International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Multifactor Authentication Techniques with Computer Hardware

Vijeet H. Meshram*[1], Dr. Ashish B. Sasankar[2]

*[1]Research Scholar, Department of Electronics and Computer Science,RTMNU, Nagpur University, Nagpur, Maharashtra, India

[2] G. H. Raisoni College of Information Technology,Nagpur Hingna, Nagpur , Maharashtra, India

ABSTRACT

For quite a long time, the password has been the standard means for user authentication on computers. In any case, as clients are required to recollect more, longer, and evolving passwords, it is apparent that a more helpful and secure answer for client verification is vital. This paper analyzes different authenticators and thinks about these authenticators and their blends. We examine effectiveness against several attacks and suitability for particular security specifications such as compromise detection and non-repudiation. The paper attempts to offer a more blended multifactor authentication technique by introducing computer hardware in the process.

Keywords : Multifactor Authentication, Security tokens, Soft tokens, Mobile Authentication

I. INTRODUCTION

1. Multi-Factor Authentication Concept

In an authentication system, multi-factor implies that there is more than one of the components of verifications being utilized. Multi-factor authentication consists of verifying and validating the authenticity of an identifier using more than one validation mechanism. Authentication factors apply for a special system of verifying a client as the person who is completely allowed get the rights. There are different factor types for authentication: [1]

- Human factors are inherently bound to the individual as for example visible features.
- Personal factors are otherwise physically or mentally allocated to the individual as for example remembered code numbers.
- Technical factors are bound to physical means as for example a pass, an ID card or a token.

Each of the types may apply independently for demanding access according to given guidelines and techniques. The introducing of a factor demonstrates consistence with access to rules and in this way must be affected in a predetermined procedure. In two factor authentication a minimum of two factors compliance is required. [1]

Multi-Factor Authentication provides additional account protection against various forms of online fraud. By adopting the multi-factor authentication, the possibilities of attacks are reduced. The authentication becomes more precise and secure.

An example of multi-factor authentication at the new accounts desk would include performing the following:

Credential validation - The ability to read and validate information encoded within the magnetic stripe and barcodes of government issued identification.

Identity screening - A system to perform positive and logical verification of furnished customer data.

Fraud detection - Comparing customer information to negative files, both internal and external from across industries, which represents known and/or attempted frauds.

One of the motivations of using MFA is to improve the single factor based Authenticated Key Exchange (AKE) by combining two or even more factors in one system . These MFA approaches are based on a single factor and in recent times, MFA has come forward as an active research topic. However, extra caution should be taken as current approaches to MFA are expensive and difficult to deploy.

Integrating the credit card payment system with biometrics in MFA has given support for more efficient verification. This method proposes to employ fingerprint verification with a credit card in a MFA. Doing this would need the installation of additional equipment that would increase the cost. Employing biometrics when using a credit card in authentication as a MFA procedure is another access control approach. This system approaches time that affects the user acceptability for the system and using fingerprint authentication comes at low to medium cost with a medium level of accuracy.

The card reader is an additional level of HW security that can use a One Time Password OTP. The chip on the client user card generates the OTP, with the caveat that the account

Multi-factor authentication has been widely used by more and more people and organizations recently. It is especially popular with Internet business. Compliance acts are also another reason for its growing usage. Multi-factor authentication is going to become the standard method of authentication in the future.

1.1 Multifactor Authentication Technologies

a. Security Tokens

A security token is a small hardware device that the user carries to authorize access to a network service. The device may be in the form of a smart card or it may be embedded in a commonly used object such as a key fob. Security tokens or hardware tokens provide an additional level of security through a strategy, which is known as two-factor authentication: the user has a personal identification number (PIN), which authorizes them as the owner of that particular device; the device then displays a number which uniquely identifies the user to the service, allowing them to log in.

b. Soft Tokens

A soft token is a software-based security token that generates a one time login PIN. Traditionally, a security token has been a hardware device that produces a new, secure and individual PIN for each use and displays it on a built-in LCD display. The system may get activated after the user presses a button or enters an initial PIN. Security tokens are generally used in environments with higher security requirements as part of a multifactor authentication system. While the hardware based frameworks are more secured than others frameworks, they are also costly and are difficult to deploy on a large scale, as is required for online banking and others, for example.

Soft tokens are an attempt to replicate the security advantages of multifactor authentication, while simplifying distribution and lowering costs. A smartphone soft token app mimics the hardware-based security token. Like a hardware token, a smartphone provides on the device itself, an easy-to-protect and easy-to-remember location for secured login information. Smartphones are connected devices, unlike a hardware token, which make them inherently less secure. The extent of their security

largely depends on the device's operating system and client software.

c. Mobile Authentication

Mobile authentication is the verification of a user's identity through the use a mobile device and one or more authentication methods for secure access. Mobile authentication may be used to authorize the mobile device itself or as a part of a multifactor authentication scheme for logging into secure locations and resources. Password entry is clumsy on cell phones, especially when including capital letters, numbers and symbols.

Some alternative methods of mobile authentication include:

- Non-text passwords, where symbols or images might be chosen from a randomly-generated field.
- Digital certificates using public key infrastructure.
- Smartcards with stored authentication data.
- Out of band authentication, where the user places a call to obtain authentication.
- One time passwords (OTP) through phone apps or SMS messages.

Some organizations have a need for extra security beyond ID and password for log in, but added devices and methods can make the procedures too cumbersome for employees. The ubiquity of smart phones can help ease the burden here, however. Most smart phones have a GPS device, enabling reasonable surety confirmation of the login location, a camera for potential facial recognition and iris scans, a microphone for voice recognition; some also have touch screens that can be used for finger scanning.

Mobile devices that use more than one of these capabilities are functionally multifactor tokens. An example is the use of a Smartphone software token app that taps into GPS location and scans a fingerprint, all within a device that the user was probably going to be carrying anyway. For administrators, the main benefit of a software implementation is that there are no extra physical devices to manage.

II. Using Hardware information in Authentication

HW has been used to facilitate authentication for a long time. The idea is that owners/users register their devices based on their MAC address so that, the devices themselves are authenticated, rather than their users. MAC addresses are used in the cryptography of files, authentication and integrity networks to support the security of data transportation. This technique uses the MAC address as a key authentication factor to secure the communication session with the Internet Protocol (IP) address to reach the device destination [2].

Filtering MAC addresses to secure the wireless network is essential in giving users access to the wireless network. Doing so will give precise control to wireless users connected with the Access Point (AP) associated with their MAC address [3]. If this filtering is not applied and the MAC address of the client is not given, the client will not be granted access to the wireless network. So, MAC addresses of the client computer device gives the authorisation needed for a wireless connection which is between the client and server [4].

Spoofing attack is a situation in which one person or program successfully masquerades as another user by falsifying data and thereby gaining an illegitimate advantage [5]. Spoofing of MAC is usually beyond the average wireless user's experience. In order to carry out spoofing on a MAC address, the client needs to be associated with a particular AP. As result, using the MAC address in wireless security depends on filtering the MAC address of the client without determining the user's characteristics.

Another method of HW authentication usage is storage media drivers such as HDDs . Each storage media item has a unique HMSPN as an identifier product code that can be used in profiling [6]. These HMSPNs are already actively used for identification, albeit that they can be modified at firmware level and thus are susceptible to spoofing. For example, Microsoft products send product and HW identifiers during the activation process. So, this HW information provides the opportunity to profile the user's computing environment.

Port security is a mechanism which is used to restrict the MAC addresses that connect via a particular port switch. This tool allows defined and specific access to a particular port to allow a unique MAC addresses, or a range of MAC addresses. To connect to the LAN port, it will allow access of MAC addresses which belong to a range according to a configured list. When a frame arrives to the switch it will compare the MAC addresses with the MAC addresses on the configured allowed list. If the MAC address matches one of items on the list then the packet is allowed to go through. In contrast, if the MAC address does not belong to the configured list the port will drop the packet. So, MAC addresses can be specified to connect to a certain port. This type of firewall can support authentication [7]. This level of information has some characteristics of the user's HW environment which can profile the user activity by using particular HW.

In "Active Directory Integrated Media Access Control" based wireless authentication, the Internet Authentication Source (IAS) needs to be installed on a domain controller to ensure that the domain controller belongs to the Remote Access Service (RAS) and IAS source group. To proceed with this process, a Security Group in Active Directory is created which should have the MAC address of the laptop's Wireless Cards. These are identified as "Wireless MACs".

Users are created by using the MAC address as a USERNAME and the AP is shared by a secret password. These users should be controlled by a security group created earlier by the network administrator. After creating a remote access policy in the IAS, this will permit remote access through the membership in the Windows group that was made previously. This course of action has been taken earlier in "authenticate wireless MAC accounts, based on group membership" [8]. A unique and constant MAC address is transmitted by 802.11 devices and thus are identifiable. It was recently proposed to replace such identifiers with pseudonyms, i.e. temporary names which were unable to be linked to the IT device due to the fact that implicating identifiers or identifying characteristics of 802.11 networks traffic can identify many users with high accuracy [9].

Another profiling technique uses four implicit identifiers visible to the piece of HW to quantify how well a passive adversary can identify users. A lower boundary is placed on how accurately users can be identified implicitly by using the following:

1. Identifying four previously unrecognized implicit identi- fiers: network destinations, network names advertised in 802.11 probes, differing configurations of 802.11 options and sizes of broadcast packets that hint at their contents.
2. Develop an automated procedure to identify users which quantifies how much information is revealed via implicit identifiers, both singularly and in multiples, and which can reveal about several hundred users in three empirical 802.11 traces.
3. The evaluation shows users produce highly discriminating implicit identifiers. Even a small sample of network traffic can identify them, i.e. more than half (56%) of the time in public networks. Moreover, it is most unlikely that they would be mistaken as being the source of other network traffic (1% of the time). Since

adversaries will obtain multiple traffic samples from a user over time, this high level of accuracy in traffic classification enables them to track many users with even higher accuracy than in common wireless networks.

4. It is the first time it has been shown with empirical evidence that design considerations beyond eliminating explicit identifiers, such as unique names and addresses, must be addressed to protect anonymity in wireless networks.

During one research it was [9] noted that by considering a subset of all possible identifiers and a weak, passive adversary, the results only place a lower boundary on the accuracy with which users can be profiled. The efforts are continuing to uncover implicit identifiers exposed in 802.11, such as those exposed by timing channels. The accuracy of the implicit identifiers over longer timescales and across different locations will be evaluative, since this study analysis is limited by the duration and location of the traces.

In 1998 the University of Pittsburgh established a network connection to residence hall students because the number of residence hall beds had increased to 6,000 and the connection rate had continued to increase to 74 percent of resident students. Students were implementing a manual process to assign static IP addresses and record each computer's MAC address. This then required the entry of a username and password each time the user established a connection. After that, the 2000 Dynamic Host Configuration Protocol Automated Teller Machine (DHCPATM) was used to provide IP addresses for each student in conjunction with registration software to record the necessary machine information. This technique, however, was considered to be too time consuming for tracking security activity [10]. Point-to-Point Protocol over Ethernet "PPPoE" technology was used to improve the ability of secure access to the wireless network. So, a single and easy system can be con- figured and used for all users. In spite of this the wireless or traditional wired ports connection must be implemented in order to avoid confusion and to offer users flexibility in public areas without needing to re-authenticate or switch to a different authentication mechanism wireless network [11,12]. Therefore, using additional HW information may support this access control approach to avoid the confusion of roaming from wireless to traditional wired ports in LAN.

Another technique uses specific network security devices. Network security devices are connected between a protected client and a network. The network security device negotiates a session key with another protected client. Then, all communications between the two clients are encrypted. The device is self-configuring and locks itself to the IP address of its client. Thus, the client cannot change its IP address once this has been set and therefore cannot emulate the IP address of another client. When a packet is transmitted from the protected host, the security device translates the MAC address of the client to its own MAC address before transmitting the packet into the network. Packets addressed to the host contain the MAC address of the security device [13].

In order to verify the client's username and password the Secure Remote Password protocol (SRP) [14] modular performs large integer exponentiations. This task requires many operations and consumes a large part of the total execution time of software implementations of the SRP protocol that are affected by HW performance. Modifying or designing a suitable HW environment to accelerate the exponentiations modular in the SRP protocol [15,16] is associated to user's HW and affects in observing user behaviour.

A mouse is a dynamic biometric that is similar to keystroke dynamics. The mouse is very important for graphical user interface (GUI). In contrast, the keyboard is essential for command line based applications. The behaviour of both these devices can

be combined in a common detector. Adapting keystroke technology by addressing issues such as passive and dynamic monitoring could improve the detection [17]. However both detectors may be affected by the keyword and mouse environment that motivate the focus in users' devices which affect user detection. A user's HW can support a reduction in digital identity fraud. However, because of natural or analytic HW authentication, this level of information is related to the user's confidentiality and integrity which are a primary concern and thus, any implementation of a new authentication method will have to be aware of this. In this research, HW information is used as the authentication factor.

III. REFERENCES

[1] https://en.wikipedia.org/wiki/Multi-factor_authentication

[2] R. P. R, Corporate computer and network security. New Jersey United States of America: Pearson Education, Inc, 2004

[3] C. Wang and H. Leung, "A private and efficient mobile payment protocol," Computational Intelligence and Security.

[4] J. Tellez and J. Sierra, "Anonymous payment in a client centric model for digital ecosystem," IEEE DEST, pp. 422–427, 2007.

[5] M. Rajalingam, S. Alomari, and P. Sumari, "Prevention of phishing attacks based on discriminative key point features of webpages," International Journal of Computer Science and Security (IJCSS), vol. 6, no. 1, p. 527, 2012.

[6] K. Patowary. (2009) How to interpret hard disk model numbers. [Online]. Available: http://www.instantfundas. com/2009/02/how-to-interpret-hard-disk-model.html

[7] S. Malik, Network Security Principles and Practices. 800 East 96th Street Indianapolis, USA: Cisco Press logo of Cisco System, Inc, 2003.

[8] C. Mongoho, "Mac based wireless authentication with ias," Techre public. [Online]. Available: http: //techrepublic.com.com/5208-7343-0.html?forumID= 102&threadID=226120&start=0&tag=content;left Colm, Bibliography 206

[9] J. Pang, B. Greenstein, R. Gummadi, S. Srinivasan, and D. Wetherall, "802. 11 user fingerprinting," in International Conference on Mobile Computing and Networking: Proceedings of the 13 th annual ACM international conference on Mobile computing and networking, vol. 9, no. 14, 2007, pp. 99–110.

[10] I. Graham and W. Joseph, "Authenticating public access networking," in Proceedings of the 30th annual ACM SIGUCCS conference on User services. ACM.

[11] O. Corre, I. Fodil, V. Ksinant, and G. Pujolle, "An architecture for access network management with policies (an-pbm)," in Management of Multimedia Networks and Services, ser. Lecture Notes in Computer Science, A. Marshall and N. Agoulmine, Eds. Springer Berlin Heidelberg, 2003, vol. 2839, pp. 328–340. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-39404-4 25

[12] D. Fye, "Evolution of wlan roaming services," in CDG WLAN Technical Forum, Dallas, Texas, vol. 2, 2003.

[13] F. A. and B. Levy, "Network security device which performs mac address translation without affecting the ip address," uS Patent 5,757,924.

[14] P. Hamalainen, M. Hannikainen, M. Niemi, and T. Hamalainen, "Performance evaluation of secure remote Bibliography 207 password protocol," in Circuits and Systems, 2002 IEEE International Symposium on, vol. 3. IEEE, 2002, pp. III–29.

[15] T. Wu, "The secure remote password protocol," in Internet Society Symposium on Network and Distributed System Security, 1998.

[16] A. Menezes, P. Van Oorschot, and S. Vanstone, Handbook of applied cryptography. CRC, 1996.

[17] A. Ahmed, "Security monitoring through human computer interaction devices," Ph.D. dissertation, UNIVERSITY