A Study on Security of Authentication Systems

OTUEKONG UMOREN
otuekong.umoren.uws.ac.uk
Presenter: OTUEKONG UMOREN
University of the West of Scotland

Resume of Presenter

Otuekong Umoren is a Research student at the University of the West of Scotland, He holds a Master’s Degree in Information and Network Security.

Detailed Education/Qualification:

2019 - Master’s Degree Information and Network Security (University of the West of Scotland)

2016 - Bachelor of Science in Computer Science (Ternopil National Technical University, Ukraine).

Outline

- Motivation
- Background
- Security threats
- Current Protection techniques
- Security aspects
- Conclusion
- References

Motivation

User authentication is important for the security and confidentiality of information and services.

The use of passwords to authenticate users has been a common practice all over the world. With the introduction of other authentication systems, many users still depend fully on password authentication or single factor authentication despite various security threats.

Background

Text-based passwords are the most implemented and widely adopted passwords in various segments. While humans find it difficult in recalling complicated passwords, various schemes are available to assist users to keep multiple passwords secure. The major problems associated with passwords are memorizing strong passwords and also they are vulnerable to various pernicious attacks.

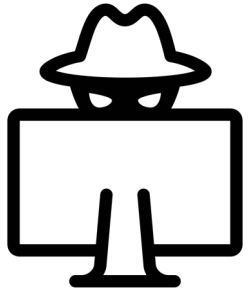
Security Threats 1/5

- Brute force attack:
- The brute force attack applies to all the possible password characters and combinations to break encrypted passwords usually when the passwords are saved as encrypted text. This attack technique is also known as exhaustive key search and can be used on any encrypted data (Apostol, 2012).

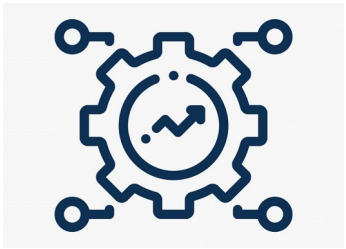
Security Threats 2/5

Brute Force Attack

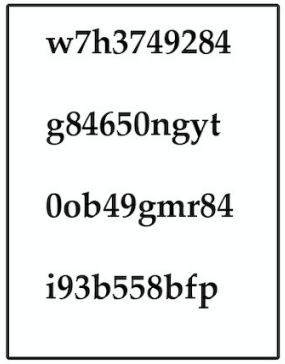
Attacker

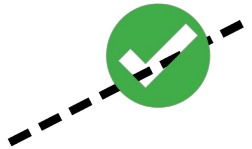


Hash



Attack's Password Digest





Password Digest

Attack Attempts different password combinations with several trials, the generated passwords are then hashed.

The digest requires to be compared to those in the stolen file

A match is found with the correct password's digest.

Security Threats 3/5

Dictionary attack:
The attacker uses a combination of meaningful words, mostly daily and occurring words, and tries to match those words with the password.

Security Threats 4/5

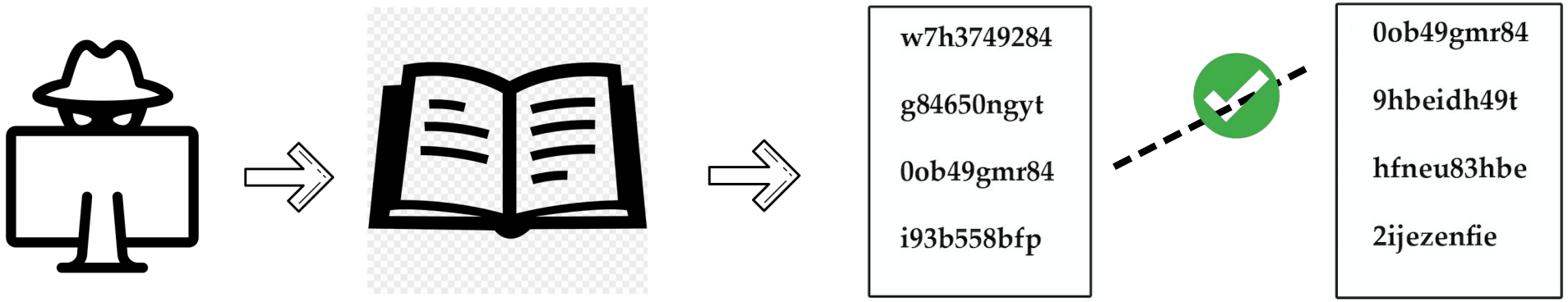
Dictionary Attack

Attacker

Dictionary words/Hash

Attack's Password Digest

Password Digest



The attacker generates digests from dictionary words.

The attacker then compares the digests to those in the stolen digest file.

The process continues until a match is found.

Security Threats 5/5

Other Security Threats

- Shoulder surfing
- Phishing attacks
- Spyware
- Video recording attacks
- Spoofing attacks
- Sweeper attacks
- Man-in-the-Middle attack

Current Protection Techniques: Graphical Authentication 1/2

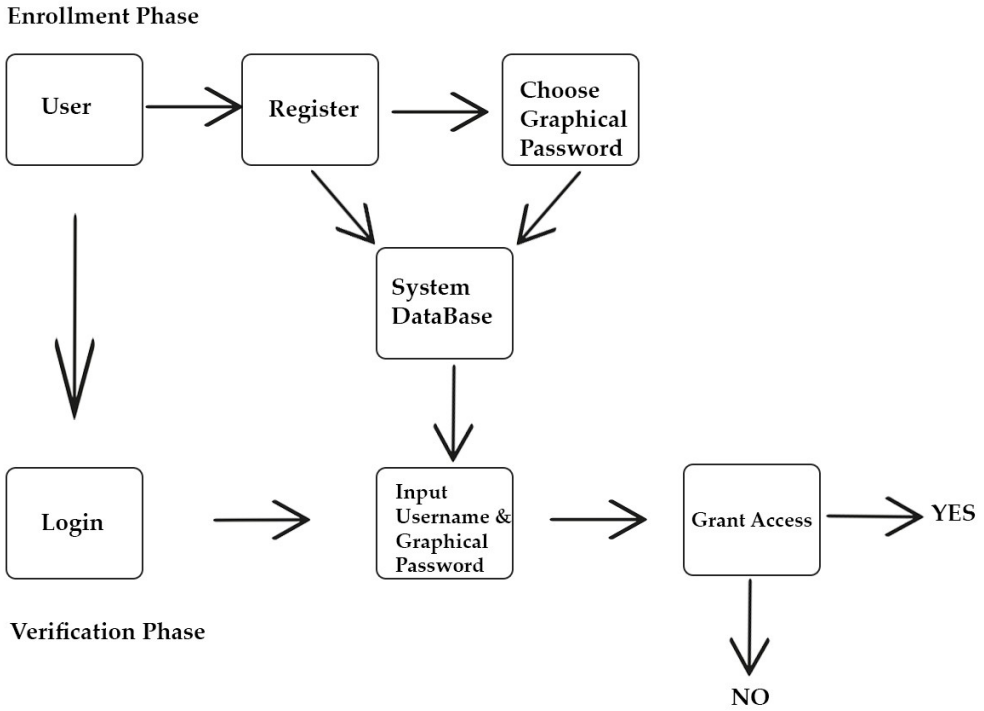
Is an authentication scheme where the authorized user is authenticated or the identity of the authorized user is verified through their knowledge on images or graphical objects (Agarwal et al., 2010).

Graphical authentication is very effective against man-in-the-middle attack, the man-in- the-middle attack is not feasible on graphical authentication.

Categories of Graphical password Authentication	
Recognition-based system	Recall-based system

Current Protection Techniques: Graphical Authentication 2/2

Enrollment & Verification



Current Protection Tecniques: Biometric Authentication 1/3

Biometric Authentication
The user’s biometrics such as:

- Finger print recognition
- Face recognition
- Signature verification

are processed and stored in the database, and those data are matched to authenticate user (Raza et al., 2012).

Biometric authentication is very effective against shoulder surfing, however this attack technique is not realistic against it.

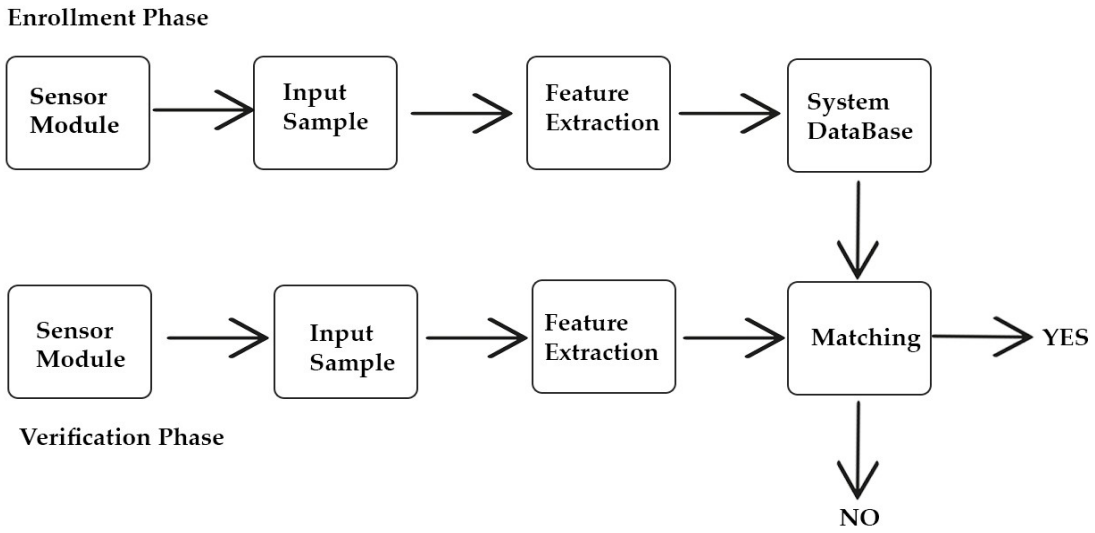
Current Protection Techniques: Biometric Authentication 2/3

Types of Biometrics

Physiological traits	Behavioral traits
Fingerprint	Keystroke
Hand geometry	Signature
Iris	Voice
Face	Typing patterns
DNA	Navigation patterns

Current Protection Tecniques: Biometric Authentication 3/3

Enrollment & Verification



Current Protection Techniques: Token-based Authentication 1/3

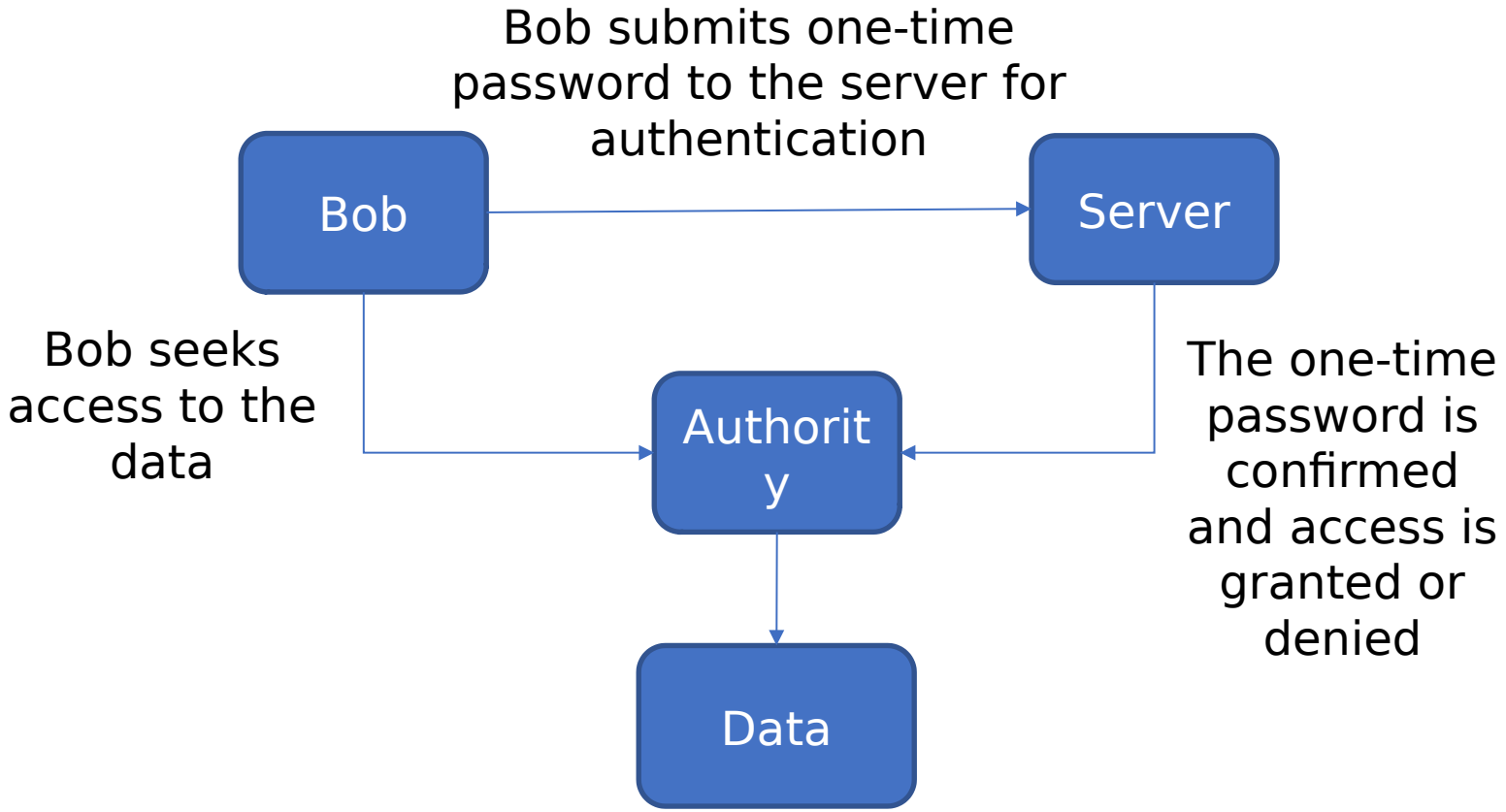
A token is a string that a server generates for a client and can be passed through an HTTP request (Kubovy et at., 2016).

- Token-based authentication offers high level protection against brute force and dictionary attacks.
- The short lifetime of the randomly generated passwords makes the token-based authentication somewhat resistant to brute force and dictionary attacks (Gorman, 2003).

Current Protection Techniques: Token-based Authentication 2/3

Types of tokens (Balaj, 2017)	
Access tokens	used several times but can’t be renewed
Session tokens	valid for a session and can be used severally with that session
Perishable tokens	valid for a single authentication process
Refresh token	valid for use just once (one-time password)

Current Protection Techniques: Token-based Authentication 3/3
Token-based Authentication (Verification)



Security Aspects

Authentication System	Security Features	
Graphical Authentication	Large password space (Biswas And Sankar, 2014). Decoys) (Rittenhouse et al., 2013),	Brute force search (Hafiz et al., 2008) Guessing, shoulder surfing, spyware, dictionary attack (Biswas and Sankar, 2014)
Biometric Authentication	Randomly created passwords (Gorman, 2003)	Spoofing attack, Denial- of-service attack, Replay attack, man-in-the-middle attack (Joshi et al., 2018)
Token-Based Authentication	Short ticket life-time, large entropy, one time password (Gorman, 2003).	Lost or Stolen token, Denial of service attack (Gorman, 2003)

Conclusion

All protection techniques fulfil the purpose of security to a minimal extent, but all are vulnerable to different attacks. Therefore, a robust security technique must be in place to defend.

A combination of these authentication factors in a multi-factor authentication will mitigate security threats.

References

M. Raza, M. Iqbal, M. Sharif, and W. Haider, “A survey of password attacks and comparative analysis on methods for secure authentication,” World Applied Sciences Journal, vol. 19, no. 4, 2012, pp. 439–444.

S. S. Biswas and S. Sankar, “Comparative study of graphical user authentication approaches,” International Journal of Computer Science and Mobile Computing, vol. 3, 2014, pp. 361–375.

R. G. Rittenhouse, J. A. Chaudry, and M. Lee, “Security in graphical authentication,” International Journal of Security and Its Applications, vol. 7, no. 3, 2013, pp. 347–356.

L. O’Gorman, “Comparing passwords, tokens, and biometrics for user authentication,” Proceedings of the IEEE, vol. 91, no. 12, 2003, pp. 2021–2040.

M. D. Hafiz, A. H. Abdullah, N. Ithnin, and H. K. Mammi, “Towards identifying usability and security features of graphical password in knowledge based authentication technique,” in 2008 Second Asia In- ternational Conference on Modelling & Simulation (AMS). IEEE, 2008, pp. 396–403.

M. Joshi, B. Mazumdar, and S. Dey, “Security vulnerabilities against fingerprint biometric system,” arXiv preprint arXiv:1805.07116, 2018.

J.Kubovy,C.Huber,M.Ja¨ger,andJ.Ku¨ng,“Asecuretoken-based communication for authentication and authorization servers,” in Interna- tional Conference on Future Data and Security Engineering. Springer, 2016, pp. 237–250.

Y. Balaj, “Token-based vs session-based authentication: A survey,” 09 2017.

G. Agarwal, S. Singh, and R. Shukla, “Security analysis of graphical passwords over the alphanumeric passwords,” International Journal of Pure and Applied Sciences and Technology, vol. 1, no. 2, 2010, pp. 60–66.

K. Apostol, “Brute-force attack,” 2012.