As hacking grows, biometric security gains momentum

March 7 2015, by Rob Lever

With hackers seemingly running rampant online and millions of users compromised, efforts for stronger online identity protection—mainly using biometrics—are gaining momentum

With hackers seemingly running rampant online and millions of users compromised, efforts for stronger online identity protection—mainly using biometrics—are gaining momentum.

Biometrics, which can include fingerprints, iris scans, facial or voice

recognition and other methods, got a major boost with Apple's introduction of its iPhones with Touch ID.

Samsung followed with its own fingerprint scanner and Qualcomm recently unveiled its 3D fingerprint technology incorporated in the chips used in many mobile devices.

From major tech firms such as Google, Microsoft and Yahoo to US cybersecurity officials, consensus is growing that the simple password, often the weak link in security breaches, needs to be replaced.

'Kill the password dead'

"I would love to kill the password dead as a primary security method because it's terrible," White House cybersecurity coordinator Michael Daniel told a security forum last year.

Tens of millions of passwords have been stolen in breaches of major retailers and banks including Target, Home Depot and JPMorgan Chase. Password theft is a key element in identity theft, the biggest source of fraud complaints in the United States.

And a survey of large corporations using mobile commerce by RSA and TeleSign found around three percent of revenue lost due to fraud.

Biometrics are likely to be a major part of any new identity verification effort, says Ramesh Kesanupalli, vice president of the standard-setting Fast IDentity Online Alliance (FIDO) which now has over 170 members including makers of hardware, software and financial firms.

Kesanupalli said that even solutions that add verification on top of a password are not as robust as biometrics.

"If you don't eliminate dependency on the password you're not solving the problem, you are only treating the symptom," Kesanupalli told AFP.

Fingerprint ID, facial recognition

He says fingerprint identification made major strides with the iPhone, and that other technologies such as facial recognition are still being improved.

Biometrics, which can include fingerprints, iris scans, facial or voice recognition and other methods, got a major boost with Apple's introduction of its iPhones with Touch ID

Apple, in a "master stroke," used a fingerprint ID on the home button which is already used to activate the phone, said Kesanupalli. That

means consumers don't need encouragement or special training to use it.

Additionally, e-commerce firms can piggyback onto the phone's authentication to allow for a more secure transaction without passwords, Kesanupalli said.

And significantly, the Apple fingerprint is stored only on the device, so there is no database to be hacked.

Another important development was Microsoft's announcement in February that it was joining FIDO and implementing new authentication methods in Windows 10 that will include biometrics.

"Moving the world away from passwords is an enormous task, and FIDO will succeed where others have failed," said Microsoft program manager Dustin Ingalls.

International Data Corp says some 15 percent of mobile devices will be accessed with biometrics in 2015, and the number will grow to 50 percent by 2020.

Yahoo, for one, is developing new security that will eliminate passwords, according to its chief information security officer Alex Stamos.

"We strongly believe at Yahoo that we need to get rid of passwords and that users need to move to other ways of communication," Stamos told AFP, noting that new login credentials will be forthcoming.

AcuityMarket Intelligence meanwhile projects that by 2020, global mobile biometric market revenues will reach $33.3 billion including biometrically enabled mobile devices, apps and software for payments.

Biometric fears

Biometrics are likely to be a major part of any new identity verification effort, says Ramesh Kesanupalli, vice president of the standard-setting Fast IDentity Online Alliance (FIDO)

But not everyone in the tech world sees biometrics as the solution to security problems.

"If you have a credit card that gets compromised you can get a new credit card, but what do you do if your iris or your fingerprints get compromised?" says Sascha Meinrath, head of the New America Foundation's X-Lab studying new technologies.

Meinrath noted that there have already been successful efforts to fake

someone's fingerprint, and that other biometrics may also see the same fate.

"This presents an entire new realm of security problems," he said.

New technologies are helping make biometrics more secure.

Microsoft chief executive Satya Nadella touts Windows 10 and HoloLens capabilities at a press event in Redmond, Washington on January 21, 2015

Stephanie Schuckers, a Clarkson University professor and head of the industry-academic Center for Identification Technology Research, said some research is focused on "liveness detection," to guard against faking fingerprints or other biometrics.

"This would ensure that the real biometric is there at that time and place, and recognize a fake version of that stolen fingerprint," Schuckers said.

Some of the pressure for new identity verification systems is a response to huge losses hitting the financial sector, said James Lewis, a cybersecurity specialist at the Center for Strategic and International Studies in Washington.

"We don't know what the technology will be," Lewis told AFP.

"Consumers will decide what they like, and we will then see if the bad guys can figure out how to crack it."