

USING “GUMMY” FINGERS TO DECEIVE A CAPACITANCE FINGERPRINT SCANNER

OBJECTIVE:

The objective of this lab is to explore inherent limitations of capacitance fingerprint scanners by attempting to falsely authenticate a “gummy” finger as an authorized individual. The primary question to be answered is as follows: using only common household or inexpensive items, can a capacitance fingerprint scanner be deceived into falsely authenticating an individual?

EQUIPMENT/SOFTWARE USED:

Hardware:

- HP Pavilion ZD7000
- Billionton PCMCIA FingerPrint Reader

Software:

- Windows XP Professional
- Omni-pass (with Billionton Hardware)

PROCEDURES:

Background Information

There are two common fingerprint scanners used for computer authentication. The first is an optical scanner, which uses light to scan an image of the print. The second is a capacitance scanner, which relies on the properties of flesh and air to measure differences in capacitance on the scanner when the finger is placed upon the surface. One advantage of capacitance scanners over optical scanners is the fact that the capacitance scanner requires a three-dimensional print, whereas an optical scanner requires only a two-dimensional print. This makes the capacitance scanners more difficult to deceive. However, if one could recreate a three-dimensional representation of a print, then one could theoretically “trick” the scanner into falsely authenticating a user.

Lab Procedures

To begin this lab, the student obtained a Billionton Fingerprint Scanner and installed the necessary software on a laptop with Windows XP Professional. This particular scanner uses capacitance scanning to authenticate users and allow them access to the PC. Once the software was installed, the scanner needed to be “trained” to recognize the authorized user’s fingerprint. The right fore-finger was placed upon the scanner several times, as directed by the software, in order to train the software to recognize the fingerprint. Once the software was trained, the scanner was used to authenticate into the computer. The authorized user was able to authenticate into the machine each time the finger was placed on the surface of the scanner. Four other

individuals were asked to attempt authentication, just to ensure proper rejection. Each of the four individuals was rejected by the scanner on every attempt.

Once it was certain that the scanner was correctly recognizing the user's fingerprint, and rejecting unauthorized users, the next task was to create a "gummy" finger. A pack of silly putty (\$1.75) and a box of gelatin (\$1.75) were purchased for the experiment from a local grocery store. One package of gelatin was mixed in a bowl with approximately 3-4 large spoonfuls of boiling water. The user's right fore-finger was pressed into the ball of silly putty in order to make a mold of the fingerprint. The mixture of gelatin was poured into the mold and was left for several hours to harden.

After several hours, the gummy finger was peeled from the mold. At a glance, it was very obvious that the silly putty had lost its shape during the hardening process, because the ridges of the fingerprint were very skewed and irregular. The unsuccessful attempt was confirmed when trying to authenticate into the computer using the gummy finger.

Another attempt was made to create a gummy finger, using the same proportions of gelatin and water. This time, after the finger was placed in the silly putty to create a mold, the silly putty was placed in the refrigerator to help it keep its shape. Once the gelatin had been properly mixed, it was allowed to cool (so as to not "melt" the silly putty mold). When the gelatin had cooled sufficiently, but was still liquid enough to pour, the mixture was again poured into the fingerprint mold, and was then placed in the refrigerator to cool and harden.

After several hours, the gummy finger was peeled from the silly putty and was placed on a paper towel in order to warm to room temperature. Once the gummy finger was at room temperature, it was placed upon the fingerprint scanner in an attempt to falsely authenticate the fake finger. After 4-5 tries, the computer finally accepted the

gummy finger as being an authorized print. Several more attempts were made to repeat the authentication using the gummy finger. Although most of the initial attempts were rejected, after some practice as to how to place and position the gummy finger, the computer would authenticate the fake finger approximately four of five times.

The gummy finger was allowed to set overnight, but would no longer authenticate the next day. The gummy finger had become too hard, and had shrunken considerably from its original size. It is assumed that this is the reason for why it would no longer falsely authenticate after setting overnight.

REPORT:

The first attempt to create a “gummy” finger was unsuccessful in authenticating into the protected PC. This was due to the fact that the warm temperature “melted” the silly putty so that it did not keep the shape of the fingerprint. The second attempt was different in that the silly putty was refrigerated in order to help it keep the original shape of the print. This second attempt was successful approximately four of five times, after practicing proper placement of the fake finger.

CONCLUSIONS:

The results of this lab can be considered a success in light of the fact that it was proven that household or inexpensive products can be used to falsely authenticate a “fake” finger with a capacitance fingerprint scanner. This shows that even biometric authentication devices should also be treated with some amount of skepticism before relying wholly on a single device for authentication. However, there are also a few things to consider based on this particular experiment. In order for a person to create a “gummy” finger of another person, they would first need to obtain a mold of that person’s finger. Asking a person to place their finger on a ball of silly putty, and then rushing off to refrigerate it might not be a realistic situation. However, a quick search on the Internet will provide several references with instructions on how to retrieve a two-dimensional fingerprint from a pop-can, or other object, and then etch the print into a circuit board to create a three dimensional mold. One suggestion for future experimentation would be to expand this experiment to attempt to retrieve a third-party’s fingerprint from an object, and then find some way of creating a three-dimensional mold from that print.

Overall, this lab was an interesting way to learn about fingerprint scanners as an IO device. It provided some unique insight into fingerprint scanners, resulted in surprising information, and produced suggestions for future research.