FRAME GENERATOR BASED ON 802.11 STANDARD

Pavel Švanda
Master Degree Programme (2), FIT BUT
E-mail: xsvand00@stud.fit.vutbr.cz

Supervised by: Matej Kačic
E-mail: ikacic@fit.vutbr.cz

Abstract: This paper deals with a design and realization of a frame generator used for a transmission of information in 802.11 wireless networks. There is a sample of a frame description realized using a special language designed for this purpose. This paper also describes the implementation of the designed tool for generating the frames. In conclusion it describes usage of the tool for potential attacks in wireless networks.

Keywords: Frame generator, wireless security, standard 802.11, RadioTap header, IEEE header

1 ÚVOD

Bezdrátové sítě standardu 802.11, známé také jako bezdrátové sítě Wi-Fi, nabízí uživatelům alternativní možnost přístupu do jejich počítačové sítě a do sítě Internet. Vlivem použitého přenosového média jsou ale tyto sítě náchylnější na případné útoky než sítě drátové. Motivací útočníka k těmto útokům může být například bezplatný přístup do sítě Internet nebo možnost získat citlivá data uživatelů sítě. K tomu, aby se mu toto podařilo, musí v řadě případů využít nějaké zranitelnosti, které tyto sítě obsahují. Abychom mohli případným útokům předcházet, je zapotřebí vlastnit nástroje, pomocí nichž bychom byli schopni tyto zranitelnosti odhalit dříve než samotní útočníci.

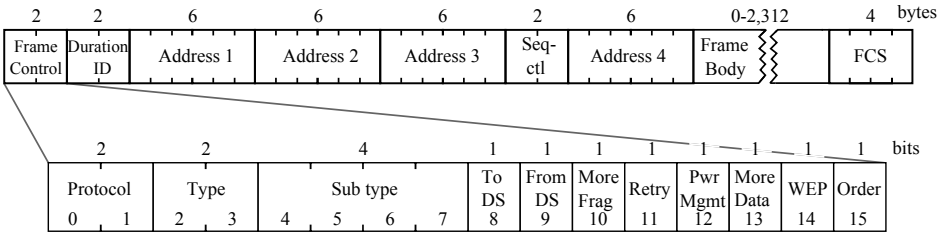
Generátor rámců, který článek popisuje, je nástroj umožňující popis, generování a následné zasílání rámců používaných pro přenos informací v bezdrátových sítích Wi-Fi. Jednotlivé rámce se skládají z hlaviček RadioTap a IEEE. V případě datových rámců pak obsahují také vlastní přenášená data.

2 STRUKTURA RÁMCŮ

Jak již bylo zmíněno výše, jednotlivé rámce použité pro přenos informací ve Wi-Fi sítích, se skládají ze tří částí. V první části rámce se nachází hlavička RadioTap [1]. Tato hlavička slouží k doplnění informací z ovladačů síťové karty k přenášenému rámci. Mezi těmito informacemi lze například nalézt informace o použitém kanálu nebo číslu antény, která byla použita pro přijetí rámce.

V druhé části rámce se nachází hlavička IEEE [2]. Pomocí této hlavičky se přenáší informace důležité pro činnost bezdrátových sítí Wi-Fi. Mezi informacemi přenášenými v hlavičce nalezneme například adresu zařízení, ke kterému rámec v síti směřuje, informaci, zdali je rámec zabezpečen, a mnoho dalšího. Obecnou strukturu hlavičky znázorňuje obrázek 1. Tato struktura se ovšem může měnit dle významu rámce. Standard 802.11 definuje tři typy rámců – datové, řídící a management rámce – rozlišeny pomocí informačního pole *type* v hlavičce. Jednotlivé typy rámců se dále dělí na různé podtypy. Podtyp rámce je v hlavičce zachycen v poli *sub type*. Mezi podtypy rámců patří například Beacon rámce, RTS, CTS rámce a řada dalších.

V případě datových rámců se v poslední části za hlavičkou IEEE vyskytují vlastní data. Tato data mohou být v otevřené případně zabezpečené podobě. Bezdrátové sítě Wi-Fi nabízí tři metody zabezpečení rámců [3]. Metodu WEP, která využívá algoritmu RC4. Dále pak metodu TKIP, která před-



Obrázek 1: IEEE 802.11 hlavička

stavuje vylepšení předchozí metody za použití stávajících hardwarových prostředků. A jako poslední metodu CCMP, která je zcela novou metodou využívající šifrovacího algoritmu AES.

3 POPIS RÁMCŮ

K popisu rámců byl navržen jazyk, pomocí něhož je umožněno definovat jejich jednotlivé části. Jazyk obsahuje příkazy k definici vlastností jednotlivých hlaviček, příkazy k definování informačního obsahu datových rámců a v neposlední řadě příkazy, které umožňují manipulaci s popsanými rámci. Návrh jazyka byl proveden ve zjednodušené verzi Backus-Naurovy formy, zkráceně BNF, kterou využívají aplikace použité při realizaci nástroje.

Jednotlivé rámce jsou v tomto popisu reprezentovány identifikátorem skládajícím se z alfanumerických znaků. Pomocí tohoto identifikátoru a odpovídajících operací je provedena definice jednotlivých vlastností rámce. Při této definici je umožněno využívat jednak příkazy k nastavování hodnot, ale také k jejich vypsání, případně navrácení na výchozí hodnotu. Ukázka použití tohoto jazyka je naznačena na krátkém příkladu uvedeném níže. V této ukázce je provedena tvorba a následné zaslání RTS rámce.

```
rtsFrame = IEEE(type="rts" receiverAddress="00:21:91:15:51:A2")
send(rtsFrame)
```

4 REALIZACE NÁSTROJE

Vlastní nástroj byl realizován jako konzolová aplikace v prostředí Linux pomocí programovacího jazyku C++ s využitím objektově orientovaného návrhu. Díky tomuto postupu vznikla sada tříd, které lze také využívat samostatně, což umožňuje vznik dalších aplikací. Tyto aplikace mohou již realizované třídy využívat jako knihovnu pro práci s rámci bezdrátových sítí Wi-Fi.

K realizaci analyzátorů navrženého jazyka bylo využito aplikací LEX a YACC, které umožňují generovat lexikální a syntaktický analyzátor ze zadaného popisu. Díky využití těchto aplikací byl urychlen celý postup realizace a zároveň vznikla možnost snadných úprav jazyka. Postačuje pouze pozměnit zadaný popis jazyka a provést opětovné vygenerování analyzátorů.

Pomocí vygenerovaných analyzátorů je provedena analýza zadaného popisu rámce, z něhož je následně vygenerován vlastní rámec. V případě datových rámců umožňuje nástroj zvolit metodu, kterou je zabezpečen informační obsah. Nástroj umožňuje obsah rámce zabezpečit pomocí metod WEP, TKIP a CCMP. Po vygenerování rámce je umožněno jeho zaslání na předem zvolené rozhraní.

5 DOSAŽENÉ VÝSLEDKY

V současnosti existuje řada nástrojů, které se zabývají podobnou problematikou. Jmenujme například nástroj aircrack-ng [6] obsahující řadu aplikací pracující s Wi-Fi rámci. Definice těchto rámců je do značné míry omezena. Uživateli je umožněno definovat pouze některé vlastnosti rámce. Tento rámec je následně použit, například k předdefinovanému útoku. Dalším podobným nástrojem je Scapy [7].

Tato aplikace se zaměřuje především na definici hlaviček vyšších vrstev. Ale i tento nástroj umožňuje, byť pouze v omezené míře, definovat strukturu rámců 802.11. Po definici rámce úmožňuje i tento nástroj jednotlivé rámce zasílat. Nástroj popsaný v tomto článku se zaměřuje pouze na popis hlaviček nižších vrstev. Hlavičky dalších vrstem mohou být vloženy jako datový obsah. Nástroj, podobně jako předchozí, umožňuje odchytávat rámce použité při komunikaci na síti. Z takto odchyceného rámce následně umožňuje získat inicializační vektor. Ten může být po zvětšení o jedna použit k zašifrování nového rámce pomocí klíče, který si aplikace načte z operačního systému.

Nástroj je možné využít například při bezpečnostních auditech bezdrátových sítí Wi-Fi. Při těchto auditech může být využíváno různých typů útoků, které ověří, jak je síť zabezpečena. Nástroj umožňuje vytvářet útoky od těch nejjednodušších až po útoky, které jsou značně složité. Příkladem jednoduššího útoku může být RTS případně CTS flood útok [5]. V obou případech se útočník snaží zabránit uživatelům ve využívání přenosového pásma sítě. V případě RTS flood útoku zasílá útočník RTS rámce směrem k přístupovému bodu sítě (AP - access point), čímž mu dává najevo, že požaduje přidělení pásma k přenosu dat. Přidělení pásma potvrzuje AP pomocí CTS rámce a zároveň tak dává ostatním najevo, že je pásmo obsazeno. Pomocí CTS flood útoku zasílá útočník přímo CTS rámce, čímž opět dochází k pozastavení přenosu u všech uživatelů.

Značně složitějším útokem pak může být útok na zabezpečení sítě WPA2, který využívá zranitelnosti nazvané Hole196 [4]. Pomocí tohoto zabezpečení je komunikace každého uživatele šifrována unikátním klíčem. Pouze rámce, které jsou určeny všem uživatelům – broadcast a multicast rámce zaslané AP – jsou šifrovány shodným klíčem. Útok využívá skutečnosti, že když je útočník přihlášen do sítě, zná také tento klíč. Poté postačuje, aby zaslal broadcast rámec zašifrovaný tímto klíčem a adresou zdroje rámce shodnou s AP. Přijímající stanice nerozezná, zdali byl odeslán od AP nebo od útočníka, a tak tento rámec v pořádku přijme. Tento rámec poté může obsahovat jako datovou část například ARP paket, který zapříčiní, že uživatel začne zasílat data útočníkovi místo skutečnému příjemci.

6 ZÁVĚR

Nástroj popsaný v tomto článku umožňuje generovat rámce použité pro přenos informací v bezdrátových sítích Wi-Fi. Generování rámců je provedeno z popisu, který byl pro tento účel navržen. Nástroj dále umožňuje vygenerované rámce zaslat na předem specifikované rozhraní. Tento nástroj je možné využít například pro generování různých rámců, se kterými může být dále experimentováno. Případně lze tento nástroj také použít k tvorbě útoků, které mohou být využity pro bezpečnostní audit Wi-Fi sítí, tak jak bylo naznačeno v části Dosažené výsledky.

REFERENCE

[1] "RadioTap hlavička [online]", http://www.radiotap.org/, cit. 2012-12-27

[2] Gast, M. S., "802.11 Wireless Networks - The Definitive Guide", O'Reilly, 2002, iSBN 0-596-00183-5

[3] Benton, K., "The Evolution of 802.11 Wireless Scurity", 2010

[4] Ahmad, Md, "Wpa too!", http://www.defcon.org/images/defcon-18/dc-18-presentations/Ahmad/DEFCON-18-Ahmad-WPA-Too-WP.pdf, 2010

[5] Rajinder, S., Wireless Network Security", http://www.rgsociety.org/journals/index.php/ijwwc/article/download/329/154, 2012

[6] "Aircrack-ng [online]", http://www.aircrack-ng.org/, cit. 2013-03-23

[7] "Scapy [online]", http://www.secdev.org/projects/scapy/, cit. 2013-03-23