Hamilton Fonte II

Modelo de plano de pesquisa - PCS5012 - 2016/1

São Paulo

2016

Resumo

O objetivo é coletar dados de memória de processos em máquinas em núvem de modo que os mesmos sejam aceitos em um processo legal. Através de um método que visa associar os dados relacionados a máquina de onde eles saíram, de modo a ajudar a diminuir a quantidade de dados a ser analisada propondo uma mudança no paradigma da coleta assim fechando uma rota de fuga para criminosos escaparem pela via legal.

Segundo a norma ABNT, o resumo deve ressaltar o objetivo, o método, os resultados e as conclusões do documento.

1 Descrição do problema de pesquisa

Forense digital é um conjunto de técnicas de coleta e análise de evidências geradas por computadores que tem por objetivos, entender a sequência de eventos que permitiu que um ataque fosse perpetrado, impedir que a vulnerabilidade que tornou possível um ataque seja explorada novamente e apoiar um processo legal (SANG, 2013). A forense digital cresceu a partir de técnicas usadas na forense tradicional. Começou de forma ad-hoc, passou por uma fase de adaptação aos requisitos legais até a era atual de ferramental avançado de coleta e análise (CHARTERS, 2009).

A utilização crescente de virtualização, ferramentas online e hospredagem em núvem (AMAZON, 2016), esta inviabilizando algumas práticas forenses (SHARMA; SABHARWAL, 2012). Especificamente a funcionalidade da elasticidade de carga ofertada pelos provedores de nuvem por meio da qual infraestrutura pode ser alocada e desalocada dinamicamente, trouxe o problema da volatilidade dos dados nas máquinas virtuais. Com algumas ameaças que não deixam evidências em disco (RAFIQUE; KHAN, 2013), a memória de uma máquina despejada de um pool seria para sempre perdida e com ela evidências importantes. O simples armazenamento do conteúdo da memória não satisfaz o princípio de Daubert. A abordagem de armazenar constantemente todas as alterações na memória não contribui para a solução do crescente backlog de dados que os investigadores tem para analizar (QUICK; CHOO, 2014). O ferramental forense disponível hoje esta pouco adaptado a desafios trazidos pela nuvem (DYKSTRA; SHERMAN, 2012), focam em completude, resposta a incidente e raros geram evidências aceitaveis em um processo legal (REICHERT; RICHARDS; YOSHIGOE, 2015).

A solução deste problema passa pela confirmação das seguintes hipóteses:

1. É possível associar um conjunto de dados de memória coletados a uma máquina e um processo específico na núvem.
2. É possível conseguir o mesmo resultado da coleta mesmo se a máquina e o processo de origem não existirem mais.
3. Não é necessário todo os histórico de alterações da memória para a análise do incidente.
4. É possível coletar as informações da memória sem a cooperação do provedor de núvem.

Essa pesquisa se justifica pela necessidade da forense em se adaptar a computação em nuvem. Não ser capaz de levantar evidências impede investigações, prisão de criminosos e correção de vulnerabilidades. Tal cenário é um convite a criminalidade e garantia de impunidade.

2 Objetivos

O princípio de Daubert é uma norma da lei Norte-Americana que versa sobre a admissibilidade de evidências oriundas do trabalho de peritos em um processo legal. Pertinentes a esta pesquisa estão a obrigatoriedade em garantir que as provas não foram comprometidas ou alteradas durante o processo de coleta, a reprodutibilidade do processo e por fim conhecer sua taxa de erro. Sendo assim, o objetivo principal deste projeto é provar que é possível coletar de dados de memória de processos em máquinas na nuvem de modo que estes se submetam com sucesso a parte cabível do Princípio de Daubert. Para alcançar este objetivo, os seguintes subobjetivos precisam ser alcançados:

1. Conseguir reproduzir o processo de coleta mesmo se a máquina de onde se originaram os dados tiver sido despejada.
2. Conseguir realizar análise de um incidente com no máximo 10% da informação de memória resultantes de processos de coleta existentes hoje.
3. Conseguir realizar a coleta sem violar jurisdição e privacidade de usuários não relacionados a investigação.
4. Conhecer a taxa de erro relacionada ao processo.

3 Método

Através de conteinerização, janela de dados e coleta fora do sistema de nuvem. Apresentar a evidência para um devogado, sei lá

4 Revisão bibliográfica

automated data acquisition in the cloud
Digital forensics framework for a cloud environment
Evidence and cloud computing the virtua machine introspection approach
Design and implementation of FROST: FoRensic tools for Open STack
Automated Forensic Data Acquisition in the cloud
A log based approach to make digital forensics easier on cloud computing
Volatile memory acquisitio using backup for forensic investigation

5 Resultados esperados

Fechar uma das portas de fuga para criminosos na núvem hoje.Fornecer mais um mecanismo de coleta de dados para investigação. Propor uma mudança de paradigma da coleta de modo a
diminuir a quantidade de informação que precisa de análise.

Referências

AMAZON. *Amazon Media Room Press Release*. [S.l.], 2016. 2 p.

CHARTERS, I. The Evolution of Digital Forensics. n. January, p. 1–39, 2009.

DYKSTRA, J.; SHERMAN, A. T. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, Elsevier Ltd, v. 9, n. SUPPL., p. S90–S98, 2012. ISSN 17422876. Disponível em: <http://dx.doi.org/10.1016/j.diin.2012.05.001>.

QUICK, D.; CHOO, K. K. R. Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*, Elsevier Ltd, v. 11, n. 4, p. 273–294, 2014. ISSN 17422876. Disponível em: <http://dx.doi.org/10.1016/j.diin.2014.09.002>.

RAFIQUE, M.; KHAN, M. N. A. Exploring Static and Live Digital Forensics: Methods, Practices and Tools. *International Journal of Scientific & Engineering Research*, v. 4, n. 10, p. 1048–1056, 2013. Disponível em: <http://www.ijser.org/researchpaper{%}5CExploring-Static-and-Live-Digital-Forensic-Methods-Practices-and-Tools.pdf>.

REICHERT, Z.; RICHARDS, K.; YOSHIGOE, K. Automated forensic data acquisition in the cloud. *Proceedings - 11th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2014*, p. 725–730, 2015.

SANG, T. A log-based approach to make digital forensics easier on cloud computing. *Proceedings of the 2013 3rd International Conference on Intelligent System Design and Engineering Applications, ISDEA 2013*, p. 91–94, 2013.

SHARMA, H.; SABHARWAL, N. Investigating the Implications of Virtual Forensics. *Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on*, p. 617–620, 2012.