WHITE PAPER

Protecting Against Criminal Use of Stolen Biometric Data

Major news sources reported in mid-2015 that 21.5 million people were affected by a breach of U.S. government systems. Identity data gathered over the last 15 years was compromised, including personal information about individuals who were part of government employee background checks. Unfortunately, even the best risk-based, multi-layered breach defense is imperfect, and incidents like this are inevitable. For this reason, there must be greater focus on controlling what happens after the breach, including ensuring that stolen identities are unusable by anyone but their legitimate owners.

Ensuring Biometric Data is Useless to Identity Thieves

Biometrics is the only authentication method that binds a myriad of digital and physical credentials to a person. As such, biometrics is playing an important role in eliminating digital identity theft in today's increasingly complex and vulnerable digital environment.

Fingerprint images were among the sensitive information that was stolen in the 2015 U.S. Office of Personnel Management (OPM) breach. Conceivably, this biometric data could be used by the perpetrators to hijack a user's identity and gain fraudulent access to security systems.

It is important to understand that ***biometric characteristics are not secrets***. For example, our facial characteristics are quite public — not only observable, but also generally associated with our names and other personal information. In the OPM example, now that fingerprints have been stolen from government databases and can never be taken back, the key question becomes what can or should be done to render this information useless to any would-be impostor? Given the premise that databases are inherently vulnerable to attack, the challenge is one of minimizing negative impacts of a breach on individuals and organizations.

As always, the answer depends on the use case, and each category of applications must be examined individually and its associated threats assessed. In this complex and interconnected digital world, systems must be thoughtfully designed and deployed in order to protect user identities and ensure appropriate levels of security within the context of the application.

In the case of biometric data that is already "in the wild" (such as that stolen from the OPM), numerous tactics and best practices should be considered in order to render identities useless to anyone but the legitimate owner. Of critical importance is the ability to detect fraudulent attempts to use biometric data. ***Liveness detection*** — the real-time determination that the biometric characteristics presented are genuine and not fake — is a highly effective design feature in solutions where users physically interact with authentication systems.

Augmenting biometric liveness detection with other security layers for multi-factor authentication greatly enhances digital security and renders the theft of any one personal data element inconsequential. There are also a number of concepts that combine biometric data and other data elements to create an even more robust digital credential that will ensure that stolen biometric data is insufficient and therefore useless in enabling the fraudulent use of legitimate identities.

Following are the key elements in a strategy that extends beyond breach defense to include tactics for neutralizing the effects of an identity breach after it has happened.

Improving Liveness Detection

The most effective liveness detection approach for fingerprint biometrics uses Lumidigm® multispectral imaging technology, which virtually eliminates the possibility of counterfeit fingerprints being used for authentication. The technology is used to compare the complex optical characteristics of the material being presented against known characteristics of living skin. This unique capability, in addition to the collection of unique fingerprint characteristics from both the surface and subsurface of the finger, results in superior and reliable matching performance paired with the exceptional ability to detect whether the finger is alive or not. Multispectral imaging sensors are different from competitive offerings in that they:

- Use multiple sources and types of light along with advanced polarization techniques to capture information from the surface and subsurface of the finger — all the way down to capillary beds and other sub-dermal structures;
- Utilize advanced machine learning algorithms that can be updated in the field as new threats and spoofs are identified, enabling the sensors to very quickly respond and adapt to new vulnerabilities.

Multi-Factor and Multi-Modal Authentication

For strong and reliable user authentication, organizations should consider, where practical, multi-factor and even multi-modal authentication. Today's authentication technologies enable solutions that can enhance security while replacing passwords and improving convenience in a seamless way that is non-intrusive to the legitimate user.

For example, personal devices like smartphones, wearables, RFID cards and other intelligent personal devices can all generally be used as factors of authentication. Regardless of which additional authentication factor is presented by the user, when it is intelligently combined with the biometric data associated with the identity claim, it is possible to quickly determine a definitive "yes" or "no". Strong authentication by means of two or more factors (with one being a biometric) is fundamentally more secure than outdated username/password alternatives.

When identity is firmly established, the use of mobile devices in authentication solutions offers the opportunity for greater personalization and a seamless experience for legitimate users. Information systems can be tailored to each user's need, resulting in enhanced, individualized security, allowing individuals to fully control their real identity. Instead of the system blocking the legitimate user — an unintended consequence of blocking an attacker — the system is made more secure and efficient and thus returns a higher ROI for both the consumer and system administrator.

More Robust Biometric Templates

It may be desirable in some application-dependent situations to construct and enforce the use of enhanced biometric templates. The use of a "super template" that uniquely combines biometric data with other information — perhaps even an OTP or other out-of-band data — enables the system to recognize and reject a biometric template that was created from a stolen fingerprint image. Templates can reside on a card or chip or in a smartphone or personal wearable.

In the case of a government or civil application, this approach would prevent any would-be attacker from simply using the stolen biometric data, alone, to compromise either physical or data security.

In the case of commercial markets (e.g., a banking application), we might see an institution deploying a similar approach to protect user identity during online transactions. As some do today, institutions could enable multi-factor authentication and require that both the biometric and some

other data be provided. Alternatively, they could enroll biometric data and then "sign and encrypt" the template with unique or closed-system data.

The creation of a guaranteed unique "super template" might combine standard (interoperable) and proprietary data. This is the approach that HID Global takes with its Secure Identity Object™ (SIO), which is a data model for storing and transporting identity information in a single object. SIOs can be deployed in any number of form factors including contactless and contact smart cards, smartphones and USB tokens, and ensure that any of these items and the data associated with them are, in turn, only associated with the owner's identity. The SIO is digitally signed using proven cryptographic techniques as part of a seamless and secure process. Various data objects can be added, encrypted, and signed, i.e., biometric data, as well as data for computer log-on and other secure identity applications. Then, all content is secured with a wrapper and bound to the device with another signature.

Identity Proofing

Lastly, it's important to remember that the chain of trust is only as strong as the weakest link. The biometric solution used in identity-proofing must interoperate with trusted devices at each verification point. An example of this approach is HID Global's Seos™-based solutions, which create a device-independent, ***trusted*** physical identity verification process. Additionally, the physical devices themselves must be tamper-resistant to ensure that all transaction integrity is preserved. The HID Global Lumidigm biometric authenticator is a good example of this approach:

- Trusted devices must be encryption-enabled with various tamper resistance and detection capabilities that protect the integrity of the communication between the client and the sensor.
- The chain of trust must be preserved end-to-end if the goal is, for example, to simplify financial transactions for users while eliminating fraud for financial institutions.
- The end-point device must connect to the institution's systems through a cryptographically secure channel protected by hardware tamper detection and response, which establishes trust between the device and the institution's systems independent of intermediate systems and networks.
- A trusted biometric device must be able to perform a live scan of a finger with strong liveness detection to ensure that the person making the transaction is who they claim to be (that is, the same person that enrolled their biometric fingerprint).

And finally, by extension, if a card, smartphone, PIN, or other authentication factor is used for authentication, each must also be confirmed by a biometric — a biometric that is associated with a specific individual through a robust identity-proofing process at enrollment. This ensures that true identity verification has been performed and maintained in a trusted manner.

Moving Forward

Biometrics solutions offer the ideal balance of convenience and security because they are simple to use and increasingly more robust and reliable. Biometrics is also the only authentication method that "binds" a user's digital credentials to a person. As such, biometrics is playing an important role in eliminating digital identity theft in today's increasingly complex and vulnerable environment.

Making security more robust and reliable without adding complexity is difficult. But as our networks become more available and open to attacks, we simply have to find a way to enhance both trust and user convenience. Combining the universality and sophistication of biometrics with things we have (like personal devices, phones, wearables, etc.) and things we know (like PINs or passwords)

is one important step. The other is to rely on vendor technologies and solutions that can effectively guarantee a high level of trust without raising the complexity for the user.

Regretfully, we need to accept the fact that biometrics or other personal data cannot be completely protected from a breach. All we can do is design systems that preserve the integrity of users' true identities — even in situations like the OPM data breach. And perhaps the best way to discourage any future breaches is to simply render the stolen data useless to anyone except the legitimate owner.

2015-12-21-hid-biometrics-stolen-biometric-data-wp-en PLT-02691