Network Virtualization and its security loopholes

Karan Maheshwari
School of Computer Science and Engineering
Vellore Institute of Technology
+919790089155
karan.maheshwari14@gmail.com

***Abstract*— in today's world of connectivity either it is absolute security or absolute accessibility but with the present communication model of Internet finally we have reached equilibrium. The Internet is certainly well performing but one of the biggest problems it is now facing is that we have been modifying it across the periphery, not the pith and this lack of change in the system has some serious implications; one of the possible solutions is network virtualization which also copes up with the ongoing trend of green computing. Network Virtualization has a lot of benefits as it allows, to create a test bed for future internet, a stack where we can load multiple protocols, device mobility, manageability and scalability of network but all these things have a price attached with them. By virtualizing the network we create more vulnerable areas where our security is compromised. Here we discuss what network virtualization is at the same time differentiating it with NFV and SDN, the general structure of a virtualized network and security loopholes in it and how these vulnerabilities affect different user levels who are attached with it.**

Introduction

Interconnection of networks or as we say the Internet is a layered communication model and indeed its users are also layered. The physical infrastructure provider at the bottom offering a service to the network managers or what we commonly say the ISPs and these network managers taking service from infrastructure providers giving service to the end users ranging from residential to corporate enterprise users.

To create a network and to connect different users spread across the globe with different architectures of nodes that form the network, the infrastructure providers have significantly contributed by creating embedded systems with patented hardware boxes inseparable with their software, so far necessary to form and manage a network. The nodes connected by a transmission media and the special purpose hardware, are all the resources, which form up a network. The current Internet faces a lot of issues some of them being not able to comply with current technologies, problem of scalability and utilizing the underlying hardware completely. The only feasible solution to solve these problems is virtualization.

In the field of computer science virtualization is an established concept where we split up the resources as per need to maximize efficiency. It is the logical abstraction of the physically existing resources. Virtualization has already been implemented as in server virtualization. The network, which we see today is too inflexible, and is not adaptable to the new techniques and researches. So rather than using the old and stiff framework designed decades ago if we can virtualize the resources with which network is made, we can de-ossify it by creating a new architecture of network.

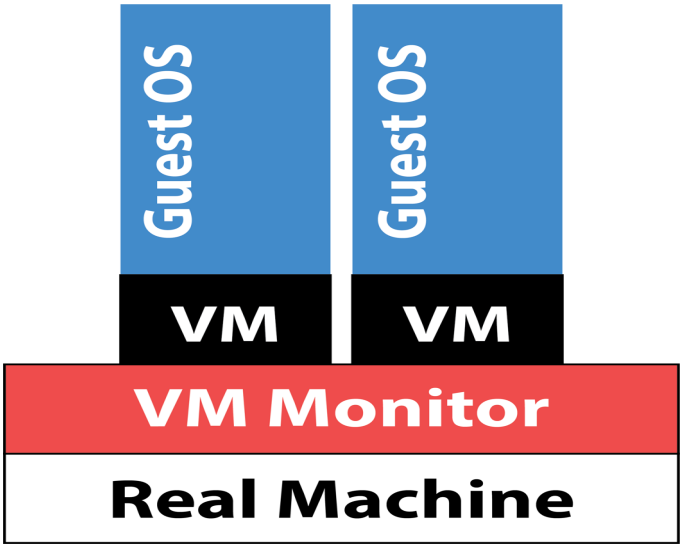

Figure1

Virtualization of network has its own three independent but interconnected sub domains, which are: Network Virtualization, Network Function Virtualization and Software Defined Networking. In the next section we will briefly tell you about three of the sub domains of Virtualization of Networks.

I. BACKGROUND

In the older networks, all possible network functions were performed using a specifically built hardware device made for specific purposes using large amount of software both interdependent on each other because the traditional servers and their operating environments were in simple words not computationally powerful enough and their bandwidth, and data processing and forwarding throughput was very less compared to these special hardware elements like Message Routers, Deep Packet Inspection devices, Content Distribution Network devices, along with Session Border Controller, WAN Acceleration, Firewall, Carrier Grade NATs, etc. used. A network's set of different functions can be sophisticatedly

divided into two planes, namely the **control plane and the data plane** also known as forwarding plane.
The control plane which deals with the setting up connections and how one node will interact with its adjacent nodes in terms of exchanging of routing tables and operations on signaling protocols.
Thus basically the work of control plane is maintaining, updating and exchanging routing table, establishing, maintaining and terminating connections and all these functions mentioned above are not bandwidth exhaustive but they require more computational resources and thus are computationally intensive. The data plane also known as forwarding plane is the engine of the routers and all the other specifically designed network elements. It has the responsibility of forwarding and processing of data. It manages all the Quality of Service functions, encryption, stuffing, fragmenting, encapsulation, queuing and that's why need fast custom-built hardware boxes. These functions all revolve around forwarding data and thus are bandwidth exhaustive. In layman terms the control plane is related with the software and data plane with the hardware. The researches in 2007-08 marked the beginning of network function virtualization leading to separation of control plane software and from the proprietary data plane hardware. The concept of virtualization is already well understood as it encompasses many areas of computer sciences. With the recent development of powerful industry set standard servers and their operating systems have now made it possible to run almost all type of network functions being executed almost completely by software which is running on shared standard hardware resources (the now powerful multi core x-86 processors) just like cloud computing based services. It is only the recent development of processing power of multi core CPUs, which can run multiple instances of different network functions on the same server with the help of virtualization, which can effectively and efficiently compete against the custom-built hardware devices used to implement different network functions in terms of cost, space and power usage. Thus network function virtualization is virtualizing the standard hardware to implement network functions completely by software on multi core processors using hypervisors rather than using highly costly custom-built boxes. In NFV the network functions are completely run by software on industry set standard servers. Thus the control plane functions and data plane functions now run on the standard servers which have now faster cache memory, high processing and forwarding speed. Also with the help of virtualization one machine can implement a variety of functions or can be used as multiple machines. Thus in NFV there is an incomplete separation between the data plane and control plane.

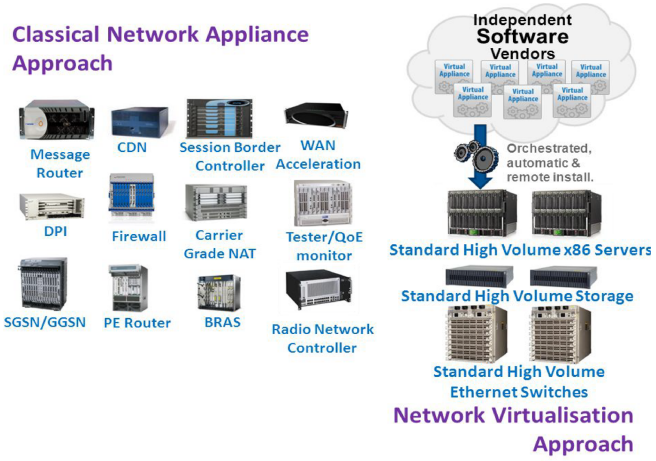

Figure 2

In Software defined networking or SDN, which looks after the transport functions of the network (up till the network layer) the data and the control plane are completely logically isolated as both are implemented across different physical systems or sandboxed.
The control plane is completely software based and the corresponding data plane is either implemented across the general x-86 processors or custom built hardware depending upon the computation power required and other factors. With SDN the infrastructure providers are able to achieve programmability to an extent that even the current routing protocols like BGP and OSPF cannot be compared with the new ones.
After NFV and SDN comes the third field under the virtualization of network where the resources with which a network is made i.e. the nodes and the media linking them are virtualized.

II. NETWORK VIRTUALIZATION

It can be seen that in NV the routers, network cards, firewalls and other network infrastructure associated resources are virtualized to create a virtual network. For instance router is virtualized by encapsulating the routing OS in Virtual Machine managed by a hypervisor or some VMM on top of the router we see today.

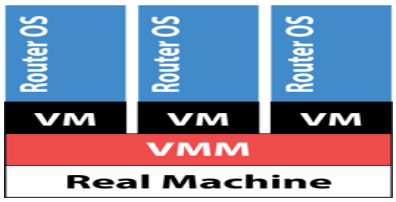

Figure 3

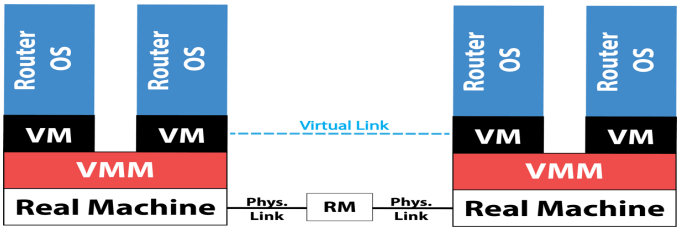

Figure 4

Virtual Routers give the advantage of having different routing mechanisms on the same machine at the same time. As seen above in Figure 4 we can see how two virtual routers are connected with a virtual link spreading across one or more than one physical (real) link and at the same time letting us program and change its properties like bandwidth.
Network Virtualization can be seen as the virtual networks created over the top of network infrastructure of one or more than one infrastructure provider by virtualizing the hardware underneath. All these virtual resources simulate the characteristics of the original hardware. After virtualizing the nodes the only way to interconnect them is by creating virtual links, which is the logical connection between these virtual nodes. As the network is now virtualized we can program the nodes and create new networks and terminate old ones dynamically thus making the network scalable and this leads to an efficient usage of resources. When we virtualize a network we change its framework and architecture and with that we create a future Internet, by not only introducing a test bed to implement new protocols but also a network hosting multiple protocol stacks with the help of programmability. As we virtualize the network the actors inside the service also change. The role of ISP is changed as now, the Network Infrastructure provider provides the infrastructure, the network is operated by Virtual Network Operator and the network is used by end users like us.

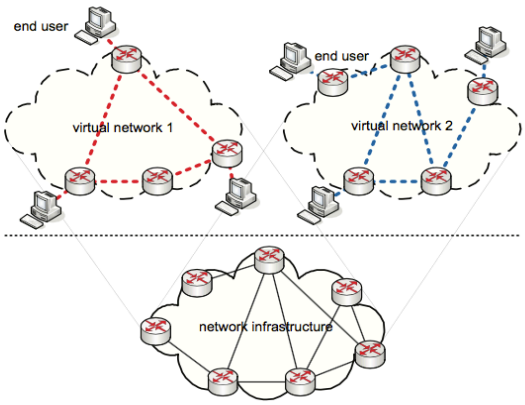

Figure 5

A virtual network can be instantiated easily by the Virtual Network Operator by finding out the network topology needed according to the physical resources available and required then determining which nodes to be set up, configuring them as per the protocols required and finally configuring the nodes' interface and connecting them with virtual links. Virtual Network can be scaled up/down dynamically by creating new nodes and connecting them with the VN or terminating a bad node. Changing the interfaces can change the configuration of the system and protocols set on the virtual node. The only performance drawbacks are minimum time required to set up a virtual node and maximum capability of the host.

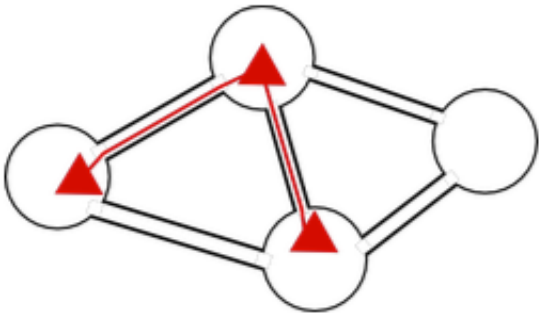

Figure 6

To promote and recognize energy efficiency and solve problems of under usage of resources, mobility, manageability and scalability of network, network virtualization acts as one for all kind of solution, but with these benefits it provides users with malicious interests new areas to exploit and access information which is being shared. This concept of virtualization of networks has a plethora of advantages but as the saying goes, with every good thing comes the bad; we have a lot of security loop holes in it. To understand these loop holes first we will understand what we mean by security. By the term security we mean to protect an object from unauthorized access thus allowing it to perform its functions continuously the way it is meant to do for the maximum amount of time in all cases. A computer network is made up of different nodes connected through different media sharing resources and these nodes can be attacked from within and outside the network. In Network Virtualization the network can be under attack both internally and externally. Before coming to the threats and vulnerabilities found in Network Virtualization we will discuss about security in general and then proceed towards possible security breaches specific to Network Virtualization.

III. SECURITY BREACHES AND MEASURES

If a system wants to connect to other systems and share resources it has to form or join a network. To maintain 100% privacy and secrecy of data the system ought not to communicate with anything. So either a system can be isolated or it can communicate within a network. If a machine wants to communicate it has to leave its security behind and rest somewhere in the middle and leave its privacy, as with the computing resources available today there is no scope for 100 percent privacy and security while communicating within Internet. The attacks can be done both from within the network and outside. Before listing out the types of attack we will list the consequences of these threats to have a better understanding.
As shown in figure 5 above the resources (nodes, switches, links) are shared in virtualized network and because of this it allows different user levels to maliciously gather information or play with the resources.
Following we have illustrated the how each user level can attack a different level.

Types of internal attacks

- VN → User
- VN → NI
- VN → VN
- NI → VN
- NI → User
- User → VN
- User → NI
- User → User

This is the list of possible user level attacks and in this paper we will be focusing on specific type of attacks possible in each type of user level interaction in different types of virtualization modes the network can go into.
A network is vulnerable to a plethora of attacks from all sides, therefore in RFC 2828: Internet Security Glossary (2000) Shirey R has listed out the attacks on the basis of what impact they have by segregating them into four different categories: disruption, usurpation, disclosure, and deception.
Disruption includes all the possible attacks, which are initiated to disrupt the services, which users have paid for or has access to. It basically deals with attacks, which overload or exhaust the network resources including the channel, routers or the storage servers in such a way that genuine users can't avail the services meant for them. DDOS and all its types are one of the major attacks, which disrupt the services. For a virtual network disruption attacks are aimed with the motto of disrupting the services provided by the network generally with the intent of vengeance, competition. Overloading the virtual nodes and exhausting them to their maximum serving capacity tampers the services. The attacks are generally distributed denial of services, which sends connection or ping requests to the nodes (including the end hosts) at rates of terabytes per second from remotely controlled network of distributed users which completely fills its buffer queues and overloads it till the point of failure, not allowing the genuine user to access the services and even not letting the operator to deploy and initiate new virtual networks. This can be purely accidental also as multiple users in a Virtual Network may have a need of resources at the same time in the same location. As mentioned earlier the attack can be from within the network also as a Virtual Network can attack another VN or Network Infrastructure itself by using more of the resources it was sharing with other virtual network, than it subscribed for. Also this attack can be from a User towards the VN or NI. Therefore a dynamic and intelligent management of resources is required in Virtual networks as to maintain the services as intentional attacks or accidental errors can overload one or more node disrupting the whole communication system. This can be avoided if Network Infrastructure isolates and sandboxes the different Virtual Networks and follows a fair resource utilization protocol. A lack of good virtual network management may lead to resource failure as while migrating from one node to another or while redistributing the load of a failed node we need to consider the factors like current resource usage, imminent resource usage otherwise the network requests may overload and hamper the node and thus the services. All internal attacks leading to disruption are from malicious interest and can be seen in the following diagram.

USER → VN **VN → co VN**

USER → NI **VN → NI**

A combination of a good management policy and security measures involving traffic flow analysis to prevent from majority of DDoS attacks can protect from the problem of disruption.
In *usurpation* the attacker tries to control the network or the system maliciously by overriding the security hurdles and then retrieve the paid services or protected data, or disrupt the legitimate services given by the network or access the underneath hardware comprising the network. These attacks are executed by mainly through SQL Injections, Cross-site scripting, and CSRF.
Creating a fraudulent identity that is privileged or authenticated by the Virtual Network can do usurpation attacks. This can be done by injecting corrupt packets in the network with fraudulent sources enacting a privileged entity through IP Spoofing letting the network to think of the attacker as an authenticated user or cross site scripting allowing the scripter to gain access to the database and then change it. The attacker can become a privileged user by initiating SQL Injection attack on the database and making themselves a privileged user. The attackers can even access the underlying hardware by attacking up with the loophole of the virtualization software by coming out of the VM and directly having control over the infrastructure as a malicious user by coming out of the Virtual Machine can control the whole router virtualized by full or para type of virtualization. These attacks are mostly internal as they can be easily implemented. For instance the network infrastructure provider can have hidden monitoring measures that can let them access the data being shared over the network. The users can try to control the resources directly or the other cohosted Virtual Networks can try to access the resources or database of the target Virtual Network. The diagram shows how different user levels can attack.

NI → VN **USER → VN**

VN → VN **USER → NI**

Implementing proper sand boxing between different virtual networks hosted on the same physical network and also checking that the accessibility powers the NI have are completely transparent can prevent these kinds of attacks. The type of virtualization being implemented should be considered and the entry holes for unauthorized users must be patched up.
Illegitimate *disclosure* is when the attacker seeks out the protected and private data by avoiding the security measures of the network. This data can be crucial to nations, institutes and thus by disclosure is in the wrong hands of hackers or people with malicious interests. Eavesdropping or Man in the Middle are the attacks in this category and mostly done through ARP Poisoning. These kinds of attacks are mostly done through sniffing on the data and gaining the knowledge of protected and private data of utmost importance. Not just eaves dropping on data leads to disclosure of information, as attacker can spoof the IP Address by corrupting the ARP tables and disable one of the nodes taking part in communication and join the communication and access the

data. This can also happen when network traffic is migrated from one virtual node to other and the attacker tries to deceive the network management and access all the crucial information by either being in the middle of the communication or at the receiving end. One way to protect all the data is to encrypt it and make it confidential, with this even if the attacker is able to intercept the data it won't be able to decipher it. Nowadays very strong encryption algorithms are used to protect the highly confidential data. But for attackers intending to plan an attack and wanting to extract crucial information about the network can do so irrespective of encryption by studying the traffic flow and analyzing it to know the topology and the architecture of the network. Traffic flow analysis enables the attacker to extract information about the server thus letting the malicious user know where to launch attacks in a virtual network. Internally this attack can be initiated by the Network Infrastructure provider by knowing the confidential routing table entries which are crucial to virtual network operator. As the network is virtualized the Virtual Network operator can introspect or in common terms only read the state and activity of processors data stored in memory, disk space utilized without able to change it. If vulnerabilities in the virtualization system are traced and exploited the administrators can access important data.
Also in a virtual network a lot of data is redundant at different locations to provide better network operations, which can be extorted and used for wrong reasons. Information Disclosure can be prevented by encrypting the data and following a fair, transparent management policy. The diagram shows how different user levels attack each other.

VN →co VN **USER → NI** **VN → USER**

NI → VN **VN → NI**

Deception is done when the attacker deceives systems and networks by imitating as a privileged or authenticated user. In this the bad users convince nodes that they are what they pose to be by creating fake identities. It can be caused mostly through the means of IP Spoofing, DNS Spoofing, and VLAN Hopping. The attacker can spoof its IP Address and deceive the system by identity fraud and its user that it's the node it is claiming to be. Identity frauds are more common in virtual networks because of its dynamic addition and removal of different entities, and migration and load balancing techniques adopted. Once system is deceived it lays down path for more threats like disclosure, usurpation, which will even enable the attacker to edit the registry entries thus cleaning the trace of all the records of network activities and logs thus cleaning the spill. Internally this attack can be done by malicious users of Virtual Networks sharing the same infrastructure with that of the victim by accessing the common nodes and deceiving the system. Also the malicious users can initiate replay attacks by creating fake packets with spoofed source and sending them in the network and deceiving it to communicate with it by taking advantage of the flow control mechanisms. Therefore to counter all these kind of breaches we need a good fool proof framework. The diagram shows how different user levels can deceive each other.

VN → VN **USER → VN**

USER → USER **VN → USER**

With the table below we summarize the attacks and their consequences

Table of Attack consequences and types

Attack Consequence	Type of attack	Measure
Disclosure	Information Leakage	Access Control, Authentication Confidentiality
Disclosure	Information Interception	Access Control, Authentication Confidentiality
Disclosure	Introspection Exploitation	Access Control, Authentication Confidentiality
Deception	Identity Fraud	Access Control, Authentication Confidentiality
Deception	Loss of Registry Entries	Access Control, Authentication Confidentiality
Deception	Replay Attacks	Access Control, Authentication Confidentiality
Disruption	Physical Resource Overloading	Availability
Disruption	Physical Resource Failure	Availability
Usurpation	Software Vulnerability Exploitation	Access Control, Authentication Confidentiality
Usurpation	Identity Fraud	Integrity

IV. CONCLUSION AND FUTURE WORK

It can summed up that everyday new attack strategies are generated to disrupt and deceive the system, for disclosure and usurpation of data and system but to tackle this network researchers and industry experts need to create a fair, transparent and fool proof management policy for virtual networks implemented through Network Virtualization. Researchers and Network programmers should focus on a policy that should ensure that the system can authenticate users based on different layers of security like verifying what the user has that is the username and password and what the user is that is by taking the biometrics of the user and thus validating and authenticating it. Authentication is done to make sure that the attackers do not deceive the system. One more layer of authentication can be implemented to counter IP Spoofing is also by verifying the location of packet's source and that of the source IP Address stored in registry entries. It should also control their access allowing the VN operator to allow different users access system with different privileges and rights transparently administering the functions of users and checking the permissions given to them. A considerable focus should be on the type of virtualization and what loop holes it has. Access Control Mechanisms are there to ensure that a fair management practice is followed. Confidentiality is required to make sure that no unauthorized disclosure of information is there and thus the data should be encrypted to provide data confidentiality. Additionally the system policy should not allow the attackers to extract the traffic flow and analyze it. To counter with usurpation mechanisms must be there to ensure that data is integral and not a bit has been changed, corrupted, destroyed to mislead. Also measures should be there for data recovery. The whole point of having a communication system is pointless if the system is unavailable, therefore a management policy with clear load balancing and migrating policies with anti DDOS measures must be followed. Also, the system must make sure that nonrepudiation is followed thus inhibiting the attacker from denying its participation in illegitimate activities.

V. LIST OF REFERENCES

[1] Shirey R (2000) RFC 2828: Internet Security Glossary. http://www.ietf.org/ rfc/rfc2828.txt

[2] Stallings W (2006) Cryptography and Network Security: Principles and Practice. Pearson/Prentice Hall, Upper Saddle River, New Jersey, USA.

[3] Cavalcanti E, Assis L, Gaudencio M, Cirne W, Brasileiro F (2006) Sandboxing for a free-to-join grid with support for secure site-wide storage area. In: International Workshop on Virtualization Technology in Distributed Computing. IEEE Computer Society, Washington, USA.

[4] Wolinsky DI, Agrawal A, Boykin PO, Davis JR, Ganguly A, Paramygin V, Sheng YP, Figueiredo RJ (2006) on the design of virtual machine sandboxes for distributed computing in wide-area overlays of virtual workstations. In: International Workshop on Virtualization Technology in Distributed Computing. IEEE Computer Society, Washington, DC, USA.

[5] Wu H, Ding Y, Winer C, Yao L (2010) Network security for virtual machine in cloud computing. In: Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference On. IEEE, Seoul, South Korea.

[6] Leonardo Richter Bays, Rodrigo Ruas Oliveira, Marinho Pilla Barcellos, Luciano Paschoal Gaspary and Edmundo Roberto Mauro Madeira (2015) Virtual network security: threats, countermeasures, and challenges.

[7] Network Functions Virtualisation – Introductory White Paper.

[8] Andreas Fischer, Network Virtualization in the Future Internet Concepts, Applications, and Challenges.

[9] Nelson Gonzalez, Charles Miers (2015) A quantitative analysis of current security concerns and solutions for cloud computing.

[10] N.M. Mosharaf Kabir Chowdhury and Raouf Boutaba (2014) Network Virtualization: State of the Art and Research Challenges.