International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 26th Dec 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue12

10.48047/IJIEMR/V11/ISSUE 12/229

TITLE: A STUDY OF REVOCATION OF KEYS IN CRYPTOGRAPHIC SYSTEMS AND KEY EXCHANGE WITH ENTITIES AUTHENTICATION

Volume 11, ISSUE 12, Pages: 1750-1757

Paper Authors **SASIKALA RASAMSETTY, DR. RAJEEV YADAV**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A STUDY OF REVOCATION OF KEYS IN CRYPTOGRAPHIC SYSTEMS AND KEY EXCHANGE WITH ENTITIES AUTHENTICATION

SASIKALA RASAMSETTY, DR. RAJEEV YADAV

DESIGNATION- RESEARCH SCHOLAR MONAD UNIVERSITY HAPUR U.P
DESIGNATION- (PROFESSOR) MONAD UNIVERSITY HAPUR U.P

ABSTRACT

Different cryptographic criteria, such as the key's length, the security of the underlying cryptographic algorithms, the channel via which the key is sent, the types of attacks that can be launched, and the computing power available to crack the key, all contribute to the key's expected lifetime. Key leakage is a major concern for crypto systems, however if the key length is sufficiently large, the current key length should be fine for a long time. Any key that has been compromised in any way (such as through insecure media, a man-in-the-middle attack, a short key length, or cryptographic attacks) must be revoked. In order to prevent algorithmic weaknesses that shorten the lifespan of keys, protect against various attacks, reduce the system's exposure, and prevent certain catastrophic failures in cryptography (for example, AES GCM mode loses protection if more than 64 GB is encrypted on the same key), key revocation is necessary. Key management frameworks are crucial for effective handling of keys. The framework not only specifies how the key should be handled at certain points in its lifetime, but also defines those stages.

KEYWORDS: Cryptographic Systems, Key Exchange, Entities Authentication, cryptographic attacks

INTRODUCTION

System assesses the remaining cryptographic period of keys and advises revocation based on the desired likelihood. The suggested model estimates the amount of time until the next key compromise based on the past history of key compromise, revocation, expiration, and the desired probability of key compromise in the near future. The system calculates the likely remaining lifetime of a compromised key based on the user's input of the desired probability. Assume the current capability to compute is 1. After a t-second delay, the processing power is 1 plus P times t. Here, the fluctuation in processing power is represented by the symbol Pt.

In the absence of any increase or decrease in computing capability after the t-second interval, Pt will be equal to zero. If a certain number of events occurs at a known constant rate and independently of each other, then the likelihood of these events occurring in a given time period is expressed by the Poisson distribution, which is a discrete probability distribution. It is presumed that if a key is lost or stolen, it will not compromise any other keys in the system. The proposed model is based on the Poisson distribution, which is consistent with the notion of key independence. This allows us to calculate the Poisson interval's likelihood of a key compromise.

KEY UPDATE

Let's assume that all cryptographic keys are the same length. The oldest key is discarded if F(t) is greater than a predetermined value. Criticality of the cryptographic application and key length determine a set threshold value. If the information is really sensitive and vital, the key should only be changed with a small percentage of success. The threshold value should consequently be lowered. If there is even a 0.001 percent probability of key compromise, the administration should have a policy to replace the key immediately. In this scenario, the cut-off is a mere 0.001. Alternatively, the administration may conclude that a 0.05% possibility of key compromise necessitates key replacement for less vital data. In this scenario, keys will be updated less frequently.

KEY EXCHANGE WITH ENTITIES AUTHENTICATION

By exchanging messages through an insecure channel, the Diffie-Hellman key exchange protocol makes it possible to find a shared secret key without first physically meeting. The scope of the Diffie-Hellman key exchange protocol is restricted to that of key exchange. This protocol is susceptible to man-in-the-middle attacks and impersonation attacks since entities are not authenticated. A research article on the Diffie-Hellma key exchange protocol was presented by Nan Li to counter the man-in-the-middle attack. It has been noted that impersonation attacks continue to plague Nanli's protocol.

Let ‘a’ is a number and power modulo p of this number generates all integer from 1 to p-1, then ‘a’ is called a generator of prime number ‘p’. Generated numbers from 1 to p-1 are : $a(mod)p$,$a^2(mod)p$,.....$a^{p-1}(mod)p$.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

These integers from 1 to p-1, make a form of permutation. For an integer b,{b:b<p}, prime number 'p' , and generator 'a'of prime number 'p' , 'b' is obtained as $b = a^i (mod) p$; where 0≤ i ≤(p-1).

In this case, we refer to 'i' as the discrete logarithm of 'b' on base 'a' modulo 'p'. For convenience, we can abbreviate ('i') as $d.\log_{a,p}(b)$. The public parameters used to characterize the key exchange protocol are the integer " and the prime number 'q,' both of which are known to the public.

The integer 'α' is a generator of 'q'.

User A selects one time random number (private key) X_A , such that X_A < q and computes public key parameter $Y_A = (\alpha^{(X_A)}) \bmod q$. A new random integer is chosen by User B for use as its private key, and its public key is calculated as $Y_B = (\alpha^{(X_B)}) \bmod q$.

The X value is kept secret on both ends, whereas the Y value is shared openly. The formula for User B's Key is $k = ((Y_A)^{(X_B)}) \bmod q$.

In above calculations, computed key is same.

$K = ((Y_B)^{(X_A)}) \bmod q$

But $Y_B = \alpha^{(X_B)} (mod) q$, therefore by putting the value of Y_B in above equation

$= ((\alpha^{(X_B)}) \bmod q)^{(X_A)}) \bmod q$

$= (\alpha(XB)\ (XA)) \bmod q$

Now after applying the commutative property

$= (\alpha(XA)\ (XB)) \bmod q$

$= (((\alpha(XA)) \bmod q)\ (XB)) \bmod q$ But $Y_A = \alpha^{(X_A)} (mod) q$, therefore $= ((Y_A)^{(X_B)}) \bmod q$.

Because of this, the secret key is the same for both parties. Since XA and XB are protected, an adversary can only use YA and YB to attack.,α, to unlock the door, q, and. So, to obtain the key, an adversary must first solve the discrete logarithm problem.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

SECURITY ANALYSIS

In this case, it is clear that User B will take the following action if User A attempts to impersonate User B. An additional user performs computations $H(N_1 \oplus P_B || ID_A)$ User B will suspect impersonation if the computed value does not match the value given by the authentication server in Step 3. After that, user B says they never talked to the sender.

EUCLIDEAN ALGORITHM, BEZOUT'S IDENTITY AND EXTENDED EUCLIDEAN ALGORITHM

1. Euclidean Algorithm

Around 300 B.C., the Euclidean algorithm made its debut in print. The gcd of two numbers can be calculated with this approach. Say a and c's greatest common divisor is d. gcd(a, c) = d.

Algorithm: (Input integers *a* and c with $a \geq c$, $a \neq 0$ and $c \neq 0$):

1. While c > 0, do

   I. Set r = a mod c,

   II. a = c,

   III. c = r 2. gcd (d)=a

2. Return d.

2. Bezout's identity

Two integers x and y exist, where at least one of them is not zero, for any two integers a and b. d=gcd(a, b) = xa + yb.

3. Extended Euclidean Algorithm

The gcd of two positive integers a and c can be calculated with this approach, as can the values of two other numbers, w and z, such that d=gcd(a, c) = wa + zc.

Algorithm: (Input integers *a* and *c* with $a \geq c$, $a \neq 0$ and $c \neq 0$):

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

1. If c = 0 then set z = 0, w = 1, d = a and return(d, w, z).

2. Set $w_1 = 0$, $w_2 = 1$, $z_1 = 1$ and $z_2 = 0$

3. While c > 0, do

4. q = floor(a/c), r = a - qc, $w = w_2 - qw_1$, $z = z_2 - qz_1$.

5. a = c, c = r, $w_2 = w_1$, $w_1 = w$, $z_2 = z_1$, $z_1 = z$.

6. Set d = a, $w = w_2$, $z = z_2$, and return(d, w, z).

ALGEBRAIC GROUP

Group theory is the branch of mathematics that investigates these algebraic structures. A group is a collection of elements and a binary operation satisfying the following conditions:-

(i) Closure

(ii) Associative

(iii) Identity

(iv) Inverse

Example: Let G = {- - - -3,-2,-1,0,1,2,3,- - - -} is a group over addition with 0 as identity element then

(i) Closure property

If a,c ε G then (a+c) ε G

(ii) Associative property

If a,c,d ε G then a+(c+d)=(a+c)+d

(iii) Identity property

If b ε G then b+0=0+b=b

(iv) Inverse property

For each a there exists an element c in G such that a+c=0=c+a

The fields of materials science, chemistry, physics, etc., all benefit greatly from the study of group theory. Group theory plays a crucial role in public key cryptography. Group theory is the foundation of public-key cryptography techniques.

CONCLUSION

The ability to revoke a key before its expiration is a crucial feature. Limiting the quantity of data that can be encrypted with a given key, protecting against various attacks, and safeguarding against present and future algorithmic weaknesses that lower key lifespan all necessitate the revocation of keys. A key revocation model is developed to estimate the time required to revoke the key. The efficiency of cryptographic key management is improved by the suggested key revocation model. Due to the fact that the Diffie-Hellman key exchange protocol does not include any mechanisms for authenticating entities. A man-in-the-middle attack can be performed against the Diffie-Hellman protocol. To prevent the man-in-the-middle attack, Nanli presented a study on the Diffie-Hellman key exchange protocol. Analyzing Nanli's method for preventing the man-in-the-middle attack in the Diffie-Hellman key exchange protocol reveals that impersonation attacks can still be carried out using this method. The proposed method eliminates the vulnerability to impersonation attacks seen in Nanli's method by doing two comparisons of hash values. Using a destination-side authentication mechanism and a pair of hash comparisons, it prevents attacks such as replay, man-in-the-middle, and impersonation.

REFERENCES

- N. Li, “Research on Diffie – Hellman Key, Exchange Protocol,” in *IEEE 2nd International Conference, on Computer Engineering and Technology*, 2010, pp. 634–637.

- A. Joux, "A one round protocol for tripartite diffie-hellman," in *4th International Symposium on Algorithmic Number Theory*, 2000, pp. 385–394.
- M. Steiner, G. Tsudik, and M. Waidner, "Diffie-Hellman Key Distribution Extended to Group Communication," in *CCS '96 Proceedings of the 3rd ACM conference on Computer and communications security*, 1996, pp. 31–37.
- A. Mahalanobis, "Deffie-Hellman Key Exchange Protocol, Its Generalization and
- Nilpotent Groups," Florida Atlantic University, Boca Raton, Florida, 2005. [Ph.D. Thesis: Online]. Available: https://eprint.iacr.org/2005/223.pdf.
- S. A. Mortazavi, A. N. Pour, and T. Kato, "An efficient distributed group key management using hierarchical approach with Diffie-Hellman and Symmetric Algorithm: DHSA," in *International Symposium on Computer Networks and Distributed Systems (CNDS)*, 2011, pp. 49–54.
- A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.
- A. Naureen, A. Akram, R. Riaz, K.-H. Kim, and H. F. Ahmed, "Performance and
- Security Assessment of a PKC Based Key Management Scheme for Hierarchical Sensor Networks," in *IEEE Vehicular Technology Conference*, 2008, pp. 163–167.
- M. M. Haque, A.-S. K. Pathan, C. S. Hong, and E.-N. Huh, "An Asymmetric KeyBased Security Architecture for Wireless Sensor Networks," *KSII Trans. INTERNET Inf. Syst.*, vol. 2, no. 5, 2008.
- J. Ma, S. Zhang, Y. Zhong, and Y. Wu, "PEAN: A Public Key Authentication
- Scheme in Wireless Sensor and Actor Network," in *Sixth IEEE International Conference on Computer and Information Technology*, 2006, p. 230.
- M. Misbahuddin, P. Premchand, and A. Govardhan, "A User Friendly Password

- Authenticated Key Agreement for Multi Server Environment," in *International Conference on Advances in Computing, Communication and Control*, 2009, pp. 113–119.

- T.-Y. Wu, C.-M. Chen, K.-H. Wang, C. Meng, and E. K. Wang, "A provably secure certificateless public key encryption with keyword search," *J. Chinese Inst. Eng.*, vol. 42, no. 1, pp. 20–28, 2019.