Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 11 (2017) pp. 3219-3226
© Research India Publications
http://www.ripublication.com

Enhanced Network Security Algorithm with Advanced Key Generation for RSA and Hashing

V.Umesh

Research Scholar Department of Computer Science,
Bharathiar University, Coimbatore, India

Abstract

This paper consists of embedded network security in the field of "security" from a computer science point of view. It is composed to be accessible to key generation, authentication authorization with enhanced features in a single algorithm. Here in this paper the proposed model embeds enhanced RSA algorithm for key generation, for authentication enhanced kerberos and enhanced digital signature for authorization .first we have started up with Enhanced RSA Algorithm, Here in this enhanced RSA we take four prime numbers instead of two prime numbers to have more efficiency in the security and is proved with an algorithm. It concludes with an overview of some actualized framework and an appraisal of the pragmatic utility of current techniques for security in networks by enhancing the RSA algorithm in order to find the best and optimal security solution to the given message

Keywords: Enhanced RSA, Authorization, Authentication, Hashing, Digital signature, Network metric, Public key, Private key, Asymmetric Encryption.

1. INTRODUCTION

Network security is generally implemented in layers, utilizing all of the above components and built around the seven-layer OSI Reference Model. Unlike the common saying "strong as the weakest link," layered network security is just the opposite. It is as strong as its strongest link. For example, end-to-end security can be achieved by a strong mechanism in the application layer only, even if link-layer security is broken or non-existent. However, that solution only provides security for that particular application. The advantage to applying security at progressively lower levels is that it becomes generally available to more applications. Also, remember that corporate Wi-Fi usually attached to a wired LAN. So even if 802.11 link-level security was very strong, it only applies to the wireless portion of the network. Higher-level

layers of security may still need to be employed, even if a firewall is utilized for the wired portion.

The user must, however, keep in mind that wireless networks cannot provide the same level of inherent security at the physical level that wired networks do. Radio waves pass through walls and can be intercepted from a distance. Even though a standard Wireless LAN (WLAN) card in a laptop may indicate a marginal or even non-existent signal, specialized equipment may be able to receive the signal from a much greater distance. More security is often required, whether the network is wired or wireless. There are many components to effective network security, including the following: Authentication - assurance that a packet comes from where it claims, Confidentiality - protection from disclosure to unauthorized persons, Access control - keeping unauthorized users out, Integrity - ensuring that data is error-free. Normally security for information is required in networked environment, not much in standalone systems. Security for information is required during transmission or the information stored in one of system in network. Since the information moves in public network, information is vulnerable or available or accessible to others easily. Pretend like authorized user by unauthorized individual to access information, Information security can be taken in any one or two or all the layers: Application Layer, Transport Layer, Network Layer. The only way to provide information security is 'Cryptography'. Cryptography is the main concept of protecting data transmission over wired or wireless network. Data security is the main aspect of secure data transmission over insecure network. It involves the authorization of access to data in a network which is controlled by authorized users only. Symmetric and asymmetric cryptography will exist in parallel and continue to serve the community. In figure 1, we actually believe that they are complements of each other: the advantages of one can compensate for the disadvantages of the other. There is a very important fact that is sometimes misunderstood: The advent of asymmetric cryptography does to eliminate the need for symmetric cryptography.

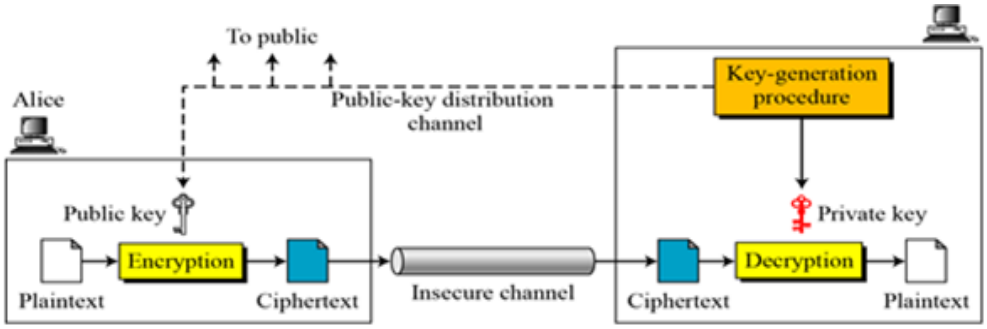

Fig.1. Asymmetric Cryptography

$C = f(K_{public}, P)$; $P = g(K_{private}, C)$

The decryption function f is used only for encryption. The decryption function g is used only for decryption.

2. RSA ALGORITHM

Secure transformation of data is one of the main challenges in present day situation even if we include secure channel, better encryption, etc. The conventional methods of encryption can only maintain the data security. The information could be accessed by unauthorized users for malicious purposes. Therefore, it is necessary to apply effective encryption/decryption models and key exchange algorithms at each phase.

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It was invented by Rivest, Shamir and Adleman in 1978 and hence the name RSA algorithm. It is an asymmetric cryptographic algorithm that is considered to be the most secure way of encryption. Asymmetric means that it works on two different keys: public key and private key. This is also called public key cryptography, because one of the keys can be given to anyone, it is used to encrypt messages. The other key must be kept private. Messages encrypted using the public key can only be decrypted with the private key.

The public key consists of two numbers where one number is the multiplication of two large prime numbers. The private key is also derived from the same two prime numbers. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers. Therefore, the security of RSA relies on the practical difficulty of factoring a large integer. Encryption strength increases exponentially if the key size is doubled or tripled. The mechanism behind RSA algorithm is described below.

STAGE 1 – Key Generation

Generating public key:

1. Choose two different large random prime numbers, p and q.
2. Calculate $n = p \times q$, where n is called the modulus for encryption and decryption.
3. Calculate $\varphi(n) = (p-1)(q-1)$.
4. Choose an exponent e such that:
    - e is an integer.
    - $gcd(e, \varphi(n)) = 1$, this means e is a co-prime to $\varphi(n)$.
    - $1 < e < \varphi(n)$.
5. The public key is $< \boldsymbol{e}, \boldsymbol{n} >$.

Generating private key:

1. Compute $d = \frac{((k \times \varphi(n))+1)}{e}$ for some integer k.
2. The private key is $< \boldsymbol{d} >$.

STAGE 2 – Encryption

Now we will encrypt plaintext "m":

1. Convert the letter to a number: $m = 9$.
2. Let $p = 7$ and $q = 11$.
3. Calculate $\boldsymbol{n} = \boldsymbol{p} \times \boldsymbol{q}$
   $= 7 \times 11$
   $= 77$
4. Calculate $\boldsymbol{\varphi(n)} = \boldsymbol{(p-1)(q-1)}$
   $= (7-1)(11-1)$
   $= 6 \times 10$
   $= 60$
5. Let e be 7 since $gcd(7,60) = 1$ and $1 < 7 < 60$.
6. Compute encrypted data, $\boldsymbol{c} = \boldsymbol{m^e}$ % $\boldsymbol{n}$
   $= 9^7$ % 77
   $= 4782969$ % 77
   $= 37$
7. Thus, encrypted data/ciphertext turns out to be 37.

STAGE 3 – Decryption

Now we will decrypt ciphertext 37:

1. Calculate $d = \frac{((k \times \varphi(n))+1)}{e}$ for k = 5.
   $= \frac{((5 \times 60)+1)}{7}$
   $= \frac{(300+1)}{7}$
   $= \frac{301}{7}$
   $= 43$
2. Compute decrypted data, $\boldsymbol{m} = \boldsymbol{c^d}$ % $\boldsymbol{n}$
   $= 37^{43}$ % 77
   $= 9$
3. Thus, decrypted data/plaintext turns out to be 9.

3. PROPOSED ALGORITHM

RSA algorithm involves two keys termed as public and private. The public key is used for encryption process and private key is used for decryption. Both the keys use the same computed 'N' value. The proposed Enhanced RSA algorithm uses two different 'N' values for encryption and decryption.

The proposed algorithm is as follows:

Step 1: Choose four different large random prime numbers, p,q,r and s.

Step 2: Calculate n = p×q×r×s.

Step 3: Calculate $\varphi(n) = (p-1)(q-1)(r-1)(s-1)$.

Step 4: Choose an integer e such that 1<e<$\varphi(n)$ and e is a co-prime to $\varphi(n)$. This means e and $\varphi(n)$ share no factors other than 1, gcd (e, $\varphi(n)$) = 1. The public key is <e, n>.

Step 5: To determine private key, compute d using the following formula: d = (k×$\varphi(n) + 1)/e$ for some integer k.

Implementation of the Enhanced RSA Algorithm:

Step 1: Let **p = 2, q = 3, r = 5 and s = 7.**

Step 2: Now first part of the Public key: **n = p×q×r×s = 210.**

Step 3: Now we need to calculate $\emptyset(n) = (p-1)(q-1)(r-1)(s-1) = 48$.

Step 4: We also need a small exponent say **e,** But e must be an integer, Not be a factor of n, **1 < e < Φ(n)** [Φ(n), Let us now consider it to be equal to 48]. Our Public Key is made of n and e.

Step 5: Now calculate Private Key, d = (k×$\varphi(n) + 1)/e$ for some integer k. For k = 2, value of d is 15.

Convert letters to numbers: A = 1 and B = 2.

Encrypted Data c = M^e mod n =>12^e mod n

Thus our Encrypted Data comes out to be 156.

Now we will decrypt Decrypted Data = c^d mod n =>12.

Thus our Encrypted Data comes out to be 12, 1 = A and 2 = B,"AB".

Coding of the above algorithm:

```
#include<stdio.h>
#include<math.h>
```

```
// Returns gcd of a and b
int gcd(int a, int h)
{
   int temp;
   while (1)
   {
      temp = a%h;
      if (temp == 0)
        return h;
      a = h;
      h = temp;
   }
}

// Code to demonstrate RSA algorithm
int main()
{
   // Two random prime numbers
   double p = 3;
   double q = 7;
   double r = 5;
   double s = 2;


   // First part of public key:
   double n = p*q*r*s;

   // Finding other part of public key.
   // e stands for encrypt
   double e = 4;
   double phi = (p-1)*(q-1)*(r-1)*(s-1);
   while (e < phi)
   {
```

```
        // e must be co-prime to phi and
        // smaller than phi.
        if (gcd(e, phi)==1)
            break;
        else
            e++;
    }

    // Private key (d stands for decrypt)
    // choosing d such that it satisfies
    // d*e = 1 + k * totient
    int k = 2;  // A constant value
    double d = (1 + (k*phi))/e;

    // Message to be encrypted
    double msg = 12;

    printf("Message data = %lf", msg);

    // Encryption c = (msg ^ e) % n
    double c = pow(msg, e);
    c = fmod(c, n);
    printf("\nEncrypted data = %lf", c);

    // Decryption m = (c ^ d) % n
    double m = pow(c, d);
    m = fmod(m, n);
    printf("\nOriginal Message Sent = %lf", m);

    return 0;
}
Message data = 12.000000
Encrypted data = 156.000000
Original Message Sent = 20736.000000
```

4. CONCLUSION

There are several algorithms and properties in network security, which play an important role in determining the level of network security. These properties known as security metrics can be applied for security quantification in computer networks. Most of the researches on this area has focused on defining the new security metrics to improve the quantification process. In this paper, we present a new approach to increase the complexity of key exchange to a higher extent and increases efficiency, analyze and quantify the keys. Our proposed method reveals the importance of each security to quantify security in the key exchange under surveillance.

REFERENCES

[1] M. S. Ahmed, E. Al-Shaer, and L. Khan, "A novel quantitative approach for measuring network security," in The 27th IEEE Conference on Computer Communications (INFOCOM'08), pp. 1957–1965, 2008.

[2] A. Anurag, "Network neutrality: Developing business model and evidence based net neutrality regulation," International Journal of Electronics and Information Engineering, vol. 3, no. 1, pp. 1–9, 2015.

[3] J. L. Garc´ıa-Dorado, A. Finamore, M. Mellia, M. Meo, and M. Munafo, "Characterization of ISP traffic: Trends, user habits, and access technology impact," IEEE Transactions on Network and Service Management, vol. 9, no. 2, pp. 142–155, 2012.

[5] H. Ge, L. Gu, Y. Yang, and K. Liu, "An attack graph based network security evaluation model for hierarchical network," in IEEE International Conference on Information Theory and Information Security (ICITIS'10), pp. 208–211, 2010.

[4] B. Heinzle and S. Furnell, "Assessing the feasibility of security metrics," in International Conference on Trust, Privacy and Security in Digital Business, pp. 149–160, Springer, 2013.

[5] A. Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison Wesley, 2007.

[6] H. Kahtan, N. A. Bakar, and R. Nordin, "Dependability attributes for increased security in component-based software development," Journal of Computer Science, vol. 10, no. 8, pp. 1298–1306, 2014.

[7] M. Khan, M. Omer, and J. Copeland, "Decision centric identification and rank ordering of security metrics," in IEEE 37th Conference on Local Computer Networks (LCN'12), pp. 208–211, 2012.

[8] Y. P. Lai and P. L. Hsia, "Using the vulnerability information of computer systems to improve the network security," Computer Communications, vol. 30, no. 9, pp. 2032–2047, 2007.