An Intelligent Approach of Sniffer Detection

Abdul Nasir Khan, Kalim Qureshi, and Sumair Khan
Department of Computer Science, COMSATS Abbottabad, Pakistan

Abstract: *ARP cache poisoning and putting host Network Interface Card (NIC) in promiscuous mode are ways of sniffer attacks. ARP cache poisoning attack is effective in an environment which is not broadcast in nature (like switch LAN environment) and other attack is effective in an environment which is broadcast in nature (like hub, bus, access point LAN environments). Sniffing is malicious activity performed by network user and because of this network security is at risk so detection of sniffer is essential task to maintain network security. Sniffer detection techniques can be divided into two main categories. First category's techniques are used to detect a sniffer host that runs it's NIC into promiscuous mode and second category's techniques are used to detect a sniffer host that uses ARP cache poisoning for sniffing. The network configuration is hidden form users. Network users do not have any information about nature of network. Therefore, users of network may invoke such sniffer detection technique that is not effective in that environment. This may result in sharing of his private and confidential information with malicious users. In this paper, we designed an intelligent invocation module that checks the nature of environment automatically and invokes appropriate, sniffer detection technique for that environment. With the help of this invocation module it is possible to detect passive as well as active sniffer hosts in both environments.*

Keywords: *Network security, sniffer, ARP cache poisoning, IP packet routing.*

Received January 7, 2009; accepted March 9, 2009

1. Introduction

We can categories network attacks into denial of services, unauthorized accesses from remote machine, unauthorized access from local super user (root) privileges and sniffing [3]. Sniffers [2, 8] are programs that allow a host to capture any network packet illicitly. Detection of sniffer attacks is very difficult task to handle [5]. Specially, if the sniffers are active because active sniffer can alter or block network traffic while passive sniffer can only monitor network traffic. There are two ways to sniff network traffic:

- A host running a sniffer sets its NIC in promiscuous mode [5, 18]. If any host's NIC is running in promiscuous mode, it will receive all packets either those packets targeted to it or not [15]. This way of sniffing is effective in an environment which is broadcast in nature like hub, access point and bus Local Area Network (LAN) environments [4, 17].
- ARP cache poisoning is also used for sniffing [6, 12]. This way of sniffing is effective in an environment, which is not broadcast in nature. ARP cache poisoning depends on local ARP cache maintained by each host of network. This cache contains IP with corresponding Media Access Control (MAC) addresses of recently accessed hosts.

Figure 1 explains ARP cache poisoning process. In this diagram, 'C' host performs ARP cache poisoning attack. 'C' host sends an ARP [10] poison packet to target host 'A' which contains host 'C' MAC address in source MAC address field and host 'B' IP address in source IP address field of ARP poison packet. When target host 'A' receives this packet, it poisons local ARP cache value either by adding false entry or updating old entry with new one. Same process is repeated with host 'B'. This process corrupts the local ARP caches of host 'A' and 'B' which are shown in Figure 1. After the completion of poisoning process, both hosts can not communicate directly with each other. Each host sends a packet to sniffer host and sniffer host reroutes packet back to actual destination. Sniffer host must have IP packet routing enabled so that it could send packet back to actual destination after stealing confidential information.

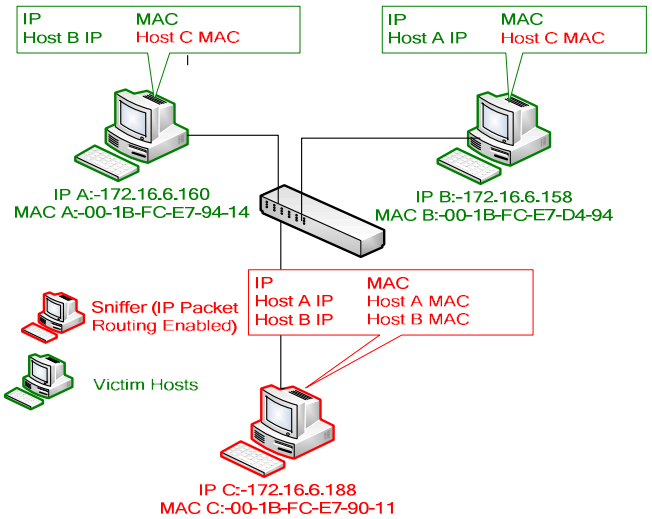

Figure 1. ARP cache poisoning process.

It is the requirement of network user to have a secure environment. Host that runs a sniffer can easily embezzle private and confidential information of network users. Hence detection of a sniffer is an essential task to maintain network security.

Different techniques are used to detect a sniffer host, which include Domain Name Server (DNS) [1], Address Resolution Protocol (ARP) [14], Round Trip Time (RTT) [14], ARP cache poisoning [16], ARP watch [12], switched network sniffer detection based on Internet Protocol (IP) packet routing [12], Man in the Middle (MiM) intrusion detection [13] and enhanced switched network sniffer detection based on IP packet routing detection techniques [9].

This paper divides sniffer detection techniques into two categories on the basis of environment in which those techniques are effective and also discusses and highlights strengths and weaknesses of sniffer detection techniques. Our objective is to select two stronger techniques, one is from category one and other is from category two and provide a system which automatically checks the nature of environment and invokes appropriate sniffer detection technique for that environment. There is a need of intelligent invocation module because user of network may invoke such sniffer detection technique which is not effective in that environment. This may result in sharing of his private information with malicious users. With help of intelligent invocation module it is possible to detect active as well as passive sniffer hosts in both environments.

The rest of the paper is organized as follows. Section 2 provides an overview of the related work done in this area. Section 3 explains the proposed work. Section 4 discusses the experimental results. Finally, conclusions are made along with future research.

2. Related Work

All sniffer detection techniques can be divided into two categories.

2.1. Promiscuous Mode Detection Category

This category includes DNS, ARP, RTT, ARP cache poisoning detection techniques. All enlisted techniques are used to detect a host running its NIC in promiscuous mode.

2.1.1. ARP, RTT and DNS Detection Techniques

In ARP detection technique, decision about sniffer is made on the basis of ARP reply packet when ARP request packet with fake destination hardware is sent to each host of the network [14].

RTT detection technique uses the measurement of the Round-Trip Time (RTT) of ICMP packets sent to suspicious hosts. Then, using a statistical model (the z-statistics) a probabilistic decision is made [14].

In DNS technique, sniffer detector host generate numerous fake TCP connections on a network segment, expecting that a sniffer pick up on those connections and resolve the IP addresses of the nonexistent hosts. When sniffer host receives this TCP packet with fake IP it performs reverse DNS lookup for the packet it captures. If sniffer detector receives the reverse DNS request and this request is for the resolution of address that does not exist on network then this response is from sniffer host [1].

2.1.2. ARP Cache Poisoning Detection Technique

Each host on network maintains a local ARP cache which contains IP addresses with corresponding MAC addresses of recently access hosts. When any host receive ARP request or response packet, it checks IP of received packet in local ARP cache. If there is no such IP address then it adds new entry of IP address with corresponding MAC in its local ARP cache. But if IP address found in local ARP cache with different MAC address then local ARP cache is updated with new entries. ARP cache poisoning detection technique is divided into three phases which are discussed below in detail:

- *Phase 1:* ARP cache poisoning is the local ARP cache of sniffing host is corrupted with fake entry that does not exist on the network. This is done by sending an ARP request packet to each host of network with fake source IP address and special purpose destination hardware FF:FF:FF:FF:FF:FE address [13]. If we use fake broadcast (FF.FF.FF.FF.FF.FE) address instead of broadcast address then all hosts whose NIC is in normal mode discard this packet. Only sniffer host receives this packet and corrupts its local ARP cache with fake entry.
- *Phase 2*: Establishing A TCP connection is sniffer detector establishes TCP connection with each host of network. This is done by sending TCP packet with SYN bit set to each host of network. Source IP address field of this packet in IP header is the same fake IP address which is used to corrupt the local ARP cache of sniffer host during phase 1.
- *Phase 3:* Detection of sniffer host is four types of possible response would be generated by the network hosts. These responses depend upon the type of hosts:
  - *Case 1:* The target host is not a sniffer is in this case target host send ARP request message in order to know the MAC address of fake IP address after receiving TCP packet with SYN bit set.
  - *Case 2:* The target host is running passive sniffer is in this case two type of packet would be

received. First, ARP reply packet sent by the host after receiving the ARP request packet in phase 1. Second, A TCP packet would be receive with SYN and ACK bit set indicate that connection can be establish or an ICMP error message would be receive which indicate that the connection can not be establish because the destination port is inaccessible.

- *Case 3:* The target host is running active sniffer is in this case there are two type of possible reply. A TCP packet which shows that the connection can be established (The SYN and ACK bit set). An ICMP error message which shows that connection cannot establish because the destination port is inaccessible [16].

2.2. MiM Attack Detection Category

This category includes ARP Watch, switched network sniffer detection based on IP packet routing, MiM intrusion and enhanced switched network sniffer detection based IP packet routing detection techniques. All above enlisted techniques are used to detect sniffer hosts that use ARP cache poisoning for sniffing.

2.2.1. ARP Watch, Switched Network Sniffer Detection Based on IP Packet Routing and MiM Intrusion Detection Techniques

ARP watch detection technique monitors network activities to maintain a database of IP with corresponding MAC addresses in order to find out a host which sends ARP poisoning packet to perform ARP cache poisoning attack or to find a host which have been the victim of ARP cache poisoning. Decision about sniffer host is made on the basis of received packet's IP and MAC addresses. If received packet's IP and MAC are not found in database, it means the packet is generated by sniffer host [12].

Switched sniffer detection based IP packet routing detection technique works in two phases. In first phase, an unusual ICMP packet is created which contains same source and destination IP addresses. This packet is sent to each host of the network by changing the destination MAC address only. Second phase is to detect a host that forward unusual ICMP echo request packet. IP packet routing enabled hosts forward this packet with same IP [7] and ICMP headers but different Ethernet header. Those host whose IP packet routing enable, most probably running a sniffer. There is no reason for a host to do IP routing in network because this activity is reserved for router [12]. Man in the middle intrusion detection technique works in three phases. First two phases are the same as in IP packet routing detection technique. Third phase is to find malicious hosts among suspicious host that have performed ARP cache poisoning attack [13].

2.2.2. Enhanced IP Packet Routing Detection Technique

This technique works in five phases. In the first phase, ARP request packets are created and send to each host of network in order to collect IP and MAC addresses of all network hosts. This information is utilized to detect a man in the middle attack, creation of ICMP packet and for remote ARP correction.

In the second phase, an unusual ICMP echo request packets are created using stocked MAC and IP addresses information and sent it to each host of the network. Destination IP address in unusual ICMP echo request packet should be an address that does not exist in network. The main reason to keep the different source and destination IP addresses is to detect a sniffer host that does not response any unusual ICMP echo request packet which has same source and destination IP addresses. If target host's IP packet routing is enabled then packet will be forwarded to source host with same IP and ICMP headers but different Ethernet header. If any host IP packet routing is enabled then that host is suspicious host. In general, there is no reason for a host to do IP packet routing in a network because this activity is usually reserved for the network's routers [12]. Figure 1 explains an ARP cache poisoning process. It is shown in Figure 1, any host that poison the local ARP cache of other hosts must contain IP and MAC addresses of suffered hosts in its local ARP cache.

In the third phase, local ARP cache entries of those hosts are collected whose IP packet routing is enabled. Psexec is a tool which is used for remote process execution [11]. Our objective is to get the local ARP caches entries of those hosts whose IP addresses are in local ARP cache of malicious host. By using the same tool local ARP caches entries of those hosts are also collected having IP addresses in malicious host's local ARP cache. These values are used in phase four to detect ARP cache poisoning attack.

Phase four compares the ARP cache entries of those hosts having IP address in local ARP cache of suspicious host with the value obtained form phase one. If mismatch occurs between values then it confirms that local ARP cache of that host is corrupted. After compilation of this phase, we have information of those hosts whose local ARP is corrupted, false entries in its local ARP and what should be the correct entries in its local ARP cache.

Phase five corrects the remote ARP cache of those hosts that became the victim of ARP cache poisoning attack. ARP request packets are created on the behalf of that hosts whose false entry is added in victim host's local ARP cache. ARP request packets fields are filled with correct entries taken from phase one and send these packets to victim hosts whose local ARP cache is corrupted. When victim hosts receives these packets, it updates its local ARP cache with new and correct

entries. This process corrects the local ARP cache of poisoned hosts.

3. Proposed Technique

There is need of intelligent invocation module which automatically checks the nature of network and invokes appropriate detection technique which is effective in that environment. If the network is broadcast in nature then it is required to invoke one of sniffer detection technique from category one but if network is not broadcast in nature then it is required to invoke one of sniffer detection technique from category two. Our objective is to select the best techniques; one from category one and second from category two for invocation module so that it could help network users to detect active as well as passive sniffer in both environments automatically without knowing the network configuration details.

Category one includes ARP, RTT, DNS and ARP cache poisoning detection techniques. The major limitation of ARP, RTT and DNS detection techniques is that it detects sniffer host on the basis of reply of ARP, ICMP and DNS packet respectively generated by sniffer host. Advance sniffer are active and can block any ARP request or reply, DNS and ICMP messages in order to stay undetectable. Any anti sniffer which depends upon the reply of these packets would fail to detect an active sniffer host. ARP cache poisoning technique does not depend upon such messages. So, advance sniffer can not stay undetectable while ARP cache poisoning detection technique is used.

Category two includes ARP watch, switched networked sniffer detection based on IP packet routing, MiM intrusion detection and enhanced switched network sniffer detection based on IP packet routing. ARP watch detection technique requires access privileges on monitoring port of switch to monitor network activities. Therefore it would be more efficient to detect a sniffer host on switch LAN environment without the use of access privileges on monitoring port of switch [12]. Switched networked sniffer based on IP packet routing does not require any access privileges on monitoring port of switch. This technique is more effective and efficient as compare to ARP watch detection technique. This technique provides information about those hosts whose IP packet routing is enabled but does not provide any information, either that suspicious hosts performed ARP cache poisoning attack against other hosts in the network. Man in the middle intrusion detection technique provides information among suspicious hosts that have performed ARP cache poisoning attack against other hosts in the network. In this technique, sniffer detector must corrupts the local ARP cache of suspicious hosts. For that purpose ARP request packets are created and send to malicious host on behalf of every network host. Experimental results shows that increase in number of normal or malicious hosts also increase in the number of injected packets [13]. If the network is flooded with heavy traffic, then its performance might be affected. Secondly, switched network sniffer based on IP packet routing and MiM intrusion detection techniques failed to detect a sniffer that does not response any unusual ICMP echo request packet which has same source and destination IP addresses. Enhanced switched network sniffer based on IP packet routing detection technique is effective to detect an active and as well as passive sniffer. This technique also provides information about malicious hosts, among suspicious hosts that have performed ARP cache poisoning attack without degrading network performance. We choose ARP cache poisoning detection technique from category one and enhanced switched network sniffer detection based on IP packet routing from category two for our proposed invocation module because both detection technique is effective to detect active and as well as passive sniffers.

3.1. An Intelligent Approach for Sniffer Detection

This intelligent approach utilizes enhanced switched network sniffer detection based on IP packet routing and ARP cache poisoning detection techniques for sniffer detection. Working of the proposed technique is shown in Figure 2.

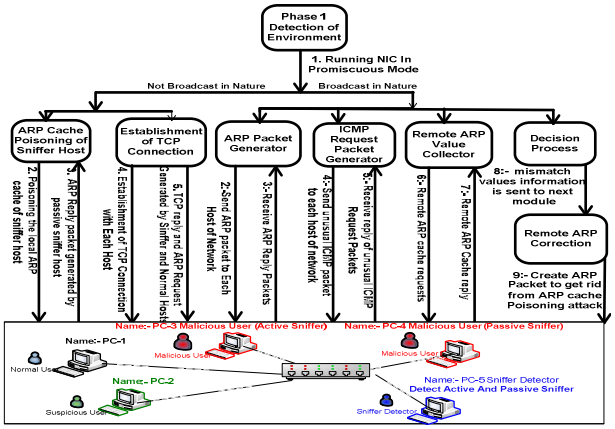

Figure 2. Sniffing host detection process diagram.

This detection technique works in the following phases:

- *Phase 1:* Detection of environment is the first phase of this detection technique is to find out the nature of environment in which sniffer detection process will be invoked. This can be done by running sniffer detector NIC in promiscuous mode for 30 to 60 second. Decision about environment is made on the basis of captured packets. Figure 3 explain setup which is used to detect nature of environment.

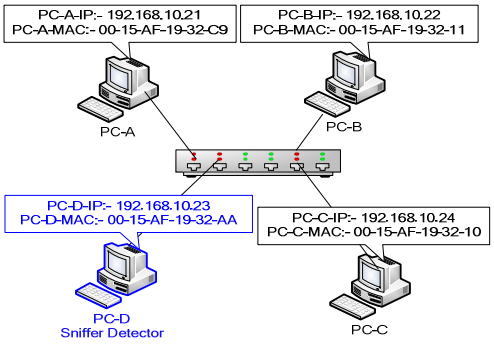

Figure 3. Detection of environment.

Here, host 'A', 'B' and 'C' are normal host and host 'D' is sniffer detector. If host 'D' runs its NIC in promiscuous mode to detect the nature of environment in which sniffer detection process is invoked. At that time if host 'A' ping host 'C' then following packet should be captured on host 'D' depend upon the environment in which pinging is in progress.

It is shown from Tables 1 and 2 if sniffer detector receives a packet in which source or destination IP address does not match with sniffer detector IP address and destination MAC address is the MAC address of some network host then network is broadcast in nature. If sniffer detector does not receive such kind of packets with in defined time then network is not broadcast in nature.

Table 1. Captured packet on host 'D' when environment is broadcast.

Packet Type	Source IP	Source MAC	Destination IP	Destination MAC
ICMP Request	192.168.10.21	00-15-AF-19-32-C9	192.168.10.24	00-15-AF-19-32-10
ICMP Request	192.168.10.21	00-15-AF-19-32-C9	192.168.10.24	00-15-AF-19-32-10
ICMP Request	192.168.10.21	00-15-AF-19-32-C9	192.168.10.24	00-15-AF-19-32-10
ICMP Request	192.168.10.21	00-15-AF-19-32-C9	192.168.10.24	00-15-AF-19-32-10
ICMP Reply	192.168.10.24	00-15-AF-19-32-10	192.168.10.21	00-15-AF-19-32-C9
ICMP Reply	192.168.10.24	00-15-AF-19-32-10	192.168.10.21	00-15-AF-19-32-C9
ICMP Reply	192.168.10.24	00-15-AF-19-32-10	192.168.10.21	00-15-AF-19-32-C9
ICMP Reply	192.168.10.24	00-15-AF-19-32-10	192.168.10.21	00-15-AF-19-32-C9

Table 2. Captured packet on host 'D' when environment is not broadcast.

Packet Type	Source IP	Source MAC	Destination IP	Destination MAC
ICMP Request	192.168.10.21	00-15-AF-19-32-C9	192.168.10.24	FF-FF-FF-FF-FF-FF
ICMP Request	192.168.10.21	00-15-AF-19-32-C9	192.168.10.24	FF-FF-FF-FF-FF-FF
ICMP Request	192.168.10.21	00-15-AF-19-32-C9	192.168.10.24	FF-FF-FF-FF-FF-FF
ICMP Request	192.168.10.21	00-15-AF-19-32-C9	192.168.10.24	FF-FF-FF-FF-FF-FF

- *Phase 2:* Invoke appropriate detection technique is if network is broadcast in nature then ARP cache poisoning detection technique is invoked to detect a sniffer host. If network is not broadcast in nature then enhanced switched network sniffer detection based on IP packet routing is invoked to detect a sniffer host.

4. Experimental Results

ARP, RTT and DNS detection techniques are used to detect a sniffer host which runs its NIC in promiscuous mode for sniffing. These detection techniques are effective to detect a sniffer host that does not block or alter any network activity. If sniffer host can block network traffic and does not generate response of any ARP, ICMP and DNS request packets then these detection techniques are failed to detect a sniffer. ARP cache poisoning detection technique is also used to detect a sniffer host which runs its NIC in promiscuous mode for sniffing. This detection technique is effective to detect active and as well as passive sniffers. ARP, RTT, DNS and ARP cache poisoning detection techniques are failed to detect sniffer in an environment which is not broadcast in nature because all those detection techniques try to find out host which runs it's NIC in promiscuous mode for sniffing but here, ARP cache poisoning is used for sniffing.

ARP watch, switched network sniffer detection based on IP packet routing, MiM intrusion detection and enhanced switched network sniffer detection based on packet routing are used to detect a sniffer host that performed ARP cache poisoning attack for sniffing. ARP watch detection technique requires access privileges on monitoring port of switch to monitor network activities. This technique is able to detect active and as well as passive sniffer in an environment which is not broadcast in nature. This detection technique is failed to detect any sort of sniffer in an environment which is broadcast in nature. Switched network sniffer detection based on IP packet routing and MiM intrusion detection techniques do not require any access privileges on monitoring port of switch. These techniques can detect passive sniffers but failed to detect active sniffer that does not response any unusual ICMP echo request packet which have same source and destination IP addresses. In Enhanced switched network sniffer based on IP packet routing, destination IP address in unusual ICMP echo request packet should be an address that does not exist in network. Because of this enhanced switched sniffer detection technique is able to detect passive sniffers as well as active sniffers that do not response any unusual ICMP packet which has same source and destination IP addresses. ARP watch, Switched network sinffer detection based on IP packet routing, MiM intrusion detection and enhanced switched network sniffer detection based on IP packet routing are failed to

detect sniffer in an environment which is broadcast in nature because all these detection techniques try to find out the host which performed ARP cache poisoning attack but here, sniffer host run its NIC in promiscuous mode for sniffing.

Invocation module checks the nature of environment automatically and invokes appropriate sniffer detection technique for that environment. If environment is broadcast then ARP cache poisoning detection technique is invoked. If environment is not broadcast then enhanced switched networked sniffer detection based on IP packet routing technique is invoked to detect a sniffer. Both detection techniques are effective to detect active as well as passive sniffer. With the help of this invocation module it is possible to detect passive as well as active sniffer hosts in both environments automatically. Sniffer detection performance of all detection techniques are shown in Table 3.

Table 3. Detection performance of sniffer detection techniques.

Detection Technique	Active Sniffer/ Broadcast Environment	Passive Sniffer/ Broadcast Environment	Active Sniffer/ Not Broadcast Environment	Passive Sniffer/Not Broadcast Environment
ARP Detection Technique	Failed	Detected	Failed	Failed
RTT Detection Technique	Failed	Detected	Failed	Failed
DNS Detection Technique	Failed	Detected	Failed	Failed
ARP Cache Poisoning Detection Technique	Detected	Detected	Failed	Failed
ARP Watch Detection Technique	Failed	Failed	Detected	Detected
Switched Network Sniffer Detection Based On IP Packet Routing	Failed	Failed	Failed	Detected
Mim Intrusion Detection Technique	Failed	Failed	Detected	Detected
Enhanced Switched Network Sniffer Detection Based On IP Packet Routing	Failed	Failed	Detected	Detected
A Hybrid Approach	Detected	Detected	Detected	Detected

5. Conclusions and Future Work

The network configuration is hidden form normal users. Network users do not have any information about nature of network. So, users of the network may invoke sniffer detection technique which is not effective in that environment. This sniffer detection technique provides wrong information to user which may be dangerous for him.

Our proposed invocation module checks the nature of environment automatically and then invokes appropriate sniffer detection technique for that environment. If environment is broadcast then ARP cache poisoning detection technique is invoked. If environment is not broadcast then enhanced Switched network sniffer detection based on IP packet routing detection technique is invoked to detect a sniffer. Both detection techniques are effective to detect active as well as passive sniffer. With the help of this invocation module it is possible to detect passive as well as active sniffer hosts in both environments automatically.

Currently, we are working on detection of an active switch sniffer that does not response any type of ICMP echo request packet.

References

[1] AbdelallahElhadj H., Khelalfa H., and Kortebi H., "An Experimental Sniffer Detector: SnifferWall," *Technical Document*, Securie des Communications sur Internet, 2002.

[2] Baxley T., Xu J., Yu H., Zhang H., Yuan X., and Brickhouse J., "LAN Attacker: A Visual Education Tool," *in Proceedings of Conference Information Security Curriculum Development*, USA, pp. 118-123, 2006.

[3] Chimphlee W., Abdullah A., Sap M., Chimphlee S., and Srinoy S., "A Rough-Fuzzy Hybrid Algorithm for Computer Intrusion Detection," *International Arab Journal of Information Technology*, vol. 4, no. 1, pp. 247-254, 2007.

[4] Clincy V. and Krithi A., "Evaluation and Illustration of a Free Software Tool for Wireless Network Monitoring and Security," *The Journal of Computing Sciences in Colleges*, vol. 21, no. 3, pp. 19-29, 2006.

[5] Fuentes F. and Kar D., "Ethereal vs. Tcpdump: A Comparitive Study on Packet Sniffing Tools for Educational Purpose," *Computer Journal of Computing Sciences in Colleges*, vol. 20, no. 4, pp. 169-176, 2005.

[6] Gibson Research Corporation, "ARP Cache Poisoning in Switch LAN Environment," available at: http://www.grc.com/ nat/arp.htm, last visited 2008.

[7] Hornig C., "A Standard for the Transmission of IP Datagrams over Ethernet Networks," *Symbolics Cambridge Research Center*, 1984.

[8] Held G., "Focus on Sniffer Portable," *International Computer Journal of Network Management*, vol. 13, no. 5, pp. 389-396, 2003.

[9] Khan A., Qureshi K., and Khan S., "Enhanced Switched Network Sniffer Detection Technique Based on IP Packet Routing," *Computer Journal of System Security*, vol. 18, no. 4, pp. 153-162, 2009.

[10] Plummer D., "An Ethernet Address Resolution Protocol-Converting Network Protocol to 48 bit

Ethernet Address for Transmission on Ethernet Hardware," *RFC Editor* , US, 1982.

[11] Russinovich M., "PsExec Tool," 2007, available at: http://technet.microsoft.com/en-us/sysinternals /bb896649.aspx, last visited 2008.

[12] Trabelsi Z., "Switched Network Sniffers Detection Technique Based on IP Packet Routing," *Computer Journal of System Security Journal*, vol. 14, no. 4, pp. 51-60, 2005.

[13] Trabelsi Z. and Shuaib K., "Man in the Middle Intrusion Detection," *in Proceedingss of IEEE Transition GLOBE COM*, San Francisco, pp. 1-6, 2006.

[14] Trabelsi Z., Rahmani H., Kaouech K., and Frikha M., "Malicious Sniffing Systems Detection Platform," *in Proceedingss of IEEE/IPSJ International Symposium on Applications and the Internet*, Tunisia, pp. 201-207, 2004.

[15] Trabelsi Z. and Rahmani H., "Detection of Sniffers in an Ethernet Network," *in Proceedingss of 7th Information Security Conference*, Berlin, pp. 170-182, 2004.

[16] Trabelsi Z. and Rahmani H., "An Anti-Sniffer Based on ARP Cache Poisoning Attack," *Information System Security Journal*, vol. 13, no. 6, pp. 23-36, 2005.

[17] Yeo J., Youssef M., and Agrawala A., "A Framework for Wireless LAN Monitoring and Its Applications," *in Proceedingss of 3rd ACM Workshop on Wireless Security*, USA, pp. 70-79, 2004.

[18] Yuan X., Vega P., Xu J., Yu H., and Li Y., "Using Packet Sniffer in Class Experience and Evaluation," *in Proceedingss of the 45th Annual Southeast Regional Conference ACMSE*, USA, pp. 116-121, 2007.

Abdul Nasir Khan received the MCS and MS (CS) degrees from the COMSATS Institute of Information Technology, Abbottabad, in 2005 and 2008, respectively. Currently, he is a lecturer in the Department of Computer Science, COMSATS Institute of Information Technology. His research interests are in various aspects of network security and their applications.

Kalim Qureshi is a professor in Computer Science Department, COMSATS Institute of Information Technology, Abbattabad, Pakistan. He is an approved supervisor for the M.S. and Ph.D. thesis by the High Education Commission, Islamabad, Pakistan. His research interests include network parallel distributed computing, thread programming, concurrent algorithms designing, task scheduling, and performance measurement. He is a member of IEE Japan and IEEE Computer Society.

Sumair Khan received the MCS and MS (CS) degrees from the OMSATS Institute of Information Technology, Abbottabad, in 2004 and 2007, respectively. Currently, he is a lecturer in the Department of Computer Science, COMSATS Institute of Information Technology. His research interests are in various aspects of network security and their applications.