The Security Implications of Virtual Local Area Network (VLAN)

NAME: DEB, HRIDOY CHANDRA ID: 18-36333-1 SEC: B

Motivation

When I was doing computer network course i was knowing about VLAN. Virtual Local Area Networks (VLANs) have seen tremendous expansion in recent years, owing to strong attempts to enhance Metro Ethernet capabilities. A virtual local area network (VLAN) is a logical grouping of network users and resources connected to specify the operation of activated ports on a switch administratively. A local area network (LAN) is a collection of computers and devices that share a communications line or wireless link with a server located within the same geographic area. VLANs make it simple for network administrators to divide a single switched network into many subnetworks. Without needing to execute additional code to meet their systems functional and security needs or make significant changes to their current network infrastructure VLANs are often set up by larger businesses to re-partition devices for better traffic management. VLANs are also important because they can help improve the overall performance of a network by grouping together devices that communicate most frequently. VLANs also provide security on larger networks by allowing a higher degree of control over which devices have access to each other. VLANs tend to be flexible because they are based on logical connections, rather than physical. So, I think there are lots of opportunities to work in this field. It needs more research and deployment.

Introduction

A virtual LAN is a broadcast domain created by one or more switches. The switch generates a VLAN simply by putting some interfaces in one VLAN and some in other. So, instead of using all ports on a switch to generate a single broadcast domain, the switch divides them into several. Without VLAN a switch treats all interfaces on the switch as being in the same broadcast domain- it means all connected devices are in the same LAN. Virtual Local Area Networks (VLANs) have seen tremendous expansion in recent years, owing to strong attempts to enhance Metro Ethernet capabilities. One of the key goals of these work was to improve scalability and enable users to capture more bandwidth at a lower cost, while also enhancing transparency for widespread use and dealing with challenges related to flexibility and security (Gobjuka, 2010). VLANs play an important function in modern networks since they connect layers 2 and 3 of the ISO hierarchy. Many enterprise networks, such as those used by industry and university campuses, as well as data centers, have extremely complicated layer-2 VLAN structures underpinning the logical layer-3 network, consisting of tens of thousands of geographically dispersed network devices. With the growth of VoIP services supplied by devices such as IP phones and multimedia applications, the demand for VLANs has skyrocketed. VLANs are logical network splits inside a single underlying network. Regardless of physical location or connectivity, devices in a VLAN communicate with one another as if they were on the same Local Area Network (Bays, 2015). All frames sent through a network are tagged with their corresponding VLAN ID, processed by VLAN-enabled routers and forwarded as necessary. Since isolation is typically based only on packet tagging, this approach is susceptible to eavesdropping attacks. In addition to creating different topologies, virtual networks are not restricted by other attributes of physical networks, such as protocol stacks. In this way, you can create virtual network infrastructure instances tailored specifically to the needs of different network applications (Fernandes, 2011). These functions also support the creation of virtual tests similar

to real-world infrastructure, which is a valuable benefit for evaluating newly developed architectures and protocols without affecting production traffic.(Anderson, 2005) For these reasons, Virtualization of networks has piqued the interest of a lot of experts throughout the world, particularly in the context of Future Internet study. The industry has embraced network virtualization as well. Virtualization is currently supported by major industry companies such as Cisco and Juniper, and this additional feature has allowed infrastructure providers to offer new services.

Literature Review

The paper ‘‘The Security Implications of Virtual Local Area Network (VLAN)" (Bassey, 2016)proposes that any subscriber who is connected to the physical network has access to the network resources on that LAN. Second, subscribers were supposed to plug a network analyzer into the hub and monitor all traffic on the network. Users could also join a workgroup by simply connecting their computers to the existing hub. These media resulted in a significant level of vulnerability across the entire network. VLAN was introduced into the internet-work to govern these practices and stop the unwholesome trend. This was done by building another LAN and creating multiple broadcast groups; thereby configuring full control over each port and user (Voelker, 2009). The idea of anyone just plugging their workstation into any switch port and gaining access to the network resources was eradicated. The administrator can now control each port and resources accessed by every port. (Inamdar, 2018)

A central, scalable and resilient protection architecture for enterprise networks is presented in (Martin Casado, 2006), which proposes a framework in Layer-2 similar to VLANs. All connectivity within the company network is governed by a single protective layer in the proposed framework. All routing and access control choices in an enterprise network are determined from a logically centralized server. The central server enables service access by distributing encrypted source routes, which are referred to as capabilities. In enterprise networks, reachability control and virtual local area network (VLAN) designs are two important design responsibilities. In (Sung, 2010), authors showed the importance of a systematic approach to these key tasks. Authors also devised a set of algorithms to solve the formulated problems, and provide a validation of the systematic approach on a unique large scale campus network data-set. A group of researchers conducted the first and most extensive evaluation of an actual VLAN design in an operational campus network using a white-box (Garimella, 2007) approach. While campus networks are distinct from enterprises in general; the size of the network, the availability of data, and the extensive use of VLANs, makes this study important in providing a framework to understand the issues involved in enterprise networks. There are several network access control solutions in the market. In a university campus network, researchers (Flores, 2017) tested devices like Packet Fence. They demonstrated the need of having a network access control technology in place to protect university networks from new assaults (Inamdar, 2018).

VLANs allow you to separate users by putting them in various VLANs, but how do you get traffic from one VLAN to another? To do so, a Layer 3 device is used to route traffic from one VLAN to another. For inter-VLAN connectivity, the ideal option is to utilize a router Each router interface is connected to an access link, which is connected to hosts in the traditional fashion. Three physical interfaces are required for three VLANs in this setup. The router fast Ethernet interface is connected to the VTP server switch interface and configured using ISL or 802.1q trunking in the paper "Effective VTP Model for Enterprise VLAN Security" (Verma, 2013)proposed, rather than being connected to an access connection. The use of a trunk link has the advantage of reducing the number of router and switch interfaces required.

The paper "Design and implementation of application-based secure VLAN" (Zhu, 2004)said they tested network applications that use static port numbers (ssh and ping) and dynamic port numbers. They monitored traffic via the S-VLAN lines with ethereal. They discovered that ethereal could not decode the S-VLAN packets beyond stating that they were compliant with the 802.1Q VLAN standard. The encrypt process, as expected, obscured the source and destination MAC addresses, as well as the L2 payload. They also evaluated the scenario in which a "attacker" attempts to utilize a secured application, such as

ssh, after entering the network through an untrusted "weak" edge switch. The "attacker" might still connect to other services on a trustworthy switch-protected server.

The paper "Security features in Ethernet switches for access networks." (Guruprasad, 2003) proposes that the YLB2800's security features, which have been fine-tuned for use in access networks. It has powerful micro-engines that are meant to process packets at wire speed and may be accessed by the service provider via API and/or other high-level interfaces. Building access aggregators, DSLAM backplanes, and mxu switches benefit from the PLB2800.

By knowing the MAC address of the target system, a malicious device can easily defeat the protection of a VLAN. In order to pose a real threat to VLAN security, attackers must have intimate knowledge of the devices they are targeting as well as their locations. Once attackers have the MAC address of the target device, they can create a static address entry for it in the attacking system's local ARP cache. This allows for direct communication between the devices even though these devices exist on separate VLANs (Farrow, 2007, Jan. 4). Trunk ports on switches create a communication channel that allows a single set of VLANs to be shared across several switches. A Trunk port is used when a switch is connected to an existing infrastructure. Packets are transmitted between switches with their VLAN tagging intact, preserving traffic separation by maintaining each packet's VLAN designation (Leischner, 2007).

One such method is to use multiple virtual network queries to discover the topology of the physical infrastructure, explored by (Pignolet, 2013). This is a security risk because infrastructure providers are generally unwilling to disclose this information. The author demonstrates this by sequentially requesting a series of virtual networks with different topological properties and analyzing the responses from infrastructure providers (i.e., whether the request can be embedded or not), You can gradually get information about the physical topology. In addition, the author defines the number of queries required to fully reveal the physical topology in networks with different topologies Conversely, the paper "Minimum disclosure routing for network virtualization and its experimental evaluation." (Fukushima, 2013) The entity claiming to manage the physical network can obtain sensitive routing information from the virtual network above. Since current routing algorithms need to send and receive routing information through virtual routers, sensitive information may be exposed in the core network.

A number of surveys on cloud computing security have been conducted in addition to the broader studies on network virtualization reported thus far. Virtualization of both machines and networks is common in cloud computing environments, making this a highly important related issue for my thesis. While there is some overlap between cloud computing security and virtual network security, I want to highlight that cloud computing is a very specialized use case of network virtualization that provides a very different set of security concerns. "Security and privacy in cloud computing: A survey." (Zhou, 2010) provide an investigation on security and privacy issues of cloud computing system providers. Additionally, the authors highlight a number of government acts that originally intended to uphold privacy rights but fail to do so in light of advances in technology. "An analysis of security issues for cloud computing." (Hashizume, 2013)in turn, focus on security vulnerabilities, threats, and countermeasures found in the literature and the relationships among them.

Main objective:

The objective of this research is to boost network security and performance while also making management easier and ensuring network flexibility.

Sub-objective 1:

To investigate how to improve vlan network security.

Sub-objective 2:

To investigate the network security large and small area.

Sub-objective 3:

to look at the most serious flaw in vlan network security.

Sub Question 1:

Is the Lan capable of ensuring the usefulness and security of the wifi system?

Sub Question 2:

Does the wifi system's usability and security rely on the Virtual Local Area Network?

Sub Question 3:

Is the Virtual Local Area Network usable and secure in both small and big area?

Proposed Research Methodology

The procedures or strategies used to find, select, process, and analyze information about a topic are referred to as research methodology. The methodology portion of a research article allows the reader to critically examine the study's overall validity and dependability. In this research topic, Formal and Experimental methodology will be followed. Formal methodology is most frequently used in theoretical Computing Science and the computer science literature is flooded with experimental articles that are irrelevant even before they are published.

To model and evaluate systems, formal approaches take a three-step approach. Engineers or designers use a modeling language to precisely characterize the system during the formal specification phase, usually utilizing formal mathematical syntax and semantics to eliminate inaccuracies and ambiguities. Writing system specs is similar, but not in the same way. Engineers then used the specifications to build a set of theorems about system behavior. These theorems are supported by mathematical proof, ensuring that the system's behavior is logically sound and really desired. It can prevent costly errors from arising late in development since it allows designers and engineers to detect usability flaws before the project is implemented in code. Following the definition and verification of the model, the implementation can finally begin with the conversion of the specification into code.

Formal techniques have a number of advantages: they aid in the clarification of system specifications and the formation of implicit assumptions, they uncover mistakes in system requirements, and their rigor aids in the better understanding of the problem. Because they employ a formal language, numerous colleagues can independently verify requirements, reducing errors early in the development process. Formal approaches, on the other hand, cannot totally replace traditional quality assurance methods, hence they should only be used in conjunction with system design.

In Experimental methodology there are some set of good practices that will make my work organized, low time consumption, resources assembling and reduce costs. The practices that I will follow are:

Record Keeping: In experimental work, keeping good records is crucial. The record-keeping practices of computing-science researchers are shockingly lax. Inexperienced researchers have a propensity to believe that because studies are done on computers, they can replicate them later if necessary. As a result, they are less diligent than they should be in labeling and filing the results in a way that allows them to be retrieved and checked later. It can be difficult for a researcher to recreate his or her own tests since he or she does not recall which machine was used, which compiler was used, which flags were set, and so on. Computers, in reality, are highly fleeting items. In a few months, the computer in the lab today will most likely no longer be available in this configuration. As a result, experimental computing science would benefit immensely if each experimental computing scientist treated her experiment with the same care that a biologist would give a slow-growing bacterial colony. An experimental scientist's work must be annotated, filed, and documented in order for it to be relevant in the future.

Experimental Setup Design: During the exploratory phase of an experimental project, speed is crucial. As a result, this step is generally handled with less attention than it should be. After the exploratory phase, a researcher should halt and document the findings, as well as the features of the hardware and software that will be utilized in the evaluation phase.

Reporting Experimental Results: Numbers should be incorporated in a document or placed into a report to answer a question or make a point. To emphasize the arguments made by the researcher, graphical or table representations should be properly chosen. They must not deceive or twist the data. Analyzing data solely on the basis of aggregation is risky since averages can be deceiving. Even if the raw data is not published in a paper, the author should thoroughly analyze the raw data to acquire a better understanding of the experiment outcomes. The numerical results in the tables and graphs should be accompanied by a careful written analysis and discussion of the results. This discussion should not merely verbally repeat the results that have been presented in tables and graphs. This discussion should provide information about these results and add knowledge that the researcher has acquired but not included in these figures. Alternatively, this discussion should try to explain the results presented.

References

Gobjuka, Hassan. "Topology discovery for virtual local area networks." *2010 Proceedings IEEE INFOCOM*. IEEE, 2010.

Bays, Leonardo Richter, et al. "Virtual network security: threats, countermeasures, and challenges." *Journal of Internet Services and Applications* 6.1 (2015): 1-19. (Bays, 2015)

Geoffrey M. Voelker (2009). Characterizing user Behavior and Network Performance in a Public Wireless LAN. Proceedings of the 2009 IEEE International Conference on Communication, 1287- 1291.

Bassey, Donatus Enang, B. E. Okon, and Remigus Umunnah. "„ Security Implications of Virtual Local Area Network (VLAN), Niger Mills, Calabar, Nigeria‟." *International Journal of Scientific & Engineering Research (IJSER)* 7.3 (2016): 1187-1194.

Inamdar, Mohammed Suhel, and Ali Tekeoglu. "Security analysis of open source network access control in virtual networks." *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. IEEE, 2018.

Casado, Martin, et al. "SANE: A Protection Architecture for Enterprise Networks." *USENIX Security Symposium*. Vol. 49. 2006.

Sung, Yu-Wei Eric, et al. "Towards systematic design of enterprise networks." *IEEE/ACM transactions on Networking* 19.3 (2010): 695-708.

Garimella, Prashant, et al. "Characterizing VLAN usage in an operational network." *Proceedings of the 2007 SIGCOMM workshop on Internet network management*. 2007.

Flores, J., Ramos, V., Lozada, R., & Flores, T. (2017, October). Analysis of solutions of network access control to improve in and out securities on corporative networks. In *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)* (pp. 1-5). IEEE.

Verma, Rajiv O., and S. S. Shriramwar. "Effective VTP Model for Enterprise VLAN Security." *2013 International Conference on Communication Systems and Network Technologies*. IEEE, 2013.

Zhu, Minli, Mart Molle, and Bala Brahmam. "Design and implementation of application-based secure VLAN." *29th Annual IEEE International Conference on Local Computer Networks*. IEEE, 2004.

Guruprasad, A., P. Pandey, and B. Prashant. "Security features in Ethernet switches for access networks." *TENCON 2003. Conference on Convergent Technologies for Asia-Pacific Region*. Vol. 3. IEEE, 2003.

R. Farrow. VLAN Insecurity. [Online]. available :http://www.spirit.com/Network/net0103.html

(2007, Jan. 4).

Leischner, Garrett, and Cody Tews. "Security through VLAN segmentation: Isolating and securing critical assets without loss of usability." *proceedings of the 9th Annual Western Power Delivery and Automation Conference, Spokane, WA*. 2007.

Zhou, Minqi, et al. "Security and privacy in cloud computing: A survey." *2010 Sixth International Conference on Semantics, Knowledge and Grids*. IEEE, 2010.

Hashizume, Keiko, et al. "An analysis of security issues for cloud computing." *Journal of internet services and applications* 4.1 (2013): 1-13.

Fernandes, N. C., Moreira, M. D., Moraes, I. M., Ferraz, L. H. G., Couto, R. S., Carvalho, H. E., ... & Duarte, O. C. M. (2011). Virtual networks: Isolation, performance, and trends. *Annals of telecommunications-annales des télécommunications*, *66*(5), 339-355.

Anderson, T., Peterson, L., Shenker, S., & Turner, J. (2005). Overcoming the Internet impasse through virtualization. *Computer*, *38*(4), 34-41.

Pignolet, Yvonne-Anne, Stefan Schmid, and Gilles Tredan. "Adversarial vnet embeddings: A threat for isps?." *2013 Proceedings IEEE INFOCOM*. IEEE, 2013.

Fukushima, Masaki, et al. "Minimum disclosure routing for network virtualization and its experimental evaluation." *IEEE/ACM Transactions on Networking* 21.6 (2013): 1839-1851.