© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

REVIEW ON CLOUD SERVER SECURITY USING PASSWORD AUTHENTICATED KEY EXCHANGE

[1]Payal Rani, Research Scholar, Department of CSA, CDLU Sirsa
[2]Monika Bansal, Assistant Professor, Deptt. Of CSA ,CDLU ,Sirsa

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.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.

1. Introduction to Cloud Computing

Cloud computing is set of resources that are being allocated on demand. Cloud computing proposes new ways to provide services. These new innovative, technical and pricing opportunities bring changes in the way business operated. Cloud computing is the matchless computing technology.

Cloud computing is a new label to an old idea. Cloud computing is a collection of resources and serviced provided by cloud service provider through internet. Cloud services are distributed from data canters sited all over the world. Cloud computing makes possible for its users to use the virtual resources via internet as per requirements. Cloud computing grabbed the spotlight in few years. General example of cloud services are Google Engine, Oracle Cloud, Office 365. As the cloud computing is growing rapidly this also leads to severe security concerns. Lack of security is the only barrier in wide adoption of cloud computing. The rapid growth of cloud computing has brought many security challenges for users and providers.

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. However, cloud computing technology challenges many traditional approaches to datacenter and enterprise application design and management. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures. An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of "applied security" and that similar security principles that apply in shared multi-user mainframe security models apply with cloud security. It is the very nature of cloud computing-based services, private or public, that promote external management of provided services. This delivers great incentive to cloud computing service providers to prioritize building and maintaining strong management of secure services. Security issues have been categorized into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues. Solutions to various cloud security issues vary, from cryptography, particularly

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

public key infrastructure (PKI), to use of multiple cloud providers, standardization of APIs, and improving virtual machine support.

2. LITERATURE REVIEW

Internet is biggest era of whole world. To access services offered through internet, several web services have been used .The users who are accessing web services must create username and password for website they had chosen. 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 same 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 (PAKE) which does use public key system for password authentication. So, it is easy for users to use same system for real world applications. The pseudo random and hash password model is a type of model which is used under password authentication system. Same research work describes use of random numeric values made under hash based mechanism for secure password system, specifically referring to internet password applications or services. Random numeric values are normally used to verify passwords for cryptography-based computer security systems. In framework of cryptographic applications, there is a chance for onlookers to hack password and to access users' confidential information. For same type of attack, method which uses key system is inefficient. Since it takes more time to complete and result will not be an appropriate one. So in order to generate an efficient system random numeric value generator is used. Same generates a numeric value which changes every time. Only sender and receiver would know about password details. None other can know password to access details. Since numeric values generated may change, it is difficult for hackers to hack password. Same random password generated system is mainly used to avoid online dictionary attack.

3. PROBLEM FORMULATION

A **hacker** is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may bmotivated by a multitude of reasons, such as profit, protest, or challenge. The subculture that has evolved around hackers is often referred to as the computer underground and is now a known community. While other uses of the word *hacker* exist that are not related to computer security, such as referring to someone with an advanced understanding of computers and computer networks, they are rarely used in mainstream context. They are subject to the longstanding hacker definition controversy about the term's true meaning.

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

Some white hat hackers claim that they also deserve the title *hacker*, and that only black hats should be called *crackers*.Security exploitsA security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are SQL injection, Cross Site Scripting and Cross Site Request Forgery which abuse security holes that may result from substandard programming practice. Other exploits would be able to be used through FTP, HTTP, PHP, SSH, Telnet and some web-pages. These are very common in website/domain hacking.Techniques ***Vulnerability scanner***

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer, 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, but they can still be circumvented.) ***Password cracking*** Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

approach is to repeatedly try guesses for the password. ***Packet sniffer*** A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network. ***Spoofing attack (Phishing)*** A spoofing attack involves one program, system or website that successfully masquerades as another by falsifying data 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.

4.RESEARCH METHODOLOGY

The **Password Authenticated Key Exchange by Juggling** or J-PAKE is a password-authenticated key agreement protocol. This protocol allows two parties to establiprivate and authenticated communication solely based on their shared low-entropy password without requiring a Public Key Infrastructure. It provides mutual authentication to key exchange, a feature that is lacking in Diffie-Hellman key exchange protocol.Two parties, Mr. Alice and Mr. Bob, agree on a group G with generator g of prime order q in which discrete log problem is hard. Typically a Schnorr group is used. In general, J-PAKE can use any prime order group that is suitable for public key cryptography, including Elliptic curve cryptography. Let s be their shared low-entropy secret, which can be a password or a hash of a password (s<>0). protocol executes in two rounds..

5. PROPOSED WORK

J-PAKE has been implemented in OpenSSL and OpenSSH as an experimental authentication protocol. It was removed from OpenSSH source code at end of January 2014. It has also been implemented in NSS and is used by Firefox Sync. Since February 2013, J-PAKE has been added to lightweight API in Bouncycastle. **PAKE-Based Web Authentication**

PAKE is a class of cryptographic protocols that allow two parties to establish a secret key based on a shared password. Since its proposal, PAKE has been studied extensively and many protocols have been proposed. In PAKE-based web authentication, when a user wishes to authenticate herself to a website, she enters her password, and browser and server run an interactive PAKE protocol to establish a session key based on user's password without explicitly revealing password in process. browser and server can prove to each other they derived same key. If protocol fails, browser can alert user, indicating that server does not know password that user entered. derived key can also be used to encrypt and authenticate their future communication between two parties. The following notations are used:

o Mr. A: assumed identity of first party in protocol o Mr. B: assumed identity of second party in protocol o s: a low-entropy secret shared between Mr. A and Mr. B o plarge prime o q: a large prime divisor of p-1 Zp*: a multiplicative group of integers modulo p o Gq: a subgroup of Zp* with primer order q o g: a generator of Gq

6. SOFTWARE USED

- Operating System Windows 7 Home premium
- Front end Use Java Language
- Framework Eclipse
- Back end Text Files

7. SCOPE OF RESEARCH

Cloud computing offers many benefits, but it also is vulnerable to threats. One of the main threat exist today is the problem of unauthorized users or entities. For avoiding this problem the new technique is developed in this cloud computing is that data owners may share their outsourced data with a large number of users, who might want to only retrieve certain specific data files they are interested in during a given session.

J-PAKE-based web authentication is designed to reduce attack surface of password leakage by using J-PAKE protocol instead of current form-based approach for authentication and key establishment. However, to gain such benefits in a real deployment, a few important USER INTERFACE issues need to be addressed beyond simply implementing J-PAKE cryptographic protocol, otherwise, an attacker could exploit weaknesses in USER INTERFACE to fool or confuse computer user and steal computer user's password.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

We revisit dilemma of J-PAKE-based web authentication, and investigate various issues that might inhibit its widespread adoption. We believe that it is important to ask and think about these questions, and we hope to stimulate discussions on this topic. We conclude by summarizing good, bad and challenges of deploying J-PAKE-based web authentication.

PROS. PAKE-based web authentication does have clear benefits over today's approach. First, when combined with right USER INTERFACE, J-PAKE can reduce attack surface of web-based authentication. Second, although careless computer users may still fall prey to social engineering attacks, at very least, we can protect security-conscious computer users, and relieve them of burden of deciding whether to trust a website. More-over, with proper computer user education, we can hope to raise global awareness of computer users over time.

[8] Future Scope & Conclusion

Cloud computing is still evolving but its benefits are enormous. Cloud computing provides excellent support for amazing infrastructures, applications and services such as shared resource pool, broad network base, reduced IT cost or rapid elasticity of the cloud to handle varying customers demands as well as cloud computing various service and deployment models which is part of the main reason for adopting this computing system. Thus this makes cloud computing an open shared system volatile to security breaches and other challenges.

So there is need to focus on solutions of the various challenges to maintain the dependence level of organization for deploying the cloud computing without any hesitation and also the need of technical support for elastic scalability to serve the ever pressing demand of the customer.

Hacking has both its benefits and risks. Hackers are very diverse. They may bankrupt a company or may protect the data, increasing the revenues for the company. The battle between the ethical or white hat hackers and the malicious or black hat hackers is a long war, which has no end. While ethical hacker help to understand the companies' their security needs, the malicious hackers intrudes illegally and harm the network for their personal benefits. An Ethical and creative hacking is significant in network security, in order to ensure that the company's information is well protected and secure. At the same time it allows the company to identify, and in turn, to take remedial measures to rectify the loopholes that exists in the security system, which may allow a malicious hacker to breach their security system. They help organizations to understand the present hidden problems in their servers and corporate network. The study also reveals that the valid users are the ethical hackers, till their intensions are clear otherwise they are a great threat, as they have the access to every piece of information of the organization, as compare to total and semi outsiders.

This also concludes that hacking is an important aspect of computer world. It deals with both sides of being good and bad. Ethical hacking plays a vital role in maintaining and saving a lot of secret information, whereas malicious hacking can destroy everything. What all depends is the intension of the hacker. It is almost impossible to fill a gap between ethical and malicious hacking as human mind cannot be conquered, but security measures can be tighten.

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.
8. Katz, J.; R. Ostrovsky; M. Yung (2001). "Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords" **2045**. Springer-Vergal.
9. T. Wu. The SRP-3 Secure Remote Password Protocol. IETF RFC 2945.
10. D. Taylor, T. Wu, N. Mavrogiannopoulos, T. Perrin. Using the Secure Remote Password (SRP) Protocol for TLS Authentication. IETF RFC 5054.
11. D. Harkins, G.Zorn. Extensible Authentication Protocol (EAP) Authentication Using Only a Password. IETF RFC 5931.
12. Y. Sheffer, G. Zorn, H. Tschofenig, S. Fluhrer. An EAP Authentication Method Based on the Encrypted Key Exchange (EKE) Protocol. IETF RFC 6124.
13. D. Harkins. Secure Pre-Shared Key (PSK) Authentication for the Internet Key Exchange Protocol (IKE). IETF RFC 6617.
14. ISO/IEC 11770-4:2006 Information technology—Security techniques—Key management—Part 4: Mechanisms based on weak secrets.
15. "IEEE Std 802.11-2012: IEEE Standard for Information Technology-- Part 11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification". IEEE. 2012.
16. F. Hao, P. Ryan. Password Authenticated Key Exchange by Juggling. Proceedings of the 16th International Workshop on Security Protocols, 2008.