DIAMOND FORTRESS
TECHNOLOGIES

Liveness Detection and other Anti-Spoofing Measures in Optical Fingerprint Acquisition Systems such as ONYX

16 FEB 2017

As biometric measurement is becoming more acceptable to the public, circumvention is becoming more attractive to those who wish to undermine the integrity and reliability of said systems. Any biometric modality and/or system is vulnerable, and it is doubtful there will ever be a system totally immune to spoofing when given enough time.

Spoofing is a sensor-level attack (often referred to as a “presentation” attack) in which a valid biometric identifier such as a fingerprint is replaced by someone wishing to impersonate the authentic and valid user.

This paper includes information about spoofing techniques to which optical fingerprint capture systems may be susceptable.

DIAMOND FORTRESS TECHNOLOGIES
+01 855 785 8646 | www.diamondfortress.com
1500 1st Ave N.
Birmingham, Alabama 35203
U.S.A.

ALL INFORMATION INVOLVING LIVENESS DETECTION AND OTHER ANTISPOOFING MEASURES AND METHODS IS VERY SENSITIVE

Diamond Fortress Technologies does not release specifics of the LDAS *(Liveness Detection and Anti-Spoofing)* technology used in the **ONYX**™ system for obvious reasons: if the measures taken were publicly known, attackers would know exactly which factors they need to compromise the system. Therefore, rather than discussing the particulars of the current and planned LDAS implementations in ONYX, an overview of current LDAS technology will be presented.

DFT will neither verify nor deny which anti-spoofing methods are utilized in ONYX v.4.x *(current release)* or that will be included ONYX v.5.x *(the next major release, scheduled for Q2 2017)*. However, a breakdown of spoofing techniques and the measures developed to combat them will be presented. DFT does employ some methods that are less widely known, and we have also developed proprietary LDAS techniques - some of which are in use currently and others which are planned to be included with future versions of ONYX.

Not only do we consider current approaches, we are constantly testing against emerging and possible future spoofing mechanisms. Just as there has never been a lock immune to picking, there isn't a biometric solution that is immune to every method of exploitation. To combat this, we at DFT are proactively predicting the future actions of possible attackers. We aren't trying to stay one step ahead of the spoofers; we're staying many steps ahead. We maintain large databases of fingerprint images and templates that we test rigorously against. We also do predictive testing against other methods that may emerge. We have the input of five engineers from our "anti-spoof group," and we sometimes consult with engineers from the biomedical, optical, electrical, computer science and computer vision fields. We have developed an enormous amount of resources in this area, and all are utilized to make our software as immune as it can be to presentation attempts.

SPOOFING COUNTERMEASURES IN OPTICAL FINGERPRINT AQUISITION

In ONYX and all other biometric systems, the goal of liveness detection is to determine if the biometric being captured is an actual measurement from the authorized, live person who is present at the time of capture. Liveness detection reduces the risk of spoofing by requiring a liveness signature in addition to matched biometric information. No system is perfect in its ability to prevent spoofing attacks. However, liveness algorithms can reduce this vulnerability and minimize the risk of spoofing. Below are some of the tactics that may be used to detect an improper presentation:

1. **Detection of parallax movement -** Parallax movement is a very simple anti-spoofing measure. It doesn't perform any type of liveness detection per se. It does detect a common and unsophisticated technique utilized by amateurs - the presentation of a flat image *(such as a photograph)*. Parallax detection is simply ensuring the movement of the finger is independent of the movement of the background. If all elements move synchronously, they are quickly identified as a false presentation

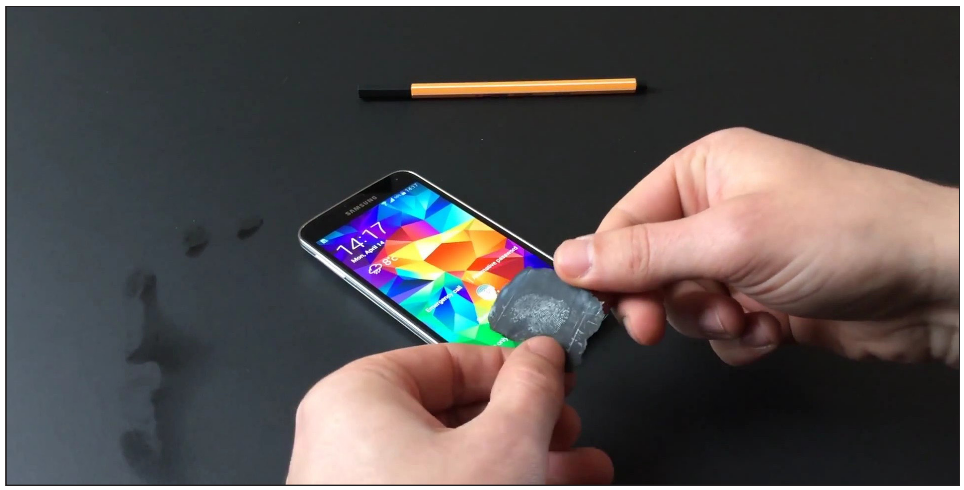
2. **Detection of movement by the finger itself -** If a finger is required to be curled before it is extended for presentation, the curl of the finger can be detected. Technology can also be used to detect the smooth extension of the finger. To combat this, a bad player would need to fabricate a robotic duplicate of the finger, which would have trouble moving in the same manner as an actual, live finger.

3. **Papillary Movement -** Papillary movement is the analysis of movements of papillary *(ridge)* lines of the fingertip. When light from the device's torch illuminates the finger, the light is reflected in a characteristic speckle pattern. Although this method is not suitable for resolving the papillary lines themselves, it can measure the small dynamic fluctuations of the papillary lines due to the heartbeat and very slight muscle movements.

4. **Pore Analysis -** Pores are very useful in detecting spoofs because the scale is very difficult to reproduce in a false sample, and pores are very often omitted by the potential attacker. Pores are considered fingerprint features, and the location of pores can indeed be useful not only in LDAS efforts but also used as a secondary or tertiary method in the matching process. Recording the number of pores and the Euclidian distance between them does serve as a form of liveness detection, as it is difficult for an attacker to reproduce the pore pattern in a fake finger. Another way pores are useful in liveness detection is via the “perspiration phenomenon.” Pores excrete sweat, and by considering the gray-level distribution in pixels surrounding the individual pores, perspiration activity can be assessed.

5. **Sub-Surface Scattering Analysis -** The interaction of light with skin tissue *(or any type of matter)* can be described in the terms of absorption, scattering, and fluorescence. The light from the torch *(the LED “flash”)* on a mobile device hits the skin and it is then partially scattered on the surface and partially enters the tissue in where it will be absorbed, scattered, or reemitted. When illuminating the finger from the side, a fraction of scattered and reemitted light waves leave the finger in different directions. Such scattered light includes information about dynamic physiological processes like blood flow, hemoglobin saturation, and pulse from inside the finger. One can detect whether the acquired object exhibits characteristics of the pulse and blood flow consistent with a live human being. It is fairly easy to determine whether the object presented indicates some kind of pulse and blood flow.

Currently ONYX contains a moderate amount of liveness detection and other anti-spoofing measures. Due to the availability of new technologies that may be useful to attackers, Diamond Fortress has developed the **LIFECheck**™ system. LIFECheck will make ONYX exponentially more robust than it is currently. The LIFECheck system will be part of the ONYX5 release and will also be offered as a free update to licensees who use previous versions of ONYX. *(Security updates are distributed at no additional cost to all licensees according to DFT’s current policies.)*



Hopefully, this document has provided a basic understanding of the LDAS technology available to Diamond Fortress. Quite a few other more obscure methods exist, and we have developed some proprietary mechanisms specific to ONYX to combat spoofing. No biometric vendor can claim to be 100% immune to these types of attacks, but DFT places considerable emphasis on anti-spoofing tactics and the overall security of ONYX. When new technology emerges, new methods of attack emerge, so DFT is continuously evaluating and strengthening the security measures that are implemented in ONYX.