

YOU Are the Password

By Tom Helou

Can a parallel be drawn between freedom to cross the Berlin Wall and the freedom to post on a Facebook wall? Can such borderless liberty be defined in a 140 character Twitter feed or does it require an updated Declaration of Independence? There's no question the proliferation of technology around the globe has opened new portals for expression to those otherwise silenced by their governments and as a means toward equality for the oppressed. Call it Freedom 2.0.

Yet while this expressive new flame flourishes, our collective failure to protect such channels threatens both the integrity and usability of online forums. This year's hacking of RSA's algorithm – the secret instruction manual, if you will, of the leading token's inner-workings – should serve as a warning sign to the international community of cyberspace's next stage of growth. First built as a tool for convenience, the Internet is simply not equipped to ward off today's sophisticated attacks. If this modern marvel is to continue to thrive and serve as a beacon for all things innovative, security must now be our top priority.

The RSA attack was not an isolated event. As the global recession drags on, sensitive information only becomes more valuable - and more vulnerable. Former employees, upset over a recent layoff in these hard economic times, have insider information that can be used to access company networks and obtain corporate data. Depending on how big their axe to grind is, now it's all too easy for the disgruntled former staffers to plaster sensitive intelligence all over the cyber-world.

Corporations are hardly the sole victims. Consumer records can be left uncovered in the process of a breach, and the virtual identities of millions are left for the taking. In 2010 alone, 563 million consumer records – or nearly one per American - were compromised.

Is the problem intractable? It is -- if we continue the same, static approach to fixing it. For a hundred years, humans have secured data primarily through two methods of identification: what you have (house keys, car keys, key fobs) and what you know (the combination to a lock, your Social Security number, your password). These methods typically work in limited and controlled environments. However, with the proliferation of the Internet and the abundance of data sharing sites, such identification tools are hardly secure. Today, the Internet has 2.1 billion users, a number that is increasing at the rate of nearly 1 million per day. Facebook itself would boast the third largest population on Earth if it were an autonomous nation. Ashton Kutcher tells his 4.25 million Twitter followers what he eats every day for breakfast. Our world has moved into a virtual dimension, and as such, security requires an upgrade. In this new environment, we need new security.

First, we must examine what makes an item "secure" through an entirely different lens, moving from simple identification to complete and sophisticated authentication. In addition to what you have and know, network access points must be able to authenticate who you are. Your palm, your face, and your typing pattern are all unique characteristics that cannot be replicated, lost or stolen unlike traditional methods of identification. Instead, you become the key to your data. You become the password. While it may surprise some, these advances are no longer the subject of sci-fi movies and are ready to be applied today. The question is how do we use them?

Must retinal scanners be immediately installed on every computer? Probably not. However, new ways to secure login portals should be considered. More importantly, we all should take the initiative

to become better educated on the state of cybersecurity. As we gain more exposure to cyberspace through e-mail, Facebook and online banking, it becomes easier to trust the security and privacy of such applications. However, it is critical that we resist this temptation and instead remain constantly aware that the information could be intercepted somewhere between send and receive.

Further, this new paradigm of security where users become their passwords is only effective if the concept is ingrained system-wide. If parts of the Internet are left unsecure, we are all still at risk.

As the Internet matures into the primary forum to exchange sensitive information, we will probably enter into a cyber-arms race of sorts – a race not only between private-sector competitors, but also foreign governments and agents (Al Qaeda) who would seek to collapse Freedom 2.0. RSA or Lockheed Martin are just notable examples of the many global businesses continuously under cyber-attack. We didn't choose this ground, but our banks, critical infrastructures, and government agencies now line the battlefield of an iGen Cold War and our traditional ways of fighting the battle are losing the war.

One approach toward solving the dilemma is by using smarter security technologies that focus on the root of the issue, eradicating the ability to use stolen information. An example is AuthenWare, a software-based, strong security solution that protects against identity theft, web fraud and other system intrusions by using behavioral biometrics. It incorporates a breakthrough, multi-dimensional approach toward validating user identity through a series of biometric security algorithms that record and measure how a person uniquely types their credentials.

AuthenWare can distinguish one person from another; ensuring that rightful users are granted access to the appropriate internal, remote or web application, while thieves are not granted access and therefore cannot use the stolen credentials. The user does not need expensive hardware, tokens or certificates – in fact the user doesn't even need to be aware that AuthenWare is there at all. The security algorithms are intelligent so the software learns and adapts to nuances in the user's typing behavior – even those caused by physical injury, medication, stress or fatigue. Behavioral biometrics are not as intrusive as physical biometrics such as fingerprint or face recognition and therefore do not face the same privacy concerns as physical biometrics.

In order to solve this problem, we need to be able to promote and embrace innovation. We will not be able to tackle the increasing cyber security challenges by reacting; retooling traditional biometrics; preventing information from being stolen; or producing new anti-virus technologies. We need to get in front of the issue and be pro-active.

We collectively need to think out of the box, be creative, innovate and realize that the solution will come only if we can implement it on every computer or device in every corner of the planet. Another option would be finding a way to transform the user into the security device. We need to do that without compromising the privacy of the user, without impacting usability and at the same time increasing security.

During the last 20 years, the U.S. has been the leader in new patents world-wide and we have led the high-tech industry with companies, such as Oracle, EMC, HP, IBM, Apple just to name few. We know how to create state-of-the-art products; we know how to solve problems, but unfortunately sometimes we are slow to adopt some of these technologies.

Keystroke Dynamics, a behavioral biometric, is a good example of an innovative cyber security solution. This technology could be a phenomenal solution to our cyber security threats; we have

created this technology, we are exporting this technology to other countries, our analysts are talking about this technology, yet the U.S. is lagging foreign countries by not adopting or at least analyzing it for protecting our cyber-boarders or for providing Freedom 2.0 to our citizens.

But the responsibility for IT security extends beyond the private sector. Public agencies and officials must also become active participants in the battle against cyber-extortion, establishing an environment where IT security is valued and cybercrimes that threaten corporate development or individual identities are treated with severity. Public agencies must adopt the “unconventional” methods of security and be leaders not laggards.

Instead we continue to discuss how to improve old technology or how we can prevent online information from being stolen. The web was not created with security in mind, but was created as an efficient form of communication. There are new paradigms that we should be discussing for leading the war against cyber-terrorism. Innovation should be the driving factor in our discussions. If we don't innovate and adopt cutting edge security solutions, we are going to be left behind.

We must face opponents as one united front – with both private and public sectors aligned. The online universe is successfully tearing down the walls that have, until now, separated and confined vast populations of the globe. Yet in its openness, danger lies. Too much money, too much proprietary information, and indeed, too many freedoms hinge on too little security. The Internet is moving forward. Will we?

** Tom Helou, a frequent lecturer on information technology and cybersecurity policy, is the president and COO of [AuthenWare](#).*