International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: 6.614
Available Online at www.journalijcar.org
Volume 7; Issue 5(L); May 2018; Page No. 13113-13116
DOI: http://dx.doi.org/10.24327/ijcar.2018.13116.2325

Research Article

A RESEARCH PAPER ON NETWORK SECURITY EMAIL ENCRYPTION

Jyoti Yadav[1] and Taruna[2]

[1]DPGITM, Maharishi Dayanand University, Haryana, India
[2]Department of computer Science and Engineering of DPGITM, Maharishi Dayanand University, Haryana, India

A R T I C L E I N F O

Article History:

Received 12th February, 2018
Received in revised form 9th March, 2018 Accepted 26th April, 2018
Published online 28th May, 2018

Key words:

Decryption, Electronic Mail Security, Encryption, AES, RC4 Algorithm, MIME

A B S T R A C T

The security of internet became a major concern and the security history allows a better understanding of the emergence of security technology. RC4 is a unique kind of design for a keystream generator. The large internal memory of RC4 and the updating dynamically of tables imply that RC4 is secure from conventional attacks on keystream generators. Over the past eight years RC4 has been extensively evaluated in the open literature. Several interesting properties of RC4 have been discovered, and some weaknesses of the original initialization process have been found. However, to date there has been no weakness discovered that is serious enough to conclude that RC4 is insecure for use. Our research reveals that using a word size of n = 8 and suppressing the first few output bytes prevents most attacks. In this paper RC4 based encryption algorithmic rule is pre-owned to secure Email communications. Protecting our incoming and outgoing emails is a top priority for us, which is why we are always working to improve mail flow encryption. The trend toward converged networks where voice, IP, video and wireless are combined over the same network infrastructure offers significant - and highly attractive - benefits. But this union introduces new vulnerabilities and new opportunities to break into the network and so we need converged security. In this paper we investigate the possibility of using RC4 to secure emails. RC4 based encryption algorithm is used to ensure secure Email communications.

INTRODUCTION

Email Security and security services in RC4 become top priority**.** E-mails have become an integral part of everyday life. For many years now, this medium has been used as a fast and uncomplicated way to communicate. As a communications media, e-mail is unsafe to risks such as monitoring of e-mail content, faking of an e-mail identity, spam. Users are not always able to detect such threats at first glance. It is possible, for example, for third parties to read or falsify unsecured messages during transport. There is a danger of e-mails that are being misdirected without the sender or the recipient ever knowing that it happened. This can cause incalculable damage for both parties. One of the reasons RC4 is used for encryption is its speed. RC4 algorithm has a fast speedencryption algorithm and it can be implemented easily on a wide variety of hardware. After all, RC4 dates back to 1987.

RC4

The first known use of a dynamic permutation in stream cipher design was RC4, designed by Ron Rivest in 1987. The algorithm details remained proprietary until 1994 when it was posted to anmailing list of internet.

Corresponding author:* **Jyoti Yadav
DPGITM, Maharishi Dayanand University, Haryana, India

The common use of this cipher in communications protocols such as SSL and WEP may make RC4 the world's most widely used stream cipher.

The RC4 algorithm is divided into two parts (we let n=8 be the nominal word size):

- Initialisation mode: accepting a variable key as a sequence of bytes
- Output mode: producing a pseudo-random byte sequence

Both these modes update the table of 256 bytes. The complete algorithm is given below

Initialisation Mode

Input: n=8,
key length (in bytes) = k;
S[i]=i for i=0 to 255
Key : K[0…(k-1)]
j=0;
For i=0 to (n-1)
j=j+S[i]+K[i mod k]
swap(S,i,j)
i=j=0;

Output Mode

Repeat

i=i+1
j=j+S[i]
swap(S,i,j)
output=S[S[i]+S[j]]
Until done

Let the k-word key be given in the array K[0…(k-1)]. The parameter n indicates the bit-width of the permutation S, which occupies $n*2^n$ bits of memory. For real applications, n=8 is used as it is a good trade-off between security and memory requirements, and it is also natural and easy to implement. Two extra bytes of memory, i and j, are used as pointers into the table. One byte pointer is incremented mod 2^n and the other takes on pseudo-random values generated by table lookups (and also by the key in Initialisation mode). The function swap (S,a,b) swaps the values in S[a] and S[b], thus updating the table while conserving the permutation property. These are both already in temporary variables, so the swap operation takes 2 clock cycles.

The algorithm of RC4 can be seen to have 4 stages. The essential parts of this cipher are:

- A simple basic counter, modulo the table size
- Another pointer that is updated using a table value
- Output a value that depends on table value of both pointers
- Update the table

A simplistic model of software suggests that RC4 uses 2 operations for each of these stages, and so, given some system inefficiencies, should run at a little less than the underlying clock speed in software. This is confirmed by some optimised implementations of the evaluators. The memory requirements are 256 bytes for the dynamic table and a few other bytes for the pointers and temporary values. This is just over ¼ Kbyte memory and so it is suited for small applications with restricted memory.

RC4 is one of the encryption method supported by HTTPS protocol, which will ensures the security of web communications.

As explained, outlining the threat, obtaining a cookie can enable an attacker to log into a website as if they were the target. The attacker can then perform actions such as posting status updates and sending messages, or gain access to personal information such as emails and chat history.

Comparision between AES and RC4

The most important reason why RC4 is very accepted is the fact that it is simple and it can be faster.

RC4 is much business oriented as AES makes the system slower (compared to RC4), leading to the risk that customers might have to wait too long because the encryption/decryption algorithm takes more time, and the customer might choose another provider. Cloud provider Google.com, Social networking portal Facebook.com (Billions of users) etc providers use RC4.

Pros of RC4

- RC4 is a simple encryption standard.
- It is faster compared to AES.
- Software based implementation is possible therefore no limitation on its frequent application.

Cons of RC4

- It is not considered to be as secure as AES is.
- RC4 is not that much effective when it is used as a block cipher.

Although RC4 is not as secure as AES but its straightforwardness and faster processing capability make this proposed authentication system more secure and it will acceptable to the users.

RC4 is one of the most accepted stream cipher of its simplicitystructural, encryption and decryption speed and its efficiency.

Users still uses RC4

Firstly, lots of people using older "candy bar" style phones. Mobile Phones like the Nokia 6120 classic which was released in 2007 (and is the phone with the greatest number of RC4 requests to CloudFlare sites: 4% of the RC4-based requests in the measurement period), the Lemon T109 or the Sony Ericson K310 which was released in 2006.

And, of course, it's not all older telephones being used to visit CloudFlare-powered web sites. There are old browsers too.

Another source of RC4-only connections is older versions of Adobe AIR. AIR is used for games and if the users do not update the runtime of AIR they can end up by using the older RC4 cipher.

Yet another source is stand-alone software that makes its own SSL connection. We've seen some software checking update servers using RC4-secured connections. The software will makea connections to its own updated server using HTTPS but the ciphers that is available are limited and RC4 is chosen. The command-line program curl was used to generate 1.9% of RC4-based requests to CloudFlare sites (all done with versions dating to 2009).There's also quite a bit of older Microsoft Internet Explorer around including Internet Explorer 5.01 (which dates back to 1999!). Here's a breakdown of Internet Explorer versions connecting using RC4:

Related Study

In 2012, Bao *et al*. [1] proposed a chaotic framework having the capability of high sensitivity to the security keys, and a sufficiently large key space. They have suggested that it can resist the brute force attack. In 2012, Abusukhon *et al*. [2] has been proposed an encryption method based on the transformation of a text file into an image file which can be replicated and rely on the client and server. They have analyzed the possible key permutations also. In 2012, Zhang *et al*. [3] proposed a multi-beneficiary time signcryption concern, and front criss-cross the signcryptionare out of it.

In 2013, Rahman *et al*. [4] analyzing, and endeavor the procedure for authorizing and reinforcing proficient and successful Attach. Opportune to the cumbersome storing up on the internet, importune upkeep, and related fasten attacks, data experts face challenges in surveying shot of their systems. The obligation of scene might change with the endeavor's necessities. In 2013, Ramaiya *et al*. [5] proposed a method for image steganography, which is based on the data encryption standard (DES) capable of using 64 bit block size of plaintext

and 56 bits of secret key. They have suggested that this method is able to provide a high level of security because image extraction is not possible without the knowledge of mapping rules of S -Box and secret key. In 2013, Ahirwal *et al*. [6] suggested a signcryption method which is based on elliptic curve cryptography (ECC). The main feature of this method is an elliptic curve is used for both encryption and signature generation. The transmitted message is sent in this method in the form of point which is embedded in elliptic curve which is efficient and safe.

Performance

- Each of the UDI implementations is a hardware block specifically designed for the implementation. RAM space is required by the key byte generator to locally maintain the state table for key generation. This state would need to be preserved and restored in case of a context switch if other processes would need the same functionality. This overhead is not considered in the above performance projections. Encryption and decryption state data may be stored in separate state memories to allow for independent processes.
- The following table summarizes the number of MIPS required for the algorithm encryption/decryption for 1 million bits per second for each of the three implementations.

	MIPS	RAM
Optimized MIPS Assembly	2.5	None
RC4 Operation Support UDI Primitives	1.75	0 bytes
RC4 Key Byte Generator UDI Accelerator	0.22	256 bytes

Background

SSL (Secure Socket Layer) is one of the security protocols to achieve secure communications over a TCP/IPnetwork. SSL has two types of authentication modes, Server Authentication mode and Client Authentication mode.The Secure Socket Layer security protocol provides server authentication, data encryption, message integrity check, and additional client authentication for a transmission control protocol (TCP)/IP connection [7].

The communication using HTTPS is triggered when a client send a request to the server by specifying an URL onHTTPS protocol using port number 443. The web server, providing a service for HTTPS, responds the client bysending the certificate to the client side. The web browser signifies a public key of the web server, packed in thecertificate. The key is used to encode the information that the client sends consecutively to the web server.

Technically, the initial information that the client sends to the web server is a session key, which would be utilizedfor further data transmission between the client and the web server. Consequently, web server uses its private key todecode the information (session key) transmitted by the client. As a consequence, only either the web server or theclient understands the session key and that the further transmission remains secured [8]. RC4 has a innerstate that is secret permutation of all the N = 2n possible n bits words, with two indices. In practicalapplications n = 8, and thus RC4 has a huge state of log2(28! x (28)2) = 1700 bits of solution space.

This willprovides Obscureemailto protectaddresses of email from harvesting a bots on mailto links generated by the Drupal l() function by unclear addresses of email addresses that are found in mailto links and its link text. A RC4original email addressciphertextare saved and is then decrypted and reinserted back to HTML by Javascript, providing a transparent experience to sites where a number of users are using a Javascript-enabled browser, at the same time prevents non-Javascript capable bots from harvestingaddresses of email. We make good use of the RC4 stream cipher for saving and restoring plain text email addresses, hence "RC4 email".

Security Analysis

- A detached signature is useful in several contexts. A user may like to set a separate signature log for all mails sent or received. A detached signature of an executable program can bedetect subsequent virus infection. So, detached signatures can be used when more than one party must sign a document, such as a legal contract. Each person's signature should be not dependent and therefore is applied only to the document. If not in that situation, the signatures will be nested, then with the second signer signing both the document and the first signature, and so on.
- RC4 converts a raw 8-bit binary stream to a stream of printable ASCII characters. Each group of three octets of binary data is mapped into four ASCII characters.
- E-mail facilities often are restricted to a message length that is maximum.
- RFC 822 defines a format for text messages that are sent using e-mail.
- MIME (Multipurpose Internet Mail Extension) is an extension to the RFC 822 framework that is intended to address some of the main problems and limitations for the use of SMTP (Simple Mail Transfer Protocol) or some other mail transfer protocol and RFC 822 for electronic mail.
- S/MIME is a secure security enhancement to the MIME Internet e-mail format standard. It based on the technology that is from RSA Data Security.

RESULTS

The RC4 was statistically tested against wide range of tests for inspecting the validity of the encryption, and it's mathematically measured for encryption efficiency. All the consequent proves that RC4with suitable key length is highly secure and efficient enough to be used within the converged network.

CONCLUSIONS

In this paper, we have presented the email security survey on the RC4 since its first public appearance to date. It is found that the simple and robust structure of RC4 is still attracting the community. It is extensively deployed in wireless network and internet protocols. We have presented a broad explanation of RC4 followed by the measure taken by various researchers to improve the security of emails. Although many improved variants of RC4 which removes the existing weaknesses and enhance the security of emails found in the literature. Further inspite of all the developments reported in the literature, there are still many open research challenges and issues related to searches of more biases, key collisions in keystream, and key

recovery attack on WPA. Therefore it is concluded that there is ample scope to further investigate the issues in RC4 particularly the non-random behavior of bytes in the state permutation, and to develop a new, more efficient and effective RC4 encryption algorithm

Future Scope

There is obviously scope for improvement and future work. The possible improvements to our work can be:

'Nature is full of surprises; we just need to explore new possibilities.' The present work found new dimensions to RC4 algorithms and operations applicable on them. The work may be extended by use of higher order or complex structures and/or related operations in development of some more new RC4 algorithms. The techniques discussed in this work may be applied to other popular ciphers that use two dimensional structures to enhance their security. This may be used to produce more complex algorithms based on the proposed work.

References

1. Bao L, Zhou Y, Chen CP, Liu H. A new chaotic system for image encryption. In international conference on system science and engineering, 2012 (pp. 69-73).IEEE.
2. Abusukhon A, Talib M. A novel network security algorithm based on Private Key Encryption. In 2012 international conference on cyber security, cyber warfare and digital forensic (CyberSec) 2012 (pp. 33-7).IEEE.
3. Zhang J, Chen Z, Xu M. On the security of ID-based multi-receiver threshold signcryption scheme.In international conference on consumer electronics, communications and networks (CECNet) 2012 (pp. 1944-8).IEEE.
4. Rahman MA, Al-Shaer E. A formal approach for network security management based on qualitative risk analysis.In international symposium on integrated network management 2013 (pp. 244-51).IEEE.
5. Ramaiya MK, Hemrajani N, Saxena AK. Improvisation of security aspect in steganography applying DES.In international conference on communication systems and network technologies (CSNT) 2013 (pp. 431-6).IEEE.
6. Ahirwal R, Jain A, Jain YK. Signcryption scheme that utilizes elliptic curve for both encryption and signature generation. *International Journal of Computer Applications.* 2013; 62(9): 41-8.
7. ThawatchaiChomsiri Faculty of Informatics, Mahasarakham University, Mahasarakham 44150, Thailand. thawatchai@msu.ac.th, HTTPS Hacking Protection.
8. Scott Fluhrer, ItsikMantin, and Adi Shamir 2002, Weaknesses in the Key Scheduling Algorithm of RC4, Springer-Verlag London, UK 2001.

How to cite this article:

Jyoti Yadav and Taruna (2018) 'A Research Paper on Network Security Email Encryption', *International Journal of Current Advanced Research,* 07(5), pp. 13113-13116. DOI: http://dx.doi.org/10.24327/ijcar.2018.13116.2325

****