Zaštita bežičnih komunikacija korišćenjem sopstvenog šifarskog algoritma

Aleksandar Jevremović, Mladen Veinović, Goran Šimić

***Sadržaj* — Zaštita bežičnih komunikacionih sistema za potrebe profesionalnih organizacija (vojska, vlade zemalja) predstavlja složen zadatak, posebno u situacijama kada je zaštitu potrebno obezbediti bez izmena nosećih hardverskih komponenata. U ovom radu opisan je proces obezbeđivanja bežičnih računarskih mreža na IP nivou korišćenjem sopstvenog šifarskog algoritma i standardnih otvorenih tehnologija i rešenja: IPsec, IKEv2 i Linux operativnog sistema. Dodatno, izvorni kod korišćenih komponenti je dostupan te je sve njihove funkcije moguće proveriti.**

***Ključne reči* — bezbednost, bežične mreže, ipsec, sopstveni šifarski algoritam.**

I. Uvod

Danas, tehnologije bežičnih računarskih mreža su u stanju da ponude visok nivo fleksibilnosti u LAN i WAN mrežnim okruženjima. Bežične mreže se mogu lako instalirati, popraviti, rekonfigurisati i uništiti (u slučaju potrebe). Ovakva vrsta fleksibilnosti je veoma poželjna kod dinamičnih primena, na primer za potrebe vojske. Međutim, takve profesionalne organizacije takođe zahtevaju i najviše nivoe zaštite podataka koji se prenose pomenutim komunikacionim kanalima. U takvim situacijama standardni bezbednosni protokoli za bežične mreže (WEP, WPA/WPA2, itd.) ne predstavljaju adekvatno rešenje [1,2,3,4]. To ne znači da upotrebu pomenutih bezbednosnih protokola treba eliminisati u potpunosti, već da oni ne smeju biti jedini bezbednosni protokoli za zaštitu poverljivih podataka u toku komunikacije.

U ovom radu opisan je proces uspostavljanja visokobezbedne bežične komunikacije korišćenjem standardnih i otvorenih tehnologija. Takođe, jedan od atributa od predstavljenog rešenja jeste i niska cena, direktno zavisna od standardnosti i rasprostranjenosti korišćenih tehnologija. Visok nivo bezbednosti ostvaren je korišćenjem sopstvenog algoritma za šifrovanje podataka. Za potrebe eksperimentalnih ispitivanja razvijen je sopstveni šifarski algoritam, nazvan MGAe2. Ovaj šifarski algoritam integrisan je u jezgro Linuks operativnog sistema a njegova upotreba se vrši putem IPsec bezbedosnog sistema. To znači da je sadržaj celokupne komunikacije šifrovan na IP (mrežnom) nivou OSI i TCP/IP modela i da ne postoji potreba za izmenom nosećeg bežičnog hardvera i protokola na sloju veze.

A. J. Autor, Univerzitet Singidunum u Beogradu, Srbija (telefon: 381-64-3093265; e-mail: ajevremovic@singidunum.ac.rs).

M. V. Autor, Univerzitet Singidunum u Beogradu, Srbija (telefon: 381-11-3093227; e-mail: mveinovic@singidunum.ac.rs).

G. Š. Autor, Vojna akademija u Beogradu, Srbija (telefon: 381-11-3600014; e-mail: gshimic@yahoo.com).

II. Sopstveni šifarski algoritam

Poznato je da se organizacije (vlade zemalja, vojska, obaveštajne službe) koje poseduju i razmenjuju osetljive podatke, ne mogu osloniti na javna bezbednosna rešenja i šifarske algoritme (DES, AES, i td.). Na primer, AES šifarski algoritam je jedan od najšire rasprostranjenih šifarskih algoritama u javnosti ali ga njegove dve karakteristike čine neprikladnim za upotrebu od strane profesionalnih organizacija:

1. najveća moguća dužina ključa od 256 bitova
2. javno dostupan način rada algoritma

Javna dostupnost načina rada algoritma podrazumeva mogućnost da napadač analizira algoritam i razvije „kontra algoritam“, odnosno, algoritam koji se može iskoristiti za razbijanje šifrata. Mala dužina ključeva čini vreme potrebno za razbijanje šifrata relativno kratkim ukoliko se razbijanje vrši na moćnim računarskim klasterima.

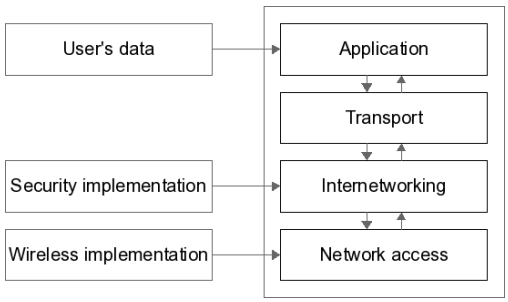
Za eksperimentalnu upotrebu razvijen je sopstveni šifarski algoritam (MGAe2). U pitanju je sekvencijalni šifarski algoritam sa podrazumevanom dužinom ključeva od 1024 bita. Takođe, dužina ključeva se može dodatno proširiti ukoliko postoji potreba za jačom zaštitom.

Još jedna stvar koju treba napomenuti je ta da je MGAe2 šifarski algoritam razvijen isključivo za eksperimentalnu upotrebu – za testiranje koncepta, procesa integracije i performansi rešenja. Podrazumeva se i čini osnovnu pretpostavku ovog rada, da će svaka profesionalna organizacija samostalno razviti šifarski algoritam za zaštitu svojih komunikacija.

Na strani implementacije, MGAe2 šifarski algoritam je kodiran u C programskom jeziku i integrisan je u jezgro Linuks operativnog sistema (verzija 2.6) korišćenjem standardnog kriptografskog API-ja. Na ovaj način je omogućena upotreba MGAe2 šifarskog algoritma od strane Ipsec sistema zaštite, kao i od strane ostalih programa koje koriste kriptografske funkcije kroz jezgro Linuks operativnog sistema.

III. Komunikacioni slojevi i arhitektura rešenja

Arhitektura rešenja predloženog u ovom radu biće analizirana kroz komunikacione slojeve TCP/IP modela. U tom modelu su specifični detalji vezani za bežične tehnologije smešteni u sloj zadužen za pristup komunikacionom mediju (engl. Network access layer). Predloženo mesto za integraciju sopstvenog šifarskog algoritma u predloženom rešenju jeste mrežni sloj (engl. Inter-networking layer).

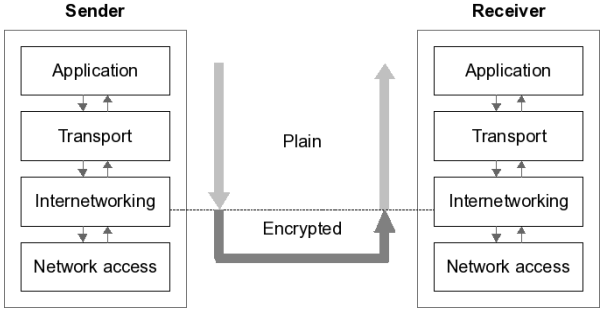


Slika. 1 – Komunikacioni slojevi i implementacije

Na osnovu prethodnih iskustava u ovom polju zaključeno je da implementacija bezbednosnog rešenja na nižem sloju stvara zavisnost od specifičnog hardvera. Takođe, implementacija na višim slojevima može biti znatno komplikovanija i pokriva manji skup protokola aplikativnog nivoa. Predložena arhitektura i mesto integracije bezbedosnog rešenja oslanja se na sledeće osnovne prednosti:

1. Propusti u protokolima vezanim za bežičan prenos podataka ne utiču na sveukupnu bezbednost sistema (koja se oslanja na viši komunikacioni sloj).
2. Nije potrebna izmena postojećeg hardvera, niti komunikacionog protokola sloja pristupa mreži.
3. Ceo sistem se može migrirati na neku drugu infrastrukturu (npr. kablovsku mrežu) bez potrebe da se prilagođava bezbednosti podsistem.

Predložena arhitektura obezbeđuje prenos šifrovanih podataka od mrežnog sloja na strani pošiljaoca do mrežnog sloja na strani primaoca.

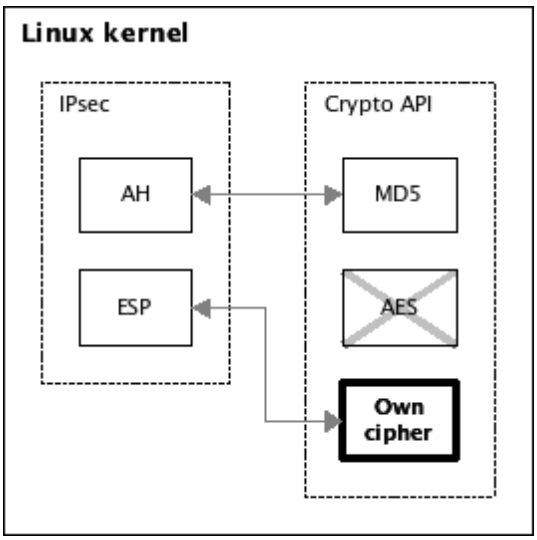


Slika 2 – Otvoren i šifrovan put podataka

Ovo čini ceo sistem otpornim na napade usmerene na komunikacioni kanal (koji su česti u slučaju bežičnih računarskih mreža). Sa druge strane, predloženo rešenje nije otporno na napade usmerene na interne magistrale pošiljaoca i primaoca.

Na nivou jezgra Linuks operativnog sistema, sopstveni šifarski algoritam je integrisan kroz dve komponente jezgra: Ipsec implementaciju i kriptografski API. Naš šifarski algoritam, MGAe2, napisan je na C programskom jeziku i preveden u izvršni oblik kao modul jezgra.

Standardni kriptografski API u jezgru Linuks operativnog sistema obezbeđuje unifikovani pristup svim uključenim šifarskim algoritmima svim internim i eksternim softverskim modulima. To znači da se uključeni šifarski algoritmi mogu koristiti i za druge namene (šifrovanje fajl-sistema i sl.), takođe. Ipak, bez obzira na to što pomenuta funkcionalnost predstavlja dodatnu prednost rešenja, takva upotreba izlazi van okvira postavljenih za ovaj rad.

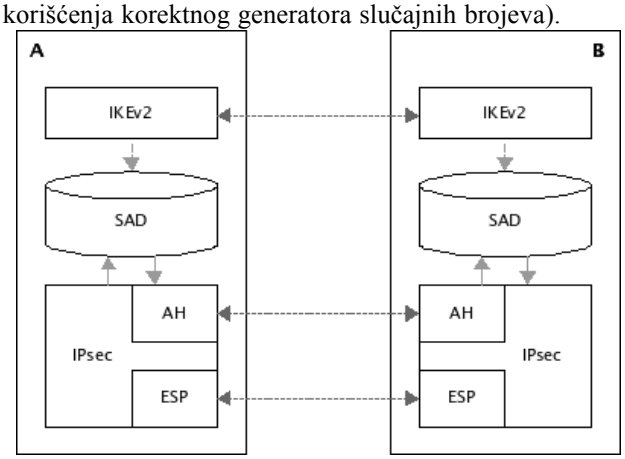


Slika 3 – Arhitektura na nivou jezgra operativnog sistema

IV. Izmenjena implementacija IKEv2 protokola

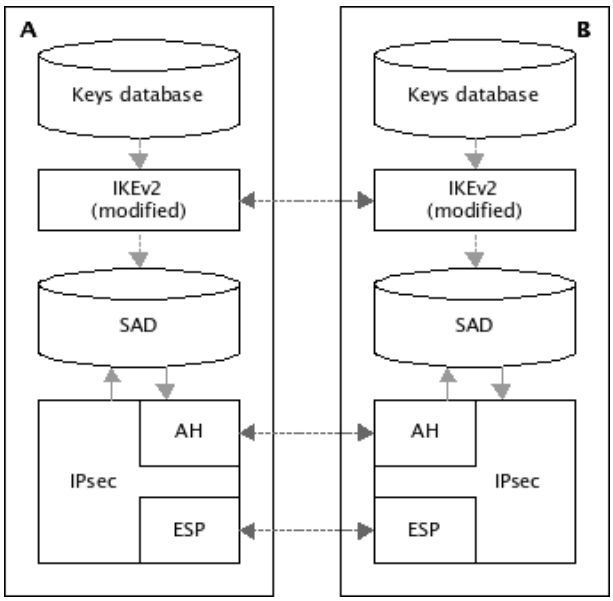
Jedan od najvažnijih koraka u obezbeđivanju bezbedne komunikacione platforme predstavlja obezbeđivanje adekvatnog sistema i polisa za razmenu ključeva. Podsistem zadužen za razmenu ključeva u opisanom kriptografskom sistemu baziran je na IKEv2 protokolu (Slika 4) sa dodatkom specifičnih i suštnskih izmena. U originalnoj postavci IKEv2 protokol koristi PKI infrastrukturu i Difi-Helman razmenu ključeva [6].

Difi-Helman je dobro poznata procedura za automatsko definisanje klasifikovanih simetričnih ključeva. Ova procedura je komplikovana za implementaciju, posebno kada su u pitanju ključevi velike bitske dužine a u potpunosti se uklapa u osnovni simetrični šifarski sistem. U predloženom rešenju, tajni simetrični ključevi se generišu putem nezavisnih uređaja koji garantuju kvalitet. U skladu sa tim, ključevi nisu samo tajni već i garantovanog kvaliteta (u slučaju korišćenja korektnog generatora slučajnih brojeva).



Slika 4 – Originalna IPsec/IKEv2 arhitektura

Predložena IKEv2 modifikovana implementacija (Slika 5) uključuje postojanje baze simetričnih ključeva (koja se distribuira putem odvojenih komunikacionih kanala). Ključ koji je ustanovljen preko IKEv2 protokola koristi se kao ključ sesije, i kao osnova za određivanje indeksa ključa (iz baze ključeva) koji će biti upotrebljen od strane šifarskog algoritma.



Slika 5 – Izmenjena IPsec/IKEv2 arhitektura

Pretpostavlja se da u bazi ključeva postoji veliki broj ključeva (najviše 2^{32}). Takođe, za svaki ključ je definisan i vremenski period validnosti (period u kome ključ može biti korišćen za šifrovanje). Na primer, ako bi se koristili ključevi dužine 1024 bita, za isti period validnosti u toku koga se koriste dva UNIX timestamp-a od 32 bita i 32 bita za indekse, indeks bi omogućio 4.294.967.296 ključeva u bazi podataka, sa ukupnom individualnom dužinom od 1120 bita. Ukupna veličina baze ključeva bi iznosila 560 gigabajta. U slučaju da se takva baza ključeva redovno koristi u toku jedne godine, 11.767.033 komunikacije dnevno mogle bi biti pokrivene jedinstvenim ključem.

V. Zaključak

Ovaj rad je fokusiran na obezbeđivanje sigurnih komunikacionih kanala za profesionalne klijente (vojsku, vladu, i sl.) korišćenjem standardne komunikacione opreme. Naši prethodni radovi [7,8,9,10,11] bili su usmereni na zaštitu kabliranih komunikacijonih kanala, ali naši skorašnji projektni zahtevi (pre svega dodatna fleksibilnost i mobilnost) pomerili su fokus na bežične tehnologije.

Rešenje, predstavljeno u ovom dokumentu, bazirano je na našim iskustvima u realnim profesionalnim mobilnim okruženjima i može biti primenjeno na takva okruženja. Sve komponente razvijene od treće strane su sa dostupnim izvornim kodom i to omogućava profesionalnim organizacijama da verifikuju rešenje, i da ga prilagode svojim potrebama.

Detalji šifarskog algoritma korišćenog u eksperimentalne svrhe u ovom radu, MGAe2, nisu dati u ovom dokumentu jer je fokus ovog dokumenta na procesu, a ne na konačnom rešenju za krajnjeg korisnika. Navedeno je i istaknuto da bilo koja profesionalna organizacija ne moža da se osloni na šifarske algoritme razvijene od strane drugih organizacija. Razvoj sopstvenog algoritma je, zbog toga, jedna od osnovnih pretpostavki ovog rada.

Opisan sistem za upravljanje ključevima je modifikovan i te modifikacije ga čine komplikovanijim za distribuciju ključeva. Međutim, predloženo rešenje za razmenu i korišćenje ključeva može se smatrati jednostavnim načinom za implementaciju jakih šifarskih ključeva koji mogu biti generisani od strane nekog realnog generatora slučajnih brojeva.

Literatura

[1] Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. Breaking 104 bit WEP in less than 60 seconds. IACR eprint server, http://eprint.iacr.org/2007/120.pdf, April 2007.

[2] W. A. Arbaugh. An Inductive Chosen Plaintext Attack Against WEP and WEP2, 2001.

[3] Tim Newsham. Cracking WEP Keys Applying known techniques to WEP Keys, 2001. http://www.lava.net/#newsham/wlan/WEP password cracker.pdf.

[4] Andrea Bittau, Mark Handley and Joshua Lackey. The Final Nail in WEP's Coffin. Proceedings of the 2006 IEEE Symposium on Security and Privacy.

[5] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. IACR eprint server http://www.iacr.org, April 2002.

[6] RFC 4385 - Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN

[7] Jevremović A., Veinović M., „Zaštita podataka na IP nivou pod Linuks OS", Zbornik radova 50. konferencije Etran, Beograd, 2005., str. 114-117;

[8] Jevremović A., Veinović M., „IPsec - analiza uticaja algoritma za šifrovanje na saobraćaj u LAN mrežama", 14. telekomunikacioni forum Telfor 2006., Beograd, 2006., CD izdanje;

[9] Veinović M., Jevremović A., Šimić G., „Implementacija sopstvenog algoritma zaštite u IPsec-u pod Linuks operativnim sistemom", Singidunum revija, Vol 5 No 1, Beograd, 2008., str. 92-102;

[10] Jevremović A., Veinović M., Šimić G., „Modifikacija IKEv2 protokola u cilju izbora radnog tajnog ključa simetričnih šifarskih sistema", Zbornik radova 53. konferencije za elektroniku, telekomunikacije, računarstvo, automatiku i nuklearnu tehniku - Etran, Beograd, 2009., CD izdanje;

[11] Veinović M., Jevremović A., Šimić G., „Analysis and implementation of custom cipher algorithm for IPsec under Linux OS", International Journal of Computer Science and Network Security, Vol. 8 No. 7, July 2008;

Abstract

Securing wireless networks for professional use (military, government) is not an easy task, especially when it must be done without modifying hardware. In this paper we described a process of securing wireless network at IP level by using proprietary cipher and standard open technologies and solutions: IPsec, IKEv2 and Linux OS. Also, all components of the solution must be open and verifiable.

PROTECTING WIRELESS COMMUNICATIONS USING PROPRIETARY CIPHER

Aleksandar Jevremović, Mladen Veinović, Goran Šimić