Chapter 14
A Systematic Empirical Analysis of Forging Fingerprints to Fool Biometric Systems

Christian Schwarzl
Vienna University of Technology and SBA Research, Austria

Edgar Weippl
Vienna University of Technology and SBA Research, Austria

ABSTRACT

This paper serves to systematically describe the attempts made to forge fingerprints to fool biometric systems and to review all relevant publications on forging fingerprints to fool sensors. The research finds that many of the related works fail in this aspect and that past successes could not be repeated. First, the basics of biometrics are explained in order to define the meaning of the term security in this special context. Next, the state of the art of biometric systems is presented, followed by to the topic of security of fingerprint scanners. For this, a series of more than 30,000 experiments were conducted to fool scanners. The authors were able to reproduce and keep records of each single step in the test and to show which methods lead to the desired results. Most studies on this topic exclude a number of steps in producing a fake finger and fooling a fingerprint scanner are not explained, which means that some of the studies cannot be replicated. In addition, the authors' own ideas and slight variations of existing experiment set-ups are presented.

INTRODUCTION

The study focuses on the issue of security of fingerprint scanners. Fingerprint scanners are used to improve identification and authentication of users to the operating system; moreover, they are used to confirm critical transactions in software systems. For the overall security of a software system it is essential for its engineers to understand the strengths and limitations of fingerprints when used for authentication. While many successful attacks have been described most papers

DOI: 10.4018/978-1-4666-2482-5.ch014

are not so precise as to allow other researchers to replicate the same experiment. This paper summarizes previous attacks and documents all steps in a detailed way. Software engineers will benefit from this study as they can use our paper as a scaffold for similar research.

There are a number of studies that have reported that fingerprint scanners can be outwitted with extremely basic technologies (Chaos Computer Club, 2004; Kaseva & Stén, 2003; Matsumoto et al., 2002). Although the approach and materials used in these studies may differ, all share certain common features: procedures are described only superficially, whereby in a few cases one gets the impression that such imprecision is entirely intentional: Some steps are mentioned in merely a brief statement, with no precise description of the procedure or of the materials and instruments used. *Our contribution is, thus, to establish a reproducible, quantifiable approach to assessing the security of fingerprint scanners* – a security-critical component in many systems. The lack of detailed descriptions in many of the reviewed papers make some steps seem much simpler and easier than they actually are. The impression thus arises that it is extremely simple to deceive a fingerprint scanner.

The study examines whether a person of average practical and technical abilities using the appropriate tools can successfully recreate "false fingers" to fool fingerprint scanners. We also examined whether a slight adaptation of the methods used in the relevant articles may be successful. Moreover, we explain why a possible success depends on the scanner used or the device's scanning method. All of these experiments are carried out under scientific conditions, and the methods are tested to determine whether success can be counted on every time, only occasionally. With the help of all of these experiments, an attempt is made to answer the question of the security of fingerprint scanners.

QUALITY MEASURES

To enable a certain comparison between various products, particular guidelines and measurement parameters are required. For biometric systems, as a rule, performance is measured by the following error rates:

One of the most important measurements in a biometric system is the *False Accept Rate (FAR)*. This states the frequency with which non-authorized people are accepted as authorized and hence given access to the system (Bromba, 2008a).

Similar in importance to the *False Accept Rate is the False Rejection Rate (FRR)*. It is, in fact, the exact opposite of the FAR and states the frequency with which an authorized person is not granted entrance/access. Although it is often perceived as annoying when a biometric characteristic is not immediately accepted, this does not compromise the confidentiality of a system, but rather impacts availability

The *False Identification Rate (FIR)* states the frequency with which a biometric characteristic is, recognized, but assigned to the wrong person. This error can obviously occur only in systems that use a biometric characteristic as identifier and not for authentication. What must also be taken into account is that the FIR is associated with the number of stored biometric references. This measure is thereby only conditionally an indicator of a possible security risk. The *Failure to Enroll Rate* has relevance only during the enrollment