© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2276-6848 | Volume: 06 Issue: 01 | Jan-April 2015

Enhancement of Password Authentication system is to prevent Security hacker's Attack

Vivek Kaushik*, Rahul Kadian**, CBS Group of Institutions.

Abstract: Battle between ethical or white hat Security hackers and malicious or black hat Security hackers is a long war, which has no end. While ethical Security hacker help to understand companies' their System security needs, malicious Security hackers intrudes illegally and harm network for their personal benefits. Objective Enhancement of Password Authentication system is to prevent Security hacker's Attack make remote servers more secure.

[I] INTRODUCTION

It is necessary to keep password safe and secure. There may be a chance to hack password by outside onlookers to access data provided by user. So, it is necessary to follow techniques to preserve password from onlookers to hack it. Several techniques are used here for password authentication. Public Key Info systems is one of technique used under public key infrastructure in which public keys are used to create to avoid password hacking. Limitation of this system is that user has to check validity of key each and every time in password system. It consumes more time for execution. Then, another system called Password only protocols or Password Authenticated Key Exchange or PAKE which does use public key system for password authentication. So, it is easy for users to use this system for real world applications.

Password Authenticated Key Exchange or PAKE is a class of cryptographic protocols that allow two parties sharing a password to authenticate each other without explicitly revealing password in process. PAKE protocols offer a potential improvement over current web authentication practices.

We examine three categories of issues

1) System security issues related to UI design;

2) System security issues related to browser's same origin policy

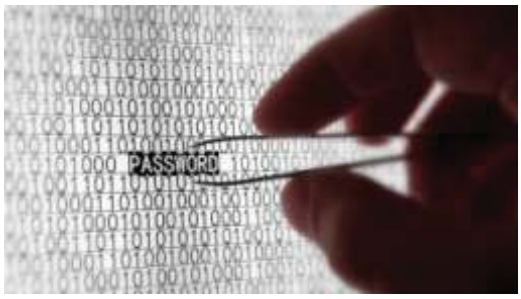
3) Potential hurdles to deployment. We propose potential solutions for some problems and identify areas for future work

[2] SECURITY HACKER

A **hacker** is person who seeks and exploits weaknesses in a computer(PC) system or computer(PC) network. Security hackers might be motivated by a multitude of reasons, such as protest challenge. Subculture evolved around Security hackers is often referred to as computer(PC) underground and is now a known community.

While other uses of word *Security hacker* exist that are not related to computer(PC) security system, such as referring to someone with an advanced understanding of computer(PC)s and computer(PC) networks security system, they are rarely used in mainstream context. They are subject to longstanding Security hacker definition controversy about term's true meaning.

In this controversy, term *Security hacker* is reclaimed by computer(PC) programmers who argue that someone who breaks into computers, whether computer (PC) criminal or computer (PC) security system expert, is more appropriately called a **cracker**.



Some white hat Security hackers claim that they also deserve title *Security hacker*, and that only black hats should be called *crackers*.

[III] TECHNIQUES OF HACKING

Vulnerability scanner

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Security hackers also commonly use port scanners. They check to see which ports on a specified computer(PC) are "open" or available to access computer(PC), and sometimes will detect what program or service is listening on that port, and its version number. Firewalls defend computers from intruders by limiting access to ports and machines.

Password cracking

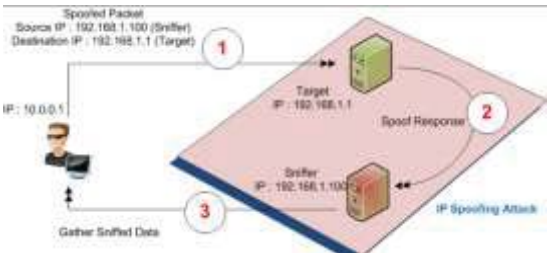
Password cracking is process of recovering passwords from information that has been stored in or transmitted by a computer(PC) system. A common approach is to repeatedly try guesses for password.

Packet sniffer

A packet sniffer is software that captures data packets, which can be used to capture passwords and other information in transit over network.

Spoofing attack or Phishing

A spoofing attack involves one program, system or website that successfully masquerades as another by falsifying information and is thereby treated as a trusted system by a user or another program—usually to fool programs, systems or users into revealing confidential information, such as user names and passwords.



Rootkit

A rootkit is a software that uses low-level, hard-to-detect methods to subvert control of an operating system from its legitimate operators. Rootkits usually obscure their installation and attempt to prevent their removal through a subversion of standard system security. They might include replacements for system binaries, making it virtually impossible for them to be detected by checking process tables.

Brute-force attack or exhaustive key search

It is a cryptanalytic attack that can be used against any encrypted information except for information encrypted in an information-theoretically secure manner. Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system if any exist that would make task easier. It consists of systematically checking all possible keys or passwords until correct one is found. In worst case, this would involve traversing entire search space.

Physical Attack

Searching password to an account is clearly possible though direct attacks such as brute force, dictionary or rainbow tables. However, They are also far from trivial to implement, and there are serious time-space trade-off concerns. In certain situations it can be preferable to crack passwords through less traditional means. The most basic of physical methods would be to actually physically force someone to give up their password for a very important account. This type of literal attack is commonly referred to as ―rubber hose cryptography" and is effective only when an

attacker who can be very persuasive is able to gain physical access to a person who knows password in question. If there are moral or logistical issues with such an attack, there are less invasive ways to obtain passwords as well. A side-channel attack is one which gathers information that leaks out of system in some way. most basic form of this would be to observe someone typing in their password ,perhaps with a well placed camera. With a tactic like this there is no need to look at password files, worry about salt values or create a chain of hashes; it is only necessary to be able to view terminal in which someone inputs a password.

A more sophisticated form of side-channel attack would be to recreate a password from sounds that typing on a keyboard generates. Especially on older keyboards, each input key generates a slightly different sound upon being pressed. Researchers at Berkeley have utilized extremely sensitive microphones to decipher which keys have been pressed on a keyboard by just sound.

[IV] PASSWORD-AUTHENTICATED KEY AGREEMENT

In cryptography, a **password-authenticated key agreement** method is an interactive method for two or more parties to establish cryptographic keys based on one or more party's knowledge of a password. An important property is that an eavesdropper or man in middle cannot obtain enough information to be able to brute force guess a password without further interactions with parties for each guesses. This means that strong security system can be obtained using weak passwords.

Simple Password Exponential Key Exchange

Step	Alice	Bob
1	Parameter: p	
2	$G = H(password)^2$	$H(password)^2 = G$
3	$A = \text{random}()$ $a = G^A \pmod p$	$\text{random}() = B$ $G^B \pmod p = b$
4	$a \longrightarrow$ $\longleftarrow b$	
5	$K = G^{BA} \pmod p = b^A \pmod p$	$a^B \pmod p = G^{AB} \pmod p = K$
6	$\longleftarrow E_K(data) \longrightarrow$	

[V] TYPES

Password-authenticated key agreement generally encompasses methods such as:

- Balanced password-authenticated key exchange method
- Augmented password-authenticated key exchange method
- Password-authenticated key retrieval method
- Multi-server methods
- Multi-party methods

In most stringent password-only security system models, there is no requirement for user of method to remember any secret or public information other than password.

[VI]PAKE

Password authenticated key exchange is where two or more parties, based only on their knowledge of a password, establish a cryptographic key using an exchange of messages, such that an unauthorized party , one who controls communication channel but does not possess password cannot participate in method and is constrained as much as possible from brute force guessing password. The optimal case yields exactly one guess per run exchange. Two forms of PAKE are Balanced and Augmented methods.

Balanced PAKE allows parties that use same password to negotiate and authenticate a shared key. Examples are:

- Encrypted Key Exchange
- PAK and PPK
- Simple password exponential key exchange
- Dragonfly-- IEEE Std 802.11-2012, RFC 5931, RFC 6617
- SPAKE1 and SPAKE2
- J-PAKE or Password Authenticated Key Exchange by Juggling -- A variant that is probably not encumbered by patents.
- ITU-T Recommendation X.1035

Augmented PAKE is a variation applicable to client/server scenarios, in which server does not store password-equivalent data. This means that an attacker that stole server information still cannot masquerade as client unless they first perform a brute force search for password. Examples include:

- AMP
- Augmented-EKE
- B-SPEKE
- PAK-Z
- Secure Remote Password protocol -- designed to be not encumbered by patents.
- AugPAKE (RFC 6628)

[VII] OBJECTIVE OF RESEARCH

The objective of research is to make password authenticated key exchange system more secure and safe by making some customization in existing mechanism. We perform a systematic investigation of various practical issues and challenges in deploying PAKE for web authentication. Although many PAKE protocols have been proposed, there is little momentum for integrating PAKE protocols into web authentication. One contribution we hope to make in this research is to help raise awareness of issues inhibiting widespread adoption of PAKE, and help stimulate future work and discussion in this area.

[VIII] REFERENCES

1. Boyko, V.; P. MacKenzie; S. Patel (2000). "Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman". Advances in Cryptology -- Eurocrypt 2000, LNCS. Lecture Notes in Computer Science (Springer-Verlag) **1807**: 156. doi:10.1007/3-540-45539-6_12. ISBN 978-3-540-67517-4.

2. Abdalla, M.; D. Pointcheval (2005). "Simple Password-Based Encrypted Key Exchange Protocols" (PDF). Topics in Cryptology – CT-RSA 2005. Lecture Notes in Computer Science (Springer Berlin Heidelberg) **3376**: 191–208. doi:10.1007/978-3-540-30574-3_14. ISBN 978-3-540-24399-1.
3. Bellare, M.; D. Pointcheval; P. Rogaway (2000). "Authenticated Key Exchange Secure against Dictionary Attacks". Advances in Cryptology -- Eurocrypt 2000 LNCS. Lecture Notes in Computer Science (Springer-Verlag) **1807**: 139. doi:10.1007/3-540-45539-6_11. ISBN 978-3-540-67517-4.
4. Bellovin, S. M.; M. Merritt (May 1992). "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks". Proceedings of the I.E.E.E. Symposium on Research in Security and Privacy (Oakland): 72. doi:10.1109/RISP.1992.213269. ISBN 0-8186-2825-1.
5. Ford, W.; B. Kaliski (14–16 June 2000). "Server-Assisted Generation of a Strong Secret from a Password". Proceedings of the IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (Gaithersburg MD: NIST): 176. doi:10.1109/ENABL.2000.883724. ISBN 0-7695-0798-0.
6. Goldreich, O.; Y. Lindell (2001). "Session-Key Generation Using Human Passwords Only". Advances in Cryptology -- Crypto 2001 LNCS (Springer-Verlag) **2139**.
7. "IEEE Std 1363.2-2008: IEEE Standard Specifications for Password-Based Public-Key Cryptographic Techniques". IEEE. 2009.