Available online at www.worldscientificnews.com

World Scientific News

WSN 37 (2016) 265-278 EISSN 2392-2192

Survey a secured privacy authentication with recovery

Dr. M. Newlin Rajkumar[1,a], V. Dhurka[2,b], P. Kayathri[2,c]

[1]Assistant Professor, Department of CSE, Anna University Regional Centre, Tamil Nadu, India

[2]PG Scholar, Department of CSE, Anna University Regional Centre, Tamil Nadu, India

[a-c]E-mail address: newlin_rajkumar@yahoo.co.in , dhurkav@gmail.com , kayathri44@gmail.com

ABSTRACT

Every person has his own data and needs it to be secure, so authentication and acceptance were found to be essential. Most web based applications are based on password level authentication only. Since passwords are easily prone to be attacked, a better authentication is needed. The biometrics and the biometric way of authentication came to existence but this also suffered from the drawback of excess hardware and complex mechanisms. This paper presents a simple and efficient user authentication approach based on OTP with four digit pin number. When the user logins into the system, the login password is matches with database and if they match, the user is identified as a legitimate user. Further, an OTP is generated and sent to the user. The user enter the OTP along with four digit pin. If this combined OTP and four digit pin is matched with database, user is authenticated. Otherwise user is not allowed to access. This achieves better authentication and efficiency. If user forget their password, recovery phase is available. In this phase user have to answer the query which is based on the image that is displayed by server. If the answer is matches, then password reset link will send to user's mail id. This recovery method is not vulnerable to password resetting attack. This paper provides different types of password, types of authentication and types of attack.

***Keywords*:** Password; Authentication; OTP

1. INTRODUCTION

Nowadays everyone used to register or signup in so many website to access the details or to connect with friends in Facebook, Twitter and etc. When signup they have to give username and password. For their convenience they gave the same password to all website. This is called password reuse. Attack of this kind of password is called "Password Reuse Attack" or "Domino Effect". To solve this kind of problem there is so many solutions are available like password management tool which is used to store all are username and password along with website name. We need to remember single password that we kept for password management tool. But people were not aware of those technology, so they simply using weak password for all sites.

A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which should be kept secret from those not allowed access. The use of passwords is known to be ancient. Sentries would challenge those wishing to enter an area or approaching it to supply a password or watchword, and would only allow a person or group to pass if they knew the password.

Passwords are secrets that stay secretive to an individual who intends to use it to authenticate oneself. Security is everyone's responsibility. Most organizations specify a password policy that sets requirements for the composition and usage of passwords, typically dictating minimum length, required categories (e.g. upper and lower case, numbers, and special characters), prohibited elements (e.g. own name, date of birth, address, telephone number).

Some governments have national authentication frameworks that define requirements for user authentication to government services, including requirements for passwords. A weak entry point in any system could allow intruders to gain access to critical information and cause havoc on an entire network. Passwords are good for authenticating who you say you are. Passwords are used in every environment around you, starting from the most insecure to the most classified ones. A good password should be easy to remember and hard to guess. Let's see various types of password, authentication method and password attacks.

2. PASSWORD

A password is a un spaced sequence of characters used to determine that a computer system user requesting access to a computer system is really that particular user. Typically users of a multiuser or securely protected single-user system claim a unique name that can be generally know. In order to verify that someone entering that user ID really is that person a second identification the password known only to that person and to the system itself, is entered by the user.

Most networks require that end users change their passwords on a periodic basis. Attackers have been trying to crack passwords of various email accounts, services [FTP, SSH, etc.], etc. on daily basis. Hence, if you are not responsible enough to pick and choose good passwords, then you would be next in the victim list. Good passwords help you secure yourself from such attacks. Password types from Novell have evolved through the following models:

- NDS Password
- Simple Password
- Enhanced Password
- Universal Password
- Distribution Password
- Graphical Password

Novell Directory Services Password

Novel Directory Service (NDS) is a popular software product for managing access to computer resource and keeping track of the users of a network, such as a company's intranet from a single point of administration. Using NDS, a network administrator can setup and control a database of users and manage them using a directory with an easy to use graphical user interface (GUI). Users of computer at remote locations can be added, updated, and managed centrally. Applications can be distributed electronically and maintained centrally. The NDS Password is used by the Novell Client, LDAP, and by applications written to the Novell client APIs. With the NDS password, public and private keys (RSA) are created and stored on the user object. The process is non-reversible only the "hash" of the password is stored. The customer cannot retrieve the password from eDirectory. The password is never sent on the wire.

Simple Password

When Novell first introduced for Native File Access, they didn't want to allow plain text passwords to be sent and compared against the NDS password. So they introduced the Simple Password. When this was first introduced it was set manually, and there was no easy way for a user to change this. The Simple password doesn't have any polices and doesn't follow the NDS-based policies. Simple password are at a low security than NDS Passwords, because simple password are sent across the wire and stored. Simple passwords only have lower case letters and numbers. They are easier for someone else to guess. Simple password were only used by Netware 6 CIFS and NFS services. Netware 6.5 and beyond uses Universal Password.

Enhanced Password

This is rarely seen but can be thought of as simple password with some policies added. The Enhanced Password model was deprecated in favor of universal password. Enhanced Password offers some degree of password Policy, including minimum/maximum length, and repeatable/consecutive characters. With this model, Password Synchronization is one way: it flows out from enhanced password to universal password and NDS Passwords. The enhanced password design was not consistent with simple or universal password, and thus offered different security characteristics.

Universal Password

Universal password was introduced to wrap up all the passwords into one place. It is reversible and can be used with IDM. It is reversible and can be used with IDM. It has very powerful centrally configured policy support and integration with NMAS, including the challenge Response. Universal password can be configured to set both the simple password

for backwards compatibility and distribution password for IDM. Universal password requires NMAS aware clients and servers in order to function correctly. Currently, NMAS/Universal password aware applications will actually try both the universal password to authenticate. If an administrator changes a universal password it is considered an administrative change and the password is automatically expired. If a user changes a universal password it is considered a normal change and the password expiry is effectively "moved on" by the number of days in the policy. This cause an issue when using IDM, because if you directly synchronize into the universal password it would be expired.

Distribution Password

The distribution password is only used with IDM. It is a reversible version of the user's password, which can be synced out to other systems. Setting the distribution password via IDM automatically sets the universal password but is seen as a user change.

Graphical Password

A graphical password is an authentication system that works by having user select from images, in a specific order, presented in a graphical user interface (GUI). A graphical password is easier than a text-based password for most people to remember. Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words. A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. But if a series of selectable images is used on successive screen pages, and if there are many images on each page, a hacker must try every possible combination at random. If there are 100 images on each of the 8 pages in an 8-image password, there are 10 quadrillion possible combinations that could form the graphical password.

Dynamic Password

Dynamic password is another name for one time password (OTP). The password changes regularly and doesn't remain constant. In this method password is different and dynamically created each time he or she logins. This password is valid for only one login session or transaction, on a computer system or other digital device. It avoids a number of shortcomings that are associated with traditional password based authentication. Most advantage of this password is, they are not vulnerable to replay attacks. To avoid the problems associated with password reuse, onetime passwords were developed. There are two types of one time passwords, a challenge response password and a password list.

3. AUTHENTICATION

Most network operating systems require that a user be authenticated in order to log onto the network. This can be done by entering a password, inserting a smart card and entering the associated PIN, providing a fingerprint, voice pattern sample, retinal scan or some other means which is used to prove to the system that you are who you claim to be. There are several physical means by which you can provide your authentication credentials to the system. In private and public computer networks (including the Internet), authentication is commonly done through the use of login passwords or pass phrases; knowledge of such is

assumed to guarantee that the user is authentic. Thus, when you are asked to "authenticate" to a system, it usually means that you enter your user name and/or password for that system.

Computer users are using three different factor authentication. They are Single Factor Authentication (SFA), Two Factor Authentication (TFA) and Multi Factor Authentication (MFA). All those authentication methods are comes under those three. Single Factor Authentication is a process for securing access to a given system, such as a network or website that identifies the party requesting access through only one category of credentials. The most common example of SFA is password based authentication. Password security relies on the diligence of the system administrator or user who sets up the account. User should create strong password so that no one can access it.

Two Factor Authentication which is also known as 2FA or 2-step verification. 2FA is a security process in which the user provides two means of identification from separate categories of credentials; one is typically a physical token, such as a card, and the other is typically something memorized, such as security code. In this context, the two factors involved are sometimes spoken of as something you have and something you know. A common example of Two Factor Authentication is a bank card: the card itself is the physical item and the personal identification number (PIN) is the data that goes with it. Including those two elements makes it more difficult for someone who trying to access user's bank account because they would have to have the physical item in their possession and also know the PIN.

Multi Factor Authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. Multi Factor Authentication combines two are more independent credentials: what the user knows (password), what the user have (security token) and what the user is (biometric verification). The goal of Multi Factor Authentication is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target. Some of authentication methods are,

- Network Access Authentication
- IPSec Authentication (IPsec)
- Remote Authentication
- Password Authentication
- Smart Card Authentication
- Biometric Authentication
- Digital Signatures
- Kerberos

Network Access Authentication

Network Access Authentication verifies the user's identity to each network services that the user's attempts to access. It differs in that this authentication process is, in most cases transparent to the user once he or she logged on. Otherwise, the user would have to reenter the password or provide other credentials every time he or she wanted to access another network service or resource. Certificates are used for network access authentication because they provide strong security for authenticating users and computers and eliminate the need for less secure password-based authentication methods.

In this method a server is defined as a VPN or Internet Authentication Service (IAS) server that is a Transport Level Security (TLS) end point. You can configure VPN servers to perform network access authentication without IAS, or you can use IAS for authentication when you have multiple Remote Access Dial-in User Services (RADIUS) clients on your network. The use of certificates for authentication of VPN connections is the strongest form of authentication available with the Windows Server 2003 family.

IPSec Authentication

IP Security (IPSec) provides a means for users to encrypt and/or sign messages that are sent across the network to guarantee confidentiality, integrity and authenticity. IPSec transmissions can use a variety of authentication methods, including the Kerberos protocol, public key certificate issued by a trusted certificate authority (CA) or a simple pre-shared secret key that is a string of characKerberos is a network protocol that uses secret-key cryptography to authenticate client-server applications. Kerberos requests an encrypted ticket via an authenticated server sequence to use services. The protocol gets its name from the three-headed dog (Kerberos, or Cerberus) that guarded the gates of Hades in Greek mythologizers known to both the sender and the recipient. Computer authentication is first performed during L2TP/IPSec connection attempts between remote access client and server. When a secure channel is established between the client and server, the user authentication and authorization attempt proceeds.

Remote Authentication

There are a number of authentication methods that can be used to confirm the identity of users who connect to the network via a remote connection such as dial-up or VPN. Remote users can authenticated via a Remote Authentication Dial-In User Service (RADIUS) or the Internet Authentication Service (IAS). Each of these will be discussed in more detail in the section titled Authentication methods and Protocols. It is especially important that remote users be properly authenticated, as they generally pose a greater security risk than on-site users.

Password Authentication

Most of us are familiar with password authentication. The worker will remotely authenticate for access to that remote network. In OSI model architecture this method is fit for application layer. To log onto a computer or network, you enter a user account name and the password assigned to that account. This password is checked against database that contains all authorized user and their passwords. To preserve security of the network, passwords must be "strong" that is, they should contain a combination of alpha and numeric characters and symbols. Password Authentication is vulnerable to a password "cracker" who uses a brute force attack or protocol sniffer to capture packets if passwords are not encrypted when they are sent over the network. It enables remote access servers to communicate with central server to authenticate dial-in users and authorize their access to the requested system or service.

Smart Card Authentication

Smart cards are credit card-sized devices that hold a small computer chip, which is used to store public and private keys and other personal information used to identify a person and

authenticate him or her to the system. Logging onto the network with a smart card requires that you need to insert the card into a reader and then enter a PIN in much the same way that you use an ATM card to access an ATM. Smart cards help to eliminate the threat of hackers stealing stored or transmitted information from a computer. The information is processed on the smart card, so it never has to leave the card or be transmitted to another machine. But only limited amount of information can be stored on smart card's small microchip. Due to this encryption option also limited in the chip.

Biometric Authentication

An even more secure type of authentication than smart cards. Biometric Authentication involves the use of biological statistics that show that the probability of two people having identical biological characteristics such as fingerprints is infinitesimally small; thus, these biological traits can be used to positively identify a person. Biometric verification is involved based on the ways in which individuals can be uniquely identified through one or more distinguishing biological traits, such as fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, keystroke dynamics, DNA and signatures. Biometrics authentication is the application of that proof of identity as part of a process validating a user for access to a system. Biometric technologies are used to secure a wide range of electronic communications, including enterprise security, online commerce and banking—even just logging in to a computer or smartphones.

Digital Signatures

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer. In many countries, including the United States, digital signatures have the same legal significance as the more traditional forms of signed documents. Digital signatures are based on public key cryptography, also known as asymmetric cryptography.

Kerberos

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. The Internet is an insecure place. Many of the protocols used in the Internet do not provide any security. Tools to "sniff" passwords off of the network are in common use by malicious hackers. Thus, applications which send an unencrypted password over the network are extremely vulnerable. Worse yet, other client/server applications rely on the client program to be "honest" about the identity of the user who is using it. Other applications rely on the client to restrict its activities to those which it is allowed to do, with no other enforcement by the server.

Some sites attempt to use firewalls to solve their network security problems. Unfortunately, firewalls assume that "the bad guys" are on the outside, which is often a very bad assumption. Most of the really damaging incidents of computer crime are carried out by insiders. Firewalls also have a significant disadvantage in that they restrict how your users can

use the Internet. (After all, firewalls are simply a less extreme example of the dictum that there is nothing more secure than a computer which is not connected to the network – and powered off!) In many places, these restrictions are simply unrealistic and unacceptable. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

4. PASSWORD ATTACKS

Password attacks are the way to gain access to a computer system is to find out the password and log in. The growth of the internet has created unlimited opportunity for these intruders to steal secrets, tinker with web sites, abscond with credit card information, or just generally make mischief. Hackers' goal might be differ, but they all have the goal of gaining power and control of a computer system or network. There are two types attack one is Active attack, another one is passive attack. All attacks are comes under those two attack.

An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target. An active attack attempts to alter system resource or affect their operation. An active attack is what is commonly thought of when you refer to "hacking". In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in modification of data or DoS.

A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target. Passive attacks include active reconnaissance and passive reconnaissance. A passive attack monitors unencrypted traffic and looks for clear text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic and capturing authentication information such as passwords. Passive interception of network operation enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user. Some common password attack methods include,

- Looking Outside the Box
- Trojan Horses
- Intercepting
- Social Engineering Attack
- Password Guessing
- Dictionary Attack
- Hybrid Password guessing Attack
- Password Resetting Attack

- Rainbow Table Attack
- Key Loggers Attack
- Insider Attack
- Hijack Attack
- Wire Sniffing
- Replay Attack
- Denial-of-service Attacks
- Back door attacks

Looking Outside the Box

A major source of password comprise is the inattentiveness of users. The earliest hackers often obtained passwords by looking for clues in discarded computer printouts. The earliest hackers often obtained passwords by looking for clues in discarded printout. Since that time, operating system vendors thankfully have become more sophisticated about protecting password information. However, a significant percentage of password compromise cases still results from offline detection. Users tell their passwords to other users or write down their passwords in some easily accessible place.

Trojan Horses

In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form a of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. Trojan horse is a computer program that purports to do one thing but actually takes other unseen and malicious actions behind the scenes. One early form of the Trojan horse was a fake login screen. The screen looks just like the login screen used for the system, but when the user attempts to log in, the user name and password are captured and stored in some secret location accessible to the intruder. A Trojan horse may be widely redistributed as part of a computer virus. The term comes from Greek mythology about the Trojan War, as told in the Aeneid by Virgil and mentioned in the Odyssey by Homer. According to legend, the Greeks presented the citizens of troy with a large wooden horse in which they had secretly hidden their warriors. During the night, the warriors emerged from the wooden horse and overran the city.

Intercepting

This can be either an active attack or passive attack. In a network environment, a passive interception might involve someone who routinely monitors network traffic. Active interception might include putting a computer system between sender and receiver to capture information as it is sent. From the perceptive of interception, this process is covert. The last thing a person on an intercept mission wants is to be discovered. Packet sniffers and other tools that monitor network traffic can easily capture passwords transmitted over the network in clear text format form. Many classic TCP/IP utilities such as Telnet and the Remote Access Utilities or SNMP and Network Management Protocols were designed to transmit passwords in clear text form. Some later versions of these utilities offer password encryption or operate through secure channels. In their basic form, however the clear text password security of these

applications makes them hopelessly ill-suited for an open and hostile environment such as the internet. Interception mission occur for years without the knowledge of the intercept parties.

Social Engineering Attack

In a social engineering attack, someone attempts to obtain your password, while masquerading as a support technician or other authorized individual who needs your login information, relying on social engineering. Social engineering is the art of interacting with people either face to face or over the telephone and getting them to give out valuable information such as passwords. Social engineering relies on people's good nature and desire to help others. Many times, a help desk is the target of a social engineering attack because their job is to help people and recovering or resetting passwords is a common function of the help desk. The best defense against social engineering attacks is security awareness is security procedures for setting passwords.

Password Guessing

The most common type of attack is password guessing. Attackers can guess passwords locally or remotely using either a manual or automated approach. Password guessing isn't always difficult as you'd expect. Most networks aren't configured to require long and complex passwords, and an attackers need to find only one weak password to gain access to a network. Not all authentication protocols are equally effective against guessing attacks. For example, because LAN manager authentication is case sensitive, a password guessing attack against it doesn't need to consider whether letters in the password are uppercase or lowercase. Many tools can automate the process of typing password after password. Some common password guessing tools are Hydra for brute force attacks against terminal services and RDP connections.

Dictionary Attack

A dictionary attack is an attempt to identify your password by using common words, names of loved ones, pets, birth dates, address, and phone numbers. A dictionary attack begins with the dictionary, essentially a database of commonly used words to which the attacker can add custom words or conduct a forensic analysis, in which software scans text documents and adds all words to the dictionary. Some passwords are so simple or poorly formed that the intruder can easily guess them. You would be surprised how many users use a password that is same as their username. Some users use a street name, a maiden name, or the name of the child for a password, and some use easily guessable character combinations, such as 123456, abcde, or ddddd.

Hybrid password guessing

This is one of the more interesting attacks out there. In a sense, hybrid attacks come very close to how real human intruder think. Hybrid password guessing attacks assumes that network administrators push users to make their passwords at least slightly differ from a word that appears in a dictionary. A hybrid attack is a mixture of both a dictionary and brute force attack. That means that like a dictionary attack, you would provide a wordlist of passwords and a brute-force attack would be applied to each possible password in that list. Hybrid password guessing rules vary from tool to tool, but most mix uppercase and lowercase

characters, add numbers at the end of password. Technically the hybrid attack uses one or more dictionaries with common words, and one or more .rul files specifying mutation rules.

Password Reset Attacking

Attackers often find it much easier to reset passwords than to guess them. Many password cracking programs are actually password re setters. In most cases, the attackers boots from a floppy disk or CD-ROM to get around the typical windows protections. Most password re setters contain a bootable version of Linux that can mount NFTS volumes and can help you locate and reset the Administrator's password.

Rainbow Table Attack

Rainbow tables are more complex. Constructing a rainbow table requires two things: a hash function and a reduction function. The hashing function for a given set of Rainbow Tables must match the hashed password you want to recover. The reduction function must transform a hash into something usable as a password. A rainbow table is a list of pre-computed hashes- the numerical value of an encrypted password, used by most systems today and that's the hashes of all possible password combinations for any given hashing algorithm mind. The time it takes to crack a password using a rainbow table is reduced to the time it takes to look it up in the list.

Key Logger Attack

A hacker uses a program to track all of a user's keystrokes. So at the end of the day, everything the user has typed-including their logon IDs and passwords- have been recorded. A key logger attack is different than a brute force or dictionary attack in many ways. Not the least of which, the key logging problem is used is malware that must first make it onto the user's device. Key logger attacks are also different because stronger passwords don't provide much protection against them, which is one reason that multi-factor authentication (MFA) is becoming a must have for all business and organizations. The use of MFA is growing rapidly. Facebook, Google, PayPal now all offer MFA options. The security guidelines for many agencies and industries require MFA for anyone trying to log in off site.

Insider Attack

An insider attack involves someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task.

Hijack Attack

Hijack Attack in a hijack attack, a hacker takes over a session between you and another individual and disconnects the other individual from the communication. You still believe that you are talking to the original party and may send private information to the hacker by accident. In one type of hijacking, the perpetrator takes control of an established connection

while it is in progress. The attacker intercepts messages in a public key exchange and then transmits them, substituting their own public key for the requested one, so that the two original parties still spear to be communicating with each other directly. This attack may be used simply to gain access to the messages, or to enable the attacker to modify them before transmitting them.

Wire Sniffing

Most of the time when we talk of passive online attack we consider it as sniffing the password on wired or wireless networks. The password is captured during authentication phase and then compared to dictionary file or word list. The majority of sniffer tools are ideally suited to sniff data in hub environment. These tools are also known as passive sniffers as they passively wait for data to be sent before capturing the information. User account passwords are commonly hashed or encrypted when sent on the network to prevent unauthorized access and use. In such cases hacker use his special tools to crack password.

Replay Attack

Replay attacks are the network attacks in which an attacker spies the conversation between the sender and receiver and takes the authenticated information. It occurs when the hacker intercepts the password and en routes to the authentication server and then captures and resend the authentication packets for later authentication. In this manner, the hacker doesn't have to break the password or learn the password through MITM but rather captures the password and reuses the password authentication packets later to authenticate as the client.

Denial-of-service Attack

They prevent access to resources by users by users authorized to use those resources. An attacker may try to bring down an e-commerce website to prevent or deny usage by legitimate customers. DoS attacks are common on the internet, where they have hit large companies such as Amazon, Microsoft and AT&T. These attacks are often widely published in the media. Several types of attacks can occur in this category. These attacks can deny access to information, applications, systems, or communications. A DoS attack on a system crashes the operation system. A common DoS attack is to open as many TCP sessions as possible. This type of attack is called TCP SYN flood Dos attack. Two of the most common are the ping of death and the buffer overflow attack. The ping of death operates by sending Internet Control Message Protocol (ICMP) packets that are larger than the system can handle. Buffer overflow attacks attempt to put more data into the buffer than it can handle. Code red, slapper and slammer are attacks that took advantage of buffer overflows, sPing is an example of ping of death.

Back door Attacks

This can have two different meanings, the original term back door referred to troubleshooting and developer hooks into systems. During the development of a complicated operating system or application, programmers add back doors allow them to examine operations inside the code while the program is running. The second type of back door refers to gaining access to a network and inserting a program or utility that creates an entrance for an attacker. The program may allow a certain user to log in without a password or gain

administrative privileges. A number of tools exist to create a back door attack such as, back orifice, Subseven, NetBus and NetDevil. There are many more. Fortunately, most anti-virus software will recognize these attacks.

5. CONCLUSION

This paper provides so many types of password, authentication method and password attacks. User can use difference authentication method depending on their application to avoid password attacks.

References

[1] [1] Janardan Choubey, Bhaskar Choubey "Secure User Authentication in Internet Banking: A Qualitative Survey", *International Journal of Innovation, Management and Technology*, Vol. 4, No. 2, April 2013.

[2] Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider, "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication", *World Applied Sciences Journal* 19 (4): 439-444, 2012.

[3] Ari Juels, "RFID Security and Privacy: A Research Survey", *IEEE Journal on Selected Areas in Communications*, Volume 24, No. 2, Feb 2006.

[4] Priti Jadhao, Lalit Dole, "Survey on Authentication Password Techniques", *International Journal of Soft Computing and Engineering (IJSCE)*, Volume 3, Issue 2, May 2013.

[5] Prajitha M V, "A Survey on User Authentication Protocols", *International Journal of Computer Science Engineering*, Volume 3, Issue 1, Jan 2015.

[6] Bin Hu, Qi Xie, Yang Li, Automatic verification of password based authentication protocols using smart card (2011).

[7] G. E. Blonder, "Graphical passwords", United States Patent 5559961, 1996.

[8] A. Hiltgen, T. Kramp, and T. Weigold, "Secure internet banking authentication," *IEEE Security and Privacy*, Vol. 4, No. 2, pp. 21-29, 2006.

[9] Anand Sharma and Vishal Ojha, 2010. Password based authentication: Philosophical Survey. IEEE.

[10] Ahmed, A.A.E. and I. Traore, 2005. Anomaly Intrusion Detection Based on Biometrics, Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, IAW '05.

[11] B. Pinkas and T. Sander, "Securing passwords against dictionary at- tacks," in CCS '02: Proc. 9th ACM Conf. Computer Communications Security, New York, ACM, 2002, pp. 161-170.

[12] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in SSYM'99: Proc. 8th Conf. USENIX Security Symp., Berkeley, CA, USENIX Association, 1999, pp. 1.

[13] B. Parno, C. Kuo, and A. Perrig, "Phoolproof phishing prevention," *Financial Cryptography Data Security*, 2006, pp. 1-19.

[14] D. Florencio and C. Herley, "A large-scale study of web password habits," in WWW '07: Proc. 16th Int. Conf. World Wide Web., New York, ACM, 2007, pp. 657-666.

[15] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, "Multiple password interference in text passwords and click-based graphical passwords," in CCS '09: Proc. 16th ACM Conf. Computer Communications Security, New York, 2009, pp. 500-511.

[16] Muhammad Sharif, Tariq Faiz and Mudassar Raza, 2008. Time Signatures - An Implementation of Keystroke and Click Patterns for Practical and Secure.

[17] Hirotaka Tazawa and Takashi Katoh, 2010. A user authentication scheme using Multiple Passphrases and its arrangements. ISITA Taiwan.

[18] Dalia Abdul Hadi Abdul Ameer and Ahmed Abdulhakim Al-Absi, 2010. Anywhere On-Keyboard Password Technique. IEEE Student conference on Research and development 2010 Putrajaya Malaysia.

[19] Manabo Hirano and Tomohiro Umeda, 2009. T-PIM: Trusted password Input method against data stealing Malware IEEE 6 International Conference on IT.

[20] http://passcodes.org/security/password-attack-methods-and-prevention/

[21] http://computernetworkingnotes.com/network-security-acess-lists-standards-and extended/types-of-attack.html

[22] http://searchsecurity.techtarget.com/definition/digital-signature

[23] http://searchnetworking.techtarget.com/definition/Novell-Directory-Services

[24] http://searchsecurity.techtarget.com/definition/biometric-authentication

(Received 16 January 2016; accepted 29 January 2016)