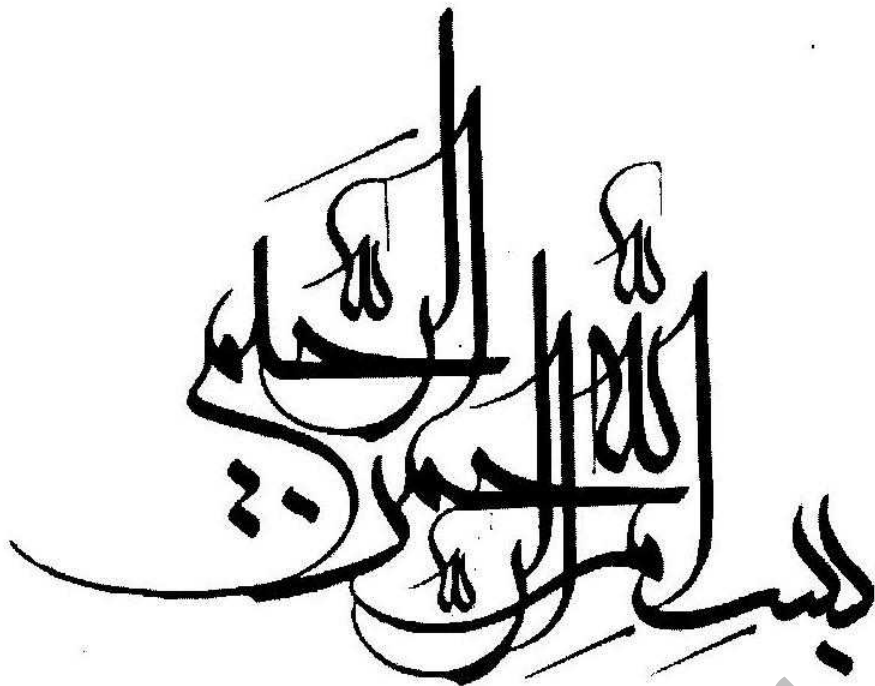




عنوان:

امنیت در شبکه های وای فای (Wi-Fi Security)



مولفان
علی شجاعی
رحیم کریمی

سرشناسه	: شجاعی، علی / ۱۳۵۴
عنوان و نام پدیدآور	: امنیت در شبکه های وی فا / علی شجاعی / رحیم کریمی
مشخصات نشر	: تهران ، نقش آفرینان بابکان
مشخصات ظاهری	: مصور
شابک	: ۹۷۸-۶۰۰-۷۷۵۶-۷۰-۶
وضعیت فهرست نویسی	: فیبا
موضوع	: ارتباطات بی سیم--تدابیر امنیتی
شناسه فزوده	: کریمی، رحیم، ۱۳۵۸-
رده بندی شنگره	: ۱۳۹۵ الف ۳ ش / ۴۸۸۵ / ۳ TK۵۱۰۳
رده بندی یوبی	: ۰۰۴/۶۷۸
شماره کتابشناسی ملی	: ۴۴۳۲۳۲۷

نام کتاب	: امنیت در شبکه های وی فا
مؤلفان	: علی شجاعی / رحیم کریمی
ناشر	: انتشارات نقش آفرینان بابکان
صفحه آرای و طراحی جلد	: بلژوفنی و حرفه ای
لینوگرافی و چاپ	: نقش آفرینان
شمارگان	: ۱۰۰ جلد
نوبت چاپ	: اول - ۱۳۹۵
قیمت:	: ۱۲۰۰۰ تومان
شابک	: ۹۷۸-۶۰۰-۷۷۵۶-۷۰-۶

چکیده

امروزه امنیت یکی از ضروری ترین مواردی است که در راه اندازی هر شبکه ای باید اعمال گردد. با گسترش شبکه های بی سیم (وای فای) و استفاده زیاد و عمومی شدن این شبکه ها، برقراری امنیت در آن یک امر مهم و ضروری می باشد. همانطور که راه اندازی این شبکه بی سیم بسیار راحت و اتصال به آن نیز بسیار سریع می باشد، به همین سادگی و سرعت نیز امکان رخنه در آن وجود دارد. امنیت در شبکه های وای فای که در کاربردهای نظامی، تجاری و سازمانی هستند به یکی از بزرگترین چالش های این شبکه ها تبدیل شده است و نشت هرگونه اطلاعات یا آسیب رسیدن به شبکه می تواند فاجعه انگیز باشد و گاهی جبران آن غیر ممکن باشد.

با توجه به ماهیت این دسته از شبکه ها، که بر اساس سیگنال های رادیویی اند، مهم ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن است. نظر به لزوم آگاهی از خطرات استفاده از این شبکه ها، با وجود امکانات نهفته در آن ها که به ما پیگردی صحیح می توان به سطح قابل قبولی از بعد امنیتی دست یافت.

در این مجموعه سعی کرده ام که معرفی اجمالی از طریقه کار این شبکه ها و استاندارد ها و پروتکل های به کار رفته در آن پردازم، سپس به معرفی راهکارهای امنیتی موجود و راه حل آنها و در نهایت ارائه پروتکل ها و استاندارد های امنیتی در این شبکه ها پردازم.

فهرست مطالب

۹	فصل اول : معرفی شبکه های وای فای
۱۰	۱-۱ شبکه های Wi-Fi چیست؟
۱۱	۲-۱ کاربردهای Wi-Fi
۱۲	۳-۱ دلایل رشد Wi-Fi
۱۴	۴-۱ ترکیب سیستم Wi-Fi با رایانه
۱۴	۵-۱ شبکه Wi-Fi چگونه کار می کنند؟
۱۵	۱-۶ تحلیل ترافیک شبکه های Wi-Fi
۱۸	۷-۱ آینده شبکه های Wi-Fi
۱۸	۸-۱ نتیجه گیری
۱۹	فصل دوم : استاندارد های شبکه محلی بی سیم
۲۰	۱-۲ معرفی
۲۳	۲-۲ معماری شبکه های محلی بی سیم
۲۳	۱-۲-۲ همبندی های ۸۰۲.۱۱
۲۵	۳-۲ خدمات ایستگاهی
۲۶	۴-۲ خدمات توزیع
۲۷	۵-۲ دسترسی به رسانه
۲۸	۵-۲-۱ الایه فیزیکی
۳۵	۶-۲ استاندارد 802.11B
۳۶	۶-۲-۱ اثرات فاصله
۳۶	۶-۲-۲ پل بین شبکه ای
۳۷	۷-۲ استاندارد 802.11A
۳۹	۸-۲ استاندارد بعدی IEEE 802.11G
۴۰	فصل سوم : مفاهیم امنیتی در شبکه های بی سیم
۴۱	۱-۳ فاکتورهای امنیتی در شبکه های بی سیم
۴۳	۲-۳ سیستم تشخیص نفوذ
۴۶	۳-۳ چالش های امنیتی در شبکه های Wi-Fi
۴۷	۴-۳ نقاط آسیب پذیر و قابل نفوذ در شبکه های Wi-Fi
۵۰	۵-۳ امن سازی شبکه های بی سیم
۵۰	۵-۳-۱ احراز هویت
۵۳	۵-۳-۲ امنیت داده ها

۵۴	۶-۳ مدیریت کلید ها.....
۵۵	۷-۳ صحت داده.....
۵۵	۸-۳ نتیجه گیری.....
۵۶	فصل چهارم: چالش های امنیتی و راه کار ها در شبکه های وای فای.....
۵۷	۱-۴ مقدمه.....
۵۷	۲-۴ مشکل اول: دسترسی آسان.....
۵۸	۱-۲-۴ راه حل مشکل اول: تقویت کنترل دسترسی قوی.....
۵۹	۳-۴ مسأله دوم: نقاط دسترسی نامطلوب.....
۶۰	۱-۳-۴ راه حل مشکل دوم: رسیدگی های منظم به سایت.....
۶۱	۴-۴ مشکل سوم: استفاده غیر مجاز از سرویس.....
۶۲	۱-۴-۴ راه حل مشکل سوم: طراحی و نظارت برای تأیید هویت محکم.....
۶۲	۵-۴ مشکل چهارم: محدودیت های سرویس و کارایی.....
۶۳	۵-۴-۱ راه حل مشکل چهارم: بدبانی شبکه.....
۶۴	۶-۴ مشکل پنجم: جعل SSID و MAC: ربایان.....
۶۵	۱-۷-۴ راه حل شماره ۵: پذیرش رمزنگاری قوی و استفاده از آنها.....
۶۵	۷-۴ مشکل ششم: تحلیل ترافیک و استراق سمع.....
۶۶	۱-۷-۴ راه حل مشکل ششم: انجام تحلیل خطر.....
۶۷	۸-۴ مشکل هفتم: حملات سطح بالاتر.....
۶۷	۸-۴-۱ راه حل مشکل هفتم: هسته را از LAN بی سیم محافظت کنید.....
۶۷	۹-۴ چند نکته در مورد امن سازی شبکه های وای فای.....
۶۹	۱۱-۴ جمع بندی.....
۸۱	فصل پنجم: پروتکل های امنیتی در شبکه های وای فای.....
۸۲	۱-۵ مقدمه.....
۸۲	۲-۵ پروتکل اتصال/دسترسی در شبکه های وای فای.....
۸۳	۳-۵ قابلیت ها و ابعاد امنیتی استاندارد ۸۰۲.۱۱.....
۸۴	احراز هویت (Authentication).....
۸۴	محرمانگی (Confidentiality).....
۸۵	صحت (Integrity).....
۸۵	۴-۵ خدمات ایستگاهی.....
۸۶	۱-۴-۵ احراز هویت Authentication.....
۸۶	۲-۴-۵ سرویس امنیت (Privacy/confidentiality).....
۸۸	۳-۴-۵ صحت (Integrity).....
۸۹	۵-۵ ضعف های اولیه ی امنیتی WEP.....

- ۹۰ ۱-۵-۵ استفاده از کلیدهای ثابت WEP
- ۹۰ Initialization Vector – IV ۲-۵-۵
- ۹۰ ۳-۵-۵ ضعف در الگوریتم
- ۹۱ ۴-۵-۵ استفاده از CRC رمز نشده
- ۹۴ ۶-۵ پروتکل WPA(Wi-Fi Protected Access)
- ۹۶ ۷-۵ پروتکل WPA2
- ۹۸ ۸-۵ پروتکل امنیتی WPS
- ۹۹ ۹-۵ جمع بندی
- ۱۰۰ مشکلات فعلی و کارهای آتی

مقدمه

شبکه های بی سیم (Wireless) یکی از تکنولوژی های جذابی هستند که توانسته اند توجه بسیاری را بسوی خود جلب نمایند و عده ای را نیز مسحور خود نموده اند. هرچند این تکنولوژی جذابیت و موارد کاربرد بالایی دارد ولی مهمترین مرحله که تعیین کننده میزان رضایت از آن را بدنبال خواهد داشت ارزیابی نیاز ها و توقعات و مقایسه آن با امکانات و قابلیت های این تکنولوژی است.

شبکه های WLAN را نمی توان جایگزینی برای شبکه های Ethernet معرفی کرده، بلکه شبکه های WLAN یک راه حل هستند برای مواقعی که امکان کابل کشی و استفاده از شبکه Ethernet امکانپذیر نیست و یا اولویت Mobility و یا حفظ زیبایی محیط است. سالن های کنفرانس، انبارها، محیط های کارخانه ای، کارگاه های عمرانی و محیط های نمایشگاهی بهترین نمونه ها برای استفاده موثر از شبکه های WLAN میباشند.

شبکه های LAN به صورت فیزیکی از شبکه های بی سیم امن تر می باشند، چرا که از نظر ساختاری قسمت عمده و یا تمام ساختار آنها در درون یک ساختمان قرار دارد و بدین دلیل از دسترسی های غیر مجاز در امان هستند. اما شبکه های بی سیم در استفاده از امواج رادیویی فعالیت می کنند از آنجا که همانند شبکه های LAN دارای ساختاری فیزیکی هستند، بیشتر در معرض نفوذ قرار داشته و آسیب پذیرترند، بنابراین مسئله امنیت به طور جدی در این شبکه ها مطرح می شود و گاهی مسائل و مشکلاتی امنیتی که در این شبکه ها وجود دارد، در شبکه های محلی بی سیم وجود نداشته و باید دنبال راه کار ها و پروتکل های امنیتی باشیم که در صدد رفع و برآورده کردن نیاز امنیتی، خاص این شبکه ها باشد.

اتصال بی سیم، یک رسانه فیزیکی است و برای تأمین امنیت آن نمی توان تنها به وجود یک دیوار آتش تکیه کرد. کاملاً واضح است که نقاط دسترسی غیرمجاز، به واسطه ایجاد راه های ورود مخفی به شبکه و مشکل بودن تعیین موقعیت فیزیکی آنها، نوعی تهدید علیه شبکه به شمار می روند. علاوه بر این نقاط دسترسی، باید نگران لپ تاپ های بی سیم متصل به شبکه سیمی نیز باشیم. یافتن لپ تاپ های متصل به شبکه سیمی که یک کارت شبکه بی سیم فعال دارند، اقدامی متداول برای ورود به شبکه محسوب می شود. در اغلب موارد این لپ تاپ ها توسط SSID شبکه هایی را که قبلاً مورد دسترسی قرار داده اند، جست و جو می کنند و در صورت یافتن آنها صرف نظر از این که اتصال به شبکه قانونی یا مضر باشد یا شبکه بی سیم در همسایگی شبکه فعلی قرار داشته باشد، به طور خودکار به آن وصل می شوند. به محض این که لپ تاپ به یک شبکه مضر متصل شود، مهاجمان آن را مورد حمله قرار داده و پس از اسکن و یافتن نقاط ضعف ممکن است کنترل آن را به دست گرفته و به عنوان میزبانی برای اجرای حمله ها به کار گیرند. در این شرایط علاوه

بر افشای اطلاعات مهم لپ تاپ، مهاجم می تواند از آن به عنوان نقطه شروعی برای حمله به شبکه سیمی استفاده کند. مهاجم در صورت انجام چنین اقداماتی، به طور کامل از دیواره آتش شبکه عبور می کند.

چنین نقطه ضعفی شبکه را به یک اسباب سرگرمی برای مهاجم تبدیل می کند. در حقیقت، نفوذ به چنین شبکه ای حتی نیازمند یک اسکن فعال یا حمله واقعی نیست. به واسطه ردیابی جریان اطلاعاتی یک شبکه بی سیم علاوه بر شناسایی توپولوژی بخش سیمی آن می توان اطلاعات مربوط به تجهیزات حیاتی شبکه و حتی گاهی اطلاعات مربوط به حساب های کاربری را به دست آورد.

با توجه به مطالب گفته شده در بالا نیاز به پروتکل ها و تدابیر امنیتی ویژه ای داریم که خاص این شبکه ها باشد و بتوان امنیت در این شبکه ها را تامین کرد. در این ادامه تکنیک ها و روش های امن سازی این شبکه ها و پروتکل ها و استاندارد های امنیتی موجود را بررسی می کنیم.