The case against biometrics as a means of authentication or as a cryptographic key in an uncontrolled environment

Vincent L Gilbert MCSE MCSA MCP
Matthew Corrinet

Abstract

In this paper we will demonstrate that any technology involving the use of biometric signatures is unsuitable for authentication and encryption purposes in unsecured installations. Whereas other papers have focused on highlighting the problems in individual biometric schemes, this paper will attempt to demonstrate that the concept itself is fundamentally flawed.

Terminology

For the purposes of this paper, the following definitions will be employed;

Secured installation - *Any location which has a secondary verification process usually human that ensures that the bio-metric signature is being presented in the way that was intended or otherwise insures against the use of falsified bio-objects.*

Unsecured installation - *Any location which does not have a secondary verification process usually human that ensures that the bio-metric signature is being presented in the way that was intended or otherwise insures against the use of falsified bio-objects.*

Biometric signature - *The byte array produced by a bio-object*

Bio-object - *The biological part or process used to present the bio-credential*

Bio-credential -*The portion of the bio-object which produces the bio-metric signature*

Bio-entity – *The entity (presumed to be human) which possesses the bio-object used to create the biometric signature.*

Fundamental problems

Kerckhoffs's principle

1. The system must be practically, if not mathematically, indecipherable;
2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;
3. Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents;
4. It must be applicable to telegraphic correspondence;
5. It must be portable, and its usage and function must not require the concourse of several people;
6. Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

In reviewing Kerckhoff's paper [1] we see that he states in part:

[1] That any cryptographic system should rely solely on the secrecy of the key.

A cursory examination of any biometric system shows that biometric authentication or crypto logic systems as a whole do not adhere to this principle and largely rely on the secrecy of the mechanics of the system to achieve security. While we will examine the failures in individual systems in the sections below, it can be here noted that the recent failure of Apples finger print scanner as an authentication system is highly representative of this flaw. In any biometric authentication or crypto logic system, the key begins as a bio-object and is readily and usually publicly available, whereas it is the mechanics of the device which is kept secret. It is therefore only necessary to back engineer the mechanics in order to break the security of the system.

[2] That the key must be changeable.

Again, a cursory examination of any biometric system will show that it does not adhere to this principle. Simply stated the bio-object in any bio-metric system is used to produce a bio-metric signature which is stored on the system which is charged with accepting or rejecting credentials. Should this biometric signature be compromised, either by a secondary collection of the bio-object or by a compromising of the system storing the biometric signature, then there is no way to replace those credentials past the biological limit of the human body. Simply stated, a human being has a limited number of bio-objects per biological category e.g. (Ten [10] fingers, two [2] retinas, etc.). Unlike a password (which adheres to Kerckhoff's principle), if the bio-signature is compromised, there are a finite number of times that it can be replaced.

System lockout during critical use scenarios

Assuming that a system which overcame these problems could be designed, there is another area where biometric systems fail at the fundamental level. Consider the process for creating a biometric signature. A bio-entity will present a bio-object to a device which results in a biometric signature which is then stored. This creation will necessarily take place under pristine conditions.

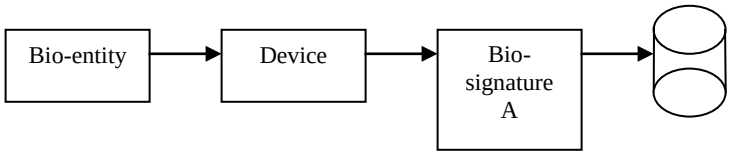


Fig. 1

When engaging in an authentication or crypto logic process, the presentation process is repeated, and the newly created biometric signature is compared with the one which was previously stored.

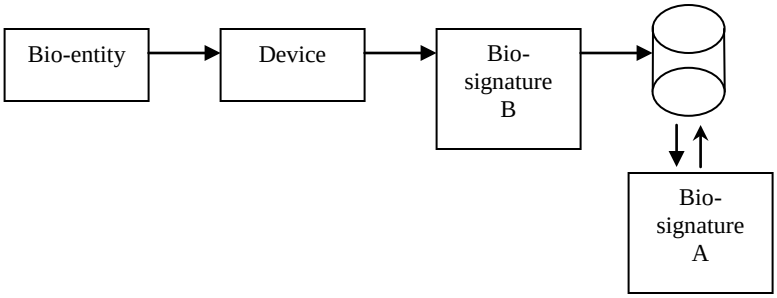


Fig. 2

The problem occurs when the concept of bio-object is extended past those objects which were originally considered for biometric authentication and crypto logic use. These objects, namely, fingerprints and retinas, were considered for use precisely because they were unchanging, however many of the bio-objects currently being considered or employed are in fact subject to change. Furthermore, if we consider emergency situations, even if the bio-object can be thought of as unchanging, there is the possibility that it may be obscured. Human dependency on devices that will necessarily employ some sort of authentication is well documented. (Adamski) [2] Let's consider a real world scenario where facial recognition has been employed to secure a smart phone; in this scenario, the individual has had an automobile accident and has struck their face, which has caused them to bleed from a scalp wound. This is a mission critical situation and the individual needs to access the device in order to secure help. The problem is that in a stressed, or less than pristine condition, the process shown in [Fig. 2] is altered, and the biometric signature produced will necessarily be differentiated from the stored signature. The user is locked out of the device at a time when the need for access is crucial.

Exploitation methodologies

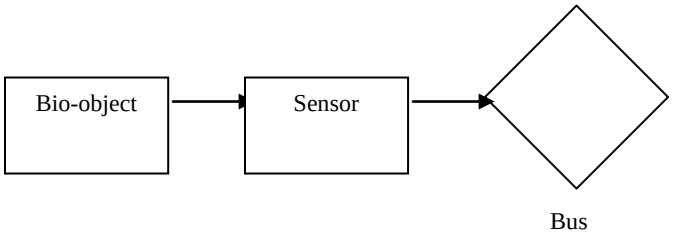
Here we will examine some of the methodologies that can be employed to exploit the fundamental flaws that will be present in any biometric device which has been deployed in an unsecured environment.

Presentation of credentials using a falsified bio-object

In this type of attack, the target's bio-signature is obtained after the system has created and stored it, or an example of the targets bi-credential is harvested. Using this material, various methodologies suitable to the type of bio-object being falsified are employed to create a physical representation of the bio-object which re-produces the targets bio-credential. In their description of the attack against Apple's "TouchID" [5], the German hacker group known as [sic] the "Chaos Computer Club" describes the ease with which persons unschooled in techniques such as special effects creation can create a falsified bio-object using crude methods. The work done by Javier Galbally [6] at Madrid's Universidad Autonoma on producing a falsified iris demonstrates that even complex bio-objects, can in fact, be re-produced.

Presentation of credentials through purely digital means

While most of the actual and theoretical breaches that have been proposed or actually carried out against biometric authentication and crypto logic schemes involve the creation and subsequent presentation of counterfeit bio-objects, there is another flaw which will necessarily affect any and all schemes that are devised.



Gathering of bio-signatures

Social means

Many of the arguments for biometrics have centered on the clandestine aspect surrounding the collection of actual biometric information as being impractical, or “James Bond” like. This should be rejected for the following reasons;

[1] The widespread use of homeless persons particularly those that are addicted to drugs such as methamphetamines to collect personal information through the process known as “dumpster diving” has demonstrated that there is a literal army of individuals that might be employed for the purpose of gathering wholesale non-targeted bio-credential material. This type of harvesting might include hair and other biological materials as DNA samples, the collection of impressionable surfaces for fingerprints or other biometric material. Furthermore, being connected anonymously through services such as TOR, they would be impossible to reliably detect and thwart. [3] [4]

[2] Social engineering attacks are routinely used against high value targets to gain access to personal information and we can expect that this methodology will continue to be employed in the harvesting of bio-credentials related to high profile targets. One example would be the collection of high resolution close up images which would detail a targets iris. This type of collection could be easily accomplished at a social gathering to which a potential target had been invited.

Purely digital means

[1] Referring to [Fig.1] above, we see that in any biometric process, at some point the bio-object is converted to a biometric signature and subsequently stored. Even if a manufacturer seeks to obfuscate the data by storing it in a proprietary format prior to encrypting it, we can access the data. We will use the fingerprint scanner as an example so that the information might look like that shown in [Fig. 3] As we have access to an example of the device, we can back engineer it to determine what process was used to black (obfuscate) the data. To begin we store a baseline by storing a snapshot of a screen with no data. The difference between the stored data and the baseline is the fingerprint irregardless of the format that the data is stored in. The process of back engineering would vary depending on the mechanics of the device; however the same techniques would be employed. If the encryption algorithm is unknown, but we can change the key, then by changing the key to a known value and running our baseline image through known encryption algorithms (done on a separate system), eventually we will get a match. Now that we have an encrypted baseline and know the process by which it was encrypted, we can brute force the key. By running the process against images of known geometric objects, we can observe the result and reduce the time necessary to break the key. Whatever the process necessary to break the security, eventually through purely digital means the biometric signature will be revealed.

Fig. 3

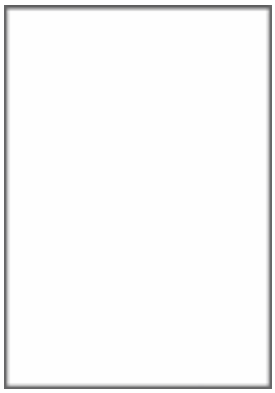


Fig. 4

Fig. 5

Consequences

The consequences which will inevitably follow the widespread use of biometrics will mirror those that came with the widespread storage of unsalted passwords. Eventually we will see large databases of bio-signatures being created and distributed for illegal purposes.

Examination of various schemes being considered

Finger print scanners

While the bio-object (fingerprint) may be thought of as being generally unchanging, there are instances where the biometric signature may be compromised resulting in a system lockout. Consider the possibility that an emergency situation such as an automobile accident has damaged the digit that was used as the bio-object. The result would be a system lockout in a mission critical situation. As such, the fingerprint scanner will also be susceptible tp the types of attacks detailed above. The most recent example of the failure of this type of system would be the confirmed breach of Apple's fingerprint scanner which was hacked by Germanys *Chaos Computer Club*. [5]

Retina scanners

As with fingerprint scanners, the bio-object (the retina) used by retinal scanners may be thought of as largely unchanging. However, there is even a higher degree of probability that in a mission critical situation, access to the bio-object may be obscured resulting in a system lockout. In addition, retinal images are not as hard to procure as is widely accepted. Most ophthalmologists regularly take retinal images as part of a routine eye exam. These images are then stored in unsecured facilities both digitally and as hard images. At the time this paper was written we could find no published examples of actual attacks against existing retinal scanners, however, in general terms retinal scanners if employed in an unsecured system would be susceptible to the types of back engineering attacks detailed above.

Iris scanners

Like the fingerprint scanner and the retina scanner, the bio-object which is used in the iris scanner (the iris) can be thought of as largely unchanging. However, like both of the bio-objects previously discussed, the iris may be obscured in an emergency situation. In addition to the common problems mentioned under the heading "retina scanners" the iris specifically may be subject to certain medical procedures which change the coloration and shape of the iris. Iris scanners are susceptible to the types of attacks described under the heading **Purely digital means** and as described by Javier Galbally, Julian Fierrez, and Javier Ortega-Garcia [10]

Facial recognition

Facial recognition scanners are susceptible to problems associated with the violation of the principles mentioned above. In addition the bio-metric signature is extremely vulnerable to change which would result in a system lockout. Actual breaches have been demonstrated with one of the most notable being the breach of Toshiba's facial recognition system at the 2012 Black Hat convention. [7] While no reviewed statistical data was available at the time this paper was published, conversations with ER nurses indicated that at least 50% of the trauma cases they encountered produced scalp lacerations of the type which would alter the nature of the bio-signature produced.

Gesture recognition

Gesture scanners would include any scheme which includes movement in a bio-object. These are relatively new and so have not been examined to the extent that other biometric schemes have, but they are susceptible to the same flaws as above. We will include positional reference schemes such as the car seat posture system developed at Tokyo's Advanced Institute of Industrial Technology institute in this category. By including bio-mechanics, the problems associated with system lockout are exacerbated. Once again consider a common occurrence, the automobile accident. In a system where biometric sensors are used to detect positional relationships, we might infer from a review of automobiles that have been involved in accidents that a significant displacement of those sensors might occur. When we add to this the probability of injury related changes in the occupants posture, once again we see that there is a high degree of probability that a system lockout would occur.

DNA recognition

DNA recognition is susceptible to problems associated with the violation of those principles mentioned above. While it may seem that DNA is not susceptible to change, research in the area of gene therapy shows that it is possible to alter the DNA gene sequence without producing a noticeable immuno response by using an Adeno-associated virus as a vector. Less than .1% of DNA separates individuals with current DNA identification techniques focusing on (VNTRs), particularly short tandem repeats (STR's) DNA recognition systems will necessarily focus on a very small part of the Genome. Although current research focuses on replacing a single gene, there does not seem to be a significant obstacle to introducing enough genetic material modification in order to produce a system lockout. As current efforts to thwart biological attacks center on large scale attacks, this type of attack would be extremely difficult to defend against.

Summary

In a secured facility, biometric authentication procedures may be safely employed as there is an independent verification of the methodology by which the credentials are presented. Using the breach of Apples fingerprint scanner as an example, we can see that this was possible because the credential (a device other than the actual thumb of the user) could not be verified as authentic. These systems accept that the key (The bio-object) is not secret, and therefore rely on the mechanics of the device to prevent an un-authenticated presentation of forged credentials.

Simply stated;

You can never create a biometric scheme which confirms to Kerckhoff's principle or one which is not susceptible to lockout and therefore it is impossible to create a device that will remain secure for even a reasonable length of time. The concept is fundamentally flawed.

Furthermore, continued attempts to do so will only result in a black market for biometric data that cannot be controlled and which jeopardizes the legitimate use of biometrics in secured facilities.

[1] Auguste Kerckhoffs, "La cryptographie militaire" Journal des sciences militaires, vol. IX, pp. 5–83, January 1883, pp. 161–191, February 1883.

[2] Adamski, Shayne. "Using your cell phone before during and after a disaster." *FEMA* 10 Mar. 2011: n. pag. Web. 10 Mar. 2011.

[3] "Dumpster diving." Def. *searchsecurity.techtarget.com.* 2005. Web.

[4] Stroup,Jeff "Identity theft how it happens" *about.com* n. pag. Web.

[5] Frank. "Chaos Computer Club breaks Apple TouchID" *CCC* 9 Sept. 2013 n. pag. Web. 9 Sept. 2013

[6] Smolaks, Max "Iris Scanners Hacked at Black Hat USA 2012" *TechWeek (Europe)* Jul. 2012 n. pag. 27 Jul. 2012

[7] Higgins, Kelly "Researchers Hack Faces In Biometric Facial Authentication Systems" *Darkreading* 12 Feb. 2009 n. pag. 12 Feb. 2009

[8] Taylor, Terry "STR Analysis" *National Institute Justice Journal 267* 3 Mar. 2011 n. pag. 27 Jul. 2012

[9] United Nations. CTIF. Interagency Coordination in the Event of a Terrorist Attack using Chemical or Biological Weapons or Materials. New York: United Nations, 2011. Print.