Digital Investigation 20 (2017) S66–S74

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

DFRWS 2017 Europe — Proceedings of the Fourth Annual DFRWS Europe

Network forensic investigation in OpenFlow networks with ForCon

Daniel Spiekermann [a, *], Jörg Keller [a], Tobias Eggendorfer [b]

[a] FernUniversität in Hagen, Germany
[b] HS Ravensburg-Weingarten, Germany

ARTICLE INFO

Article history:
Received 26 January 2017
Accepted 26 January 2017

Keywords:
Virtual networks
Digital investigation
Network forensic
OpenFlow

ABSTRACT

To resolve the challenges of forensic investigation in virtual networks, we present a new forensic framework called "Virtual Network Forensic Process". Based on this framework we present the design, implementation and workflow of ForCon — a forensic controller to implement network investigation in OpenFlow controlled networks using Open vSwitch. Current trends bear out that virtualization techniques are no longer limited to computers as virtual machines. Thus cloud service providers try to offer greater value to their customers by implementing virtual networks and storage. Virtual environments have the same requirements for forensic investigation, however to fulfil these new tools and workflows to resolve new challenges like virtual machine migration or user customization are needed. ForCon uses dislocated agents in the network to monitor the virtual environment for changes and adapt the installed capture process without the need for any further interaction by an investigator. Thus, the network forensic investigation in virtual networks becomes flexible and valid evidence of the network data is gathered.

Introduction

With the virtualization of computers, providers began to change their processes and infrastructure in their datacenters. The virtualization provides higher flexibility, improves the automation of installation, configuration and provisioning of services and offers new possibilities and cost reduction at the same time. Aspects like security, network management and customer requirements were difficult to satisfy with virtual computers only.

The next step in the evolution of datacenters was the implementation of virtual networks, which resolved the issues in the virtual environment and improved the cumbersome manual administration of network devices.

The virtualization of networks offers a logical implementation of separated networks, each isolated from the others. The isolation of the networks is independent of the underlying physical network, all data is still transmitted over the physical network switches, routers and cable connections. But with the use of new network protocols like Virtual eXtensible LAN (VXLAN) (Mahalingam et al., 2014), Stateless Transport Tunneling (STT) (Davie and Gross, 2014) or Network Virtualization using Generic Routing Encapsulation (NVGRE) (Garg and Wang, 2015) different implementations of tunneling and encapsulation techniques enable the creation of separate logical networks, using the same underlying physical infrastructure. Therefore these logical networks are called overlay network. Anderson et al. (2005) characterizes overlay networks as follows:

> *With virtualization, nodes can treat an overlay as if it is the native network, and multiple overlays can simultaneously use the same underlying overlay infrastructure.*

Despite all these changes in the infrastructure of the datacenter or the implementations of the networks, the need for investigations in networks still exists. Digital investigation methods are used to solve crimes committed with computers (Garfinkel, 2010) and to analyse unusual behaviour in digital systems like computers, networks or mobile phones. Digital investigation in virtual environments faces issues like data location, lifecycle of virtual machines (VMs), multitenancy and a valid chain-of-custody (Spiekermann et al., 2015), but this wide area of forensic in cloud-computing environments is still being researched (Dykstra and Sherman, 2013 or Ruan et al., 2013). Additionally network forensic investigations needs to resolve different arising issues like VM migration, user customization of the assigned virtual systems or the lack of physical network interface cards (NIC) (Spiekermann and Eggendorfer, 2016a). The area of network forensic investigation in

* Corresponding author.
E-mail addresses: daniel.spiekermann@fernuni-hagen.de (D. Spiekermann), joerg.keller@fernuni-hagen.de (J. Keller), tobias.eggendorfer@hs-weingarten.de (T. Eggendorfer).

http://dx.doi.org/10.1016/j.diin.2017.01.007

these environments is still under-explored, so this paper presents a framework for digital investigation in virtual networks and an implementation developed by the authors called Forensic Controller (ForCon) to provide a valid and consistent capture process in virtual networks.

The development of ForCon is based on a detailed analysis of new challenges in the virtual networks a forensic investigator is faced with. VMs are migrated from one host to another, or users customize their internal logical network which changes the encountered installation and prevents the further capture of network packets. We assume that these changes do not have to be malicious by the customer, more likely the change in the network is initiated by the cloud environment. These changes occur without any administrative input by the cloud service provider (CSP), only because of reaching predefined usage limits of the hardware resources like cpu-time or storage capacity.

Based on this assumption we discovered the need of implementing a new forensic framework to describe the network forensic investigation in virtual networks. Current frameworks exhibit a static implementation with only one identification process at the beginning of the investigation. We argue that this limited identification at the beginning is not sufficient in virtual networks. Even the migration of the target VM requires a renewed identification of the updated location of the VM. This led to the evolution of our framework called *Virtual Network Forensic Process* (VNFP), which implements a repetition of different tasks to ensure the consistent capture process.

The rest of this paper is structured as follows: Section Related work lists previous and related works related to virtual networks, network forensics and digital forensics in virtual environments. Section Virtual networking describes the different implementations of virtual networks, with a focus on software defined networks and network function virtualization. Network forensic investigation, the limitations of the current techniques and the virtual network forensic process framework are described in Section Network forensic investigation. In Section ForCon the implementation of ForCon is explained in detail. Section Evaluation provides an initial evaluation of our prototype. Section Conclusion concludes and gives an outlook to future work.

Related work

ForCon implements a workflow for network forensic investigation in virtual networks. Each of the current techniques is based on the capture, record and the subsequent analysis of the obtained data (Lazzez, 2013; Pilli et al., 2010a; Hunt and Zeadally, 2012 or Corey et al., 2002). Khan et al. (2016a) presents an overview of current research, taxonomy and open challenges of network forensics.

The process of a digital investigation is separated in different stages leading the investigator from the initial start to the concluding reporting of the analysis. Different frameworks describe this process for network forensic investigation. The first framework for network forensics was presented in Palmer (2001). Pilli et al. (2010b) lists 10 frameworks and summarizes the different phases, which led to the development of the generic framework for network forensics. Rasmi et al. (2013) lists current frameworks for network forensic investigation.

ForCon is a tool to analyse, monitor, identify, capture and, if necessary, adapt the network forensic process in OpenFlow networks. OpenFlow is explained in detail in McKeown et al. (2008) and Azodolmolky (2013), the evolutionary change of networks by Software Defined Networks (SDN) and the notability of OpenFlow is discussed in Kreutz et al. (2015). The proposed agents of ForCon interact with Open vSwitch as the involved vswitch. The implementation of Open vSwitch (OVS) is described in Pfaff et al. (2015), the communication between Open vSwitch and the SDN controller is handled with the OpenFlow protocol.

Different research is done in the field of using OpenFlow as a controlling unit for network traffic to implement IT security approaches or forensic investigations. Achumba et al. (2015) uses OpenFlow as a virtual appliance to implement a security monitoring interface. Bates et al. (2014) implements a security infrastructure based on OpenFlow by using middleboxes to monitor and analyse the transmitting network traffic. Khan et al. (2016b) proposes with a framework named FML, a forensic management layer to analyse the controlling tiers in SDN. Bremler-Barr et al. (2014) steers traffic by communicating with the native controller to implement deep-packet-inspection of network data.

Virtual networks raise different issues for digital investigation, which are discussed in great in Spiekermann and Eggendorfer (2016b) and E. T. S. I (2016). Most of the common tools are implemented to extract network information, not to capture all transmitted data transferred from or to a suspicious system. ForCon provides an entire packet capture process targeted to one system using distributed agents. A similar approach is discussed in Ren and Jin (2005), which uses agents to capture all traffic in a local net and transmit it to a network forensic server. ForCon extends this scope by following the target system and capturing only the relevant data without capturing all network traffic in the whole segment.

Virtual networking

The implementation of VMs in a datacenter infrastructure poses new problems to the provider. The administration of new VMs, the reconfiguration of running VMs or resource management of the hardware used was getting easier and more flexible. But the isolation of VMs of different customers or the interconnection between VMs of the same customer still requires a cumbersome and error-prone manual administration like reconfiguring current access control lists (ACL), VLAN[1]-tagging or routing information.

The limitation of current network infrastructures impedes the implementation of highly dynamic, flexible, secure and automated environments that might reduce the costs and provide a customizable network. These limitations are based on the one hand on the deployed network protocols like VLAN, which limits the number of different, logically separated networks, or spanning-tree-protocols, which reduce the number of usable interconnections between switches to only one, even if more links were available. On the other hand, the installed network devices do not provide interfaces, which allow the automated configuration of the connected devices based on previously defined rules or by analysing states depending on the current network situation.

These circumstances led to the development of new network protocols like Virtual eXtensible LAN (VXLAN), Stateless Transport Tunneling (STT) or Network Virtualization using Generic Router Encapsulation (NVGRE), and to the implementation of new paradigms like Software Defined Networks (SDN) and Network Function Virtualization (NFV).

Network protocols

The new network protocols try to eradicate different limitations of currently used network protocols like VLAN[2] or spanning-tree-protocols.[3] These implementations do not provide enough

[1] Virtual local area network.
[2] E. g. implemented by IEEE 802.1q.
[3] E. g. the Rapid Spanning Tree Protocol (RSTP).