[illegible] CEH (v10): [illegible]

[illegible] (NIC) [illegible].

[illegible] CEH [illegible].

[illegible]

[illegible] 1997 [illegible] 802.11 [illegible] (IEEE) [illegible] (WLAN) [illegible] WLAN [illegible].

[illegible]

Wireless NIC
Computer A
Wireless NIC
Computer B

IEEE WLAN Standard	Over-the-Air Estimates	Transmission Scheme	Frequencies
802.11b	11 Mbps	DSSS	2.4000–2.2835 GHz
802.11a	54 Mbps	OFDM	5.725–5.825 GHz
802.11g	54 Mbps	OFDM/DSSS	2.4000–2.2835 GHz
802.11n	540 Mbps	MIMO-OFDM	2.4000–2.2835 GHz
802.11ac	433.3 Mbps	MIMO-OFDM	5 GHz band
802.11ad	7 Gbps	OFDM	60 GHz band
802.11ax	Pending	MIMO-OFDM	Pending
802.11ay	20 Gbps	OFDM	60 GHz band

پرشی تداخل را کاهش داده و بسته به کیفیت سیگنال سرعت انتقال دادهها را افزایش یا کاهش میدهد . فناوری فوق اولین بار توسط صنایع نظامی به کار گرفته میشد، زیرا استراق سمع این فناوری به سختی امکانپذیر است . امروزه فناوریهای مختلف در ارتباطات بیسیم استفاده میشوند که از آن جمله به موارد زیر میتوان اشاره کرد :

پرش فرکانسی مبتنی بر طیف گسترده/ طیف گسترده پرش فرکانسی (FHSS) سرنام Frequency-hopping spread spectrum، مدولاسیونی برای ارسال سیگنال در باند فرکانسی رادیویی است . در این مدولاسیون فرکانس موج حامل به شکل پیوسته و شبه تصادفی تعویض میشود. انشعابات یا همان پرشهای کوتاه مدت باعث میشوند تا دادهها روی فرکانس خاصی درون باند انتقال پیدا کنند، در یک وضعیت دنبالهدار، پرش بعدی به فرکانس بعدی رفته و اینکار تکرار میشود . پرش از فرکانس میتواند صدها بار در ثانیه رخ دهد . دقت کنید که مدولاسیون FHSS ارزانتر از DSSS بوده و در محیطهای پر ازدحام و محیطهای داخلی بهتر از DSSS عمل میکند.

پرش فرکانسی دنباله مستقیم یا طیف گسترده دنباله مستقیم (DSSS) سرنام direct sequence spread spectrum، مدولاسیونی است که در آن جریانهای دادهای به تکههای کوچکی تقسیم میشوند که این تکههای کوچک چیپها (chips) نام دارند . چیپهایی که روی همه فرکانسهای موجود در یکی از سه کانال عریض به شکل همزمان پخش میشوند. فرایند تقسیم و رمزگذاری دادهها چیپسازی نامیده میشود . نرخ توزیع استفاده شده برای انتقال دادهها نیز کد چیپسازی نامیده شده که برای هر دستگاه کدی منحصر به فرد است . DSSS میتواند پهنای باند موجود را نسبت به FHSS به شکل کارآمدتری استفاده کرده و در نتیجه توان عملیاتی بالاتری را ارائه میکند .

مدولاسیون تقسیم فرکانس عمودبرهم (OFDM): در OFDM زیرحاملهای متعامد زیادی داده را بهصورت موازی بر جریانهای دادهای یا کانالهای موازی حمل میکنند . هریک از زیرحاملها با یک روش مدولاسیون سنتی مانند QAM با نرخ نشانه کم مدوله میشوند و میتوانند نرخ دادهای برابر با روشهای مدولاسیون سنتی در پهنای باند یکسان به دست آورند . چندین مشکل ذاتی در OFDM وجود دارد . یکی از آنها این است که یک سیگنال OFDM میتواند نقطه اوج لحظهای زیادی نسبت به سطح متوسط داشته باشد. همچنین، آنها میتوانند نوسان دامنهای زیادی داشته باشند، هنگامی که سیگنال از یک توان لحظهای کم به یک توان لحظهای زیاد انتقال مییابد . یک تقویتکننده توان باید بهصورت خطی روی پهنای باند وسیع برای پیشگیری از اعوجاج هارمونیک خارجباندی زیاد قرار داده شود .

امنیت شبکه محلی بی سیم

ماهیت بیسیم و استفاده از فرکانس رادیویی برای شبکهسازی باعث شده تا امنیت شبکههای محلی بیسیم به شکل جدی مورد توجه شرکتها قرار بگیرد . برای این منظور ابتدا پروتکل Wired Equivalent Privacy (WEP)) برای جوابگویی به این نیاز ارائه شد . این کار برای تأمین اطلاعات شخصی کاربران فعال در شبکههای بیسیم انجام شد . WEP بر مبنای استاندارد رمزگذاری متقارن RC4 کار کرده و از یک کلید 64 بیتی یا 128 بیتی استفاده میکند . با این حال، کلیدها در عمل تمامی این بیتها را استفاده نمیکنند، زیرا یک بردار اولیه 24 بیتی (IV) برای تهیه اطلاعات تصادفی استفاده میشود . بنابراین، "کلید واقعی" در واقع 40 یا 104 بیت طول دارد. دو راهکار برای پیادهسازی کلید وجود دارد . روش اول که در واقع روش پیشفرض کلید است مجموعهای متشکل از چهار کلید پیشفرض را با تمامی اکسسپوینتهای بیسیم بهاشتراک قرار میدهد . روش دوم که روش نقشهبرداری کلید است، مجموعهای از کلیدهای نگاشت شده رابطهای برای هر ایستگاه بیسیم و ارتباط آن با ایستگاه بعدی تنظیم میشود . در نتیجه، اکثر شبکههای محلی بیسیم از یک کلید مشترک منفرد در تمامی ایستگاهها استفاده میکنند که باعث میشود هکرها به راحتی به بازیابی کلیدها بپردازند .

اکنون ، اجازه دهید نگاهی دقیقتر به WEP بیندازیم و نحوه عملکرد آنرا بررسی کنیم .

برای درک بهتر عملکرد WEP ابتدا باید به منطقی بولی این مکانیزم نگاهی داشته باشیم . بهطور خاص، شما باید بدانید که چگونه عملگر XORing کار میکند . XORing فقط یک مقایسه باینری ساده بین 2 بیت انجام میدهد که در نتیجه این فرآیند بیت دیگری تولید میشود . وقتی دو بیت با هم مقایسه میشوند، XORing بررسی میکند که تفاوتهایی میان آنها وجود دارد یا خیر . اگر متفاوت باشند، نتیجه حاصل 1 است. اگر 2 بیت یکسان باشند، نتیجه 0 است. اگر دوست دارید در مورد منطق بولی اطلاعات بیشتری کسب

کنید پیشنهاد میکنم به آدرس زیر مراجعه کنید .

https://en.wikipedia.org/wiki/Boolean_algebra

با این مقدمه این پرسش مطرح میشود که چگونه RC4 و XORing برای رمزگذاری ارتباطات بیسیم استفاده میشوند. برای توضیح بهتر این مفاهیم، اجازه دهید به هفت مرحله رمزنگاری یک پیام بپردازیم :

1. ایستگاههای انتقال و دریافت با کلید مخفی مقداردهی اولیه میشوند . این کلید مخفی باید با استفاده از مکانیسم خارج از باند شبیه به ارسال از طریق ایمیل، ارسال از طریق وبسایت یا نوشتن آن روی یک کاغذ (راهکاری که هتلها از آن استفاده میکنند) توزیع شود .

2. ایستگاه انتقالدهنده بذر یک مقدار جدید تولید میکند که با افزودن کلید مخفی 40 بیتی به 24 بیتی IV، به عنوان مقدار ورودی راهکار مولد اعداد شبه تصادفی (PRNG) استفاده میشود .

3. ایستگاه انتقالدهنده مقدار را به WEP PRNG وارد میکند تا یک جریان کلیدی از بایتهای تصادفی تولید کند .

4- کلید جریان با متن ساده XORed برای به دست آوردن متن رمزگذاری شده است.

5- ایستگاه فرستنده متن رمزنگاری را به IV اضافه میکند و بیتی را برای نشان دادن این موضوع که یک بسته با الگوی WEP رمزگذاری شده استفاده میکند . این رویکرد فرآیند کپسولهسازی WEP را کامل میکند و نتایج را به صورت یک فریم از دادهها انتقال میدهد . WEP فقط دادهها را رمزگذاری میکند و در نتیجه سرآیند و دنباله به صورت یک متن واضح ارسال میشوند .

6. ایستگاه گیرنده بررسی میکند که آیا بیت دریافتی فریم رمزگذاری شده یا خیر . اگر پاسخ مثبت است ایستگاه دریافتکننده IV را از فریم استخراج کرده و IV را با کلید مخفی ضمیمه میکند .

7. گیرنده یک کلید جریان اصلی تولید میکند که باید با کلید ایستگاه فرستنده مطابقت داشته باشد . این کلید جریان اصلی XORed با متن رمزگذاری شده برای بهدست آوردن متن ساده فرستاده میشود .

برای درک بهتر نحوه عملکرد WEP به مثال زیر دقت کنید . فرض کنیم کلید تصادفی ما Hacker است. این واژه با واژه دیگری بهنام qrs ادغام میشود تا یک کلید مخفی بهنام qrshacker را تولید کند . این مقدار برای رمزگذاری یک بسته استفاده میشود . بسته بعدی نیاز به IV جدید دارد . بنابراین، هنوز هم میتوان از Hacker استفاده کرد، اما اینبار آنرا با مقدار mno به وجود می آوریم تا یک کلید مخفی جدید بهنام mnohacker ایجاد کنیم . این روند برای هر بسته دادهای که ایجاد میشود ادامه مییابد . مثال فوق باید به شما در شناخت این موضوع که چه بخشی از کلید مخفی در IV تغییر میکند کمک کرده باشد . درست در همین نقطه است که WEP کرک شده و آسیبپذیری آن فاش میشود. بعد از اینکه هکر کلیدهای دیگری را دریافت کرد به راحتی میتواند نقطه شکست الگوریتم فوق را پیدا کند .

WEP کل انتقال را رمزگذاری نمیکند، در نتیجه سرآینده و دنباله به شکل متن واضح ارسال میشوند . این بدان معنا است که حتا وقتی از رمزگذاری استفاده میشود، بازهم احتمال شنود مکآدرس وجود دارد .

برای شکستن منفعلانه WEP، هکر باید 5 تا 10 میلیون بسته را ضبط کند که اینکار در بیشتر شبکهها به مدت زمان زیادی نیاز دارد . این موضوع در سال 2004 و هنگامی که هکری بهنام Korek موفق شد از یک قطعه کد کوچک برای حمله به یک شبکه بزرگ و بازیابی کلید WEP استفاده کند تغییر پیدا کرد . Korek اعلام کرد به جای آنکه از رویکرد منفعلانه جمعآوری میلیونها بسته برای شکستن کردن کلید WEP استفاده شود، این امکان وجود دارد تا بهطور فعالانه بستههایی را به شبکه تزریق کرد . ایده این بود که پاسخی را از دستگاههای معتبر در شبکه محلی بیسیم درخواست کنیم . حتی اگر هکر نتواند این بستهها را رمزگشایی کند، میتواند حدس بزند که محتوای آن چه چیزی است و بستههای فوق به گونهای استفاده کند تا پاسخهای ایجاد کننده باعث شوند ترافیک اضافی به وجود آید . این امر باعث میشود کمتر از 10 دقیقه WEP را در بسیاری از شبکههای بیسیم کرک کرد .

در شماره آینده مبحث فوق را ادامه میدهیم .

برای مطالعه رایگان تمام بخشهای دوره CEH روی لینک زیر کلیک کنید :

آموزش رایگان دوره CEH

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
13:45 - 18/04/1399
برچسب:
دوره CEH - آموزش رایگان CEH - آموزش رایگان دوره CEH - هکر کلاه سفید - آموزش CEH v10 - آموزش رایگان CEH10 - هک اخلاقی - فناوری بیسیم - شبکه محلی بیسیم

نشانی
□□□□:https://www.shabakeh-mag.com/security/17049/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%D9%85%D8%A8%D8%A7%D9%86%DB%8C-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A8%DB%8C%E2%80%8C%D8%B3%DB%8C%D9%85-%D9%88-%D9%85%D8%AE%D8%A7%D8%B7%D8%B1%D8%A7%D8%AA-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-%D8%A2%D9%86%E2%80%8C%D9%87%D8%A7