Brian Owen
SE4930-Information Security
Article Review #2
1/11/2011

"Biometrics for Increased Security"

Access to content is an ever growing need. We as users of applications often need to authenticate ourselves with an application before gaining access to our stuff. Accessing online banking, digital media and e-mail are all done through-out the day. Currently, the principle type of authentication is passwords. Passwords are becoming growingly unreliable, due to the simplicity in which the user makes them, the reuse of passwords across applications by a user and the revealing of passwords to friends and family. In fact, the most common password used is "password". Because of the growing need for security and the ever decreasing reliability of passwords, Biometrics may provide the solution.

Biometrics can be used to identify a user's identity. It can use several different types of traits (identifiers) to determine identity These include face geometry, finger print, hand geometry, iris, keystroke, signature, and voice. These identifiers offer several advantages over the traditional ones. One advantage is that a biometric cannot be lost or forgotten, like passwords can. Biometrics are hard to steal/copy/forge, share with friends or distribute. Because of this, it is required of the user to be present at the time of authorization, unlike if you were to give a friend your username and password.

We can use these biometrics to replace passwords, but how do each work? From here out we will discuss a basic premise and idea of how face geometry, finger print, hand geometry, iris, keystroke, signature and voice biometrics work. Face geometry is a nonintrusive method, and what humans use to recognize others. However, Facial recognition software doesn't work very well. It is hard for software to recognize a face as a stored image (or mugshot) may not have been taken in the same light or at the same angle. Because of this, recognizing faces with software is difficult.

Finger prints over the decades have proven to be very accurate for proving unique identification. Finger print scanners are relatively cheap and adequate for authentication in systems that only have a few hundred users. As more users are added, however, it requires larger amounts of system resources and the use of multiple fingers becomes recommended. So while overall good, even if system power constraining, they will not work well for people who have labor intensive jobs, as cuts and scars are hands/fingers are ever changing.

Hand Geometry systems are simple, easy to use and cheap. Factors that affect skin condition do not seem to have large impact on the hand. The downside to hand geometry as it doesn't work for kids growing up, and the geometry of one's hand is not known to be distinct in any way, leaving the possibility of not working in large systems with a large user base. Typically these scanners are used in conjunction with another biometrics, such as fingerprint readers and iris scanners.

Iris scanners scan the user's eye, and have shown promising development. The iris, although not proven, is believed to be unique. This is true even for genetic twins. The iris develops in the first 2 years

of life and artificial irises are extremely difficult to manufacture. Iris scanners have a low false accept rate (mistakes unauthorized users for authorized users), but also rank as one of the top false reject rate (mistakes authorized users as unauthorized users). These factors make iris scanners as potentially one of the most secure types of biometric scanners.

The last type of biometric I will discuss is that of voice. Voice is affected by background noise, changes throughout life, and can be affected by illness. The text a user reads to a machine is also a previously uttered phrase. Overall voice is an alright solution, but not an ideal one. Too many external factors affect a noise sample, and voice recognition software is not an entirely reliable toolset as of yet.

The various types of biometrics have their pros and cons, but one of the hardest things about all biometrics is the variance. Passworded entries need to match exactly, however with most biometric applications there needs to be some sort of acceptable variance as variance between correct samples may exist. There are three common reasons for variance in biometric systems. Inconsistent presentation, signal captured by sensor may not match exactly due to a difference in how you scanned the biometric sample and the scan of you trying to log in. The second is irreproducible presentation, such as the metric changing. For example, if you have a fingerprint and you cut your finger, you can no longer access the account to change it as the original scan of the finger is not reproducible with your new cut. The third is an imperfect signal/representational acquisition. This involves the conditions around the biometric being different from when they are sampled for an entry.

Another consideration when using a biometric system is how it will be used. In some instances you may want to use it for identity verification while others identity identification. The difference being in verification you would still have an ID (say, Brian Owen) and log in with your fingerprint while in identification I would place my fingerprint down and the system would tell me I was Brian Owen. Identification would require significantly more computer resources. Furthermore, biometric systems would not be less vulnerable to certain types of attacks. They attack types, mainly circumvention, repudiation, collusion, coercion and denial of service, could still attack the systems log in to gain access to the information.

There is much more to this article, as the depth of implementations are discussed and circumventing known errors are also mentioned and discussed. But in all, this article enlightened me to the pros/cons of biometric security systems and some of the issues that may occur with them in the future, if they were ever universally used. It also summarized how attacks could still occur in a biometric system, proving that no matter how advanced a logging into a system is, it will always have vulnerabilities.

Works Cited

Jain, A Et al. (2006). Biometrics: A Tool for Information Security. *IEEE Transactions on Information Forensics and Security* , 125-143.

Brian Owen
SE4930-Information Security
Article Review #2
1/11/2011