The theft and cracking of bulk password databases has impacted nearly every digital user worldwide. With centralized biometric template databases now popping up, will these undergo a similar fate?

Many prominent cyber attacks of recent years including incidents targeting the Office of Personnel Management, Anthem and Target can be traced back to credential exposure. Look at the numbers: According to the Verizon 2017 DBIR (Data Breach Investigations Report), **81 percent** of hacking-related breaches resulted from stolen or weak passwords, an **18 percent increase** over 2016. In many cases, the attack was directed at a privileged user like a system administrator.

Other noteworthy data theft incidents linked to credential exposure include:

- October 2016 attack on Uber, exposing email addresses and phone numbers of around **57 million** Uber customers and drivers worldwide; plus **600,000** driver's license numbers.
- December 2017 discovery by 4iQ security researchers of a single **41-gigabyte database** containing **1.4 billion clear text credentials** — the largest aggregate database of username and password combinations found on the dark web to date.
- 2012 theft of **6.5 million encrypted LinkedIn passwords** which were then posted to a Russian crime forum, followed by the May 2016 discovery of of a Russian hacker selling **117 million email and password combinations** on a dark web marketplace.

The relative ease with which hackers can steal usernames and passwords is made even worse with the ready availability of password cracking software, many of which are free or low cost. While legitimate network security administrators may use this software as a last-ditch effort to save users from needing to reinstall their operating system, hackers can just as easily use them for malicious purposes.

Multifactor authentication and biometrics take data security to the next level

To keep ahead of hackers, leading companies are moving toward multifactor authentication (MFA), which uses a combination of factors including what you know, such as passwords; what you have, like a token device or RFID card; and what you are, represented by fingerprints or other physical attributes.

Biometrics are increasingly popular because they are personal identifiers that are unique to an individual. Plus, they are convenient and impossible to forget. You are your biometric. Biometrics – whether it is face, fingerprint, iris – are stored as a mathmatical representations in templates. Many are stored just locally on your personal device, but other are stored in bulk databases. Sound familiar?

With the anticipated global market of **2.5 billion users with nearly 4.8 billion biometric devices by 2020**, organizations need to get busy thinking about the security of biometric databases – lest they also become easy pickings for hackers. If a user's biometric data is stolen, can it be reverse engineered to create a gel finger or a fake face to perform a presentation spoof? The classic question you hear users asking is, if my biometric template is stolen how do I grow a new finger or face?

Biometric tokenization, where history does NOT repeat itself

Fortunately, some smart people are at work on this. Biometric tokenization is a process of substituting a stored biometric template with a non-sensitive equivalent, called a token, that lacks extrinsic or exploitable meaning or value. That means that a stolen template cannot be reversed back to a fingerprint. It also means that it is not linkable, so two bulk biometric template databases cannot be crashed together and compared – like a "pass the hash" attack on a password database – to determine if a user is a member of one or both.

Today's forward-thinking organizations are implementing ever more innovative ways to thwart data theft. Security solution companies like Crossmatch integrate MFA, biometrics and tokenization as part of our approach.