A Critical Review of Techniques for Security and Measurement in a Switched Network

Emerole Kelechi C, Achumba I

***Abstract*— A network is set up to switch calls or route packets from one point to another. This is to enable communication to occur. In this paper, we reviewed the threats being faced by networks and its users and the techniques deployed to mitigate against these threats. We also expounded on various techniques and tools for measuring network bandwidth and traffic. With the availability of these tools, proper traffic problems can be diagnosed and appropriately logged for analytical purposes**

***Index Terms*—Packet switched network, circuit switched network, hacking, Network intrusion detection, signature-based detection, replay, hijacking**

I. INTRODUCTION

A switched network is made up of switches which have the function of directing either voice or packets from the source to destination [1]. There are two categories of switched networks;

A. Packet switched networks

Here a virtual circuit is set up between network nodes for communication to occur. Datagram or packets are sent from a sending node to the destination node through routers, bridges, gateways, firewalls or switches. The forwarding of packets is aided by the use of a routing tables which enable routers determine the best path to the destination[2]. We have unicast, broadcast and multicast, anycast and geocast routing schemes which depend on the number of nodes that receive a message from a particular node and the location of such nodes[3]. They employ modems for data exchange and frequency is allocated to the various nodes connected to the network.

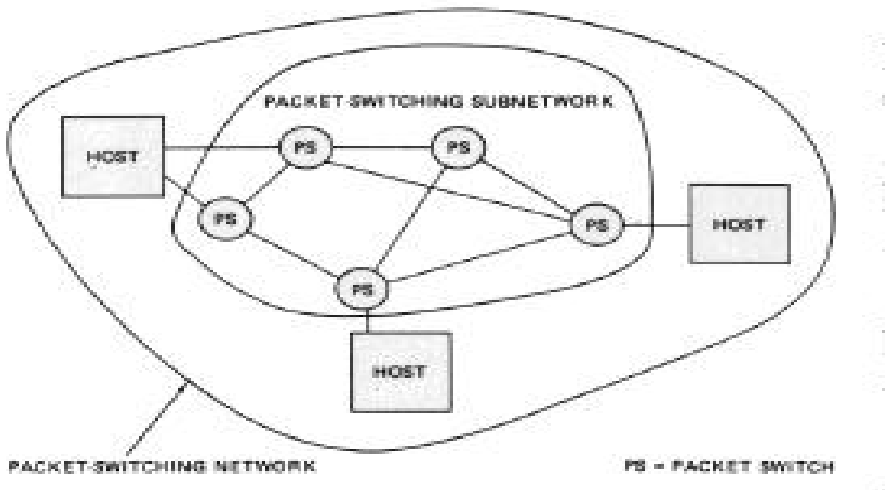

Fig1 Packet Switched Network [4]

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

B. Circuit switched network:

During call setup a dedicated circuit is used to route the call from the caller to the receiver. The circuit is engaged and no other subscriber can make use of it until the current call is terminated [29][103].

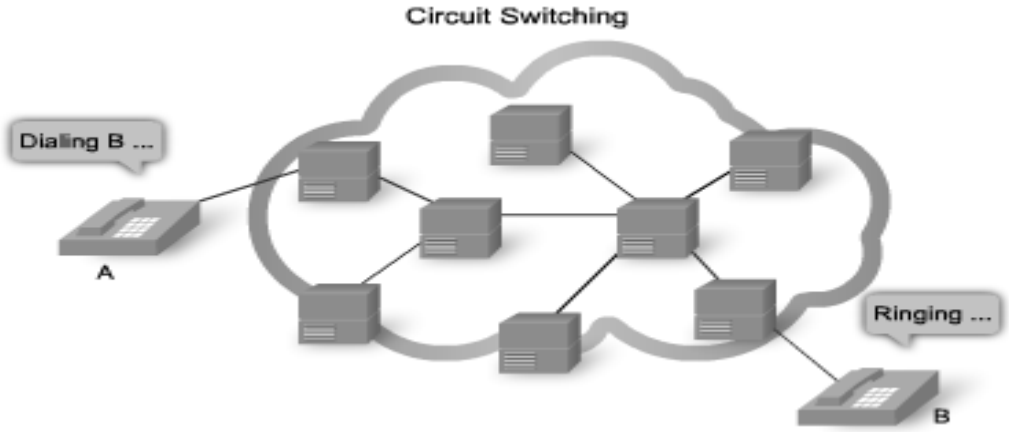

Fig 2 Circuit Switched Network[1]

II. Network Security

The goal of a network security is to monitor and analyze network events to able to sense abnormal activity which seeks to compromise data integrity and sends a log file to the network administrator[6]. We can say that the network has been attacked by outside influences, these attacks can be defined in several ways; Application Layer attack, Network Layer attack, Active attack, Passive attack and so on. The specific instance, of these attacks includes; false entry on the route table, packets dropping randomly. The security mechanism put in place against such attack have been found to lack the necessary arsenal to mitigate these attacks. The Network shared access layer is usually susceptible to the effects of these attacks. This is because of its exposure to resources from unverified sources. [7] Proposed a system which uses IDS agents to monitor and detect these anomalies. It detects these malicious activities and the source by sending control signals to the network. With cooperation from the nodes in the network, the source is detected and alerts are sent to warn other nodes about the malicious node.

A. Hacking

Hackers are agents that try to penetrate network security through the internet in order to steal resources. Activities of hackers have posed great challenges to proponents of greater network security. The hackers can break into a computer system remotely and modify the resources therein causing great harm to data storage mechanisms. Ethical hackers are employed to design systems that will protect a computer system from the activities of hackers. According to[6] hackers motives range from pay off to revenge on past deeds or just for enjoyment. There are several software tools at the disposal of these hackers to carry out their nefarious activities.

Network security systems scan the network and IP addresses to detect systems with weak defences. One of such system is the demon dialer to hack data connection equipment for network users[8][9]. After scanning, a software called Trojan is installed remotely to steal and destroy resources, passwords and files available in such a system.

B. Network Threats

Unauthorized users of a network can be potential threat to network defences and they constitute external threat to the network. Authorized users especially employees of organizations can also be a potential threat and they are difficult to detect. This is because they are part of the system and have been trusted overtime. Skills are deployed by network intruders to able to tear down these strong defences; knowledge of designs, security framework, software tools, scripting and use of the internet..

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

C. Network attacks

An authorized user can collate network data or information that would enable launching a full scale attack. Such information like domain names, IP addresses, passwords, e-mail addresses and phone numbers can be quite a handy tool for full scale attack. They use a war dialer to dial phone numbers in order to find a modem that is vulnerable and the application logs the number for future attacks [10]. They can also packet sniffing tools to hack and modify data packets. Passwords are cracked from the server and used by hackers to gain access to a system. Some password crackers can attempt to gain access by computing available passwords that can be able to grant access. [10] recommends the use of One-time passwords systems(use of tokens) and cryptographic authentication to mitigate password attacks.

Man-in-the-middle attacks take the advantage of loopholes in the IP protocols to hack into computer systems. Instance of these attacks are IP spoofing, session hijacking and replay, rerouting packets and web attacks[8].

IP spoofing involves masking an intruder's identity by using the IP address of a computer to gain access to that computer. It usually used in point-to-point networks to introduce extraneous data into data frames. To militate against IP spoofing there are schemes which would be enumerated in the next section

D. Network Security Techniques

1). RFC 2827 filtering: This removes extraneous IP addresses not available on the network. it also filters packets with IP addresses assigned to a particular network from entering another network in order to prevent spoofing the destination network[11]. This means only packets with IP addresses assigned to that network are allowed to be routed through the network.

2). RFC 1918 filtering: Packets with RFC defined ''private" addresses are filtered from a network.

3). Non-IP address authentication: Having alternative means of authentication like the cryptographic authentication and One Time password system can go a long way to eliminate spoofing.

4). Replay and Hijacking: Packets can be intercepted on the routing path especially if the traffic authentication mechanism is weak. These packets can be tampered with meaning there IP addresses and their sequence number can be changed before they are rerouted. These sequence of action constitute session replay and hijacking[11].

5). Non-repudiation: Communicating entities can use Non-repudiation techniques to ensure and efficient delivery of data. This will ensure that both entities actually entered into a contract to exchange information. A case where one entity breaches the terms of agreement, a situation called repudiation might arise [12]. Non-repudiation techniques include Use of digital signatures, confirmatory receipts and timestamps.

We have categories of Intrusion detection systems[9][13]

1) Reputation based Intrusion detection system: This system works exactly as that proposed by[7].
2) Incentive based intrusion detection system: This system works by collaboration from network nodes to reduce the incidence of malicious attacks.
3) Stack-based intrusion detection systems: The packets are monitored at the TCP/IP stack
4) Host-Based Intrusion detection system: Network clients have monitoring tools installed in them which analyzes data logs, files(password files, directories, access control lists) to detect any change and system state[6]. Example of software programmes are Tripwire, OSSEC etc
5) Network Intrusion detection system: These agents monitor all the system in a network and traffic through the network to seek malicious activity. These agents are installed on switches, hubs. Example is Snort[13].
6) Stateful Protocol Analysis Detection: These monitor packets to know whether they conform to standards and logs any discrepancy.
7) Statistical anomaly-based detection: Thresholds are set and traffic is monitored using statistical methods. It is expected that network events meets minimum threshold of normal activity.
8) Signatures-Based Detection: This employs signatures to monitor network traffic. These are simulated attack patterns. If there is any activity that matches these patterns, the system logs the activity [14].
9) Wireless Intrusion prevention systems: This deployed in wireless networks to monitor traffic and protocols. They also stop malicious activities from attacking network by sending alarms, dropping infected packets, correcting cyclic redundancy check errors, fragmentation, sequencing errors and total blocking of malicious applications.

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

10) Firewalls: They are installed between networks to monitor traffic.

Through sending echoes across the network, a suitable path can be defined for routing data packets. If acknowledgments are not received that shows the packet is having issues. Noise generated from software bugs and corrupt packets can degrade the performance of an Intrusion detection system.

A method of filtering packets based on packet send ratio(PSR) and packet delivery ratio(PDR) has been proposed[7].

1) Packet Send Ratio: Ratio of packets sent out from a network host successfully compared to the total packets required to be sent.
2) Packet Delivery Ratio: Ratio of delivered packet that reaches their destination to the total packets sent. PDR is measured at the destination host by checking the packets with no CRC errors as compared to those received.

Also a filtering database, internet client's address table and internet client blacklist table is created to store IP addresses from potential hackers [7].

III. Network Measurements

The internet is a large symposium of heterogeneous and independent networks. Expansion plans, greater transmission speeds and increased traffic have posed serious challenges to network administrators [15]. To tackle protocols like the Simple Network Management Protocol has provided Network managers with the requisite tools to be able to manage and allocate computing resources efficiently. The manager gets network data from measuring output characteristics of nodes in the network. One of the tools used for measurement is the NetFlow tool. The limitations to router design in terms of measurement capabilities can be attributed to its confinement to its core function of routing packets across the network[38]. Standards to measure the quality of services offered by the internet are defined by the Internet Engineering Task force. Nowadays, RouteViews ad RIPE RIS provide routing data and give information about the Border Gateway Protocol[16].

Passive measurement involves monitoring and collating internet data at different points of the network without any form of modification in terms of generating new data. An example of a passive measurement tool is the DAG card[15]. Active measurement new data is generated and fed to the network to monitor the response. The information provided is not as detailed as those provided by passive measurement. Test packets called probe are sent from one node to the other to monitor the traffic sent between both nodes. This indicates active measurement.

Another tool of choice is the ping facility(Packet Internet Groper) which is used to verify IP address by sending an echo request to another node which responds with an echo response. This tool also measures network delay which is the time it takes for a packet to go from the sender to destination and back. Due to the dynamic nature of network characteristics, active measurements might not be effective to measure network traffic. To measure the delay, the sender and destination should be synchronized with Network Time Protocol servers though errors abound. To militate against these errors, Global positioning system cards is used [15]. Traffic can be classified according to speed of flow and its lifetime[15].

A. Internet Measurement Techniques

In this section we enumerate several techniques to measure traffic on the internet.

1) Bandwidth Measurement: Bandwidth measurement by network administrators is done using Simple Network Management Protocol. Table 1[15] gives a picture of the tools used in measuring bandwidth

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

Table1 Bandwidth Measurement Tools [17]

Tool	Metric	Method
Pathchar	Per-link capacity	VPS
Clink	Per-link capacity	VPS
Bprobe	End-to-end capacity	PPTD
Nettimer	End-to-end capacity	PPTD
Pathrate	End-to-end capacity	PPTD
Sprobe	End-to-end capacity	PPTD
Pathload	Available bandwidth	SLoPS
IGI/PTR	Available bandwidth	SLoPS

The three ways by which network bandwidth is measured and these techniques assume that traffic characteristics is static are the[15];

i. Variable Packet size probing: This measures the bandwidth in individual communication channels
ii. Packet pair/ train dispersion: This measures the maximum bandwidth from sender to destination communication channels.
iii. Self loading of periodic streams: This measures the maximum available bandwidth of the communication channel between the sender and destination.

2) Traffic Measurement: To measure the traffic in a network, the traffic at the end points and also the individual channels should be estimated. This is defined under network tomography [15]. Routing protocols can provide information about traffic patterns and also the shortest path for routing protocols. One of such routing protocols is the Simple Network Management Protocol.

3) Traffic Diagnosis: Changes in traffic patterns at the individual channels can be detected and logged. These changes can lead to congestion issues in the network thereby degrading the reliability of the system. To detect these changes might pose challenges to network administrators when a large volume of network traffic has to be processed. These changes which might lead to poor network performance include router mis-configuration, Anomalies in BGP, denial of service and so on [15]. These changes can be classified and then logged which will give a picture of how they affect the network. To take samples of packets for analysis, a hash function is applied and if the result is between a certain thresholds such packets are processed. Applying a second hash function, the sampled packets can be labelled. This label which identifies the sampled packets is now sent to the measuring system for analysis.

IV. CONCLUSION

The issue of Network security cannot be overemphasized; this ensures that network users receive uninterrupted services and data integrity. We have tried to review network measurement techniques and its role in traffic diagnosis. We implore network administrators to take these tools seriously to ensure that network services are up and running.

REFERENCES

1. Md. Saidul Alam Khandkar and Fazlul Haque A.(2009). Comparative Analysis of Packet Switched Networks Over Circuit Switched Networks. In: Proc. of the National Conference on Communication and Information Security(NCCIS) Daffodil International University, Dhaka, Bangladesh, 14 Feb. 2009.
2. Larry L. Peterson, Bruce S. Davie(2011). Computer Networks: A systems Approach. Morgan Kaufmann 11th March 2011.
3. Forouzan B. H., Data Communication and Networking, TMH Pubilcations 4th Edition.
4. Zhan-Zhen Wei and Feng Wang(2006). Achieving Resilient Routing through Redistributing Routing Protocols and Introduction to EIGRP. Pages 4, 2006.
5. Matthew Desantis, US-Cert. Understanding of Voice Over Internet Protocol. Pp 2-3.
6. T. Boyles, CCNA Security Study Guide: Exam 640-553. John Wiley and Sons, 2010, 249-280
7. F. Anjum, D. Subhadrabandhu and S. Sarkar. "Signature based intrusion detection for wireless Ad-hoc networks, " Proceedings of Vehicular Technology Conference, Vol. 3, pp. 2152-2156, USA, Oct. 2003

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

8. M. E. Whitman, H. J. Mattord, Principles of Information Security. Cenage Learning EMEA, 2009, 289.
9. Vacca J. R(2010). Managing Information Security. Syngress 2010, pg 137.
10. E. Kirda, S. Jha, D. Balzarotti, Recent Advances in Intrusion Detection: 12th International Symposium, RAID 2009, Saint-Malo, France, September 23-25, 2009, Proceedings. Springer. Pp. 162.
11. R. C. Newman, Computer Security: Protecting Digital Resources. Jones & Bartlett Learning, 2010,273
12. NIST-Guide to Intrusion Detection and Prevention Systems(IDPS). 2007http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
13. RIPE NCC. The Routing Information Service. http://www.ripe.net/ris.
14. Patroklos G. Argyroudis and Donal O' Mahony, "Secure Routing for Mobile Ad-hoc Networks", IEEE Communications Survey & Tutorials Third Quarter 2005.
15. Artur Ziviani, "An Overview of Internet Measurements: Fundamentals, Techniques and Trends", African Journal of Information and Communication Technology, Vol. 2, No. 1, March 2006.
16. Bagad, V. S. & Dhotre, I. A. "Computer Communication Networks". (1st Ed). Pune, India: Technical Publications, 2003.
17. Murray, David and Terry Koziniec(2012). The State of Enterprise Network Traffic in 2012. In: 18th Asia-Pacific Conference on Communications(APCC 2012).

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR