Attempts at Breaching a Fingerprint-Secured Automated Medication Dispenser Using Spoofs from Simple Fingerprint Molds

Presenting Author: James Lamberg, DO; Penn State Hershey Medical Center

Co-Authors: James Mooney, MD; Penn State Hershey Medical Center

Background/Introduction: Fingerprint entry systems are marketed as providing improvements over passcodes and proximity cards as they theoretically prove each user's identity. These security systems are not perfect and have been breached with simple techniques, such as fingerprint molds. Biometrics in healthcare represents a challenge due to hand washing protocols, environmental conditions, and the consequences of a high false accept rate when securing controlled substances. We report our initial attempts at breaching a fingerprint-secured automated medication dispenser that utilizes multispectral imaging with "liveness detection" technology.

Methods: Two approaches to spoofing the system were attempted, targeting the biometrics of one of the authors (JL). The target was currently enrolled as a provider who could obtain controlled substances for clinical use. An image based approach was attempted first. These attempt utilized images of the natural finger as well as images displayed by the medication system, which printed using a personal inkjet printer. The second approach attempted to recreate the three-dimensional structure of the finger. Two molds of the finger utilized for the biometric identification system were created from platinum cure silicone. From these molds, four silicone spoof models were created; two solid fingers and two hollow fingers. One of each model type was left uncolored, while the other was tinted to emulate natural skin tone of the target. These finger models were tested on a Lumidigm® multispectral fingerprint scanner as part of a Pyxis MedStation™ 4000 system.

Results: Image-based attempts universally failed to register, leading the system to time-°©-out. Two- dimensional images of the models, displayed by the system, showed a close match to the image of the live finger. Several attempts were made at accessing the system using the solid model without success. The hollow models were placed over the finger of the other author (JM) in an attempt to overcome the "internal fingerprint" and "liveness detection" technology. This also was unsuccessful. Using the solid model without tinting, the system displayed positioning hints before registering, then rejecting the attempt. The tinted solid model and the models over the finger were processed, but led to an error regarding the accuracy of the biometric data.

Conclusion: Fingerprint molding can create spoofs that have similar surface structures to real fingers. However, the multispectral imaging scanner was effective at rejecting our spoof fingers. This is evidently due to the deeper structures of the finger being identified. Until a model is developed that produces the surface features as well as unidentified deeper features, the Pyxis MedStation™ 4000 system utilizing the

Lumidigm® multispectral fingerprint scanner seems to be a secure system. Other systems, however, may be vulnerable to these or similar spoof attacks.

References *(Optional)*: 1) T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems," Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002. 2) Willis D, Lee M. Six biometric devices point the finger at security. 1998. Network Computing; 9(10):84-96. 3) Hoshino S, et al. Mapping a Fingerprint linage to an Artificial Finger. 2001. ISEC (60):53-59.