvez alguns assuntos pudessem ser mais bem tratados, como *virtual machine introspection* e *data provenance*, que são tão recorrentes no trabalho.

5 Trabalhos correlatos

De acordo com os autores, diversos documentos foram publicados no campo de segurança e privacidade dos serviços de nuvem e, as características de segurança mais desejadas circulam em torno da isolação de multiplataformas, segurança no hypervisor, com o intuito de proteger as máquinas virtuais, e segurança na infraestrutura de rede. Afirma-se também que apesar de ainda ser um dos desafios da computação forense na nuvem, alguns trabalhos sobre *digital provenance* foram publicados e contribuiram significativamente para

o desenvolvimento da técnica. Já a utilização de criptografia para uma verificação da integridade de dados armazenados na nuvem, foram propostos, mas não implementados. A computação forense tradicional, se mostrou útil em alguns casos, segundo algumas publicações. Os autores acreditam que deveria haver mais esforço voltado nessa direção e que tanto a indústria quanto a comunidade científica anda negligenciando a forense na nuvem.

5.1 1 – Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing
2 – Provenance as First-Class Cloud Data – Rongxing Lu et al. [6, 5]

Relação com o artigo avaliado: Os documentos propõe a inserção do conceito de *Digital Provenance* na computação em nuvem, uma ferramenta que seria muito útil para a forense na nuvem, já que isso permitiria que, através de algoritimos propostos em Rongxing Lu et al, seja possível rastrear usuários suspeitos de alguma atividade maliciosa ou vazamento de informação.

Descrição: Nestes artigos, é proposto a inserção do *Digital Provenance* na nuvem. O segundo explica o que é, e apresenta motivações para os CSPs o adotarem. Eles reforçam que até então nenhum serviço de nuvem usa *Digital Provenance* e que os próximos deveriam considerar fortemente a utilização dessa ferramenta.

O primeiro artigo propõe não apenas que os provedores de serviços de nuvem utilizem o *Digital Provenance*, mas também apresenta algoritimos e todo um modelo de segurança para a computação em nuvem utilizando o conceito, em que é possível rastrear ações maliciosas, vírus e outros processos suspeitos. É notável a preocupação dos autores em fazer isso sempre tentando manter a privacidade das informações dos clientes, que é uma preocupação constante dos CSPs.

Ambos artigos podem ser considerados importantes para a forense na nuvem, entretanto o primeiro é mais notável, por apresentar técnicas e não apenas motivos. É importante, porém, perceber que essas propostas dependem dos CSPs estarem dispostos à implementar essas tecnologias.

5.2 Forensics Examination of Volatile System Data Using Virtual Introspection – Hay and Nance [2]

Relação com o artigo avaliado: O documento propõe uma abordagem para analisar dados voláteis, que não podem ser analisadas do modo tradicional. Dados voláteis podem conter informações importantes e que devem ser analisadas, informações que não podem ser encontradas no disco rígido. No contexto da nuvem, a maioria dos dados ao qual se tem acesso é volátil, portanto o método é relevante. Analisar os dados e descobrir como aconteceu um ataque e as extensões do mesmo, não só contribui para uma recuperação mais rápida, como possibilita um planejamento melhor para a segurança no futuro.

Descrição: O artigo propõe o uso de *Virtual Introspection (VI)* para realizar a *live analysis*. Essa abordagem se revela interessante, pois ela observa uma máquina virtual sem influenciar no funcionamento ou no sistema da mesma. Observar aqui, significa poder ver todos os processos, *threads* e serviços que estejam em execução em uma máquina virtual. Tais informações podem revelar ataques, comportamentos indesejados e falhas de segurança.

No artigo, utiliza-se o *VIX tools*, uma ferramenta que pode realizar a *VI* em máquinas virtuais gerenciadas pelo *Xen*. É preciso lembrar, todavia, que existem outros gerenciadores de máquinas virtuais, e mesmo dentro do *Xen*, os autores revelam que a ferramenta utilizada não funciona bem em VMs que utilizam outros sistemas operacionais que não o Linux. Pode-se dizer, portanto que a forma como executaram a ideia ainda deixa a desejar, já que usa-se diversos VMMs e diversos sistemas operacionais.

6 Extensões

O trabalho apresentado abre uma vasta gama de extensões. A priori, o trabalho pode servir de fonte a outros trabalhos de mesmo teor detalhando um pouco mais cada área explorada, cada problema. O desenvolvimento de um padrão é, talvez, o alvo de mérito deste artigo. Trazer para a comunidade os problemas relacionados e os cenários forenses relacionados poderia resultar na elaboração de um conjunto de *standards* para a área.

O artigo também apresenta vários caminhos a se seguir para solucionar os problemas indicados, inclusive destaca alguns, detalhando um pouco mais de seu funcionamento. Várias áreas de pesquisa podem se beneficiar dessas ideias iniciais, de onde podem surgir estudos sólidos e técnicas aplicáveis ao ambiente da nuvem.

7 Notas

1. Relevância: 9.0
2. Originalidade: 7.0
3. Qualidade científica: 7.5
4. Apresentação: 9.0
5. Nota final: 8,0

[]

Referências

[1] Wegener C. Birk, D. Technical issues of forensic investigation in cloud computing environments. In *6th International Workshop on Systematic Approaches to Digital Forensic Engineering (in conjuntion with IEEE Security and Privacy Symposium)*.

[2] Brian Hay and Kara Nance. Forensics examination of volatile system data using virtual introspection. In *ACM SIGOPS Operating Systems Review table of contents archive Volume 42 Issue 3*, pages 74–82, 2008.

[3] C. E. Marins. Desafios da informática forense no cenário de cloud computing. In *Fourth International Conference of Forensic Computer Science*, pages 78–85, 2009.

[4] Grance T. Mell, O. The nist definition of cloud computing. National Institute of Standards and Technology. http://csrc.nist.gov/publications/drafts/900-145/Draft-SP-900-145_cloud-definition.pdf, 2009. Access: 17/10/2011.

[5] Kiran-Kumar Muniswamy-Reddy and Margo Seltzer. Provenance as first-class cloud data. In *3rd ACM SIGOPS International Workshop on Large Scale Distributed Systems and Middleware (LADIS'09)*, 2009.

[6] Xiaohui Liang Rongxing Lu, Xiaodong Lin and Xuemin (Sherman) Shen. Secure provenance: The essential of bread and butter of data forensics in cloud computing. In *The 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2010), Beijing, China*, 2010.

[7] F. R. H. da Silva. Um estudo sobre os benefícios e os riscos de segurança na utilização de cloud computing. http://fabriciorhs.files.wordpress.com/2011/03/cloud_computing.pdf, 2010. Access: 14/10/2011.

[8] Glavac D. Zimmerman, S. Cyber forensics in the cloud. *IAnewsletter*, 14(1):4–7, 2011.