University of Benin

ICERD2010

7th - 9th September, 2010
Benin City, Nigeria

3rd International Conference on Engineering Research and Development (ICERD2010)
Benin City, Nigeria, 7th - 9th September 2010

Conference Secretariat:
Office of the Conference Chairman
Department of Production Engineering
University of Benin.
Benin City. Nigeria
Tel: +234 (0)8066596180
+234(0)8023438765
E-mail: icerd2010@uniben.edu
Website: www.uniben.edu

28 April 2010

Dear Author(s)

ACCEPTANCE OF PAPER FOR ICERD2010

On behalf of the Conference Organizing Committee, I am glad to inform you that your Abstract(s) titled

RC42's: Improved Data Security Technique in Wireless Local Network by O. O Olakanmi and O. A Fakolujo, Electrical & Electronics Engineering Department, University of Ibadan, Ibadan, Nigeria. olarad4u@yahoo.com (icerd10115)

(Please always quote the paper reference number in your correspondence).

has/have been accepted for presentation at the 3rd International Conference on Engineering Research & Development (ICERD2010). Find enclosed the Author instructions for writing the full length paper, and the conference registration form.

The deadline for receipt of full length papers which will be put in the conference CD is 30 June 2010. Papers presented at the conference will be reviewed for the journal of Advanced Materials Research published by Trans Tech Publications Ltd, Switzerland.

We look forward to receiving your full length paper(s) and seeing you at the conference. The conference program will be sent to you in July 2010.

Kind regards and best wishes.

Sincerely

A.I. Igbafe, Ph.D

Chairman, ICERD2010 Technical Committee

3rd International Conference on Engineering Research & Development: Advances in Engineering Science & Technology (7th - 9th September 2010), Benin City, Nigeria

RC42's: Improved Data Security Technique in Wireless Local Network

Olakanmi O . O and Fakolujo O . A (PhD)

Electrical & Electronics Engineering Department

University of Ibadan, Ibadan.

Abstract

This paper exposes the weakness of RC4 encryption; a data protection algorithm used by wired equivalent privacy of WLAN. It shows that in spite of general acclaim invulnerability of Wired Equivalent Privacy WEP used in WLAN there are still several loop holes that computer hackers can use to circumvent through our wireless networks. These vulnerabilities create the potential for active and passive attacks which could allow attackers to decrypt or inject data into a network.

To buttress the extent of the vulnerability of RC4 used by WEP, Stuart J.Kerry, the chairman for the IEEE 802.11 standard groups, pointed out that WEP has shortcomings and promised to address all the weaknesses of WEP

This paper proffers an improved method called RC4-2's algorithm, which makes it difficult for hackers to detect the key and cipher text of RC4, whenever there is collision. The RC4-2's encrypts by exclusively Oring the message with the key and 2's complement of the result will then become the encrypted message. Therefore, this paper is not only an eye opener to the vulnerability of WEP in WLAN but provides a perfect improvement on RC4 which takes care of RC4 weaknesses.

INTRODUCTION

1.1 WIRED EQUIVALENT PRIVACY (WEP)

In order to get the clearer picture of this paper, there is need to understand WEP and its relationship with WLAN. WEP is a part of the IEEE 802.11. The 802.11 is a standard created and it came in three versions: 802.11a, 802.11b and 802.11g. 802.11b- equipment operate between 2.4000GHz to 2.4835-GHz and can operate at up 11Mps although with interference its throughput can reduce to 1Mps. 802.11a came after 802.11b and operates at different frequency which is 5.15 to 5.35GHz and 5.725 to 5.825GHz and with increased throughput of about 54Mps. These two standards are not compatible due to different frequency at which the standards operate. The last standard is 802.11g though not yet approved but it operates at the same frequency with 802.11b but with the more bandwidth than 802.11b [1].

Back to WEP which as it has been said earlier is part of 802.11x. It provides confidentiality, integrity of data on our wireless local area network WLAN. Wired LAN uses physical means to protect data or unauthorized access to data or network, however, in WLAN anybody can connect to wireless LAN without physically connection. Therefore, there must be secured means to prevent unauthorized wireless connection to the WLAN. This is achieved by encrypting the data on WLAN with RC4. This not only protects the data on the network but also prevent eavesdropping or sniffing on the network.

1.2 RC4 ENCRYPTION ALGORITHM

RC4 is a stream cipher encryption algorithm which expands a fixed-length secret key into infinite pseudo-random key stream for encrypting message on the WLAN [1][4]. It exclusively OR the data or message with the randomly generated secret key to produce the encrypted message. This will be decrypted at the receiving node of the network. The secret key may be manually entered, however, the WEP make use of initialization vector to vary the secret key entered by the user, so as to prevent guessing of the secret key [1]. This is to change the encryption secret key for each

packet send on the network. The initialization vector IV is 24 bits field which is appended on the message sent through the network. At the receiving end the recipients stations uses the appended IV with the secret key to decrypt the message.

The IV makes sure that the subsequent packets are encrypted with different secret key. This algorithm demonstrates how RC4 encrypts data.

1. Begin
2. getNextpacket() /* also needs to return a placeholder for the next packet of message when sending */
3. while (0 >= (*packet* = getNextpacket()))
4. secretkey = secretkey+initialiationvector
5. *encryptedPacket* = (*packet)* XOR (secretkey)
6. }
7. return *encryptedPacket*
8. End

1.2.1 VULNERABILITIES OF RC4 ALGORITHM

According to earlier research from University of California at Berkeley, and from Zero Knowledge Systems Incorporation on RC4 algorithm in WEP, the use of 24-bit initialization vector IV is not adequate because the same IV will be reused over a period of time [2][3]. This is called collision of key which hackers rely on in order get the cipher key. Let us look at this, a 24-bit IV generates 2^{24} or 16777216 ^{possible} key streams.

For a network running at 400Mbps and 2,000-byte packets,

$$\text{No. of Transmitted Packet in the network per second} = \frac{400Mbps}{2000 \text{ bytes} * 8 \text{ bits}}$$

$$= \frac{419430400}{16000} = 26214.4 \text{ Packets per second}$$

This shows that the network transmits 26,214.4 packets per sec.

Since different IV must be appended to each packet, then time to exhaust all the generated IV is:

$$= \frac{16777216 \text{ Possible IV}}{26214.4 \text{ Packet per second}}$$

= 640 seconds to exhaust all the IVs

= 10.67 minutes to exhaust all the available IVs

This analysis shows that for every 10.67minutes there will be repetition of IV on the packet on this network. Better still, for every 10.67 minutes there will be key collision. With this, it is assumed that only one device is connected if more devices is connected using the same initialization vector IV, the time will be reduced.

This means collision will occur in no time and once there is collision the hacker is having two different plain texts both encrypted with the same key stream. Then, it is possible for the hacker to XOR these two encrypted plain text. The XORing of these plain texts will nullify the key stream thereby decrypt the encrypted text as shown below.

E_1 = Encrypted text$_1$

E_2 = Encrypted text$_2$

T_1 = Text$_1$

T_2 = Text$_2$

IV = Initialization Vector

K = Secret Key

$\oplus$ = XOR

If $E_1 = T_1 \oplus RC4\ (IV, K)$ (0.1)

And, $E_2 = T_2 \oplus RC4\ (IV, K)$ (0.2)

Then $E_1 \oplus E_2 = (T_1 \oplus RC4(IV,K)) \oplus (T_2 \oplus RC4(IV,K))$ (0.3)

since $RC4(IV,K) \oplus RC4(IV,K) = 0$

$E_1 \oplus E_2 = T_1 \oplus T_2$

The above equation (0.3) shows that if there is collision of key, the exclusive OR of the two encrypted message will knock off the key leaving the exclusive OR of the two messages. Therefore, if a hacker has the inkling of one of the messages, he can decipher the other message. The above equations(0.1),(0.2) and (0.3) can be further explained diagrammatically.

Table I: RC4 to encrypt message 'a' using key 'n'.

	Data
Letter "a" $text_1$	01100001
Letter "n" RC4 Key	01101110
XOR "a" with RC4 key (E_1)	00001111

Table II: RC4 to encrypt message 'b' using key 'n'.

	Data
Letter "b" $text_2$	01100010
Letter "n" RC4 Key	01101110
XOR "b" with RC4 key (E_2)	00001100

Table III: Exclusive OR of message 'a' and 'b'

	Data
Letter "a" $text_1$	01100001
Letter "b" $text_2$	01100010
XOR "a" with "b"	00000011

Table IV: Exclusive OR of encrypted message 'E1' and 'E2'

	Data
Encrypted text1 (E1)	00001111
Encrypted text2 (E2)	00001100
E_1XOR E_2	00000011

These tables show that if there is collision, hacker will have two encrypted texts both encrypted with the same secret key. What hacker needs to do is exclusive ORing these encrypted texts in order to nullify the secret key, and the result will be XOR of the two text messages. This , therefore shows that if a hacker has the knowledge of the content of one of the text messages, when collision occur the hacker could then decrypt the other encrypted message. Thereby defeats the reason for encryption. This shows the greatest weakness of RC4 as an encrypting algorithm.

2.0 METHODS

RC42's – a NEW WAY TOWARD WLAN DATA PROTECTION

The previous section has shown weakness of RC4 through stream key collision which is the latent weakness of this algorithm. However, this algorithm can be improved on in order to make it overcome the weaknesses of stream key collision without increasing the size of the initialization vector field.

RC42's to the Rescue of RC4!

Collision of IVs makes RC4 ciphers to be more susceptible to decryption. Therefore, once the exclusive OR of two texts is obtained, at least the partial knowledge of one of the text leads attacker to decipher the other text.

RC42's uses the same concept as the RC4; however, it incorporates 2's complement to circumvent the effect of stream key collision in RC4. With RC42's, the message is exclusively OR with the stream key and two complement of the resulting encrypted message is taken. The result is the RC42's encrypted message which will be transmitted wirelessly.

At the receiving node, decryption takes place. The RC42's message is first decreased by one, and then it is de-complemented by inverting the resulting RC42's message. Then the secret key stream will be exclusively OR with de-complemented message this will give the plain message.

Effect of collision on RC42's encrypted message

Collision of RC42's encrypted messages can not knock off the key even if an attacker has the partial knowledge of the message. This can be proved by using the previous procedure which shows weaknesses in RC4 algorithm.

E_1 = Encrypted $text_1$

E_2 = Encrypted $text_2$

T_1 = $Text_1$

T_2 = $Text_2$

IV = Initialization Vector

K = Secret Key

$\oplus$ = XOR

[]'+1 = 2's complement

If $E_1 = [T_1 \oplus RC4\ (IV, K)]'+1$ (0.4)

And, $E2 = [T_2 \oplus RC4\ (IV, K)]'+1$ (0.5)

From equation(0.4) and (0.5) let's show tha

$E1 \oplus E_2 \neq [(T_1 \oplus RC4\ (IV, K))]' \oplus [(T_2 \oplus RC4\ (IV, K))]'+1 \oplus 1$ (0.6)

Proof

Since

$$[(T_1 \oplus RC4(IV,K))]'+1 \oplus [(T_2 \oplus RC4(IV,K))]'+1 = [(T_1 \oplus RC4(IV,K))]' \oplus [(T_2 \oplus RC4(IV,K))]'+1 \oplus 1 \quad (0.7)$$

Remember $1 \oplus 1 = 0$

This implies that,

$$[(T_1 \oplus RC4(IV,K))]'+1 \oplus [(T_2 \oplus RC4(IV,K))]'+1 \neq [(T_1 \oplus RC4(IV,K))]' \oplus [(T_2 \oplus RC4(IV,K))]' \quad (0.8)$$

Therefore,

$$E_1 \oplus E_2 \neq [(T_1 \oplus RC4(IV, K))]' \oplus [(T_2 \oplus RC4(IV, K))]' \quad (0.9)$$

This is proved diagrammatically in the next section, by using the RC42's algorithm on two message text 'a' and 'b' assuming that the secret key is 'n'.

3.0 RESULT and DISCUSSION

From equation (0.6) shows the effect of key collision on the RC42's encrypted messages. If there is collision of the key, exclusive OR of the two encrypted key will never knock off the key. This is proved in equation (1.8) and(0.9). Also, it is proved in table V, VI and VII that exclusive OR of the encrypted messages is not equal to the exclusive OR of the plain text. This proves that the key can not be knocked off as it is the RC4 algorithm. Table V (row 5) and table

	Data
$[(T_1 \oplus RC4\ (IV, K))]'$	11110000
$[(T_2 \oplus RC4\ (IV, K))]'$	11110011
$E_1 \oplus E_2$	00000101
$E_1 \oplus T_2$	00000011
$[(T_1 \oplus RC4\ (IV, K))]' \oplus [(T_2 \oplus RC4\ (IV, K))]'$	00000011

REFERENCES

1. Micheal Sutton "Hacking the Invisible network Insecurities in 802.11x". Available at www.idefense.com.
2. Kerry, Stuart J. "Chair of IEEE 802.11 Respond to WEP security flaws." Available at http://slashdot.org/articles/01/02/15/1745204.shtml.
3. University of Berkeley FAQ. Available at http://www.isaac.cs.berkeley.edu/isaac/wep.faq.html.
4. Fuhrer, Scott,Itsik Mantin and Adi shamir. "Weakness in the key scheduling Algorithm of RC4.". Available at http://online security.focus.com/data/library/rc4 ksaproc.pdf.