Biometrics and Failures in understanding Security – Copy & Paste Iris Scans

Posted on **May 23,2017** by **lynx**

Biometrics has an irresistible attraction. Simply by mentioning the fact that you can measure parts (or surfaces) of the body and convert them to numbers a lot of people are impressed out of their mind. Literally. In theory biometric information serves as a second set of data to be used for any purposes. A common purpose is to use it for authentication. Most physical sources of biometric data are easily accessible. Fingers (for fingerprints), eyes (for your iris), limbs (for your veins), voice (for the Cloud), and other examples show this well. Where does the security come into play? Well, it doesn't.

Image not found
http://blog.dustball.com/wp-content/uploads/2017/05/Biometrics-can-be-copied.jpg
Biometrics can be copied

For starters, passwords can be changed. Biometrics can't unless you have a transplant. In contrast to passwords biometrics can be faked. The biometric source can be copied. In most cases this is as easy as doing a scan and printing it again. The German Chaos Computer Club has repeatedly demonstrated that copies work extremely well. They used simple iris photographs (for gaining access to a Samsung Galaxy S8) and fingerprint copies (to overcome Apple Touch ID) in the past. Almost any multi-factor authentication beats this security record easily.

Furthermore the biometric check is based on a comparison of digital data sets. Algorithms compensate for variations during the measurement, i.e. the scan phase, of the body part used. Since no two measurements are alike, there is some room for errors. This can be exploited by adversaries. Think of it as trying to manipulate optical character recognition (OCR) by manipulating text and fonts. You can do this for voices, too. Recently a Canadian company was in the news, because they showed recreated voices of Barack Obama and Donald Trump . The source were samples from interviews and speeches.

So please don't use biometrics as a silver bullet to solve problems which can be solved more efficiently by other technologies. And don't use sensors designed to work for and in your living-room for critical security. In case you won't do this, we welcome you or your company as a show case at DeepSec 2017. The presentation title might even contain your name.

Posted in:High Entropy,Security | Tagged:Mindset,Observation,Security | With 0 comments