IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.116118

Dynamic Key Generation On Asymmetric Key Cryptography

Snehal D. Hiware[1], Ass. Prof. S. K. Purve[2], Ass. Prof. P. T. Tandekar[3]

Department of Computer Science and Engineering, SSCET Bhadravati[1-3]

Abstract: There is a new and better password key generation method is proposed in this paper. This algorithm is going to provide fast and secure ki generation in public Cryptography world in this case we are going to use the RSA algorithm with the help of random numbers (Dynamic keys) without waste of offline and online dictionary malware. In this new proposed algorithm is closely related to prime number generation techniques that can creating a new pair of keys between authorised users. Methods are much important for some uses, i.e. reducing password guessing and knowing probability by others in other ways. And this propose class of secure password generating method is provides safest and continuous transaction between authorised users.

Keywords : Dynamic keys, RSA, Asymmetric Key Cryptography, prime number

I. INTRODUCTION

In all the world of computer system which can be accessed by a user is protected by password. Nowadays users data can be surely protected in Computer world and those operations can be secured with the password usage. Password can be only authorised by users in client end and receiver end. In the online guessing type of attack, the attacker repeatedly makes guesses of the password, most likely first and test them by attempt to log on to the system. In this model our system has acquired and implemented “account lockout”, by locking the system after a certain number. Let’s say b is unsuccessful log on attempts which can limits there attempts and effectiveness of the attack. Also in offline guessing type of attack the attacker gets hold of some test data from the system that enables him to test password guesses. We distinguish two kinds of offline attacks. This information good for instance be a Windows SAM Database or more generally to secure hash of a password. In an incomplete attack the attacker is only willing to take certain computational effort, a number of L guesses, in the attack, dear by finding the password only with the certain probability. So to illustrate this, suppose that an attacker has the SHA-1 hash of the password. If the attacker is willing to let the gases versus run on a 1 GHz Pentium machine for a day this means he can willingly to perform about 236 tries; one might find it as an acceptable that the probability of success is at most 1%.

The main issues of this paper deals with the generation of passwords that they are on the one hand have functional requirements and that they are “small” And also on the other hand have the security requirements as they are adequately resistant against both online and offline attacks, complete as incomplete. Sach passwords are specifically applicable in the context of OTP (One Time Password).

A. Concept Of Public Key

Cryptography Two keys are used in public key cryptography. With help of two keys, we can reduces the probability of guessing or occur correct keys. With the public key one could encrypt messages, and Decrypt them with the private key. Thus the owner of the private key would be the only one who could decrypt the messages, but anyone knowing another idea that was observed was that of a key exchange. In a two-party communication it would be useful to generate a common secret key for bulk encryption using a secret key cryptosystem; public could send them in privacy. The public key cryptosystem algorithms have the following important characteristics

1. It is computationally infeasible for a intruder to determine the decryption key given by the owner, even with knowledge of the cryptographic algorithm and the encryption key.
2. Either one of the two related key can be used for encryption, while the other used for decryption.

B. Password Guessing and Cracking

Attackers attempt to determine weak passwords and to recover passwords from password hashes through two types of techniques: guessing and cracking. Guessing involves repeatedly attempting to authenticate using default passwords, dictionary words, and other possible passwords. Cracking is the process of an attacker recovering cryptographic password hashes and using various analysis methods to attempt to identify a character string that will produce one of these hashes, thereby being the equivalent of the password to the targeted system. Guessing can be attempted by any attacker that can access the authentication interface, whereas cracking can only be attempted by an attacker who has already gained access

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.116118

to password hashes. This section describes guessing and cracking in detail and recommends strategies for mitigating these threat. C. Guessing

There are several forms of guessing. In a brute force attack, the attacker attempts to guess the password using all possible combinations of characters from a given character set and for passwords up to a given length. This method is likely to take an extensive amount of time if there are many combinations to be tested. In a dictionary attack, the attacker attempts to guess the password using a list of possible passwords. The list may contain numbers, letters, and symbols, but is not an exhaustive list of all possible passwords or combinations that could create a password. In a hybrid attack, the attacker uses a dictionary that contains possible passwords and then uses variations through brute force methods of the original passwords in the dictionary to create new potential passwords. Since the attacker is adding characters and in some cases replacing characters based on a rule set in a controlled manner, the attack is more exhaustive than a dictionary attack but takes less time than a brute force attack. Another form of guessing attack is to search the victim's information for possible password content, such as family member names or birthdates.

D. Cracking

Cracking involves attempting to discover a character string that will produce the same encrypted hash as the target password. The discovered string may be the actual password or another password that happens to produce the same hash. If the hash algorithm is weak, cracking may be much easier. Hash functions should be one-way, otherwise attackers that can access hashes may be able to identify passwords from them and successfully authenticate. Another example of a hash algorithm weakness is that some algorithms do not use salting. Salting is the inclusion of a random value in the password hashing process that greatly decreases the likelihood of identical passwords returning the same hash. If two users choose the same password, salting can make it highly unlikely that their hashes are the same.

II. EXISTING ALGORITHM

We have number of public key algorithm is available in this world for secure communication. The one of strongest algorithm is RSA public key cryptography. RSA has been widely used for establishing secure communication channels and for authenticating the identity of service providers over insecure communication mediums. In the authentication scheme, the server implements public key authentication with clients by signing a unique message from the client with its private key, thus creating what is called a digital signature. The signature is then returned to the client, which verifies it using the server's known public key

The algorithm flow is:

• To encrypt a message M the sender:

– obtains public key of recipient

KU={e,N}

– computes: C=Me mod N, where

0≤M<N

• to decrypt the ciphertext C the owner:

– uses their private key KR={d,p,q}

– computes: M=Cd mod N=(Me

)

d mod

N=Med mod N

– note that the message M must be smaller than the modulus N (block if needed)

• From Euler's theorem – In RSA, n=pq and 0<m<n, where p&q are prime numbers and n&m are integers

– m

kΦ(n)+1=mk(p-1)(q-1)+1 where Φ(pq)=(p- 1)(q-1)

– Ed=k Φ(n)+1 ie ed≡1 mod Φ(n) and d ≡ e -1 mod Φ(n) where, e with gcd(Φ(n),e)=1; 1<e< Φ(n)

III. DYNAMICS KEYS

RSA is one of powerful algorithm with static prime numbers. RAS entire key establishment only based on two prime numbers. If once prime numbers identified or stolen by others, then all further message transaction will move to insecure channel. So in this new technique we create different set of keys i.e. prime numbers for secure all further transaction with help of new keys. Dynamic key establishment based on only prime number generation.

A dynamic key theory is described and analyzed. We discuss the security requirements for the sequence of dynamic keys and how they are used as a guide to build dynamic key generation functions. Based on that guide, we present a family of dynamic key generation functions. The dynamic key sequence created by this family of dynamic key generation functions is examined and analyzed. The analysis shows the advantages of dynamic keys in both security and efficiency. In the

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022
DOI: 10.17148/IJARCCE.2022.116118

security analysis, we show that while one compromised dynamic key exposes one message, the other messages in the session and system are still secure. Although perfect secrecy from onetime pad is impossible, the security of cryptographic system using dynamic key is close to one-time pad. Besides minimizing cryptanalysis attack risks, dynamic keys are also able to prevent replay-attacks on authentication and payment systems. In terms of performance, by storing intermediary keys, dynamic keys used as one-time symmetric cryptographic keys can achieve high levels of security without scarifying performance by increasing key size. Because the dynamic keys are generated online, there is no key exchange before every encryption. A study is conducted to find the most appropriate sequence size and dynamic key lifetime to balance between security and performance. Hence, the dynamic key generation scheme can adjust to suit different applications requiring different security levels.

IV. ONE TIME PASSWORD

The idea of the one-time password was firstly introduced by Lamport in 1981. In a one-time password system, both client and server mutually agree to share a sequence of one-time passwords for authentication. Every authentication request uses a different password in the password sequence. Therefore, the one-time password system can prevent third parties from extracting authentication passwords via eavesdropping. There are two ways to share the sequence of passwords in one-time password systems. The first approach uses a mathematical algorithm to generate the sequence of passwords. A new password is generated from the previous passwords. This approach relies heavily on the synchronization index of the current password in the password sequence. The second approach is based on the synchronous time between client and server to generate the sequence of passwords.
Each password has a short life-time.
Authentication using the password is valid within that time period. Any attacks launched by reusing the password after the expired time of password are unsuccessful. This approach requires time synchronization between clients and servers. Conversely, the adversary can still gain unauthorized access by reusing password attacks within its life-time.

V. CONCLUSION

In this propose model can provide more secured RSA public key cryptography with dynamic keys. This method also provide accurate random number compared to previous normal implementation techniques, while occupying lovely the same amount of hardware resources.
This new technique can generates random numbers without need of secret seeds and also reduces the time requirement for generating random numbers. This paper describes the various techniques available for the prevention of denial of service attacks. The information contains the lifetime of the packet. So they purpose a new method along with the existing packet marking technique.

REFERENCES

[1] IEEE Std 1363-2000"IEEE Standard Specifications for public - Key Cryptography" IEEE Computer Society, August 29,2000.
[2] ISO/IEC WD18032"Prime number generation.Working draft" April 18, 2001
[3] Matsumoto,M.and Nishimura,T. Mersenne twister"a 623- dimensionally equidistributed uniform pseudo-random number generator" ACM Transactions on Modeling and Computer Simulation (TOMACS) 8(1). 3-30.
[4] Matsumoto, M. and Nishimura, T. Dynamic Creation of "Pseudorandom number generator. in Niederreiter, E.H. and Spanier, J. eds. Monte Carlo and Quasi-Monte Carlo Methods", Springer, 2000, 56-69
[5] Shui Yu, Member, IEEE, Wanlei Zhou, Senior
Member, IEEE, "Traceback of DDoS Attacks Using Entropy Variations", IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 3, pp 412-425, March 2011.
[6] A Survey on Packrat Parser by Prof. S. K. Purve Sir.