Name: Shihao Dong, Liang Fang, Naing, Ye Htet,

Two factors Authentication

Do you know how many authenticator we carry everyday? We carry a lot of authenticators like ID, key, phone, computer, credit card and etc. Without these things we can’t do anything for our daily life. Authentications is a kind of process to verify the identity of the users. If the user put the username and password are matching, then the user will be prompted to enter the authentication code. One can only login or access to his or her account if all those data input are match. Currently, there are a lot of authentication methods in the industry, here are three basic types of authentication which are Password Authentication Protocol (PAP), SMS code authentication, Token/Chip and Biometric.

Password Authentication Protocol(PAP) is a kind of authentication which protect our information when going online and this authentication is the most commonly use for website and it asks the user to create the password and store in the server. When the user wants to access to his or her account in the website, the user has to put username and password. So the server checks what the user types in and if the user name is match with the password; if match, the user can access the account. “In password authentication, the user must supply a password for each server, and the administrator must keep track of the name and password for each user, typically on separate servers” (ORACLE 2010). For this authentication, the users are often required to put more than eight characters which are mixing with characters, symbols and numbers. However, this authentication method is the most unsecure way to protect the account information. For example, for the old-schools who don’t realize the importance of creating a complicated password, they will use their birthday or licence plate numbers as the password, which are super unsafe because people who know them can easily guess the password. The ideal way is to create a password that combine with symbols, numbers, letters, and most importantly - long enough. According to a recent research, “instead of using a name or a word, start with a sentence: “I want to run a marathon before I turn 40.” Then take the first letter of each word for your password, and change at least one letter to a symbol: “Iw2r@mb4It40” ”(Birken 2018). Using this method, the users can prevent their account being cracked by hackers.

Biometric authentication is a security processes that based on the unique biological characteristics of an each person like: facial recognition, retina scans, fingerprints, voice recognition, palm prints, and more. This authentication is also known as very useful authentication tool these days because cloning the biological material of human body is really hard and very expensive. “Security experts often differentiate biometric authentication from other types of authentication, such as knowledge-based authentication, which involves passwords or other pieces of information unique to a specific user” (Techopedia 2018). Fingerprint, iris scans and face ID are easier to use than a password, instead of remembering different passwords for different accounts. For the biometric authentication, it only takes a second to access, so that it is more convenient for user to access their accounts. Now days, most of the technological devices like: smartphones and computers has fingerprints and face ID that allow the user to access their devices. Moreover, most of the banks use voice recognition for their customer to access their bank account. Apple also uses voice recognition to authenticate the user in order to use Siri. The major advantages of using biometrics authentication is we do not need to memorize anything just use our face, fingerprint, iris or palm to gain access. Imagine that, each user has different passwords and different accounts, so that we have to memorize these different passwords and sometimes, we will forget or confuse with our password.

Token or chip is a device that the user can store the user’s personal information and that device can use as the personal identification for the user. When the user plugs in the token or chip into a system, the user can access the system or his or her account. “Security tokens come in many different forms, including hardware tokens that contain chips, USB tokens that plug into USB ports, wireless Bluetooth tokens or programmable electronic key fobs, which activate devices remotely (for example, to gain access to a car or apartment building)” (Dragonette 2016). There are a lot of ways to use the token or chip. For example: Some people use tokens or chips for cryptographic keys for cryptocurrency and some use for a bank account to add another layer for security to access their accounts. Using the token or chip for authentication is secure for the user because those kinds of devices are “encrypted and digitally signed. And more so, token based authentication systems work well in a web API environment where most applications are available via their APIs. And so tokens can be used to obtain access to multiple services and applications across domains at once (provided there is some form trust agreement) without worrying about the single domain policy” (LoginRadius 2018). This advice also has disadvantage because it is a physical device and every time the user has to carry this advice. So that it can be lose or stolen that device by someone.

Multi-layered authentication can be more secure by generating a real time passcode, and it also help us to prevent the attack from the hackers to access our own device and online accounts. “It’s pretty clear that plain old passwords are an antiquated form of security and not enough when it comes to keeping our communications, accounts, and sensitive data secure. While we use passwords for nearly everything—from banking and social accounts to email—most of us still aren’t using basic best practices for creating strong passwords, or are failing to use unique passwords for each account. It all adds up to increased vulnerability that’s making it easier than ever for hackers to steal our passwords and information” (Wodehouse 2018). In other words, if the user uses two ways authentication, his or her account will be more secure than traditional authentication that is one layer password and the attackers may not be able to hack or crack the user’s account easily. In these days, people are more and more focusing on doing credential things in their account such as Gmail account, bank account and others social media like Facebook, Whatsapp, Instagram, Twitter, PayPal, Yahoo, Linkedin and etc. Therefore, using the two ways authentication is the best authentication for user who wants to secure his or her account.

Basically, it provides with two steps of verification to access the account, it is also known as 2FA. Without two factors authentication, it only requires username and password to login user’s account; however, with two factors authentication, it provides an additional security layer for users to access. “ Two Factor authentication has been around for some time now, it is a practical way to add further security to the user logon sequence, this is accomplished b requiring a second factor to the username/password sequence” (SecurEnvoy 2018).

Reference

Birken, Emily Guy. “Topics.” *Money Crashers*, [www.moneycrashers.com/create-password-prevent-hacking-phishing/](http://www.moneycrashers.com/create-password-prevent-hacking-phishing/). Accessed 28 May, 2018.

Dragonette, Laura. “Security Token.” *Investopedia*, Investopedia, 25 May 2016, [www.investopedia.com/terms/s/security-token.asp](http://www.investopedia.com/terms/s/security-token.asp). Accessed 28 May, 2018.

Hoffman, Chris. “The Different Forms of Two-Factor Authentication: SMS, Autheticator Apps, and More.” *How-To Geek*, How-To Geek, 8 June 2017, [www.howtogeek.com/232598/5-different-two-step-authentication-methods-to-secure-your-online-accounts/](http://www.howtogeek.com/232598/5-different-two-step-authentication-methods-to-secure-your-online-accounts/). Accessed 28 May, 2018.

“Password-Based Authentication (Sun Directory Server Enterprise Edition 7.0 Reference).” *Lesson: All About Sockets (The Java™ Tutorials > Custom Networking)*, <https://docs.oracle.com/cd/E19424-01/820-4811/gdzeq/index.html>. Accessed 28 May, 2018.

Shinder, Deb. “Understanding and Selecting Authentication Methods.” *TechRepublic*, [www.techrepublic.com/article/understanding-and-selecting-authentication-methods/](http://www.techrepublic.com/article/understanding-and-selecting-authentication-methods/)

Accessed 28 May, 2018.

“Token Based Authentication | Learn SEO Blog.” *Engineering Blog*, [www.loginradius.com/cIAM-basics/token-based-authentication/](http://www.loginradius.com/cIAM-basics/token-based-authentication/). Accessed 28 May, 2018.

“What Is Biometric Authentication? - Definition from Techopedia.” *Techopedia.com,* [www.techopedia.com/definition/29824/biometric-authentication](http://www.techopedia.com/definition/29824/biometric-authentication). Accessed 28 May, 2018.

“Why Use 2FA?” What Is Two Factor Authentication? | SecurEnvoy, [www.securenvoy.com/two-factor-authentication/why-use-two-factor-authentication.shtm](http://www.securenvoy.com/two-factor-authentication/why-use-two-factor-authentication.shtm).

Accessed 28 May, 2018.

Wodehouse, Carey. “Why You Should Use Two-Factor Authentication For Better Mobile Security.” *Hiring* | Upwork, 23 May 2018, [www.upwork.com/hiring/development/two-factor-authentication/](http://www.upwork.com/hiring/development/two-factor-authentication/). Accessed 28 May, 2018.