

Towards More Secure Biometric Readers for Effective Digital Forensic Investigation

Zouheir Trabelsi¹, Mohamed Al-Hemairy², Ibrahim Baggili³, and Saad Amin⁴

¹ Faculty of Information Technology

² Research Affairs Sector,

UAE University, Al Ain, P.O. Box 17551, UAE

{trabelsi,m.hussien}@uaeu.ac.ae

³ College of Information Technology, Advanced Cyber Forensics Research Laboratory

Zayed University, Abu Dhabi, UAE

Ibrahim.Baggili@zu.ac.ae

⁴ College of Informatics, British University in Dubai,

Dubai, P.O. Box 502216, UAE

Saad.Amin@BUiD.ac.ae

Abstract. This paper investigates the effect of common network attacks on the performance, and security of several biometric readers. Experiments are conducted using Denial of Service attacks (DoSs) and the ARP cache poisoning attack. The experiments show that the tested biometric readers are vulnerable to DoS attacks, and their recognition performance is significantly affected after launching the attacks. However, the experiments show that the tested biometric readers are secure from the ARP cache poisoning attack. This work demonstrates that biometric readers are easy targets for malicious network users, lack basic security mechanisms, and are vulnerable to common attacks. The confidentiality, and integrity of the log files in the biometric readers, could be compromised with such attacks. It then becomes important to study these attacks in order to find flags that could aid in a network forensic investigation of a biometric device.

Keywords: Fingerprint reader, Iris reader, Biometrics scanners, Denial of Service attack (DoS), forensic investigation, Firewall, Intrusion Detection/Prevention Systems (IDS/IPS).

1 Introduction

Digital forensic investigations focus on finding digital evidence after a computer or network security incident has occurred, or locating data from systems that may form part of some litigation, even if it is deleted. The goal of digital forensics is to perform a structured investigation to find out what happened on the digital system, and who was responsible for it.

Nowadays, many networks include biometric readers, such as fingerprint, face and iris readers, used for user identification and verification, in addition to the common network devices (computers, servers, switches, routers and firewalls). These readers

exchange biometric data with remote servers via networks. In case of incidents, the readers' logs and the biometric data may be used by digital forensic investigators to acquire digital evidence. However, insecure and vulnerable biometric readers may not contribute in finding exactly what happened on the digital systems. Therefore, prior to any digital investigation, it is important that digital forensic investigators have sufficient knowledge about the security level of the biometric readers, and the data involved in the investigation.

This paper focuses on investigating the security of some biometric readers, and the corresponding exchanged biometric data. Precisely, we investigate the effect of common network attacks on the performance and security of the biometric readers. Experiments are conducted using DoS attacks and ARP cache poisoning attack, and they are part of a master thesis submitted to the British University in Dubai (BUiD), School of Informatics, in partial fulfillment of the requirements for the degree of M.Sc. in Information and Networking Security.

2 Biometric Technologies

In 2001 MIT Technology Review [7] named biometrics as one of the "top ten emerging technologies that will change the world". The term "Biometric" comes from the Greek words "bio" (life) and "metric" (to measure). Biometric refers to technologies used for measuring and analyzing a person's unique characteristics. There are two types of biometrics: behavioral and physical. Behavioral biometrics are generally used for verification while physical biometrics can be used for either identification or verification.

Identification is determining who a person is. It involves trying to find a match for a person's biometric data in a database containing records of biometric information about people. This method requires time and a large amount of processing power, especially if the database is large. Verification is determining if a person is who he/she say he/she really is. It involves comparing a user's biometric data to the previously recorded data for that person to ensure that this is the same person. This method requires less processing power and time, and is usually used for authentication and access control.

The most common types of biometric technologies are fingerprint, iris, voice, hand geometry, and face recognition [1, 2, 3, 9]. Each technology has its own benefits and challenges. Today, fingerprint and iris technologies are widely used [10] because they are fast, reliable, stable, cost effective, and provide excellent identification accuracy rates. Iris recognition is the most precise of all biometric identification systems. The false acceptance ratio is so low that the probability of falsely identifying one individual as another is virtually zero [8].

Biometric technologies may seem trendy, but their use is becoming increasingly common. Currently, biometric readers are deployed in many public sites and are used for user identification and verification. They play an important role in implementing security policies within the institutions. Most biometric readers are able to connect to local area networks (LAN), and communicate with remote biometric servers to exchange biometric data.

Biometric reader manufacturers have been focusing on offering easy to use, practical devices, with low cost, low enrollment and recognition time, and low rate of false match and non-match. However, since these devices are as any network host with IP and MAC addresses and may be targets of malicious network users.

3 Network Attacks

DoS attacks and the ARP cache poisoning attack [11] are the two classes of network attacks that are used in this research. Mainly, two experiments have been conducted. In the first experiment, we investigate the effect of DoS attacks on the performance of fingerprint, and iris readers. In the second experiment, we investigate the ability of ARP cache poisoning attack to corrupt the ARP cache entries of the biometrics readers. Network hosts with corrupted ARP caches may not be able to communicate properly with the other network hosts.

3.1 DoS Attacks

A DoS is an attack which attempts to render a system unusable or significantly slow down the system for legitimate users by overloading the resources so no one else can access it. A DoS attack may target users, preventing them from establishing outgoing connections on a network. A DoS attack may also target an entire organization, to either prevent outgoing traffic or to prevent incoming traffic to certain network services, such as an organization's web page.

DoS attacks are much easier to accomplish than remotely gaining administrative access to a target system. Because of this, DoS attacks have become common on the Internet. DoS attacks can either be deliberate or accidental. It is caused deliberately when an unauthorized user actively overloads a resource. It is caused accidentally when an authorized user unintentionally performs an action that causes resources to become unavailable.

Most DoS attacks rely on weaknesses in the TCP/IP protocols. The next subsections introduce the selected DoS attacks used in this paper's experiments, namely the SYN flood, Land, Teardrop and UDP flood attacks.

Land Attack: Land attack occurs when an attacker sends spoofed TCP SYN packets (connection initiation) with the target host's IP address, and an open port as both source and destination. The target host responds by sending the SYN-ACK packet to itself, creating an empty connection that lasts until the idle timeout value is reached. Flooding a system with such empty connections can overwhelm the system, causing a DoS (Figure 1).

SYN Flood Attack: A SYN flood occurs when a host becomes so overwhelmed by SYN packets initiating incomplete connection requests that it can no longer process legitimate connection requests.

When a client system attempts to establish a TCP connection to a system providing a service (the server), the client, and server exchange a sequence set of messages known as a three-way handshake.

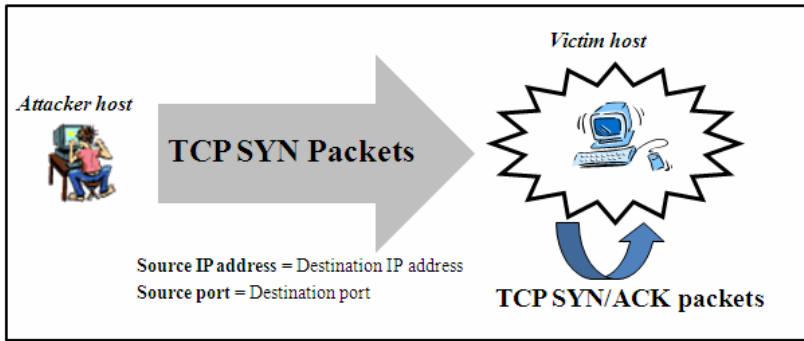


Fig. 1. The Land attack

The client system begins by sending a SYN (synchronization) message to the server. The server then acknowledges the SYN message by sending a SYN-ACK (acknowledgment) message to the client. The client then finishes establishing the connection by responding with an ACK message. The connection between the client and the server is then opened, and the service-specific data can be exchanged between the client and the server.

The potential for abuse arises at the point where the server system has sent an acknowledgment (SYN-ACK) back to the client, but it has not yet received the final ACK message. This is what is known as a half-opened connection. The server has in its system memory a built-in data structure describing all pending connections. This data structure is of finite size, and it can be made to overflow by intentionally creating too many partially-opened connections (Figure 2).

Creating a half-opened connection is easily accomplished with IP spoofing. The attacker's system sends SYN messages to the victim's server that appear to be legitimate, but in fact, the source address is spoofed to a system that is not currently connected to the network. This means that the final ACK message is never sent to the victim server. Because the source address is spoofed, there is no way to determine the identity of the true attacker when the packet arrives at the victim's system.

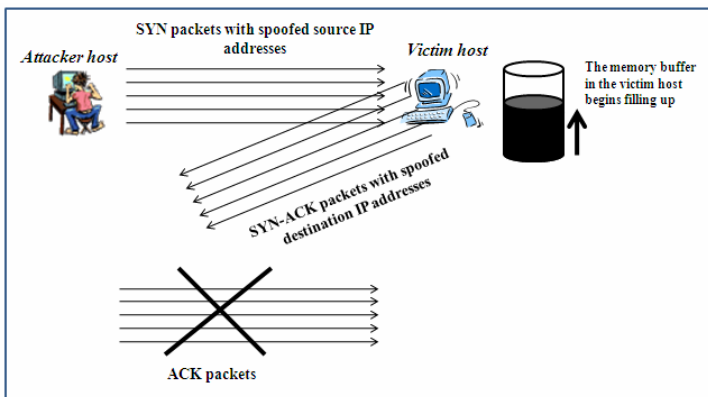


Fig. 2. The SYN Flood attack

Teardrop Attack: The Teardrop attack targets a vulnerability in the way fragmented IP packets are reassembled. Fragmentation is necessary when IP datagrams are larger than the maximum transmission unit (MTU) of a network segment across which the datagrams must traverse. In order to successfully reassemble packets at the receiving end, the IP header for each fragment includes an offset to identify the fragment's position in the original unfragmented packet. In a Teardrop attack, packet fragments are deliberately fabricated with overlapping offset fields causing the host to hang or crash when it tries to reassemble them. Figure 3 shows that the second fragment packet claims to begin 20 bytes earlier (at 800) than the first fragment ends (at 820). The offset of fragment Packet #2 is not in accord with the packet length of fragment Packet #1. This discrepancy can cause some systems to crash during the reassembly attempt.

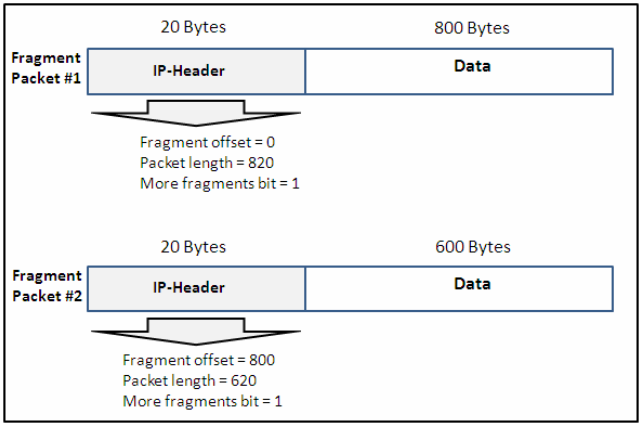


Fig. 3. The Teardrop attack

UDP Flood Attack: UDP (User Datagram Protocol) is a connectionless protocol, and it does not require any connection set up procedure to transfer data. A UDP Flood attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet, it will determine what application is waiting on the destination UDP port. Two cases are possible. If there is no application that is waiting on the port (closed UDP port), the victim host will generate an ICMP (Internet Control Message Protocol) packet of destination unreachable to the forged source address. However, if there is an application running on the destination UDP port, then the application will handle the UDP packet. In both cases, if enough UDP packets are delivered to destination UDP ports, the victim host or application may slow down or go down (Figure 4).

3.2 ARP Cache Poisoning Attack

Sniffing consists of re-routing (redirecting) the network traffic between two target hosts to a malicious host. Then, the malicious host will forward the received packets to the original destination; so that the communication between the two target hosts is

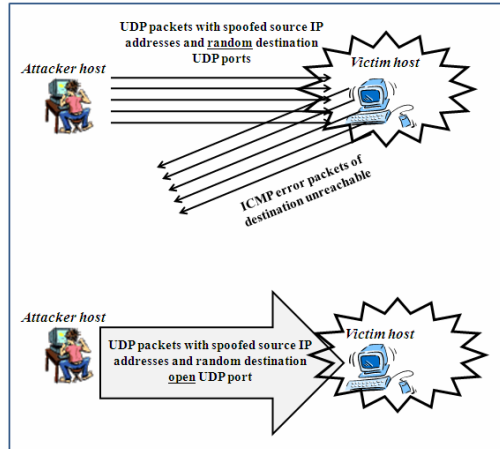


Fig. 4. UDP Flood attack

not interrupted and the two communicating hosts' will not notice that their traffic is being sniffed by a malicious one.

Man-in-the-Middle attack (MiM) is the most common attack used to sniff switched LAN networks. MiM attack uses ARP cache poisoning[11]. ARP cache poisoning is the malicious act, by a host in a LAN, of introducing a spurious IP address to MAC address mapping in another host's ARP cache. This can be achieved by manipulating the ARP cache of a target host, independently of the ARP messages sent by the target host. To do that, the malicious host can either add a new fake entry in the target host's ARP cache, or update an already existing entry using fake IP and MAC addresses.

In MiM attack, the malicious user first enables the host's IP packet routing, in order to become a router and forward the redirected packets. Then, using an ARP cache poisoning attack, the malicious user corrupts the ARP caches of the two target hosts in order to force the two hosts to forward all their packets. It is important to notice that if the malicious host corrupts the ARP caches of the two target hosts without enabling its IP packet routing, then the two hosts will not be able to exchange packets, and it will be a DoS attack. In this case, the malicious host does not forward the received packets to their legitimate destination as shown in Figure 5.

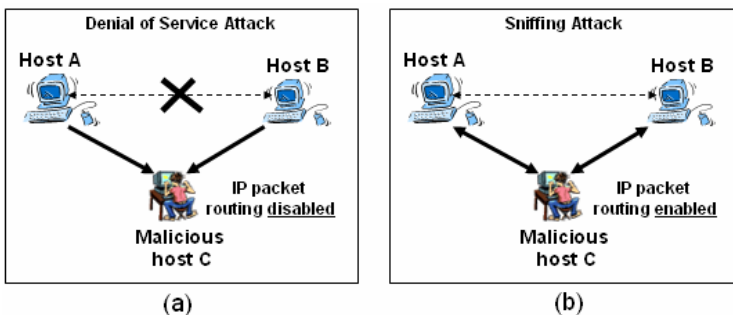


Fig. 5. Biometric data sniffing based on the MiM attack

4 Experiments

Two experiments are conducted. In the first experiment [14], we investigate the effect of four common DoS attacks on the performance of several fingerprint and iris readers. In the second experiment, we investigate the effect of ARP cache poisoning attack on the entries of the ARP caches of the biometric readers.

4.1 Network Architecture

Figure 6 shows the network architecture used in the experiments. Three attacker hosts, a biometric server, fingerprint readers, and iris readers are connected to a switch. The attacks are launched from the three attack hosts using two tools.

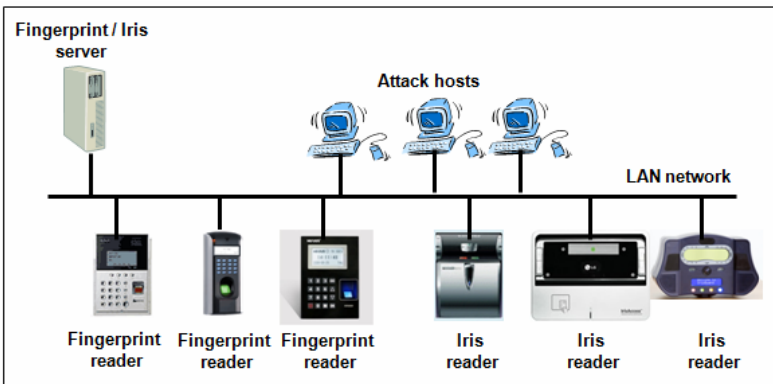


Fig. 6. Network architecture

4.2 Attack Tools

The following are the two tools used in the experiments [14]:

- FrameIP packet generator [12] is a packet generator that allows generating any type of IP and ARP packets. The tool is used by the attack hosts to generate the Land, Teardrop, and UDP flood attacks; it is also used to perform an ARP cache poisoning attack.
- SYNflood tool [13] is a ready-to-use attack tool used to generate the SYN flood attack.

Figure 7 show the online command used to generate the SYN flood attack, using the tool SYNflood. After executing the online command, a flood of fake TCP SYN packets is sent to the target biometric reader whose IP address is 10.10.10.5.

Using the three attack hosts, SYN flood, Land, Teardrop and UDP flood attacks are launched simultaneously. The following section presents the experimental results.

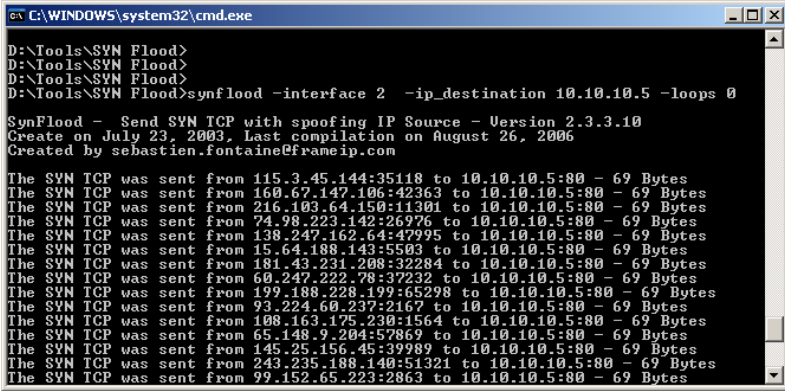


Fig. 7. The SYN flood attack online command

4.3 DoS Attacks Results for Fingerprint Readers

A few seconds after launching the 4 DoS attacks, the recognition performances of all tested fingerprint readers deteriorated significantly. For example, Figure 8 shows that before launching the DoS attacks, the response times were less than 0.4 ms when pinging the NitGen Fingerprint reader NAC 3000 [5]. However, the response times increased considerably and reached more than 20 ms just after launching the attacks [14]. This is due to the fact that after launching the DoS attacks, the reader became busy with treating the flood of packets, and consequently became unable to process the Ping requests on time. Additionally, the reader was unable to process several registered users when they were attempting to use it [14]. That is, the reader was unable to give any recognition results. Table 1 summarizes the experimental results for each fingerprint reader.

Table 1. DoS attacks results for fingerprint readers

	Effect of DoS attacks on the recognition performance of the fingerprint readers
NitGen Fingerprint reader NAC 3000 (http://www.nitgen.com)	Recognition status is unstable: <ul style="list-style-type: none"> The reader recognition response is very slow or there is no response. The readers often disconnect from the network.
F7 Standalone Biometric Access Control Terminal (http://www.fslocks.com/f7stbiaccote.html)	
MX600 Fingerprint Access Control (http://www.miaxis.net/1070012/1/products_details.htm)	

4.4 DoS Attacks Results for Iris Readers

In this experiment [14], the iris readers are the targets of the attack hosts. The same four DoS attacks are used in this experiment. A few seconds after launching the DoS attacks, the recognition performances of all tested iris readers deteriorated significantly. Table 2 summarizes the experiments results for each iris reader [14].

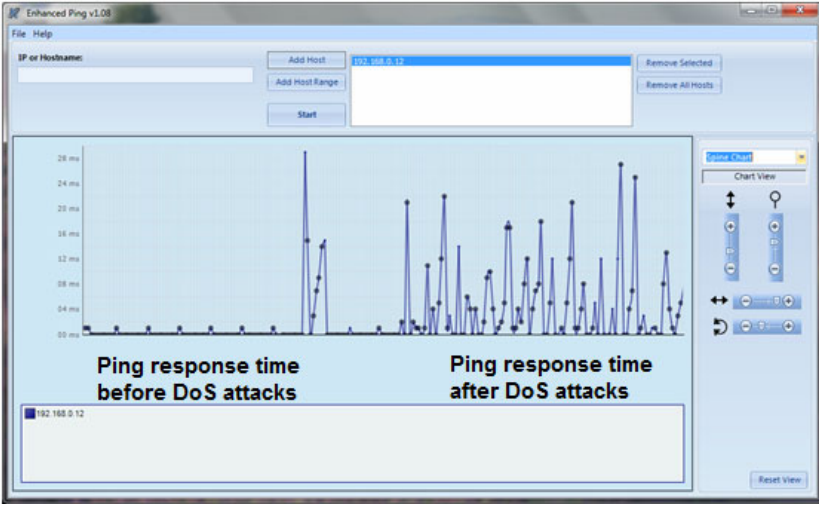


Fig. 8. Response time of Nitgen Fingerprint reader NAC 3000 before and after the DoS attacks

Table 2. DoS attacks results for iris readers

	Effect of DoS attacks on the recognition performance of the iris readers
Panasonic Iris reader BM-ET330 (ftp://ftp.panasonic.com/pub/Panasonic/cctv/SpecSheets/BM-ET330.pdf)	Recognition status is unstable: -The reader recognition response is very slow or there is no response.
LG's IrisAccess 4000 (http://www.irisid.com) IG-AD100@ Iris Camera System, (http://www.irisguard.com)	-The readers disconnected from the network. But, when the DoS attack stopped, the readers reconnected to the network.

For example, Figure 9 shows that before launching the DoS attacks, the response times were less than 0.1 ms when pinging the Panasonic Iris reader BM-ET330 [4]. However, just after launching the attacks, the reader crashed, and consequently there were no ping responses. The reader became unable to recognize users and completely disconnected from the network. When the DoS attack stopped, the reader reconnected to the network [14].

4.5 ARP Cache Poisoning Attack Results for Fingerprint and Iris Readers

This attack consists of corrupting the ARP caches of the biometric readers. Network hosts with corrupted ARP caches may not be able to communicate properly with other network hosts.

We use the FrameIP packet generator tool to build fake ARP packets [14]. The packets are used to corrupt the ARP caches of the fingerprint and iris readers. Figure 10 shows the online command used to generate the fake ARP packets.

The experimental results indicate that the ARP cache poisoning attack has no effect on the tested readers. Consequently, the readers are protected from this type of attack. This is because of the simple implementation of the ARP protocol in these readers. In fact, the readers do not allow the updating of their ARP caches [14]. They use static

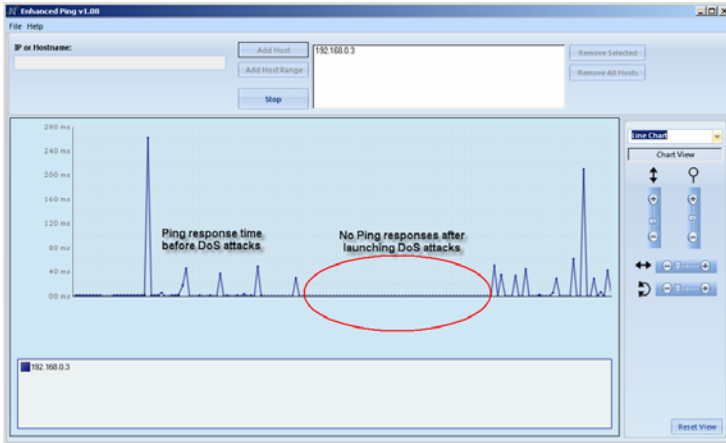


Fig. 9. Response time of Panasonic Iris reader BM-ET330 of before and after the DoS attacks

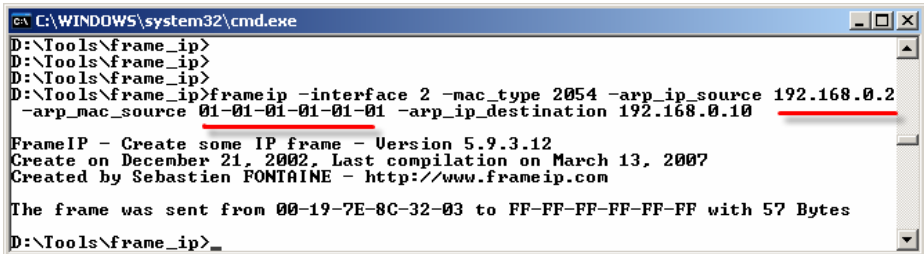


Fig. 10. FrameIP online command used to perform ARP cache poisoning attack

ARP cache entries, so that the entries cannot be updated by fake ARP request and replies. The ARP cache entries are created when the readers connect to the network. Once they get the MAC addresses of the biometric servers, they create static entries (IP/MAC addresses) in their ARP caches.

5 Enhanced Network Architecture for e-Forensic Investigation

In case of incident, forensic investigators need to collect, and analyze the data exchanged between the network devices (routers, firewalls, intrusions detection systems, etc.), including the biometric readers and the servers. This investigation allows to propose a more enhanced configuration for a network that includes biometric readers. The log files of the network devices and biometric readers should be collected to be used in any investigation. In addition, sniffers should be installed in order to collect the exchanged traffic between the devices. A host running a sniffer, and connected to a network will not be able to sniff the traffic, unless it is connect to a monitoring port (SPAN), Figure 11. A host connect to a SPAN port will receive all the network traffic exchanged between all the network devices. Hence, forensic investigators can use the

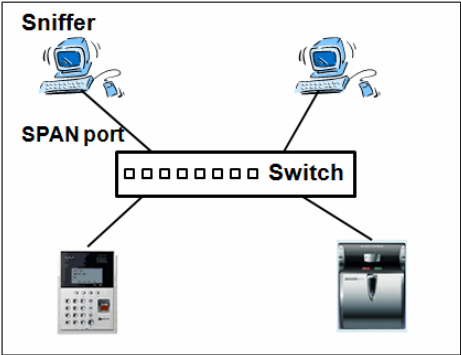


Fig. 11. A network architecture with SPAN port for sniffing network traffic

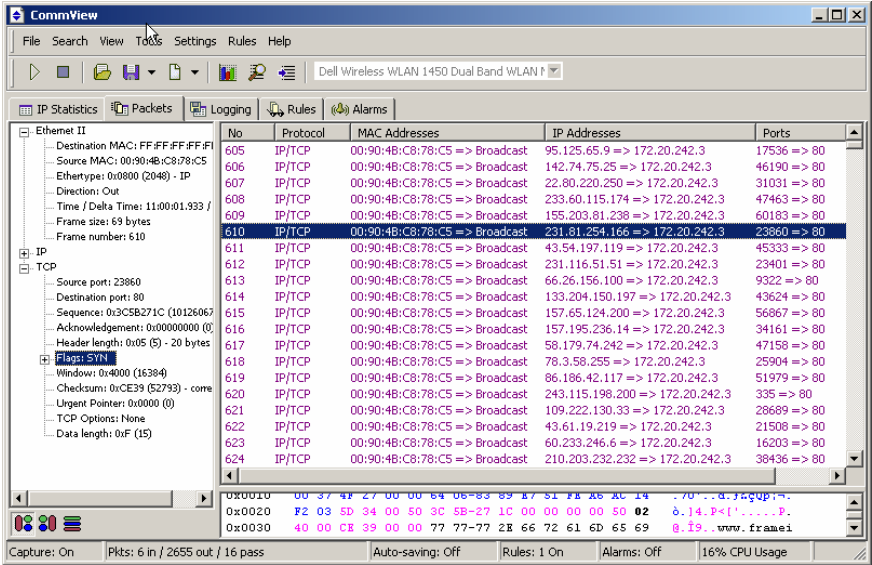


Fig. 12. CommView sniffer showing traffic generated by SYN flood attack

sniffed traffic to start their investigation in case of incidents. For example, Figure 12, shows the collected SYN flood attack traffic using the CommView sniffer. By investigating the collected traffic, it is clear that host 172.20.242.3 has been under SYN flood attack.

6 Conclusion

This paper investigated the effect of common network attacks on the performance and security of several fingerprint and iris readers. Experiments were conducted using DoS attacks and ARP cache poisoning attacks.

The experimental results demonstrate that the tested biometric readers are vulnerable to DoS attacks, and their recognition performances are significantly affected after launching the attacks. However, the tested biometric devices are protected from the ARP cache poisoning attack since they use a simple implementation of the ARP protocol. They use static ARP caches entries; instead of using dynamic entries as it is the case in ordinary computers.

Biometric devices are designed to offer practical user interfaces with effective costs, low enrollment and recognition time, and low false nonmatch and match rates. However, our work in this paper shows that they are not designed to include basic security mechanisms, mainly firewalls to filter the network traffic and IDS/IPS systems to detect and prevent network attacks, and malicious network activities. Therefore, they are targets for malicious users. These biometric readers can be crashed or disconnected from the network by common DoS attacks. Consequently, their availability and efficiency may become questionable within any institution, and it will be difficult to rely on such devices to implement security policies, and conduct digital forensic investigations in case of an incident. Furthermore, since these biometric readers lack basic security features, the confidentiality and integrity of their log files and the exchanged biometric data are questionable. Digital forensic investigators should be aware of the fact that current biometric readers are insecure and vulnerable devices and may exchange biometric data that can be easily attacked and altered.

As a future work, we are working on conducting further experiments using other types of attacks and biometric readers.

References

1. Vacca, J.: *Biometric Technologies and Verification Systems*. Butterworth-Heinemann Publisher, Butterworths (2007) ISBN-10: 0750679670
2. Wayman, J., Jain, A., Maltoni, D., Maio, D.: *Biometric Systems: Technology Design and Performance Evaluation*. Springer Publisher, Heidelberg (2004) ISBN-10: 1852335963
3. Chirillo, J., Blaul, S.: *Implementing Biometric Security*. Wiley Publisher, Chichester (2003) ISBN-10: 0764525026
4. Panasonic Iris reader BM-ET330, Specification Sheet, <ftp://ftp.panasonic.com/pub/Panasonic/cctv/SpecSheets/BM-ET330.pdf>
5. Nitgen Fingerprint reader NAC 3000, Specification Sheet, <http://www.nitgen.com>
6. Daugman, J.: Recognising Persons by Their Iris Patterns. In: Li, S.Z., Lai, J.-H., Tan, T., Feng, G.-C., Wang, Y. (eds.) *SINOBIOMETRICS 2004*. LNCS, vol. 3338, pp. 5–25. Springer, Heidelberg (2004)
7. The MIT Technology Review in the Emerging Technologies That Will Change the World, Ten emerging technologies that will change the world (January/February 2001), <http://www.techreview.com>
8. Daugman, J.: How Iris Recognition Works. *IEEE Transactions on Circuits and Systems for Video Technology* 14, 21–30 (2004)
9. Tony, M.: Biometric authentication in the real world, Centre for Mathematics and Scientific Computing, National Physical Laboratory, UK (Online) (2001), http://www.npl.co.uk/upload/pdf/biometrics_psrevho.pdf

10. Al-Raisi, A., Al-Khouri, A.: Iris Recognition and the Challenge of Homeland and Border Control Security in UAE. *Journal of Telematics and Informatics* 25, 117–132 (2008)
11. Trabelsi, Z., Shuaib, K.: A Novel Man-in-the-Middle Intrusion Detection Scheme for Switched LANs. *The International Journal of Computers and Applications* 3(3) (2008)
12. FrameIP Packet Generator, <http://www.FrameIP.com>
13. SYN flood, <http://www.FrameIP.com>
14. Al-Hemairy, M., Trabelsi, Z., Amin, S.: Sniffing Attacks Prevention/Detection Techniques in LAN networks & the effect on Biometric Technology. A thesis submitted to The British University in Dubai, School of Informatics (May 2010)