بررسی روش‌های نفوذ در شبکه‌های بی‌سیم wi-fi [1]

حمیدرضا محمدی

[۱]کارشناسی ارشد مهندسی رایانه در گرایش شبکه‌های رایانه‌ای، دانشگاه آزاد اسلامی واحد لاهیجان
hamidsoftdev@gmail.com

چکیده

فناوری شبکه‌های بی‌سیم باعث شد تا ارتباط به‌گونه‌ای آسان با امواج الکترومغناطیسی مخابره و عنصر سیم که بزرگ‌ترین مانع در ارتباطات متحرک است، حذف شود، این شبکه‌ها از هوا به‌عنوان رسانهٔ ارتباطی استفاده می‌کنند. همین مسأله باعث شده آسیب‌پذیری بیشتری را شامل شود. شبکه‌های بی‌سیم قسمت عمده‌ای از زندگی ما را تشکیل می‌دهند، از مودم‌های خانگی گرفته تا تجهیزات سازمانی، همه و همه از روش‌های مرسوم رمزنگاری برای تبادل داده در شبکهٔ خود می‌پردازند. حال اگر شخصی بتواند به این شبکه‌ها نفوذ کند، می‌تواند حملات متنوعی را علیه کلیه کاربران متصل به شبکه انجام دهد. در این مقاله به بررسی روش‌های نفوذ در پروتکل در شبکه‌های بی‌سیم wi-fi با پروتکل رمزنگاری WEP و WPA-WPA2 پرداخته که این پروتکل‌ها قسمت عمده‌ای از ارتباطات خانگی و سازمانی را در ارتباطات بی‌سیم انجام می‌دهند، با ارائه WPA3 کلیهٔ این ایرادات و مشکلات امنیتی رفع شده است؛ اما تجهیزات مجهز به این نوع رمزنگاری در ایران به تعداد کمتری وجود دارند که طبق مطالعات انجام‌شده پروتکل WEP در بهره‌برداری از آسیب‌پذیری رتبه نخست را دارد و پس از آن پروتکل‌های WPA نسخه نخست و دوم در رتبه‌های بعدی هستند.

واژگان کلیدی: روش های نفوذ، شبکه های بی‌سیم wi-fi، تست نفوذ، WPA_2، WPA و WEP.

۱- مقدمه

شبکه بی‌سیم یک شبکهٔ رایانه‌ای است که به تجهیزات مختلف امکان برقراری ارتباط را با یکدیگر بدون این‌که از طریق یک رسانهٔ ارتباطی فیزیکی مانند کابل شبکه متصل شوند، امکان‌پذیر می‌کند. شبکه‌های بی‌سیم مدرن به‌طورمعمول به ارتباطات رادیویی متکی هستند که در باند فرکانس‌های فراتر از مادون قرمز در طیف الکترومغناطیس فعالیت می‌کنند.

با پیشرفت ارتباطات بی‌سیم در انواع کاربردهای مختلف نظیر: اینترنت اشیا و تجهیزات هوشمند و افزایش یافتن نقاط دسترسی در مناطق مختلف، امنیت wi-fi را نمی‌توان نادیده گرفت. پروتکل مورد استفاده بیش‌تر شبکه‌های بی‌سیم، wi-fi است که با انتقال مسافت طولانی‌تر نسبت به پروتکل‌های دیگر مانند بلوتوث، RFID[۲]و IR [۳]با ثبات و پایداری بیشتری نیز همراه است. ارتباطات wi-fi به این دلیل بسیار رایج است که سهولت در استفاده و سرعت بالای آن همواره مورد استفاده مردم است، امنیت ارتباطات پروتکل wi-fi توسط پروتکل‌های WPA[۴]و WPA2 که اکنون مرسوم‌ترین پروتکل‌های توسعه‌یافته توسط انجمن مؤسسه مهندسان برق و الکترونیک[۵] برقرار می‌شود؛ اما در این پروتکل‌ها، تنها از داده‌ها محافظت می‌شود و این فرصت برای مهاجمین پیش می‌آید که اطلاعات حساس مورد تبادل در شبکه را مورد نفوذ قرار دهند.

مسائل امنیتی شبکه‌های بی‌سیم در سال‌های اخیر زمینه پژوهشی مستمر بوده است که با پیشرفت سامانه‌های شبکه بی‌سیم، برقراری ارتباط ایمن و قابل اعتماد از اهمیت ویژه‌ای برخوردار است. اهمیت این حوزه از امنیت سامانه‌های بی‌سیم برای جلوگیری از دسترسی غیرقانونی یا آسیب‌رساندن به سامانه و داده‌ها توسط مهاجمان است. از آنجایی که شبکه‌های بی‌سیم از نظر ماهیت فعالیت، باز و بدون مرز هستند، از این‌رو، امنیت شبکه بی‌سیم همچنان یک مسألهٔ جدی و چالش‌برانگیز است. در اینجا این سؤال پیش می‌آید که امنیت این پروتکل‌ها چگونه است؟

[1] Wireless Fidelity(wi-fi)
[2] Radio Frequency Identification (RFID)
[3] Infrared Radiation (IR)
[4] WIFI Protected Access (WPA)
[5] IEEE

در پژوهش موجود ما ابتدا پروتکل‌های شبکه‌های بی‌سیم، دسته‌بندی انواع حملات و تهدیدات و در انتها روش‌های نفوذ شبکه‌های بی‌سیم wi-fi در پروتکل‌های WPA-WPA2 و WEP[1] بررسی خواهیم کرد و در انتها جمع‌بندی جامعی از این روش‌ها را در قالب جدولی ارائه خواهیم‌داد.

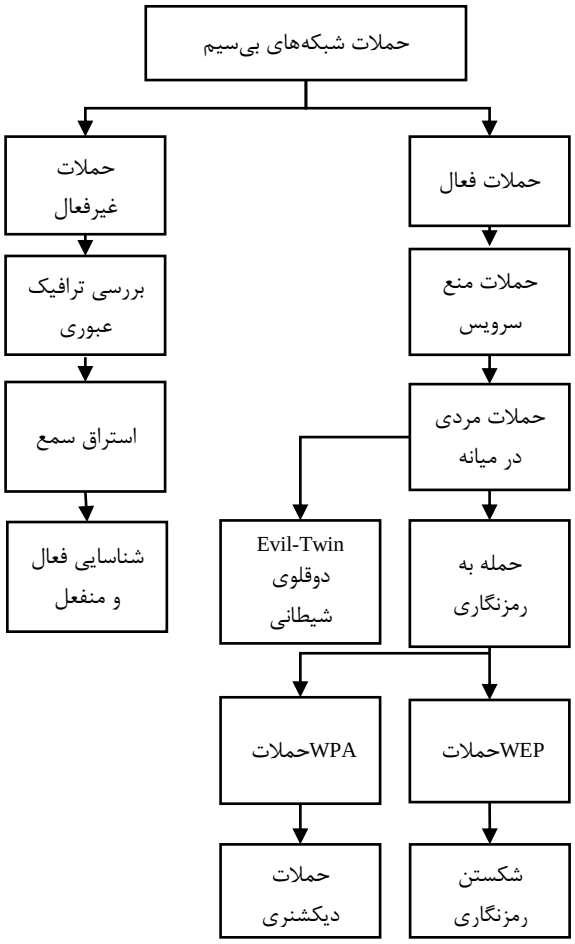
۲- پروتکل‌های امنیتی wi-fi

دهه ۹۰ میلادی زمانی که استفاده از شبکه‌های بی‌سیم همگانی شد، پروتکل‌هایی جهت حفظ امنیت در طی سال‌های مختلف ارائه شد. این پروتکل‌ها برای مدیریت امنیت کاربرانی هستند که به دستگاه متصل می‌شوند. جدول (۱) مشخصات حائز اهمیت سه پروتکل کاربردی در شبکه‌های بی‌سیم عمومی را نشان می‌دهد.

(جدول-۱): مشخصات کلیدی سه پروتکل [۱] WEP ,WPA ,WPA2

نام الگوریتم	WEP	WPA	WPA2
سال ارائه	۱۹۹۹	۲۰۰۳	۲۰۰۴
طول کلید	۴۰ بیت	۱۲۸ بیت	۱۲۸،۱۹۲،۲۵۶ بیت
نوع کلید	ثابت	پویا	پویا
مدیر کلید مرکزی	ندارد	Radius[2]	Radius
احراز هویت	کلیدWEP	پروتکل احراز هویت 802.1X (EAP)	پروتکل احراز هویت 802.1X (EAP)
الگوی رمزنگاری	RC4	کلید موقتی TKIP همراه با رمزنگاری RC4	پروتکل CCMP با رمزنگاری AES
سازگاری دستگاه	802.11a,b,g	802.11a,b,g	802.11a,b,g

- پروتکل WEP نخستین نسخه از پروتکل‌های امنیت شبکه‌های بی‌سیم خانواده IEEE 802.11 بوده که در سال ۱۹۹۹ ارائه شد. این پروتکل به‌دلیل طول کم‌کلید و ساختار ضعیف، دو سال بعد از ارائه، الگوریتم رمزنگاری آن شکسته شد.
- پروتکل WPA برای رفع مشکلات پروتکل قبلی یعنی WEP ارائه شد. این پروتکل مجهز به رمزنگاری قوی‌تر و TKIP[3] بوده و کلید آن ۱۲۸ بیتی است.
- پروتکل WPA2 در سال ۲۰۰۴ جایگزین پروتکل WPA شد. این پروتکل مجهز به CCMP[4] و الگوریتم AES[5] شد.
- در سال ۲۰۱۸ پروتکل جدیدی که تمامی ایرادات پروتکل‌های قبلی را رفع می‌کرد، تحت عنوان WPA3 ارائه شد.



(شکل-۱) : دسته‌بندی تهدیدات در شبکه‌های بی‌سیم

در ادامهٔ پژوهش به بررسی روش‌های ارائه‌شده در شکل (۱) می‌پردازیم.

۳- تهدیدات در شبکه‌های بی‌سیم

بیاییم در ابتدا تعریفی از آسیب‌پذیری داشته باشیم، آسیب‌پذیری را می‌توان نوعی ضعف در یک شبکه بی‌سیم، در یک مجموعه پروتکل یا هر چیز دیگری دانست که امنیت شبکه بی‌سیم را در معرض تهدید قرار دهد. آسیب‌پذیری ضعف داخلی سامانه‌های شبکه بی‌سیم است. شبکه‌های بی‌سیم به‌طوردقیق مانند تلویزیون یا رادیو از امواج الکترومغناطیسی استفاده می‌کند. درحقیقت، ارتباط از طریق شبکه بی‌سیم تقریباً شبیه ارتباطات رادیویی دو

[1] Wired Equivalent Privacy (WEP)
[2] Remote Authentication Dial-In User Service
[3] Temporal Key Integrity Protocol (TKIP)
[4] Counter Mode Cipher Block Chaining (CCMP)
[5] Advanced Encryption Standard (AES)

طرفه است. سیگنال‌های بی‌سیم می‌توانند به‌راحتی منعکس و پراکنده شوند، بنابراین به‌طور بالقوه امکان دسترسی مهاجمان برای دسترسی به ارتباطات بی‌سیم فراهم می‌شود.

نقطه دسترسی[1] خدمات خود را با شناسهٔ SSID[2] منتشر می‌کنند، کاربران برای دسترسی به سرویس‌های مرتبط سعی می‌کنند به نقطه اتصال متصل شوند. شبکه‌های بی‌سیم می‌توانند به‌صورت بدون رمز و آزاد و یا رمزعبور برای اتصال تنظیم شوند. در نوع رمزنگاری شده، انواع مختلفی از روش‌های رمزنگاری مورد استفاده قرار می‌گیرد که کاربر نیاز داشته از یک کلید مشترک یا رمز عبور را برای اتصال به شبکه مورد نظر استفاده کند.

حملات فعال: در این نوع حملات، مهاجم اطلاعات مورد نظر را که از منبع یا مبدأ به‌دست می‌آید، تغییر می‌دهد.

حملات غیر فعال: در این حملات، مهاجم تنها به منبع اطلاعات دست می‌یابد؛ اما اقدام به تغییر محتوای اطلاعات منبع نمی‌کند. نوع حمله می‌تواند از نوع استراق‌سمع ساده یا تجزیه و تحلیل ترافیک باشد.

۴- حملات رایج در wi-fi

به این دلیل شبکه‌های wi-fi در برابر مهاجمان آسیب‌پذیر هستند که امواج نقاط اتصال بی‌سیم بدون حد و مرزی در بستر هوا در معرض دسترسی همه قرار می‌گیرد؛ بنابراین مهاجمان می‌توانند تا زمانی که در محدوده امواج رادیویی باشند، اقدام به شنود اطلاعات تبادلی و نفوذ کنند. از مهم‌ترین خصیصه‌های این نوع نفوذ این است که ما می‌توانیم بدون شناسایی فیزیکی، تنها با یک لپ‌تاپ و یک کارت شبکهٔ وایرلس[3] از راه دور این کار را انجام دهیم. این مورد از مشکلات عدیده در امنیت بی‌سیم است، با این حال، ما پروتکل‌های امنیتی WPA و WPA2 را داریم. برای اینکه بتوانیم بیشترین کنترل را بر شبکه داشته باشیم؛ بهترین راه، به‌دست‌آوردن رمز عبور در شبکه‌های بی‌سیم است [۱].

(جدول-۲): نمونه‌هایی از حملات در شبکه‌های بی‌سیم [۲]

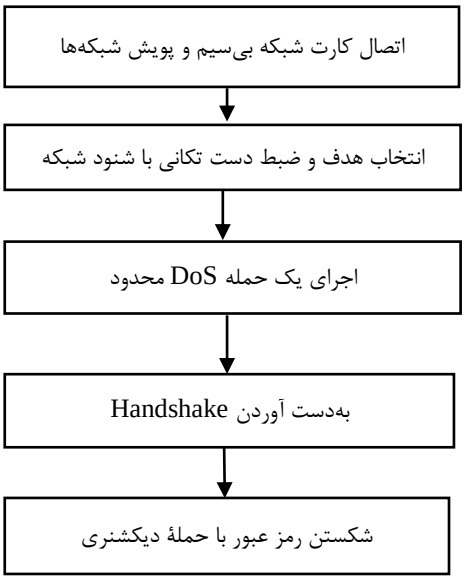
روش غیرفعال[4]	روش فعال[5]
مانیتور و استراق سمع	حملات منع سرویس
تظاهر به‌عنوان گرهٔ نرمال	حملات مسیریابی
تحلیل ترافیک عبوری	کرم چاله[6]

[1] Access Point (AP)
[2] Service Set Identifier (SSID)
[3] Wireless Network Adapter
[4] Passive
[5] Active
[6] Wormhole

۴-۱- حمله به WPA Handshake[7]

از نخستین روش‌های موفق در زمینه حملات شبکه‌های بی‌سیم است. در این روش مهاجم شبکه‌های اطراف خود را پویش و یک شبکه را برای حمله انتخاب می‌کند، همیشه باید دقت کنید شبکهٔ مورد نظر به اندازهٔ کافی به مهاجم نزدیک باشد تا حمله موفقیت‌آمیز انجام شود. بعد از انتخاب نیاز است که دستگاهی به شبکه مورد نظر متصل باشد تا از ارتباط مابین آن‌ها بتوان یک دست‌تکانی چهارمرحله‌ای WPA به‌دست آورد [۲].

پروتکل WPA2 از یک الگوریتم رمزنگاری قوی به نام AES استفاده می‌کند، که شکستن آن بسیار دشوار است؛ اما غیرممکن نیست. ضعف در سامانه WPA2-PSK این است که رمزعبور رمزنگاری‌شده در آنچه که به دست‌تکانی چهارمرحله‌ای شناخته می‌شود، مشترک است. هنگامی که کاربر به نقطه اتصال احراز هویت می‌کند، کاربر و نقطه اتصال یک فرآیند چهارمرحله‌ای را برای تأیید اعتبار کاربر انجام می‌دهند. اگر در آن زمان بتوانیم رمز عبور را به‌دست آوریم، می‌توانیم آن را با حملات دیکشنری[8] مورد نفوذ قرار دهیم [۳].



(شکل-۲): مراحل روش شکستن WPA Handshake

[7] دست تکانی WPA فرایند خودکار مذاکره بین یک شبکه محافظت شده WPA و رایانه شخصی کاربر مجاز برای دست‌یابی به آن است.

[8] در این حمله، مهاجم یک لیست از رمزعبور که شامل رمزهای عبور پر استفاده است را برای احراز هویت امتحان می‌کند.

۴-۲- انتخاب نقطه اتصال برای حمله

در گام نخست باید با ابزارهای مرسوم در سیستم عامل لینوکس کلیه نقاط اتصال را مورد پویش قرار داد، بعد از پویش شبکه‌ها شبکه‌ای را باید انتخاب کنید که از لحاظ فیزیکی نزدیک باشد و دست‌کم یک دستگاه به آن متصل شده باشد تا بتوان از ارتباط مابین آن‌ها Handshake را به‌دست آورد. مرحلهٔ بعدی انتخاب شبکهٔ مورد نظر و تلاش برای به‌دست‌آوردن Handshake است [۳].

۴-۳- به‌دست‌آوردن Handshake

در این روش تمام تلاشمان را باید کنیم تا دست‌تکانی چهارمرحله‌ای مابین نقطه اتصال و دستگاه متصل را به‌دست بیاوریم. در این صورت رمز عبور در دستان ما است. برای به‌دست‌آوردن این اطلاعات مهم می‌بایست در هنگام شنود ارتباطات آن دو، در پنجره‌ای دیگر یک حملهٔ DoS[۱] علیه آن انجام دهید، این حمله Deauthentication[۲] نامیده می‌شود.

Deauthentication نوعی از حملات منع سرویس است که توسط امواج رادیویی انجام می‌شود که اتصال مابین نقطه اتصال و کلاینت را متوقف می‌کند. تنها راهی که می‌توانیم WPA Handshake را به‌دست بیاوریم یک حملهٔ DoS چندثانیه‌ای انجام می‌دهیم تا اتصال آن‌ها قطع شود و در اتصال مجدد Handshake را به‌دست می‌آوریم [۴].

۴-۴- شکستن WPA Handshake برای کسب رمز عبور

بعد از به‌دست‌آوردن Handshake باید یک حملهٔ دیکشنری علیهٔ آن انجام دهیم. ساختار این حمله به این صورت است که هر دیکشنری شامل تعدادی واژگان پیش‌بینی‌شده از کلمه عبور که برای بررسی‌کردن کلیهٔ واژگان دیکشنری با کلید اصلی موجود در Handshake چک می‌شود، اگر کلمه عبور موفق‌آمیز باشد، رمز عبور را یافته‌شده می‌داند [۴].

۴-۵- حمله به PMKID[۳]

شکستن رمز عبور برای شبکه‌های WPA سال‌ها بود که به‌طورتقریبی یکسان مانده بود، تا اینکه یک متخصص امنیت در سال ۲۰۱۸ روش جدیدی برای نفوذ شبکه‌های مبتنی بر WPA کشف کرد. در این روش حمله جدید نیاز به مراحل و اطلاعات کمتری نسبت به روش‌های قبلی دارد و از این مزیت هم برخوردار است که نقاط دسترسی‌ای را که هیچ فردی به آن متصل نیست، هدف قرار دهد. این حمله جدید علیه PMK[۴] از Hashcat[۵] برای کرک رمزهای عبور WPA استفاده می‌کند و به مهاجمان این امکان را می‌دهد تا شبکه‌ها را با رمزهای ضعیف را راحت‌تر کرک کنند.

(شکل-۳): شکستن رمز عبور با روش دیکشنری در لینوکس

در این روش یک مهاجم به جای این‌که به برقراری ارتباط متقابل دو طرفه بین دستگاه‌های wi-fi برای امتحان‌کردن رمز عبور، امتحان کند، می‌تواند با استفاده از این روش جدید به‌طورمستقیم با یک نقطه اتصال آسیب‌پذیر ارتباط برقرار کند. در این روش از یک قاب EAPOL[۶] تکی برای گرفتن اطلاعات مورد نیاز برای تلاش برای حمله می‌توان پرداخت. مهاجم باید مانند روش‌های قبلی حمله علیه WPA، در مجاورت شبکه‌ای باشد که می‌خواهد حمله کند. گفتنی است، هر شبکه‌ای در مقابل این حمله آسیب‌پذیر نیست. از آنجا که PMKID یک بسته اختیاری است که توسط برخی تولیدکنندگان تجهیزات اضافه شده است، نباید انتظار موفقیت همگانی را با این روش داشته باشید. اینکه آیا شما قادر به دریافت PMKID هستید، بستگی به این دارد که آیا سازنده نقطه اتصال شما این فیلد را در آن بسته قرار داده است یا خیر و مورد بعدی اینکه رمز عبور انتخابی آسان باشد تا به‌وسیلهٔ دیکشنری‌ها قابل حدس شود [۵].

۴-۶- حملهٔ EVIL-TWIN یا دوقلوی شیطانی

اگرچه سازوکارهای امنیتی wi-fi موجود در درجه نخست روی حفاظت از شبکه متمرکز شده‌اند، اما در سمت کاربر

[1] Denial of Service (DoS)

[۲] نوعی حمله DoS در شبکه‌های بی‌سیم

[۳] PMKID شناسه کلیدی منحصربه‌فردی است که توسط نقطه اتصال برای ردیابی استفاده از PMK برای کاربر استفاده می‌شود.

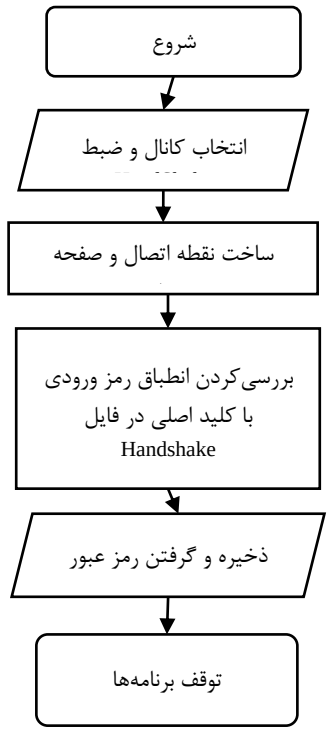
[4] Pairwise Master Key (PMK)

[۵] ابزاری متن باز برای بازگردانی رمز عبور با سرعت بالا و متن باز

[6] Extensible Authentication Protocol Over Local Area Network (EAPOL)

این مسأله به‌نسبه مورد بی‌توجهی قرار گرفته است. حملاتی از قبیل Evil-Twin، که در آن حمله‌کننده یک نقطه اتصال را جعل می‌کند، هنوز امکان‌پذیر هستند؛ اما این حمله چطور اتفاق می‌افتد؟

در این روش مهاجم ضمن ایجاد یک نقطه اتصال جعلی به‌طورتقریبی یکسان، رمزهای wi-fi را سرقت می‌کند. این روش قربانی را مجبور می‌کند تا به شبکهٔ جعلی متصل شود و رمز عبور wi-fi را برای دسترسی مجدد به اینترنت وارد کند. حملهٔ دوقلوی شیطانی، حمله‌ای از نوع wi-fi است که با بهره‌گیری از این واقعیت که بیشتر رایانه‌ها و تلفن‌ها فقط "نام" یا ESSID یک شبکه بی‌سیم را مشاهده می‌کنند، کار می‌کند که این درواقع باعث می‌شود تفاوت بین شبکه‌هایی با همین نام و همان رمزنگاری بسیار دشوار باشد. اگر می‌خواهید ببینید که چگونه این روش کار می‌کند، می‌توانید یک نقطه اتصال wi-fi را بر روی تلفن خود ایجاد کرده و آن را مانند همان شبکه خانگی خود نام‌گذاری کنید تا ببینید که تفاوت بین این دو شبکه قابل تمایز نیست [۶].



(شکل-۴): مراحل روش دوقلوی شیطانی

در شبکهٔ ایجادشدهٔ نهایی، قربانی باید پسورد ورود به شبکه بدون رمز را که مهاجم ایجاد کرده است، در صفحه فیشینگ ظاهری که برای آن‌ها هدایت می‌شود، وارد کند. اگرچه تفاوت‌های زیادی برای تمایز مابین صفحه فیشینگ و صفحه اصلی روتر[1] وجود دارد. ممکن است یک کاربر حرفه‌ای این حمله را متوجه شود، اما به‌طرز شگفت‌انگیزی در برابر افرادی که در مورد رفتارهای مشکوک شبکه آموزش ندیده‌اند، روش مؤثری است [۷].

اکنون که قربانی خود را به نقطه اتصال خود متصل کرده‌اید، می‌توانید اقدامات بعدی را برای شناسایی فعالیت‌های وی روی شبکه انجام دهید. می‌توانید از نرم‌افزاری مانند Ettercap[2] برای انجام یک حملهٔ MITM[3] استفاده کنیم. به این ترتیب، می‌توانیم ترافیک مورد نظرمان را از این کاربر تحلیل و حتی تزریق کنیم، زیرا به نقطه اتصال ما متصل شده است و به‌طورتقریبی به تمام ترافیک عبوری او دسترسی کامل داریم [۸].

این روش برای نفوذ بیش‌تر شبکه‌های بی‌سیم استفاده می‌شود و محدود به پروتکل WPA نمی‌شود. اما باید توجه داشت که بعضی سیستم عامل‌ها نظیر مک[4] زمانی که نوع رمزنگاری شبکه فعلی تغییر می‌کند، این مسأله را به اطلاع کاربر می‌رسانند.

(شکل-۵): نقطه اتصال جعلی و اتصال قربانی [۹]

۷-۴- حمله به پروتکل WEP

این پروتکل در تلاش برای ارائه سطح حفاظت از شبکه‌های wi-fi و حریم خصوصی برابر با سیم در سال ۱۹۹۷ منتشر و در ۱۹۹۹ به‌طوررسمی پذیرفته شد. WEP برای ایجاد ارتباطات بی‌سیم با سطح امنیت و حریم خصوصی آنالوگ با ارتباطات سیمی در نظر گرفته شده بود. با این حال ضعف‌های زیادی در حریم شخصی معادل سیمی مشخص شده است [۱۰].

نخستین ضعف در طی دو سال پس از انتشار رسمی این پروتکل کشف شد. به‌عنوان مثال، WEP از یک کلید ثابت اشتراکی استفاده می‌کند.

[1] Router

[2] یک ابزار امنیتی شبکه برای حملات MITM و تحلیل پروتکل شبکه رایانه‌ای و مدیریت امنیتی استفاده می‌شود.

[3] Man In The Middle (MITM)

[4] Mac

۱-۷-۴- ضعف‌ها و محدودیت‌های WEP

پروتکل WEP دارای ضعف امنیتی از قبیل:

۱- رمزنگاری ضعیف: ترافیک شبکه ضبط‌شده نشان داده که کلید مشترکی را که توسط WEP استفاده می‌شود، می‌توان به‌راحتی برای تجزیه و تحلیل داده‌ها و آن را رمزگشایی کرد که این مسأله می‌تواند منجر به دست‌کاری داده‌ها و از بین رفتن یک‌پارچگی آن شود.

۲- فقدان مدیریت کلید: پروتکل WEP از ویژگی مدیریت کلید برای مدیریت کلیدهای مختلف در جدول کلید خود برخوردار نیست، بلکه از همان کلید برای مدت‌زمان بسیار طولانی استفاده می‌شود.

۳- اندازه کلید کوتاه: اندازه کلید استاندارد WEP فقط کلید چهل بیت است. این مسأله باعث می‌شود که سریع بتوان رمز عبور WEP را به‌وسیلهٔ حملهٔ دیکشنری حدس زد.

۴- مشکلات احراز هویت: با توجه به طرح چالش و پاسخ که در تأیید اعتبار مشترک کلید استفاده می‌شود، حملهٔ مردی در میانه مسیر می‌تواند در WEP انجام شود. این نوع حمله که تلاشی برای دست‌یابی به اطلاعات محرمانه در حال گذر است که این امر منجر به به‌خطرافتادن اطلاعات حساس و در صورت امکان می‌تواند منجر به از بین رفتن اطلاعات نیز شود.

۵- جعل بسته: در WEP هیچ گونه محافظتی در برابر جعل بسته‌ها وجود ندارد. بسته‌های داده با استفاده از برنامه شخص ثالث قابل جعل و تزریق به شبکه هستند، این مسأله می‌تواند منجر به دست‌کاری داده‌ها و ازبین‌رفتن یک‌پارچگی داده‌ها شود.

۶- حملات منع سرویس: این حملات همان‌طور که در قبل هم اشاره کردیم، شامل ارسال بسته‌های داده عظیمی به یک سرویس‌دهنده است که از این طریق از دسترسی کاربران به شبکه جلوگیری می‌شود [۱۱].

در زمان فعلی استفاده از این پروتکل قدیمی بسیار کاهش یافته است، اما با امنیت بسیار پایین آن در رمزنگاری می‌توان در زمان بسیار کوتاهی با ابزارهای موجود در لینوکس این شبکه‌ها را مورد نفوذ قرار داد.

۸-۴- مقایسهٔ امنیتی پروتکل‌ها

طبق بررسی‌های این پژوهش در جدول (۳)، بهترین پروتکل از لحاظ نفوذ در میان سه پروتکل مرسوم WPA2 است با این امکان که رمز عبور انتخابی از طول مناسبی برخوردار باشد. گفتنی است که پروتکل WPA3 تمام مسائل امنیتی موجود را حل کرده است، اگرچه مشکلات جدیدی در آن کشف شده اما جزو پروتکل‌های مورد بحث در این پژوهش نیست.

در جدول (۳) مقایسهٔ کاملی از جانب امکان نفوذ قرارگرفتن در پروتکل‌های مختلف با روش‌های متفاوتی نشان داده شده است.

(جدول-۳): مقایسهٔ امنیت پروتکل‌های رمزنگاری بی‌سیم

روش	WEP	WPA	WPA2
آسیب‌پذیری در رمزنگاری	بله	خیر	خیر
امکان شکستن رمز عبورضعیف	بله	بله	بله
امکان حملهٔ Evil-Twin	بله	بله	بله
امکان حمله PMKID	خیر	بله	بله

۵- افزایش امنیت تجهیزات بی‌سیم

در این قسمت از پژوهش روش‌هایی برای افزایش امنیت شبکه‌های بی‌سیم در مقابل مهاجمان ارائه می‌کنیم.

۱-۵- مخفی‌کردن SSID شبکه

این ویژگی به‌سادگی مانع از انتشار نام شبکهٔ بی‌سیم شما در اطراف می‌شود. طبیعی است که اگر نام شبکه شما در "فهرست شبکه‌های موجود" در اطرافیان در حال جستجوی شما ظاهر شود انگیزهٔ کافی برای نفوذ به آن‌ها در ذهنشان تداعی می‌شود [۱۲].

۲-۵- استفاده از فیلتر نشانی فیزیکی[1]

به‌طور معمول، یک دستگاه بی‌سیم سابقه‌ای از نشانی MAC[2] همهٔ دستگاه‌های متصل به آن را در خود نگه می‌دارد. نشانی MAC یا نشانی فیزیکی منحصربه‌فرد هر وسیله اتصال اینترنتی مانند تبلت و لپ‌تاپ و هرچیزی را شناسایی می‌کند. دستگاه‌هایی که در این فهرست وجود ندارند، به‌طور خودکار از دسترسی به شبکه محروم می‌شوند [۱۳].

[1] MAC Filtering
[2] Media Access Control

۵-۳- انتخاب رمز عبور مناسب

تأکید بر اهمیت رمزعبور قوی در همه حساب‌های شما دشوار است. استفاده از ۱۲۳۴۵۶ یا نام حیوان خانگی به‌عنوان رمز عبور دستگاه شما مانند قفل‌کردن درب خانه و قراردادن کلیدها در زیر گلدان گل در کنار درب است. مهاجمان افرادی باهوش هستند که از جمله تمام رمزهای عبور ممکن شما را حدس می‌زنند. برای یک رمز عبور قوی از ترکیبی از حروف، اعداد، نمادها و نویسه‌های ویژه استفاده کنید. هرگز از گذرواژه‌ای که به شما یا خانواده‌تان مرتبط است استفاده نکنید [۱۴].

۵-۴- خاموشی دستگاه

خاموش‌کردن دستگاه خود در طی ساعات طولانی عدم استفاده مزایای مختلفی را دارد، در ابتدا وقتی دستگاه خاموش است، امواج آن هم در محیط وجود ندارد تا افرادی برای نفوذ به آن تلاش کنند و این مورد باعث کاهش هزینه مصرف برق و افزایش عمر قطعات الکترونیکی خواهد شد [۱۵].

۵-۵- استفاده از رمزنگاری امن

رمزنگاری قوی مهاجم را در نفوذ ناکام خواهد گذاشت. برای ارتقای امنیت خود از پروتکل WPA3 استفاده کنید و درصورت عدم پشتیانی این نسخه، از نسخه دوم آن استفاده کنید [۱۵].

۵-۶- به‌روزرسانی دستگاه

نرم‌افزارهای قدیمی دارای آسیب‌پذیری‌های بی‌شماری هستند که می‌توانند توسط مهاجمان برای دسترسی به شبکه شما مورد سوء استفاده قرار بگیرد. از این بدتر، بیش‌تر نرم‌افزارهای قدیمی منسوخ‌شده حمایت شرکت سازنده را شامل نمی‌شوند که ممکن است، توسعه‌دهندگان آن دیگر وصله‌های امنیتی را برای حفره‌های جدید منتشر نکنند؛ درنتیجه اطمینان حاصل کنید که دستگاه بی‌سیم با جدیدترین نسخه به‌روزرسانی شده است. نسخه‌های جدید را در تارنمای توسعه‌دهنده نرم‌افزار خود بررسی کنید [۱۵].

۶- نتیجه

شبکه‌های بی‌سیم یکی از محبوب‌ترین فناوری‌هایی است که در سراسر جهان گسترش یافته است؛ اما با این وجود تعداد اندکی از کاربران از وضعیت ایمنی و تحت نفوذ قرار گرفتن شبکه بی‌سیم wi-fi خود اطلاع دارند، کاربران معمولی اغلب فقط یک مودم روتر wi-fi خریداری می‌کند و آن را با پیکربندی پیش‌فرض خود راه‌اندازی می‌کنند و هیچ گام دیگری را برای تأمین امنیت بیشتر برنمی‌دارند که این مسأله به‌طور بالقوه می‌تواند به‌خودی خود بسیار خطرناک باشد. در این مقاله ما مطالعات نظری و عملی در مورد امنیت شبکه‌های بی‌سیم را با تجزیه و تحلیل عمیق در حملات مختلف در انواع شبکه‌های بی‌سیم wi-fi و نقاط ضعف پروتکل WPA و به‌دست‌آوردن رمز عبور این شبکه‌ها مورد بررسی قرار داده‌ایم. کلیه مطالبی که در این پژوهش ارائه شده است، نه‌تنها به کاربران خانگی به حفظ امنیت کمک می‌کند، بلکه به کارمندان سازمانی نیز برای تأمین امنیت شبکه خود کمک شایانی می‌کند.

۷- مراجع

[1]R.Guo," Survey WiFi infrastructure attacks" International Journal of Wireless and Mobile Computing 16, pp.97-101, 2019

[2]T.Chang,L.Jiunn-Wu,Ch.Chia-Mei,L.Gu-Hsin,"The Method of Capturing the Encrypted Password Packets of WPA & WPA2, Automatic, Semi-Automatic or Manual?" , IEEE Conference,Dependable and Secure Computing (DSC), pp. 1-4, 2018.

[3]Cracking WPA2-PSK Passwords Using Aircrack-Ng, https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-psk-passwords-using-aircrack-ng-0148366/

[4]Getting Started with the Aircrack-Ng Suite of Wi-fi Hacking Tools, https://null-byte.wonderhowto.com/how-to/hack-wi-fi-getting-started-with-aircrack-ng-suite-wi-fi-hacking-tools-0147893/

[5]Cracking WPA2 Passwords Using the New PMKID Hashcat Attack, https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-passwords-using-new-pmkid-hashcat-attack-0189379/pmkid

[6]A. Esser, S. Carlos,"Wi-fi network testing using an integrated Evil-Twin framework.",Fifth International Conference on Internet of Things: Systems, Management and Security, pp.216-221. IEEE, 2018

[7]O,Nakhila, , Z,Cliff,"User-side wi-fi evil twin attack detection using random wireless channel monitoring." ,MILCOM IEEE Military Communications Conference, pp. 1243-1248. IEEE, 2016.

[8]Stealing Wi-fi Passwords with an Evil Twin Attack, https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-with-evil-twin-attack-0183880/

[9]P. Čisar,Maravić Čisar. "ETHICAL HACKING OF WIRELESS NETWORKS IN KALI LINUX ENVIRONMENT.", Annals of the Faculty of Engineering Hunedoara 16: pp.181-186,2018.

[10]Rahman,Ur Rizwan,S. Tomar Deepak."Security Attacks on Wireless Networks and Their Detection Techniques." Springer, Singapore, Emerging Wireless Communication and Network Technologies, pp. 241-270., 2018.

[11]A.Sari,K. Mehmet. "Comparative analysis of wireless security protocols: WEP vs WPA." International Journal of Communications, Network and System Sciences 8, no. 12 ,pp.483-491 ,2015.

[12]10 Tips to harden the Wireless Network Security ,https://securitygladiators.com/secure-wireless-network/

[13]Furqan, Haji M., Muhammad Sohaib J. Solaija, Halise Türkmen, and Hüseyin Arslan. "Wireless communication, sensing, and REM: a security perspective." IEEE Open Journal of the Communications Society 2 ,287-321.

[14]Al-Ghamdi, Mohammed I. "Wireless Networks Between Security and Efficiency.", 2021

[15]Azhar, Nurul Fatini, Qi Jie Ngoo, Tae Hyun Kim, Kohei Dozono, and Fatima tuz Zahra. "Security and Privacy Issues in Wireless Networks." 2020.

حمیدرضا محمدی تحصیلات مقطع کارشناسی ارشد را در رشته مهندسی رایانه گرایش شبکه‌های رایانه‌ای در دانشگاه آزاد اسلامی واحد لاهیجان گذرانده است. وی دارای مدارک بین المللی سیسکو و امنیت است و هم اکنون به‌عنوان مدرس دوره‌های امنیت فناوری اطلاعات، برنامه‌نویس پایتون با رویکرد امنیتی و پژوهش‌های امنیتی در توسعه پروتکل‌های شبکه در حال فعالیت است.