



Beware of Biometric Images

By Larry Hamid,
Chief Technology Officer, MXI Security

Recently there was an article published whereby several USB sticks with biometric authentication were found to be completely insecure (See “Easy to crack” <http://www.heise-online.co.uk/security/Secure-USB-sticks-cracked--/features/110280/0>).

In the article it was demonstrated how on some “secure” USB devices biometric authentication can be bypassed completely. Rest assured that biometric devices from MXI Security do not fall into this category. We have secure implementations of biometric and encryption technology within our devices.

I want to delve into this topic a bit deeper and provide a bit of insight for readers who want to be better equipped to challenge biometric technology vendors on the security of their implementation.

I like to categorize the deployment of biometric technology in four ways based on where the biometric matching is actually done.

Match-on-PC
Match-on-Server
Match-on-Card (on a smart card that is)
Match-on-Device

First, matching is not the only part of a biometric process. There is also image capture whereby an image of a biometric sample is captured from a sensor, and template creation where the image is processed to extract the important features for the matching algorithm. Template creation is actually done in two places within the overall biometric system; a) to create enrollment templates when you first register your biometric, and b) to create verification templates that are used in the actual matching when you are attempting to authenticate. For the best biometric security, all three of these processes (image capture, template creation, and matching) must be done in a trustworthy environment.

Here is a useful fact that is generally true for biometric technology and can help you read between the lines: matching is computationally much cheaper than template creation.

In Match-on-PC the local host system is used to do the biometric comparison. What does this mean? Well it means that your enrollment templates and your verification templates are compared in software on the PC, out in open, and exposed to the seething pool of malware that might be on the system. Furthermore, it probably means that template creation is also done on the PC because if the matching needs to be done there, most likely there is no where else to do the template creation either. If your biometric templates are compromised it could be bad news for whatever systems you are protecting with biometric authentication. *Tip: don't ever*



use a Match-on-PC implementation at an Internet Café. Until PCs become trustworthy platforms I would never contemplate using this mode.

Match-on-Server is much better than Match-on-PC. Assuming the server is protected and trusted, it is a safe environment to do the biometric matching. Most often though the server will have a database of user templates, which raises privacy concerns for many people. Unfortunately server implementations can be expensive to deploy because of the need to protect biometric information in transit, and the need to provide scalability, fault tolerance, and high-availability. Another thing to watch out for in a Match-on-Server implementation - and this is important - is that template creation has to occur somewhere. I'll bet that 90% of the time it won't be on the server because of the extra processing requirements. So where is it done? It might be on the PC where the sensor is attached which would be bad. If instead it is done on the biometric sensing device then there needs to be a good reason to have a server since the device probably has the power to also do the matching. A couple of potential reasons could be: a) the biometric devices are not portable and since many users use the machines the templates need to be stored centrally, or b) the server is doing biometric identification (checks against many templates, not just yours), for some reason or other.

Match-on-Card is rather interesting. Smart cards are very secure platforms in which to perform any kind of security function. Biometric matching has been tough to achieve on a smart card because of the processing requirements but there are several implementations now available on the market. Smart cards don't have biometric sensors built into them and they certainly don't have the power to do template creation. So again, a Match-on-Card solution needs a trustworthy environment (outside of the card) where the other parts of the biometric processing can occur securely. One option here is a portable device that contains the smart card chip or a secure smart card reader with the biometric sensor and processing power built in.

Match-on-Device can be the most deployable and the most secure type of biometric implementation. Here the image capture, template creation and matching are all done within hardware (preferably a hardware device with certified security). No biometric information ever leaves the device. Furthermore as mentioned above, this can also be a good hybrid solution with a Match-on-Card technology. Because of the portability and no requirement for a server infrastructure it is a very attractive solution from a cost and usability perspective. In addition, the enrollment templates are carried securely in the possession of the user so there are no privacy issues to be concerned about.

This brings me back to the title of this article and why you should be wary of biometric images. *If you see a biometric image being displayed in a user interface while your sample is being captured, then your biometric information is being exposed to the system that is displaying the user interface.* I know it's cool to see your fingerprint displayed, but think about where the software is running.