ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Survey of Authentication Methods for Mobile Phones

Harshalee D. Korde, Jyoti More

PG Student, Dept. of Computer Engineering, Lokmanya Tilak College of Engineering, Navi Mumbai, Mumbai University, Maharashtra, India

Assistant Professor, Dept. of Computer Engineering, Lokmanya Tilak College of Engineering, Navi Mumbai, Mumbai University, Maharashtra, India

ABSTRACT: Authentication is a procedure by which a system authenticates the uniqueness of a user. User authentication is the mechanism for authentication and protects user data or unauthorized access of information. The most common computer authentication method is text-based passwords. Text based passwords are vulnerable to social engineering attacks, either weak-and-memorable or secure-but-difficult-to-remember. This method has been shown to have significant drawbacks. To address this problem some researchers have established authentication methods that alphanumerical password. Often alphanumerical passwords are combination of alphabets and numbers which makes the password greater in length and hard to remember. User can write our password in page or in computer files but if the page is damaged or that computer file is corrupted then password is lost. Existing password scheme is easy through different attack i.e. dictionary attack, brute force attack, shoulder-surfing. This paper presents the survey of three main authentication methods, challenges,security attack and the strengths of graphical password.

KEYWORDS:Authentication; Biometric-Based Authentication; Identification; Knowledge-Based Authentication; Possession-Based Authentication

I. INTRODUCTION

Authentication is any method by which a system authenticates the identity of a user who desires to access it.Any security system protects information they store, their resources and human factors like ease of use and accessibility. The ultimate security system deliberates security, reliability, usability and human factors.A password is a secret that is shared by the verifier and the customer. ”Passwords are simply secrets that are provided by the user upon request by a recipient” [4]. Passwords are stored in encrypted form on server so that even if invader tries to break the system, it will not be disclosed. Password authentication does not require any extraordinary hardware. Usually, password is collection of digits and letters also called alphanumeric which are difficult to remember.

Many security issues have risen because of increase in usage of mobile devices. The foremost security threat is related to authentication the user that is the process of authorizing the user. Important factors for creating secured communication are authenticated user and confidentiality. The main authentication schemes are:

1. Token based: what you have
2. Biometrics: what you are
3. Knowledge based: what you know

II. LITERATURE SURVEY

Zippy Erlichin paper “Authentication Methods for Computer Systems Security” [1]presents the three main authentication approaches, their technology and implementation issues, and the factors to be considered when choosing an authentication method.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Xiaoyuan Suo Ying Zhu G. Scott. Owen in paper "Graphical Passwords: A Survey" [2] discusses the strengths and limitations of each method and point out the future research directions in this area. He also try to answer two important questions this survey will be useful for information security researchers and practitioners who are interested in finding an alternative to text-based authentication methods.

The article "Authentication Methods for Computer Systems Security (information science)" [3] presents the three main authentication approaches, their technology and implementation issues, and the factors to be considered when choosing an authentication method.

III. CLASSIFICATION OF AUTHENTICATION METHODS

Authentication is relatively simple where a user provides some sort of credentials such as a password, smart card, fingerprint, digital certificate which identifies that user as the person who is authorized to access the system [5].There are, however, multiplicities of methods and protocols that can be used to accomplish this. Regardless of the method, the basic authentication process remains the same. In most instances, a user must have a valid user account configured by the network administrator that specifies the user's permissions and rights. User credentials must be associated with this account—a password is assigned, a smart card certificate is issued, or a biometric scan is entered into the database against which future readings will be compared [6].When the user wants to log on, he or she provides the credentials and the system checks the database for the original entry and makes the comparison. If the credentials provided by the user match those in the database, access is granted.Multiple unique features are used to authenticate user. Mobile phones are using these features to authenticate users. The authentication methods are categorized into three types according to the unique features they have [8]:

A. *Token -based authentication:*

It is based on what user has which is mostly physical objects like memory card and card token. It is also stated as possession-based authentication. Valid user has valid tokens but tokens can be stolen or duplicated by fake resources. There are few problems related to token:Administration of token and Inconvenience to carry tokens.

Mainly tokens are divided into two types:

1. Memory tokens: Memory tokens like magnetic card store data but do not process it. Memory tokens are inexpensive and trained for authentication composed with a knowledge-based authentication mechanism such as a PIN. Using magnetic card with PIN offers more secured system.
2. Smart Tokens: One or more integrated circuits like microprocessor are embedded to process data. Smart tokens are expensive, flexible, and secure and are also trained for authentication composed with a knowledge-based authentication mechanism. As it is highly secure, it's used for authentication in one-time passwords over open networks.

B. *Biometric-based authentication*

It is based on what user is which can be behavioral like keystroke dynamics or physiological like fingerprint. Authentication is based on characteristics of user alike functional physiological or behavioral which are distinct from each individual. Hence the probability to create an identity of a user grounded on who the user is is more than what user has or knows.

Biometrics authentication requires extraordinary hardware so it is practically difficult and generally exclusive. This technology provides high level of security but on other hand user acceptance is low as it is intrusive and violating privacy. Therefore, they are less popular and only used in highly secure system.A biometric system has three modules: the sensor module, the feature abstraction module and the feature matching module. User's characteristics are captured and equated with reference files for authentication. The accuracy is calculated using two factors false non-matching and erroneous acceptance

The biometrics is divided into two types:

1. Physiological biometric: It is established on user's constant physical features. Few examples are facial scan, retinal scan, Finger scan, etc.
2. Behavioral biometrics: It is established on user's movement. Few examples are facial scan, retinal scan, Finger scan, etc.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

C. *Knowledge-based authentication:*

It is broadly used authentication that is based on what user knows which is mostly password, pass code or PIN. This technology uses Public Key Infrastructure (PKI) with public and private key pair over unsafe public network to authenticate the user. It consists of pair of user ID and password for authentication. A password is conceptually simple for both system designers and end users. It consists of a secret series of characters according to some predefined rules [1].

Some drawbacks related to knowledge based authentication are:

1. Difficult to guess:The collection of numbers, alphabets and special characters are highly secure passwords which are difficult to be guessed. Althoughthese arechallenging to recall and thus users tends to note it down which leads to ruining the secrecy.
2. Difficult to breach: User usually uses passwords with names, initials or nicknames that can be easily recalled but can be easily breached. They also tend to duplicate their passwords and thus cause the domino effect of password reuse; namely, all the systems with the same password are no more secure than the weakest system using this password[9].

The following are the rules for selecting a password [10]:

- Password shouldn't be made public and shouldn't be copied down anywhere.
- Collection of characters with enough lengthy.
- Number of failed authentication efforts should be restricted.
- No glossary words
- Password should be easy to predict and recall.
- Password should be abbreviations, sayings.
- A password shouldn't be used again and again.

These rules increase the security of system and defend it from dictionary and brute force attack. Passwords should never be stored in clear text; they should be encrypted or hashed.

There are two levels of authentication:

1. First level of authentication: There is the password that permits the right to use system's information resources via Operating System (OS). Primary passwords are responsible for passwords generated by system and password generated by user with previously well-defined rules. User generated are easier to recall as compared to system generated but less secure. System generated passwords can be easily guessed.
2. Second level of authentication: Also called Secondary passwords. These passwords provide multilevel authentication to access fragments of resources like data files and sensitive application. The drawbacks of first level of authentication that is difficult to recall password is overcame in this level. This leads to new method of authentication called a question and answer password where information is interchanged between user and system.

In question and answer method, the user answers few questions from set of questions which are unsystematically chosen from his profile. A particular application is used is used to permit access to user which matches the user's answer to the answers saved in his profile.

There are two categories of question and answer password:

1. Cognitive password: User has to answer the questions based on personal facts or opinion. The few examples are user's first teachers name which is fact based and user's favorite food which is opinion based.
2. Associative password: User has to provide a set of word suggestions.

IV. CHALLENGES AMONG AUTHENTICATION SCHEMES

Following are the challenges for different authentication methods as described above:

A. *Token -based authentication:*

Tokens based authentication has challenges:

1. Tokens are problematic as user has to enter value and password manually.
2. Tokens are exclusive and should be substituted every few years

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

3. Theft of token is easy hence can lead destruction of token.

B. *Biometric -based authentication:*

Biometric based authentication has challenges:

1. For biometric based authentication, user's computer should have sensors and related software which is exclusive.
2. On other hand, the probability of erroneously accepting unauthenticated user and rejecting authenticated user is more in economical schemes

C. *Knowledge -based authentication:*

Knowledge based authentication has challenges:

1. A distinct password can be used for several websites which is not secure. An intruder can easily find out the password and can pretence the user's identity.
2. Recovering the forgotten password is exclusive and highly unsecure.
3. Although these are challenging to recall and thus users tends to note it down which makes it vulnerable to theft.
4. Using a single password for multiple users can be loss for revenue. Also, Administrator losses capability to inspect and trace the particular user.

V. SECURITY ATTACKS

Following are the few possible security attacks:

1. Man in middle attack:In man-in-the-middle attack, anintruder inserts him/herself into a communication between two parties, imitates both parties and gains contact to information that the two parties were trying to send to each other [11]. A man-in-the-middle attack allows an intruder to interrupt, send and accept data intended for someone else, or not intended to be sent at all, without either external party knowing until it is too late. If there are long range channels available, such as a phone network or Wi-Fi, they can be used as a secure side channel to protect against MitM attacks. Such protection is needed for level 3 and higher. Without long range channels, mutual authentication or similar methods can be used to prevent MitM attacks [12].

2. Brute force attack: In brute force attack, a trial-and-error method used whichacquires information such as a user password or personal identification number (PIN). Automated software is used to produce an enormous number of successive guesses as to the value of the desired data. The most obvious way to block brute-force attacks is to simply lock out accounts after a defined number of incorrect password attempts. Account lockouts can last a specific duration, such as one hour, or the accounts could remain locked until manually unlocked by an administrator [13]. However, account lockout is not always the best solution, because someone could easily abuse the security measure and lock out hundreds of user accounts. In fact, some Web sites experience so many attacks that they are unable to enforce a lockout policy because they would constantly be unlocking customer accounts.

3. Dictionary attack: In dictionary attack, an intruder ruptures the computer security which is password protected machine or server. An intruder thoroughly enters each word in a dictionary as a password. Sometimes he tries to decide the decryption key of an encrypted message or document.

4. Shoulder-surfing: In shoulder surfing, direct observation is done like looking over someone's shoulder, to get information. From crowded places it is easy to get information person standing next to you.It can also be done elongated distance with the help of binoculars or other vision-enhancing devices.

VI. CONCLUSION AND FUTURE WORK

Graphical passwords are easy to recall as compared to text based password. According to survey, it is challenging to break graphical password as compared to other authentication mechanism. Most of the methods are

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

prone to traditional attacks like shoulder surfing, man in middle attack. The strength of authentication mechanism when it overcomes the traditional attack.In this paper analysis of authentication methods were conducted. Specific aspects of the technology were chosen for the analysis, namely, three main authentication methods, challenges. It then discusses current probable security threats that can be launched on the mechanism.

REFERENCES

1. Zippy Erlich, Moshe Zviran,"Authentication Methods for Computer Systems Security", Encyclopedia of Information Science and Technology,ch049, 2009.
2. The-Crankshaft Publishing, "Authentication Methods for Computer Systems Security (information science)".
3. Patrick, A.S., Long, A.C., & Flinn, S., "HCI and security systems", CHI 2003 Conference Proceedings: Extended Abstracts (Workshops), 2003.
4. Tushar Gaikwad, Mayur Patil, Prof. Vijaya Sagvekar, Prof. Divya Racha,"Network Security: A Study Using Cryptography Techniques" International Journal for Research in Applied Science & Engineering Technology, Volume 3, Issue II, 2015.
5. Deb Shinder, "Understanding and Selecting Authentication Methods", 2001.
6. Adams and m. A. Sasse, "Users Are Not The Enemy: Why Users Compromise Computer Security Mechanisms and How to Take Remedial Measures,"International Journal of Computer Applications, vol. 42, pp. 41-46, 1999.
7. Kailas I Patil, Jaiprakash Shimpi, "A Graphical Password Using Token, Biometric, Knowledge Based Authentication System For Mobile Devices" International Journal of Innovative Technology and Exploring Engineering, Volume-2, Issue-4, 2013.
8. Mehdi Khosrow-Pour,"Encyclopedia of Information Science and Technology", Second Edition, 2008.
9. Fred B. Schneider, "Authentication for People", chapter 5, 2009.
10. Patricia SengstackCharles Boicey, "Mastering Informatics: A Healthcare Handbook for Success", 2015.
11. Anna Vapen, Nahid Shahmehri,"Security Levels for Web Authentication using Mobile Phones",IFIP Advances in Information and Communication Technology, Volume 352 , pp 130-143, 2011
12. Mark Burnett,"Blocking Brute Force Attacks", The Open Web Application Security Project", 2015

BIOGRAPHY

Harshalee D. Kordeis pursuing M.E (Computer) from Lokmanya Tilak College of Engineering, Navi Mumbai, Mumbai University. She did her graduation B.E (Computer) from Mumbai University, Maharashtra. She is currently working on Smartphone Enabled Secure Access to Multiple Entities (SESAME).

Jyoti Moreis working as Assistant Professor in Department of Computer Engineering at Lokmanya Tilak College of Engineering, Navi Mumbai, Mumbai University. She has done B.E. (Comps), M.E. (Comps) and pursuing Ph.D. from University of Mumbai. She has guided many projects at UG and PG level. Her areas of interest areData Mining, System Security, Artificial intelligence, Soft Computing, etc.