Securing Access Using Different Types of User Authentication

Ann Funk

East Carolina University

ABSTRACT

Everyone in this day and age interacts with a computer in some form or another. These computers can take the form of ATM's, Gas Pumps, laptops, and even watches. The one thing they all have in common is that they store or access our personal data. In this paper, we will discuss the ways that this data is secured by the use of User Authentication. We will begin by talking a little about the different types of user authentication and how it is used. Giving a little insight into the positives of each method and even giving some information about the challenges of each method allowing the user to decide exactly which method is right for them.

Securing Access Using Different Types of User Authentication

User Authentication is defined as any system that verifies the identity of a user who wishes to access it. In today's world, it is something that almost everyone has dealt with at one time or another. Whether it be to log into a personal computer, typing in a pin code at the ATM machine, or using a badge to enter a building, user authentication is a huge part of our day to day lives. That is why it is important to understand the different types of user authentication that is in use today, and also look to the future to see where user authentication is headed.

One of the oldest and still widely used methods for securing access to our data with user authentication is the combination of the username and password. This is probably the most convenient way for most users to secure their data and they are a very easy concept for most users to understand. This is due in large part to how widespread the usage of this method is. For the user all they need to do is come up with a password that meets the password security criteria laid out by the administrator. These criteria could be very loosely based and allow passwords that only contain letters of the alphabet, or they could be more strict, and make the password be a certain length, include capital letters, characters, numbers, and have the password expire after so many days.

The username and password combination can still have many drawbacks. Most user's will pick out passwords that are easy to remember. These simple passwords are usually found in the dictionary, making them much easier for hackers to guess or brute force their way through. When stricter criteria are used for passwords it creates other issues. While the password itself is more secure, these stricter criteria makes it much harder for the user to remember the password they have chosen. This makes it more likely that the user will write down the password onto a

piece of paper so they won't forget it. Once this is done, anyone with access to the paper now has access to the password and the users accounts.

There are even more issues with just using the username and password combination. Passwords can be easily stolen. This can be done by monitoring keyboard keystrokes with a keylogger, sniffed out through network traffic, shoulder surfing, or even through social engineering. A great deal of users will use the same username and password for multiple accounts or systems. This can create a huge security risk and compromise any account that the username/password is attached to.

When looking at all the different ways to keep a system safe the username and password authentication method is one of the cheapest to deploy. Even though it is the cheapest to deploy it doesn't mean the costs won't go up in the long run. If you look at all the potential flaws in this system you can see it can create real havoc on the administrative end. This cans cause the administrative costs to skyrocket and with rising cost come research and implementation into other methods that will keep the cost of ownership down.

One-Time password system is another user authentication system that is in use today. "One of the authentication mechanisms to withstand many of the traditional textual password security issues is the One-Time Password (OTP). The nature of this technique makes it appropriate to secure various financial services and online payments." (Alsaiari, 2016) Unlike the username and password system, where the user is required to use a reusable password, the one-time password system requires the user to use a new password every time authentication is required. Once this password is used it is no longer valid and cannot be used again. There are a couple of different ways that these one-time passwords can be created. One way is by using a password list and another is by using the password token.

When using the password list method of a one-time password system, a list of passwords is generated that will allow a user to use each password on the list once. Once a password is used it becomes invalid and the user will not be able to use it again. Once all passwords are used another list must be generated for the user. These lists are usually distributed in paper form where the user can carry them around at will. This can sometimes become a hassle for the user as they will need to mark off the passwords as they use them. If for some reason this doesn't happen, the user may not be able to get into the system. Creating these lists can also become a burden administratively. The reason for this is the fact that the lists must be generated, distributed and managed by the users.

Password token systems are the most popular one-time password system. With the password token system passwords are generated by either software or hardware that is synchronized with an authenticating server. Each user account is bound to a token during token initialization, and a new password is generated intermittently. Since the token is synchronized with the authenticating server only the software knows which password is valid for the user at the moment the user logs on. Since only the software knows the password and the fact that the password changes periodically this method is great for granting temporary access to a system. However, there are a few drawbacks to this system. Most users who must use a token system find them to be very inconvenient. Most feel that the hassle of keeping up with a piece of hardware or adding another step to sign in just takes too long and is way too much work.

If you are needing to have a stronger way to authenticate users than the ones provided above, you might consider using a method where you provide your user with hardware tokens. These hardware tokens contain the user's identity and a pin creating a two-factor authentication method. This hardware is known as a smart card system. Smart cards closely resemble the size

and shape of a credit card and can even be stored in a wallet. In order to use a smart card, the user will need to have access to a card reader on the computer he wishes to access and then simply insert his card into said reader. Once his card has been inserted into the reader he will then be prompted for a pin that will allow him to access the stored credentials and start the authentication process.

There are two different options when dealing with smart cards. Ones of those options is that of memory. With the memory option, data is simple stored on the card and be viewed as a small floppy disk with security. With this type of card, the user will need to provide a correct PIN before the card will provide the user with the correct password. This password can then be used to log into the system. This type of system can be quite popular for providing two-factor authentication since they store the user's password securely and are quite cost effective. Another option when dealing with smart cards is the microprocessor option. With this option, public key certificates and private keys are stored in the chip on the card. They are then able to be used on either a system that uses the public key infrastructure, a system that uses digital certificates, certification authority systems, or any other registration authority. "The chip also processes information during authentication so that security-critical computations for authentication are restricted to the smart card, making identity interception very difficult and preventing masquerading and data manipulation." (Whyne, 2016) The microprocessor option has a few advantages. They are able to commit extra processing power to other applications that have nothing to do with authentication. For a business, this can be great at reducing costs since they will be able to reduce the number of devices by supplying one card that carries out multiple functions. "Due to the low cost, the portability, and the efficiency and the cryptographic

capacity, smart cards have been widely adopted in many E-commerce applications, network security protocols and also remote authentication schemes." (Chien, 2002)

Smart cards can also be setup to perform more functions for user authentication. For example, they can be set up to lock after a certain number of failed log in attempts. This can help prevent hackers from brute forcing their way in if they get ahold of the device. These cards are also considered to have tamper-resistant storage. This storage helps protect the any private information that is programmed into the card. This information can be the user's private keys, personal information or information related to work.

While the smart card system has many positive attributes, there are also some drawbacks to the system as well. The smart card system can be very difficult to deploy, much more so than a simple password. There are many parts, like a PKI, that need to be in place for the system to work. Management of the cards can also be a bit of a hassle. Users will need to be educated on the use of the cards, how the cards actually work, and be assigned a PIN in order to use the card. Not only do these things need to be done but each card needs to be tracked and issued to its user. These cards can also be viewed by users as inconvenient since they need to be kept close and can be lost or stolen. Some users also have problems with remembering the PINs and if the they enter the PIN wrong to many times, they can lock themselves out of the system.

One of the last user authentication methods that we will be discussing is that of biometrics. "Biometric systems recognize individuals based on their anatomical traits (fingerprint, face, palmprint, iris, voice) or behavioral traits (signature, gait). Because such traits are physically linked to the use." (Jain, 2012) Most of the systems that use these kinds of traits include the following:

- **Fingerprint Scan:** "This biometric system's strengths are its acceptance, convenience, reliability, and price; however, it is one of the easiest physiologically based biometrics to defeat." (Whyne, 2016)
- **Facial Recognition:** "This biometric system is most suitable for identification scenarios in non-cooperative settings, such as large venues, airports, and so on. The technology has not developed the accuracy required for authenticating a user." (Whyne, 2016)
- **Retinal Scan/Iris Scan:** "This biometric system is more intrusive than other methods. Health information about the user can be revealed during the scanning process and diseases of the eye can alter the results over time. This system is most often found in high-security access-control settings because it yields extremely good results but is expensive to deploy." (Whyne, 2016)
- **Hand Geometry:** "This biometric system requires fewer data points to yield good authentication results; therefore, the storage space requirements are smaller than other biometric authentication procedures, speeding up retrieval time. However, the False Match Rate (FMR) is relatively high because hands are less unique than fingerprints, for example, and there is also the possibility of hand deformation." (Whyne, 2016)

The first thing that must be done when using a biometric authentication system is the enrollment of the user and their particular physiological and/or behavioral patterns. From this information, a user profile is created and this profile is then used by the system to identify the user. Once the user is in the system, they can then access the system using the type of biometric identification required, the system will then check the stored profile and compare the stored information to what the user is presenting. If there is a match the user is granted access to the system, if not they are rejected.

While a biometric system can be very secure, there are a few drawbacks to the system as well. When using biometrics, there can be limitations of the sensors, algorithms, user actions, the environment. Maybe the user needs to use a hand scanner but has injured his hand in some way. Maybe they have broken it and are using a cast or they have cut their finger and are wearing a band aid. In either case, the user will be unable to have their hand scanned by the system and will be unable to get authentication. Another drawback is that of convenience. Some users experience longer wait times due to the system rejecting their legitimate credentials. This is known as a false non-match and can cause users to become frustrated fairly quickly, especially when this happens several times in a row. Deployment of a biometric system can also cause companies a lot of headache, especially in large businesses. Since every user needs to be enrolled, there needs to be a system in place that can import the system and their traits into the system. The more people that have to be enrolled into the system make it more likely to have two people who have similar characteristics. This can cause the fail rate of enrollment to increase exponentially.

In this paper, we have talked about many of the different types of user authentication methods. We covered the simple method of just using a username and password, up to a more advanced method of using a biometric system. All of these systems have good things and bad things about them, especially when used alone. However, if used in combination they could provide a much more secure environment for any computer user.

References

*Alsaiari, H., Papadaki, M., Dowland, P., & Furnell, S. (2016). Graphical one-time password (GOTPass): A usability evaluation. *Information Security Journal: A Global Perspective, 25*(1-3), 94-108. doi:10.1080/19393555.2016.1179374

*Chien, H., Jan, J., & Tseng, Y. (2002). An efficient and practical solution to remote authentication: Smart card. *Computers & Security, 21*(4), 372-375. doi:10.1016/S0167-4048(02)00415-7

Fathy, M. E., Patel, V. M., Yeh, T., Zhang, Y., Chellappa, R., & Davis, L. S. (2014). Screen-based active user authentication. *Pattern Recognition Letters, 42*(1), 122-127. doi:10.1016/j.patrec.2014.02.007

* Jain, A. K., & Nandakumar, K. (2012). Biometric authentication: System security and user privacy. *Computer, 45*(11), 87-92. doi:10.1109/MC.2012.364

Kumari, S., Khan, M. K., & Li, X. (2014). An improved remote user authentication scheme with key agreement. *Computers and Electrical Engineering, 40*(6), 1997-2012. doi:10.1016/j.compeleceng.2014.05.007

Prasetio, B. H., Nurwarsito, H., & Kurniawan, W. (2014). One-time password implementation on lego mindstorms NXT. *Telkomnika, 12*(3), 689. doi:10.12928/v12i3.92

Torres, J., Izquierdo, A., & Sierra, J. M. (2007). Advances in network smart cards authentication. *Computer Networks, 51*(9), 2249-2261. doi:10.1016/j.comnet.2007.01.010

Vielhauer, C. (2005;2006;). *Biometric user authentication for IT security: From fundamentals to handwriting* (1st ed.). New York: Springer. doi:10.1007/0-387-28094-4

Wang, D., Wang, N., Wang, P., & Qing, S. (2015). Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity. *Information*

Sciences, 321, 162-178. doi:10.1016/j.ins.2015.03.070

Whyne, J. (n.d.). Secure User Authentication for the Next-Generation Secure ... Retrieved November 15, 2016, from www.microsoft.com/resources/ngscb/documents/ngscb_authentication.doc