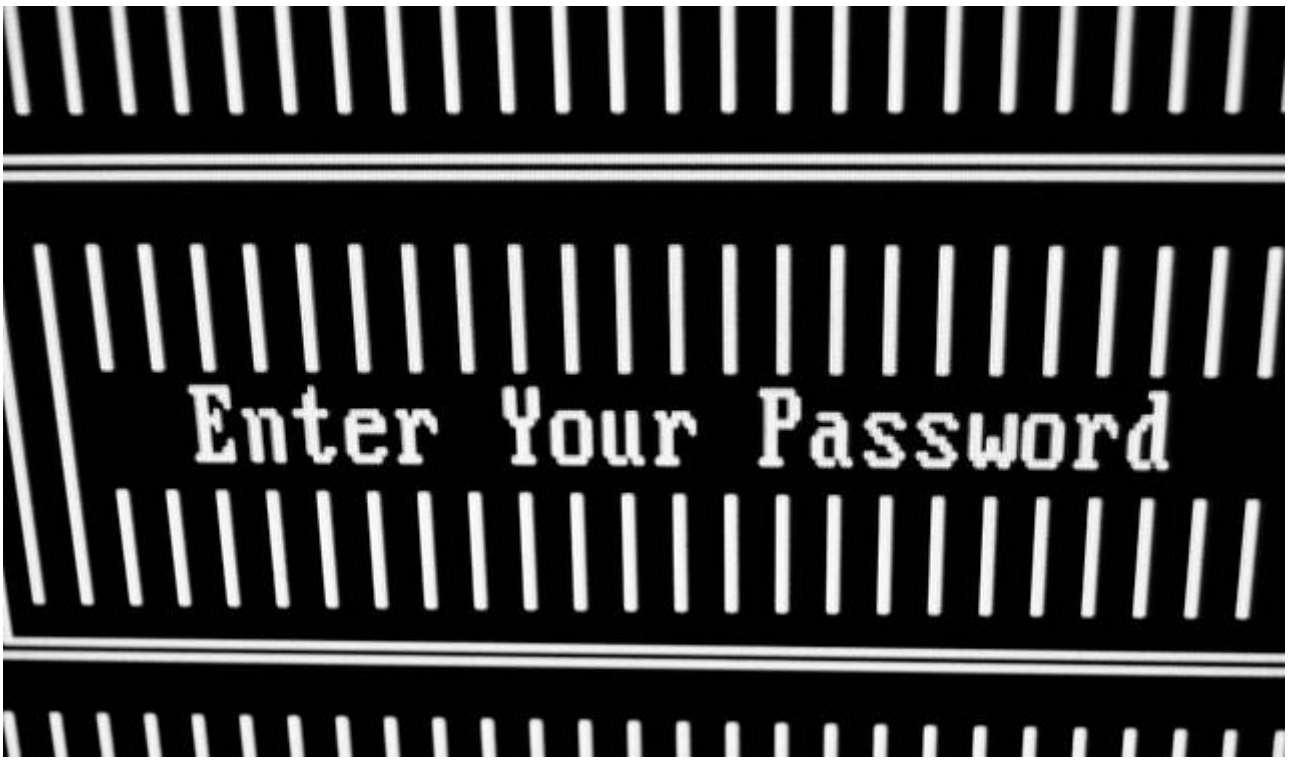
The Fletcher Forum of World Affairs



FEB10

Brainprints: Implications for Security and Civil Liberties

SECURITY, TECHNOLOGY

By **Nayef Al-Rodhan**

In May 1998, a group of hackers called L0pht had a meeting with a panel of senators in Washington to warn them about the many security risks of the Internet. At the time, computer networking was still in its early days but was nevertheless beginning to become popular for commerce and communication. The hacker group foretold some of the problems with internet (in)security, which remains to date a vastly complicated matter. For example, the "WannaCry" ransomware attacks of May 2017, which quickly spread globally, exposed the incredible vulnerability of services and companies reliant on the Internet and internet-based communications.

In the 1990s, the L0pht group discovered an easy way to crack the cryptography for user password protection for Windows, which they deridingly called "kindergarten crypto." At the public hearing in May 1998, one member of the group said that "If you are looking for computer security, then the Internet is not the place to be," adding that the Internet itself could be taken down "by any of the seven individuals seated before you." Offline platforms may seem less exposed and vulnerable than online sites but security and password protection is crucial there too.

We have certainly come a long way since the late 1990s, but security concerns remain a high priority for tech companies, individual users, and government agencies. This applies to online and offline sites. Anything from access to personal photographs stored on a computer to entrance into the Pentagon or nuclear sites relying on passwords is exposed to varying risks of security breaches.

In recent years, following advances across biotechnologies, security companies have started to take identification systems to unconventional realms. This is the result of a growing realization that passwords are weak security systems: a string of letters is hardly theft-proof and it can be hacked within hours. "Security through biology" is indeed a very enticing idea and already with a good but controversial track record. After 2011, police departments across the United States have relied extensively on scanning biometric data, with the help of devices such as Mobile Offender Recognition and Information System (MORIS). Additionally, research on iris scans, voice data, and other systems is fast-developing. Another technology known as "biometrics of intent" (which scans for suspicious behavior and malevolent intent *before* it materializes into action), raises serious concerns in terms of profiling and civil liberties – yet it may be ultimately useful if strict and transparent oversight mechanisms are put into place.

One trend is clear: research into password security is closely looking at biology for better and uniquely reliable security.

Alternatives to passwords: Looking inwards – literally

For a start, the change of paradigm in password security has manifested in a search for *alternatives to passwords*, or to make passwords as one step in a multi-stage authentication system.

However, the best security locks could be within one's own body and mind. The use of fingerprints to unlock devices is already common but these systems are not fail-safe and security companies recognize the need to go a step further. Moreover, the mechanisms to bypass the fingerprint systems are multiplying each year. In 2016, it was reported that the police in Michigan approached a University Professor to help develop a system to unlock criminals' phones, based on prerecorded scans. The solution (which is still in testing) was to recreate 3D printed fingerprints that could then unlock the phones. This is a revealing case: in this instance, it was law enforcement that needed to break a security barrier, but it could well be the case that rogue actors will attempt similar stratagems in the near future.

Other prospective security solutions developed in recent years include heartbeat monitors, voiceprints, face and vein recognition devices, ingestible devices, and finally, "brainprints," which draw on the uniqueness of each human brain's processing of information. Some banks are already starting to rely on voice-recognition technology and have started to slowly phase out passcodes or replace them with individuals' voices.

Another approach is to use the signals and patterns of one's heartbeat to replace passwords. This could be made possible with wearable devices that authenticate identity based on one's unique heartbeat or electrocardiogram (ECG) measurements. The Canadian company Nymi has already put one such device on the market. The product is a bandwhich provides "always-on authentication", promising "to transform the burden of authentication." The HeartID feature uses an individual's unique ECG signals, and the band communicates with the enabled devices via Bluetooth.

Other companies have charted similar territories, in the form of sub-dermal implants of silicon chips or "wearable computer tattoos." These tattoos feature sensors and ECG monitors embedded under the skin, as well as a wireless power coil.

The search for smarter authentication methods is seen as a race against time because the community of hackers, acting alone or on behalf of rogue states, does not lack ingenuity. But bio- and neuro-technologies that can go as far as to process distinct personal signals and use those as identification codes, hail a new era in authentication security. Biometric systems that use the uniquely intimate responses of our bodies, such as heartbeats or brainwaves as security keys are – theoretically – much more difficult to break and a step ahead of the know-how and tools commonly used by hackers today.

Brainprints: making use of the uniqueness of the brain

Our thoughts and reactions to the surrounding world are unique to each and every one of us, in a very profound way. Human neurochemistry shares many baseline features across our species, but there are distinct reactions at the neurochemical and neurocellular levels that are distinct from person to person and cannot be replicated in two individuals. "Uniqueness" is a fundamental selling point of the brainprint technology.

Many studies over the years have demonstrated that "brainprints" – or reading how the brain reacts to certain words or tasks – are unique to each individual simply because each one of us is wired differently and thus thinks differently. In other words, being exposed to an image of a book will not trigger the same reaction in the brains of two people.

Brainwave-based authentication uses sensors to capture electroencephalograms (EEGs) – or the measurement of brain waves. Setting the password takes place by looking at an image while being connected to an electroencephalograph, which record the specific brain activity in response to that stimulus. Next time an attempt is made to unlock the system, the user is exposed to the same image (or stimulus) once again, their reaction is recorded and compared against the record established initially.

The turn to electroencephalography (EEG) came after initial studies using functional magnetic resonance imaging (fMRI), which measures brain activity differently as it tracks changes in blood flow. fMRI is less practical because it involves lying still in the scanning machine for a prolonged period of time. EEG works by applying small electrodes on the brain, which track the brain waves; the EEG machine then amplifies those signals and records the wave patterns. In everyday life, EEG is also impractical as it involves wearing a cap of gel-based electrodes, an option which is hardly convenient. However, alternatives to the typical EEG, such as in the form of wireless devices or standard earphones, could prove to be more convenient and thus more likely to enter everyday use. The team of researchers at UC Berkley who used a low-cost brainwave-reading headset called this authentication method "passthoughts", essentially premised on the same principle as the brainprints.

Absolute protection – ownership, neuroplasticity and hacking

In theory, brainprints could provide high-security sites with unparalleled levels of protection. For instance, a team of researchers at Binghamton University in New York recorded the brain activity of

50 volunteers who had looked at several images and the results showed 100% identification accuracy.

A major problem that has yet to be overcome regards the reliability of brainprints. Neuroplasticity – which refers to the changes in brain connections as a result of experience – means that the response to certain images could well vary and evolve over time. Looking at an image of the Statue of Liberty, for example, can evoke a specific reaction for a certain amount of time, but the reaction could change in time if, for instance, there is a new, different mental association to that image. Would this mean that repeated and frequent updates with EEG will need to be made? Most likely so, but this could be a price worth paying if brainprints could provide unbeatable protection to high-security environments. Even so, there remain open questions of feasibility because the frequency of EEG updates could be quite arbitrary.

Another issue that could arise is that, ironically, one might have "too much" control and ownership over their brainprint, meaning there is no way of passing it on to others, even in cases of emergencies. No other person could understand and have an EEG identical to your own, and thus your brainprint is in your complete ownership, and cannot be transferred or shared with others even if one would want or need to do so.

If the technology is to go full-speed ahead, such conundrums will need to be addressed responsibly and with foresight. No less important is that as soon as the most advanced and reliable of security protocols are in place, there will inevitably be attempts to hijack or break them. Given the unique characteristics of brainprints, it is still hard to anticipate how these attempts will play out, but we must never remain complacent about the creative capacity of those who want to do harm.

Image "ENTER YOUR PASSWORD" Courtesy marc falardeau/CC BY 2.0

About the Author

Professor **Nayef Al-Rodhan** is a Neuroscientist, an Honorary Fellow at St Antony's College, University of Oxford, and Senior Fellow and Head of the Geopolitics and Global Futures Programme at the Geneva Centre for Security Policy. He is also the author of *The Politics of Emerging Strategic Technologies. Implications for Geopolitics, Human Enhancement and Human Destiny* (Basingstoke: Palgrave, 2011). Tweets *@SustainHistory.*