Dr Lazar Stošić*
Visoka škola za vaspitače strukovnih studija,
Aleksinac, Republika Srbija

UDK 004.421
Stručni članak
Primljen: 02. II 2013.

SIGURNOST RC4 I WEP

SAŽETAK: U radu je prikazan osvrt na neke slabosti RC4 algoritma koji su prikazani tokom istraživanja mnogih autora. Prikazane su neke od prednosti i nedostataka, sličnosti i razlike RC4 algoritma koji su dobijeni u brojnim istraživanjima kao i princip rada KSA i PRGA algoritma. Pokazaće se da je RC4 algoritam potpuno nesiguran u zajedničkom načinu rada koji se koristi u WEP (Wired Equivalent Privacy Protocol) protokolu. Prikazaće se da 802.11 WEP je potpuno nesiguran i biće objašnjeni njegovi nedostaci.

KLJUČNE REČI: RC4 algoritam, WEP, WEP napad, KAS, PRGA, sigurnost.

1. Uvod

Jedan od najčešće korišćenih kriptosistema na internetu je simetrični ključ enkripcionog algoritma RC4. RC4 je dizajnirao Ronald LinRivest (engl. *Ronald Linn Rivest*) još 1987. godine za RSA Data Security, Inc. Ronald Rivest je bio poznat jos po svom radu na javnom ključu enkripciji sa svojim kolegama Leonardom Ejdlmanom i Adijem Šamirom na RSA algoritmu za koji su dobili Tjuringovu nagradu 2002. godine. RC označava „Rivestovu brojku ili kod“. RC4 je bio strogo čuvan sve do 1994. godine kada je postao dostupan za javnu analizu i proveru [1]. RC4 je standardizovan od strane IETF pod imenom „Arcfour“ [6] mada RSA DSI nije potvrdio da je objavljen. RC4 se najčešće koristi kao podrazumevana šifra za SSL (Secure Sockets Layer) da bi zaštitio saobraćaj na internetu, TLS (Transport Layer Security) protokolaida štiti bežične mreže kao deo WEP(Wired EquivalentPrivacy) i WPA (Wi-Fi Protected Access) protokole [16].

2. WEP – Wired Equivalent Privacy

Svi računari imaju bezbednosni protokol koji se zove Wired Equivalent Privacy (WEP). Uređaji koriste karticu 802.11 konfigurisanu sa ključem, koji se u praksi najčešće sastoji od lozinke ili ključa izveden iz lozinke. Potencijalni rizici sa pojavom bežičnih mreža su se mnogostruko povećali. Postavljanjem većeg broja „pristupnih tačaka“ otvara se mogućnost krađe i upada u računar korisnika. Bežične mreže su definisane u IEEE 802.11, koji je doneo IEEE (Institut inženjera elektrotehnike i elektronike inženjera). Prvobitna verzija IEEE 802.11 standard sa 2,4 GHz frekvencije i dve brzine prenosa podataka (od 1 i 2 Mb/s) formirana je sredinom 1997. godine. U početku je bio namenjen za mobilne računarske uređaje (laptop računari, internet pristup, VoIP, igre...).

WEP (Wired Equivalent Privacy) je bezbedonosni algoritam za IEEE 802.11 bežičnu mrežu. To je protokol za enkripciju bežično prenosivih paketa na IEEE 802.11 mrežama. Mreže koje su zaštićene WEP protokolom se šifruju pomoću RC4 algoritma pod zajedničkim ključem. Uloga WEP je bila da obezbedi poverljivost podataka. Uveden je kao deo originalnog standarda

* lazarstosic@yahoo.com

802.11 još septembra 1999. godine. Prepoznatljiv je po ključu 10 ili 26 heksadecimalnih šifara. I pored toga što je postavljen kao vrsta zaštite, WEP se pokazao da ima brojne nedostatke i da je zastareo i njegovo mesto od 2003. godine zauzimaju novi standardi WPA (Wi-Fi Protected Access) i nešto kasnije standard 802.11 i poznat kao WPA2.

WEP protocol je dizajniran da obezbedi privatnost paketa zasnovanih na bežičnim mrežama na osnovu 802.11b standarda [9]. Zaštita se vrši tako što WEP koristi 40-bitni tajni ključ koji je zajednički između svih korisnika i mrežne pristupne tačke. Pošto je poznato da se podaci šalju putem paketa, za svaki paket pošiljalac bira novi 24 bitni inicijalizacioni vektor (IV) kao i 64-bitni RC4 ključ za spajanje izabranog IV. Pri svakoj inicijalizaciji računari resetuju IV na 0 i zatim ga povećavaju za 1.

U ovom principu rada slabost je u maloj veličini tajnog ključa i IV: 40-bitni ključ može da se otkrije u toku jednog dana. Ograničena veličina prostora IV od 2^{24} podrazumeva da se ponovo koristi IV tokom šifrovanja svakog paketa. Izgradnjom rečnika svih 2^{24} IV omogućava se otkrivanje šifre. WEP nema mehanizam za promenu deljenog ključa pa se sami ključevi retko menjaju, a samim tim povećava se i verovatnoća napada. Prvu analizu projektnih neuspeha WEP protokola su objavili Borisov, Goldberg i Vagner [11] još 2001. godine. Ova analiza je pokazala da IV štiti samo od slučajnih grešaka, ali ne i od zlonamernih napadača.

Mantin [4] i Mironov [5] su analizirali distribuciju KSA izlaza. Njih dvoje su izračunali, za svaku vrednost permutacije, distribucije njihovih lokacija u KSA finalnu permutaciju i prikazali da mogućnost vrednosti a raste na kraju lokacije b u S na kraju KSA procesa (1) i (2).

$$P[S^*[b] = a] = \begin{cases} p(q^a + q^{\bar{b}} - q^{a+\bar{b}}) & a \leq b \\ p(q^a + q^{\bar{b}}) & a > b \end{cases} \tag{1}$$

Gde je S^* KSA izlazna permutacija.

$$\bar{x} \stackrel{def}{=} N - 1 - x, p = 1/N, \quad q = 1 - p. \tag{2}$$

Fluhrer, Mantin i Šamir su prikazali vezu između ključa i napada na RC4 [14] koji se koristi u WEP protokolu. U WEP protokolu algoritam ne koristi ni jedan 64-bitni paketni ključ (40-bitni tajni ključ, plus 24-bitni IV) ili 128-bitni ključ (104-bitni tajni ključ, plus 24-bitni IV) da podesi RC4 niz S, koji je permutacija od {0, ..., 255}. Izlazni generator koristi niz S, kao i dva brojača i i j da bi stvorio niz pseudoslučajnih sekvenci. Takođe su objasnili da su prve x reči KSA ključa poznate. To omogućava da se simuliraju prve runde x na KSA i izračuna permutacija S_{x-1} i indeksi i_{x-1} i j_{x-1} u tom trenutku. Sledeću vrednost i je takođe poznata ($i_x = x$), ali sledeća vrednost j(j_x) zavisi od nepoznate ciljne ključne reči K [x] (od $j_x=j_x-1+S_{x-1}[x]+K[x]$) i na taj način svaka od vrednosti j_x i K [x] se može lako izvesti iz drugog. Shodno tome, s obzirom na S[x], možemo izračunati čija je vrednost bila u poziciji j_x u poznatoj permutaciji S_{x-1}, i preokrenuti ovu permutaciju, možemo oporaviti vrednost j_x.

Stubble-field et al. [15] su pokazali da bi bilo potrebno da IV ima tzv. „rešeno stanje“ i da je potrebno oko 4 miliona različitih kadrova koje treba biti uhvaćeno da bi se izračunao ovaj napad. Za razliku od njih, Klajn [7] je pokazao poboljšanu verziju napada na RC4 koristeći

povezane ključeve koji, po njemu, ne treba da imaju "rešeno stanje" na IV i dobija znatno smanjeni broj kadrova.

3. Simetrični ključ enkripcionog algoritma − RC4

RC4 se sastoji od dva algoritma: Key Scheduling Algorithm (KSA) i Pseudo Random Generation Algorithm (PRGA).

KSA koristi tajni ključ za kreiranje pseudo-slučajnog početnog stanja. On pretvara, slučajnim izborom, ključ (čija je veličina tipičnog 40-256 bita) u početnoj permutaciji S na {0,...,N-1}. Ažuriranje indeksa j zavisi od tajnog ključa, dok se ključ ne koristi u PRGA.

Pseudo Random Generation Algorithm (PRGA) generiše pseudo slučajni protok do pseudo slučajni niz izlaznih podataka. On generiše dva indeksa i i j na 0, a zatim preko petlje uz četiri jednostavne operacije povećava slučajno vrednost j i izlaznu vrednos S prikazuje $S_{[i]+}S_{[j]}$. KSA i PRGA algoritmi su prikazani na slici 1.

KSA(K)	PRGA(S)
Initialization: For $i = 0$ to $N - 1$ $S[i] = i$ $j \leftarrow 0$ Scrambling: For $i = 0$ to $N - 1$ $j \leftarrow j + S[i] + K[i \bmod l]$ Swap$(S[i], S[j])$	Initialization: $i \leftarrow 0$ $j \leftarrow 0$ Generation loop: $i \leftarrow i + 1$ $j \leftarrow j + S[i]$ Swap$(S[i], S[j])$ Output $S[S[i] + S[j]]$

Slika 1. The RC4 Algorithms
(The Key Scheduling Algorithm and the Pseudo-Random Generation Algorithm)

U svakoj iteraciji PRGA povećava i gleda na elemente S, S(i), i dodaje da j razmeni vrednost S(i) i S(j), koristi zbir S(i)+S(j) po modulu 256 kao indeks kako bi dobio treću vrednost S. Svaki element S je zamenjen sa drugim elementom najmanje jednom svakih 256 iteracija. Ako izuzmemo nekoliko manjih detalja KSA i PRGA su skoro isti.

Najvažnija slabost RC4 potiče od nedovoljnog ključnog rasporeda koji se može ispraviti jednostavnim odbacivanjem dela izlaznih podataka (RC4-dropN, gde je N obično više od 256)[5]. RC4 vrši permutaciju svih N=2n mogućih n bita rečima. Na primeru n=8 RC4 daje (3)

$$\log_2([[256]]^2 \cdot |S_{256}|) = \log_2(2^{16} \cdot 256!) \approx 1700 \text{ bits} \quad (3)$$

Konačnu vrednost koju daje RC4 zavisi od promenljive vrednosti KSA (Key-Scheduling Algorithm) algoritma. RC4 se sastoji od 256-bitna niza S, definisanje permutacija, kao i dva cela broja u rasponu $0 \leq i; j \leq 255$.

RC4 taster za podešavanje pokreće unutrašnje stanje koristeći ključnu K do 256 bajtova. RC4 tasteri su 2048 bita dugi, a njihove unutrašnje stanje se sastoji od dva indeksa *ii j*, plus niz od 256 8-bitnim bajtovima, pod nazivom S-boks.

S-boks je inicijalizovan pomoću tastera K (4):

```
for  i = 0 to 255
        S(i) = i
        j = 0

for  i = 0 to 255
        j = (j + S(i) + K(i)) mod 256
        swap S(i) and S(j)

i = 0
j = 0
```
(4)

Svaki sledeći bajt b je proizveden korišćenjem (5):

```
i = (i + 1) mod 256
j = (j + S(i)) mod 256
swap S(i) and S(j)
b = S(S(i) + S(j)) mod 256
```
(5)

Ključ se ponavlja onoliko puta koliko je potrebno da se popuni 2048-bitni ključ. RC4 samo štiti tajnost poruke a ne njen integritet. Kada se jednom S-boks pokrene ključem RC4 algoritam se ponaša kao petlja koja ažurira unutrašnje stanje S-boksa i vraća bajt.

Već je rečeno da se RC4 koristi za zaštitu SSL (Secure Sockets Layer) da bi zaštitio saobraćaj na internetu, TLS (Transport LayerSecurity) protokola i da štiti bežične mreže kao deo WEP (Wired EquivalentPrivacy) i WPA (Wi-Fi Protected Access) protokole kako bi se onemogućio njihov napad. Napad na ove protokole su opisali Fluhrer, Mantin and Shamir [14]. Oni su šifrovali pojedinačne karaktere (uglavnom binarne šifre) jednog teksta. Za razliku od RC4 koji je simetrični ključ, enkripcionom šemom, *Blum-Goldwasser probabilistic public-key schema,* opisana u [10] je primer asimetričnog ključa. Isti algoritam se koristi i za šifrovanje i dešifrovanje podataka. Ključ koji se koristi je potpuno nezavistan od teksta koji se koristi za šifrovanje jer koristi promenljivu dužinu od 1 do 256 bita. Ova dužina omogućuje biranje i generisanje pseudoslučajnih bita koji omogućuju šifrovanje poruke.

Koraci RC4 algoritma za šifrovanje su [18]i [19]:

1. Prikupite podatke koje treba da šifrujete i odaberite ključ;
2. Kreirajte dva niza brojeva;
3. Inicirajte jedan niz brojevima od 0 do 255;
4. Popunite drugi niz odabranim ključem;
5. Randomizujte prvi niz u zavisnosti od niza ključa;
6. Randomizujte prvi niz u okviru njega samog kako biste generisali konačni tok ključa;
7. Izvršite EKSILI operaciju (XOR) između konačnog toka ključa i podataka koje treba šifrovati kako biste dobili šifrovani tekst.

Jedna od slabosti inicijalizacije RC4 algoritma je glavna statistička pristrasnost u distribuciji prvih izlaznih reči. Ova pristrasnost pravi trivijalnu razliku između nekoliko stotina kratkih izlaza RC4 i slučajnim nizom analizirajući njenu drugu reč. Prikazana slabost se može koristiti za pravljenje šifre za napad na RC4 u nekim elektronskim aplikacijama, u kojima se isti otvoreni tekst može poslati na više adresa pod različitim ključevima. Ovo jedinstveno statističko ponašanje je nezavisno od KSA i dalje se primenjuje čak i onda kada RC4 počinje sa permutacijom slučajnih izbora.

RC4 prednosti [18]:

1. Teškoća određivanja koje lokacije u tabeli se koriste da bi se izabrala svaka vrednost u nizu;
2. Poseban RC4 ključ se može koristiti samo jednom;
3. Šifrovanje je 10 puta brže nego DES.

RC4 slabosti [18] i [19]:

1. RC4 algoritam je ranjiv na analitičke napade formulisanih tabela [3]i [17];

2. Slabi ključevi su identifikovani kriptoanalizom koja je u stanju da pronađe okolnosti pod kojima su jedan ili više generisanih bajtova u snažnoj korelaciji sa malim podskupom ključnih bajtova. Ovi ključevi se mogu pojaviti u jednom od 256 generisanih [13], [2] i [17].

4. Zaključak

Ovaj rad prikazuje ustanovljene i prikazane nedostatke RC4. Inicijalizacija pseudoslučajnih indeksa j do 0 predstavlja najveći problem. Slabost IV se može izbeći korišćenjem složenije inicijalizacije od j. Snaga RC4 ključa ne raste linearno sa povećanjem dužine ključa. Ako RC4 koristi ključeve duže od uobičajenih 128 bitnih savetuje se da se odbaci prvih 256 bajta. Odbačeni prefiks treba da raste na isti način (eksponencijalno) kada se vrši proširenje RC4 reči na 16 bita [8]. Ovo se preporučuje zbog bržeg šifrovanja velike količine podataka.

RC4 ključ se može koristiti samo jednom. Neke od prednosti RC4 su što se teže nalazi mesto u tabeli koje se koristi za izbor svake vrednosti u nizu. Nasuprot tome slabosti su da je RC4 ranjiv na napade.

Mnogi napadi da se probije RC4 su klasifikovani kao prepoznatljivi napadi. Mogući napad se može izvesti ako izvedemo proizvoljno dug ključ u vremenu koji raste linearno sa svojom dužinom. IV štiti samo od slučajnih grešaka ali je bezuspešan od zlonamernih napada. Međutim, snaga RC4 ne raste linearno sa povećanjem dužine ključa.

LITERATURA

[1] B. Schneier (1996). *Applied Cryptography*, John Wiley and Sons, New York, 2nd edition.

[2] E. Biham and Y. Carmeli (2008). "Efficient Reconstruction of RC4 Keys from Internal States", FSE 2008, (pp. 270-288), vol. 5086, Lecture Notes in Computer Science, Springer.

[3] G. Paul, S. Rathi and S.Maitra (2008). "Non-negligible Bias of the First Output Byte of RC4 towards the First Three Bytes of the Secret Key", Proceedings of the International Workshop on Coding and Cryptography (WCC) 2007, pp. 285-294 and Designs, Codes and Cryptography Journal, (pp. 123-134), vol. 49, no. 1-3, December 2008.

[4] I. Mantin (2001).The Security of the Stream Cipher RC4. Master`s thesis. The Weizmann Institue of Science. Octobar 2001.http://www.wisdom.wizmann.ac.il/~itsik/RC4/thesis.html

[5] I. Mironov (2002). "(Not So) Random Shuffles of RC4", *Advances in Cryptology – CRYPTO 2002*, Lecture Notes in Computer Science, 2442, Springer-Verlag, (pp. 304–319),doi:10.1007/3-540-45708-9_20, ISBN 3-540-44050-X, Cryptology ePrint Archive: Report 2002/067, retrieved 2011-11-04.

[6] K. Kaukonen and R. Thayer (1999). "A Stream Cipher Encryption Algorithm *Arcfour*", http://tools.ietf.org/html/draft-kaukonen-cipher-arcfour-03,*Internet Engineering Task Force (IETF)*, July 1999.

[7] Klein A. (2008). "Attacks on the RC4 stream cipher", volume 48 Issue 3, (pp. 269 – 286), *Designs, Codes and Cryptography*, September 2008.doi>10.1007/s10623-008-9206-6.

[8] L. Stošić, M. Bogdanović (2012). RC4 stream cipher and possible attacks on WEP, *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 3, No. 3, march 2012, (pp. 110-114), ISSN 2156-5570 (Online), ISSN 2158-107X (Print), https://www.thesai.org/Downloads/Volume3No3/Paper19-RC4_Stream_Cipher_And_Possible_Attacks_On_WEP.pdf

[9] LAN/MAN Standard Committee (1999). *Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*, 1999 edition, IEEE standard 802.11, IEEE Computer Society.

[10] M. Biriyukov, A. Shamir, and D. Wagner (2000). "Real time cryptanalysis of A5/1 on a PC", FSE: Fast Software Encryption, (pp. 1-18).

[11] Mantin (2001). The Security of the stream cipher RC4. Master`s thesis. *The Weizmann Institue of Science*. Octobar 2001.http://www.wisdom.wizmann.ac.il/~itsik/RC4/thesis.html

[12] N. Borisov, I. Goldberg, and D. Wagner (2001). "Intercepting mobile communications: the insecurity of 802.11", *In ACM MobiCom 2001*, (pp. 180-189).ACM Press, 2001.

[13] R. Basu, S. Maitra, G. Paul and T. Talukdar (2009). "Some Sequences of the Secret Pseudo-random Index j in RC4 Key Scheduling", Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error Correcting Codes (AAECC), June 8-12, 2009, Tarragona, Spain, (pp. 137-148), vol. 5527, Lecture Notes in Computer Science, Springer.

[14] S. R. Fluhrer, I. Mantin, and A. Shamir (2001). "Weaknesses in the key scheduling algorithm of RC4", In Serge Vaudenay and Amr M. Youssef, editors, *Selected Areas in Cryptography 2001*, volume 2259 of Lecture Notes in Computer Science, (pp. 1-24). Springer, 2001.

[15] Stubble, J. Ioannidis, and A. D. Rubin (2004). "A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP)", *ACM Transactions on Information and System Security*, Volume 7 Issue 2, May 2004, (pp. 319-332).

[16] T. Dierks and C. Allen (1999). *The TLS Protocol*, Version 1.0, Internet Engineering Task Force, January 1999.

[17] V. Tomašević, S. Bojanić, O. Nieto-Taladriz (2007). "Finding an internal state of RC4 stream cipher", *Information Sciences*, Volume 177, issue 7, 01. April, 2007, (pp.1715-1727).

[18] W. Mao (2004). *Modern Cryptography Theory and Practice*, Prentice Hall, New Jersey, 2004.

[19] W. Stilings (2006). *Cryptography and Network Security Principles and practices*, Fourth Edition, PEARSON, USA, 2006.

Lazar Stošić, Ph.D.

WEB SECURITY THROUGH WEP ALGORITHM USING RC4 ENCRYPTION

Summary

This paper presents a review of some of the weaknesses of RC4 algorithm, which are presented during the research of many authors. Some of the advantages and disadvantages are displayed, along with some similarities and differences of RC4 algorithm, which were obtained in a number of research studies as well as the working principles of KSA and PRGA algorithm. It will be shown that the RC4 algorithm is completely insecure in a common mode used in the WEP (Wired Equivalent Privacy) protocol. It will also be shown that 802.11 WEP is totally insecure and its shortcomings will be explained.

Key words: RC4 algorithm, WEP, WEP attack, KAS, PRGA, security.