**DDoS Attack Protection in the Era of Cloud Computing and Software-Deﬁned Networking**

Cloud computing has become the real trend of enterprise IT service model that offers cost-effective and scalable processing. Meanwhile, Software-Deﬁned Networking (SDN) is gaining popularity in enterprise networks for ﬂexibility in network management service and reduced operational cost. There seems a trend for the two technologies to go hand-in-hand in providing an enterprise’s IT services. However, the new challenges brought by the marriage of cloud computing and SDN, particularly the implications on enterprise network secu- rity, have not been well understood. This paper sets to address this important problem. We start by examining the security impact, in particular, the impact on DDoS attack defense mechanisms, in an enterprise network where both technologies are adopted. We ﬁnd that SDN technology can actually help enterprises to defend against DDoS attacksif the defense architecture is designed prop- erly. To that end, we propose a DDoS attack mitigation architecture that integrates a highly programmable net- work monitoring to enable attack detection and a ﬂexible controlstructuretoallowfastandspeciﬁcattackreaction. The simulation results show that our architecture can effectively and efﬁciently address the security challenges brought by the new network paradigm. As cloud computing provides on-demand, elastic, and accessible computing services, more and more enterprises begin to embrace this paradigm shift by moving their database and applications into the cloud. At the same time, another epochal concept of the Internet architecture comes to forefront, i.e., Software- Deﬁned Networking (SDN). While cloud computing facilitates the management of computation and storage resources, SDN is proposed to address another labori- ous issue hindering the evolvement of today’s Internet, i.e., the complicated network management. Besides the fact that SDN has been proposed as a candidate of the next generation Internet architecture, companies like Google have already adopted SDN in their internal data centers. Thus, the arrival of the era when cloud computing and SDN go hand-in-hand in providing enterprise IT services is looming on the horizon. Besides all the widely perceived beneﬁts, the mar- riage between cloud computing and SDN may also introduce potential risks, especially on network secu- rity. Among all the network security problems, we ﬁrst take a look at Denial-of-Service (DoS) attack. A DoS attack and its distributed version, Distributed Denial-of-Service (DDoS) attack, attempt to make a service unavailable to its intended users by draining thesystem or network resource. Although network security experts have been devoting great efforts for decades to address this issue, DDoS attacks continue to grow in frequency and have more impact recently. Existing DDoS attack defense solutions (to list a few [1], [2], [3], [4]) assume a fully controlled network by the network administrators of enterprises. Therefore, the network administrators could place certain hardware pieces in the network to detect or mitigate DDoS at- tacks. However, in the new network paradigm of cloud computing and SDN, these assumptions no longer stand. Other researchers [5], [6] focus on exploiting the beneﬁts of cloud or SDN to defend DDoS attacks. But their target victims still reside in the traditional network environment, which makes their solutions un- suitable for the new network paradigm. To the best of our knowledge, little effort in research community has been made to look into the potential problems or opportunities to defend DDoS attacks in the new enterprise network environment that adopts both cloud computing and SDN.

**Distributed Denial of Service (DDOS) Attacks in Cloud Computing**

Cloud computing is the use of computing resources (hardware & software) that delivered as service over internet. For sensitivity or security of data, existing solutions usually apply cryptographic methods by using encryption and decryption keys and giving these keys to only authorized users. But when we apply these methods to real cloud the problem of simultaneously achieving fine-grainedness, scalability and data confidentiality of access control actually still remains unsolved. In the cloud computing, the prevalence and sophistication of DoS and DDoS on the internet are rapidly increasing. Service providers are under mounting pressure to prevent, monitor and mitigate DoS/DDoS attacks directed towards their customers. Attacks that are seen every day on the internet in the cloud computing include Zombie attack, phishing attack, DoS and DDoS attack, man-in-middle attack, service injection attack, metadata spoofing attack. These attacks can cause damage and wide spread out gages when directed at a service provider’s infrastructure. The monitoring and mitigation of these attacks is a crucial part of a service providers operation. In this paper we have studied cloud computing, attacks (mainly DDoS attacks) on cloud computing and techniques to cover these attacks. Further we have tried to explain the pros and cons of different techniques and its impact on real world cloud. In cloud computing, the word cloud represents the metaphor “the internet” and the phrase cloud computing “means a type of internet based computing” where different services such as servers, storage and application are delivered to an organizations, computers and devices through the internet. Cloud computing has emerged as a way for IT businesses to increase capabilities on the fly without investing much in new infrastructure, training of personals or licensing new software [1]. National Institute of Standards and Technology NIST [2] defines Cloud computing as a “model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and delivered with minimal managerial effort or service provider interaction”.

The Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are the most common but fatal type of attack on cloud service providers (CSPs) which are working hard to prevent, monitor and mitigate these types of attacks as the frequency of these types of attacks have risen sharply in the last few years. DDoS are directed at service provider’s infrastructure can be very damaging. In cloud computing, the DoS or DDoS attack is when a machine or network resources unavailable to its intended users. DDoS attacks are sent by two or more persons or bots. DDoS attacks are sent by one person or system. In this paper we have discussed the most common types of DoS/DDoS attacks seen on the internet and ways that service providers can prevent or mitigate damages from the attack threats. The monitoring of DoS/DDoS and black hole filtering became mandatory as entry for service providers to sell the service of internet in the financial industry. The financial industry is easily susceptible to DoS/DDoS attacks as millions of consumers move to electronic bill payments, purchases and On-line banking.

**Intrusion Detection System in Cloud Computing**

Today, Cloud Computing is the preferred choice of every IT organization since it provides flexible and pay-per- use based services to its users. However, the security and privacy is a major hurdle in its success because of its open and distributed architecture that is vulnerable to intruders. Intrusion Detection System (IDS) is the most commonly used mechanism to detect attacks on cloud. This paper provides an overview of different intrusions in cloud. Then, we analyze some existing cloud based intrusion detection systems (IDS) with respect to their type, positioning, detection time, detection technique, data source and attacks they can detect. The analysis also provides limitations of each technique to evaluate whether they fulfill the security requirements of cloud computing environment or not. We emphasize the deployment of IDS that uses multiple detection methods to cope with security challenges in cloud. Cloud Computing offers omnipresent, convenient, demand-based access to a shared group of configurable computing resources (like storage, network, services applications and servers) that can be quickly provisioned and released with least management effort or service provider interactions [1]. It provides services to its users in different ways: Infrastructure as a Service (IaaS), where the user has control over complete virtual machines [2] such as Eucalyptus, Open Nebula [3]. Platform as a Service (PaaS), where the user can deploy user-created applications in cloud if the provider supports the languages, APIs, and tools used for creating application, [1] like Google App Engine, Microsoft’s Azure [3]. Software as a Service (SaaS) which enables users to execute provider’s applications [1] such as Google apps [3]. These services are provided via the Internet. There are four deployment models for cloud: Public cloud, its infrastructure is intended to be used by general public and managed by a governmental academic or business organization. Private cloud, it is deployed for a particular organization having

multiple users. Its management is the responsibility of organization using its services or a third party. Community cloud which is deployed for use by a particular group of users from organizations having common goals. It can be managed by any of the organizations within that group or a third party. Hybrid cloud, its infrastructure consists of two or more different cloud infrastructures (public, private, or community) that ensures the portability of applications and data using a standard technology. The unique features of clouds forming hybrid cloud are retained [1].

**Improving Network Intrusion Detection System Performance through Quality of ServiceConfiguration and Parallel Technology**

This paper outlines an innovative software development that utilizes Quality of Service (QoS) and parallel technologies in Cisco Catalyst Switches to increase the analytical performance of a Network Intrusion Detection System (NIDS) when deployed in high-speed networks. We have designed a real network to present experiments that use a Snort NIDS to demonstrate the weaknesses of NIDSs, such as inability to process multiple packets and propensity to drop packets in heavy traffic and high-speed networks without analysing them. We tested Snort’s analysis performance, gauging the number of packets sent, analysed, dropped, filtered, injected, and outstanding. We suggest using QoS configuration technologies in a Cisco Catalyst 3560 Series Switch and parallel Snort NIDSs to improve NIDS performance and to reduce the number of dropped packets. Our results show that our novel configuration improves performance. In order to provide new developments and the highest- quality services, companies implement the latest technologies in their infrastructure. A company’s network plays a vital role in its business projects; it can achieve success in its business career by keeping its computer network up-to-date with the latest software and security techniques. Reliability and safety are the major concerns in enabling a company to achieve success and boost its progress. However, these networks can also be considered a major risk in any business project. Security issues have increased as technology has advanced. Fuchsberger [1] reported that, according to a survey conducted by Federal Bureau of investigation and Crime Scene of investigation (FBI/CSI), viruses are behind many attacks on business networks. Moreover, denial of service (DoS) attacks and unauthorized user access (which can be initiated from external or internal LAN sources) have also increased dramatically. In order to provide new developments and the highest- quality services, companies implement the latest technologies in their infrastructure. A company’s network plays a vital role in its business projects; it can achieve success in its business career by keeping its computer network up-to-date with the latest software and security techniques. Reliability and safety are the major concerns in enabling a company to achieve success and boost its progress. However, these networks can also be considered a major risk in any business project. Security issues have increased as technology has advanced. Fuchsberger [1] reported that, according to a survey conducted by Federal Bureau of investigation and Crime Scene of investigation (FBI/CSI), viruses are behind many attacks on business networks. Moreover, denial of service (DoS) attacks and unauthorized user access (which can be initiated from external or internal LAN sources) have also increased dramatically.

**Managing NFV using SDN and Control Theory**

Control theory and SDN (Software Deﬁned Net- working) are key components for NFV (Network Function Virtualization) deployment. However little has been done to use a control-theoretic approach for SDN and NFV management. In this demo, we describe a use case for NFV management using control theory and SDN. We use the management architecture of RINA (a clean-slate Recursive InterNetwork Architecture) to manage Virtual Network Function (VNF) instances over the GENI testbed. We deploy Snort, an Intrusion Detection System (IDS) as the VNF. Our network topology has source and destination hosts, multiple IDSes, an Open vSwitch (OVS) and an OpenFlow controller. A distributed management application running on RINA measures the state of the VNF instances and communicates this information to a Proportional Integral (PI) controller, which then provides load balancing information to the OpenFlow controller. The latter controller in turn updates trafﬁc ﬂow forwarding rules on the OVS switch, thus balancing load across the VNF instances. This demo demonstrates the beneﬁts of using such a control- theoretic load balancing approach and the RINA management architecture in virtualized environments for NFV management. It also illustrates that the GENI testbed can easily support a wide range of SDN and NFV related experiments. NFV elastic management includes tasks related to Virtual Network Function (VNF) stateful migration from one Virtual Machine (VM) to another, and adding or removing VNF instances depending on the load on the system [1], [2], [3]. NFV elastic management has recently received considerable attention in the research community [1], [2], [3]. However, most of this work focuses on VNF stateful migration. In this demo, we use a new internet architecture – the Recursive InterNetwork Architecture (RINA) [4] – to share VNF state information across the system and use a control-theoretic approach for managing load across VNF instances. To the best of our knowledge, this is the ﬁrst work that uses a control- theoretic approach to NFV management. Figure 1 shows an overview of the system. We deploy Snort [5], an Intrusion Detection System (IDS) as the VNF. There can be multiple source and destination hosts and all traf- ﬁc directed from any source to any destination passes through Snort-IDS. VNF hosts run a distributed monitoring application (deployed over RINA) where each application instance shares the state of the VNF (i.e., load information) with the central controller. The controller runs a control-theoretic Proportional Integral (PI) control algorithm that balances load across the VNF instances by providing the OVS controller with load balancing information, which is then used to update the ﬂow forwarding rules on the OVS switch so new ﬂows are directed to less loaded VNF instances.