Int. J. Advanced Networking and Applications
Volume: 01 Issue: 03 Pages: 205-209 (2009)

Implementation of Improved NK Protocol using MATLAB

K K Goyal
Faculty of Management & Computer Application
R.B.S.College, Khandari, Agra-282002 (U.P), India.
E-Mail:kkgoyal@gmail.com
Kuldeep Bharadwaj
Institute of Basic Science
Dr.B.R.Ambedkar University, Khandari, Agra-282002 (U.P)
Email:kuldeepibs@yahoo.co.in
Pankaj Saxena
Faculty of Management & Computer Application
R.B.S.College, Khandari, Agra-282002 (U.P), India
E-Mail:pankaj_rbs@yahoo.com

----------ABSTRACT----------
In 2003, Novikov and Kiselev [6] proposed an authentication of the user from the remote autonomous object. In 2005 Yang et al [10] pointed out that Novikov and Kiselev scheme is insecure against the man-in-middle attack. In 2009, Goyal and Bhardwaj[12], proposed that Novikov-Kiselev scheme is insecure against a reflection attack and also proposed an improvement in this scheme. In this paper, we propose the implementation of the improved NK protocol using MATLAB.

Keywords: Authentication, Remote User, RSA, Security, MATLAB.
Date of Submission: December 03, 2009, Accepted: December 15, 2009

1. Introduction

The authentication scheme is commonly used for verifying a user's identity. Only the authenticated users can access the remote systems. The scatter of remote systems in different places allows more efficient and convenient access for geographically dispersed users. Remote access is one of the applications which ascertain whether the user is legal and whether it can access [1, 2, 3, 4, 5, 8, 9]. In Novikov-Kiselev scheme [6], the authentication of the user is done from the remote autonomous object with public key cryptosystem. The scheme has applications in the telecommunications systems. But Yang et al [10] pointed out that Novikov and Kiselev scheme is insecure against the man-in-middle attack. Goyal and Bhardwaj[12], proposed that Novikov-Kiselev scheme is insecure against a reflection attack and also proposed an improvement in this scheme. In this paper, we propose the implementation of the improved NK protocol using MATLAB.

2. Notations

- U_i, O, and I denote the User, the remote autonomous Object, and the Intruder.
- ID_i and K denote the user's identifier and the control command.
- (P_{KU},S_{KU}) and (P_{KO},S_{KO}) denote a pair of session keys of U_i and O, generated by RSA algorithm.
- (P_{KI},S_{KI}) are the keys of Intruder generated by the RSA algorithm.
- T_i denotes the time parameter.
- E(.) and D(.) are the encryption and decryption functions.

3. Review of the Novikov-Kiselev Scheme

The Novikov-Kiselev scheme consists of two stages. In the first stage a user negotiates the identity with remote autonomous object before functioning as an object. In the second stage the user's identity is verified, when the user communicates with the object.

3.1 The First Stage : -

The user negotiates the identity ID and the time parameter T_0 with the remote object beforehand. This step is executed just once. The ID and T_0 are stored in the operative memory of the object by the user.

3.2 The Second Stage: -

Step 1: The user sends start communication request S to the object through the public communication channel.

Step 2: The object generates a pair of keys P_{KO} and S_{KO} by the RSA algorithm [7] and sends the public key P_{KO} to the user. Note that S_{KO} is kept securely by the object. Simultaneously, the object turns on the timer and records the start transmission time T_1.

Step 3: The user sends the encrypted message E_{PKO}(ID, P_{KU}) to the object, where E_A(M) is that message M is encrypted by the public key A using the encryption function E(.) of the RSA algorithm. The identity ID and public key P_{KU} are encrypted with P_{KO} using the encryption function of the RSA algorithm. Note that the user also has a pair of keys P_{KU} and S_{KU} are generated by the RSA algorithm and S_{KU} is kept securely by the user.

Step 4: The object decrypts the message $D_{SKO}(E_{PKO}$(ID, P_{KU}))= (ID, P_{KU}) with secure key S_{KO} using the decryption function of the RSA algorithm, where D_B(M) is that message M is decrypted by the secret key B using the decryption function D(.) of the RSA algorithm. T_2 is recorded simultaneously. If the difference in time ΔT between $T_1$and T_2 is smaller than T_0 compared with the user's ID. Supposing ID discord with user's ID saved in memory of the object, then the object terminate the session. Otherwise, the object encrypts the message X with the user's public key P_{KU} using the RSA algorithm, and then sends it to the user.

Step 5: When the user receive the message from the object, the user decrypts X with secure key S_{KU} using the RSA algorithm. The user can derive the command K from the message X and encrypt the command K and new identity ID' with pubic key P_{KO} of object using the RSA algorithm. And then, the encrypted message is sent to the object.

The object decrypts the message with the secure key S_{KO} after receiving the message from the user. The object executes the command K, if the difference in time ΔT between T_1 and T_2 is smaller than T_0. The object terminate the session, or else. The procedures of this stage are shown in Figure 1.

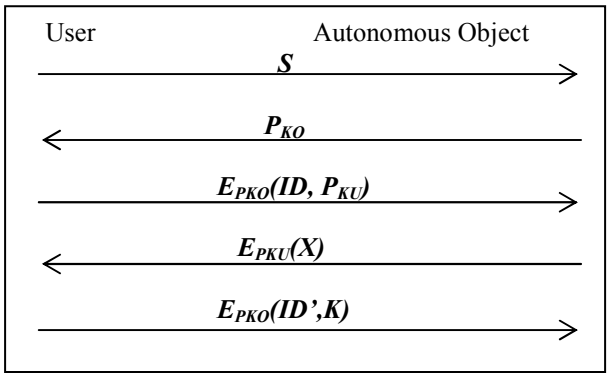

Figure 1: The procedures of the second stage

4. Reflection Attack

4.1 The First Stage : -

The first stage is the pre-tuning of the parameters U_i and O. U_i produces ID_i and synchronizes T_i with the remote object. This processing is executed just once. ID_i and T_0 are produces and stored in the operative memory of O by U_i.

4.2 The Second Stage : -

1) The user sends start request *S* to the object. He uses public channel for this purpose but intruder intercepts *S* and does not send S to object.

2) The Intruder uses RSA key generation algorithm. He computes (S_{KI},P_{KI}) as private and public key respectively. Intruder sends P_{KI} to the user and starts timer to note the time T_1.

3) The user computes the encrypted message using public key P_{KI} of Intruder $E_{PKI}(ID,P_{KU})$

Where P_{KU} is RSA public key of user and corresponding private key of user is $S_{KU.}$ User sends this encrypted message to the object.

4) The Intruder decrypts the message using S_{KI}.

5) The Intruder encrypts his own message *M* with the public key of user P_{KU} and sends to the user: $E_{PKU}(M)$

6) When the user received the message from the Intruder he decrypts it with his secret key S_{KU}. The user derives the command *K* from *M*. User sends the following information : $E_{PKI}(ID',K)$

7) Now intruder decrypts this message with S_{KI}. Intruder can get the ID' and K. After that, Intruder can make whatever modification he wants.

Here we observe that whole communication is open in front of Intruder and Intruder intercept in between the user and object and create illusion of object.

5 Our Improved Scheme with Matlab Code

We have improvement the Novikov-Kiselev scheme by taking into account the reflection attack. In our protocol we have two stages. In first stage user sends his ID_i and Ti via secure channel at that time object computes a pair of session keys (P_{KO},S_{KO}) and sends his public key P_{KO} via secure channel to U_i. In second stage object identify the user U_i. We have used the concept of random number in this stage.

5.1 The First Stage : -

The first stage is the pre-tuning of the parameters U_i and O. U_i produces ID_i and T_0 and sends to object O via secure channel. This processing is executed just once. ID_i and T_0 are produces and stored in the operative memory of O by U_i. Object computes a pair of session keys (P_{KO},S_{KO}) and sends his public key P_{KO} via secure channel to U_i.

Pre-tuning of parameters U_i and O

Let the U_i is 'kkg' and T_0 is any time stamp. Convert the text 'kkg' into integer using the function text2int('kkg') = 111107 and send it to object O using secure channel. U_i and T_0 are stored in the operative memory of O.

Generation of session key by object

Select p,q Let p = 659 and q = 1249
Calculate n=p*q n=659*1249=823091
Calculate $\Phi(n) = (p-1)*(q-1)$
$\Phi(n) = 658*1248=821184$
Select integer e gcd($\Phi(n)$,e)=1;1<e<$\Phi(n)$
e=17
Calculate $d \equiv e^{-1} \bmod \Phi(n)$ d=48305
Public key **P_{KO}={17,823091}**
Private key **S_{KO}={48305,823091}**

5.2 The Second Stage : -

1. User also computes a pair of session keys (P_{KU},S_{KU}) and encrypts his public key P_{KU} and start request *S* with public key of object. The user sends $E_{PKO}(S,P_{KU})$ to the object via public channel.

Generation of session key by user

Select p,q Let p = 59 and q = 61
Calculate n=p*q n=59*61=3599
Calculate $\Phi(n) = (p-1)*(q-1)$
$\Phi(n) = 58*60=3480$
Select integer e gcd($\Phi(n)$,e)=1;1<e<$\Phi(n)$
e=31
Calculate $d \equiv e^{-1} \bmod \Phi(n)$ d=3031
Public key **P_{KU}={31,3599}**
Private key **S_{KU}={3031,3599}**

Encryption of start request by user

Now encrypt S,31,3599 using public key of object P_{KO}={17,823091} using powermod(message,17,823091) encryption function.
text2int1('s') = 19
powermod(19,17,823091) = 433258
powermod(31,17,823091) = 75578
powermod(3599,17,823091) = 251923
User send cipher text 433258,75578,251923 to object O using public channel.

2. The object decrypt the message by using his private key S_{KO} and sends the following message to the user

$E_{PKU}(r)$

Simultaneously, the object turns on the timer and record the start transmission time T_1.

Decryption of message by object

Object decrypts the encrypted message using his private key S_{KO}={48305,823091}and powermod(,,) function.
Cipher text 433258,75578,251923
powermod(433258,48305,823091) = 19 int2text1(19) = '*S*'
powermod(75578,48305,823091) = 31
powermod(251923,48305,823091) = 3599
and gets the start request '*S*' and public key of user P_{KU}={31,3599}. Now object encrypts a random no r=3221 using public key of user and send it to user.
powermod(3221,31,3599) = 3526

3. The user decrypt the encrypted message using his private key and get the random number send by object

$r'=D_{SKU}(E_{PKU}(r))$
powermod(3526,3031,3599) = 3221

Where $S_{KU}=\{3031,3599\}$ is RSA secret key of user. User sends the following encrypted message to the object.

$E_{PKO}(ID_i,r')$
ID_i=text2int('kkg') = 111107
powermod(111107,17,823091) = 627494
powermod(3221,17,823091) = 508532

4. The object decrypts the message using S_{KO} and finds the ID_i and r'. T_2 is recorded simultaneously. If the difference in time ΔT between T_1 and T_2 is smaller than T_0 and r' is same as r then compared with the user's *ID*. Supposing *ID* discord with user's *ID* saved in memory of the object, then the object terminate the session. Otherwise, the object encrypts the message *M* with the user's public key P_{KU} using the RSA algorithm, and then sends it to the user:

$E_{PKU}(M)$
powermod(627494,48305,823091) = 111107
int2text1(111107) = kkg
powermod(508532,48305,823091) = 3221

User id 'kkg' and random no.(3221) are matched with the saved in memory so the mutual authentication is

successfully done in between user and the remote autonomous object.

5. When the user received the message from the object he decrypts it with his secret key S_{KU}. The user derives the command K from M. User sends the following information:

$$E_{PKO}(ID', K)$$

Now we see that in our protocol the intruder can't intercept in any stage. Because the public key of object send to user via private channel and the start request message and other conversation is done with encrypted form. User identification is done with the help of random number.

6 MATLAB code for used functions

1.powermode function [used for encryption and decryption]

```
function y = powermod(a,z,n)
[ax,ay]=size(a);
a=mod(a,n);
if (z<0),
  z=-z;
  for j=1:ax,
            for k=1:ay,
      a(j,k)=invmodn(a(j,k),n);
    end;
  end;
end;
for j=1:ax,
for k=1:ay,
 x=1;
 a1=a(j,k);
 z1=z;
 while (z1 ~= 0),
   while (mod(z1,2) ==0),
     z1=(z1/2);
     a1=mod((a1*a1), n);
   end;  %end while
   z1=z1-1;
   x=x*a1;
   x=mod(x,n);
 end;
 y(j,k)=x;
end;
end;
```

2. text2int1 function [Used to convert a text into integer]

```
function y = text2int1 (x)
[s1,s2]=size(x);

yvec=x - 'a'+1;
inds=find(yvec<1);
yvec(inds)=zeros(size(inds));
y=zeros(s1,1);
for k=1:s1,
for j=0:s2-1,
  ind=s2-j;
  y(k)=y(k)+yvec(k,ind)*100^(j);
end;
end;
```

3.int2text1 function [used to convert an integer into text]

```
function y = int2text1 (x)
j=1;
flag=1;
xv=x;
while flag,
  xrem=rem(xv,100);
  xv=floor(xv/100);
  xstore(j)=xrem;
  j=j+1;
  if xv<1,
    flag=0;
  end;
end;
xstore=xstore(:);
yvec=flipud(xstore)';
y=char(yvec+'a'-1);
ind=find(y=='`');
y(ind)=' ';
```

7 Conclusion

In this paper we have reviewed the the Novikov and Kislev's scheme. We discussed reflection attack and proposed authentication scheme of the user from the Remote Autonomous Object. we also proposed the implementation of the improved NK protocol using MATLAB.

Acknowledgement

The authors thank **Prof. Sunder Lal** [Pro.V.C., *Dr.B.R.Ambedkar University, Khandari, Agra - 282002 (U.P)*] for his kind supervision of the work.

References

[1] M. S. Hwang, "A remote password authentication scheme based on the digital signature method," International Journal of Computer Mathematics, vol. 70, pp. 657–666, 1999.

[2] M. S. Hwang, C. C. Lee, and Y. L. Tang, "An improvement of SPLICE/AS in WIDE against guessing

attack,"International Journal of Informatica, vol. 12, no. 2, pp. 297–302, 2001.

[3] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 46, no. 1 pp. 28–30, 2000.

[4] C. C. Lee, M. S. Hwang, and W. P. Yang, "A flexible remote user authentication scheme using smart cards." ACM Operating Systems Review, vol. 36, no. 3, pp.46-52, 2002.

[5] C. C. Lee, L. H. Li, and M. S. Hwang, "A remote user authentication scheme using hash functions," ACM Operating Systems Review, vol. 36, no. 4, pp. 23–29, 2002.

[6] Sergei N. Novikov and Anton A. Kiselev. "The authentication of the user from the remote autonomous object,". in 4th Siberian Russian Workshop and Tutorial on Electron Devices and Materials EDM,Section II, NSTU, Altai, Erlagol, July 2003.

[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Communications of the ACM, vol. 21, pp. 120–126, Feb. 1978.

[8] Y. L. Tang, M. S. Hwang, and C. C. Lee, "A simple remote user authentication scheme," Mathematical and Computer Modelling, vol. 36, pp. 103–107, 2002.

[9] Lal Sunder, K.K.Goyal,"An improved remote user authentication scheme using bilinear pairing", http://eprint.iacr.org/2007/440.pdf.

[10] C. Y. Yang, C. C. Lee, and S. Y. Hsiao, "Man-in-the-middle attack on the authentication of the user from the remote autonomous object," International Journal of Network Security, vol. 1, no. 2, pp. 81-83,Sep. 2005.

[11] A. K. Awasthi, "On the authentication of the user from the remote autonomous object," International Journal of Network Security, vol. 1, no. 3, pp. 166-167, Nov. 2005.

[12] K.K.Goyal and Kuldeep Bharadwaj, "User Authentication From the Remote Autonomous Object" in 3rd National Conference on Computing For Nation Development held at BVICAM, New Delhi on February 26-27, 2009 (INDIACom-2009) ISSN:0973-7529.

Authors Biography

Mr. K. K. Goyal is presently working as a faculty member in the Department of Computer Application, Faculty of Management and Computer Application, R.B.S.College, Agra. and having eight years experience of teaching to U.G. and P.G. classes. He obtained B.Sc.(maths), M.C.A., M.A.(maths), M.Tech. (Computer Science) degrees and pursuing Ph.D. in Cryptography from Dr. B. R. A. University, Agra. He is a life member of IACSIT, Singapore, CRSI, India and RMS, India. He has published his research works at national and international level. His current research interests include Network Security, Cryptography and Applied Mathematics.

Kuldeep Bhardwaj received his M. Sc. in Mathematics & Computer Science from Department of Mathematics, Institute of Basic Science, Dr. B. R. Ambedkar (Agra) University, Agra, INDIA in 2004. His current research interests include Elliptic Curve Cryptography and Implementation of Cryptographic Protocols in which he is working for Ph. D. Degree.

Mr. Pankaj Saxena is presently working as a faculty member in the Department of Computer Application, Faculty of Management and Computer Application, R.B.S.College, Agra. and having twelve years experience of teaching to U.G. and P.G. classes. He obtained B.Sc.(maths), M.C.A., M.Sc.(Physics), M.Tech. (Computer Science) degrees and pursuing Ph.D. in Data Mining from Dr. B. R. A. University, Agra. He has published his research works at national and international level. His current research interests include Artificial Intelligence, Artificial Neural Network, Data Warehouse and Mining, and Cryptography