

دانشگاه زنجان

دانشکده مهندسی

گروه برق

پایان نامه کارشناسی

گرایش: مخابرات

عنوان:

امنیت شبکه های بی سیم

استاد راهنما: دکتر مهدی قمری ادیان

نگارش: سید محمد علی قاسمی ۹۲۴۴۳۱۱۵

محمد خیام ۹۲۴۴۳۱۰۷

تابستان ۹۶

مابان نام کارسناسی

فهرست

مقدمه	۱
فصل اول	۳
معرفی شبکه های Wi-Fi	۳
۱-۱ شبکه های Wi-Fi چیست؟	۴
۲-۱ کاربرد های Wi-Fi	۴
۳-۱ ترکیب سیستم Wi-Fi در رایانه	۵
۴-۱ شبکه Wi-Fi چگونه کار می کند؟	۵
۵-۱ تحلیل ترافیک شبکه های Wi-Fi	۷
فصل دوم	۱۰
استاندارد های شبکه محلی بی سیم	۱۰
۱-۲ معرفی	۱۱
۲-۲ معماری شبکه های محلی بی سیم	۱۲
۲-۲-۱ همبندی های ۸۰۲,۱۱	۱۳
۳-۲ خدمات ایستگاهی	۱۵
۴-۲ خدمات توزیع	۱۶
۵-۲ دسترسی به رسانه	۱۷
۵-۲-۱ لایه فیزیکی	۱۹
۶-۲ مروری بر استاندارد جدید ۸۰۲,۱۱n	۱۹
فصل سوم	۲۱
مفاهیم امنیتی در شبکه های بی سیم	۲۱
۱-۳ فاکتور های امنیتی در شبکه های بی سیم	۲۲
۲-۳ سیستم تشخیص نفوذ	۲۴
۳-۳ چالش های امنیتی در شبکه های Wi-Fi	۲۷

۳-۴	نقاط آسیب پذیر و قابل نفوذ در شبکه های Wi-Fi	۲۹
۳-۵	امن سازی شبکه های بی سیم	۳۲
۳-۵-۱	احراز هویت	۳۳
۳-۵-۱-۱	Authentication بدون رمزنگاری	۳۴
۳-۵-۱-۲	Authentication با رمزنگاری RC۴	۳۴
۳-۵-۲	امنیت داده ها	۳۶
۳-۶	مدیریت کلید ها	۳۷
۳-۷	صحت داده ها	۳۷
۳-۸	نتیجه گیری	۳۸
۳-۹	فصل چهارم	۳۹
۳-۹	چالش های امنیتی و راه کار ها در شبکه های وای فای	۳۹
۴-۱	مقدمه	۴۰
۴-۲	مشکل اول: دسترسی آسان	۴۰
۴-۲-۱	راه حل مشکل اول : تقویت کنترل دسترسی قوی	۴۱
۴-۳	مشکل دوم : نقاط دسترسی نامطلوب	۴۳
۴-۳-۱	راه حل مشکل دوم : رسیدگی های منظم به سایت	۴۳
۴-۴	مشکل سوم : استفاده غیر مجاز از سرویس	۴۵
۴-۴-۱	راه حل مشکل سوم : طراحی و نظارت برای تأیید هویت محکم	۴۶
۴-۵	مشکل چهارم : محدودیت های سرویس و کارایی	۴۶
۴-۵-۱	راه حل مشکل چهارم : دیدبانی شبکه	۴۷
۴-۶	مشکل پنجم : جعل MAC و SESSION ربای!	۴۸
۴-۶-۱	راه حل شماره ۵ : پذیرش پروتکل های قوی و استفاده از آنها	۴۹
۴-۷	مشکل ششم : تحلیل ترافیک و استراق سمع	۵۰
۴-۷-۱	راه حل مشکل ششم : انجام تحلیل خطر	۵۰
۴-۸	مشکل هفتم : حملات سطح بالاتر	۵۲
۴-۸-۱	راه حل مشکل هفتم : هسته را از LAN بی سیم محافظت کنید	۵۲
۴-۹	چند نکته در مورد امن سازی شبکه های وای فای	۵۲
۴-۹-۱	کلمه عبور پیش فرض مدیر سیستم (ADMINISTRATOR) را روی نقاط دسترسی و مسیر یاب های بی سیم تغییر دهید	۵۲
۴-۹-۲	فعال سازی قابلیت WPA/WEP	۵۳
۴-۹-۳	تغییر SSID پیش فرض	۵۳
۴-۹-۴	قابلیت پالایش آدرس MAC را روی نقاط دسترسی و مسیر یاب های بی سیم فعال کنید	۵۴
۴-۹-۵	قابلیت همه پختی SSID را روی نقاط دسترسی و مسیر یاب های بی سیم غیر فعال کنید	۵۵
۴-۹-۶	به شبکه های Wi-Fi باز ، وصل نشوید	۵۶
۴-۹-۷	به تجهیزات آدرس (IP) ایستا اختصاص دهید	۵۷
۴-۹-۸	قابلیت فایروال را روی کامپیوترها و مسیر یاب ها فعال کنید	۵۸

۹-۹-۴	مسیر یاب ها و نقاط دسترسی را در مکان های امن قرار دهید.....	۵۸
۱۰-۹-۴	در فواصل زمانی طولانی که از شبکه استفاده نمی کنید تجهیزات را خاموش کنید	۵۹
۱۰-۴-۴	پنج اشتباه متداول در باره امنیت شبکه های بیسیم.....	۶۱
۱-۱۰-۴	دیوار آتش = تأمین امنیت کامل در برابر ورود غیر مجاز به شبکه.....	۶۱
۲-۱۰-۴	دیوار آتش = تأمین امنیت کامل در برابر ورود غیر مجاز به شبکه.....	۶۲
۳-۱۰-۴	اسکن دستی = شناسایی تمام نقاط دسترسی غیر مجاز.....	۶۳
۴-۱۰-۴	به روز رسانی تمام نقاط دسترسی به منظور حذف پروتکل WEP = تأمین امنیت کامل شبکه.....	۶۳
۵-۱۰-۴	استفاده از نرم افزار کلاینت VPN = محافظت از کارمندان سیار.....	۶۴
فصل پنجم	۶۶
انواع حملات و تهدیدات	۶۶
۱-۵	مقدمه.....	۶۷
۲-۵	حملات کنترل دسترسی.....	۶۷
۳-۵	حملات ضد پیکار چگی داده ها.....	۶۸
۴-۵	حملات ضد محرمانگی داده ها.....	۶۹
۵-۵	حملات ضد در دسترس پذیری.....	۷۰
۶-۵	حملات ضد احراز هویت.....	۷۱
۷-۵	بررسی برخی حملات.....	۷۲
۱-۷-۵	حمله بر اساس اکسپوینت جعلی.....	۷۲
۲-۷-۵	قطع ارتباط کلاینت.....	۷۴
۳-۷-۵	حمله بر مبنای اکسپوینت که به اشتباه پیکربندی شده است.....	۷۴
۴-۷-۵	ارتباط غیر مجاز.....	۷۵
۵-۷-۵	حمله بر اساس کانکشن Ad Hoc.....	۷۵
۶-۷-۵	حمله HoneySpot Access Point.....	۷۶
۷-۷-۵	حملات AP MAC Spoofing.....	۷۶
۸-۷-۵	حملات منع سرویس (DoS) مک.....	۷۷
۹-۷-۵	حملات سیگنال های پارازیت (Jamming Signal).....	۷۸
فصل ششم	۷۹
ارائه روشی برای مقابله با حملات DoS ناشی از فریم های مدیریت در IEEE ۸۰۲.۱۱i.....	۷۹	
۱-۶	مقدمه.....	۸۰
۲-۶	حملات DoS.....	۸۱
۳-۶	فریم های مدیریت.....	۸۱
۴-۶	حملات روی فریم های مدیریت.....	۸۳
۱-۴-۶	جعل آدرس MAC.....	۸۴
۲-۴-۶	حملات DoS.....	۸۴
۳-۴-۶	سرقت نشست.....	۸۵

۴-۴-۶	حمله MitM	۸۵
۵-۶	IEEE 802.11i	۸۵
۶-۶	طرح بهبود امنیت در IEEE 802.11i	۸۶
۱-۶-۶	الگوریتم فیلترینگ ترافیک	۸۹
۲-۶-۶	الگوریتم فیلترینگ آدرس MAC	۹۰
۷-۶	ارزیابی طرح بهبود امنیت IEEE 802.11i	۹۲
۱-۷-۶	احتمال جعل فریم ها	۹۲
۲-۷-۶	سربار محاسبه فریم های مدیریت	۹۳
۸-۶	نتیجه گیری	۹۶
	فصل هفتم	۹۸
	سرقت نشست (Session Hijacking)	۹۸
۱-۷	مقدمه	۹۹
۲-۷	پروتکل TCP	۹۹
۳-۷	پروتکل UDP	۱۰۱
۴-۷	پروتکل TCP	۱۰۲
۵-۷	قربانی ها کجای داستان قرار میگیرند؟	۱۰۲
۶-۷	سطوحی که حمله در آن رخ میدهد	۱۰۴
۱-۶-۷	سطح Network	۱۰۴
۷-۷	Session چیست؟	۱۰۹
۱-۷-۷	یک session به چه دردی میخورد؟	۱۰۹
۲-۷-۷	ساختار یک session	۱۱۰
۳-۷-۷	یک session چگونه کار میکند؟	۱۱۰
۸-۷	Network Level	۱۱۱
۱-۸-۷	پروتکل های انتقال رمز شده	۱۱۱
۲-۸-۷	IPSec	۱۱۲
۳-۸-۷	SSL	۱۱۲
۴-۸-۷	SSH	۱۱۲
۵-۸-۷	خنثی کردن ترفندهای مهاجم	۱۱۳
۹-۷	نتیجه گیری	۱۱۳
	فصل هشتم	۱۱۴
	نقاط دسترسی غیر مجاز و حمله ی مردی در میانه	۱۱۴
۱-۸	مقدمه	۱۱۵
۲-۸	دستگاه های بی سیم غیر مجاز داخلی	۱۱۵
۳-۸	عوامل تهدید در دسترسی غیر مجاز داخلی	۱۱۶
۴-۸	انواع دستگاه های بی سیم غیر مجاز	۱۱۷
۵-۸	خسارت های ناشی از دستگاه های بی سیم مخرب داخلی	۱۱۹

مقدمه

شبکه های بی سیم (Wireless) یکی از تکنولوژی های جذابی است که توانسته در ۳ دهه اخیر توجه بسیاری را به خود جلب کند و به دنبال آن پژوهش ها و تحقیقات زیادی صورت گرفته و هم اکنون نیز شاهد پیشرفت های زیادی در این زمینه هستیم. ارزیابی نیازها و توقعات و مقایسه آن با امکانات و قابلیت هایی که این تکنولوژی در اختیار میگذارد، مهم ترین مرحله ی تعیین کننده میزان کارآمدی و رضایت از این دسته شبکه ها می باشد.

شبکه های WLAN را نمی توان جایگزینی برای شبکه های کابلی Ethernet کرد، بلکه این شبکه ها راه حلی است برای مواردی که امکان کابل کشی و استفاده از شبکه Ethernet امکان پذیر نیست و یا اولویت با امکان جابجایی (Mobility) و یا زیبا سازی محیط میباشد. سالن های کنفرانس، انبارها، کارخانجات، کارگاه های عمرانی و محیط های نمایشگاهی بهترین نمونه ها برای استفاده موثر از شبکه های WLAN می باشند.

شبکه های سیمی به صورت ذاتی از شبکه های بی سیم امن تر می باشند، چرا که تمام و یا بخش عمده ی آن دارای ساختاری یکپارچه می باشد و به همین دلیل است که امکان دسترسی غیر مجاز به این شبکه ها بسیار کم تر از شبکه های بی سیم است. این در حالی است که شبکه های بی سیم با استفاده از امواج رادیویی فعالیت میکنند و به علت فیزیکی نبودن آن ها مانند شبکه های سیمی، بیشتر در معرض نفوذ قرار داشته و آسیب پذیرتر میباشند.

بنابراین مساله 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 سیمی وجود نداشته و باید به دنبال راه کارها و پرتکل های امنیتی باشیم که در صدد رفع و برآورده کردن نیازهای امنیتی مختص این شبکه ها باشد. اتصال بی سیم، یک رسانه غیر فیزیکی است و برای تامین امنیت آن نمی توان تنها به وجود یک دیوار آتش بسنده کرد. به وضوح می توان نقاط دسترسی غیر مجاز را به واسطه ی ایجاد راه های ورود مخفی به شبکه و

مشکل بودن تعیین موقعیت فیزیکی آن ها، نوعی تهدید برای شبکه به شمار آورد.

مابان نامہ کارسناسی

فصل اول

معرفی شبکه های Wi-Fi

۱-۱ شبکه های Wi-Fi چیست ؟

وای فای (Wi-Fi) مخفف عبارت Wireless Fidelity است و استاندارد از زیر مجموعه Bluetooth

است و تحت آن ارتباطی با قدرت بیشتر از خود Bluetooth ایجاد می شود. ارتباط Wi-Fi بیشتر بر

پایه ارتباط شبکه اینترنت به صورت بی سیم تاکید می کند و همین امر باعث محبوبیت بسیار زیاد آن

شده است. با استفاده از این تکنولوژی میتوان به راحتی در مسافرت، هتل، هواپیما، دانشگاه و... از طریق

لپتاب، موبایل و یا تبلت خود به اینترنت متصل شد. Wi-Fi که همان استاندارد IEEE 802.11 است در

مدل های 802.11g و 802.11b مورد استفاده قرار می گیرد و استاندارد اصلی آن IEEE 802.11b است.

در این مدل حد اکثر سرعت انتقال اطلاعات 11 مگابیت بر ثانیه است و از فرکانس رادیویی 2/4 گیگاهرتز

استفاده میکند. برای سرعت بخشیدن به این استاندارد مدل دیگری نیز به نام 802.11n ایجاد شده که

سرعت انتقال را تا 200 مگابیت بر ثانیه افزایش می دهد. افزایش سرعت در 802.11n به دلیل استفاده

از سیستم های چند آنتنه (MIMO)، استفاده همزمان از دو محدوده ی فرکانسی 2/4 و 5 گیگاهرتز، و

برخی تکنیک های خاص در دسترس محیط (Medium Access-MAC) است. برد Wi-Fi در حدود

20 متر است. امروزه افراد برای استفاده از این نوع ارتباط بیشتر با موبایل و تبلت های خود که دارای این

نوع خدمات هستند استفاده میکنند البته اغلب لپتاب های امروزی نیز دارای آن می باشند. کسانی که

خواهان استفاده از آن بر روی PC یا همان رایانه شخصی خود می باشند نیز می توانند از یک کارت خارجی

گیرنده امواج Wi-Fi و یا مودمی که درون دستگاه قرار میگیرد استفاده کنند.

۱-۲ کاربرد های Wi-Fi

همانطور که گفته شد تکنولوژی Wi-Fi علاوه بر ارتباط رایانه های شخصی به اینترنت، این امکان را

برای تلفن های همراه نسل جدید و تبلت ها نیز فراهم می کند. همچنین به عنوان راه حلی موثر به منظور

توسعه شبکه های داخلی، بدون صرف هزینه سیم کشی مطرح شده است.

دو تکنولوژی Wi-Fi و Bluetooth به عنوان رقبای یکدیگر در شبکه های بی سیم مطرح شده اند و هم اکنون نیز رقابت آن ها در حال افزایش است ، اما هدف این دو فناوری یکسان نیست و هرکدام هدف جداگانه ای را در پیش گرفته اند .

Bluetooth برای استفاده در شبکه های بی سیم کوچک در نظر گرفته شده است که دارای مصرف

پایین برق و برد کوتاه تری است اما Wi-Fi برای استفاده در شبکه های بی سیم متوسط با برد و پهنای باند وسیع تری مطرح شده است .

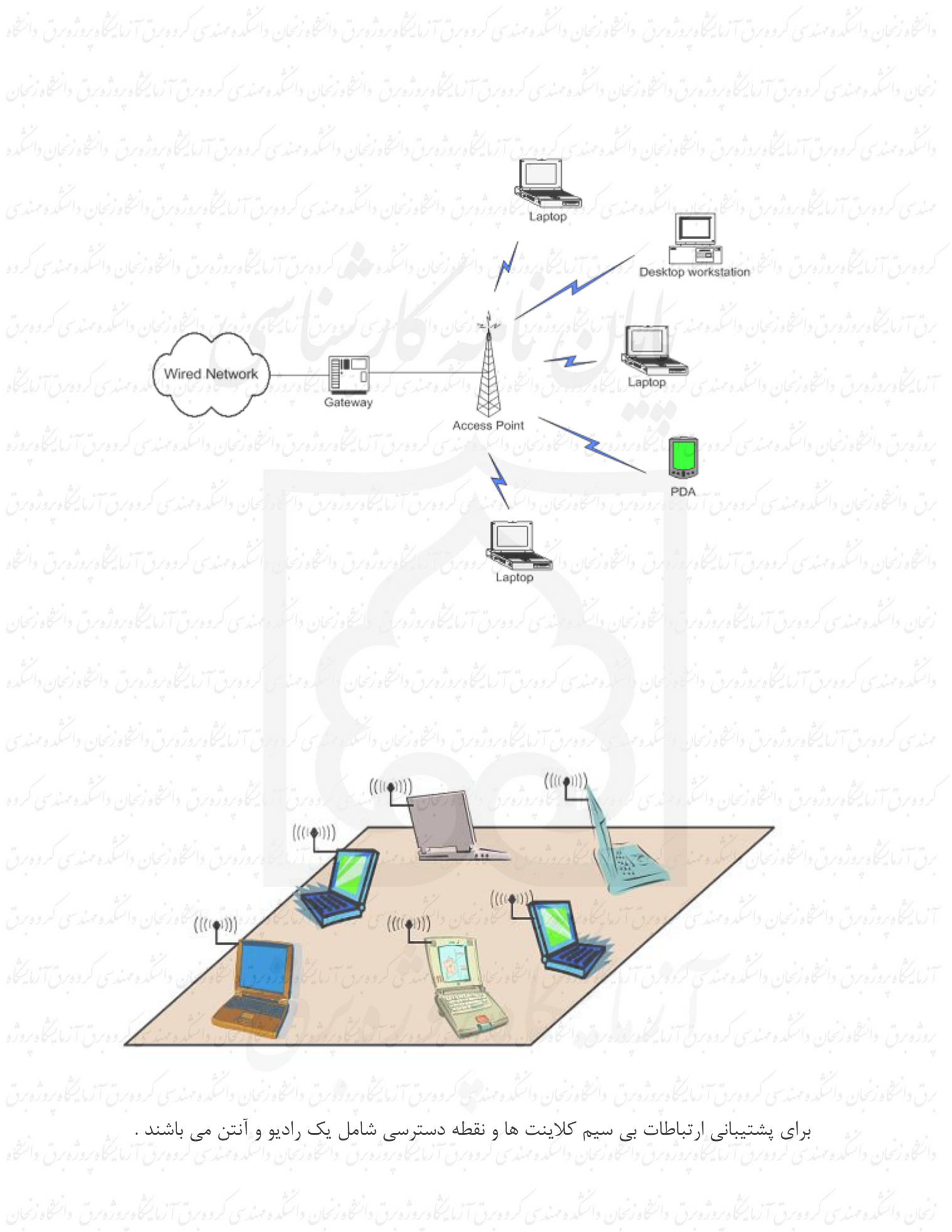
۱-۳ ترکیب سیستم Wi-Fi در رایانه

امروزه اغلب رایانه های لپتاب مجهز به سیستم Wi-Fi داخلی هستند و در غیر این صورت نیازمند نصب یک کارت Wi-Fi بر روی لپتاب و رایانه رومیزی خود خواهیم بود . شما می توانید یک کارت Wi-Fi در سیستم ۸۰۲٫۱۱a یا ۸۰۲٫۱۱b یا ۸۰۲٫۱۱n تهیه کنید که البته نوع ۸۰۲٫۱۱n نسبت به تجهیزات دارای استاندارد های دیگر از سرعت بالاتری برخوردار است. برای لپتاب ها این تجهیزات در قالب کارت های PCMCIA که در محل مخصوص خود نصب می شوند و یا به صورت اتصال خارجی از طریق درگاه USB عرضه می شوند . برای رایانه های رومیزی ، می توانید از کارت های PCI و یا درگاه USB برای این منظور استفاده کنید . پس نصب و با به کار گیری این تجهیزات کاربر قادر است تا در مکان هایی که سرویس Wi-Fi ارائه می شود با داشتن یک اشتراک ، از خدمات بهره گرفته و به شبکه متصل شود .

۱-۴ شبکه Wi-Fi چگونه کار می کند ؟

دو نوع مود عملیات برای برقراری ارتباطات در استاندارد تعریف شده وجود دارد ، حالت دارای زیر ساخت (Infrastructure - based) و حالت بدون زیر ساخت یا موردی (Ad hoc) . در حالت دارای زیر ساخت ، هیچکدام از نود های شرکت کننده در شبکه به عنوان نقطه دسترسی عمل نمی کند و سایر نود ها برای ارتباط با یکدیگر ، ابتدا باید با نقطه دسترسی ارتباط برقرار کنند . اما در حالت بدون زیر ساخت هیچگونه مرکز و نقطه دسترسی وجود ندارد و نود ها برای ارتباط با یکدیگر به طور مستقیم عمل می کنند و احتمالاً از نود های یکدیگر می توانند برای کمک در مسیریابی استفاده کنند .

نمونه ای از این شبکه ها :



برای پشتیبانی ارتباطات بی سیم کلاینت ها و نقطه دسترسی شامل یک رادیو و آنتن می باشند .

دانشجویان محترم:

جهت دسترسی به متن کامل پایان نامه‌ها به کتابخانه دانشکده مهندسی و یا آزمایشگاه پروژه گروه برق مراجعه فرمایید.

موارد همواره وجود دارد، استفاده از اینترنت شخصی که ممکن است برای کاربران هزینه داشته باشد، ایمن تر خواهد بود.

- در مواقعی که به اینترنت بی سیم نیاز ندارید، واسط شبکه بی سیم را غیرفعال نمایید. مادامی که واسط بی سیم دستگاه هایی مانند تلفن های همراه هوشمند و تبلت ها که قابل حمل هستند فعال باشد، این دستگاه ها در جستجوی شبکه های بی سیم ذخیره شده ی قبل، به طور مرتب فریم های probe را در محیط اطراف ارسال می کنند. این امر دستگاه بی سیم را در معرض اتصال خودکار به نقطه ی دسترسی مخرب با نام جستجو شده ی مشابه قرار می دهد.
- از ابزارهای اتصال امن جهت اتصال به نقاط دسترسی عمومی استفاده نمایید. به عنوان مثال، برنامه ای مانند IPASS مشتریان را از طریق یک صفحه ی ورود رمزنگاری شده به شبکه متصل می نماید که به این ترتیب تهدید حملات Phishing وب در بستر بی سیم را از بین خواهد برد.

۸-۱۲ نتیجه گیری

دستگاه های بی سیم مخرب و در رأس آن ها نقاط دسترسی ممکن است توسط عاملی داخلی (کارمندان سازمان) و یا خارجی (مهاجم) به طور غیرمجاز به کار گرفته شوند. در مورد اول، تهدیدی شکل می گیرد که خود شبکه ی سازمان را هدف قرار می دهد. به کارگیری نقطه ی دسترسی غیرمجاز توسط یک مهاجم با اهداف بدخواهانه، حمله ی مردی در میانه بی سیم را شکل می دهد که دستگاه های مشتریان را مورد هدف قرار می دهد. هر دو مورد از تهدیدات جدی و فعال در حوزه ی شبکه های محلی بی سیم تلقی می گردند.

مؤثرترین روش برای مقابله با تهدید نقاط دسترسی داخلی مخرب، استفاده از مکانیزم احراز هویت و کنترل دسترسی $802.1X/EAP$ در سمت کابلی شبکه است. همچنین، اگر $802.1X/EAP$ در سمت بی سیم شبکه به کار گرفته شود، حملات مردی در میانه و دزدیدن اتصال بی سیم را متوقف خواهد نمود. روش دیگر برای مقابله با این تهدیدات به کارگیری سیستم های تشخیص و جلوگیری از نفوذ بی سیم است. شناسایی نقاط دسترسی مخرب در حال حاضر از زمینه های پژوهشی فعال در حوزه ی شبکه های بی سیم 802.11 است.

منابع

[۱] "Wi-Fi Security How to Break and Exploit", Thesis for the degree Master of Science Hallvar Helleseth Department of Informatics University of Bergen

June ۲۰۰۶

[۲] "An Introduction to Wi-Fi®", Part Number ۰۱۹-۰۱۷۰ • ۰۹۰۴۰۹-B • Printed in U.S.A. Digi International Inc. © ۲۰۰۷-۲۰۰۸

[۳] IEEE ۸۰۲,۱۱ Working group website, <http://www.ieee۸۰۲.org/۱۱>

[۴] Introduction to IEEE ۸۰۲,۱۱ "intellgraphics",

<http://www.intellgraphics.com>

[۵] Steve Kapp, "۸۰۲,۱۱: Leaving the wire behind", IEEE internet computing, January-February ۲۰۰۲, pp. ۸۲-۸۵

[۶] Steve Kapp "۸۰۲,۱۱a: More bandwidth without the wire", IEEE internet computing, July-August ۲۰۰۲, pp. ۷۵-۷۹

[۷] Edgar Danielyan "IEEE ۸۰۲,۱۱", the internet Protocol Journal

, Vol. ۵, No. ۱, March ۲۰۰۲, pp. ۲-۱۳

[۸] "A condensed review of Spread Spectrum Techniques for ISM band System

", Intersil Application Note, AN۹۸۲۰, ۱, May ۲۰۰۰

[۹] "Wi-Fi Security" Stewart S. Miller, McGraw-Hill-New York Chicago San

Francisco Lisbon London Madrid Mexico City Milan New Delhi San Juan Seoul Singapore Sydney Toronto

[۱۱] "Overview of Wi-Fi Security What is left?", Philippe Teuwen, Security

Engineer and Contributor to Wi-Fi Alliance Easy Setup Task Group, N.V. Philips, October ۱۴ & ۱۵, Hack.lu ۲۰۰۵

- دانشگاه زنجان دانشکده مهندسی گروه برق آزمایشگاه پروژه برق دانشگاه زنجان دانشکده مهندسی گروه برق آزمایشگاه پروژه برق دانشگاه زنجان دانشکده مهندسی گروه برق آزمایشگاه پروژه برق دانشگاه زنجان دانشکده مهندسی گروه برق آزمایشگاه پروژه برق دانشگاه زنجان
- زنجان دانشکده مهندسی گروه برق آزمایشگاه پروژه برق دانشگاه زنجان دانشکده مهندسی گروه برق آزمایشگاه پروژه برق دانشگاه زنجان دانشکده مهندسی گروه برق آزمایشگاه پروژه برق دانشگاه زنجان دانشکده مهندسی گروه برق آزمایشگاه پروژه برق دانشگاه زنجان
- [۱۲] Andrew A. Vladimirov, Konstantin V. Gavrilenko, and Andrei A. Mikhailovsky. Wi- Foo: Addison Wesley, ۲۰۰۴
- [۱۳] Rob Flickenger. Wireless Hacks: O'Reilly, ۲۰۰۳
- [۱۴] Chris Hurley, Michael Puchol, et al. WarDriving: Drive, Detect, Defend: A Guide to Wireless Security: Syngress Publishing, ۲۰۰۴
- [۱۵] Wright, Joshua. "Layer ۲ Analysis of WLAN Discovery Applications for Intrusion Detection". ۱۳ Apr. ۲۰۰۵. < <http://home.jwu.edu/jwright/papers/۱۲-wlan-ids.pdf> >
- [۱۶] Brenner, Pablo. "A Technical Tutorial on IEEE ۸۰۲,۱۱ Protocol". ۱۳ Apr ۲۰۰۵. < http://www.sss-mag.com/pdf/۸۰۲_۱۱_tut.pdf >
- [۱۷] Loud Fat Blokes. ۸۰۲,۱۱ Home Page. ۱۳ Apr. ۲۰۰۵ < <http://www.loud-fatbloke.co.uk/w۸۰۲۱۱.html> >.
- [۱۸] Ossmann ,Michael. " WEP: Dead Again, Part ۲" Securityfocus. ۸ Mar. ۲۰۰۵, ۱۳ Apr. ۲۰۰۵ < <http://www.securityfocus.com/infocus/۱۸۲۴> >.
- [۱۹] Frankel Sh. And Eydt B. and Owens L. and Kent K., " Guide to IEEE ۸۰۲,۱۱i: Establishing Robust Security Networks," Computer Security Division Information technology Laboratory National Institute of Standards and Technology ,Gaithersburg, MD ۲۰۸۹۹-۸۹۳۰ June ۲۰۰۶
- [۲۰] Miller Stewart S. , " WiFi Security", Copyright ۲۰۰۳ by The McGraw-Hill Companies.
- [۲۱] C. He and J. C. Mitchell. "Security analysis and improvements for IEEE ۸۰۲,۱۱i." In Proceedings of the ۱۲th Annual Network and Distributed System Security Symposium (NDSS'۰۵), ۲۰۰۵.
- [۲۲] The Bell Labs Security Framework: "Making the Case for End-to-End Wi-Fi Security" , Wi-Fi Security v۱, ۰۹۰۶ , <http://www.lucent.com>., ۲۰۰۶, whitepaper.

دانشگاه زنجان دانشکده مهندسی گروه برق آزمایشگاه پروژه برق دانشگاه زنجان دانشکده مهندسی گروه برق آزمایشگاه پروژه برق دانشگاه زنجان دانشکده مهندسی گروه برق آزمایشگاه پروژه برق دانشگاه زنجان دانشکده مهندسی گروه برق آزمایشگاه پروژه برق دانشگاه زنجان دانشکده مهندسی گروه برق آزمایشگاه پروژه برق دانشگاه زنجان

[۲۳] Buttyán L. and Dóra L. "WiFi Security – WEP and ۸۰۲, ۱۱i," Technical Report, CrySyS Lab, Budapest University of Technology and Economics, May ۲۰۰۶.

[۲۴] Wireless LAN Security (۸۰۲, ۱۱) Wardriving & Warchalking. ۱۳ Apr. ۲۰۰۵ < <http://۸۰۲,۱۱-security.com/security/tools> >

[۲۵] AbsoluteValue Systems, Inc. "WLAN Adapter Chipset Directory". ۲ Feb. ۲۰۰۴, ۱۳ Apr ۲۰۰۵. <http://www.linuxwlan.org/docs/wlan_adapters.html. gz >

[۲۶] Kismet.HomePage. ۲ Apr. ۲۰۰۵, ۱۳ Apr. ۲۰۰۵. <<http://www.kismetwireless.net> >

[۲۷] Ethereal.HomePage. ۱۱ Mar. ۲۰۰۵, ۱۳ Apr. ۲۰۰۵. <<http://www.ethereal.com> >

[۲۸] David Coleman, CWSP (Certified Wireless Security Professional) Official Guide, Sybex Publishing , ۲۰۱۰.

[۲۹] <http://www.watchguard.com/infocenter/editorial/۲۷۰۶۱.asp>

[۳۰] Vivek Ramachandran, "BackTrack Wireless Penetration Testing Beginner's Guide: Chapter ۶ Attacking the Client", ۲۰۱۱

[۳۱] Vivek Ramachandran, Advanced WLAN attacks , ۲۰۱۱.