SINFONIA: uma Ferramenta para o Encadeamento Seguro de Funções Virtualizadas de Rede Através de Corrente de Blocos*

Gabriel Antonio F. Rebello[1], Igor D. Alvarenga[1], Igor J. Sanz[1], Martin Andreoni Lopez[1,2], Diogo M. F. Mattos[1]e Otto Carlos M. B. Duarte[1]

[1]GTA / PEE-COPPE / UFRJ – Brasil
[2]LIP6/CNRS (UPMC Sorbonne Universités) – França

Abstract. *Real-time monitoring and threat detection are essentials to prevent and to mitigate the damage caused by security attacks. Threat detection relies on traffic processing through various network security functions, chained together in a logical sequence. Service chaining adds functionality to the network service and, thus, it is sensitive and should be auditable. In this paper, we propose and develop SINFONIA, a tool for providing a secure chaining of virtual network functions by using blockchain. The tool uses the Open Platform for Network Function Virtualization (OPNFV) and presents a modular stateless architecture to allow the orchestration of security functions in a simple, intelligent and agile way on a web interface. Network function chaining operations are registered safely in a blockchain, ensuring non-repudiation and auditability. The SINFONIA tool demonstrates the ability to create a user-transparent service function chain to prevent host threats and thereby improve end-to-end security.*

Resumo. *A monitoração de tráfego e a detecção de ameaças à segurança da rede em tempo real são essenciais para impedir e mitigar os prejuízos causados por ataques. A eficácia da proteção depende de diversas funções de segurança de rede, encadeadas em uma sequência lógica. Contudo, o encadeamento de funções agrega funcionalidades ao serviço de rede e, portanto, é sensível e deve ser auditável. Este artigo propõe e apresenta o protótipo SINFONIA, uma ferramenta que oferece o encadeamento seguro das funções virtualizadas de rede usando uma corrente de blocos, garantindo o não repúdio, integridade e auditabilidade das operações de orquestração. A ferramenta SINFONIA usa a Open Platform for Network Function Virtualization (OPNFV) e possui uma arquitetura modular sem armazenamento de estados, para permitir a orquestração de funções de segurança de forma simples, inteligente e ágil por uma interface de usuário web. A demonstração do protótipo da ferramenta SINFONIA comprova a capacidade de criar uma cadeia de funções transparente às extremidades para prevenir ameaças aos hospedeiros e assim melhorar a segurança fim-a-fim.*

1. Introdução

A tecnologia de virtualização de funções de rede (*Network Function Virtualization* – NFV) permite reduzir gastos e flexibilizar o funcionamento das redes através da substituição de recursos em *hardware* específicos por funções virtualizadas em *software* de fácil gerenciamento sobre *hardware* de uso geral [Pattaranantakul et al. 2016]. As funções de rede são também conhecidas como sistemas intermediários (*middleboxes*) e são tradicionalmente implementadas por equipamentos específicos, como *firewalls*, sistemas de detecção e prevenção de intrusão (*Intrusion Detection and Prevention Systems* – IDPS), balanceadores de carga, entre outras. No novo paradigma, as funções de rede são executadas em computadores de uso geral, propiciando

*Este trabalho foi realizado com recursos do INCT INTERNET DO FUTURO, do CNPQ, da CAPES, e da FAPERJ.

uma redução significativa de custos aos operadores da rede [Sekar et al. 2012]. Ao utilizar a virtualização de funções de rede com a tecnologia de redes definidas por *software* (*Software-Defined Networking* – SDN), os serviços de rede podem ser controlados de forma centralizada, migrados e instanciados dinamicamente para atender às necessidades de cada aplicação. Devido a essa flexibilidade, a popularização dessas técnicas significa uma oportunidade de prover um sistema ágil e adaptativo que garanta segurança de maneira otimizada. É possível, por exemplo, definir zonas de segurança, redefinir a direção do tráfego para isolar elementos de rede comprometidos e impedir propagação de *malware* [Pattaranantakul et al. 2016].

O encadeamento de funções de serviço (*Service Function Chaining* – SFC) é o procedimento fundamental para se conseguir um controle e um gerenciamento flexível do tráfego de um serviço ou de uma aplicação. O encadeamento de funções virtualizadas de rede (*Virtual Network Functions* – VNFs) possui enormes desafios, pois requer uma execução eficiente do encadeamento, a correta ordenação das funções e a garantia de localização da função virtual na máquina física apropriada [Medhat et al. 2017]. Em especial, encadeamentos que visam a segurança de uma aplicação podem sofrer com a alta latência introduzida por cada função ou com as vulnerabilidades intrínsecas à arquitetura do SFC e do SDN, como a centralização do controle da rede e da aplicação de políticas nos pacotes [Mattos et al. 2016]. Portanto, é importante criar uma ferramenta que considere todos esses desafios, implemente essas tecnologias de forma segura e garanta a adaptabilidade à necessidade do usuário.

Este artigo propõe SINFONIA (*Secure vIrtual Network Function Orchestrator for Non-repudiation, Integrity, and Auditability*), uma ferramenta para orquestração fácil e segura de cadeia de funções virtuais de rede através de corrente de blocos (*blockchain*). A ferramenta garante a autenticidade, a integridade e o não repúdio dos comandos enviados ao orquestrador da plataforma de nuvem. Assim, pode-se garantir que nenhum comando é adulterado e confirmar sua proveniência. A ferramenta também garante a imutabilidade e irretroatividade do histórico de operações realizadas. A combinação das propriedades de não repúdio, imutabilidade e irretroatividade garantem a possibilidade de auditoria de todo histórico de transações efetuadas por cada inquilino, o que é essencial em um ambiente multi-inquilinos. Portanto, a ferramenta SINFONIA provê evidências da operação correta da orquestração de funções de rede na nuvem. Essas evidências são imprescindíveis em caso de um incidente de segurança. Ademais, a ferramenta garante que o sistema de orquestração de nuvem está de acordo com as boas práticas de segurança da informação [Vroom e von Solms 2004].

A ferramenta utiliza a nuvem *Open Platform for Network Function Virtualization* (OPNFV) como base para implementação, execução e repositório de VNFs. As cadeias de funções orquestradas estão de acordo com as especificações e normas da *Internet Engineering Task Force* (IETF) e do *European Telecommunications Standards Institute* (ETSI) [Pattaranantakul et al. 2016] para o encadeamento de funções de rede e utilizam o protocolo de cabeçalho de serviço de rede (*Network Service Header* – NSH) [Quinn e Elzur 2017]. A arquitetura proposta é composta por três camadas que se comunicam sem armazenagem de estados. Além disso, a ferramenta possui uma interface *web* amigável para orquestração com controle de acesso de inquilinos. O protótipo implementado é pioneiro no Brasil e seus resultados mostram que é possível encadear funções de serviços fim-a-fim em poucos segundos, de forma segura e em uma infraestrutura de uso geral.

O restante do artigo está organizado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados. A virtualização de funções de rede é discutida na Seção 3. A Seção 4 expõe a arquitetura e o funcionamento da ferramenta. A Seção 5 descreve a demonstração a ser realizada. Por fim, a Seção 6 conclui o trabalho.

2. Trabalhos Relacionados

O encadeamento de funções de rede é um procedimento sensível de segurança, pois flexibiliza o serviço de encaminhamento fim-a-fim provido pela rede, permitindo a adição de novas funcionalidades. Um dos principais desafios em encadear funções de rede é garantir a correta operação e gerar evidências imutáveis das ações tomadas. Nesse sentido, há trabalhos que buscam prover auditabilidade e proveniência às operações de encadeamento.

Em trabalhos anteriores, os autores propuseram uma heurística para encadeamento e alocação de funções virtuais de rede [Andreoni Lopez et al. 2016]. Dölitzscher e Clarke definiriam o conceito de Auditabilidade de Segurança como Serviço (Security Audit as a Service – SAaaS) com o objetivo de detectar incidentes de segurança na nuvem [Doelitzscher et al. 2013]. Os autores desenvolveram uma arquitetura e uma linguagem para auditabilidade leve e em tempo real que é realizada conforme a dinamicidade da infraestrutura da nuvem. Rübsamen *et al.* propuseram um esquema para garantir a segurança e a privacidade de evidências coletadas na nuvem também para fins de auditabilidade [Rübsamen et al. 2016]. Essas evidências se resumem a *logs*, provas criptográficas, documentações, entre outras. Os autores implementam um protótipo de coleta de *snapshots* de VMs em uma nuvem baseada em Openstack com o objetivo de detectar possíveis violações nessas imagens. Apesar de proverem auditabilidade, os trabalhos mencionados acima não garantem confiabilidade, por considerarem que a nuvem é uma entidade confiável e segura para armazenamento da proveniência de dados. Dessa forma, não há proteção contra possíveis modificações maliciosas por parte do provedor.

A tecnologia de corrente de blocos trouxe novos horizontes para o registro de proveniência na nuvem, pois suprime a dependência de uma entidade centralizadora confiável. Zawoat e Hasan propuseram SECAP, um esquema baseado em corrente de blocos que armazena de forma segura uma árvore de proveniência de aplicações na nuvem [Zawoad e Hasan 2016]. No entanto, o esquema proposto se restringe apenas ao registro das mudanças de estados de aplicações. Tierion é uma ferramenta baseada em corrente de blocos para comprovar a integridade e a estampa de tempo de dados genéricos de usuários [Vaughan et al. 2017]. A ferramenta fornece uma plataforma para que o usuário publique dados na corrente em forma de transações associadas ao seu ID, para que a validação possa ser conferida publicamente. tornando a validação publicamente verificável. Uma aplicação baseada em corrente de blocos para prover segurança na distribuição de conteúdo de uma rede centrada em informação foi proposta [Fotiou e Polyzos 2016]. Enigma é uma plataforma de computação descentralizada com garantia de privacidade que utiliza corrente de blocos para controlar a rede, gerenciar controle de acesso e identidade e registrar *logs* de eventos à prova de adulterações [Zyskind et al. 2015]. Liang *et al.* propuseram ProvChain, um sistema descentralizado e confiável baseado em corrente de blocos para coletar e verificar a proveniência de dados na nuvem [Liang et al. 2017]. Bosic *et al.* propõem um esquema de orquestração de máquinas virtuais usando um sistema baseado em corrente de blocos [Bosic et al. 2017] como mediador de alterações no estado de execução destas máquinas. Na proposta, os comandos enviados para o hipervisor de virtualização são registrados na corrente de blocos como transações.

Enquanto os trabalhos anteriores se concentram em registrar de forma segura a proveniência de dados na nuvem, este artigo propõe um orquestrador de cadeias de funções de rede que assegura a proveniência das operações de orquestração. Para garantir isso, o protótipo SINFONIA usufrui das vantagens da tecnologia de corrente de blocos para o gerenciamento de funções virtuais de rede. Essa funcionalidade de segurança é particularmente importante em ambientes compartilhados por múltiplos inquilinos. SINFONIA garante a autenticidade, a integridade e o não repúdio dos comandos enviados ao orquestrador da plataforma de nuvem.

3. A Virtualização de Funções de Rede

A virtualização de funções de rede (NFV) e as redes definidas por *software* (SDN) são tecnologias complementares, visto que o gerenciamento das funções de rede se beneficia do controle logicamente centralizado para configurar o plano de dados e encadear funções de rede coerentes [Mattos e Duarte 2016]. A infraestrutura de virtualização de funções de rede (*NFV Infrastructure* – NFVI), em acordo com a arquitetura de gerência e orquestração das funções virtuais de rede (*Network Function Virtualization MANagement and Orchestration* – NFV-MANO), pode compor microsserviços fim-a-fim sob medida para cada aplicação através do encadeamento das funções. A NFVI fornece as abstrações de processamento, armazenamento e acesso à rede às funções virtuais. Além disso, o controle do encaminhamento de pacotes e a consequente abstração da infraestrutura em um grafo de encadeamento de funções virtuais podem ser realizados de forma flexível pelo controle SDN [Medhat et al. 2017].

Um dos conceitos básicos de encadeamento de NFV é o de grafo de encaminhamento de VNF, que consiste na definição abstrata do encaminhamento de pacotes na rede, desacoplando a função de rede da implementação física. O grafo de encaminhamento de VNF simplifica o provisionamento da cadeia de serviços criando, modificando e removendo as cadeias de serviços [Rosa et al. 2014, Han et al. 2015]. A ferramenta SINFONIA tem como objetivo principal facilitar a interação do operador da rede com o sistema de orquestração para definir o grafo de encaminhamento da rede de forma segura. A correta operação do sistema é dada pelo registro das operações sobre o grafo de encaminhamento através da corrente de blocos.

A aplicação principal para a virtualização de funções de rede é a substituição dos sistemas intermediários, compostos por equipamentos de *hardware* específicos, por funções virtualizadas. Contudo, a adoção de uma plataforma de orquestração e de virtualização de redes deve satisfazer os seguintes requerimentos [Martins et al. 2014]:

- **flexibilidade** para executar diferentes serviços baseados em *software* de diferentes fornecedores e requeridos pelo operador de infraestrutura ou por terceiros;
- **isolamento** de memória, processamento e desempenho para que inquilinos possam compartilhar a mesma infraestrutura física;
- **alta vazão e baixo atraso** na comunicação fim-a-fim, pois as funções são implementadas no núcleo da rede e não devem implicar em perda de desempenho na comunicação;
- **escalabilidade** de recursos para as funções, permitindo a elasticidade, para mais ou para menos, adequando as funções às necessidades e às demandas dos inquilinos.

Neste trabalho, a OPNFV é a plataforma usada, pois atende aos requisitos de orquestração e virtualização de funções de rede.

4. A Arquitetura da Ferramenta SINFONIA

A SINFONIA visa garantir a auditabilidade da execução de uma plataforma multi-inquilinos para orquestração de funções virtuais de rede na nuvem. Para tanto, é utilizada uma corrente de blocos como repositório do registro de solicitações de escritas que modifiquem o estado de configuração dos serviços da plataforma, bem como o resultado dessas solicitações. A Figura 1 mostra a arquitetura da ferramenta SINFONIA. A arquitetura é composta por três módulos: i) o módulo de visualização, responsável pela interface entre os inquilinos e a plataforma de nuvem responsável pela oferta de serviços de NFV e SFC; ii) o módulo de orquestração, responsável pela execução das requisições enviadas pelos inquilinos da plataforma de nuvem através do módulo de visualização; e iii) o módulo de corrente de blocos, responsável por mediar a execução de requisições de escrita do módulo de visualização para o módulo de orquestração.

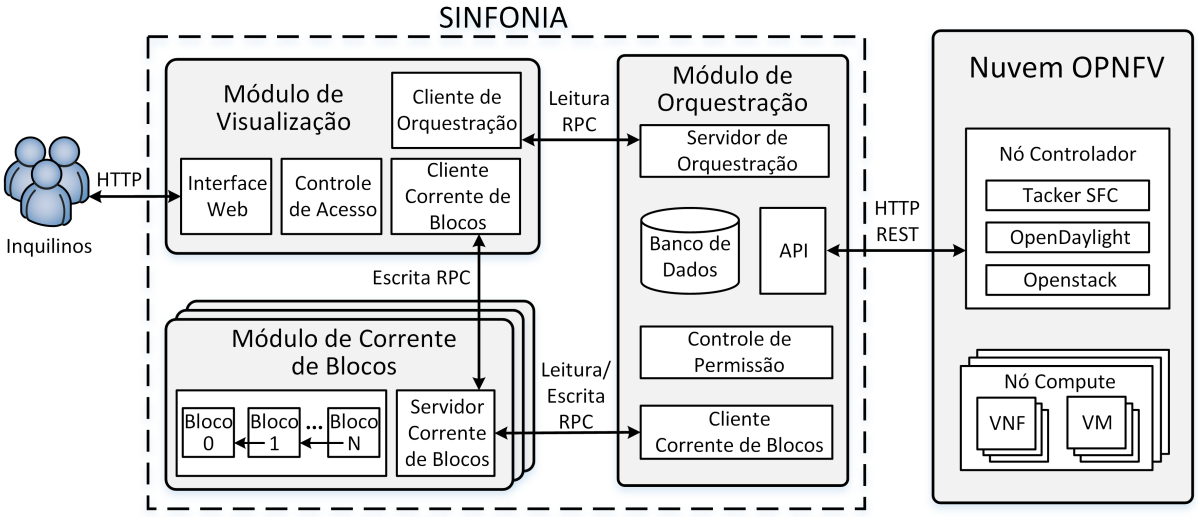

Figura 1: Arquitetura da ferramenta SINFONIA. Inquilinos realizam operações de orquestração através de uma interface Web, que são assinadas e enviadas ao módulo de corrente de blocos em forma de transações. As transações validadas são incorporadas à corrente para serem lidas pelo módulo de orquestração. O módulo de orquestração envia requisições HTTP REST para o nó controlador que então retorna o resultado da operação.

O **Módulo de Visualização** é composto por quatro componentes principais. O primeiro componente é uma interface web amigável, que permite ao inquilino monitorar e modificar seus serviços de NFV e SFC contratados. A Figura 2 mostra a página principal com os menus para execução de cada função. O segundo, um gerenciador de controle de acesso, que aplica as políticas de acordo de nível de serviço a cada usuário, bem como restringe o acesso de cada usuário a seus serviços contratados. O terceiro é um cliente de orquestração, que se comunica com o módulo de orquestração a fim de executar solicitações e leitura de estado de serviços na plataforma. Por fim, o último componente é um cliente de corrente de blocos, que se comunica com o módulo de corrente de blocos a fim de executar solicitações de escrita de estado de serviços na plataforma. Através do módulo de visualização, um inquilino pode criar VNFs, SFCs, classificadores e redes de forma gráfica e intuitiva. A comunicação dos componentes clientes é realizada através de chamadas de procedimento remoto (*Remote Procedure Call* – RPC), protegidas pelo protocolo TLS (*Transport Layer Security*).

O **Módulo de Orquestração** é composto por cinco componentes principais. O primeiro componente é um servidor de orquestração, que recebe as chamadas RPC do módulo de visualização. O segundo, um banco de dados que registra as informações de conta e serviços pertencentes a cada usuário. O terceiro, um sistema de controle de permissão, que atua em conjunto com o banco de dados para verificar se um usuário é autorizado a executar qualquer requisição. O quarto, um cliente de corrente de blocos, que se comunica com o módulo de corrente de blocos a fim de verificar a existência de requisições de escrita, bem como para registrar o resultado de uma requisição executada. Por fim, uma API (*Application Programming Interface*) para conexão à plataforma OPNFV e efetivação das requisições autorizadas.

O **Módulo de Corrente de Blocos** atua como mediador de solicitações de escrita e é composto por um servidor de corrente de blocos e pela própria corrente de blocos. O servidor de corrente de blocos recebe chamadas RPC para escrita e consulta da corrente de blocos. A corrente de blocos é um repositório imutável de todas as requisições de escrita solicitadas na plataforma. Cada requisição de escrita é assinada através da utilização de um par de chaves assimétrico RSA pertencente a um inquilino, de forma que não é possível o repúdio de uma

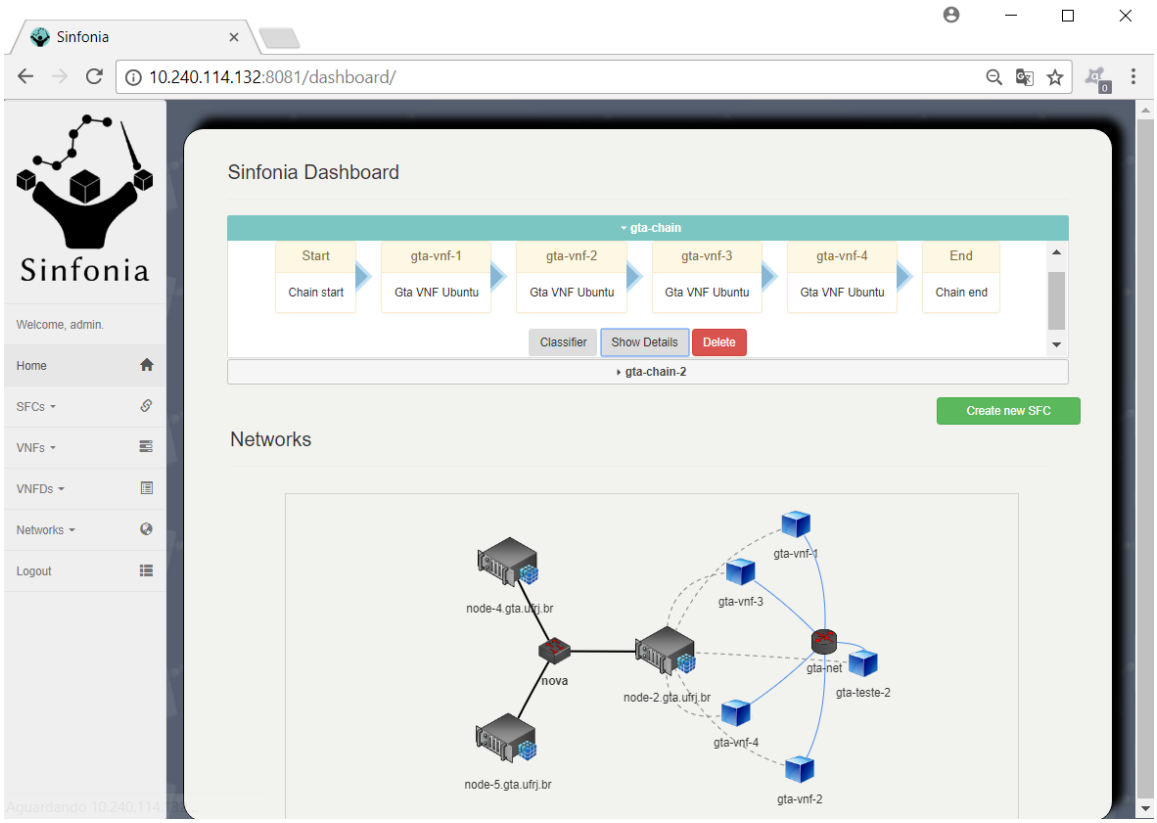

Figura 2: Interface web com o usuário com as funcionalidades da ferramenta e a visualização das cadeias de funções.

solicitação efetuada. A cada intervalo de tempo contante, da ordem de um segundo, todas as requisições solicitadas são registradas em um bloco, associado a função resumo (*Hash*) do bloco anterior e assinado pelo módulo de corrente de blocos, com um par de chaves fornecido pelo gestor do serviço de nuvem. Dessa forma, é construída uma corrente imutável e íntegra. A combinação dessas funcionalidades permite a auditagem das requisições de uso dos serviços oferecidos pela plataforma, indispensável no caso da ocorrência de um incidente de segurança. Vários módulos de corrente de blocos são executados simultaneamente e mantêm a réplica da correte de blocos, realizada através de um protocolo de consenso [Bosic et al. 2017], de forma que esse repositório é resiliente a ataques e altamente disponível.

5. A Demonstração da Ferramenta SINFONIA

O funcionamento do protótipo da ferramenta SINFONIA é demonstrado através de um computador, com acesso à Internet, nas premissas do SBSeg ou em um portátil providenciado pelos autores. A interface, servidor e corrente de blocos são executados localmente na máquina citada e o servidor irá se conectar ao ambiente OPNFV previamente instalado no Grupo de Teleinformática e Automação (GTA), no Rio de Janeiro, através de uma rede virtual privada (VPN).

As funcionalidades da ferramenta SINFONIA a serem demonstradas estão resumidas na Tabela 1. Essa tabela compara a ferramenta SINFONIA com outras existentes, ressaltando que a ferramenta SINFONIA é a capaz de prover segurança ao encadeamento de funções de rede. A demonstração consiste em criar uma cadeia de funções de rede de segurança através das funcionalidades apresentadas pela ferramenta. O primeiro passo da demonstração é criar uma rede virtual por onde os pacotes da cadeia atravessarão. Em seguida, cria-se dentro dessa rede um *firewall* e um *IDPS* virtuais através de imagens existentes no ambiente. Por fim, são feitas a criação da cadeia com as VNFs citadas e a visualização das informações na página

principal. Durante todo o processo é possível observar que o processamento das informações é transparente entre a interface e o servidor e entre o servidor e o ambiente.

Tabela 1: Comparação da proposta SINFONIA com outras ferramentas.

	Horizon	Tacker	[Bosic et al. 2017]	SINFONIA
Interface Web	✓	-	-	✓
Criar VM	✓	-	✓	✓
Criar Rede	✓	-	-	✓
Criar VNF	-	✓	-	✓
Encadear VNF	-	✓	-	✓
Auditoria	-	-	✓	✓
Integridade	-	-	✓	✓
Não repúdio	-	-	✓	✓

6. Conclusão

A tecnologia de encadeamento de funções permite fornecer serviços de rede complexos e formados por funcionalidades desenvolvidas por diferentes fornecedores de *software*. No entanto, a introdução de funções no serviço de rede é uma operação sensível, pois altera o comportamento do serviço de rede fim-a-fim, e, portanto, é necessário garantir que o encadeamento ocorra de forma correta, com controle de acesso e auditabilidade. Esse artigo propôs a ferramenta SINFONIA que oferece uma interface de usuário simples e prática para orquestrar de forma segura os serviços de redes através de corrente de blocos. As ações de orquestração são mediadas por um módulo de corrente de blocos que isola o orquestrador de qualquer ameaça externa à plataforma de virtualização. Assim, a ferramenta SINFONIA provê evidências irrefutáveis de que toda e qualquer cadeia de funções em operação é autêntica, íntegra e segue as especificações definidas pelo usuário da rede.

No sítio `http://www.gta.ufrj.br/sinfonia` é disponibilizada a ferramenta SINFONIA em conjunto com seu manual do usuário, que detalha os procedimentos de instalação, o uso da ferramenta e a documentação. O sítio permite compreender o projeto de *software* e obter mais detalhes sobre o código da ferramenta, além de outras informações úteis. Como trabalhos futuros, pretende-se estender o mecanismo de corrente de blocos para executar a configuração do *software* das funções virtuais, fazendo com que a própria função virtual possa descarregar sua configuração a partir da corrente de blocos.

Referências

Andreoni Lopez, M., Mattos, D. M. F. e Duarte, O. C. M. B. (2016). Evaluating allocation heuristics for an efficient virtual network function chaining. Em *7th International Conference on the Network of the Future (NoF)*, páginas 1–5.

Bosic, N., Pujolle, G. e Secci, S. (2017). Securing virtual machine orchestration with blockchains. Em *2017 1st Cyber Security in Networking Conference*. A ser publicado.

Doelitzscher, F., Ruebsamen, T., Karbe, T., Knahl, M., Reich, C. e Clarke, N. (2013). Sun behind clouds-on automatic cloud security audits and a cloud audit policy language. *International Journal on Advances in Networks and Services*, 6(1-2):1–16.

Fotiou, N. e Polyzos, G. C. (2016). Decentralized name-based security for content distribution using blockchains. Em *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, páginas 415–420.

Han, B., Gopalakrishnan, V., Ji, L. e Lee, S. (2015). Network function virtualization: Challenges and opportunities for innovations. *IEEE Communications Magazine*, 53(2):90–97.

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K. e Njilla, L. (2017). Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. Em *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, páginas 468–477. IEEE Press.

Martins, J., Ahmed, M., Raiciu, C., Olteanu, V., Honda, M., Bifulco, R. e Huici, F. (2014). ClickOS and the art of network function virtualization. Em *Proceedings of the 11th USENIX Conference on Networked Systems Design and Implementation*, NSDI'14, páginas 459–473, Berkeley, CA, USA. USENIX Association.

Mattos, D. M. F. e Duarte, O. C. M. B. (2016). Authflow: authentication and access control mechanism for software defined networking. *Annals of Telecommunications*, 71(11):607–615.

Mattos, D. M. F., Duarte, O. C. M. B. e Pujolle, G. (2016). Reverse update: A consistent policy update scheme for software-defined networking. *IEEE Communications Letters*, 20(5):886–889.

Medhat, A. M., Taleb, T., Elmangoush, A., Carella, G. A., Covaci, S. e Magedanz, T. (2017). Service function chaining in next generation networks: State of the art and research challenges. *IEEE Communications Magazine*, 55(2):216–223.

Pattaranantakul, M., He, R., Meddahi, A. e Zhang, Z. (2016). SecMANO: Towards network functions virtualization (nfv) based security management and orchestration. Em *IEEE Trustcom/BigDataSE/ISPA*, páginas 598–605.

Quinn, P. e Elzur, U. (2017). Network service header. Internet-Draft draft-ietf-sfc-nsh-12, IETF Secretariat. `http://www.ietf.org/internet-drafts/draft-ietf-sfc-nsh-12.txt`.

Rosa, R., Siqueira, M., Barea, E., Marcondes, C. e Rothenberg, C. (2014). Network function virtualization: Perspectivas, realidades e desafios. Em *Minicursos do XXX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos - SBRC 2014*.

Rübsamen, T., Pulls, T. e Reich, C. (2016). *Security and Privacy Preservation of Evidence in Cloud Accountability Audits*, páginas 95–114. Springer International Publishing, Cham.

Sekar, V., Egi, N., Ratnasamy, S., Reiter, M. K. e Shi, G. (2012). Design and implementation of a consolidated middlebox architecture. Em *9th Symposium on Networked Systems Design and Implementation (NSDI)*, páginas 323–336, San Jose, CA. USENIX.

Vaughan, W., Bukowski, J. e Rempe, G. (2017). Tierion network: A global platform for verifiable data. Relatório técnico.

Vroom, C. e von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23(3):191 – 198.

Zawoad, S. e Hasan, R. (2016). Secap: Towards securing application provenance in the cloud. Em *2016 IEEE 9th International Conference on Cloud Computing*, páginas 900–903.

Zyskind, G., Nathan, O. e Pentland, A. (2015). Enigma: Decentralized computation platform with guaranteed privacy. *CoRR*, abs/1506.03471.