Multi-domain DDoS Mitigation Based on Blockchains

Bruno Rodrigues(✉), Thomas Bocek, and Burkhard Stiller

Communication Systems Group (CSG), Department of Informatics (IfI),
University of Zürich (UZH), Zürich, Switzerland
{rodrigues,bocek,stiller}@ifi.uzh.ch

Abstract. The exponential increase of the traffic volume makes Distributed Denial-of-Service (DDoS) attacks a top security threat to service providers. Existing DDoS defense mechanisms lack resources and flexibility to cope with attacks by themselves, and by utilizing other's companies resources, the burden of the mitigation can be shared. Technologies as blockchain and smart contracts allow distributing attack information across multiple domains, while SDN (Software-Defined Networking) and NFV (Network Function Virtualization) enables to scale defense capabilities on demand for a single network domain. This proposal presents the design of a novel architecture combining these elements and introducing novel opportunities for flexible and efficient DDoS mitigation solutions across multiple domains.

Keywords: Distributed Denial-of-Service (DDoS) · Security · Blockchain · Software-defined Networks (SDN) · Network management

1 Introduction and Motivation

A Distributed Denial-of-Service (DDoS) attack is a large-scale, coordinated attempt to make a target system's resources unavailable. Although being a known category of attack, it remains as one of the major causes of concern for service providers. The increasing number of unsecured connected devices (stationary and portable) and their growing processing capacity, allow attackers to take control of a vast amount of unsecured devices that ranges from connected cameras to smart fridges to generate malicious attacks.

Major causes of concern for service providers is that not only the volume of traffic of DDoS attacks is growing, but also their complexity. Botnets taking advantage of unsecured IoT (Internet of Things) devices are the primary cause of these large-scale attacks. The Mirai botnet [4], for example, exploits default and weak security credentials to spread itself for other devices.

In an attack launched on Krebs Security [1] website in September 2016, Mirai peaked 623 Gbps in volume of traffic. Akamai, the service hosting the website, had to shut down the site because defending it during three days became too costly. It was reported that so many devices were used that the attacker did not have to use any sophisticated strategy.

D. Tuncer et al. (Eds.): AIMS 2017, LNCS 10356, pp. 185–190, 2017.
DOI: 10.1007/978-3-319-60774-0_19

2 Problem Description

As DDoS attacks become progressively sophisticated and coordinated, the defense from such attacks likewise needs distribution and coordination. To prevent or reduce damages caused by these DDoS attacks, different detection and mitigation methods are available.

Typical implementation is based on dedicated ASIC-based appliances to analyze flow records exported from edge routers, and further filtering or load balancing traffic. Cloud-based solutions such as Cloudfare [3] and Akamai [1] can take away the burden of detection and mitigation, serving as a proxy able to load balance, reroute, or drop the traffic in case of DDoS attacks.

Many centralized defense systems lack of hardware resources or software capabilities to detect and mitigate attacks themselves. Traditional or cloud-based defenses can become a communication bottleneck due to the need to download and process all the traffic measurements at a single location. Thus, if an attack is highly sophisticated and there is no countermeasure available, legitimate users may be impaired until the attack stops.

An alternative is sharing hardware and defense capabilities with other systems, an approach called cooperative DDoS mitigation. However, existing cooperative approaches involve the proposal of a particular distributed architecture and protocols that usually require the modification of existing hardware and software in its support.

3 State-of-the-Art

Although there are several related works, concepts and technologies guiding the development of the proposal, for brevity in this section we highlight only three main related works. Internet Engineering Task Force (IETF) is proposing a protocol [5] named DOTS (DDoS Open Threat Signaling) covering both intra-organization and inter organization communications. DOTS requires servers and clients organized in both centralized and distributed architectures to advertise black or whitelisted addresses. However, DOTS presents a complex architectural design, which hinders your deployment without the complete standardization of the DOTS protocol. A different approach is [7], proposing a collaborative framework that allows the customers to request DDoS mitigation from ASes. However, the solution requires an SDN controller at customer side interfaced with the service provider, which can change the label of the anomalous traffic and redirect them to security middle-boxes. A similar approach is seen in [6]. The authors propose a cooperation between domains that implements VNFs to alleviate DDoS attacks by redirecting and reshaping excessive traffic to other collaborating domains for filtering. However, the proposal still requires the support of a gossip-based protocol by the network infrastructure to exchange information about attacks.

4 Research Questions

Many research challenges are found in the current scenario to improve current DDoS defense mechanisms not only in a single domain, but in a cross-domain perspective. Expected contributions of this work are categorized herein into three major stages of the DDoS protection: (1) analysis and detection, (2) collaboration across multiple domains, and (3) scalability of the proposed solution. Therefore, contributions of this work are expected to answer the following research questions:

RQ1: How to efficiently identify traffic types avoiding that, in presence of attacks, legitimate users may be hampered by the traffic of attackers? This proposal involves the identification of techniques based on machine learning to promote the signaling of attacks.

RQ2: How to simplify existing cooperative DDoS architectures and protocols so minimal hardware and software modifications are necessary to advertise DDoS information across multiple domains? In addition, it is necessary to investigate an incentive scheme to balance the relationship between cooperative entities, preventing a domain from abusing the cooperative scheme.

RQ3: How does the solution scale to report a number of addresses given the scale of devices involved in large-scale attacks?

5 Approach and Next Steps

A novel approach is presented herein to mitigate DDoS attacks across multiple domains. Recent advances on networking technology, such as Software-defined Networking (SDN) and Network Function Virtualization (NFV) are gaining attention towards the establishment of software-defined infrastructures. Blockchain and Smart Contracts may be used to advertise information across multiple domains, reducing the complexity of distributed protocols and architectures for gossiping DDoS attacks information. Figure 1 illustrates the proposed architecture of the system.

- **Software-Defined Networks (SDN):** enable the development of customizable security policies and services managed in a dynamic, software-based fashion. Among the available SDN controllers, Ryu is an open-source controller providing an well defined API for interacting and managing applications.
- **Network Function Virtualization (NFV):** enforce the security policies of the centralized control through virtualized functions provisioned in generic hardware. The VNF-BC is the virtual appliance deployed both on the network domain and customers, that may interface with network management systems, and optionally import flow-records of widely used network monitoring tools, as sFlow or NetFlow.
- **Blockchain**: Ethereum-based blockchain, which is public, decentralized and provide a trusted consensus in which data of DDoS attacks can be advertised and accessed between the cooperative domains. In an Ethereum blockchain,

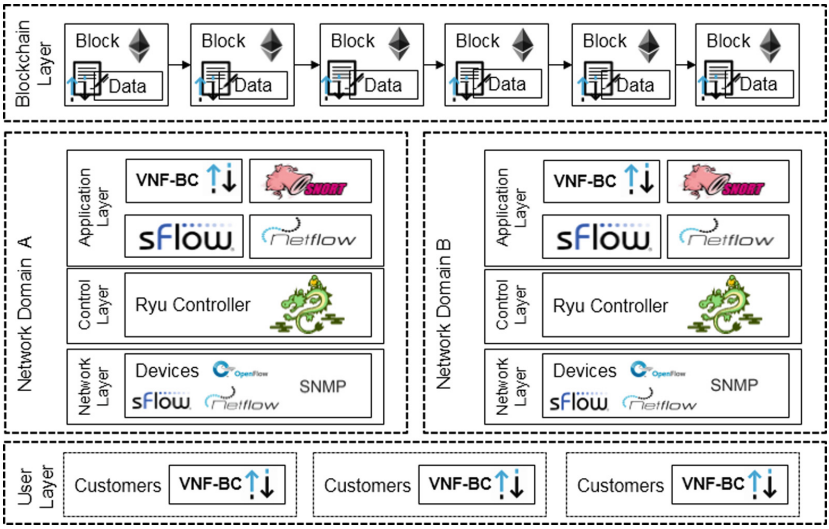

Fig. 1. Proposed architecture

VNF-BC appliances listening to the blockchain may see new addresses reported within a new 14 s, which is the time a block is mined.

– **Smart Contracts:** a Solidity-based contract implementing the logic of the collaborative approach, advertising of white or blacklisted IP addresses of certified customers, as well as information on the reporting entity and attack characteristics.

SDNs optimize the management of flows in response to attacks by enabling the deployment of sophisticated traffic analysis based on global network awareness given by a centralized controller. Aligned, SDN and NFV offer flexible and programmable network infrastructures toward generic network hardware deployed on open software, in which functions of the centralized control can be performed through virtualized network functions (VNF) and capabilities from NFV.

Security policies and thresholds may be defined based on historical records directly obtained from southbound protocols such as OpenFlow or SNMP, or exported from monitoring tools as sFlow or NetFlow. In response to attacks, the SDN controller may dynamically provision virtual functions for firewalling, packet inspection (*e.g.*, Snort), or black-holing malicious traffic.

Blockchain and Smart Contracts can be used to advertise DDoS attacks information across multiple domains [2]. This simplifies existing cooperative DDoS mechanisms by using an existing distributed infrastructure to broadcast black or whitelisted addresses without the need to build specialized registries or other distribution mechanisms/protocols. The Ethereum blockchain supports a Turing-complete contract language [2], such as Solidity. Therefore, a node participating in the Ethereum blockchain runs a Solidity smart contract by executing a script,

which is used to store references to the advertised addresses. The contracts is further processed checking if the entity reporting addresses is certified and its result is stored in a block.

However, entities issuing addresses need to have its identity certified. Similar to IETF-DOTS, certificates can be used to ensure authenticity of entities. Therefore, a network domain may issue to its customers a an authentication service to its customers through a registered VNF appliance able to report black or whitelisted addresses to the blockchain. For example, an LDevID certificates signed by the device owner may encode an owner assigned unique identifier and a PKI matching a private key held within the VNF appliance. Inter-domain trust can be established through any of the multi-PKI trust models in use today [8]. Then, information on the registered appliances will be hashed and referenced in the smart contract.

6 Summary

An architecture for multi-domain DDoS Mitigation based on Blockchains, SDN and VNFs was presented. Although designed based on SDN, a VNF appliance to read/write in the blockchain could be integrated with different networking-systems that exports flow records with sFlow or NetFlow. Expected contributions are not limited to the collaborative perspective of the DDoS defense, but also on the detection and mitigation of these attacks in a single domain based on key technologies such as SDN and NFV.

References

1. Akamai: How to Protect Against DDoS Attacks - Stop Denial of Service (2016). https://goo.gl/pfcWph. Accessed 10 Jan 2017
2. Bocek, T., Stiller, B.: Smart Contracts - Blockchains in the Wings, pp. 1–16. Springer, Heidelberg (2017). Tiergartenstr. 17, 69121
3. CloudFare: Cloudflare advanced DDoS protection (2016). Accessed 10 Jan 2017
4. Gamblin: Source code of the mirai botnet available on github, January 2016. https://goo.gl/CB5vx4. Accessed 14 Mar 2017
5. Nishizuka, K., Xia, L., Xia, J., Zhang, D., Fang, L., Gray, C.: Inter-organization cooperative DDoS protection mechanism. Draft, December 2016. https://goo.gl/szsalO
6. Rashidi, B., Fung, C.: Cofence: a collaborative DDoS defence using network function virtualization. In: 12th International Conference on Network and Service Management (CNSM 2016), October 2016
7. Sahay, R., Blanc, G., Zhang, Z., Debar, H.: Towards autonomic DDoS mitigation using software defined networking. In: SENT 2015: NDSS Workshop on Security of Emerging Networking Technologies. Internet Society (2015)
8. Shimaoka, M., Hastings, N., Nielsen, R.: Memorandum for multi-domain public key infrastructure interoperability (2008)