Ninth Int. Workshop on GNs, Sofia, 4 July 2008, 20-27

MODELING NET ATTACKS FOR LISTENING AND BREAK-DOWN CRYPTTED MESSAGES BY USING GENERALISED NETS MODEL

Ivelina Vardeva
University of „Prof. d-r Assen Zlatarov" – Bourgas, Bulgaria, iveto@btu.bg

Abstract
The article examines the structure of two of the basic attacks of sent in the public net cipher messages. It is used the apparatus of generalized net for modeling the processes of attacks for listening and braking the sent messages. About the examined ciphered messages is used RSA asymmetric algorithm.

Key words: generalized nets, cryptography, cryptoattack, listening, break-down, RSA, attacker's capabilities, attacker's goal

Introduction

In the connection with Internet development and e-commerce many companies-producers offer high-technological program and technological solutions for security. Using the available resources on the market is possible to build a policy and practices for security, which can defend the information of powerful threats and attacks.

The threats about the information security of all systems are reality today and they incessantly grow up. The information security must to be a key aspect for every information technology used in the systems of state management and in the systems ensuring national security and defense.

Using the security resources for "disloyal" purposes grow up repeatedly with the development of information relationships and the increasing of attacks and threats on the computers systems – in that way the problems of computer security become more serious. The most important thing is that the computer security defends the information saved in the system. That's why the computer security often is called information security.

Security could never be absolute, it is relative quantity because it depends on the efforts, which exerts the respective company for determination and supporting the desired level of security of its own network.

According to [1,11] is present cryptographic system with asymmetric key for encryption and decryption the information passes through the public net - Internet. It's used asymmetric algorithm [5,6,7] with a pair of keys – open (public) and secret (private) with which the procedures enciphering and deciphering are convertible and simple.

Public key is designed only for ciphering messages while the private one is used for deciphering. Each of the keys could be used for ciphering and deciphering if the required rule is observed - one of them must be private and accessible only for one of the users.

RSA asymmetric algorithm with different keys for coding (K_E) and decoding (K_D) information $K_E \neq K_D$ is used, as it is known the "public key" of the message recipient. The asymmetric algorithms are named algorithms with "public key", the coding key in this algorithm is spread free. Therefore everybody could cipher a message, but only the private key owner could decipher it.

These algorithms use the fact, that there are irreversible mathematical functions which inverse function is difficult to find for a short period of time.

RSA [3,6,10,15] is considered as one of the best asymmetric algorithm in the cryptographic protocol SSL. It is the most wide-spread encryption system with a public key for safety the traffic passing through web to e-mail, e-commerce and some wireless devices. **RSA is based on arithmetical large numerical therefore it could be unusually slow and difficult to enciphering.**

The most often attacks against the RSA algorithm are like "the rough force" working on the principle of comprehensive check-up of the all possible keys.

Review of the basic RSA system

We review the basic RSA public key system and refer to [4] for more information. We describe three constituent algorithms: key generation, encryption, and decryption.

Key generation: The key generation algorithm takes a security parameter n as input. Throughout the paper we use n =1024 as the standard security parameter. The algorithm generates two (n/2)-bit primes, p and q, and sets $N \leftarrow pq$. Next, it picks some small value e that is relatively prime to $\varphi(N) = (p-1)(q-1)$. The value e is called the encryption exponent, and is usually chosen as e = 65537.

The RSA public key consists of the two integers <N,e>. The RSA private key is an integer d satisfying $e.d = 1 \bmod \varphi(N)$. Typically, one sends the public key <N,e> to a certificate authority (CA) to obtain a certificate for it.

Encryption*:* To encrypt a message X using an RSA public key $<N,e>$, one first formats the bit-string X to obtain an integer M in $ZN = \{0, \ldots, N-1\}$. This formatting is often done using the PKCS #1 standard [9, 10, 14]. The ciphertext is then computed as $C \leftarrow Me \bmod N$. (Other methods for formatting X prior to encryption are described elsewhere in this issue.)

Decryption: To decrypt a ciphertext C the decrypter uses its private key d to compute an e'th root of C by computing $M \leftarrow Cd \bmod N$. Since both d and N are large numbers (each approximately n bits long) this is a lengthy computation for the decrypter. The formatting operation from the encryption algorithm is then reversed to obtain the original bit-string X from M. Note that d must be a large number (on the order of N) since otherwise the RSA system is insecure [3, 15].

It is standard practice to employ the Chinese Remainder Theorem (CRT) for RSA decryption. Rather than compute $M \leftarrow Cd \pmod N$, one evaluates:

$Mp \leftarrow Cp$

$dp \pmod p$ $Mq \leftarrow Cp$

$dq \pmod q$.

Here $dp = d \bmod p - 1$ and $dq = d \bmod q - 1$. Then one uses the CRT to calculate M from Mp and Mq . This is approximately four times as fast as evaluating $Cd \bmod N$ directly [3, 7].

It is represented a scheme of the cryptoattacks for listening and breaking-down in transmission the ciphertext by using the generalized nets model [1,2,11] which gives the opportunity for modeling the whole process.

1. **Attacker's capabilities:** The strongest attacker capability in the standard model is called "adaptive chosen-ciphertext attack" and is denoted by (CCA) [16]. This means that the adversary has the ability to decrypt any ciphertext of his choice except for

some challenge ciphertext (imagine the attacker is able to exploit a decryption box that will decrypt anything except for some known challenge ciphertext).

2. **Attacker's goal:** The standard security goal is called "semantic security" [12] (also known as "indistinguishability of ciphertexts"), and is denoted by (IND). Roughly speaking, the attacker's goal is to deduce just one bit of information about the decryption of some given ciphertext. We say that a system is semantically secure if no efficient attacker can achieve this goal. We note that a deterministic encryption algorithm can never give semantic security.

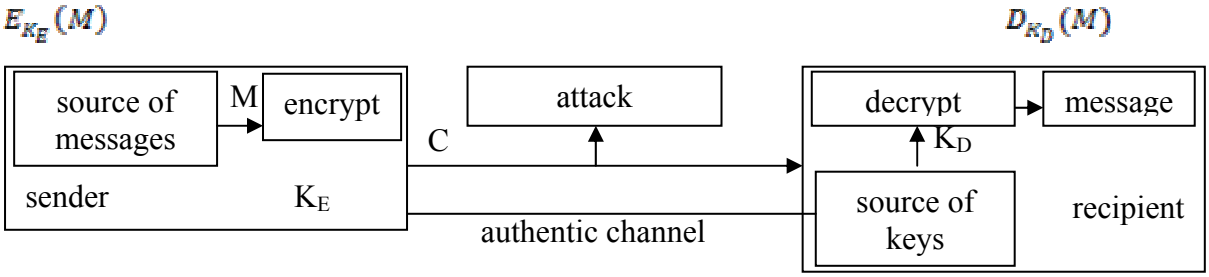
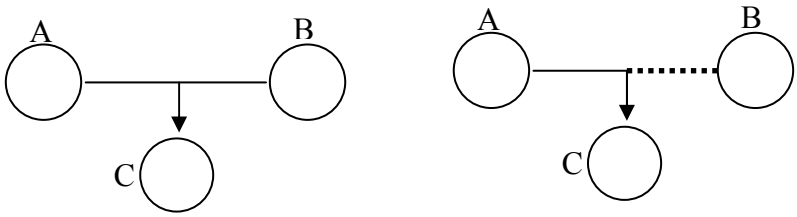


Fig 1. Net attack during the ciphering message sending



A) listening B) break-down in transmission

Fig 2. Standard attack

The RSA permutation, proposed by Rivest, Shamir and Adleman [6, 8], is the most well known trapdoor permutation. Its one-wayness is believed to be as strong as integer factorization. The RSA setup consists of choosing two large prime numbers p and q, and computing the RSA modulus $n = pq$. The public key is n together with an exponent e (relatively prime to $\varphi(n)=(p-1)(q-1)$). The secret key d is defined to be the inverse of e modulo $\varphi(n)$. Encryption and decryption is defined as follows:

$$En,e(m) = me \bmod n \; Dn,d(c) = c\,d \bmod n.$$

This primitive does not provide by itself an IND-CCA secure encryption scheme. Under a slightly stronger assumption than the intractability of the integer factorization, it gives a cryptosystem that is only one-way under chosen-plaintext attacks — a very weak level of security. Semantic security fails because encryption is deterministic. Even worse, under a CCA attack, the attacker can fully decrypt a challenge ciphertext $C = me \bmod n$ using the homomorphic property of RSA:

$$En,e(m1)\; En,e(m2) = En,e\;(m1\; m2) \bmod n.$$

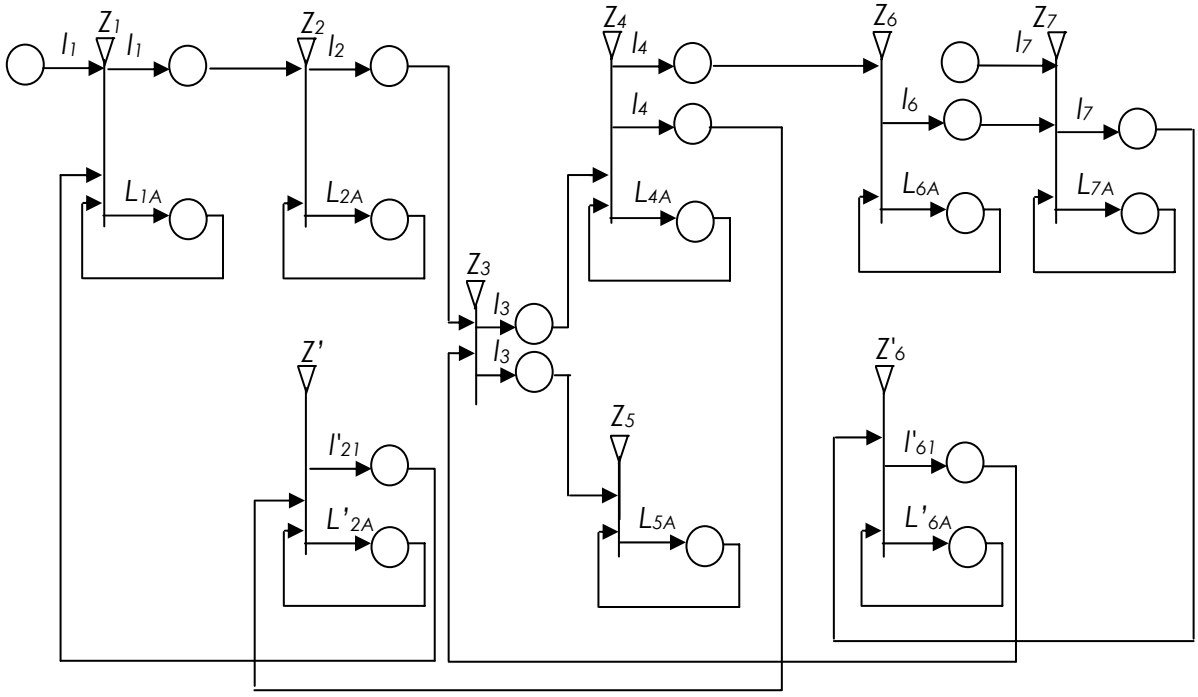
To decrypt $C = me \bmod n$ using a CCA attack do:
(1) compute $C' = C.2e \bmod n$,
(2) give C' (≠ C) to the decryption oracle, and
(3) the oracle returns $2m \bmod n$ from which the adversary can deduce m.

To overcome RSA this simple CCA attack, practical RSA-based cryptosystems randomly pad the plaintext prior to encryption. This randomizes the ciphertext and eliminates the homomorphic property.

Generalized nets model

Initially are set the following kernels included in the generalized net:

- at position l_{11} enters - α_1 token with a characteristic "plaintext", at position l_{71} enters β_1 token with a characteristic "plaintext".
- at position L_{1A} enter - α_2 – token with an initial characteristic "plaintext for sending" and β_2 with a characteristic "receive plaintext";
- at position L_{7A} enter – β_2 – token with an initial characteristic "plaintext for sending" and α_2 with a characteristic" receive plaintext";
- at positions L_{2A}, L'_{2A} include – γ_1 – token with an initial characteristic " a pair of public and private key of A and public key of B";
- at positions L_{6A}, L'_{6A} include – γ_2 – token with initial characteristic " a pair of public and private key of B and public key of A";
- at position l_{21} enters ε_1 token with a characteristic „cipher text", at position l'_{61} enters ε_2 token with a characteristic „ciphertext".



It is developed a generalized network model with leaded in the multitude of transitions A which:

A= { Z_1, Z_2, Z'_2, Z_3, Z_4, Z_5, Z_6, Z'_6, Z_7}, where the transitions describe the following processes :

Z_1 ="Tasks done by source A"

Z_2 ="Tasks done by cryptographic algorithm for encrypting"

Z'_2 ="Tasks done by cryptographic algorithm for decrypting"

Z_3 ="Attacks done"
Z_4 ="Tasks done by listtening attack"
Z_5 ="Tasks done by break-down attack"
Z_6 ="Tasks done by cryptographic algorithm for decryption"
Z'_6 ="Tasks done by cryptographic algorithm for encryption"
Z_7 ="Tasks done by source B "
Transitions have the following description:

$Z_1 = < \{ l_{11}, l'_{21}, L_{1A} \}, \{l_{12}, L_{1A} \}, R_1, M_1, \vee (l_{11}, l'_{21}, L_{1A}) >$

$R_1 =$	l_{12}	L_{1A}
l_{11}	*false*	*true*
l'_{21}	*false*	*true*
L_{1A}	*true*	*true*

The token α_1 from position l_{11} enters aт position L_{1A}, where it is added to token α_2 from the current position. The token α_2 from position L_{1A} is divided by two tokens α_2' and α_2'' coming out with the following current characteristic "plaintext sending" for encryption. The tokens at position l_{12} do not receive a new characteristic.

$Z_2 = < \{ l_{12}, L_{2A} \}, \{l_{21}, L_{2A} \}, R_2, \vee (l_{12}, L_{2A}) >$

$R_2 =$	l_{21}	L_{2A}
l_{12}	*false*	*true*
L_{2A}	$W_{2A,21}$	*true*

$W_{2A,21}$ - "Message for sending is encrypted"

The token α_2'' from position l_{12} enters at position L_{2A}, where it connects with the token γ_1 from the current position in the token ε and receive its new characteristic „ciphertext from source A" on the basis of cryptographic algorithm for enciphering. The token ε from position L_{2A} divides by two tokens ε_1 and ε_2 coming out with the following current characteristic „sending ciphertext from source A". The tokens at position l_{21} do not receive a new characteristic.

$Z'_2 = < \{ l_{42}, L'_{2A} \}, \{l'_{21}, L'_{2A} \}, R'_2, \vee (l_{42}, L'_{2A}) >$

$R'_2 =$	l'_{21}	L'_{2A}
l_{42}	*false*	*true*
L'_{2A}	$W'_{2A,21}$	*true*

$W'_{2A,21}$ - „the reseived message is decrypt".

The token $\zeta_{(2'')}'$ from position l_{42} enters at position L'_{2A} where it connects with the token γ_1 and it receives its new characteristic β_2 „received plaintext from source B" on the basis of cryptographic algorithm for deciphering. The token β_2 from position L'_{2A} is divided by two tokens β_2' and β_2'' and comes out with the following current characteristic „plaintext from source B". The entered tokens at position l'_{21} do not receive a new characteristic.

$Z_3 = < \{ l_{21}, l'_{61} \}, \{l_{31}, l_{32} \}, R_3, \vee (l_{21}, l'_{61}) >$

$R_3 =$	l_{31}	l_{32}
l_{21}	$W_{21,31}$	$W_{21,32}$
l'_{61}	$W_{61,31}$	$W_{61,32}$

$W_{21,31} = W_{21,32} = W_{61,31} = W_{61,32}$ -"cryptoattack - a ciphertext is caught".

The token ε_2 from position l_{21} is divided by two equal tokens ε_2' and ε_2", which enter respectively at position l_{31} and l_{32} with a characteristic (caught) „ciphertext from source A".

The token ζ_2 from position l_{72} is divided by two equal tokens ζ_2' and ζ_2" , which enter respectively at position l_{31} and l_{32} receive a characteristic (caught) „ciphertext from source B".

$Z_4 = < \{ l_{31}, L_{4A} \}, \{l_{41}, l_{42}, L_{4A} \}, R_4, \vee (l_{31}, L_{4A}) >$

R_4	l_{41}	l_{42}	L_{4A}
l_{31}	*false*	*false*	*true*
L_{4A}	*true*	*true*	*true*

The tokens ε_2' and ζ_2' enter at position L_{4A}, where they are divided by $\varepsilon_{(2')}$' , $\varepsilon_{(2'')}$' and $\zeta_{(2')}$', $\zeta_{(2'')}$'.The entered tokens at positions l_{41} and l_{42} do not receive a new characteristic.

$Z_5 = < \{ l_{32}, L_{5A} \}, \{L_{5A}\} R_5, \vee (l_{31}, L_{5A}) >$

R_5	L_{5A}
l_{32}	*true*
L_{5A}	*true*

The tokens $\varepsilon_{(2'')}$' and $\zeta_{(2'')}$' coming respectively from position l_{32} enter at L_{5A} position, (ciphertext received from sources A and B) and break-down the sent messages to the receiver.

$Z_6 = < \{ l_{41}, L_{6A} \}, \{l_{61}, L_{6A} \}, R_6, \vee (l_{41}, L_{6A}) >$

R_6	l_{61}	L_{6A}
l_{41}	*false*	*true*
L_{6A}	$W_{6A,61}$	*true*

$W_{2A,21} = W_{6A,61}$

The token $\varepsilon_{(2'')}$' from position l_{41} enters at position L_{6A} and unifies with the token γ_2 and it receives its new characteristic α_2 „received plaintext from source A" on the basis of cryptographic algorithm for deciphering. The token α_2 from position L'_{2A} is divided by two tokens α_2' and α_2" comes out with the following current characteristic „plaintext from source A". The entered tokens at position l_{61} do not receive a new characteristic.

$Z'_6 = < \{ l_{72}, L'_{6A} \}, \{l'_{61}, L'_{6A} \}, R'_6, \vee (l_{72}, L'_{6A}) >$

R'_6	l'_{61}	L'_{6A}
l_{72}	*false*	*true*
L'_{6A}	$W'_{6A,61}$	*true*

$W'_{6A,61} = W_{2A,21}$

The token β_2" entering in position L'_{6A} unifies in whole with the token γ_2 and receives its new characteristic „ciphertext" – the token ζ on the basis of cryptographic algorithm for enciphering. The token ζ from position L'_{6A} is divided by two ζ_1 and ζ_2 and comes out with the following current characteristic „sending ciphertext from source B". The tokens at position l'_{61} do not receive a new characteristic.

$Z_7 = < \{ l_{61}, l_{71}, L_{7A} \}, \{l_{72}, L_{7A} \}, R_7, \vee (l_{61}, l_{71}, L_{7A}) >$

$$R_7 = \begin{array}{c|cc} & l_{72} & L_{7A} \\ \hline l_{61} & false & true \\ l_{71} & false & true \\ L_{7A} & true & true \end{array}$$

The token β_1 from position l_{71} enters at position L_{7A} and is added to the token β_2 from the current position. The token β_2 from position L_{7A} is divided by two tokens β_2' and β_2'' with a characteristic „sending plaintext" for coding. The tokens at position l_{72} do not receive a new characteristic.

The token α_2'' from position l_{61} enters in position L_{7A} with a characteristic „received plaintext".

Conclusion

Two of the basic attacks for message catching in sending standard RSA ciphertext are examined. The spread model could help in researching and analyzing the processes for catching encoded messages exchanged in the net.

Generalized net model describes the main conception of the cryptographic theory for conventional encrypting by the classic structure of cryptographic system using RSA asymmetric key. The model allows to be looked through the different stages of proceeding the process and its simulation observed and behavior in future. To resolve the problems of one system however is necessary: to make a complete analysis and a choice of entire defending solution. Providing the safety of the information for the present is the major challenge for the information technologies for the 21-st century.

References

[1] Atanassov, K., „Introduction in the theory generalized net", Burgas, Bulgaria, 1992г.

[2] Atanassov, K., Generalized nets, World Scientific, Singapore, New Jersey, London1991

[3] Bellare, M., Rogaway, P., "Optimal Asymmetric Encryption." In A. De Santis, ed, Proceedings of Eurocrypt '94 vol. 950 of Lecture Notes in Computer Science (LNCS), pp. 92–111. Springer-Verlag,1994.

[4] Blaze, M., Ioannidis, J., University of Pennsylvania,"DSA and RSA Key and Signature Encoding for the KeyNote Trust Management System", March 2000

[5] C. Rackoff and D. R. Simon. Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack. In Crypto '91, LNCS 576, pages 433-444. Springer-Verlag, Berlin, 1992.

[6] CryptoBytes Volume 5, No. 1 Winter/Spring 2002

[7] D. Boneh and G. Durfee. "Cryptanalysis of RSA with Private Key d Less than n0.292." IEEE Transactions on Information Theory 46(4):1339–1349, Jul. 2000. Early version in Proceedings of Eurocrypt '99

[8] Goldwasser, S., Micali, S., Probabilistic Encryption. Journal of Computer and System Sciences, 28:270-299, 1984.

[9] Hristov, H., Trifonov, V., „Reliability and security of communications", Sofia, Bulgaria 2005

[10] http://www.rsa.com/

[11] Menezes, A., Van Oorschot, P., Vanstone, S., Handbook of Applied Cryptography. CRC Press, 1997.

[12] Piper, F., Murphy, S., „Cryptography: A Very Short Introduction", Oxford University Press 2002
[13] RSA Labs. Public Key Cryptography Standards (PKCS), Number 1 Version 2.0. Version 2.1 draft is available at http://www.rsalabs.com/pkcs/pkcs-1/index.html
[14] Vardeva, I., Generalized Net model of the Creation of Virtual Private Network by using Point-to-Point Potocol over Secure Shell, Issue on Intuitionistic Fuzzy Sets and Generalized nets,Volume 4, Warsaw, 2006
[15] Vardeva, I., Sotirov, S., Generalized Net model of SSL with intuitionistic fuzzy estimations, Notes on IFS Proceendings of the Eleventh International Conference on Intuitionistic Fuzzy Sets, Sofia , Volume 13, April 2007, 48-53
[16] Wiener, M., "Cryptanalysis of Short RSA Secret Exponents." IEEE Trans. on Info. Th. 36(3):553–558. May 1990.