Passwords are dead

Alternative authentication methods

Michael Bachmann
Department of Criminal Justice
Texas Christian University
Fort Worth, TX USA
m.bachmann@tcu.edu

***Abstract*—The idea of protecting information has been around for many centuries. Modern computers use a system of authentication to protect the machine from unauthorized access. One of the greatest challenges today is that the average user has about 40 personal and professional accounts that rely on user names and passwords for authentication. These logins are rarely unique, hardly ever changed, oftentimes simplistic, and rely on insecure "security questions" fallback options because they are regularly forgotten and reset [1]. The past few years have seen a dramatic increase in the number of data breaches of major corporations and government agencies and that number only continues to grow. These significant breaches make it now more important than ever to find some new ways to access private data. In order for us to stay safe and secure online, we must look at emerging technologies to conceptualize the future of login authentication. From biometrics to sound-based passwords to electronic tattoos and ingestible pills, the future holds numerous ways for us to interact with our machines in a safer and more efficient manner than ever before.**

Keywords—user authentication, password, web security, 2-step authentication, one-time password

I. PASSWORD ALTERNATIVES

Researchers from National Taiwan Ocean University and the Taiwan Institute of Science have proposed authenticating a user without a preset password [2]. Instead of requiring users to remember static login credentials, the one-time authentication scheme is deployed server side and communicated to the client requiring authentication. The authors believe that such on-demand, one-time, and constantly changing password methods will substantially reduce the amount of phishing attacks relying on static credentials. Two promising realizations of preset password methods include Pingrid by Winfrasoft and SlickLogin by Google.

Another, more established password alternative that is gaining popularity is the idea of using biometrics to authenticate users. Users' unique features, such as fingerprint or retina patterns, are translated and saved as digital hashes. Upon login, the submitted pattern is checked against stored hashes, the match quality is scored, and the user is either accepted or rejected. The decision threshold is based on the application and the extensiveness of security requirements. More modern cellphones feature fingerprint sensors, and the popularity of this authentication method is growing despite concerns over privacy issues related to potential theft of stored hashes. Unlike user-generated content, biometric ID patterns are permanent and cannot be reset.

A similar technology that is also building off physical traits is the concept of using cognitive traits for authentication. Researchers at DARPA are examining "keystroke dynamics" to recognize individual users. Features such as a hidden rhythm in keyboard or laptop track pad usage, or even the speed of typical webpage scans, can accurately and securely identify individual users. Users are recognized based on unique usage-pattern traits and are granted access without the requirement to supply any particular login information.

Since the 1990s, researchers have investigated the idea of using visual passwords. The theory behind using images as opposed to text is that pictures are more secure and easier to remember. Image authentication is generally broken down into searchmetric, locimetric, and drawmetric methods [3]. Searchmetric systems involve a user selecting a set of specific images that comprise his or her authentication key. One of the most popular searchmetric systems is known as Pointsec. Locimetric systems rely on a user picking out a set of specific points within an image. Two popular systems that use such authentication methods are VisKey and PicturePassword.

While one-time passwords, biometrics, and visual passwords do not seem implausible, some have proposed more obscure ideas involving electronic tattoos and edible electronic pills to replace the password. Researchers at Motorola's Advanced Technology Team are working on both of those solutions. Motorola recently debuted a stretchable circuit that was placed on her arm. The tattoo was created in cooperation with MC10 Electronics as a form of authentication. Along with the tattoo, Motorola is developing what they call "vitamin authentication." This technology proposes the user swallow a tiny ingestible sensor that doubles as a medical device. The device would be powered by the acid of the stomach and essentially turn the entire body into an authentication token.

REFERENCES

[1] L. Tam, M. Glassman, and M. Vandenwauver, The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, *29*(3), 2010, pp. 233-244.

[2] C. Huang, S. Ma, and K. Chen, Using one-time passwords to prevent password phishing attacks. *Journal Of Network & Computer Applications*, *34*(4), 2011, pp. 1292-1301.doi:10.1016/j.jnca.2011.02.

[3] K. Renaud, and A. De Angeli, Visual passwords: Cure-all or snake-oil?. Communications Of The ACM, 52(12), 2009, pp. 135-140

978-1-4799-6364-5/14 $31.00 © 2014 IEEE
DOI 10.1109/JISIC.2014.67