

Contribution on Biometric Peer Review Issues to AHGBEA

Date: January 30, 2006

Contributors:

- Jim Kottas, Viisage (POC)
- Matthew Young, Purdue University
- Shimon Modi, Purdue University
- Cathy Tilton, Daon

Peer Review and Biometrics

Public peer review of cryptographic systems is a popular practice for proving the strength of the algorithm or methodology being tested. If a cryptographic methodology is in fact able to be broken, tremendous publicity often ensues describing the details of how it was broken and the amount of resources needed to successfully break it. Generally speaking, there are three important aspects of a cryptographic system as it relates to the peer review process. These are the encryption and decryption functions, the cipher text, and the key. Cryptographic systems rely on the secrecy of a key; so in order to effectively “break” the system, the encrypted information must be revealed without any knowledge of the key. The other two aspects of the system are made completely open so that the encryption-decryption functions do not provide a single point of failure.

In comparison, a biometric system also has three important aspects that are analogous to a cryptographic system: the biometric sample, the biometric template or reference, and the matching algorithm. As it stands right now, the security of the biometric system is reliant on the strength and secrecy of the matching algorithm. The sample provided by many live-capture biometric systems is considered non-secretive information. The template or reference corresponding to that biometric sample should also be considered non-secretive as a template or reference could be created using the sample. In this sense, the biometric sample and its associated template should be considered non-secretive and thus are the two open parts of the system. It should be noted that the process of creating a template and the data it contains is still considered secretive information.

There remains some debate as to the secrecy of biometrics, at least for certain biometric modalities. While most biometrics (samples, etc.) are not secret, strictly speaking, they can be hard to capture by someone else. However, in the view of NIST Special Publication 800-63, “Electronic Authentication Guideline” [SP80063]:

Biometrics do not constitute secrets suitable for use in the conventional remote authentication protocols addressed in this document. In the local authentication case, where the claimant is observed and uses a capture device controlled by the verifier, authentication does not require that biometrics be kept secret. The use of biometrics to “unlock” conventional authentication tokens

and to prevent repudiation of registration is identified in this document.

The perceived downfall of requiring physical presence for the authentication to work is why biometric technologies are viewed as inadequate secrets in the remote environment.

When considering peer reviews for biometrics, these same principles of starting with no previous knowledge must apply in order to be compared on the same level. Whether or not it is believed that biometrics are secrets, the worst case scenario must be assumed that they are not secretive and can be obtained without voluntary assistance from the individual.

Fundamentally, the cryptographic community and the biometrics community approach peer review from very different perspectives. These differences, along with a comparison with other aspects from the two communities, are summarized in Table 1 below. From William Burr's presentation at the 2004 Biometric Consortium [Burr], there is a "culture clash" between the two communities. The cryptographic community is very adversarial and believes they have done a good job if they can publish an attack that can defeat a particular algorithm. They believe the algorithms should be completely open so everyone knows how the process works and the security comes as a result of the secretive key chosen for each individual case.

In contrast, the biometrics community is just the opposite – it is very test-oriented and market-driven with intellectual property rights at stake. While these two approaches may seem completely incongruent, they derive from fundamentally different factors. Cryptography is algorithm-based and completely repeatable and deterministic. That is, given a particular algorithm and its necessary data, the cryptographer will always get the same results. On the other hand, all biometrics are based on one or more statistical techniques with noisy input data from the biometric capture process. While any given biometric algorithm will process the same input in the same way, the probability of capturing an identical sample of an individual's biometrics is extremely low. For example, imagine the difficulty in capturing the exact same image of someone with a digital camera. With subtle changes in ambient lighting and the various auto-compensation mechanisms built into the camera, it is effectively impossible.

Biometric algorithms are more in the realm of statistical pattern matching, signal analysis, and classification and communication theory rather than the non-statistical algorithms that cryptographers use. This is not to say that cryptographers do not use statistical approaches. However, they do so in order to break a cryptographic algorithm, not as the basis of the algorithm itself.

Because all biometrics are statistical in some way, there will always be some probability of generating some type of error (for example, false match, false non-match, failure to enroll, etc.). This is true even of biometric algorithms and capture devices that are completely open and in the public domain. The cryptographic community is not accustomed to dealing with systems that inherently cannot have zero error rates of any kind.

Because of the expense in developing and maintaining biometric algorithms and capture hardware, the financial marketplace demands that biometrics vendors give proper consideration

to intellectual property rights. Consequently, the best algorithms for the different biometric modalities are kept private and proprietary and may be disclosed only when sufficiently protected by patents and the like.

Some analogy can be made here with the history of the RSA patent in the cryptographic community in the 1980s and 1990s [RSAPat]. RSA published their new algorithm, and then took advantage of patenting it, which resulted in several years of contentious usage until the patent expired in 2000. Now, with the RSA algorithm freely available, the main business opportunities for RSA-like cryptography lie not with developing new algorithms but in building and deploying infrastructure implementations and applications that use it (see Table 1). The biometrics marketplace is arguably not as mature as the cryptographic marketplace, and many biometrics companies are in a somewhat analogous situation as RSA in the 1980s – they have patented algorithms that may or may not have been published. While the biometrics community agrees that “security by obscurity” is not a viable way to promote the use of biometric technology in security contexts, the biometrics marketplace has not yet developed sufficient drivers to accommodate and support open algorithms and open live-capture devices.

To deal with the statistical nature of biometrics plus the market tendency for algorithmic secrecy, the biometrics community relies heavily on public testing of their systems, more or less in a black-box configuration with standardized input data, and prototype installations by evaluation customers.

Certainly, the adversarial approach by the cryptographic community can be beneficial to the biometrics community in several ways. For example, it can help ensure that claims made by biometric vendors are valid and can be substantiated. Furthermore, adversarial attacks can help to discovered new ways of breaking a biometric system so that these problems can be addressed and fixed.

For example, Burr [Burr] claims that, “Cryptographers believe that a dental technician has the skills and materials to construct a copy of a fingerprint that will fool most fingerprint readers.” However, it is important to keep in mind that with a biometric system, the success of any attack needs to be viewed in the context of the entire system, including an analysis of the tradeoffs between risk, security, convenience, and user alternatives. For example, the best cryptographic system in the world is useless if the user community writes down their passwords on yellow sticky notes and affixes them to their monitors. The cryptographic community is proud when they break a biometric system using fake fingerprints made from common materials [Matsumoto, Schuckers]. While certainly these findings will help improve current and future biometric systems, it does raise the question of how easy it is to actually capture the biometrics for people who are already enrolled in the system, and what skill set is needed in order to create falsified biometric data that might work.

For example, in the case of trying to create false but valid fingerprints, the question becomes how much interaction is needed by the enrolled (i.e., known good) individual to effectively fool the fingerprint sensors. If the individual cooperatively submits their fingerprint into a mold or other means for the spoofing attempt; then biometrics are not being compared equally to the peer review process of cryptographic systems. It is significantly harder to extract a fingerprint which

is capable of being used to spoof a sensor from the surface of a desk, for instance. This type of peer review would be non-cooperative. Beyond the difficulty of effectively retrieving a latent print, more variables also come into play:

To whom does the extracted fingerprint belong?
From which finger does the print come?

This type of “user-cooperative” biometric peer review is not at the same level as peer reviews of cryptographic systems and thus is not an apples-to-apples comparison of the relative strengths of biometrics. In some ways, the effort needed to successfully fool sensors can be viewed as an added advantage because the biometric data can be known; but still not be used to break the system.

Biometrics is just one piece of a system that can help secure it and maintain a level of trust in the users of the system. However, for systems and environments that have increasing security requirements, it is much more likely that multiple authentication methods will be used. Biometrics is the only one that has a chance of tying an individual to a credential or a token.

Because of its statistical nature, biometrics will always need to be analyzed, reviewed, and evaluated in at least a partially different way from cryptographic systems. The biometrics community has responded to this challenge by drafting and using standardized testing and reporting protocols. This approach will continue to be used until a better one is proposed, either within the biometrics community or by an external group such as the cryptographic community. Unless the cryptographic community can come up with a non-statistically-based way to guarantee the integrity of the relationship between an individual and a token or credential or a claim of identity, biometrics will continue to be used for this important purpose.

Table 1 – Comparison of Approaches for the Cryptographic and Biometrics Communities.

Category	Issue	Cryptographic Community	Biometrics Community
Assumptions	Data	The strength is in the data (key), not the algorithm. Therefore, share the algorithm and maybe the implementation with everyone.	Biometric data is unique to each individual.
	Computational Complexity	Only a concern for embedded devices.	Only limited by implementation performance considerations.
	Devices	Hardware implementations can be implemented securely.	Biometric capture can be done and be made secure.
	Privacy	Not applicable.	Enrolled biometric data must be protected at the system level using conventional best practices.

Category	Issue	Cryptographic Community	Biometrics Community
	Secrecy	All cryptographic mechanisms depend on the secrecy of the data (key).	Although there is debate over how secretive biometric data really is, biometric technologies do not rely on maintaining secrecy.
	Business Incentives	Primarily at the infrastructure level and not at the algorithmic level.	At all levels of the technology and deployment.
	History	Established history of best practices with cryptography (see, for example [FIPS1402]).	Immature, not viewed as truly established.
Technological Characteristics	Dependency on Human Interactions	None.	Very dependent. All input data originates with the live capture of a person's biometric data.
	Algorithmic Approaches	Completely deterministic, at least mathematically.	Effectively only statistical approaches are used. Can be based on a wide variety of algorithms.
	Key Generation	Determined by algorithm.	Template generation is determined by algorithm
	Key Storage	Stored key must be protected against unauthorized access at the system level to ensure secrecy of the key.	Enrolled biometric data must be protected against tampering at the system level to ensure integrity of the biometric data.
	Repeatability	For each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur (e.g., guessing a password or PIN, false acceptance error rate of a biometric device, or some combination of authentication methods) [FIPS1402].	Nothing guaranteed. Any two biometric capture events corresponding to identical mode are not guaranteed to produce identical data inputs (raw biometric samples).
Peer Review	Philosophy	Open reviews with open and even confrontational discussions of results.	No peer review of algorithms, which usually are proprietary. The biometric engine and its enclosed algorithms are treated as black boxes and tested accordingly (see below).
	Methodology	Theoretical algorithm analysis and experimental cracking techniques.	Performance tests by independent bodies/agencies.
Data Compatibility	Key Formats	Keys are either ASCII strings or arbitrary 8-bit binary data. No compatibility issues or interoperability issues.	M1.3 Data Interchange Format standards for each biometric modality.

Category	Issue	Cryptographic Community	Biometrics Community
	Data Formats	Several standards apply (PKCS, etc.).	M1.3 Data Interchange Format standards for each biometric modality.
	Output Results	Binary – either the cryptographic operation works or it doesn't (meaning that the desired data is not returned).	Analog range of comparison scores. Scores are more akin to probabilities than definitive ratings.
Interfaces	APIs	Various common APIs but no common standard API.	M1.2 Interface standards.
Testing	Approach	Mathematical analyses of various kinds plus experimental attack implementations. Any and all attack challenges are welcome.	M1.5 Testing standards.
	Input Test Data	Any data can be used.	Should be collected from live individuals under documented conditions. Many variables to control or at least acknowledge.
	Output Test Data	Decrypted messages which are either the same as the original messages or not the same. Also, the rate at which a particular cryptographic algorithm and/or implementation can be compromised or the computational complexity to do so.	Sets of performance graphs representing various cross-sections of the possible statistics of the comparison scores.
	Publication of Results	Open and encouraged. No restrictions for serious algorithms under consideration.	Restricted or governed strictly by the testing organization.
System Level	Integrity (Spoofing)	Integrity maintained at the system level using key management standards.	Liveness checking in various stages of development and deployment, depending on modality. Furthermore, a multimodal system will help ameliorate any spoofing attempts.
	Data Injection or Monitoring (Replay Attacks)	Have been dealing with this issue successfully for a long time.	Possible, but the biometric algorithm should reject an exact data match. Furthermore, conventional cryptographic techniques can be used to mitigate the risk.

References

M1/06-0084

- [FIPS1402] Federal Information Processing Standard (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules," May 25, 2001.
- [SP80063] William E. Burr, Donna F. Dodson, and W. Timothy Polk, NIST Special Publication 800-63, "Electronic Authentication Guideline," Version 1.0.1, September 2004.
- [Burr] William E. Burr, "NIST E-Authentication Guidance SP 800-63 and Biometrics," presented at the Biometrics Consortium Conference on September 21, 2004, available at http://www.biometrics.org/bc2004/Presentations/Conference/2%20Tuesday%20September%2021/Tue_Ballroom%20B/2%20NIST%20Session/3%20Burr_presentation.pdf.
- [RSAPat] United States Patent 4,405,829. Some historical context is available at <http://www-cse.stanford.edu/classes/cs201/projects-99-00/software-patents/rsa.html>.
- [Matsumoto] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems," Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.
- [Schuckers] For example, see "Clarkson University Engineer Outwits High-Tech Fingerprint Fraud," available at http://www.yubanet.com/artman/publish/article_28878.shtml. More experiments on spoofing biometrics can be found at <http://www.extremetech.com/article2/0%2C1697%2C13919%2C00.asp>.