Volume 5, Issue 3, March 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Comparative Analysis of Various Factors of Authentication

Surbhi Chug[*], Sunny Dagar
Computer Science and Engineering
Manav Rachna College of Engineering
India

Abstract— ***In the continuous changing world of global data communications, reasonable Internet connections, and rapid software development, security has become a critical issue. Security is the basic requirement for global computing as it is inherently insecure. Unauthorized access to the system may be obtained by attackers or intruders, who are commonly known as "crackers", who then use the advanced knowledge to impersonate the actual user, steal information, or even deny the access to resources and computer system. Firstly, remember that no computer system is completely secure. Therefore, all that can done is to make increasingly difficult for the intruder to compromise with the system. Therefore, it is necessary to prove your identity. The process of determining and proving the identity of the user is known as authentication. This paper describes various factors of authentication and their comparisons.***

Keywords— Authentication, Biometric, GAIT, Graphical Password, Multi-Factor Authentication, Usability-Deployability-Security Framework, ZEBRA.

I. INTRODUCTION

The secure system considers security, reliability, usability, and human factors. The process of determining the identity of the user is called authentication. It is required as a prerequisite to allow accessing the computer system and its resources. A person may get access of a system by passing the authentication mechanism. But what if an unintended person gets the credentials of an intended user and authenticate himself on behalf of actual user. So a scheme is required in which a user has to pass two or more levels of authentication in order to get access of the system. So authenticating a user in more than one ways is known as multifactor authentication.

Authentication is done by using something you know (such as your password), something you have (such as your smartphone, tokens), or something unique to you (such as a retinal scan or fingerprint). Most early authentication is solely based on password but they are easily cracked, therefore to provide more security more than one factor authentication is required.

A single factor of authentication does not provide security. For example:- Password Based Authentication. Typically passwords are strings of letters and digits, i.e. they are alphanumeric. Such passwords have the disadvantage of being hard to remember. Weak passwords are vulnerable to dictionary attacks and brute force attacks where as Strong passwords are harder to remember. Therefore, to provide more security more than one factor authentication is required. Multi-factor authentication is one of the strongest ways to protect access to your accounts and information. Multifactor authentication means combining two or more factors of authentication. It is both secure and stable.

II. RELATED WORK

In 2004, Yoon et al. proposed a mutual authentication scheme based on generalized EIGamal signature scheme using smart cards. The Yoon-Ryu-Yoo's scheme can be divided into three phase: registration, login and authentication. In addition, user can change their passwords freely and securely without the help of remote system. The drawback of their authentication is that the intruder is able to reveal previous session keys by means of the disclosed secret parameters. Then in 2005, Bin Wang and Zheng-Quan Li [1] proposed a new scheme which offer forward secrecy. Text-based username and password is vulnerable to guessing, dictionary attack, key-loggers, shoulder-surfing and social engineering.

In 2011, Li Yang, Jian-Feng Ma, Qi Jiang [5] proposed a mutual authentication scheme based on smart cards and password under trusted computing, in which hash functions are used to authenticate identities, and remote attestation is used to verify the platform. Analysis showed this scheme can resist most of the possible attacks. Is secure and efficient and fulfills the designed security goals, such as secure session key agreement, user identity anonymity, password free changing, platform certification updating.

Smart card scheme still suffers from the smart card loss problem and fails to provide user untraceability and also vulnerable to desynchronization attack. Qi Jiang, Jianfeng Ma, Guangsong Li, Li Yang [4] proposed a robust two-factor authentication and key agreement scheme with user privacy preservation achieving all the goals of security.

Ayu Tiwari, SudipSanyal, Ajith Abraham, Svein Johan Knapskog, SugataSanyal [3] proposed the secure and stable protocol using multifactor authentication. They used a unique approach based on TIC (Transaction Identification Code) and SMS (Short Message Service) to provide extra security level with traditional Login/Password based system. Al-

Qayedi et al. have proposed the use of SMS but have not used TIC's in their protocol TIC's are user specific unique transaction identification codes which are issued by banks or financial institutions to the user. This code is similar to One Time Password (OTP) and code is used only once. They suggested to use TIC's as secret codes on cell phones. The user if authenticated only when he enters the TIC's code which he receives. Therefore, this scheme is more secure and stable than other schemes.

Alireza Pirayesh Sabzevar ,Angelos Stavrou [2] proposed a series of methods to authenticate the user with a graphical password. To that end, they employ the user's personal handheld device as the password decoder and the second factor of authentication. In their methods, a service provider challenges the user with an image password. To determine the appropriate click points and their orders, the user needs some hint information only to its handheld device. They have proposed the system that leverages both graphical passwords and multifactor authentication. They have employed graphical password combined with a handheld device to form a novel method of multifactor authentication.

J.K. Lee, S.R. Ryu and K.Y. Yoo proposed fingerprint-based remote user authentication scheme [11]. They proposed that the fingerprint verification method is based on minutia extraction and matching. Whenever a fingerprint is input, a different map of minutia is made and matched. This scheme requires a system to authenticate each user by each user's knowledge, possession and biometrics and this makes the authentication mechanism more reliable.

The biometrics uses physiological or behavioural characteristics like fingerprint or facial scans and iris or voice recognition to identify users. The biometrics includes the following: - voice recognition, fingerprints, face recognition, iris scan, retinal scan, hand and finger geometry, signature, gait, and keystroke dynamics.

Gait authentication has gained a lot of interest in recent years. It is basically developed for mobile phones for quick, easier and secure authentication. Gait recognition systems can be categorized into three classes: machine vision based (MV-based), Floorsensor based (FS-based) and Wearable sensor based (WSbased) [12]. Gait recognition is based on person's movements like walking, moving hands.

In May, 2014 Shrirang Mare, Andr´es Molina-Markham, Cory Cornelius, Ronald Peterson, and David Kotz described and evaluated Zero-Effort Bilateral Recurring Authentication called ZEBRA [7]. ZEBRA is a token-based authentication scheme that authenticates users based on their interactions with the device. Unlike keystroke-based biometrics that authenticates users based how they type, ZEBRA authenticates users based on what interactions (e.g., typing, scrolling) they perform on the device and when. In ZEBRA users wear a wrist-bracelet (token) that has built-in accelerometer and gyroscope sensors and a short range wireless radio to communicate with the device. ZEBRA authenticates users by monitoring their hand movements, using the sensors in the wrist-bracelet, when they are interacting with the device, and comparing the hand movements with the inputs received by the device during the interaction. In ZEBRA the bracelet contains the identification information for its associated user, which it shares with the device to authenticate the user. The user can associate the bracelet with herself when she wears the bracelet, say by entering a PIN on the bracelet or through a secure channel to the bracelet. The bracelet clasp can detect when it is being taken off and it de-associates with the user when it is taken off.

III. COMPARISON FRAMEWORK

We have compared various authentication schemes using the usability-deployability-security (UDS) evaluation framework [6]. The UDS framework defines a set of benefits to evaluate web authentication schemes, but many of those benefits are relevant to device authentication schemes.

A. BENEFITS

The UDS framework defines total 25 benefits to evaluate web authentication schemes: 8 usability benefits, 6 deployability benefits, and 11 security benefits. We use total 14 benefits to evaluate and compare various authentication schemes: 12 benefits from the UDS framework and 3 additional benefits that are applicable to continuous authentication schemes. As in the UDS framework, we rate each scheme as either offering or not offering the benefit of a property, if the scheme almost offers the benefit, but not completely, it is indicated with the Quasi- prefix.

1. USABILITY BENEFITS

U1 Memory-wise-Effortless : Users of the scheme do not have to remember any secrets or confidential information at all.

U2 Nothing-to-Carry : Users do not need to carry any physical device or object to use the scheme. We grant a Quasi-Nothing-to-Carry if the scheme can be implemented on an object that users carry or wear everywhere all the time anyway, such as their mobile phone, wrist watch, wearable fitness devices.

U3 Easy-Recovery-from-Loss : The user can comfortably regain the ability to authenticate if the authentication credentials are forgotten or the token is lost. We grant a scheme Quasi-Easy Recovery-from-Loss benefit if the user has to purchase a token, but can reset the authentication credentials herself without having to involve the other party. A user's authentication credential is the information that the user presents to the device to get authenticated, e.g., username and password, fingerprint.

U4 Physically-Effortless : The process of authentication does not require any physical user effort beyond what the user performs while interacting with the device to get his/her task done on the device. In other words, the scheme should be passive, i.e., it should not require any explicit input from the user, but the scheme can use the inputs the user anyway provides to the device to get his/her task done. We grant schemes Quasi-Physically-Effortless benefit if they require the user to perform an action which is easy and effortless to perform once.

U5 No-Constraint-on-Using-the-Device : The scheme should not add any constraint on how the user should use the device or interact with the device. We grant Quasi-No-Constraint-on-Using-the-Device benefit to schemes that add constraints that are easy to follow but do not require any additional physical effort from the user. For example, the facial-recognition scheme requires the user to be in the camera's field of vision, which can be easy, buta voice-based scheme requires the user to provide audio input, which is easy but requires physical effort.

2. Deployability Benefits

D1 Accessible : The users can use passwords that are not prevented from using the scheme by disabilities or other physical (not cognitive) conditions.

D2 Negligible-Cost-per-User : The total cost the user requires to access the scheme, includes the costs at the prover's end (any device/token required for the user to authenticate) and the cost at the verifier's end (any hardware and/or software required on the device to authenticate the user). Quasi-Negligible-Cost-per-User is awarded to the scheme if the required cost on prover's end can be masked with the devices users carry anyway and the verifying device already contains the required hardware.

3. Security Benefits

Security benefits S1-S5 are from the UDS framework. We introduce two additional security benefits, S7 and S8, for continuous authentication schemes.

S1 Resilient-to-Physical-Observation : The intruder is not able to impersonate a user after observing them authenticate one or more times. Attacks include shoulder surfing, filming the keyboard or mouse use [10], recording keystroke timings based on sensors near the keyboard [8], or thermal imaging the keypad[9].

S2 Resilient-to-Internal-Observation : The intruder cannot impersonate a user by intercepting the user's inputs from inside the user's device (e.g., by keylogging malware) or eavesdropping on the cleartext communication between the user's token (prover) and the authenticating device (verifier).

S3 Resilient-to-Leaks-from-Other-Verifiers : Anything that a verifier could possibly leak could not help the intruder impersonate the user to another device.

S4 Resilient-to-Phishing : The intruder who simulates the authentication process, e.g., by spoofing the authentication screen, is not able to collect credentials that can be used later to impersonate the user on the actual device.

S5 Resilient-to-Theft : If the credentials are lost they are not used for authentication by any another person who gains knowledge and possession of it. The lost credentials can be passwords written down by paper or hardware tokens. This benefit penalizes single-factor schemes (For Example, text-passwords) that do not offer any protection against theft. In the UDS framework this benefit is considered only for schemes in which physical objects or devices are used for authentication. In addition, theft of even non-physical credentials such as passwords is also considered, which can be stolen when people write them down. As in the UDS framework, Quasi-Resilient-to-Theft is granted if the scheme protects the credential with the modest strength of a PIN.

S7 Verify-Actual-User : The scheme can verify whether the user is actually using the device at any point in time. This benefit penalizes schemes such as one-time authentication schemes, which do not verify the user after the user authenticates once. Quasi-Verify-Actual-User benefit is granted to schemes that do weak verifications, such as verifying whether the user is in front of the device (face-based schemes) or whether the user is speaking to the device (voice-based).

S8 Continuous-Authentication : The scheme should continuously authenticate the user while the user uses the device.

IV. Comparative Evaluation

Now we will compare various factors of authentication, according to the above framework :

Table I: Comparative evaluation of various authentication schemes on basis of usability benefits

USABILITY BENEFITS	Memory – wise-Effortless	Nothing-to-Carry	Easy-Recovery-from-Loss	Physically-Effortless	No-Constraint-on-Using-the-Device
Passwords	🟢	⚫	🟢	⚫	⚫
Smart Cards	🟢	⚫	🟢	⚫	⚫
One Time Password	🟢	⚫	🟢	⚫	⚫
Graphical Password	🟢	⚫	🟢	⚫	⚫
Finger-print Based	🟢	⚫	🟢	⚫	⚫
Face- based	🟢	⚫	🟢	⚫	⚫
GAIT Authentication	🟢	⚫	🟢	⚫	⚫
ZEBRA	🟢	⚫	🟢	⚫	⚫

Table II: Comparative evaluation of various authentication schemes on basis of deployability benefits.

DEPLOYABILITY BENEFITS	Accessible	Negligible-Cost-per-User
Passwords	⚫	⚫
Smart Cards	🔵	🔵
One Time Password	🔵	🔵
Graphical Password	⚫	⚫
Finger-print Based	🔵	🟢
Face- based	🔵	🔵
GAIT Authentication	🔵	🔴
ZEBRA	⚫	🔵

Table III: Comparative evaluation of various authentication schemes on basis of security benefits.

SECURITY BENEFITS	Resilient-to-Physical-Observation	Resilient-to-Internal-Observation	Resilient-to-Leaks-from-Other-Verifiers	Resilient-to-Theft	Verify-Actual-User	Continuous-Authentication
Passwords	🟢	🟢	🟢	🟢	🟢	🟢
Smart Cards	🟢	🟢	🟢	🟢	🟢	🟢
One Time Password	🟢	🟢	🟢	🟢	🟢	🟢
Graphical Password	🔵	🔵	🔵	🔵	🔵	🔵
Finger-print Based	⚫	🟢	🟢	🟢	🟢	🟢
Face- based	⚫	🟢	🟢	🟢	🟢	🟢
GAIT Authentication	🟢	🟢	🟢	🟢	🟢	🟢
ZEBRA	⚫	⚫	⚫	🔵	⚫	⚫

⚫	Offers Benefit
🔴	Does Not Offer Benefit
🔵	Almost Offers Benefit
🟢	Somewhat Offers Benefit
🟡	Average Offers the Benefit

V. Conclusion

In this paper, we represent the UDS framework which provides the way to compare various factors of authentication. As per our evaluation, single factor of authentication does not provide as much security. But if we combine two or more factors then security is ensured. Moreover, passwords and graphical passwords based scheme are more deployable than other authentication schemes. but graphical passwords provide more security than the text passwords. However, ZEBRA rates the highest and is secure, usable and deployable as compared to other schemes.

References

[1] Bin Wang and Zheng-Quan Li, “A Forward-Secure User Authentication Scheme With smart Cards”, 11, Oct. 2005.

[2] Alireza Pirayesh Sabzevar, Angelos Stavrou, “Universal Multi-Factor Authentication Using Graphical Passwords”. SITIS, 2008, 2013 International Conference on Signal-Image Technology & Internet-Based Systems, 2013 International Conference on Signal-Image Technology & Internet-Based Systems 2008, pp. 625-632, doi:10.1109/SITIS.2008.92.

[3] Ayu Tiwari, Sudip Sanyal, Ajith Abraham, Svein Johan Knapskog, Sugata Sanyal, “A Multi-Factor Security Protocol For Wireless Payment- Secure Web Authentication Using Mobile Devices”. IADIS International Conference on Applied Computing Proceedings of the IADIS International Conference on Applied Computing, Salamanca, Spain, 18-20 February 2007,Submitted on 13 Nov 2011.

[4] Qi Jiang, Jianfeng Ma, Guangsong Li, Li Yang, “Robust Two-Factor Authentication and Key Agreement Preserving User Privacy”. JOURNAL = "I. J. Network Security",PAGES = 321-332, 2014.

[5] Li Yang, Jian-Feng Ma, Qi Jiang, “Mutual Authentication Scheme with Smart Cards and Password under Trusted Computing”. Journal - IJ Network Security - Volume 14 Issue 3 Pages 156-163, 2012.

[6] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. “The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes”. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), pages 553–567, May 2012. DOI 10.1109/SP.2012.44.

[7] Shrirang Mare, Andr´es Molina-Markham, Cory Cornelius2, Ronald Peterson, and David Kotz. "ZEBRA: Zero-Effort Bilateral Recurring Authentication (Companion Report)", Proceedings of the IEEE Symposium on Security and Privacy, May 2014.

[8] P. Marquardt, A. Verma, H. Carter, and P. Traynor. (sp)iPhone: "Decoding Vibrations from Nearby Keyboards Using Mobile Phone Accelerometers". In Proceedings of the ACM Conference on Computer and Communications Security (CCS), pages 551–562. ACM, Oct. 2011. DOI 10.1145/2046707.2046771.

[9] K. Mowery, S. Meiklejohn, and S. Savage. Heat of the moment: "Characterizing the Efficacy of Thermal Camera Based Attacks". In Proceedings of the USENIX Workshop on Offensive Technologies (WOOT), 2011. Online at http://www.usenix.org/events/woot11/tech/final files/Mowery.pdf .

[10] R. Raguram, A. M. White, D. Goswami, F. Monrose, and J.-M. Frahm. iSpy: "Automatic Reconstruction of Typed Input from Compromising Reflections". In Proceedings of the ACM Conference on Computer and Communications Security (CCS), CCS '11, pages 527–536. ACM, 2011. DOI 10.1145/2046707.2046769.

[11] J.K. Lee, S.R. Ryu and K.Y. Yoo, "Fingerprint-Based Remote User Authentication Scheme Using Smart Card", Electronics Letter, 6th June 2002, Vol 38 No. 12.

[12] LI Yuexiang, WANG Xiaobo and QIAO Feng, "Gait Authentication Based on Accelerating Signals of Ankle", Chinese Journal of Electronics Vol.20, No.3, July 2011.