CROSSMATCH®

The world identifies with us.℠

WHITE PAPER

BIOMETRICS BEST PRACTICES

Optimizing Security in Fingerprint Technology Deployments

Moving on from Antiquated Security Schemes

There is no argument the world is becoming more digital and more connected. Most of the transactions we conduct are with people we never have, or ever will, meet. At work, we collaborate with people spread out over multiple offices, campuses and countries. We access critical work information virtually anywhere, using smartphones, tablets and computers. Even government services — which used to require paper forms and standing in line — are accessed remotely, any time of the day.

Layering technologies is more effective than relying on human behavior.

This digital and highly connected way of living has outgrown traditional methods of identification. ID cards and passwords present unacceptable risks and costs. Almost any public or private enterprise that values secure identity and secure transactions has moved to — or is moving to — the use of biometrics.

Biometrics, like any other advanced identification technology, is not a magic silver bullet. While fingerprints and other biometrics are central to our new digital ecosystems, they must be deployed in a manner that optimizes the security of identity and transaction data.

One lesson that can be taken from the tens of thousands of successful biometrics deployments around the world is that layering and configuring technologies is easier to control and more effective than relying on human behavior. This white paper outlines the points of attack of a fingerprint authentication solution and provides a realistic assessment of the cost/benefit of recommended mitigation strategies.

Initial Security Considerations for Biometrics Deployments

When deploying fingerprints for identity and authentication, it's important to only consider solutions that include technologies and the flexibility required to mitigate the specific threats in your environment.

First, there are two general considerations that can apply to any deployment. While it's not unique to fingerprints, it is always good practice to ensure that computers and servers in your ecosystem are all running anti-malware software with up-to-date virus definitions. The second key consideration is the use of multifactor authentication policies. Each method of authentication has strengths and weakness, so using more than one by definition will resolve a wider range of threats than any by itself.

A fingerprint is uniquely convenient for multifactor authentication, as it does not require the user to carry or remember anything. People may forget to bring cards or tokens, but they never travel without their fingerprints. In a multifactor authentication deployment, multiple factors need not be present for every logon. Depending on the application, a good strategy is to use a strong "front" door to a system such as a strong, multifactor policy for initial access, but then use a simple, single, convenient factor (such as a fingerprint) for subsequent access once within. This is analogous to a secure perimeter (e.g. the exterior door) but then internal doors are without a key. In the IT world, this is classic ESSO. But recently there has been a shift to transactional authentication, sometimes called "Step Up" authentication. In this model the front door is weak, but then the user is asked to re-authenticate each time they access a service or do a high value transaction. The convenience of a fingerprint is especially

suitable to such transactional authentication (e.g. a password, or especially a OTP is very inconvenient if one needs to enter it repeatedly, such as a manager override of a cash register or at a nurses workstation).

Multifactor policies may also be determined by user location. For example, distinct policies could be created for instances when authorized users are inside or outside a corporate firewall. Policies can also be dynamically based on the capabilities of the specific endpoint, which is a particularly useful approach for businesses with large populations of BYOD devices.

Specific Threat: Producing and Using a Fake Finger

A fingerprint is not a secret and people leave parts of their fingerprint patterns wherever they touch. Though difficult and time consuming, it is possible to create a mold of this pattern. Of course, some fingerprint readers incorporate mechanisms that attempt to detect when a fake finger is being placed on the reader. Some readers may detect static electrical properties, others static visual or spectral properties.

Randomization safeguards against fake finger attacks.

On a given reader, some forging materials will work, other materials will not. Adding additional mechanisms to detect fake fingers generally add cost, may reduce reliability and offer little long term fundamental improvement since it is simply a matter of one person discovering the next material and method that can work. These mechanisms give a false sense of security since one can never prove that such a material won't eventually be found.

As activity around hacking the iPhone 5S has widely reported, creating fake fingers is a challenging process, which requires specialized skills and equipment.[1] Additionally, one needs the individual target to be within physical proximity and needs to interact with them to be successful. This greatly reduces the threat landscape in comparison to the possibility of compromising a password, which can be accomplished by unauthorized users next door or on the other side of the globe. However, for users who want to mitigate such risk, one option is to have the user enroll multiple fingers. Then, during the authentication process, challenge the user for a specific finger or fingers chosen randomly from the enrolled digits. Randomization safeguards against fake finger attacks, as it will be especially hard for an attacker to lift all fingers and determine which print came from which finger. An authentication solution should allow for such policies and log/alert possible fake finger attempts. No single method is foolproof, but such system level considerations can raise the bar against the use of fake fingers as much as methods which rely on the detection of specific materials.

Security and Integrity of the Fingerprint Matching Process

Effective fingerprint authentication is comprised of several steps — obtaining the fingerprint image from the sensor, extracting features, matching them against encrypted images stored for that user, and declaring a match or no match. Each of these steps needs to be performed with integrity. The fingerprint image should be securely transmitted into the process that executes feature extraction. The enrolled fingerprint templates must be securely bound to the user. The match also must be securely encrypted and conveyed to the process that will use it.

Overall, the security strength of each step needs to be at least as secure — but not necessarily more secure — than the application or OS that will use the result of the authentication. For example, if the system requires a logon to Windows or the entry of passwords into an application, the security of the fingerprint-match process should ensure that this logon or password entry process is not vulnerable to attack. It should not be the weak link in the process.

As fingerprints graduate beyond Windows and into more mission critical applications — such as financial services, payments and native authentication to external services — end-to-end security is necessary to achieve strong compliance and non-repudiation. In these cases, fingerprint processing and cryptographic key management should take place not in the host OS, but instead in secure hardware. Mainstream microprocessors from Intel, ARM, and Broadcom offer such Trusted Execution Environments (TEE) for PCs, mobile and embedded. Fingerprint sensors may also be coupled with a dedicated co-processor for feature extraction and match to ensure the highest protection and ease of integration.

False Accept/False Reject/Failure to Enroll Tradeoffs

The accuracy of fingerprints makes them a strong security credential. Fingerprints are time-tested and proven to be highly unique. However, any single capture of a fingerprint is subject to noise and variation due to environmental conditions and finger placement. This induces the need for a tolerance that can result in a false accept or false reject. For reference, a typical operating point for false accept is 1 in 100k, and false reject of 1%.[2] This means you would need 100k attempts of non-matching prints to have a statistical likelihood of a false positive match. Also, the authentication solution should perform throttling or track failed attempts making it impractical for an attacker to make the necessary repeated attempts. Fingerprints from the same person are largely independent. By enacting an authentication policy requiring multiple fingers to authenticate, the chance of a false accept drops to practically zero.

Unlike consumer applications, where fingerprints are a personal choice and used mostly for convenience, biometrics in business applications should be mandated to derive strong identity and authentication benefits. In businesses, the fingerprint credential must offer a high bar of reliability to work for everyone, each time. This is not possible to achieve using just a single finger. Any single finger may work consistently well for 95% of the population, but that is not “everyone.” Instead of falling back on the use of a password or other non-biometric credential (which will compromise the unique security properties of fingerprints), best practices call for a process that requires some users to authenticate with multiple fingers.

In the same way that multiple fingers can radically reduce the chance of false accepts, using the information content across multiple fingers (most people have 10) can also be used to greatly reduce the probability of failure to match, or false reject. A small percentage of users may be inconvenienced, but deploying this strategy will ensure that fingerprints are usable across the entire population without the added complexity of additional biometrics or maintaining other credentials. Of course, there may be rare exceptions where users refuse to enroll their fingerprints. But, if few in number, these can be administered as one-off exceptions with the appropriate policies and safeguards. When security is the goal, other credentials — such as passwords, tokens or smart cards — and multifactor policies should be introduced not as a fallback for use when the fingerprint doesn’t work, but instead to strengthen security or for use in environments where a fingerprint reader isn’t available at every access point.

Compromise of the Credential Database

In order to use fingerprints to ensure one identity per person — and one person per identity — a central database of fingerprint templates is required. This database is often mentioned as a concern, mostly because biometrics credentials cannot be revoked. If this database is compromised, unlike a password, the user cannot change their fingerprint. This is the very property that makes them so uniquely useful, but is it a risk as well? Unlike other credentials, the crux of ensuring fingerprint security is to make the process secure, not the credential. If the fingerprint credential fraudulently obtained from a database cannot be inserted into the process (through secure hardware or encryption, as noted above) or doing so isn't the weakest link of attack, then it is of no practical use to have it. This makes revocation entirely irrelevant. Furthermore, fingerprint templates necessarily contain a great deal of noise and spurious features mixed in with the real features making it impossible to reconstruct a real fingerprint pattern or a fake finger, from just a fingerprint template.

The crux of ensuring fingerprint security is to make the process secure.

Though it's a minimal risk in most environments, if you have a high-security use case, you may want to consider heightened strategies to protect the fingerprint database. Depending on the goals, approaches may include allowing the user to choose a short PIN, which can be used to transform the fingerprint into a fingerprint template so that an attacker cannot derive which PIN decodes the user's actual template. The user supplies the PIN and the fingerprint template is applied each time the user authenticates. This would protect all users in the online authentication database. A database of raw templates to perform de-duplication, may still be needed to prevent a fingerprint being registered more than once, with two different identities, but such a database can be stored and accessed offline.

Another strategy is to give users the option, upon enrollment, of enrolling their fingerprint template on their mobile phone or through the use of other tokens (smart cards, USB token). This template could be signed with a private key as certification of the enrollment. Subsequent authentication would require users to have their phones or tokens. In some cases, the fingerprint match would be performed in the secure element of the token.

A Fingerprint-Centric Multifactor Authentication Platform

It is clear that no piece of hardware, no single configuration and no one credential is a magic bullet when it comes to security. A flexible, easy to manage software platform is desirable to unite these elements and address specific threats and a full range of risks for an enterprise. Successfully deploying fingerprints to elevate security, compliance and identity fraud in an enterprise setting is far different than using biometrics-based identification in consumer or government applications. One cannot simply treat a fingerprint like any other credential in a multifactor solution. To optimize security, enterprises and governments must deploy fingerprint authentication systems that support multiple factors, which can be used to create a highly effective multi-layered solution.

TO LEARN MORE

For more information, visit www.crossmatch.com or contact us at:

- In North America, call: +1 561 622 1650
- In EMEA, call: +44 1189 654001
- In Asia, call: +886 2 2735 5586

About Crossmatch®

Crossmatch helps organizations solve their identity management challenges through biometrics. Our enrollment and authentication solutions are trusted to create, validate and manage identities for a wide range of government, law enforcement, financial institution, retail and commercial applications. Our solutions are designed using proven biometric technologies, flexible enrollment and strong multi-factor authentication software, and deep industry expertise. We offer an experienced professional services capability to assess, design, implement and optimize our identity management solutions for a customer's individual challenges. Our products and solutions are utilized by over 200 million people in more than 80 countries.

Learn more at www.crossmatch.com

REFERENCES
1. Pogue's Post, September 2013
2. Biometric Accuracy Standards NIST Presentation, June 2014

Crossmatch
3950 RCA Boulevard
Palm Beach Gardens, FL 33410
USA
Tel: +1 561.622.1650
Fax: +1 561.622.9938
www.crossmatch.com

CROSSMATCH®

20141014