Towards More Secure Biometric Readers for Effective Digital Forensic Investigation

Zouheir Trabelsi[1], Mohamed Al-Hemairy[2], Ibrahim Baggili[3], and Saad Amin[4]

[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

I. Baggili (Ed.): ICDF2C 2010, LNICST 53, pp. 65–77, 2011.

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.