

ProjehCenter

w w w . P r o j e h C e n t e r . i r

Instagram | @projehcenter

Telegram | @projehcenter_ir



ش

۱

فهرست مطالب

صفحه

موضوع

۱.....	پیرامون شبکه های بی سیم
۲.....	مقدمه:
۳.....	بخش اول: شبکه های بی سیم، کاربردها، مزایا و ابعاد
۴.....	۱-۲ اساس شبکه های بی سیم
۵.....	۱-۲-۱ حکومت عالی Wi - Fi
۶.....	۱-۲-۲ ۸۰۲,۱۱۰ یک استاندارد نوپا
۷.....	۱-۲-۳ قطع کردن سیم ها Blue tooth
۱۰.....	۱-۲-۴ پشتیبانی خصوصی: Blue tooth
۱۱.....	۱-۲-۵ آچه پیش رو داریم
۱۲.....	۱-۳ منشا ضعف امنیتی در شبکه های بی سیم و خطرات معمولی
۱۴.....	بخش دوم: شبکه های محلی بی سیم
۱۴.....	۲-۱ پیشینه
۱۵.....	۲-۲ معماری شبکه های محلی بی سیم
۱۷.....	بخش سوم: عناصر فعال و سطح پوشش WLAN
۱۷.....	۳-۱ عناصر فعال شبکه های محلی بی سیم
۱۷.....	۳-۱-۱-۳ ایستگاه بی سیم
۱۸.....	۳-۱-۲ نقطه دسترسی

ب

۱۸.....	بر دو سطح پوشش.....	۳-۱-۳
۲۱.....	بخش چهارم: امنیت در شبکه های محلی براساس استاندارد ۸۰۲,۱۱	
۲۲.....	۴-۱- قابلیت ها و ابعاد امنیتی استاندارد ۸۰۲,۱۱	
۲۲.....	Authentication -۴-۱-۱	
۲۳.....	Confidentiality -۴-۱-۲	
۲۳.....	Integrity -۴-۱-۳	
۲۴.....	بخش پنجم: سرویس های امنیتی WEP- Authentication	
۲۴.....	Authentication -۵-۱	
۲۵.....	۵-۱-۱ Authentication بدون رمزگاری	
۲۶.....	۵-۱-۲ Authentication با رمزگاری RC4	
۲۸.....	بخش ششم: سرویس های امنیتی Integrity, ۸۰۲,۱۱b-privacy	
۲۸.....	privacy -۶-۱	
۲۹.....	۶-۲ Integrity	
۳۲.....	بخش هفتم: ضعف های اولیه امنیتی WEP	
۳۳.....	۷-۱ استفاده از کلیدهای ثابت WEP	
۳۳.....	۷-۲ Initialization vector	
۳۴.....	۷-۳ ضعف در الگوریتم	
۳۴.....	۷-۴ استفاده از CRC رمز نشده	
۳۶.....	بخش هشتم: خطرها، حملات و ملزمومات امنیتی	
۴۰.....	بخش نهم: پیاده سازی شبکه بی سیم	
۴۰.....	۹-۱ دست به کار شوید	
۴۱.....	۹-۲ دنده درست را انتخاب کنید	

۴۲.....	۹-۳- راه اندازی یک شبکه بی سیم
۴۳.....	۹-۴- دستورالعمل ها را بخوانید.....
۴۶.....	۹-۵- محافظت از شبکه
۴۹.....	بخش دهم: معرفی WAP
۴۹.....	۱۰-۱- WAP چیست؟
۵۱.....	۱۰-۲- ایده WAP
۵۲.....	۱۰-۳- معماری WAP
۵۳.....	۱۰-۴- مدل WAP
۵۴.....	۱۰-۵- انطباق با محدودیت های شبکه بی سیم
۵۴.....	۱۰-۶- WAP تا چه اندازه امن است؟
۵۶.....	منابع

پیرامون شبکه های بی سیم

مقدمه:

از آنجا که شبکه بی سیم، در دنیای کنونی هر چه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه ها، که بر اساس سیگنالهای رادیویی اند، مهمترین 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 مدد پیکره بندی صحیح می توان به سطح قابل قبولی از بعد امنیتی دست یافت، ضمن معرفی این شبکه ها با تاکید بر ابعاد امنیتی آن ها، به روش های پیکره بندی صحیح که احتمال رخداد حملات را کاهش می دهند می پردازیم.

بخش اول: شبکه های بی سیم، کاربردها، مزایا و ابعاد

تکنولوژی شبکه های بی سیم، با استفاده از انتقال داده ها توسط امواج رادیویی، در ساده ترین صورت، به تجهیزات سخت افزاری امکان می دهد تا بدون استفاده از بسترهای فیزیکی همچون سیم و کابل، یا یکدیگر ارتباط برقرار کنند. شبکه های بی سیم بازه وسیعی از کاربردها، از ساختارهای پیچیده ای چون شبکه های بی سیم سلولی - که اغلب برای تلفن های همراه استفاده می شد- و شبکه های محلی بی سیم (WLAN- wireless LAN) گرفته تا انواع ساده ای چون هدفون های بی سیم، مرا شامل می شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده می کنند، مانند صفحه کلیدها، ماوس ها و برخی از گوشی های همراه، در این دسته بندی جای می گیرند. طبیعی ترین مزیت استفاده از این شبکه ها عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل به این گونه شبکه ها و هم چنینی امکان ایجاد تغییر در ساختار مجازی آن ها است. از نظر ابعاد ساختاری، شبکه های بی سیم به سه دسته تقسیم می شوند: WPAN ، WLAN، WWAN .

مفهوم از WWAN که مخفف Wireless WAN است، شبکه ها ساختار بی سیم سلولی مورد استفاده در شبکه های تلفن همراه است. WLAN پوشش محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می کند. کاربرد شبکه های WPAN یا Blue tooth و مادون قرمز در این دسته قرار می گیرند.