امنیت در شبکه های بی سیم

مقدمه :

از آن‌جا که شبکه‌های بی سیم، در دنیای کنونی هرچه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه‌ها، که بر اساس سیگنال‌های رادیویی‌اند، مهم‌ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن‌ست. نظر به لزوم آگاهی از خطرات استفاده از این شبکه‌ها، با وجود امکانات نهفته در آن‌ها که به‌مدد پیکربندی صحیح می‌توان به‌سطح قابل قبولی از بعد امنیتی دست یافت، بنا داریم در این سری از مقالات با عنوان «امنیت در شبکه های بی سیم» ضمن معرفی این شبکه‌ها با تأکید بر ابعاد امنیتی آن‌ها، به روش‌های پیکربندی صحیح که احتمال رخ‌داد حملات را کاهش می‌دهند بپردازیم.

بخش اول

۱-۱ 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 .

مقصود از WWAN که مخفف Wireless WAN است، شبکه ها ساختار بی سیم سلولی مورد استفاده در شبکه های تلفن همراه است. WLAN پوششس 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 Wireless Personal Area Netuork برای موارد خانگی است. ارتباطاتی چون Blue tooth و مادون قرمز در این دسته قرار می گیرند.

شبکه های WPAN از سوی دیگر در دسته شبکه های Ad Hoc نیز قرار می گیرند. در شبکه های Ad Hoc یک سخت افزار، به محض ورود به فضای تحت پوشش آن، به صورت پویا به شبکه اضافه می شود. مثالی از این نوع شبکه Blue tooth است. در این نوع، تجهیزات مختلفی از جمله صفحه کلید، ماوس، چاپگر، کامپیوتر کیفی یا جیبی و حتی تلفن همراه، در صورت قرار گرفتن در محیط تحت پوشش، وارد شبکه شده و امکان رد و بدل داده ها با دیگر تجهیزات متصل به شبکه را می یابند. تفاوت مکان شبکه های Ad Hoc با شبکه های محلی بی سیم (WLAN) در ساختار مجاز آنها است. به عبارت دیگر، ساختار مجازی شبکه های محلی بی سیم بر پایه طرحی استیاست در حالی که شبکه های Ad Hoc از هر نظر پویا هستند. طبیعی است که در کنار مزایایی که این پویایی برای استفاده کنندگان فراهم می کند، حفظ امنیت چنین شبکه های نیز با مشکلات بسیاری همراه است. با این وجود، عملاً یکی از راه حل های موجود برای افزایش امنیت در این

شبکه ها، خصوصاً در انواعی همچون Blue tooth کاشتن از شعاع پوشش سیگنالهای شبکه است. در واقع مستقل از این حقیقت که عملکرد Blue tooth بر اساس فرستنده و گیرنده های کم توان استوار است و این مزیت در کامپیوتر های جیبی برتری قابل توجهی محسوب می گردد، همین کمی توان سخت افزار مربوطه، موجب کاهش محدود تحت پوشش است که در بررسی امنیتی نیز مزیت محسوب می گردد. به عبارت دیگر این مزیت به همراه استفاده از کدهای رمز نه چندان پیچیده، تنها ضربه های امنیتی این دسته از شبکه های به حساب می آیند.

۲-۱ اساس شبکه های بی سیم

در حال حاضر سه استاندارد در شبکه های Wireless با یکدیگر در حال رقابت هستند.

استاندارد Wi-Fi (802.11b) که بر مناسبی برای استفاده در مکان های اداری دارد.

استاندارد 802.11a که پهنای باند بیشتری داشته و مشکلات تداخل فرکانس رادیویی آن کمتر می باشد ولی برد کوتاهتری دارد.

استاندارد Blue tooth برای برد کوتاه مثل شبکه های موقت در اتاق های کنفرانس، مدرسه ها، یا خانه ها استفاده می شود.

۱-۲-۱ حکومت عالی Wi – Fi

Wi – Fi در حال حاضر محبوب ترین و ارزان ترین شبکه محلی بی سیم (Wireless LAN) را دارد.

Wi – Fi در طیف رادیویی 2.4GH2 عمل می کند و می تواند سرعت انتقال اطلاعات را تا 11ubps با دامنه ۳۰ متر بالا ببرد.

تعادلی که Wi – Fi بین اقتصاد، پهنای بلند، و مخصوصاً برد برقرار کرده، آن را به صورت استانداردی برجسته برای تجارت درآورده، و کارمندان بسیاری از این تکنولوژی برای کار و محاسبات شخصی استفاده می کنند. WECA[1] سهم خود را با تضمین صدها هزار محصول و اطمینان از کار و هماهنگی آنها با یکدیگر انجام داده، اما در Wi – Fi دو اشکال دارد.

اولاً از فضای هوایی، مشترکاً برای موبایل B;ue tooth امواج[2] رادیویی مهم و بقیه وسایل استفاده می کند. بنابراین، این تداخل امواج رادیویی، آ. را آسیب پذیر می کند.

---

[1]- Wireless Ethernet compatibitity Alliance

[2]- Security radios

ثانیاً به دلیل انتقال داده در هوا و وجود دیوار و دیگر موانع اجتناب ناپذیر، عملکرد واقعی به 5Mbps، یا تقریباً نصف سرعت مورد انتظار از آن می رسد.

۲-۲-۱ 802.11a یک استاندارد نوپا

802.11a دو مزیت بیشتر نسبت به Wi-Fi در فرکانس 5.35GH2 E5.15GH2 کار می کند که کمتر مورد استفاده است، در نتیجه تداخل امواج رادیویی در آن کمتر است. ثانیاً پهنای باند آن بسیار بالا است، و از نظر تئوری به 54cubp می رسد.

با وجود این که عملکرد واقعی آن نزدیک به 22Mbps است، همچنان فضای خالی برای انتقال صوت و تصویر دیجیتالی با کیفیت بالا و بقیه فایل های بزرگ، و همچنین به اشتراک گذاشتن اتصال Broad band در شبکه بیشتر از استاندارد Wi-Fi است و بعضی از تولید کننده ها، روشهای مخصوصی ارائه می دهند، که عملکرد آن را کمی بهتر می کند.

مشکل اصلی 802.11a از Wi-Fi در حال کاهش است، ولی در حال حاضر تجهیزات 802.11a بسیارگران تر از Wi-Fi است.

802.11a از Wi-Fi با یکدیگر سازگار نیستند، زیرا از دو تکنولوژی رادیویی متفاوت و دو قمست متفاوت از طیف رادیویی استفاده می کنند. به هر حال، تجهیزات استانداری برای هر دو تکنولوژی وجود دارد، که تبدیل آنها به یکدیگر را بسیار راحت کرده است. اگر می خواهید یکی از این دو استاندارد را انتخاب کنید، عوامل زیر را در نظر بگیرید:

اگر در حال حاضر از یکی از این استانداردها در کار خود استفاده می کنید، حتماً از همان استاندارد در منزل استفاده کنید، این کار ارتباط ر راحت تر می کند. اگر از لحاظ قیمت و سازگاری (تجهیزاتی که برای سازگاری با استانداردهای دیگر هستند)، مشکلی ندارید، 802.11a کارایی بهرتری دارد و می تواند ارزش پرداخت هزیهنه اضافی را داشته باشد. اما اگر می خواهید دامنه بیشتری را با قیمت کمتر، تحت پوشش قرار دهید، Wi-Fi انتخاب بهتری است.

۲-۲-۳ Blue tooth قطع کردن سیم ها

Blue tooth بطور اصولی یک فن آوری جایگزین کابل است. استاندارد فعلی Setup کردن کامپیوتر را در نظر بگیرید: یک صفحه کلید یک ماوس و مانیتور و احتمالاً یک چاپگر یا اسکنر به آن متصل هستند. اینها معمولاً به وسیله کابل به کامپیوتر متصل می شوند. یک تراشه Blue tooth برای جایگزین نمودن کابل ها بوسیله گرفتن اطلاعات حمل شده بصورت معمولی توسط یک کابل و انتقال آن در یک فرکانس خاص به

یک تراشه گیرنده Blue tooth در کامپیوتر، تلفن، چاپگر یا هر چیز دیگری طراحی شده است. Blue tooth که در ابتدا توسط Ericsson ایجاد شده، استانداردی برای تراشه های رادیویی ارزان قیمت و کوچکی است که درون کامپیوترها، تلفن ها، موبایل ها و چاپگر ها و ممیره قرار می گیرد.

این ایده اصلی بود، اما سریعاً آشکار شد که کارهای بیشتری امکان پذیر است. شما می توانید اطلاعات را بین هر دو دستگاهی انتقال دهید، کامپیوتر و چاپگر، صفحه کلید و تلفن و موبایل، و غیره. هزینه کم تراشه Blue tooth (حدود ۵ درصد) و مصرف نیروی برق پایین آن، به این معنی است که می توان آن را تقریباً در هر جایی قرار داد.

می توانید تراشه های Blue tooth را در کانتینر های باری برای تشخیص بار در هنگام حرکت بار در گمرک یا در انبار داشته باشید، یا یک هدست که با یک تلفن موبایل در جیب شما یا در اتاق دیگری مرتبط می گردد. یا یک e-mail که به دستگاه موبایل شما ارسال شده و به محض رسیدن شما به محدوده کامپیوتر اداره چاپ می شود.

در حال حاضر می توان از یک ماوس و صفحه ملید بی سیم استفاده کرد، می توان عقب نشست و صفحه کلید را روی پاهای خود قرار داد، بدون اینکه سیم صفحه کلید مانع از انجام این کار شود.

کابل ها در اداره ها و خانه ها دردسر زیادی را ایجاد می کنند. اکثر ما این تجربه را داشته ایم که سعی نموده ایم تا سردر بیاوریم کدام کابل به کجا می رود و در سیم های پیچیده شده در پشت میز کار خود سردر گم شده ایم. رفع این مشکل با استفاده از تکنولوژی Blue tooth انجام می گیرد. Bluetooth همچنین یک استاندارد جهانی را برای ارتباط بی سیم ارائه می دهد. و پس از سال ۲۰۰۲ یک ریز تراشه Blue tooth در هر دستگاه دیجیتالی ساخته شده قرار خواهد گرفت. روش کار چنین است که اگر دو دستگاه Blue tooth در فاصله ۱۰ متری از یکدیگر قرار بگیرند، می توانند با هم ارتباط برقرار کنند و چون Blue tooth از یک ارتباط رادیویی بهره می گیرد، تراشه نیازی به یک خط مرئی برای برقراری ارتباط ندارد.

تراشه رادیویی روی باند فرکانس 2.4GH2 قابلیت دسترسی جهانی دارد عمل می کند و سازگاری را در کل دنیا تضمین می کند فن آوری های Blue tooth، تمامی ارتباطات را بطور آنی برقرار می کنند و انتقال سریع و ایمن داده و صدا را ارائه می دهند.

در اینجا برخی کارهای ساده ای که می توانند بعنوان نتیجه استفاده از تکنولوژی Blue tooth برای ما فراهم شوند را می بینیم.

- یک شبکه شخصی که امکان اجتماع بدون درز منابع محاسباتی یا موبایل را در اتومبیل شما با بسترهای محاسباتی و ارتباطی دیگر در محل کار و خانه فراهم می نماید.
- سوئیچ خودکار ما بین تلفن و موبایل Hands - Free و دستگاه موبایل
- بروز رسانه های بی سیم از تمامی فهرست های انجام شدنی، فهرست های ارتباطی و غیره، به محض اینکه به محدوده کامپیوتر خود برسید.
- انجام عمل همزمان سازی با شرکت های محلی و ارائه دهندگان خدمات برای اطلاعات Push و تجارت الکترونیکی.
- دسترسی مطمئن به شبکه های داده خصوصی، از جمله سیستم های e- mail اداره شما.
- تشخیص Over- the - air در اتومبیل شما، برای سیستم مدیریت موتور و برنامه نویسی مجدد آن در صورت نیاز.

در آینده، احتمال می رود Blue tooth استاندارد دهها میلیون تلفن موبایل، PC، Laptop و دامنه وسیعی از دستگاه های الکترونیکی دیگر باشد. در نتیجه باید تقاضای زیادی برای برنامه های ابتکاری جدید، خدمات با ارزش افزوده، رهیافت های to-end و غیره وجود داشته باشد. احتمالات نامحدود هستند.

در ابتدا، Blue tooth شروع به جایگزینی کابل هایی خواهد نمود که دستگاه های دیجیتال متنوعی را به هم متصل می کنند و با افزایش تعداد ارتباطات، پتانسیل نیز افزایش می یابد. با پذیرش Blue tooth توسط تولید کنندگان بیشتری که آن را پشتیبانی می نمایند، توسعه دهندگان راه های جدیدی که پیشتر تصور آنها نمی رفت را برای به کارگیری نیروی آن خواهند یافت.

٤-٢-١ پشتیبانی خصوصی: Blue tooth

نام Blue tooth از نام یک پادشاه دانمارکی (به نام Harald Blaatand) که در قرن دهم زندگی می کرد، گرفته شده است. Blue tooth تا حدی متفاوت از دو استاندارد Wi-Fi و 802.11a می باشد. Blue tooth انعطاف پذیری بیشتری دارد ولی در مقیاس کوچکتر شبکه های[1] خانگی عمل می کند. عملکرد واقعی آن، فقط 300Kbps است و برد آن تقریباً ۱۰ متر است.

Wi-Fi و 802.11a برای برقراری ارتباط بین دستگاه ها به Adaptor، مسیریابها Gateway ، Routers ها، ایستگاه های Access Point و برنامه های راه اندازی هم زمان، نیاز دارند. اما برخلاف آنها، تمام دستگاه هایی که امواج رادیویی و آنتن های Blue tooth داشته باشند، با تدارکات کمی، می توانند با یکدیگر

[1]- Personal area network

ارتباط برقرار کنند. دستگاه هایی که با اشعه مادون قرمز کار می کنند، روشی برای انتقال فوری هستند. Blue tooth به وسیله جانشین کردن پورت های این دستگاه ها آنها را متعادل می کند و این کار را با برد بهتر و بدون نیاز به دید مستقیم (Line -of- sign) انجام می دهد. حضار در جلسات به وسیله Blue tooth هایی که به Blue tooth مجهز شده، می توانند فایل ها را از یک سر میز کنفرانس، به سر دیگر انتقال دهند، و یا فایلی را به پرینتری که به Blue tooth مجهز شده بفرستند، بدون نصب هیچ درایوی. کیوسک های مجهز به Blue tooth در فرودگاه ها و Coffee Houses به مشا اجازه می دهند تا از طریق کامپیوتر[1] کیفی یا کامپیوتر قابل حمل خود به اینترنت متصل شوید.

Blue tooth به زودی یک وسیله استاندارد بر روی بسیاری از موبایل ها و کامپیوتر های قابل حمل خواهد بود. حتی صحبت از برقرار دادن Blue tooth در وسایل خانگی می باشد.

اما با تمام منفعت که در تئوری برای Blue tooth وجود دارد، واقعیت این است که در حال حاضر، آشفتگی در سخت افزار و نرم افزار سازگار وجود دارد، به دلیل اینکه Blue tooth و Wi-Fi ، هر دو از یک رنج فرکانسی استفاده می کنند، در پهنای باند آنها تداخل صورت می گیرد و عملکرد را تا ۱۰٪، با بیشتر کاهش می دهد.

۱-۲-۵ آنچه پیش رو داریم

با ورود این استانداردها به بازار، طی چند سال آینده، الفبای Wireless پیچیده تر خواهد شد. برای مثال 802.11g پهنای باند Wi- Fi را تا 54Mbps افزایش خواهد داد (در عمل 22Mbps)، در همین حال 802.11I ، تعدادی از سوارخ های امنیتی را در پروتکل WEP خواهد بست Blue tooth جدید در فرکانس بالاتر عمل خواهد کرد، در نتیجه دو برابر پهنای باند فعلی اش بهره می دهد.

ساختما ن ها می توانند سیگنالهای Wireless شما را ببلعند، به همین دلیل اسکلت اداره یا منزلتان – مکان دیوارها، حالت تالار (راهرو)، و درها – همه چیز را به حساب آورد – اگر شما نقشه کف اتاقتان را نادیده بگیرید به شبکه ای که در هر گوشه و کناری قابل دسترسی است، خاتمه می دهید.

۱-۳ منشا ضعف امنیتی در شبکه های بی سیم و خطرات معمولی

خطر معمول در کلیه شبکه های بی سیم متصل از پروتکل و تکنولوژی مورد نظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار، مبتنی بر استفاده از سیگنال های رادیویی به جای سیم و کابل، استوار است. با استفاده از این سیگنالها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذ گران قادرند در

---

[1]- Laptop

صورت شکستن موانع امنیتی نه چندان قدرت مند این شبکه ها، خود را به عنوان عضوی از این شبکه ها جا زده و در صورت تحقق این امر امکان دست یابی به اطلاعات حیاتی، حمله به سرویس دهندگان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره های شبکه با یکدیگر، تولید داده ذهای غیر واقعی و گرمراه کننده، سوء استفاده از پهنای باند موثر شبکه و دیگر فعالیتهای مخرب وجود دارد.

در مجموع، در تمامی دسته های شبکه های بی سیم، از دید امنیتی حقایقی مشترک صادق است:

- تمامی ضعف های امنیتی موجود در شبکه های سیمسی در مورد شبکه های بی سیم نیز صدق می کند. در واقع نه تنها هیچ جنبه ای چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه های بی سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند. بلکه همان گونه که ذکر شد مخابرات ویژه ای را نیز موجب است.

- نفوذ گران، با گذر از تدابیر امنیتی موجود، می توانند به راحتی به منابع اطلاعاتی موجود بر روی سیستم های رایانه ای دست یابند.

- اطلاعات حیاتی که یا رمز نشده اند و یا با روشی با امسنیت پایین رمز شده اند، و میان دو گروه در شبکه های بی سیم در حال انتقال می باشند، می توانند توسط نفوذ گران سرقت شده یا تغییر یابند.

- حمله Dos ها به تجهیزات و سیستم های بی سیم بسیار متداول است.

- نفوذ گران با سرقت کدهای عبور و دیگر عناصر امنیتی مشابه کاربران مجاز در شبکه های بی سیم، می توانند به شبکه های مورد نظر بدون هیچ مانعی متصل گردند.

- با سرقت عناصر امنیتی، یک نفوذ کر می تواند رفتار یک کاربر را پایش کند. از این طریق می توان به اطلاعات حساس دیگری نیز دست یافت.

- کامپیوترهای قابل حمل و جیبی، که امکان و اجازه استفاده از شبکه بی سیم را دارند، به راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می توان اولین قدم برای نفوذ به شبکه را برداشت.

- یک نفوذگر می تواند از نقاط مشترک میان یک شبکه بی سیم در یک سازمان و شبکه های سیمی آن (که اغلب موارد شبکه اصلی و حساس تری محسوب می گردد) استفاده کرده و با نفوذ به شبکه بی سیم عملاً راهی برای دست یابی به منابع شبکه سیمی نیز بیابد.

- در سطحی دیگر، با نفوذ به عناصر کنترل کننده یک شبکه بی سیم، امکان ایجاد اختلال در عملکرد شبکه نیز وجود دارد.

بخش دوم

شبکه های محلی بی سیم

در این بخش به مرور کلی شبکه های محلی بی سیم می پردازیم. اطلاع از ساختار و روش عملکرد این شبکه ها، حتی به صورت جزئی، برای بررسی امنیتی لازم به نظر می رسد.

۱-۲ پیشینه

تکنولوژی و صنعت WLAN به اوایل دهه ۸۰ میلادی باز می گردد. مانند هر تکنولوژی دیگری، پیشرفت شبکه های محلی بی سیم به کندی صورت می پذیرفت. با ارائه استاندارد IEEE802.11b ، که پهنای باند نسبتاً بالایی را برای شبکه های محلی امکان پذیر می ساخت، استفاده از این تکنولوژی وسعت بیشتری یافت. در حال حاضر، مقصود از WLAN تمامی پروتکلها و استانداردهای خانواده IEEE 802.11 است.
جدول زیر اختصاصات این دسته از استانداردها را به صورت کلی نشان میدهد:

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), infrared (IR)
Frequency Band	2.4GHz (ISM band) and 5GHz
Data Rates	1Mbps, 2Mbps, 5.5Mbps, 11Mbps (11b), 54Mbps (11a), 54Mbps (11g)
Data and network security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management.
Operating Range	About 150 feet indoors and 1500 feet outdoors
Throughput	Up to 11Mbps (54Mbps planned)
Positive Aspects	Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

اولین شبکه محلی بی سیم تجاری توسط Motorola پیاده سازی شد. این شبکه، به عنوان یک نمونه از این شبکه ها، هزینه ای بالا و پهنای باندی پایین را تحمیل می کرد که ابداً مقرون به صرفه نبود. از همان زمان به بعد در اوایل دهه ۹۰ میلادی، پروژه استاندارد 802.11 در IEEE شروع شد. پس از نزدیک به ۹ سال کار، در سال ۱۹۹۹ استانداردهای 802.11a و۸۰۲.۱۱b توسط IEEE نهایی شده و تولید محصولات بسیاری بر پایه این استانداردها آغاز شد.

نوع a با استفاده از فرکانس حاصل 5GH2 ، پهنای باندی تا 54Mbps را فراهم می کند. در حالی که نوع b با ساتفاده از فرکانس حامل 2 04 GH2 تا 11Mbps پهنای باند را پشتیبانی می کند. با این وجود تعداد کانال های قابل استفاده در نوع b در مقایسه با نوع a بیشتر است. تعداد این کانال ها، باتوجه به کشور مورد نظر، تفاوت می کند. در حالت معمول مقصود از WLAn استاندارد 802.11b است. استاندارد دیگری نیز به تازگی توسط IEEE معرفی شده است که به 802 .11g شناخته می شود. این استاندارد بر اساس فرکانس حامل 204 GH2 عمل می کند ولی با استفاده از روشهای نوینی می تواند پهنای باند قابل استفاده را تا 54 Mbps بالا ببرد، تولید محصولات بر اساس این استاندارد، که مدت زیادی از نهائی شدن و معرفی آن نمی گذرد، بیش از یک سال است که آغاز شده و با توجه به سازگاری آن با استاندارد 802. 11b ، استفاده از آن در شبکه ها بی سیم آرام آرام در حال گسترش است.

۲-۲ معماری شبکه های محلی بی سیم

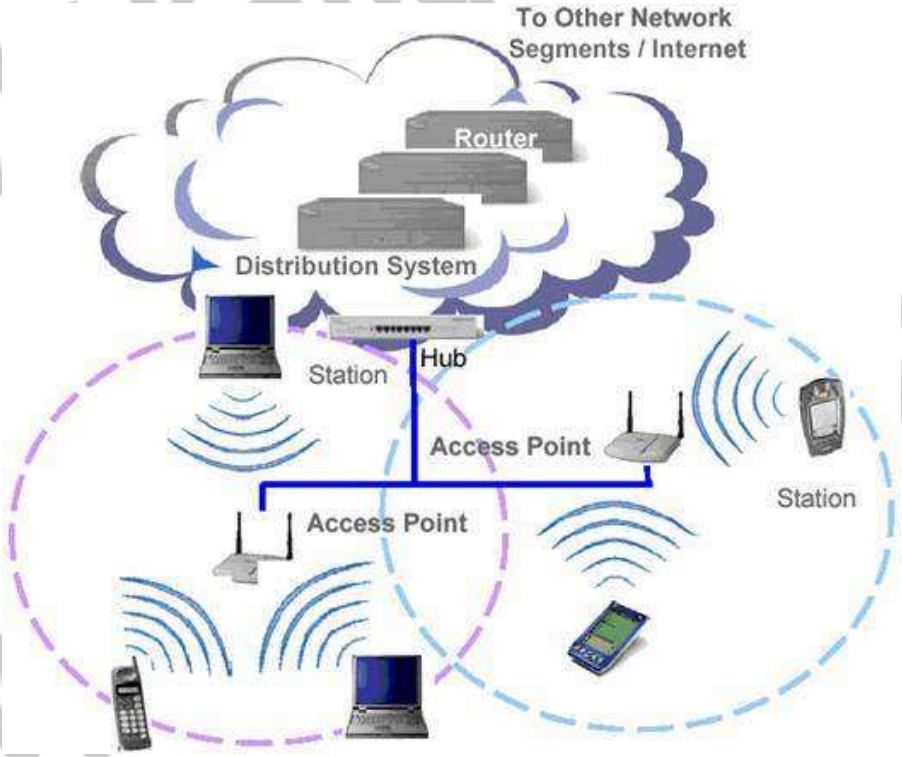
استاندارد 802 .11b به تجهیزات اجازه می دهد که به دو روش ارتباط در شبکه برقرار شود. این دو روش عبارت اند از برقراری ارتباط به صورت نقطه به نقطه - همان گونه در شبکه های Ad Hoc به کار می رود- و اتصال به شبکه از طریق نقاط تماس یا دسترسی[1] معماری معمول در شبکه های محلی بی سیم بر مبنای استفاده از AP است. با نصب یک AP عملاً مرزهای یک سلول مشخص می شود و با روشهایی می توان یک سخت افزار مجهز به امکان ارتباط بر اساس استاندارد 802.11b را میان سلولهای مختلف حرکت داد. گستره ای که یک AP پوشش می دهد را BSS[2] می نامند. مجموعه تمامی سلولهای یک ساختار کلی شبکه، که ترکیبی از BSS های شبکه است، را ESS[3] می نامند با استفاده از ESS می توان کستره وسیع تری را تحت پوشش شبکه محلی بی سیم درآورد.

1- AP=AccessPoint

2- Basic Sev\rvice Set

3- Extended Service Set

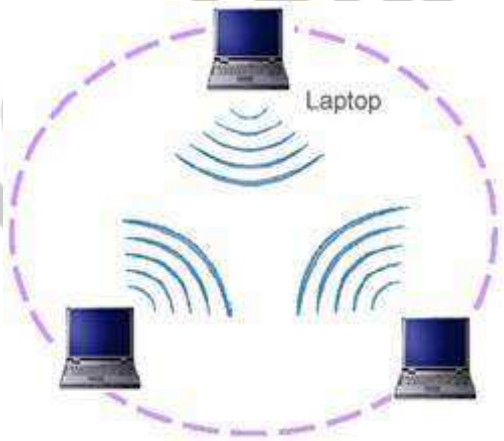
در سمت هر یک از سخت افزارها که معمولاً مخدوم هستند، کارت شبکه ای مجهز به یک مودم بی سیم قرار دارد که با AP ارتباط را برقرار می کند. AP علاوه بر ارتباط با چند کارت شبکه بی سیم، به بستر پر سرعت شبکه سیمی مجموعه نیز متصل است و از این طریق ارتباط میان مخدوم های مجهز به کارت شبکه بی سیم و شبکه اصلی برقرار می شود.



همانگونه که گفته شد. اغلب شبکه های محلی بی سیم بر اساس ساختار فوق، که به نوع Infrastructure نیز مرسوم است پیاده سازی می شوند. با این وجود نوع دیگری از شبکه های محلی بی سیم نیز وجود دارند که از همان منطق نقطه به نقطه استفاده می کنند. در این شبکه ها که عموماً Ad Hoc نامیده می شوند یک نقطه مرکزی برای دسترسی وجود ندارد و سخت افزار های همراه – مانند کامپیوترهای کیفی و جیبی یا گوشی های موبایل – با ورود به محدوده تحت پوشش این شبکه، به دیگر تجهیزات مشابه به

متصل می گردند. این شبکه ها به بستر شبکه سیمی متصل نیستند و به همین منظور IBSS[1] نیز خوانده می‌شوند.

شکل زیر شمایی ساده از یک شبکه Adhoc را نشان می دهد



شبکه های Ad Hoc از سویی مشابه شبکه های محلی درون دفتر کار هستند که در آنها نیازی به تعریف و پیکربندی یک سیستم رایانه ای به عنوان خادم وجود ندارد. در این صورت تمامی تجهیزات متصل به داین شبکه می توانند پرونده های مورد نظر خود را با دیگر گره ها به اشتراک بگذارند.

در بخش بعدی به دسته بندی اجزایی فعال یک شبکه محلی بی سیم پرداخته و شعاع پوشش این دسته از شبکه ها را مورد بررسی قرار خواهیم داد.

[1]- Independent Basic Service Set

بخش سوم

عناصر فعال و سطح پوشش WLAN

۳-۱ عناصر فعال شبکه های محلی بی سیم

در شبکه های محلی بی سیم معمولاً دو نوع عنصر فعال وجود دارد:

۳-۱-۳- ایستگاه بی سیم

ایستگاه نامحدود بی سیم به طور معمول یک کامپیوتر کیفی یا یک ایستگاه کاری ثابت است که توسط یک کارته شبکهٔ بی سیم به شبکهٔ محلی متصل می شود. این ایستگاه می تواند از سوی دیگر یک کامپیوتر جیبی یا حتی یک پوشش گر بار کد نیز باشد. در برخی از کاربردها برای این که استفاده از سیم در پایانه های رایانه ای برای طراح و مجری دردسرساز است، برای این پایانه اه که معمولاً در داخل کیوسک هایی به همین منظور تعبیه می شود، از امکان اتصال بی سیم به شبکهٔ محلی استفاده می کنند. در حال حاضر اکثر کامپیوترهای کیفی موجود در بازار به این امکان به صورت سرخود مجهز هستند و نیازی به اضافه کردن یک کارت شبکه بی سیم نیست.

کارت های شبکه بی سیم عموماً برای استفاده در چاک های PCMCIA است. در صورت نیاز به استفاده از این کارت ها برای کامپیوترهای رومیزی و شخصی ، با استفاده از رابطی این کارت ها را بروی چاک های گسترش PCI نصب می کنند.

۳-۱-۲- نقطهٔدسترسی

نقاط دسترسی در شبکه اهی بی سیم، همانگونه که در قسمت های پیش نیز در مورد آن صبحت شد، سخت افزارهای فعالی هستند که عملاً نقش سوئیچ در شبکه های بی سیم را بازی کرده، امکان اتصال به شبکه های بی سیم را نیز دارند. در عمل ساختار بستر اصلی شبکه عموماً سمی است و توسط این نقاط دسترسی مخدوم ها و ایستگاههای بی سیم به شبکهٔ سیمی اصلی متصل می گردد.

۳-۱-۳- برد و سطح پوشش

شعاع پوشش شبکهٔ بی سیم براساس استاندارد 802.11 به فاکتورهای بسیاری بستگی دارد که برخی از آنها به شرح زیر هستند:

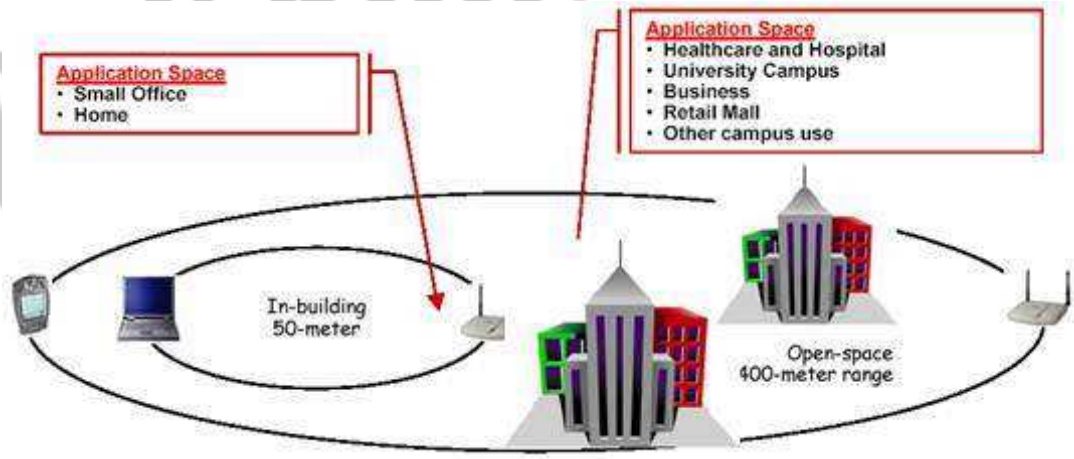
- پهنای باند مورد استفاده
- منابع امواج ارسالی و محل قرارگیری فرستنده ها و گیرنده ها

- مشخصات فضای قرارگرفتن و نصب تجهیزات شبکهٔ بی سیم
- قدرت امواج
- نوع و مدل آنتن

شعاع پوشش از نظر تئوری بین ۲۹ متر (برای فضاهای بسته داخلی) و ۴۸۵ متر (برای فضاهای باز) در استاندارد 802.11b متغیر است. با این وجود این مقادیر، مقادیری متوسط هستند و در حال حاضر با توجه به گیرنده ها و فرستنده های نسبتاً قدرتمندی که مورد استفاده قرار می گیرند، امکان استفاده از این پروتکل و گیرنده ها و فرستنده های آن، تا چند کیلومتر هم وجود دارد که نمونهای عملی آن فراوان اند.

با این وجود شعاع کلی که برای استفاده از این پروتکل (80.2.11b) ذکر می شود چیزی میان ۵۰ تا ۱۰۰ متر است. این شعاع عملکرد مقداری است که برای محل های بسته و ساختمان های چند طبقه نیز معتبر بوده و می‌تواند مورد استفاده قرار گیرد.

شکل زیر مقایسه ای میان بردهای نمونه در کاربردهای مختلف شبکه های بی سیم مبتنی بر پروتکل 802.11b را نشان می دهد

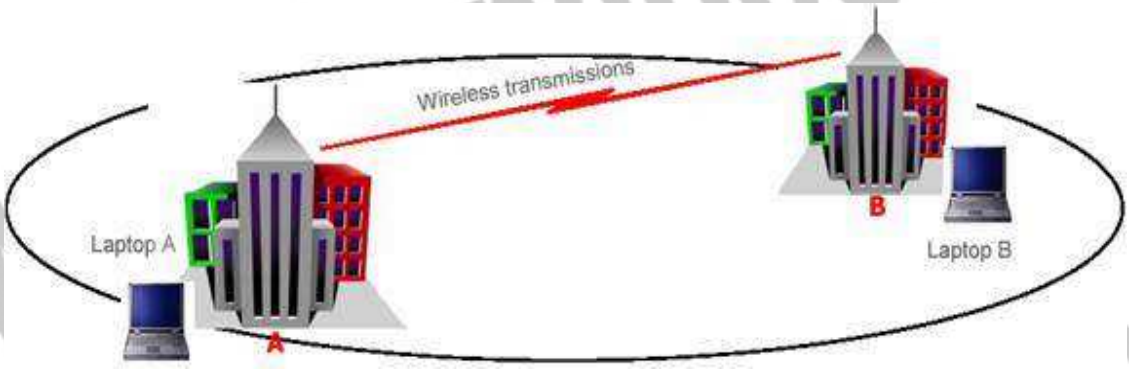


یکی از عمل کردهای نقاط دسترسی به عنوان سوئیچ های بی سیم، عمل اتصال میان حوزه های بی سیم است به عبارت دیگر با استفاده از چند سوئیچ بی سیم می توان عملکردی مشابه Bridge برای شبکه اهی بی سیم را بدست آورد.

اتصال میان نقاط دسترسی می تواند به صورت نقطه به نقطه ، برای ایجاد اتصال میان دو زیر شبکه به یکدیگر ،یا به صورت نقطه ای به چند نقطه یا بالعکس برای ایجاد اتصال میان زیرشبکه های مختلف به یکدیگر به صورت همزمان صورت گیرد.

نقاط دسترسی که به عنوان پل ارتباطی میان شبکه های محلی با یکدیگر استفاده می شوند از قدرت بالاتری برای ارسال داده استفاده می کنند و این به معنای شعاع پوشش بالاتر است. این سخت افزارها معمولاً برای ایجاد اتصال میان نقاط و ساختمان هایی به کار می روند که فاصلهٔ آنها از یکدیگر بین ۱ تا ۵ کیلومتر است. البته باید توجه داشت که این فاصله، فاصلهٔ متوسط براساس پروتکل 802.11b است. برای پروتکل های دیگری چون 802.11a می توان فواصل بیشتری را نیز بدست آورد.

شکل زیر نمونه‌یی از ارتباط نقطه به نقطه با استفاده از نقاط دسترسی مناسب را نشان می‌دهد :



از دیگر استفاده های نقاط دسترسی با برد بالا می توان به امکان توسعهٔ شعاع پوشش شبکه های بی سیم اشاره کرد. به عبارت دیگر برای بالا بردن سطح تحت پوشش یک شبکه بی سیم، می توان از چند نقطهٔ دسترسی بی سیم به صورت همزمان و پشت به پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا می توان با استفاده از

یک فرستندهٔدیگر در بالای هر یک از ساختمان ها، سطح پوشش شبکه را تا ساختمان های دیگر گسترش داد.

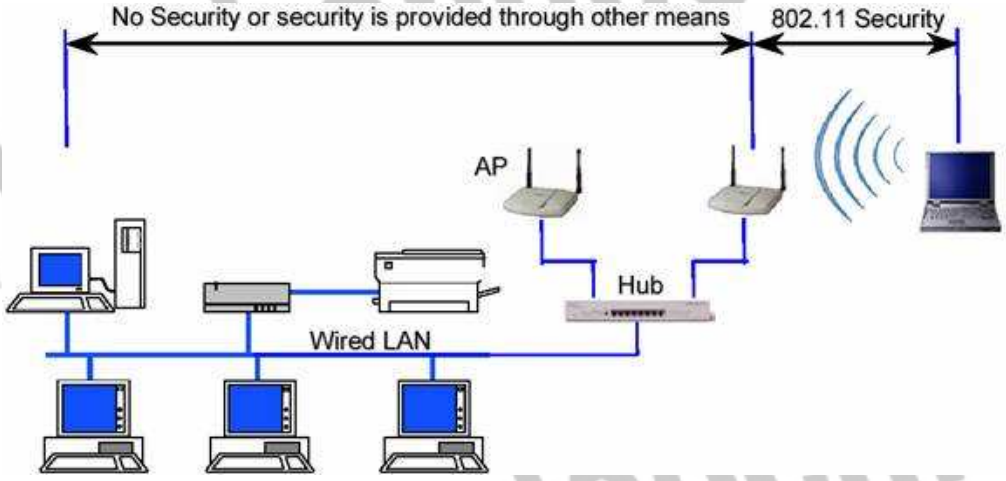
بخش بعد به مزایای معمول استفاده از شبکه های محلی بی سیم و ذکر مقدماتی در مورد روش های امن سازی این شبکه ها می پردازیم.

بخش چهارم

امنیت در شبکه های محلی براساس استاندارد 802.11

پس از آنکه در سه بخش قبل به مقدمه ای در مورد شبکه های بی سیم محلی و عناصر آن ها پرداختیم، از این بخش بررسی روش ها و استانداردهای امن سازی شبکه های محلی بی سیم مبتنی بر استاندارد IEEE.802.11 را آغاز می کنیم. با طرح قابلیت های امنیتی این استاندارد، می توان از محدودیت های آن آگاه شد و این استاندارد و کاربرد را برای موارد خاص و مناسب مورد استفاده قرار داد.

استاندارد 802.11 سرویس های مجزا و مشخصی را برای تأمین یک محیط امن بی سیم در اختیار قرار می دهد این سرویس ها اغلب توسط پروتکل[1] Wep تأمین می گردند و وظیفه آن ها امن سازی ارتباط میان مخدوم ها و نقاط دسترسی بی سیم است. درک لایه ای که این پروتکل به امن سازی آن می پردازد اهمیت ویژه ای دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه های دیگر، غیر از لایهٔ ارتباطی بی سیم که مبتنی بر استاندارد 802.11 است،کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکهٔ بی سیم به معنی استفاده از قابلیت درونی استاندارد شبکه های محلی بی سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.



[1]- wired Equivalent privacy

۱-٤- قابلیت ها و ابعاد امنیتی استاندارد 802.11

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه های بی سیم براساس استاندارد 802.11 فراهم می کند WEP است. این پروتکل با وجود قابلیت هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه های بی سیم را به نحوی، ولو سخت و پیچیده، فراهم می کند. نکته ای که باید به خاطر داشت این است که اغلب حملات موفق گرفته در مورد شبکه های محلی بی سیم، ریشه در پیکره بندی ناصحیح WEP در شبکه دارد.

به عبارت دیگر این پروتکل در صورت پیکره بندی صحیح درصد بالایی از حملات را ناکام می گذارد، هر چند که فی نفسه دچار نواقص و ایرادهایی نیز هست.

بسیاری از حملاتی که بر روی شبکه های بی سیم انجام می گیرد از سویی است که نقاط دسترسی با شبکه سیمی دارای اشتراک هستند. به عبارت دیگر نفوذگران بعضاً با استفاده از راههای ارتباطی دیگری که بر روی مخدوم ها و سخت افزارهای بی سیم، خصوصاً مخدوم های بی سیم وجود دارد ، به شبکه های بی سیم نفوذ می کنند که این مقوله نشان دهندهٔ اشتراکی هر چند جزئی میان امنیت در شبکه اهی سیمی و بی سیمی است که از نظر ساختاری فیزیکی با یکدیگر اشتراک دارند.

سه قابلیت و سرویس پایه توسط IEEE برای شبکه های محلی بی سیم تعریف می گردد:

Authentication -٤-١-١

هدف اصلی WEP ایجاد امکانی برای احراز هویت مخدوم بی سیم است. این عمل که در واقع کنترل دست رسی به شبکهٔ بی سیم است. این مکانیزم سعی دارد که امکان اتصال مخدوم هایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد.

Confidentiality -٤-١-٢

محرمانگی هدف دیگر WEP است. این بعد از سرویس ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکهٔ محلی بی سیم است.

Integrity -٤-١-٣

هدف سوم از سرویس ها و قابلیت های WEP طراحی سیاستی است که تضمین کند پیام ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان مخدوم های بی سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه های ارتباطاتی دیگر نیز کم و بیش وجود دارد.

نکته مهمی که در مورد سه سرویس WEP وجود دارد نبود سرویس های معمول , Authorization Auditing در میان سرویس های ارائه شده توسط این پروتکل است.

در بخش های بعدی از بررسی امنیت در شبکه های محلی بی سیم به بررسی هر یک از این سه سرویس می پردازیم.

بخش پنجم

سرویسهای امنیتی WEP- Authentication

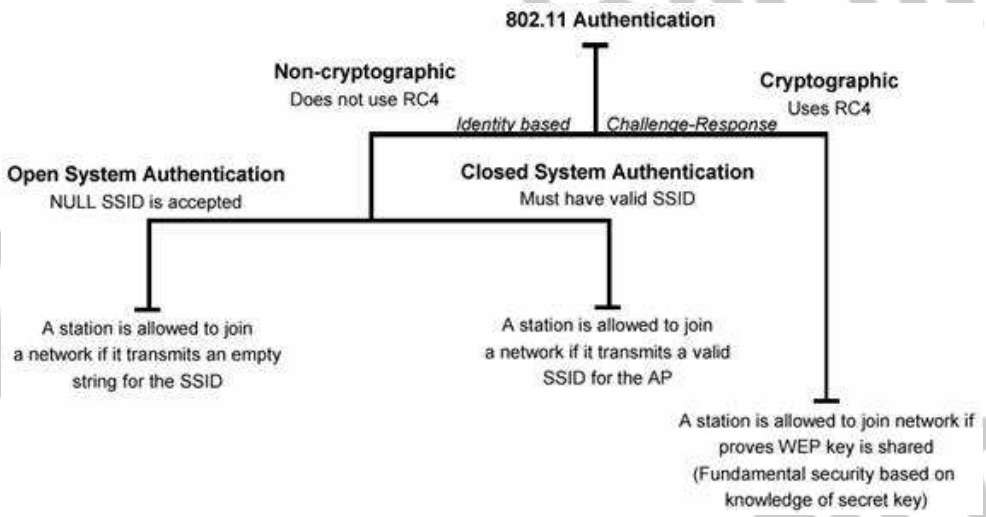
در بخش قبل به معرفی پروتکل WEP که عملاً تنها روش امن سازی ارتباطات در شبکه های بی سیم بر مبنای استاندارد 802.11 است پرداختیم و در ادامه سه سرویس اصلی این پروتکل را معرفی کردیم. در این بخش به معرفی سرویس های اول یعنی Authentication می پردازیم.

۵-۱- Authentication

استاندارد 802.11 دو روش برای احراز هویت کاربرانی که درخواست اتصال به شبکهٔ بی سیم را به نقاط دسترسی ارسال می کنند،دارد که یک روش بر مبنای رمزنگاری است و دیگری از رمزنگاری استفاده نمی کند.

شکل زیر شمایی از فرآیند Authentication را در این شبکه ها نشان می دهد

.



یک روش از رمزنگاری PC4 استفاده می کند و روش دیگر از هیچ تکنیک رمزنگاری استفاده نمی کند.

۵-۱-۱- Authentication بدون رمزنگاری

در روشی که مبتنی بر رمزنگاری نیست، دو روش برای تشخیص هویت مخدوم وجود دارد. در هر دو روش مخدوم متقاضی پیوستن به شبکه، درخواست ارسال هویت از سوی نقطهٔ دسترسی را با پیامی حاوی یک SSIP[1] پاسخ می دهد.

در روش اول که به Open system Authentication موسوم است،یک SSIP خالی نیز برای دریافت اجازهٔاتصال به شبکه کفایت می کند. در واقع در این روش تمامی مخدوم هایی که تقاضای پیوستن به شبکه را به نقاط دسترسی ارسال می کنند را با پاسخ مثبت روبرو می شوند و تنها آدرس آن ها توسط نقطهٔ دسترسی نگهداری می شود. به همین دلیل به این روش Null Authentication اطلاق می شود.

در روش دوم از این نوع، باز هم یک SSIP به نقطه دسترسی ارسال می گردد با این تفاوت که اجازهٔ اتصال به شبکه تنها در صورتی از سوی نقطهٔ دسترسی صادر می گردد که SSID ارسال شده جزء SSID های مجاز برای دسترسی به شبکه باشند. این روش به Closed system Authentication موسوم است.

نکته ای که در این میان اهمیت بسیاری دارد، توجه به سطح امنیتی است که این روش در اختیار ما می گذارد. این دو روش عملاً روش امنی از احراز هویت را ارائه نمی دهند و عملاً تنها راهی برای آگاهی نسبی و نه قطعی از هویت درخواست کننده هستند. با این وصف از آنجایی که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران کم تجربه و مبتدی،به شبکه هایی که براساس این روش ها عمل می کنند رخ می دهد، لذا این دو روش تنها در حالتی کاربرد دارند که یا شبکه ای در حال ایجاد است که حاوی اطلاعات حیاتی نیست، یا احتما رخداد حمله به آن بسیار کم است. هر چند که با توجه به پوشش نسبتاً گسترده یک شبکه بی سیم که مانند شبکه های سیمی امکان محدودسازی دسترسی به صورت فیزیکی بسیار دشوار است اطمینان از شانس پایین رخ دادن حملات نیز خود تضمینی ندارد!

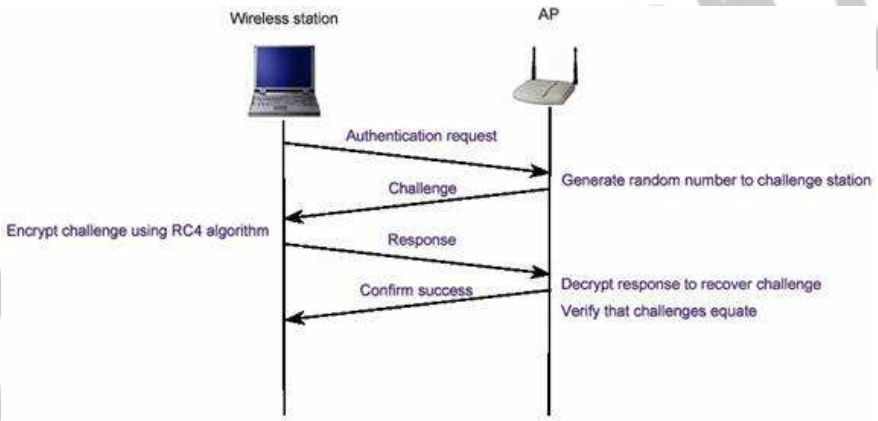
۲-۱-۵- Authentication با رمزنگاری RC4

این روش که به روش «کلید مشترک» نیز موسوم است،تکنیکی کلاسیک است که براساس آن پس از اطمینان از اینکه مخدوم از کلیدی سری آگاه است،هویتش تأیید می شود.

---

[1]- Serivce Set Identifier

شکل زیر این روش را نشان می دهد.



در این روش، نقطه دسترسی (AP) یک رشتهٔ تصادفی تولید کرده و آن را به مخدوم می فرستد. مخدوم این رشتهٔ تصادفی را با کلیدی از پیش تعیین شده (که کلید WEP نیز نامیده می شود) رمز می کند و حاصل را برای نقطهٔ دسترسی ارسال می کند. نقطهٔ دسترسی به روش معکوس پیام دریافتی را رمزگشایی کرده و با رشتهٔ ارسال مقایسه می کند. در صورت همسانی این دو پیام، نقطهٔ دسترسی از اینکه مخدوم کلید صحیحی را در اختیار دارد اطمینان حاصل می کند. روش رمزنگاری و رمزگشایی دراین تبادل روش RC4 است. در این میان با فرض اینکه رمزنگاری RC4 را روشی کاملاً مطمئن بدانی، دو خطر در کمین این روش است:

الف)در این روش تنها نقطهٔ دسترسی است که از هویت مخدوم اطمینان حاصل می کند. به بیان دیگر مخدوم هیچ دلیلی در اختیار ندارد که بداند نقطهٔدسترسی که با آن در حال تبادل داده های رمزی است نقطهٔ دسترسی اصلی است.

ب) تمامی روش هایی که مانند این روش بر پایهٔ سؤال و جواب بین دوطرف، با هدف احراز هویت یا تبادل اطلاعات حیاتی، قرار دارند یا جملاتی تحت عنوان man-in-the - middle در خطر هستند. در این دسته از حملات نفوذگری میان دو طرف قرار می گیرد و به گونه ای هر یک از دو طرف را گمراه می کند.

در بخش بعد به سرویس های دیگر پروتکل WEP می پردازیم.

بخش ششم

سرویس های امنیتی Integrity, 802.11b-privacy

در بخش قبل به سرویس اول از سرویس های امنیتی 802.11b پرداختیم. این بخش به بررسی دو سرویس دیگر اختصاص دارد. سرویس اول privacy (محرمانگی) و سرویس دوم Integrity است.

۶-۱- privacy

این سرویس که در حوزه های دیگر امنیتی اغلب به عنوان confidentiality از آن یاد می گردد، به معنای حفظ امنیت و محرمانه نگاه داشتن اطلاعات کاربر یا گره های در حال تبادل اطلاعات با یکدیگر است. برای رعایت محرمانگی عموماً از تکنیکهای رمزنگاری استفاده می گردد، به گونه ای که در صورت شنود اطلاعات در حال تبادل،این اطلاعات بدون داشتن کلیدهای رمز، قابل رمزگشایی نبوده و لذا برای شنودگر غیر قابل سوء استفاده است.

در استاندارد 802.11b ،از تکنیک های رمزنگاری WEP استفاده می گردد که بر پایهٔ RC4 است. RC4 یک الگوریتم رمزنگاری متقارن است که در آن یک رشتهٔ نیمه تصادفی تولیدمی گردد و توسط آن کل داده رمز می شود این رمزنگاری بر روی تمام بستهٔ اطلاعاتی پیاده می شود. به بیان دیگر داده های تمامی لایه های بالای اتصال بی سیم نیز توسط این روش رمز می گردند، از IP گرفته تا لایه های بالاتری مانند HTTP . از آنجایی که این روش عملاً اصلی ترین بخش از اعمال سیاست های امنیتی در شبکه های محلی بی سیم مبتنی بر استاندارد 802.11b است، معمولاً به کل پروسهٔ امن سازی اطلاعات دراین استاندارد به اختصار WEP گفته می شود.

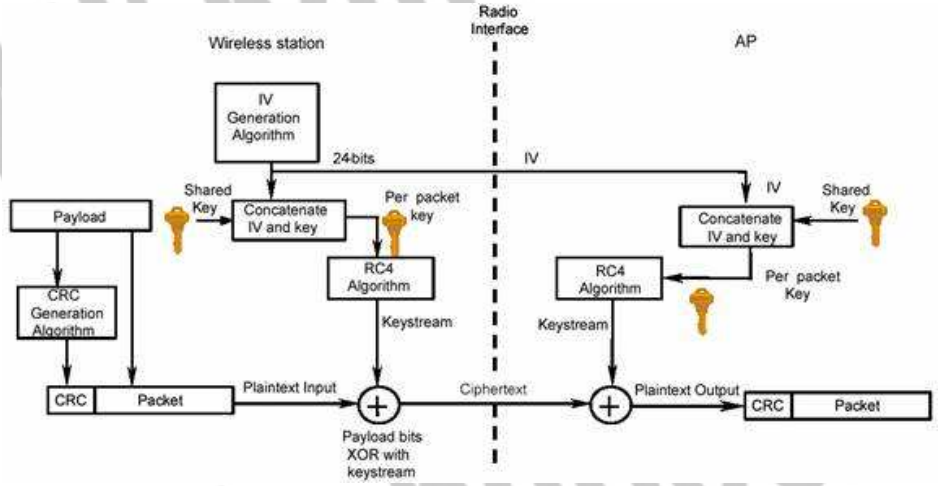
کلیدهای WEP اندازه هایی از ۴۰ بیت تا ۱۰۴ بیت می توانندداشته باشند. این کلیدها با بردار اولیهٔ[1] IV ۲۴ بیتی ترکیب شده و یک کلید ۱۲۸ بیتی RCL را تشکیل می دهند. طبیعتاً هر چه اندازهٔ کلیدبزرگتر باشد امنتی اطلاعات بالاتر است. تحقیقات نشان می دهد که استفاده از کلیدهایی با اندازهٔ ۸۰ بیت یا بالاتر عملاً استفاده از تکنیک brute - force را برای شکستن رمز غیرممکن می کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازهٔ ۸۰ بیت (که تعداد آن ها از مرتبهٔ ۲۴ است) به اندازه ای بالاست که قدرت پردازش سیستم های رایانه ای کنونی برای شکستن کلیدی مفروض در زمانی معقول کفایت نمی کند.

---

[1]- Initialization Vector

هر چند که در حال حاضر اکثر شبکه های محلی بی سیم از کلیدهای ۴۰ بیتی برای رمز کردن بسته های اطلاعاتی استفاده می کنند ولی نکته ای که اخیراً ، براساس یک سری آزمایشات بدست آمده است، این است که روش تأمین محرمانگی توسط WEP در مقابل حملات دیگری غیر از استفاده از روش brute - force ، نیز آسیب پذیر است و این آسیب پذیری ارتباطی به اندازهٔ کلید استفاده شده ندارد.

نمایی از روش استفاده شده توسط WEP برای تضمین محرمانگی در شکل زیر نمایش داده شده است.



Integrity -٦-٢

مقصود از Integrity صحت اطلاعات در حین تبادل است و سیاست های امنیتی که Integrity را تضمین می کنند روش هایی هستند که امکان تغییر اطلاعات در حین تبادل را به کمترین میزان تقلیل می دهند.

در استاندارد 802.11b نیز سرویس و روشی استفاده می شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان مخدوم های بی سیم و نقاط دست رسی کم می شود. روش مورد نظر استفاده از یک کد CRC است. یک CRC-32 قبل از رمز شدن بسته تولید می شود. در سمت گیرنده، پس از رمزگشایی ، CRC داده های رمزگشایی شده مجدداًمحاسبه شده و با CRC نوشته شده در بسته مقایسه می گردد که هر گونه اختلاف میان دو CRC به معنای تغییر محتویات بسته در حین تبادل است. متأسفانه این روش نیز مانند روش رمزنگاری

توسط RC4 ، مستقل از اندازهٔ کلید امنیتی مورد استفاده، در مقابل برخی از حملات شناخته شده آسیب پذیراست.

متأسفانه استاندارد 802.11b هیچ مکانیزمی 802.11b هیچ مکانیزمی برای مدیریت کلیدهای امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلیدها انجام می گیرد باید توسط کسانی که شبکهٔ بی سیم را نصب می کنند به صورت دستی پیاده سازی گردد. از آنجایی که این بخش از امنیت یکی از معضل های اساسی در مبحث رمزنگاری است،با این ضعف عملاً روش های متعددی برای حمله به شبکه های بی سیم قابل تصور است. این روش ها معمولاً بر سهل انگاری های انجام شده از سوی کاربران و مدیران شبکه مانند تغیر ندادن کلید به صورت مداوم، لو دادن کلید، استفاده از کلیدهای تکراری یا کلیدهای پیش فرض کارخانه و دیگر بی توجهی ها نتیجه ای جز درصد نسبتاً بالایی از حملات موفق به شبکه های بی سیم ندارد. این مشکل از شبکه های بزرگ تر بیشتر خود را نشان می دهد. حتی با فرض تلاش برای جلوگیری از رخ دادن چنین سهل انگاری هایی، زمانی که تعداد مخدوم های شبکه از حدی می گذرد عملاً کنترل کردن این تعداد بالا بسیار دشوار شده و گه گاه خطاهایی در گوشه و کنار این شبکهٔ نسبتاً بزرگ رخ می دهد که همان باعث رخنه در کل شبکه می شود.

در بخش بعد به مشکلات و ضعف هایی که سرویس های امنیتی در استاندارد 802.11b دارند می پردازیم.

بخش هفتم

ضعف های اولیه امنیتی WEP

در بخش های قبل به سرویس های امنیتی استاندارد 802.11 پرداختیم در ضمن ذکر هر یک از سرویس ها، سعی کردیم، به ضعف های هر یک اشاره ای داشته باشیم. در این بخش به بررسی ضعف های تکنیکهای امنیتی پایه ای استفاده شده در این استاندارد می پردازیم. همانگونه که گفته شد، عملاً پایهٔ امنیت در استاندارد 802.11 براساس پروتکل WEP استوار است. WEP در حالت استاندارد بر اساس کلیدهای ۴ بیتی برای رمزنگاری توسط الگوریتم RC4 استفاده می شود، هر چندکه برخی از تولیدکنندگان نگارش های خاصی از WEP را با کلیدهایی با تعداد بیت های بیشتر پیاده سازی کرده اند.

نکته ای که در این میان اهمیت دارد قائل شدن تمایز میان نسبت بالارفتن امنیت و اندازهٔکلیدهاست. با وجود آن که با بالا رفتن اندازهٔ کلید (تا ۱۰۴ بیت) امنیت بالا می رود،ولی از آنجا که این کلیدها توسط کاربران و براساس یک کلمهٔ عبور تعیین می شود، تضمینی نیست که این اندازه تماماً استفاده شود. از سوی دیگر همان طور که در قسمت های پیشین نیز ذکر شد، دستیابی به این کلیدها فرایند چندان سختی نیست، که در آن صورت دیگر اندازهٔ کلید اهمیتی ندارد.

متخصصان امنیت بررسی های بسیاری را برای تعیین حفره های امنیتی این استاندارد انجام داده اند که در این راستا خطراتی که ناشی از حملاتی متنوع، شامل حملات غیرفعال و فعال است، تحلیل شده است.

حاصل بررسی های انجام شده فهرستی از ضعف های اولیهٔاین پروتکل است:

۷-۱- استفاده از کلیدهای ثابت WEP

یکی از ابتدایی ترین ضعف ها که عموماً در بسیاری از شبکه های محلی بی سیم وجود دارد استفاده از کلیدهای مشابه توسط کاربران برای مدت زمان نسبتاً زیادی است. این ضعف به دلیل نبود یک مکانیزم مدیریت کلید رخ می دهد. برای مثال اگر یک کامپیوتر کیفی یا جیبی که از یک کلید خاص استفاده می کند به سرقت برود یا برای مدت زمانی در دسترس نفوذ گر باشد،کلید آن به راحتی لو رفته و با توجه به تشابه کلید میان بسیاری از ایستگاههای کاری عملاً استفاده از تمامی این ایستگاهها ناامن است.

از سوی دیگر با توجه به مشابه بودن کلید، در هر لحظه کانال های ارتباطی زیادی توسط یک حمله نفوذپذیر هستند.

Initialization vector -۷-۲

این بردار که یک فیلد ۲۴ بیتی است در بخش قبل معرفی شده است. این بردار به صورت متنی ساده فرستاده می شود. از آنجایی که کلیدی که برای رمزنگاری مورد استفاده قرار می گرد براساس IV تولید می شود، محدودهٔ IV عملاً نشان دهندهٔ احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است. به عبارت دیگر در صورتیکه IV کوتاه باشد در مدت زمان کمی می توان به کلیدهای مشابه دست یافت.

این ضعف در شبکه های شلوغ به مشکلی حاد تبدیل می شود. خصوصاً اگر از کارت شبکهٔ استفاه شده مطمئن نباشیم. بسیاری از کارت های شبکه از IV های ثابت استفاده می کنند و بسیاری از کارت های شبکه ای یک تولید کنندهٔ واحد IV های مشابه دارند. این خطر به همراه ترافیک بالا در یک شبکه شلوغ احتمال تکرار IV در مدت زمانی کوتاه را بالاتر می برد و در نتیجه کافی است نفوذ گر در مدت زمانی معین به ثبت داده های رمز شده شبکه بپردازد و IV های بسته های نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت.

۳-۷- ضعف در الگوریتم

از آنجایی که IV در تمامی بسته ها تکرار می شود و براساس آن کلید تولید می شود، نفوذگر می تواند با تحلیل و آنالیز تعداد نسبتاً زیادی از IV ها و بسته های رمز شده براساس کلید تولید شده بر مبنای آن IV، به کلید اصلی دست پیدا کند، این فرایند عملی زمان بر است و لی از آنجا که احتمال موفقیت در آن وجود دارد لذا به عنوان ضعفی برای این پروتکل محسوب می گردد.

٤-۷- استفاده از CRC رمز نشده

در پروتکل WEP ،کد CRC رمز نمی شود لذا بسته های تأییدی که از سوی نقاط دسترسی بی سیم به سوی گیرنده ارسال می شود براساس یک CRC رمز نشده ارسال می گردد و تنها در صورتی که نقطهٔدسترسی از صحت بسته اطمینان حاصل کند تأیید آن را می فرستد. این ضعف این امکان را فراهم می کند که نفوذگر برای رمزگشایی یک بستهٔ محتوایی آن را تغییر دهد و CRC را نیز به دلیل این که رمز نشده است،به راحتی عوض کند و منتظر عکس العمل نقطهٔ دسترسی بماند که آیا بتسهٔتأیید را صادر می کند یا خیر.

ضعف های بیان شده از مهمترین ضعف های شبکه های بی سیم مبتنی بر پروتکل WEP هستند نکته ای که در مورد ضعفهای فوق باید به آن اشاره کرد این است که در میان این ضعف ها تنها یکی از آن ها (مشکل

امنیتی سوم) به ضعف در الگوریتم رمزنگاری باز می گردد و لذا با تغییر الگوریتم تنها این ضعف است که بر طرف می گردد و بقیهٔمشکلات امنیتی کماکان به قوت خود باقی هستند.

جدول زیر ضعفهای امنیتی پروتکل WEP را به اختصار جمع بندی کرده است

.

	Security Issue / Vulnerability	Remarks
1.	**Security features in vendor products are frequently not enabled.**	Security features, albeit poor in some cases, are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.
2.	**IVs are short (or static).**	24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
3.	**Cryptographic keys are short.**	40-bit keys are inadequate for any system. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a comprise is possible from a brute-force attack.
4.	**Cryptographic keys are shared.**	Keys that are shared can compromise a system. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
5.	**Cryptographic keys cannot be updated automatically and frequently.**	Cryptographic keys should be changed often to prevent brute-force attacks.
6.	**RC4 has a weak key schedule and is inappropriately used in WEP.**	The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 keystream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries.
7.	**Packet integrity is poor.**	CRC32 and other linear block codes are inadequate for providing cryptographic integrity. Message modification is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of noncryptographic protocols often facilitates attacks against the cryptography.
8.	**No user authentication occurs.**	Only the device is authenticated. A device that is stolen can access the network.
9.	**Authentication is not enabled; only simple SSID identification occurs.**	Identity-based systems are highly vulnerable particularly in a wireless system.
10.	**Device authentication is simple shared-key challenge-response.**	One-way challenge-response authentication is subject to "man-in-the-middle" attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

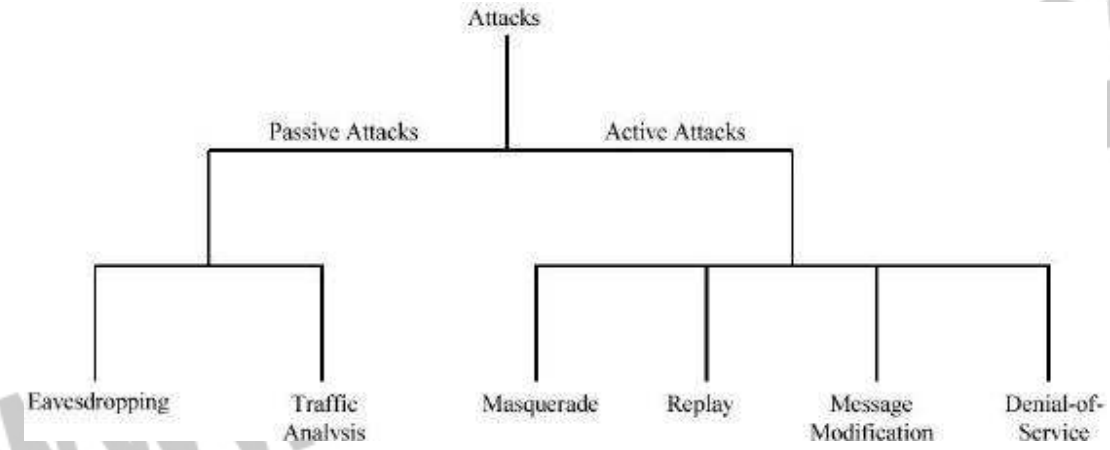
در بخشهای آتی به بررسی خطرهای ناشی از این ضعف ها و نیازهای امنیتی در شبکه های بی سیم می پردازیم.

بخش هشتم

خطرها، حملات و ملزومات امنیتی

همانگونه که گفته شد، با توجه به پیشرفت های اخیر، در ینده ای نه چندان دور باید منتظر گستردگی هر چه بیشتر استفاده از شبکه های بی سیم باشیم. این گستردگی، با توجه به مشکلاتی که از نظر امنیتی در این قبیل شبکه ها وجود دارد نگرانی هایی را نیز به همراه دارد این نگرانی ها که نشان دهندهٔ ریسک بالای استفاده از این بستر برای سازمان ها و شرکت های بزرگ است، توسعهٔ این استاندارد را در ابهام فرو برده است. در این قسمت به دسته بندی و تعریف حملات و خطرها و ریسک های موجود در استفاده از شبکه های محلی بی سیم براساس استاندارد IEEE 802.11x می پردازیم.

شکل زیر نمایی از دسته بندی حملات مورد نظر را نشان می دهد.



حملات امنیتی به دو دستهٔ فعال و غیر فعال تقسیم می گردند.

حملات غیرفعال

در این قبیل حملات،نفوذگر تنها به منبعی از اطلاعات به نحوی دست می یابد ولی اقدام به تغییر محتوای اطلاعات منبع نمی کند. این نوع حمله می تواند تنها به یکی از اشکال شنود ساده ای آنالیز ترافیک باشد.

شنود

در این نوع،نفوذگر تنها به پایش اطلاعات رد و بدل شده می پردازد. برای مثال شنود ترافیک روی یک شبکهٔ محلی یا یک شبکهٔ بی سیم (که مد نظر ما است) نمونه هایی از این نوع حمله به شمار می آیند.

آنالیز ترافیک

در این نوع حمله، نفوذگر با کپی برداشتن از اطلاعات پایش شده، به تحلیل جمعی داده ها می پردازد. به عبارت دیگر بسته یا بسته های اطلاعاتی به همراه یکدیگر اطلاعات معناداری را ایجاد می کنند.

حملات فعال

در این نوع حملات، بر خلاف حملات غیرفعال، نفوذگر اطلاعات مورد نظر را، که از منابع به دست می آید، تغییر می دهد که تبعاً انجام این تغییرات مجاز نیست. از آنجایی که در این نوع حملات اطلاعات تغییر می کنند، شناسایی رخ داد حملات فرآیندی امکان پذیر است. این حملات به چهار دستهٔ مرسوم تقسیم بندی می گردند:

- تغییر هویت

در این نوع حمله، نفوذگر هویت اصلی را جعل می کند،این روش شامل تغییر هویت اصلی یکی از طرف های ارتباط یا قلب هویت و یا تغییر جریان واقعی فرآیند پردازش اطلاعات نیز می گردد.

- پاسخ های جعلی

نفوذ گر در این قسم حملات،بسته هایی که طرف گیرنده اطلاعات در یک ارتباط دریافت می کند را پایش می کند، البته برای اطلاع از کل ماهیت ارتباط یک اتصال از ابتدا پایش می گردد ولی اطلاعات مفید تنها اطلاعاتی هستند که از سوی گیرنده برای فرستنده ارسال می گردند. این نوع حمله بیشتر در مواردی کاربرد دارد که فرستنده اقدام به تعیین هویت گیرنده می کند. در این حالت بسته های پاسخی که برای فرستنده به عنوان جواب به سؤالات فرستنده ارسال ی گردند به معنای پرچمی برای شناسایی گیرنده محسوب می گردند. لذا در صورتی که نفوذگر این بسته ها را ذخیره کند و در زمانی که یا گیرنده فعال نیست،یا فعالیتهای ارتباط آن به صورت آگاهانه - به روشی - توسط نفوذ گر قطع شده است، می تواند مورد سوء استفاده قرار گیرد. نفوذ گر با ارسال مجدد این بسته ها خود را به جای گیرنده جا زده و از سطح دسترسی مورد نظر برخوردار می گردد.

- تغییر پیام

در برخی موارد مرسوم ترین و متنوع ترین نوع حملات فعال تغییر پیام است. از آن جایی که گونه های متنوعی از ترافیک بر روی شبکه رفت و آمد می کنند و هر یک از این ترافیک ها و پروتکل ها از شیوه ای برای مدیریت جنبه های امنیتی خود استفاده می کنند، لذا نفوذگر با اطلاع از پروتکل های مختلف می تواند برای هر یک از این انواع ترافیک نوع خاصی از تغییر پیام ها و در نتیجه حملات را اتخاذ کند. با توجه به گستردگی این نوع حمله، که کاملاً به نوع پروتکل بستگی دارد، در اینجا نمی توانیم به انواع مختلف آن بپردازیم،تنها به یادآوری این نکته بسنده می کنیم که این حملات تنها دست یابی به اطلاعات را هدف نگرفته است و می تواند با اعمال تغییرات خاصی به گمراهی دو طرف منجر شده و مشکلاتی را برای سطح مورد نظر دست رسی که می تواند یک کاربر عادی باشد فراهم کند.

- حمله های Denial - of - service (Dos)

این نوع حمله، در حالات معمول، مرسوم ترین حملات را شامل می شود. در این نوع حمله نفوذگر یا حمله کننده برای تغییر نحوهٔ کارکرد یا مدیریت یک سامانهٔ ارتباطی یا اطلاعاتی اقدام می کند. ساده ترین نمونه سعی در از کار انداختن خادم های نرم افزاری و سخت افزاری است. پیرو چنین حملاتی،نفوذ گر پس از کار انداختن یک سامانه، که معمولاً سامانه ایست که مشکلاتی برای نفوذگر برای دسترسی به اطلاعات فراهم کرده است، اقدام به سرقت تغییر یا نفوذ به منبع اطلاعاتی می کند. در برخی از حالات،در پی حملهٔ انجام شده، سرویس مورد نظر به طور کامل قطع نمی گردد و تنها کارآیی آن مختل می گردد. در این حالت نفوذگر می تواند با سوء استفاده از اختلال ایجاد شده به نفوذ از طریق / به همان سرویس نیز اقدام کند.

تمامی ریسکهایی که در شبکه های محلی ، خصوصاً انواع بی سیم،وجود دارد ناشی از یکی از خطرات فوق است.

بخش نهم

پیاده سازی شبکه بی سیم

۹-۱- دست به کار شوید[1]

اول، اندازه محلتان را برآورد کنید، می دانیم که wi-fi مهمترین کارآیی را در مکان های بزرگ دارد، و 802.11a برای کارهایی با عملکرد بالاست،در حالیکه Bluetooth وسیله هایی برای کار در فواصل کم نیاز دارد. شما می توانید فقط از یک ایستگاه Access point واقع در مرکز برای wi-fi استفاده کنید، تا فضای کاری 20000-square-foot را پوشش دهد. این ایستگاه Access Point می تواند یک خانه یک طبقه یا دو طبقه را با محوطه اطراف آن پوشش دهد. یک ایستگاه access pointo برای 802.11a می تواند یک خانه متوسط یا آپارتمان را تحت پوشش قرار دهد. به خاطر داشته باشید که برد شبکه wireless هم به صورت عمودی و هم به صورت افقی – بستگی به ترکیب (بنای) ساختمان دارد – ممکن است توانایی پوشش طبقات زیادی در بالا یا پایین access point یا را داشته باشد. هنوز هم به دلیل وجود موانع متعدد فیزیکی و تکنیکی ممکن است مجبور شوید ابزارهای شبکه را به طور یدکی در محلی قرار دهید تا در مواقع بروز مشکل، از آنها برای جبران خسارت استفاده کنید.

هر دیوار و سقفی ، یک مانع بالقوه، برای هر نوع موج رادیویی است. دیوارهای گچی راحت تر امواج رادیویی را از خود عبور می دهند گر چه بناهای قدیمی (که شامل چوب، کاهگل، دیوارهای فلزی و گچی هستن) ،می توانند سیگنالها را جذب کنند (از بین ببرند) . فولاد و سنگ بدترین مواد دیوار هستند (سیگنال ها بسیار به زحمت از داخل آنها عبور می کنند)،در حالیکه شیشه ماند یک منعکس کننده رفتار می کند،و سیگنال را بر می گرداند، تنها راه حل این است که access point ها را در جایی که دیوار یا نقطه کوری نیست قرار دهید.

۹-۲- دنده درست را انتخاب کنید.

در اکثر محیطها، سه نوع مختلف از تجهیزات را نیاز خواهید داشت، مقایسه پهلو به پهلوی ما را برای این دستهٔ انواع مختلف بررسی کنید. هر وسیله ای که بخواهد به صورت wireles ارتباط برقرار کند، احتیاج به امواج رادیویی دارد. اگر notebook شما قدیمی است، با اضافه کردن wireless pc and card adapter به راحتی می توانید به شبکه wireles متصل شوید،در حالیکه notebook های جدید مثل Dell Inspirson 8200 لوازم

---

[1]- Break out the blueprints

مورد نیاز را به صورت استاندارد در خود دارند. امواج رادیویی یکپارچه 802.11a به تازگی در اختیار note book ها قرار گرفته compact flash card های کوچکمتر مانند D-LinkDCF-G50w کارآیی خوبی برای کامپیوترهای قابل حمل دارند، اما گران هستند و برد محدودی دارند. برای کامپیوترهای رومیزی USB ، desk Tops یا PCI مناسب است. WECA سازگاری wi-fi را تضمین کرد. اما این سازمان به تازگی اقدام به تست ابزارهای 802.11a کرده است.

زمانی که تمام وسایل شما برای برقراری ارتباط wireless آماده شد، به یک ایستگاه access pointo نیاز دارید. Ap مانند یک Hub در شبکه wireles عمل می کند. کامپیوترها از طریق Ap می توانند ارتباط طیف باز[1] برقرار کنند. در شبکه های سیمی[2] ، از Ap برای اضافه کردن وسایل wireles استفاده می شود. با اضافه کردن Ap های بیشتر می توانید شبکه تان را به مکانی بزرگتر گسترش دهید. Ap ها در الگویی که همدیگر را پوشش دهند قرار دهید تا نقاط کور را به حداقل برسانید. با اضافه کردن Ap ها به شکل سیمی می توانیم از آنها به عنوان bridge استفاده کنیم، که این Ap ها سیگنال ها را برای Ap هی دیگر تقویت می کنند.

۳-۹- راه اندازی یک شبکه بی سیم

بعد از انتخاب استانداردهای مورد نظر، چندوسیله دیگر نیاز خواهید داشت. این وسایل شامل نوار اندازه گیری [3] و چند کابل شبکه از نوع cat-5 می باشند. راه اندازی شبکه محلی wireles ، از آغاز تا پایان، کمتر از از یک ساعت وقت می گیرد.

ابتدا، یک بازدید کلی از محل اداره یا منزلتان داشته باشید. برای یافتن بهترین مکان برای Ap خود، از اطراف منطقه ای که می خواهید شبکه را برقرار کنید، بازدیدی داشته باشید تعدادی موارد عمومی برای انتخاب مکان خوب عبارتند از:

- ماکزیمم فاصله ای که می خواهید از Ap استفاده کنید، باید داخل برد Ap باقی بماند.
- برای از بین بردن تداخل امواج، از مناطقی که دیوارهای ضخیم دارند، اجتناب کنید.
- برای اینکه کابل کشی را به حداقل برسانید،باید Ap را نزدیک اتصال broad band خود قرار دهید.
- مطمئن شوید که Ap را در محل نزدیکی به خروجی جریان برق قرار می دهید.
- برای حفظ زیبایی و امنیت، Ap را در محلی به دور از شلوغی و تردد مخفی کنید.

---

[1]- Broad band

[2]- wired

[3]- tape measure

- سطوحی صاف و دور از رفت و آمد، مانند قفسه های کتاب، (مراکز استخدام ؟!) و قسمت های فوقانی وسایلی مانند بالای یک یخچال می توانند مکانهایی مناسب برای نگهداری Ap باشند. راه دیگری برای نگهداری از Ap, kit سوار شونده ایست که توسط بسیاری از تولید کنندگان به فروش می رسد که توسط آن Ap به دیوار متصل می شود.
- Ap را در بلندی قرار دهید که موانع کاهش یابند و یا آن را پایین (در زیر وسیله ای) قرار دهید تا کابل ها و سیم های برق از دید مخفی بمانند.

٤-٩- دستورالعمل ها را بخوانید.

برای ساختن شبکه محلی wireless خود،ابتدا Ap را در مکان خود مستقر کنید . در هر کامپیوتری از نوع desktop یا notbook که تصمیم دارید توسط آن به شبکه متصل شوید، ابتدا Wireless adapter را نصب و راه اندازی کنید. توصیه جدی در این زمینه آن است که قبل از شروع دستورالعمل ها را به دقت بخوانید زیرا نرم افزار و سخت افزار عرضه شده توسط فروشندگان، مختلف و متفاوت می باشند. زمانی که adapter نصب و راه اندازی شد، قسمت کاربر را باز کنید و سپس به SSID یا نام شبکهٔ خود وارد شوید.

با توجه به تولید کننده ، ممکن است برای شناساندن کاربر، مجبور به استفاده از نرم افزار شبکه wireless در ویندوز شوید. کاربرانی که ویندوز XP دارند از این مسیر استفاده کنند.

start/setting/network connections/ wireless network connection

و در آنجا روی کلید Advanced ، کلیک کنید و وارد قسمت مشخصات شبکهٔخود شوید چنانچه شما همین نصب ها را برای سایر وسایل شبکه بخواهید، ضبط و نگهداری این نصب های انجام شده مفید است.

برای اینکه نصب و راه اندازی شبکهٔ wireless برای شما راحت تر باشد، بگذارید تا DHCP به طور خودکار،آدرس IP را به کامپیوترهای شبکه شما اختصاص دهد و اجازه دهید سیستم امنیت WEP خاموش بماند. متأسفانه بعضی از تولیدکنندگان شما را مجبور می کنند قبل از آنکه بتوانید به AP دسترسی پیدا کنید، از آدرس IP معینی استفاده کنید. برای راهنمایی و کمک بیشتر می توانید دستورالعمل ها را مجدداً بررسی کنید.

وقت آن رسیده که AP را مشخص کنید. با استفاده از کابل cat-5 ،کابل یا مودم DSL خود را به Ap وصل کنید. اگر Ap شما بدون کابل نصب شده است، به راحتی می توانید از مغازه های الکترونیکی و یا

کامپیوتری، کابلی تهیه کنید. برای هماهنگی کاربران [1] وارد جزئیات شبکه Ap شوید و سپس AP را reboot کنید.

حالا چند لحظه صبر کنید تا از به کار افتادن شبکه مطمئن شوید. راحت ترین راه برای حصول این اطمینان این است که آدرس مطمئنی را در صفحه نمایش وب بنویسید و ببینید که آیا به اینترین وصل می شوید یا خیر. اگر اخطار صفحه قابل دسترسی نیست را دریافت کردید، دوباره سعی کنید. هنوز مشکل حل نشده؟ در اینجا فهرستی از راه حل های سریع را ارائه می دهیم:

- مطمئن شوید همه نصب های بین کاربر و access poitn هماهنگ هستند. که این نصب ها شامل SSID, DHCP و encryption می باشند.
- حالت چراغ روی Ap را چک کنید و در رابطه با خطرهای احتمالی به دستورالعمل های سیستم مراجعه کنید.
- مطمئن شوید که آنتن های Ap را درست نصب و راه اندازی کرده اید، و همه اتصالات کابل ها محکم هستند.
- قدرت سیگنال را روی کاربر چک کنید تا مطمئن شوید که در برد Ap قرار دارید.
- نمایشگر وب خود را خالی کرده و AP یا مسیریاب [2] را مجدداً راه اندازی نمایید[3].
- به دنبال تداخل احتمالی با دیگر وسایل مانند security radios و یا اتصالات Bluetooth بگردید.
- Ap را reboot کنید تا آن را به نصب های پیش فرضش برگردانید،و سپس دوباره شروع کنید.

با به کار افتادن همه موارد،بالاترین حد امنیت را در WEP eneryption برای کاربر و access point تنظیم کنید معمولاً 128bit یا (encrytion) bit - 152 ، اگر چه در حال حاضر گاهی 256 bit است.

۵-۹- محافظت از شبکه

به علت آنکه اغلب سیگنال های wireless ماوراء محوطه خانه یا اداره شما سیر می کنند، برای امنیت شبکه خود باید بیشتر احتیاط کنید. در غیر این صورت ، هر Hacker در خیابان با یک رادیویی مناسب می تواند به

---

[1]- client

[2]- router

[3]- restar

شبکه شما دسترسی پیدا کند. علاوه بر توجه به مراحلی که در زیر آمده، مطمئن شوید که نرم افزار firewall خود را به روز کرده اید[1].

اولین خط دفاعی SSIP است، که طولش می تواند ۳۲ کاراکتر باشد، همین الان اطمینان حاصل کنید که SSIP را به نام یک شبکه واحد تغییر داده اید، رها کردن نصب پیش فرض کارخانه، در محل – مانند any و wireless یا اسم تولید کننده مانند بازگذاشتن در جلوی خانه تان است.

شما از در پشتی[2] شبکه خود با نصب wep encryption روی کاربر و Ap محافظت می کنید. گر چه Ap می تواند برای هر قسمت یک کلید wep key جدید ایجاد کند، با این حال هنوز هم لازم است کلیدها از هوا عبور کنند، که این خود می تواند باعث کاهش امنیت شود، تولید کننده ها وعده به روز کردن پروتکل امنیت را در آینده ای نزدیک می دهند، ولی درحال حاضر به شما پیشنهاد می کنیم که یک کلید را بصورت دستی روی Ap و کاربر وارد کنید. متأسفانه این، بدان معنی است که شما باید ۲۶ حرف و عدد را برای کلید ۱۲۸ بیتی وارد کنید. بهتر است که ترتیب حرف ها و عددها را به صورت تصادفی انتخاب کنید و سپس متناوباً آن را تغییر دهید.

هنوز هم دربارهٔ امنیت شبکه خود نگران هستید؟ شما می توانیدEAP را روی Ap[3] نصب نمائید تا فقط به کاربرانی که کارت هوشمند دارند و یا بقیه وسایلی که به حد بالایی از امنیت نیاز دارند[4] اعتبار دهد – اگر شما از یکی از معدود notebook هایی که آنها را پشتیبانی می کنند، استفاده می کنید.

شما می توانید از یک سیستم امنیتی مناسب استفاده کنید که پنجره های شبکه را به خوبی درهای آن قفل کند. یکی از موارد مورد علاقهٔ ما kerberos است، که در MIT رشد کرد. نام kerberos از روی نام یک افسانه یونانی گذاشته شد که در آن سگ سه سری، از دروازه های Hades مراقبت می کند.

Kerboeros با تمام سیستم عامل های مهم، به جز Mac کار می کند. Kerberos کلیدها را به شکل encrypt شده می فرستد،در نتیجه snooper برای شکستن آن باید زحمت زیاد بکشند.

برای خارج نگه داشتن evildoers می توانید DHCP را خاموش کنید. به جای آن، آدرس IP دقیق را رنج آدرس IP را به کامپیوترهای خود بدهید. از نظر تئوری hacker خارج از شبکه شما گیر خواهد افتاد. شما می

---

[1]- update

[2]- back dorr

[3]- Access point

[4]- authenticate

توانید Ap را طوری تنظیم کنید که فقط به لیست آدرس های فیزیکی [1] که قبلا مشخص شده اند، اجازه اتصال یا دسترسی کامل به شبکه را بدهد.

با وجود بسیاری از پارامترهای مختلفی که باید مراقبت شوند، به شما پیشنهاد می کنیم که تمام آنها را بنویسید و نگهداری کنید. اگر در خانه هستید، آدرس IP در Ap، SSIP ، سطح WEP و بقیهٔ جزئیات را روی کارتی بگذارید، سپس آن را پشت Ap ضبط کنید یا همراه اسناد نگه دارید، کاربرانی که در اداره هستند، بهتر است تمام تنظیمات شبکه را در جای امنی نگه دارند.

و بدین ترتیب می توان یک شبکه بی سیم محلی را طراحی و پیاده سازی نمود.

[1]- MAC Addapter

بخش دهم

معرفی WAP

۱-۱۰- WAP چیست؟

WAP سرنام wireless Application protocad است. برای تعریف هر یک از این واژه ها داریم:

- Application یک برنامه کامپیوتری یا قطعه ای از نرم افزار کامپیوتری می باشد که برای انجام کاری خاص طراحی شده است.
- wireless فقدان یا عدم نیاز به سیم یا سیم کشی:متوسل به انتقال رادیویی
- protecol مجموعه ای از فوائد فنی دربارهٔ چگونگی انتقال (تبادل) اطلاعات از طریق کامپیوترها

WAP مجموعه از قوانین است که بر انتقال و پذیرش داده به وسیله برنامه های کاربردی کامپیوتری و یا دستگاههای بی سیم نظیر تلفن های موبایل نظارت دارد. در واقع، WAP تنها یک پروتکل نیست، بلکه مجموعه ای از پروتکل ها و مشخصه ها است که هر چیزی از طرز کار دستگاه WAP و user agent گرفته تا چگونگی تعامل پروتکل های انتقال با خود حاملها[1] را پوشش می دهد.

WAP یک تکنولوژی استاندارد شده مستقل از سکو می باشد که برای محاسبات توزیعی که تشابه زیادی به ترکیب HTML و HTTP دارند در اینترنت به کار می رود، با این تفاوت که دارای یک امکان حیاتی است:استفاده بهینه از قابلیت نمایش پایین، حافظه ضعیف و ابزارهای باند پایین نظیر PDAS ها، تلفن های بی سیم و pagerها.

بزرگترین مزیت WAP در این است که برای غلبه بر موانع موجود در دستگاههای دستی سازماندهی شده است:

- دارای صفحات نمایش کوچکی هستند.
- دارای حافظه خالی زیادی برای اجرای برنامه های کاربردی با اندازه های متفاوت نیستند.
- پهنای باندی محدود به ۹۶۰۰ بیت در ثانیه دارند.

تمامی این نکات هر لحظه قابل تغییر هستند و احتمالاً بزودی بیشتر از قبل خواهند شد. گر چه در همین حال، تمامی این نکات دست به دست هم داده اند تا زندگی را برای توسعه دهنده WAP بلندپرواز دشوار نمایند.

---

[1]- bearers

WAP به دستگاهای بی سیم امکان می دهد تا صفحات طراحی شده برای اینترنت را تنها با استفاده از متن ساده و تصاویر بسیار کم حجم سیاه و سفید مشاهده نمایند. کد برنامه نویسی WAP در سایت وب باید بطور صریح برای رمز مرورگر[1] بکار رفته در دستگاه WAP با مدل خاص طراحی و نوشته شود. خود صفحات باید کوچک باشند، زیرا سرعت داده در تلفن های موبایل محدود است.

۲-۱۰- ایدهٔ WAP

بر طبق گفتهٔ انجمن WAP ،اهداف WAP اینها هستند که :

- یک پروتکل بی سیم عمومی برای کار در مشخصات تکنولوژی های شبکه بی سیم گوناگون که مستقل از استانداردهای شبکه بی سیم هستند ایجاد شود.
- مشخصاتی را برای پذیرش توسط صنایع خاص و بدنه های استاندارد ارائه کند.
- در محتوا و برنامه های کاربردی امکان مقیاس پذیری در گزینه های انتقال گوناگون را فعال کند.
- در محتوا و برنامه های کاربردی امکان مقیاس پذیری در انواع گوناگون دستگاهها را فعال کند.
- در طول زمان قابلیت گسترش در شبکه ها و انتقالات را داشته باشد.

با در نظر گرفتن محدودیت های بی سیم و تطابق فن آوری اینترنتی موجود در تقابل با این محدودیت ها، انجمن WAP در ایجاد یک استاندارد در مقیاس وسیعی از دستگاههای بی سیم و شبکه ها موفق شده است. این استاندارد license - free (بدون گواهی نامه) است و اطلاعات و سرویس های تلفن (به دستگاههای بی سیم می رساند. برای دسترسی به این سرویس ها، WAP از اینترنت و پارادیم وب بهره می گیرد. WAP در پهنه ای با برد وسیع از شبکه های بی سیم قرار می گیرد. در ضمن اینکه قوهٔ تبدیل به یک استاندارد جهانی را دارد و اینکه گسترش اقتصادها نیز قابل دستیابی می باشد.

۳-۱۰- معماری WAP

WAP در یک وضعیت لایه بندی شده طراحی شده است، بگونه ای که می تواند انعطاف پیدا کند، قابل بسط و مقیاس پذیر باشد. در نتیجه پروتکل WAP بیشتر به پنج لایه تقسیم می شود.

۱- لایه برنامه کاربردی (WAP) wireless Application Environment

۲- لایه طبسه (WSP) wireless session protocol

۳- لایه تراکنش (WTP) wireless transaction protocol

[1]- micro-browser

۴- لایه امنیت (WTLS) wireless transport layer security

۵- لایه انتقال (WDP) wireless Datagram protocol

هر یک از این لایه ها یک واسط خوش تعریف [1] را برای لایه بالاتر ارائه می نماید. این به آن معنی است که امور داخلی هر لایه برای لایه بالایی خود نامریی یا شفاف هستند.

این معماری لایه ای به برنامه های کاربردی و سرویس های مستقل دیگر امکان می دهد تا از امکانات ارائه شده توسط هر یک از لایه های WAP استفاده کنند و امکان استفاده از لایه های WAP را برای سروس ها و برنامه های کاربردی که فعلاً توسط WAP مشخص نشده اند را فراهم می کند.

چون پشته پروتکل WAP به عنوان مجموعه ای از لایه ها طراحی شده ، که همچنین این معنی را دارد که قابلیت گسترش دارد و در آینده قابل استفاده خواهد بود، هر لایه ای می تواند طبق نیاز یا بدلخواه گسترش یافته و تغییر پذیرد. تا زمانی که واسطهای ما بین لایه ها ثابت هستند،هر لایه ای می تواند بدون اثر گذاشتن روی لایه های دیگر تغییر پیدا کند.

٤-١٠- مدل WAP

هنگامی که نوبت به استفاده واقعی می رسد، WAP به این طریق کار می کند:

۱- کاربر گزینه ای را در دستگاه موبایل خود انتخاب می کند که دارای URL با محتوای WML تخصیص یافته به آن است.

۲- تلفن درخواست URL را از طریق شبکه تلفن به یک WAP gateway با استفاده از پروتکل WAP کدگذاری شده باینری ارسال می کند.

۳- gateway این درخواست WAP را به درخواست HTTP قراردادی برای URL مشخص شده ترجمه کرده و آن را به اینترنت ارسال می‌نماید.

۴- سرویس دهنده وب مناسب در خواست HTTP را بر می گزیند.

۵- سرویس دهنده درخواست را پردازش می‌کند، یعنی همان کاری که با هر درخواست دیگری انجام می‌دهد. اگر URL استیا اشاره کند، سرویس دهنده آن را می‌رساند. اگر یک اسکریپت CGI درخواست شود، پردازش می گردد و محتویات طبق معمول برگشت داده می‌شود.

۶- سرویس دهنده وب، هدر HTTP را به محتوای WML را به فرم باینری کامپایل می کند.

۷- WML, Wapgateway را به فرم باینری کامپایل می کند.

---

[1]- well - defined

۸- سپس gateway پاسخ WML را به تلفن بر می‌گردان.

۹- تلفن WML را از طریق پروتکل WAP دریافت می‌کند.

۱۰- ریزمروگر WML را پردازش نموده و محتوا را روی صفحه نمایش نشان می‌دهد.

WAP استفاده از مدل اینترنت را میسر می‌سازد تا یک بستر سرویس انعطاف پذیر را ارائه دهد. اگر چه به صنعت پذیرش دسترسی بی‌سیم به اطلاعات روی وب، WAP، تلفن‌های موبایل خواهند بود، اما مهم است که به خاطر داشته باشید که WAP تنها محدود به تلفن‌ها نیست دامنه WAP دامنه وسیعی از شبکه‌های بی سیم تا حاملها را می‌پوشاند، در نتیجه WAP به گونه‌ای طراحی شده تا دسترسی به سرویس را از طریق اینترنت با اسفتاده از SMS و همچنین شبکه‌های داده بسته‌ای نظیر GPRS[1] فراهم نماید. WAP می‌تواند سرویس‌ها و برنامه‌های کاربردی مشابه آنهایی که در اینترنت موجود است را ارائه نماید اما اینها در یک محیط سرویس گیرنده نازک خواهد بود، منظور از ناک محدودیت از نظر برخی فاکتورهاست: پهنای باند کم، تأخیر زیاد اتصال پایدار محدود، نمایش کوچک و امکانات ورودی، حافظه و CPU و نیروی باتری محدود.

۱۰-۵ WAP تا چه اندازه امن است؟

مقیاس امنیت در WAP وابسته به آن چیزی است که سعی دارید انجام دهید و آن چیزی است که به نظر شما امن است. برای استفاده کلی و روزمره، ایمنی WAP به اندازهٔ استاندارد تلفن دیجتالی که تلفن شما روی آن کار می‌کند می‌باشد که در برابر استراق سمع بسیار مطمئن است. از این رو اگر مشتاق تئاتر از طریق یک دستگه WAP می‌باشید، کاملاً امن است. سیگنال از دستگاه WAP شما تا WAP gateway از WTLS، استفاده می‌نماید و از WAP gateway تا از اینترنت به ایمنی یک سایت وب تجارت الکترونیکی وب تجارت الکترونیکی معمولی می باشد. اگر چه، در WAP gateuay کسری از ثانیه طول می‌کشد تا اطلاعات از WTLS به متن ساده تبدیل گردد و پیش از آنکه به TLS رمز نگاری می‌شود، در تئوری می‌تواند توسط کسی با دسترسی مستقیم به WAP gateway گرفته شود. از نقطه نظر یک بان، این نوع امنیت برای استفاده در بانک از امنیت کافی برخوردار نیست. در این حالت، این موضوع واقعاً به اندازهٔ اطمینان شما به صاحبت gateway یی که به کار می‌برید خلاصه می‌شود. در اینجا است که مسأله رمزگذاری مطرح می‌شود که این خود یک مبحث گسترده‌ای را در بر می‌گیرد.

[1] General packet Radio services

بخش یازدهم

مفاهیم امنیت شبکه

امنیت شبکه یا Network Security پردازه ای است که طی آن یک شبکه در مقابل انواع مختلف تهدیدات داخلی و خارجی امن می شود. مراحل ذیل برای ایجاد امنیت پیشنهاد و تایید شده اند:

۱- شناسایی بخشی که باید تحت محافظت قرار گیرد.

۲- تصمیم گیری درباره مواردی که باید در مقابل آنها از بخش مورد نظر محافظت کرد.

۳- تصمیم گیری درباره چگونگی تهدیدات

۴- پیاده سازی امکاناتی که بتوانند از دارایی های شما به شیوه ای محافظت کنند که از نظر هزینه به صرفه باشد.

۵- مرور مجدد و مداوم پردازه و تقویت آن درصورت یاقتن نقطه ضعف

مفاهیم امنیت شبکه

برای درک بهتر مباحث مطرح شده در این بخش ابتدا به طرح بعضی مفاهیم در امنیت شبکه می پردازیم.

11-1 منابع شبکه

در یک شبکه مدرن منابع بسیاری جهت محافظت وجود دارند. لیست ذیل مجموعه ای از منابع شبکه را معرفی می کند که باید در مقابل انواع حمله ها مورد حفاظت قرار گیرند.

۱- تجهیزات شبکه مانند روترها، سوئیچ ها و فایروالها

۲- اطلاعات عملیات شبکه مانند جداول مسیریابی و پیکربندی لیست دسترسی که بر روی روتر ذخیره شده اند.

۳- منابع نامحسوس شبکه مانند عرض باند و سرعت

۴- اطلاعات و منابع اطلاعاتی متصل به شبکه مانند پایگاه های داده و سرورهای اطلاعاتی

۵- ترمینالهایی که برای استفاد هاز منابع مختلف به شبکه متصل می شوند.

۶- اطلاعات در حال تبادل بر روی شبکه در هر لحظه از زمان

۷- خصوصی نگهداشتن عملیات کاربرن و استفاده آنها از منابع شبکه جهت جلوگیری از شناسایی کاربران.

مجموعه فوق به عنوان دارایی های یک شبکه قلمداد می شود.

11-2- حمله

حال به تعریف حمله می پردازیم تا بدانیم که از شبکه در مقابل چه چیزی باید محافظت کنیم. حمله تلاشی خطرناک یا غیر خطرناک است تا یک منبع قابل دسترسی از طریق شبکه ، به گونه ای مورد تغییر یا استفاده قرار گیرد که مورد نظر نبوده است.برای فهم بهتر بد نیست حملات شبکه را به سه دسته عمومی تقسیم کنیم:

۱- دسترسی غیرمجاز به منابع و اطلاعات از طریق شبکه

۲- دستکاری غیرمجاز اطلاعات بر روی یک شبکه

۳- حملاتی که منجر به اختلال در ارائه سرویس می شوند و اصطلاحا Denial of Service نام دارند.

کلمه کلیدی در دو دسته اول انجام اعمال به صورت غیرمجاز است. تعریف یک عمل مجاز یا غیرمجاز به عهده سیاست امنیتی شبکه است، اما به عبارت کلی می توان دسترسی غیرمجاز را تلاش یک کاربر جهت

دیدن یا تغییر اطلاعاتی که برای وی در نظر گرفته نشده است، تعریف نمود اطلاعات روی یک شبکه نیز شامل اطلاعات موجود بر روی رایانه های متصل به شبکه مانند سرورهای پایگاه داده و وب ، اطلاعات در حال تبادل بر روی شبکه و اطلاعات مختص اجزاء شبکه جهت انجام کارها مانند جداول مسیریابی روتر است. منابع شبکه را نیز می توان تجهیزات انتهایی مانند روتر و فایروال یا مکانیزمهای اتصال و ارتباط دانست.

هدف از ایجاد امنیت شبکه ، حفاظت از شبکه در مقابل حملات فوق است، لذا می توان اهداف را نیز در سه دسته ارائه کرد:

۱- ثابت کردن محرمانگی داده

۲- نگهداری جامعیت داده

۳- نگهداری در دسترس بودن داده

11-3- تحلیل خطر

پس از تعیین دارایی های شبکه و عوامل تهدیدکننده آنها ، باید خطرات مختلف را ارزیابی کرد. در بهترین حالت باید بتوان از شبکه در مقابل تمامی انواع خطا محافظت کرد، اما امنیت ارزان به دست نمی آید. بنابراین باید ارزیابی مناسبی را بر روی انواع خطرات انجام داد تا مهمترین آنها را تشخیص دهیم و از طرف دیگر منابعی که باید در مقابل این خطرات محافظت شوند نیز شناسایی شوند. دو فاکتور اصلی در تحلیل خطر عبارتند از :

۱- احتمال انجام حمله

۲- خسارت وارده به شبکه درصورت انجام حمله موفق

11-4- سیاست امنیتی

پس از تحلیل خطر باید سیاست امنیتی شبکه را به گونه ای تعریف کرد که احتمال خطرات و میزان خسارت را به حداقل برساند. سیاست امنیتی باید عمومی و در حوزه دید کلی باشد و به جزئیات نپردازد. جزئیات می

توانند طی مدت کوتاهی تغییر پیدا کنند اما اصول کلی امنیت یک شبکه که سیاست های آن را تشکیل می دهند ثابت باقی می مانند.در واقع سیاست امنیتی سه نقش اصلی را به عهده دارد:

۱- چه و چرا باید محافظت شود.

۲- چه کسی باید مسئولیت حفاظت را به عهده بگیرد.

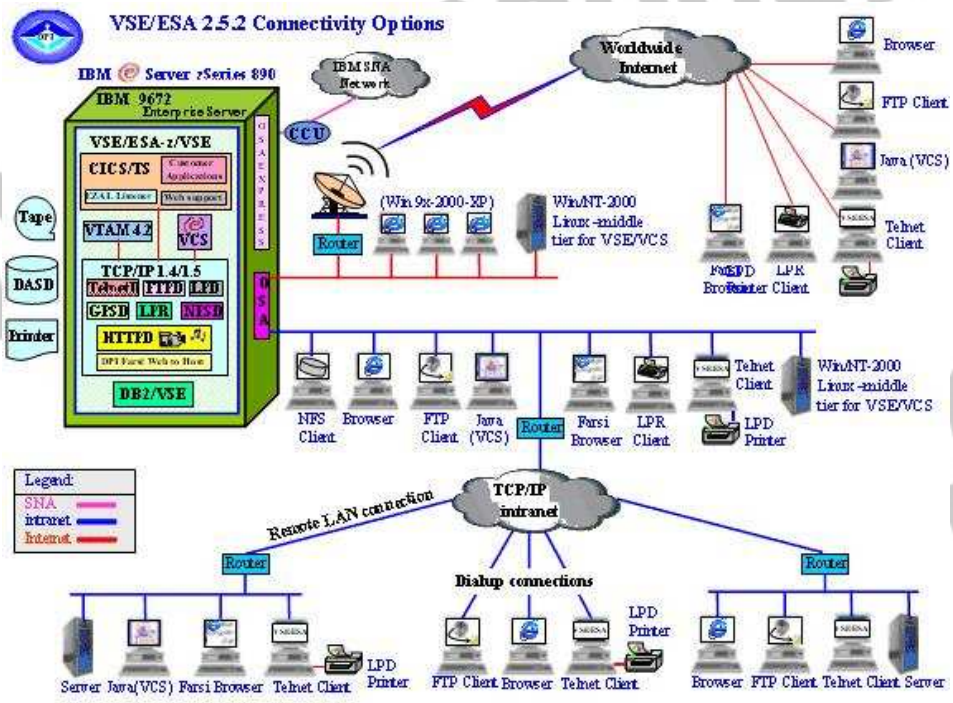
۳- زمینه ای را بوجود آورد که هرگونه تضاد احتمالی را حل و فصل کند.

سیاستهای امنیتی را می توان به طور کلی به دو دسته تقسیم کرد:

۱- مجاز (Permissive) : هر آنچه بطور مشخص ممنوع نشده است ، مجاز است.

۲- محدود کننده (Restrictive) : هر آنچه بطور مشخص مجاز نشده است ، ممنوع است.

معمولا ایده استفاده از سیاستهای امنیتی محدودکننده بهتر و مناسبتر است چون سیاستهای مجاز دارای مشکلات امنیتی هستند و نمی توان تمامی موارد غیرمجاز را برشمرد. المانهای دخیل در سیاست امنیتی در RFC 2196 لیست و ارائه شده اند.



11-5- طرح امنیت شبکه

با تعریف سیاست امنیتی به پیاده سازی آن در قالب یک طرح امنیت شبکه می رسیم. المانهای تشکیل دهنده یک طرح امنیت شبکه عبارتند از :

۱- ویژگیهای امنیتی هر دستگاه مانند کلمه عبور مدیریتی و یا بکارگیری SSH

۲- فایروالها

۳- مجتمع کننده های VPN برای دسترسی از دور

۴- تشخیص نفوذ

۵- سرورهای امنیتی AAA (Authorization and Accounting،Authentication) و سایر خدمات AAA برای شبکه

۶- مکانیزمهای کنترل دسترسی و محدودکننده دسترسی برای دستگاههای مختلف شبکه

11-6- نواحی امنیتی

تعریف نواحی امنیتی نقش مهمی را در ایجاد یک شبکه امن ایفا می کند. در واقع یکی از بهترین شیوه های دفاع در مقابل حملات شبکه ، طراحی امنیت شبکه به صورت منطقه ای و مبتنی بر توپولوژی است و یکی از مهمترین ایده های مورد استفاده در شبکه های امن مدرن ، تعریف نواحی و تفکیک مناطق مختلف شبکه از یکدیگر است. تجهیزاتی که در هر ناحیه قرار می گیرند نیازهای متفاوتی دارند و لذا هر ناحیه حفاظت را بسته به نیازهای امنیتی تجهیزات نصب شده در آن ، تامین می کند. همچنین منطقه بندی یک شبکه باعث ایجاد ثبات بیشتر در آن شبکه نیز می شود.

نواحی امنیتی بنابر استراتژی های اصلی ذیل تعریف می شوند.

۱- تجهیزات و دستگاههایی که بیشترین نیاز امنیتی را دارند (شبکه خصوصی) در امن ترین منطقه قرار می گیرند. معمولا اجازه دسترسی عمومی یا از شبکه های دیگر به این منطقه داده نمی شود.

دسترسی با کمک یک فایروال و یا سایر امکانات امنیتی مانند دسترسی از دور امن (SRA) کنترل می شود. کنترل شناسایی و احراز هویت و مجاز یا غیر مجاز بودن در این منطقه به شدت انجام می شود.

۲- سرورهایی که فقط باید از سوی کاربران داخلی در دسترس باشند در منطقه ای امن ، خصوصی و مجزا قرار می گیرند. کنترل دسترسی به این تجهیزات با کمک فایروال انجام می شود و دسترسی ها کاملا نظارت و ثبت می شوند.

۳- سرورهایی که باید از شبکه عمومی مورد دسترسی قرار گیرند در منطقه ای جدا و بدون امکان دسترسی به مناطق امن تر شبکه قرار می گیرند. درصورت امکان بهتر است هر یک از این سرورها را در منطقه ای مجزا قرار داد تا درصورت مورد حمله قرار گرفتن یکی ، سایرین مورد تهدید قرار نگیرند. به این مناطق DMZ یا Demilitarized Zone می گویند.

۴- استفاده از فایروالها به شکل لایه ای و به کارگیری فایروالهای مختلف سبب می شود تا درصورت وجود یک اشکال امنیتی در یک فایروال ، کل شبکه به مخاطره نیفتد و امکان استفاده از Backdoor نیز کم شود.

11-7-مرکزی برای امنیت شبکه

امروزه استفاده از تکنولوژی شبکه اهمیت بسیار زیادی دارد و این اهمیت برای شرکت های تجاری که می خواهند در بازار رقابت باقی بمانند دو چندان است. در واقع سیستم عامل های جدید نیاز به مکانیسم هایی برای مدیریت اشیا و روابط توزیع شده در محیط شبکه دارند. Directory Service مکانی است برای ذخیره سازی اطلاعات در مورد کلیت شبکه، مثل برنامه های کاربردی، فایل ها، پرینترها و کاربران. بر همین اساس سرویس Active Directory یک راه مطمئن برای نامگذاری، تشریح، محل قرارگیری، نحوه دسترسی، مدیریت ایمنی و اطلاعات در مورد این منابع را فراهم می سازد. با این وجود Active Directory مانند یک تقسیم کننده اصلی در سیستم عامل شبکه کار می کند. از سوی دیگر این سرویس مرکزی برای

مدیریت سیستم ها و رابط بین این منابع توزیع شده است. اکتیو دایرکتوری به خاطر اینکه این توابع اصلی را برای سیستم عامل فراهم کند می بایست با سیستم های مدیریتی و مکانیسم های ایمنی سیستم عامل شبکه در ارتباط باشد تا درستی اطلاعات و اختصاصی بودن آن را تضمین نماید. Directory Service نیز نقش مهمی را در توانایی شرکت ها برای تعریف و نگهداری زیربنای شبکه، اجرای مدیریت سیستم و کنترل تمام تجاربی را که کاربران از سیستم های اطلاعاتی شرکت به دست می آورند بر عهده دارد.

11-8-چرا Service Directory

نیاز به یک Active Directory قوی و شفاف، از رشد انفجاری شبکه ها ناشی می شود. همان طور که شبکه ها رشد می کنند و پیچیده تر می شوند و برنامه های کاربردی که نیاز به شبکه و سیستم های دیگر در اینترنت دارند افزایش می یابند، به همان میزان نیاز فراوانی به Service Directory احساس می شود. دایرکتوری سرویس یکی از مهمترین ابزارهای سیستم های پیشرفته کامپیوتری است که در این جا بد نیست مزایای این سرویس را با هم مرور می کنیم:

۱- فراهم کردن یک مرکز واحد و یکنواخت مدیریتی برای کاربران، برنامه های کاربردی و دستگاه ها.

۲- فراهم کردن یک نقطه ورود جهت دسترسی به منابع شبکه و همچنین فراهم کردن ابزارهای قوی و یکنواخت مدیریتی برای مدیریت سرویس های ایمنی برای کاربران داخلی و نیز کاربرانی که از راه دور و توسط تلفن ارتباط برقرار می کنند.

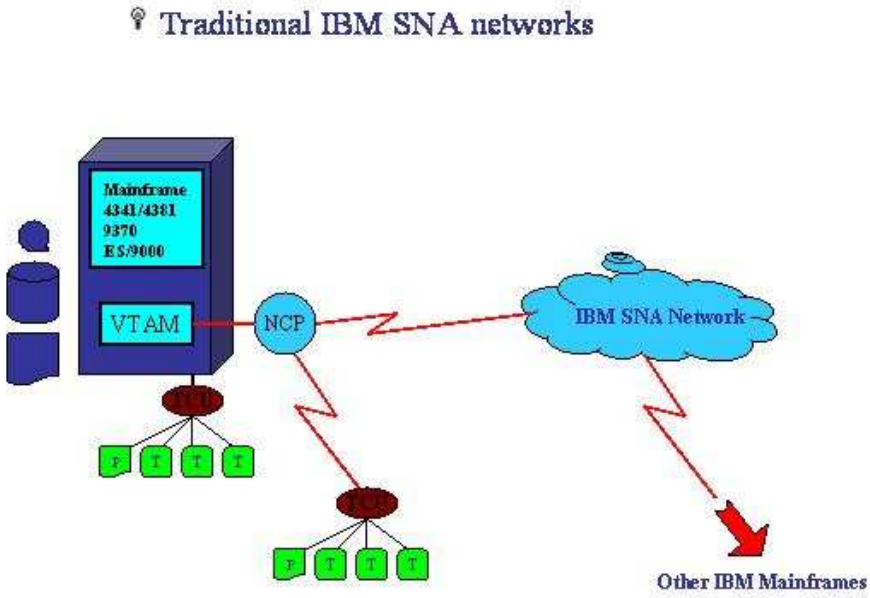
۳- مهیا کردن دسترسی استاندارد و یکسان به همه امکانات اکتیو دایرکتوری.

اکتیو دایرکتوری یک جزء اصلی از معماری شبکه ویندوز ۲۰۰۰ و هسته های مشابه است. Active Directory به سازمان ها اجازه می دهد که اطلاعات خود را در شبکه، شامل منابع موجود در شبکه و کاربران شبکه به اشتراک بگذارند و مدیریت کنند. اکتیو دایرکتوری همچنین به عنوان یک مرکز اصلی برای امنیت شبکه عمل می کند. به طوری که اجازه می دهد سیستم عامل به طور شفاف هویت کاربر را تعیین

نماید و همچنین دسترسی به منابع شبکه را توسط آن کاربر کنترل نماید. نکته مهمتر این است که Active Directory به عنوان نقطه ای برای گردآوری تعمیم ها و مدیریت آنها عمل می کند.

این قابلیت ها به سازمان ها اجازه می دهند که قوانین کاری استانداردی را برای برنامه های کاربردی توزیع شده و منابع شبکه به کار ببرند، بدون اینکه نیازی به مدیرانی داشته باشند که توانایی نگهداری دایرکتوری های مخصوصی را داشته باشند. در عین حال Active Directory یک نقطه مرکزی را برای مدیریت حساب های کاربران و سرورها و برنامه های کاربردی در محیط ویندوز فراهم می کند که با برنامه های کاربردی تحت ویندوز و دستگاه های سازگار با ویندوز ارتباط برقرار کنند. به این ترتیب Active Directory باعث توسعه سرمایه گذاری در شبکه می شود. همچنین باعث کم شدن هزینه استفاده از کامپیوتر از طریق افزایش مدیریت بیشتر و راحت تر شبکه، افزایش ایمنی شبکه و افزایش قابلیت همکاری بین شبکه ها می شود. استراتژی Directory Service شرکت مایکروسافت سبب می شود که بسیاری از فروشنده ها و مراکز، Service Directory های خاصی را در برنامه های کاربردی یا دستگاه هایشان تعبیه نمایند تا بتوانند درخواست ها و عملیات هایی را که مورد نیاز مشتریان است برآورده سازند. برای مثال سرویس E-mail شامل Directory Service هایی است که به کاربران اجازه می دهد تا صندوق پست خود را جست وجو کنند.

سیستم عامل های سرور نیز می توانند از Directory Service ها برای امکاناتی نظیر مدیریت حساب کاربران، ذخیره کردن اطلاعات و پیکربندی برای برنامه های کاربردی استفاده کنند.Directory Active اولین Director Service کامل و جامع است که اندازه پذیر بوده و از اندازه های کوچک شروع می شود و به اندازه های بسیار بزرگ می رسد و نیز براساس تکنولوژی اینترنتی ساخته شده و کاملاً با سیستم عامل هماهنگ است... علاوه بر این جهت برنامه های کاربردی تحت ویندوز، Directory Active طوری طراحی شده که برای کاربران، محیط های ایزوله و محیط های انتقال، محیط مدیریت متمرکز را با حداقل Directory Service مورد نیاز شرکت ها فراهم می کند و این توانایی Directory Active را برای مدت طولانی به عنوان پایه و ستون اصلی جهت اشتراک گذاشتن اطلاعات و مدیریت مشترک منابع شبکه، شامل استفاده از برنامه های کاربردی، سیستم عامل های شبکه و سرویس های وابسته به دایرکتوری مطرح می کند.



11-9-اکتیو دایرکتوری چگونه کار می کند

اکتیو دایرکتوری به سازمان ها اجازه می دهد تا اطلاعات را به صورت سلسله مراتبی طبقه بندی کنند و برای پشتیبانی محیط های شبکه ای توزیع شده، مدل تکثیر اطلاعات در سرورهای متناظر را ارائه می کند. اکتیو دایرکتوری از اشیا برای نمایش منابع شبکه استفاده می کند. کاربران، گروه ها، ماشین ها، دستگاه ها و برنامه های کاربردی از بسته ها برای نشان دادن سازمان ها استفاده می کنند مثل بخش بازاریابی و یا مجموعه ای از اشیای وابسته به هم مانند پرینترها. این اطلاعات در ساختارهای درختی که از این اشیا ایجاد می شوند سازماندهی می شوند و همانند روشی است که سیستم عامل های ویندوز برای فایل ها و شاخه ها جهت سازماندهی اطلاعات در کامپیوتر استفاده می کنند. علاوه بر این اکتیو دایرکتوری روابط بین اشیا و بسته ها را فراهم می کند تا یک دید متمرکز و جامع را نشان دهد و این باعث می شود که درک و کنترل منابع راحت تر شده و مدیریت آنها بهینه شود. ساختار سلسله مراتبی اکتیو دایرکتوری که یک ساختار انعطاف پذیر و قابل پیکربندی است باعث می شود که سازمان ها منابع را آن طور که به آن نیازمند هستند سازماندهی کنند. گروه بندی اشیا در داخل دایرکتوری اجازه می دهد که مدیران اشیا را در سطح ماکرو مدیریت کنند. این کار کارایی، دقت و مدیریت را افزایش می دهد، به طوری که سازمان ها مدیریت شبکه را با نیازهای تجاری خودشان انجام می دهند.

برای فراهم کردن قابلیت اجرایی بالا، دسترسی بهتر و قابلیت انعطاف در محیط های توزیع شده، اکتیو دایرکتوری از تکثیر اطلاعات در سرورهای متناظر استفاده می کند و این به سازمان ها اجازه می دهد که نسخه های گوناگون از دایرکتوری ها ایجاد کنند. در نتیجه، تعویض ها و تغییراتی که در هر جای شبکه صورت بگیرد به طور اتوماتیک در سراسر شبکه کپی می شوند. از سوی دیگر اکتیو دایرکتوری از تکثیر اطلاعات در سرورهای متناظر برای قابلیت انعطاف، جهت افزایش و بالا بردن میزان دسترسی و اجرا پشتیبانی می کند. برای مثال کپی دایرکتوری Syncron می تواند از هر موقعیت و مکانی در شبکه مورد استفاده قرار گیرد. چنین پردازشی می تواند اجرای سریع تر را در اختیار کاربر بگذارد. به این دلیل که کاربران برای دسترسی به منابع مورد نیازشان به جای جست وجو در شبکه ، آن را از طریق جست وجو در دایرکتوری سرور محلی خود پیدا می کنند. این دایرکتوری ها بسته به منابع مدیریتی که در دسترس است می توانند به طور محلی یا از راه دور مدیریت شوند.

10-11- مزایای اکتیو دایرکتوری

به علت ارتباط تنگاتنگ و کاملاً مجتمع اکتیو دایرکتوری با ویندوز ۲۰۰۰ این قابلیت در اختیار مدیران شبکه، برنامه نویسان و کاربران قرار گرفته که به Service Directory زیر دسترسی داشته باشند:

۱- آسان تر کردن کارهای مدیریت

۲- افزایش امنیت شبکه

۳- قابلیت استفاده از سیستم های موجود در محیط شبکه های مختلف و آسان کردن مدیریت سیستم های توزیع شده که اغلب منجر به اشتراک زمانی می شوند.

در عین حال زمانی که شرکت ها برنامه های کاربردی را به زیرساخت و شالوده خود اضافه کنند و یا پرسنل خود را بازنشسته می کنند و همچنین نیاز به توزیع نرم افزار بر روی کامپیوترهای خود و همچنین مدیریت دایرکتوری های برنامه های کاربردی دارند، اکتیو دایرکتوری به شرکت ها اجازه می دهد که هزینه های خود را با استفاده از کنترل مرکزی کاربران، گروه ها و منابع شبکه به همراه نرم افزار توزیع شده و مدیریت

پیکربندی کامپیوترهای کاربران کاهش دهند.اکتیو دایرکتوری از سوی دیگر به شرکت ها کمک می کند که مدیریت آسان تر و راحت تری داشته باشند.

این سرویس با سازماندهی کاربران و منابع شبکه به طور سلسله مراتبی به مدیران اجازه می دهد تا یک مرکز واحد مدیریت را برای حساب های کاربران و سرورها و برنامه های کاربردی داشته باشند. اکتیو دایرکتوری مدیریت منابع شبکه را آسان می کند. در واقع اکتیو دایرکتوری با تعویض اختیار وظایف مدیریتی به افراد یا گروه های خاص، انجام کارهای مدیریتی منابع شبکه را ارتقا می دهد. اکتیو دایرکتوری یک مزیت بزرگ دیگر نیز دارد و آن هم بالا بردن امنیت است.

Active Directory مدیریت را متمرکز می کند و نقش هایی که دارای امنیت مستحکم و استوار هستند را به وسیله پردازش قوانین جاری در سازمان ها اجرا می کند. Active Directory امنیت رمزها و مدیریت را بالا می برد. انجام این کار با فراهم آوردن نقطه ورود یکسان در منابع شبکه با کار گروهی و سرویس های امنیتی با قدرت بالا مقدور می شود. Active Directory عملکرد کامپیوتر را نیز تثبیت می کند.

این سرویس این کار را با قفل کردن پیکربندی کامپیوتر و جلوگیری از دسترسی عملیات در سطح کامپیوتر مشتریان انجام می دهد و با فراهم کردن ساختارهای پشتیبانی کننده ایجاد امنیت در پروتکل های استاندارد اینترنت و سنجش تصدیق ورود مکانیسم ها سرعت تجارت الکترونیکی را بالا می برد.یکی دیگر از مزایای Active Directory کنترل امنیت و سیستمهای ایمنی است که با تنظیم کردن امتیازات دسترسی بر روی اشیای دایرکتوری و عنصرهای فردی اطلاعات که آنها را ایجاد میکند این کار را انجام می دهد.

11-11-افزایش همکاری بین شبکه ها

بسیاری از شرکت ها مجموعه های مختلفی از تکنولوژی ها را دارا هستند که می باید با هم کار کنند. Active Directory دارای مجموعه روابط استاندارد برای کلیه امکانات از جمله سرمایه گذاری فعلی و انعطاف پذیری برای برنامه های کاربردی است. با به هم پیوستن مدیریت دایرکتوری ها برنامه های کاربردی متعدد و اجازه استفاده از دایرکتوری به شبکه ها این کار امکان پذیر می شود. ضمناً Directory Active یک محیط مناسب را برای برنامه های کاربردی که از سرویس های دایرکتوری استفاده می کنند به وجود

می آورد. این امکان اجازه می دهد که نرم افزارنویسان، برنامه های کاربردی خود را براساس نقش کاربر در شرکت کنترل کنند. به هر صورت با توسعه این تکنولوژی مزایای Active Directory در محیط ویندوز می تواند گسترش یابد. سرویس Active Directory یک مرکز مهم برای مدیریت و ایجاد امنیت برای کاربران، سرورها و برنامه های کاربردی است. Active Directory ارزش سرمایه ایجاد شده سازمان ها را بالا می برد و با کاهش هزینه ها و مدیریت بهینه توسط سیستم های کامپیوتری به تدریج با توزیع مناسب اطلاعات، داده ها، ابزار و امکانات رهبر عصری می شود که افزایش ثروت و تجارت با کامپیوتر به خوبی امکان پذیر شده ضمن اینکه پیچیدگی های اولیه این پدیده در مدیریت و کنترل و حداقل خود می رسد.

در واقع Active Directory فقط یک شروع است و باید منتظر بود تا با توسعه این تکنولوژی و سایر تکنولوژی های همگام، به تدریج شاخص های مدیریت و کنترل در دنیای کامپیوتر و اداره امور به وسیله آن به سطوح درخشان و کارآمد خود نائل آیند.

بخش دوازدهم

امنیت شبکه: چالشها و راهکارها

راهکارهای امنیتی شبکه

۱۲-۱: کنترل دولتی

علاوه بر بهره‌گیری از امکانات فنی، روشهای کنترل دیگری نیز برای مهار اینترنت پیشنهاد شده است. در این روش، سیاست کلی حاکم بر کشور اجازه دسترسی به پایگاههای مخرب و ضد اخلاقی را نمی‌دهد و دولت شبکه‌های جهانی را از دروازه اتصال و ورود به کشور با فیلترهای مخصوص کنترل می‌کند.

۱۲-۲: کنترل سازمانی

روش دیگر کنترل سازمانی است که معمولاً سازمان، اداره یا تشکیلاتی که مسئولیت سرویس‌دهی و اتصال شهروندان را به اینترنت به عهده می‌گیرند، خود موظف به کنترل شبکه و نظارت بر استفاده صحیح از آن می‌شود تا با الزامات قانونی و اخلاقی تواماً انجام این وظیفه را تضمین کند.

۱۲-۳: کنترل فردی

کنترل فردی روش دیگری است که قابل انجام است. در این نوع کنترل تمام تضمینهای اجرایی، درون فردی است و شخص با بهره‌گیری از وجدان فردی و مبانی اخلاقی و تعهد دینی، مراقبتهای لازم را در ارتباط با شبکه‌های جهانی به عمل آورد. این اعتقاد و فرهنگ در محدودهٔ خانواده نیز اعمال می‌شود و چه بسا اطرافیان را نیز تحت تأثیر قرار دهد. البته شیوهٔ اخیر در صورتی ممکن خواه بود که واگذاری خط اشتراک IP پس از شناسایی کامل افراد و با ملاحظه خصوصیات اخلاقی آنان انجام پذیرد. در غیر این صورت تصور اعمال چنین کنترلی از سوی تک تک افراد جامعه صرفاً در حد آرزو باقی خواهد ماند. آرزویی که نمی‌تواند بسیاری از تأثیرات سوء این شبکه را از بین ببرد و آن را بسوی شبکه سالم سوق دهد.

۱۲-٤: تقویت اینترانت‌ها

از سوی دیگر تقویت شبکه‌های داخلی که به اینترانت معرو ف است می‌تواند نقش بسزایی در کاهش آلودگیهای فرهنگی و اطلاعاتی اینترنت یاری کند. قرار دادن اطلاعات مفید اینترنت به صورت ناپیوسته و روی شبکه‌های داخلی یا اینترانتها، علاوه بر ارائهٔ خدمات و اطلاع‌رسانی سالم، پس از چندی، بایگانی غنی و پرباری از انواع اطلاعات فراهم آمده از چهار گوشه جهان را در اختیار کاربران قرار می‌دهد که با افزایش اطلاعات داخلی و یا روزآمد کردن آن، به عنوان زیربنای اطلاعاتی کشور قابل طرح می‌باشد. به هر حال سرعت بالا و هزینه کم در استفاده از اینترانتها، دو عامل مورد توجه کاربران به شبکه‌های داخلی است که به نظر نمی‌رسد محمل مناسبی برای اطلاعات گزینش شده اینترنت باشد.

۱۲-۵: وجود یک نظام قانونمند اینترنتی

مورد دیگر که کارشناسان از آن به عنوان پادزهر آسیبهای اینترنتی از قبیل تهاجم فرهنگی، اطلاعات نادرست و یا پیامدهای ضد اخلاقی نام می‌برند، وجود یک نظام قانونمند اینترنتی در جامعه است که ادارهٔ آن از سوی یک متولی قدرتمند و کاردان می‌تواند اینترنت سرکش و افسار گسیخته را مهار کند و از آن به نحو شایسته بهره‌برداری نماید.

این نظام اگر با یک نظام حقوقی و دادرسی جامع و عمیق توأم باشد، موارد تخلف و سوءاستفاده از این ابزار به راحتی قابل تشخیص و پیگیری قضایی خواهد بود. در این صورت امکان سوءاستفاده و تأثیرپذیری از فرهنگهای بیگانه که عموماً مغایر با اصول اخلاقی ماست، به طرز چشمگیری کاهش می‌یابد.

۱۲-٦: کار گسترده فرهنگی برای آگاهی کاربران

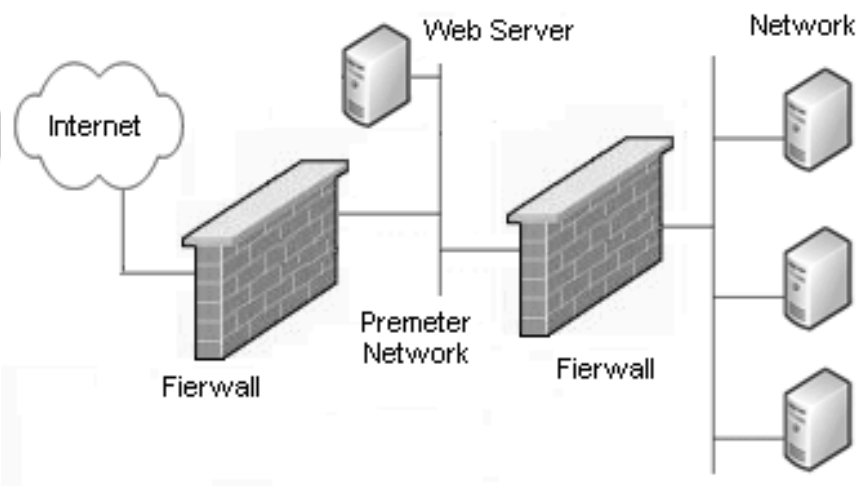
اما بهترین روش، کار گستردهٔ فرهنگی، برای آگاهی کاربران است. کافی است که آنها آگاه شوند که گرایش و ارتباط با پایگاههای غیرمتعارف جز ضلالت و تباهی ثمره‌های ندارد. باید تقوای درونی و اعتقادات دینی کاربران را رشد داد و آنها را تقویت کرد. بنابراین بهترین بارو (فایروال) برای ممانعت از خطرات اینترنت و جلوگیری از تأثیر ابعاد منفی آن، وجدان درونی و ایمان هر نسل است که بخشی از این ایمان را علمای دین باید در وجود نسل جوان و انسانهای این عصر بارور سازند.

۱۲-۷: فایروالها

در حقیقت فایروال یا بارو شبکه‌های کوچک خانگی و شبکه‌های بزرگ شرکتی را از حملات احتمالی رخنه‌گرها (هکرها) و وب سایتهای نامناسب و خطرناک حفظ می‌کند و مانع و سدی است که متعلقات و دارایهای شما را از دسترس نیروهای متخاصم دور نگاه می‌دارد.

بارو یک برنامه یا وسیله سخت‌افزاری است که اطلاعات ورودی به سیستم رایانه و شبکه‌های اختصاصی را تصفیه می‌کند. اگر یک بسته اطلاعاتی ورودی به وسیلهٔ فیلترها نشان‌دار شود، اجازه ورود به شبکه و رایانه کاربر را نخواهد داشت.

به عنوان مثال در یک شرکت بزرگ بیش از صد رایانه وجود دارد که با کارت شبکه به یکدیگر متصل هستند. این شبکهٔ داخلی توسط یک یا چند خط ویژه به اینترنت متصل است. بدون استفاده از یک بارو تمام رایانه‌ها و اطلاعات موجود در این شبکه برای شخص خارج از شبکه قابل دسترسی است و اگر این شخص راه خود را بشناسد می‌تواند یک یک رایانه‌ها را بررسی و با آنها ارتباط هوشمند برقرار کند. در این حالت اگر یک کارمند خطایی را انجام دهد و یک حفره امنیتی ایجاد شود، رخنه‌گرها می‌توانند وارد سیستم شده و از این حفره سوء استفاده کنند.



اما با داشتن یک بارو همه چیز متفاوت خواهد بود. باروها روی خطوطی که ارتباط اینترنتی برقرار می‌کنند، نصب می‌شوند و از یک سری قانونهای امنیتی پیروی می‌کنند. به عنوان مثال یکی از قانونهای امنیتی شرکت می‌تواند به صورت زیر باشد:

از تمام پانصد رایانه موجود در شرکت فقط یکی اجازه دریافت صفحات ftp را دارد و بارو باید مانع از ارتباط دیگر رایانه‌ها از طریق ftp شود.

این شرکت می‌تواند برای وب سرورها و سرورهای هوشمند و غیره نیز چنین قوانینی در نظر بگیرد. علاوه بر این، شرکت می‌تواند نحوهٔ اتصال کاربران- کارمندان به شبکه اینترنت را نیز کنترل کند به عنوان مثال اجازه ارسال فایل از شبکه به خارج را ندهد.

در حقیقت با استفاده از بارو یک شرکت می‌تواند نحوهٔ استفاده از اینترنت را تعیین کند. باروها برای کنترل جریان عبوری در شبکه‌ها از سه روش استفاده می‌کنند:

۱:Packet Filtering

یک بسته اطلاعاتی با توجه به فیلترهای تعیین شده مورد تحلیل و ارزیابی قرار می‌گیرند. بسته‌هایی که از تمام فیلترها عبور می‌کنند به سیستمهای موردنیاز فرستاده شده و بقیه بسته‌ها رد می‌شوند.

۲: Proxy Services

اطلاعات موجود در اینترنت توسط بارو اصلاح می‌شود و سپس به سیستم فرستاده می‌شود و بالعکس.

۳: Stateful Inspection

این روش جدید محتوای هر بسته با بسته‌های اطلاعاتی ویژه‌ای از اطلاعات مورد اطمینان مقایسه می‌شوند. اطلاعاتی که باید از درون بارو به بیرون فرستاده شوند، با اطلاعاتی که از بیرون به درون ارسال می‌شود، از لحاظ داشتن خصوصیات ویژه مقایسه می‌شوند و در صورتی که با یکدیگر ارتباط منطقی داشتن اجازه عبور به آنها داده می‌شود و در غیر اینصورت امکان مبادلهٔ اطلاعات فراهم نمی‌شود.

۱۲-۸: سیاست‌گذاری ملی در بستر جهانی

واقعیت این است که بدون ملاحظه چند الگوی ملی در برخورد با اینترنت نمی‌توان از سیاست‌گذاری مبتنی بر فهم جهانی سخن گفت. لذا معرفی اجمالی چند نمونه که با سه رویکرد تحول‌گرا، ثبات‌گرا، و اعتدال‌گرا تناسب بیشتری دارند ضروری است.

۱۲-۸-۱: الگوی آمریکایی

اینترنت در آمریکا هم به عنوان تهدید امنیتی و هم به عنوان بزرگترین فرصت ملی تلقی می‌شود. کاخ سفید در پنجم ژانویه سال ۲۰۰۰ بیانیه‌ای را تحت عنوان «استراتژی امنیت ملی در قرن جدید» منتشر کرد. در این بیانیه ضمن برشمردن منافع حیاتی آمریکا، از اینترنت به عنوان مهمترین ابزار دیپلماسی مردمی نام برده شده است.

پیشرفت جهانی تکنولوژیهای آزاد و اطلاع‌رسانی چون اینترنت توانایی شهروندان و مؤسسات را برای تأثیرگذاری بر سیستمهای دولتها تا حد غیرقابل تصوری بالا برده است. دیپلماسی مردمی یعنی تلاش برای انتقال اطلاعات و پیامهایمان به مردم جهان یکی از ابعاد مهم استراتژی امنیت ملی ماست. برنامه‌ریزی ما باید به گونه‌ای باشد که توانایی ما را برای اطلاع‌رسانی و تأثیرگذاری بر ملل کشورهای دیگر در جهت منافع آمریکا تقویت کند و گفتگوی میان شهروندان و مؤسسات آمریکایی را با نظائرشان در دیگر کشورها توسعه ببخشد. توسعهٔ اینترنت در داخل و استفاده از آن برای تأثیرگذاری بر دیگران بخش مهمی از سیاستهای استراتژیک آمریکاست.

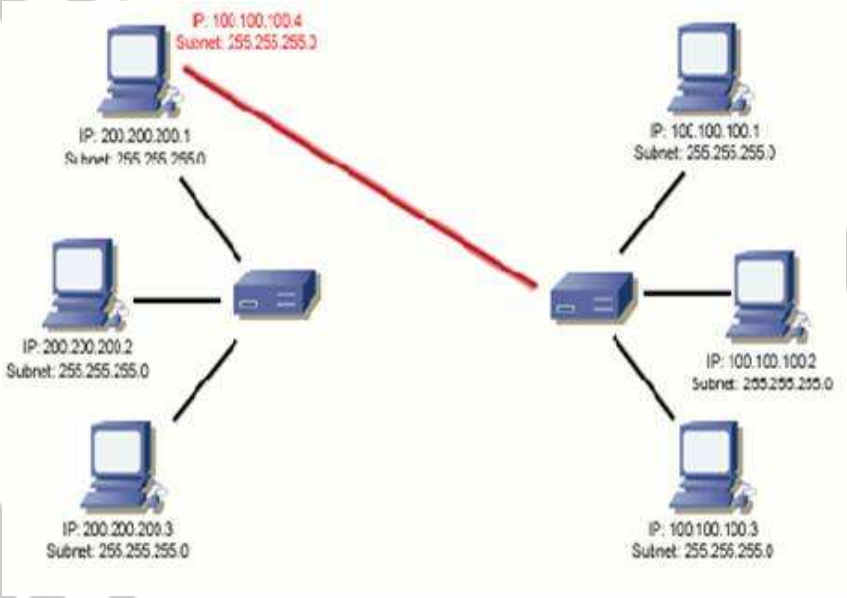
افزایش جرایم رایانه‌ای در آمریکا از جمله حمله به سایتهای Amazon و yahoo، ریس FBI را واداشت تا در فوریه ۲۰۰۰ از کنگره بخواهد ۳۷ میلیون دلار به بودجه ۱۰۰ میلیون دلاری وزارت دادگستری برای مبارزه با جرایم رایانه‌ای بیفزاید و کلینتون در همان ماه درخواست یک بودجه ۹ میلیون دلاری برای تأسیس مرکز امنیت ملی، مشارکت شرکتهای اینترنتی و تجارت الکترونیک علیه حمله‌کنندگان به سایتهای رایانه‌ای را به کنگره ارائه داد.

۱۲-۸-۲: الگوی فلسطین اشغالی

این کشور در فاصله سال ۱۹۹۴ تا ۲۰۰۰ تبدیل به یک غول صنعت اینترنت شده است این کشور در سطح داخلی چنین سیاستهایی اتخاذ کرده است:

- اختصاص ۳٪ از GDP کشور معادل ۹۰ میلیارد دلار به تحقیق و توسعه در زمینه تکنولوژی پیشرفته
- آموزش مهارتهای پیشرفته رایانه‌ای در دوران سربازی و تداوم آموزش در دوران خدمت احتیاط.

تولید Checkpoint با پیشینه و ریشه در کاربردهای نظامی و به عنوان یکی از قابل اطمینان‌ترین و پرفروشترین باروهای جهان که کشورهای عربی نیز به آن متکی هستند، یکی از سیاستهای جهانی کشور مذکور است.



۱۲-۸-۳: الگوی چینی

چین رسماً اعلام کرده است به دنبال برقراری توازن میان جریان آزاد اطلاعات و صیانت فرهنگ و ارزشهای اجتماعی خود می‌باشد. پیتر پیت معاون شرکت دولتی اینترنت چین گفته است:

ما علاقه به قمار، پورنوگرافی و موارد حساسیت برانگیز سیاسی نداریم اما حتی با محتوای فیلتر شده، اینترنت را تنها و مهمترین نیرویی می‌دانیم که درهای چین را بر روی دنیا می‌گشاید راه تغییرات اقتصادی را هموار می‌کند.

در اجرای این استراتژی چین اقدامات زیر را انجام داده است:

- سرمایه‌گذاری عظیم در صنایع الکترونیک، مخابرات و رایانه
- اقدامات وسیع و سازمان یافته برای تکثیر، شکستن قفل و شبیه‌سازی نرم‌افزارها و برنامه‌های کاربردی رایانه‌ای و تقویت صنعت عظیم نرم‌افزار در چین
- تأسیس شرکت دولتی اینترنت چین و انحصار ورود اینترنت به کشور از طریق این شرکت
- همکاری شرکت با غولهای اینترنتی آمریکا برای ایجاد خدمات مبتنی بر وب با استانداردهای کیفی AQL و استانداردهای اخلاقی و قانونی چین
- جلب همکاری AQL و Netscape برای تولید یک پویشگر اینترنت به زبان چینی
- هزینه عظیم برای فیلتر کردن محتوای نامناسب اخلاقی و سیاسی در اینترنت

۱۲-۸-٤:الگوی کشورهای عربی حاشیه خلیج فارس

تقریباً در تمام کشورهای حاشیه خلیج فارس کنترل قوی دولتی بر محتوا و توزیع اطلاعات وجود دارد. این کنترلها به علل مذهبی، سیاسی و فشارهای داخلی صورت می‌گیرد. روش اصلی کنترل اطلاعات الکترونیک، در این کشورها انحصار مخابرات در شرکتهای دولتی است. یکی از پیامدهای اصلی این کنترل دولتی تأخیر در رسیدن اینترنت و کندی در همه‌گیر شدن آن در این کشورهاست. در کشورهای عربی منطقه خلیج فارس دولت و بخش دانشگاهی عامل گسترش اینترنت نبوده‌اند، در عوض تجارت آزاد و بازرگانان خارجی مقیم، بیشترین مشتاقان و کاربران اینترنت را تشکیل می‌دهند. در واقع هیچ شخص، سازمان، و تجارت مدنی نمی‌تواند بدون اتکاء به وب و اینترنت در رقابت جهانی برای دسترسی به منابع طبیعی و اقتصادی خلیج فارس به بقاء خود ادامه دهد. اقتصاد وابسته و ادغام منطقه در اقتصاد جهانی، اتصال به اینترنت را گریزناپذیر می‌کند. بازار مصرف اینترنت در کشورهای عربی خلیج فارس، اساساً تجاری است.

کشورهای خلیج فارس از نظر سیاستگذاری در مورد اینترنت روی یک طیف قرار دارند که یک طرف آن عراق و طرف دیگر آن یمن و قطر است.

عراق تاکنون رسماً به اینترنت متصل نشده است و مودمهای شخصی را ممنوع کرده است. از طرف دیگر یمن و قطر با حذف هرگونه کنترلی بر روی اینترنت و سرمایه‌گذاری برای گسترش زیر ساختها به منافع اینترنت بیشتر از خطرات آن بها داده‌اند.

کویت با برخورداری از سیستم مخابراتی کاملاً پذیرفته در سال ۱۹۹۴ ارائه خدمات عمومی اینترنت را آغاز کرد. وزارت مخابرات کویت امتیاز ISP را ابتدا به گلف نت و سپس به یک کمپانی دیگر واگذار کرد. گلف نت از طریق ماهواره Sprint به آمریکا متصل است. دانشجویان کویتی بدون هیچ گونه هزینه به اینترنت دسترسی دارند

عمان به واسطه جبران عقب ماندگی نسبی از دیگر کشورهای خلیج فارس، بازسازی سیستم مخابراتی را در اولویتهای خود قرار داده است. در چارچوب یک طراحی ملی برای زیرساختها و خدمات مخابراتی GTO سازمان عمومی مخابرات طرحی را برای سال ۲۰۰۰ ارائه کرد که در آن امکان دسترسی به هر اطلاعی در هر زمانی در هر کجا و به هر شکل برای دولت و بخش خصوصی پیش‌بینی شده‌اند. GTO در سال ۱۹۹۵ یک مناقصه بین‌المللی را برای ISP اعلام کرد. در این مناقصه Sprint آمریکا برگزیده شد و علاوه بر ایجاد سایت، اداره آن را به مدت ۵ سال تعهد کرد. دسترسی عمومی به اینترنت از دسامبر ۱۹۹۶ فراهم شد و کاربری تجاری آن به سرعت توسعه یافت.

قطر مدرن‌ترین شبکهٔ مخابراتی منطقه را ایجاد کرده است و انحصار مخابرات دولتی توسط Qtel اعمال می‌شود که تنها ISP کشور را دارا می‌باشد، ولی بررسیهایی به منظور خصوصی‌سازی، ولی به صورت غیررقابتی در حال انجام است. دولت در کنار اینترنت، یک سیستم اطلاعاتی ژئوفیزیکی را با اهداف توسعه بخشی عمومی و خصوصی به سرعت توسعه داده است ولی آموزش عالی و دانشگاه بهره چندانی از آن نبرده‌اند. قطر تنها کشور حاشیه خلیج فارس است که خود را منطقه فارغ از سانسور اطلاعات معرفی کرده و هیچ‌گونه کنترلی بر محتوای اینترنت اعمال نمی‌کند. تنها حساسیت دولت مسأله پورنوگرافی است که با استفاده از باروها تا حدی کنترل می‌شود.

امارات متحده عربی از سال ۱۹۹۵ ارزان قیمت‌ترین و نظارت شده‌ترین خدمات اینترنت منطقه را ارائه می‌کند و نسبت به جمعیت دارای بیشترین تعداد رایانه متصل به اینترنت است. دولت و بخش تجاری و دانشگاهها همه

پشتیبان اینترنت هستند و از آن به خوبی بهره‌برداری می‌کنند. وزارت مخابرات با راه‌اندازی چند پراکسی سرور گران قیمت تمام تبادلات داده‌ها را فیلتر و کنترل می‌کند. در عین حال امارات شاهد بیشترین مباحثات افکار عمومی درباره خطرات استفاده از اینترنت بوده است.

عربستان سعودی بزرگترین و محافظه‌کارترین کشور منطقه است و به موارد غیراخلاقی و فعالیتهای تبعیدیان خارج نشین بسیار حساس است. هنوز اینترنت در سعودی توسعهٔ چندانی پیدا نکرده است و دسترسی عمومی در اینترنت همگانی نشده است، اما برخی از بخشهای دولتی، پزشکی و دانشگاهی از طریق یک اتصال ماهواره‌ای به آمریکا از خدمات اینترنت استفاده می‌کنند. سعودی گران‌ترین طرح مطالعاتی در مورد کاربردها و استلزامات اینترنت را به مدت دو سال پیگیری کرد و در نتیجه روش مدیریت کاملاً متمرکز برای ورود اینترنت به کشور و کنترل کل ورودی توسط یک باروی ملی برای جلوگیری از دسترسی به محتوای نامناسب از طرف دولت پذیرفته شد.

12-9- اینترنت و امنیت فرهنگی ایران

در بحبوحه جنگ نگرشها، این واقعیت را نباید از نظر دور داشت که در حال حاضر اینترنت در ایران نقش بسیار مهمی از لحاظ امنیت فرهنگی ایفاء می‌کند. از نظر علمی افزایش توانایی دسترسی دانشجویان، اساتید، و محققان ایرانی به منابع الکترونیک و تماسهای علمی با دانشمندان دیگر کشورها کاملاً مرهون اینترنت دانشگاهیان است.

از نظر افزایش توان کسب آگاهیهای سیاسی و اجتماعی و دریافت آراء مختلف و امکان گفتگو نمی‌توان نقش اینترنت را انکار کرد. امروزه سایتهای مختلف ایرانی با تشکیل گروههای مباحثاتی بسیار جدید در مورد مسائل جهانی و ملی عرضه وسیعی را برای آگاهی جویی و اعلام نظرهای تخصصی و عمومی فراهم کرده‌اند (سیک، ۱۹۹۹). پیگیری نظرسنجی‌های اینترنتی در مورد انتخاب مجلس ششم، انتخاب رئیس مجلس، فایده یا ضرر ارتباط با آمریکا، انتخاب مهمترین شخصیت قرن اخیر ایران، نشان می‌دهد که اینترنت برای ایرانیان امکانات کاملاًمساعدی برای ابراز آزادانه عقاید و مشارکت سیاسی و فرهنگی فراهم آورده است. حتی برخی احزاب و داوطلبان نمایندگی برای تبلیغات انتخاباتی خود، از اینترنت استفاده کرده‌اند. به این ترتیب می‌توان نقش مهمی برای اینترنت در گسترش آزادیها و مشارکت سیاسی و دمکراسی فرهنگی قائل شد.

12-9-۱: معیارهای امنیت فرهنگی در سیاستگذاری

برای تحلیل فرآیند سیاستگذاری در مورد اینترنت در ایران، پاسخ به سؤالاتی در مورد آزادی بیان، کنترل جریان اطلاعات، قوانین مربوط و در یک بیان نظریه هنجاری حاکم بر رسانه‌های جدید ضروری است. این سؤالات به ۵ حیطه اصلی قابل تحلیل است:

حق ارتباط خصوصی

حق ارتباط ناشناس

حق رمزگذاری در ارتباط

معافیت کانال ارتباطی از مسئولیت محتوی

دسترسی عمومی و ارزان

با توجه به تحقیق محسنیان راد (۱۳۷۶) نظریه حاکم بر رسانه‌های مرسوم در ایران در سال ۱۳۷۶، آمیزه‌ای از نظریه مسئولیت اجتماعی، توسعهٔ بخش و ایدئولوژیک بوده است. تغییرات سیاسی سال ۷۶ به بعد نقش نظریه مسئولیت اجتماعی را تقویت کرده است. ولی در مورد اینترنت وضع کاملاً متفاوت است و حاکمیت تئوری آزادی‌گرا بر دسترسی و انتشار از طریق اینترنت کاملاً ملموس است. تا اواخر نیمه اول سال ۱۳۸۰، دولت هیچ گونه نظارت و دخالت ملموسی در مورد آن نداشته است. زیرا:

۱. قوانین مربوط به مطبوعات که عمده‌ترین قانون در حوزهٔ محدوده محدودیتهای آزادی بیان است شامل گفتار روی شبکه نمی‌شود.

۲. افراد، سازمانها و شرکتها امکان دسترسی به سرویس دهندگان اینترنت را از طریق خطوط تلفن دارند.

۳. برای دسترسی به اینترنت هیچ گونه مجوز دولتی لازم نیست.

۴. دسترسی به اینترنت با پست یا پست الکترونیک نیاز به هیچ گونه تأییدای از طرف هیچ سازمان دولتی ندارد.

۵. هیچ دستورالعمل یا بخشنامه‌ای وجود ندارد که سرویس دهندگان را موظف کند اطلاعات مربوط به مشترکان، کاربران و محتوای داده‌های تبادل شده را به سازمانهای دولتی ارائه دهند.

۶. هیچ قانون یا دستورالعملی برای منع رمزگذاری محتوای داده‌های مبادله شده وجود ندارد.

۷. هیچ قانونی وجود ندارد که سرویس‌دهندگان ملزم به کنترل محتوا نماید.

۸. هیچ سیاست و اقدام مشخصی در مورد سانسور یا بلوک کردن سایتها، گروههای مباحثاتی و آدرسهای پست الکترونیکی وجود ندارد و ایران فاقد یک بارو و سیستم فیلترینگ ملی و مرکزی است.

۹. هیچ قانونی وجود ندارد که سرویس‌دهندگان را مسئول محتوای سایتهای روی سرویس بداند.

۱۰. کافه‌های اینترنتی به سرعت در حال رشد است و هیچ قانون خاصی برای نحوهٔ تأسیس و نحوهٔ اداره وجود ندارد، این کافه‌ها تابع قانون اماکن عمومی هستند.

۱۱. خدمات اینترنت در ایران به سرعت ارزان شده است و دولت برای دسترسیهای دانشگاهی سوبسید قابل ملاحظه‌ای را پذیرفته است. سیاست گسترش فیبر نوری و افزایش ظرفیت تبادل بین‌المللی داده‌ها از سیاستهای جاری دولت است.

۲-9-12: مشکلات فعلی سیاستگذاری در امنیت فرهنگی و اینترنت

در جریان سیاستگذاری برای اینترنت در کشور ما موانع جدی وجود دارد. این موانع را می‌توان به شرح زیر مرتب کرد:

۱. فقدان استراتژی فرهنگی کلان در مورد صنایع فرهنگی جدید

۲. فقدان سیاست ملی مخابراتی

- روشن نبودن اولویت‌بندی در مورد گسترش تلفن ثابت، همراه و مخابرات داده‌ها

- روشن نبودن میزان ظرفیت دولت در پذیرش مشارکت بخش خصوصی در وارد کردن و توزیع اینترنت

۳. فقدان سیاست روشن گمرکی

در مورد مجاز یا ممنوع بودن واردات تجهیزات، دریافت و ارسال ماهواره‌ای برای خدمات اینترنت

۴. وجود رقابت تخریبی میان ارگانهای عمومی

متولی اینترنت در کشور از جمله فیزیک نظری، شرکت مخابرات، صدا و سیما

۵. فقدان سیاست ملی اطلاع‌رسانی

علی‌الرغم تشکیل شورای عالی اطلاع‌رسانی این شورا به سیاست‌گذاری تفصیلی و اعلام شده‌ای در زمینهٔ اطلاع‌رسانی دست نیافته است. وجود مدعیان و متولیان متعدد در مدیریت ملی اطلاعات و عدم تفکیک وظایف آنها موجب کندی و بلکه عقب‌ماندگی جدی ایران در تولید و سازماندهی اطلاعات الکترونیک شده است. امروزه به علت عدم سازماندهی اطلاعات علمی کشور، دسترسی به کتابخانه کنگرهٔ آمریکا بسیار ساده‌تر و مفیدتر از دسترسی به کتابخانه‌های ملی، مجلس و دانشگاه تهران است.

۶. فقدان سیاستهای نظارتی و امنیتی

هم اکنون بایستی روشن شود که مسئول حفاظت از داده‌های موجود در سامانه‌های نظامی، امنیتی، اقتصادی کشور کیست؟

چه سازمانی مسئول جلوگیری، پیشگیری و پیگیری حملات الکترونیکی و نقش امنیت سامانه‌های ملی است؟

چه سازمانی متولی سیاستگذاری و تعیین موارد ممنوعه در تبادل داده‌ها است؟

کدام سازمان مسئول نظارت بر کیفیت فرهنگی و محتوای سایتهای تولیدشده و قابل دسترس در کشور است؟

۱۲-۹-۳: ملاحظات فرهنگی در سیاستگذاری

به نظر می‌رسد ملاحظات اساسی فرهنگی در سیاستگذاری آتی در مورد اینترنت در ایران به شرح زیر می‌باشد:

- گسترش اینترنت در کشور ایران باید به گونه‌ای باشد که به خلاقیت‌گستری مدد رسانده، نه اینکه موجبات خلاقیت‌زدایی را فراهم آورد. سیاستگذاری در مورد توسعه اینترنت نباید به توسعه مصرف یا باز تولید محتوای آن محدود شود، بلکه باید گسترش فرهنگ بومی و مذهبی و مقاومت فرهنگی را به دنبال داشته باشد.

- بیش و پیش از توسعه اینترنت باید به نظام تولید و سازماندهی الکترونیک اطلاعات علمی، اداری و مالی براساس استانداردهای قابل تبادل در شبکهٔ اهتمام داشت و بودجه‌های کلانی را به این امر اختصاص داد.

- تدوین و اجرای قوانین موردنیاز و روزآمد در حوزهٔ ارتباطات شبکه‌ای بسیار اساسی است این قوانین به خصوص موضوع حقوق تکثیر و مالکیت آثار فرهنگی و نرم‌افزارها و اطلاعات الکترونیک تأثیر قطعی در تشویق تولید فرهنگی بر روی شبکه دارد.

- در سیاستگذاری فرهنگی باید چگونگی کاربرد تکنولوژی توسط مؤسسات فرهنگی و تأثیر آن را بر مخاطبان در نظر گرفت. معلوم نیست که هرگونه استفاده از تکنولوژی جدید لزوم به افزایش تأثیرپذیری مخاطبان منجر شود.

- نظام نظارت فرهنگی بر محتوای داده‌های مبادله شده و ثبت ملی نقش اساسی در پیشگیری از گسترش فساد، تهدیدات امنیتی، رسوخ جاسوسی و خرابکاری الکترونیک و عملیات روانی دارد.

10-12-جمع‌بندی

به نظر می‌رسد تهدید اصلی و بالفعل کشور در مورد اینترنت، فقدان گفتمان امنیتی در مورد این پدیده است. اینترنت که بطور بالقوه می‌تواند هم تهدید و هم فرصتی طلایی برای امنیت فرهنگی و سیاسی باشد، به وسیله‌ای برای فشار سیاسی و اقتصادی تبدیل شده است.

فقدان دانش جامع‌نگر در مورد صورت مسأله و عدم وجود مطالعات سیاستگذاری مقایسه‌ای در کشور، حاکمیت روش آزمون خطا و اعمال سلایق فردی و سازمانی را به دنبال داشته است.

مسئولیت‌پذیری دولت در سیاستگذاری علمی، کارشناسانه و همه سو نگر و بهره‌گیری از تمام توان علمی کشور، شرط اصلی تحقق بیشترین منافع و کمترین آسیبها از صنعت اینترنت در ایران است.

برای جلوگیری از اثرات مخرب ارتباط با پایگاههای ضداخلاقی باید به سمتی حرکت کنیم که سایتهای مفید، جذابیت پیدا کند. یعنی ابتدا در حد توان باید در زمینهٔ سایتهای مفید و درعین حال جذاب سرمایه‌گذاری کنیم. از طرف دیگر هم باید موارد منفی را سد کنیم، یعنی از نفوذ سایتهای مخرب، به این سو جلوگیری کنیم. چون در کشورهای غربی، مثل انگلیس، مسأله استفاده از سایتهای مستهجن توسط دانش‌آموزان مدارس به صورت یک بحران درآمده است و آنها به این نتیجه رسیده‌اند که دو راه در پیش رو دارند: بستن راه‌های دسترسی به اینترنت یا کنترل آن بطور کلی آنچه را که از مطالب بالا می‌توان نتیجه‌گیری کرد می‌توان در پنج بند خلاصه نمود:

۱) اینترنت به عنوان یک پدیدهٔ مثبت ارزیابی می‌شود.

۲) سوءاستفاده از شبکهٔ جهانی نباید مانع از بهره‌برداری از این رسانه دو سویه شود.

۳) امکان گزینش اطلاعات سالم و ارائه آن برای عموم وجود دارد.

۴) امکان کنترل این شبکه تا حدود زیادی با روشهای فنی، سازمانی و فرهنگی وجود دارد.

۵) همه کشورهای جهان در پی مسدود کردن نفوذ اطلاعات آلوده هستند و سعی در تدوین قوانین و مقرراتی برای جلوگیری از بهره‌برداری سوء از شبکهٔ جهانی‌اند.

در هر حال نیاز اساسی جوامع در حال رشد به دریافت اطلاعات مفید و سازنده را نمی‌توان نادیده گرفت. و این در حالی است که از تخریب مبانی اعتقادی و اجتماعی جامعه نیز می‌باید با حساسیت تمام جلوگیری کرد. نفوذ اطلاعات آلوده به شبکه‌های اطلاع‌رسانی به مثابه سرایت سموم مهلک و خطرناک به شبکهٔ آب آشامیدنی سالم شهری است. این درحالی است که آلاینده‌های روحی و اخلاقی ضرباتی دهشتناکتر و جبران‌ناپذیرتر از آلاینده‌های جسمی بر پیکر اجتماعات انسانی وارد می‌سازند

بخش سیزدهم

امنیت تجهیزات شبکه

برای تامین امنیت بر روی یک شبکه، یکی از بحرانی ترین و خطیرترین مراحل، تامین امنیت دسترسی و کنترل تجهیزات شبکه است. تجهیزاتی همچون مسیریاب، سوئیچ یا دیوارهای آتش.

اهمیت امنیت تجهیزات به دو علت اهمیت ویژه‌ای می‌یابد :

الف – عدم وجود امنیت تجهیزات در شبکه به نفوذگران به شبکه اجازه می‌دهد که با دستیابی به تجهیزات امکان پیکربندی آنها را به گونه‌ای که تمایل دارند آن سخت‌افزارها عمل کنند، داشته باشند. از این طریق هرگونه نفوذ و سرقت اطلاعات و یا هر نوع صدمه دیگری به شبکه، توسط نفوذگر، امکان‌پذیر خواهد شد.

ب – برای جلوگیری از خطرهای DoS (Denial of Service) تأمین امنیت تجهزات بر روی شبکه الزامی است. توسط این حمله‌ها نفوذگران می‌توانند سرویس‌هایی را در شبکه از کار بیاندازند که از این طریق در برخی موارد امکان دسترسی به اطلاعات با دور زدن هر یک از فرایندهای AAA فراهم می‌شود.

در این بخش اصول اولیه امنیت تجهیزات مورد بررسی اجمالی قرار می‌گیرد. عناوین برخی از این موضوعات به شرح زیر هستند :

- امنیت فیزیکی و تأثیر آن بر امنیت کلی شبکه
- امنیت تجهیزات شبکه در سطوح منطقی
- بالابردن امنیت تجهیزات توسط افزونگی در سرویس‌ها و سخت‌افزارها

موضوعات فوق در قالب دو جنبه اصلی امنیت تجهیزات مورد بررسی قرار می‌گیرند :

- امنیت فیزیکی
- امنیت منطقی

1-13 – امنیت فیزیکی

امنیت فیزیکی بازه وسیعی از تدابیر را در بر می‌گیرد که استقرار تجهیزات در مکان‌های امن و به دور از خطر حملات نفوذگران و استفاده از افزونگی در سیستم از آن جمله‌اند. با استفاده از افزونگی، اطمینان از صحت عملکرد سیستم در صورت ایجاد و رخداد نقص در یکی از تجهیزات (که توسط عملکرد مشابه سخت‌افزار و یا سرویس‌دهنده مشابه جایگزین می‌شود) بدست می‌آید.

در بررسی امنیت فیزیکی و اعمال آن، ابتدا باید به خطرهایی که از این طریق تجهزات شبکه را تهدید می‌کنند نگاهی داشته باشیم. پس از شناخت نسبتاً کامل این خطرها و حمله‌ها می‌توان به راه‌حل‌ها و ترفندهای دفاعی در برار این‌گونه حملات پرداخت.

1-1-13 – افزونگی در محل استقرار شبکه

یکی از راه‌کارها در قالب ایجاد افزونگی در شبکه‌های کامپیوتری، ایجاد سیستمی کامل، مشابه شبکه‌ی اولیه‌ی در حال کار است. در این راستا، شبکه‌ی ثانویه‌ی، کاملاً مشابه شبکه‌ی اولیه، چه از بعد تجهیزات و چه از بعد کارکرد، در محلی که می‌تواند از نظر جغرافیایی با شبکه‌ی اول فاصله‌ای نه چندان کوتاه نیز داشته باشد برقرار می‌شود. با استفاده از این دو سیستم مشابه، علاوه بر آنکه در صورت رخداد وقایعی که کارکرد هریک از این دو شبکه را به طور کامل مختل می‌کند (مانند زلزله) می‌توان از شبکه‌ی دیگر به طور کاملاً جایگزین استفاده کرد، در استفاده‌های روزمره نیز در صورت ایجاد ترافیک سنگین بر روی شبکه، حجم ترافیک و پردازش بر روی دو شبکه‌ی مشابه پخش می‌شود تا زمان پاسخ به حداقل ممکن برسد.

با وجود آنکه استفاده از این روش در شبکه‌های معمول که حجم جندانی ندارند، به دلیل هزینه‌های تحمیلی بالا، امکان‌پذیر و اقتصادی به نظر نمی‌رسد، ولی در شبکه‌های با حجم بالا که قابلیت اطمینان و امنیت در آنها از اصول اولیه به حساب می‌آیند از الزامات است.

13-1-2 – توپولوژی شبکه

طراحی توپولوژیکی شبکه، یکی از عوامل اصلی است که در زمان رخداد حملات فیزیکی می‌تواند از خطای کلی شبکه جلوگیری کند.

در این مقوله، سه طراحی که معمول هستند مورد بررسی قرار می‌گیرند :

الف – طراحی سری : در این طراحی با قطع خط تماس میان دو نقطه در شبکه، کلیه سیستم به دو تکه منفصل تبدیل شده و امکان سرویس دهی از هریک از این دو ناحیه به ناحیه دیگر امکان پذیر نخواهد بود.

ب – طراحی ستاره‌ای : در این طراحی، در صورت رخداد حمله فیزیکی و قطع اتصال یک نقطه از خادم اصلی، سرویس‌دهی به دیگر نقاط دچار اختلال نمی‌گردد. با این وجود از آنجاییکه خادم اصلی در این میان نقش محوری دارد، در صورت اختلال در کارایی این نقطه مرکزی، که می‌تواند بر اثر حمله فیزیکی به آن رخ دهد، ارتباط کل شبکه دچار اختلال می‌شود، هرچند که با درنظر گرفتن افزونگی برای خادم اصلی از احتمال چنین حالتی کاسته می‌شود.

ج – طراحی مش : در این طراحی که تمامی نقاط ارتباطی با دیگر نقاط در ارتباط هستند، هرگونه اختلال فیزیکی در سطوح دسترسی منجر به اختلال عملکرد شبکه نخواهد شد، با وجود آنکه زمان‌بندی سرویس‌دهی را دچار اختلال خواهد کرد. پیاده‌سازی چنین روش با وجود امنیت بالا، به دلیل محدودیت‌های اقتصادی، تنها در موارد خاص و بحرانی انجام می‌گیرد.

13-1-3 – محل‌های امن برای تجهیزات

در تعیین یک محل امن برای تجهیزات دو نکته مورد توجه قرار می‌گیرد :

- یافتن مکانی که به اندازه کافی از دیگر نقاط مجموعه متمایز باشد، به گونه‌ای که هرگونه نفوذ در محل آشکار باشد.
- در نظر داشتن محلی که در داخل ساختمان یا مجموعه‌ای بزرگتر قرار گرفته است تا تدابیر امنیتی بکارگرفته شده برای امن سازی مجموعه‌ی بزرگتر را بتوان برای امن سازی محل اختیار شده نیز به کار گرفت.

با این وجود، در انتخاب محل، میان محلی که کاملاً جدا باشد (که نسبتاً پرهزینه خواهد بود) و مکانی که درون محلی نسبتاً عمومی قرار دارد و از مکان‌های بلااستفاده سود برده است (که باعث ایجاد خطرهای امنیتی می گردد)، می‌توان اعتدالی منطقی را در نظر داشت.

در مجموع می‌توان اصول زیر را برای تضمین نسبی امنیت فیزیکی تجهیزات در نظر داشت :

- محدود سازی دسترسی به تجهیزات شبکه با استفاده از قفل‌ها و مکانیزم‌های دسترسی دیجیتالی به همراه ثبت زمان‌ها، مکان‌ها و کدهای کاربری دسترسی‌های انجام شده.
- استفاده از دوربین‌های پایش در ورودی محل‌های استقرار تجهیزات شبکه و اتاق‌های اتصالات و مراکز پایگاه‌های داده.
- اعمال ترفندهایی برای اطمینان از رعایت اصول امنیتی.

13-1-4 – انتخاب لایه کانال ارتباطی امن

با وجود آنکه زمان حمله‌ی فیزیکی به شبکه‌های کامپیوتری، آنگونه که در قدیم شایع بوده، گذشته است و در حال حاضر تلاش اغلب نفوذگران بر روی به دست گرفتن کنترل یکی از خادم‌ها و سرویس‌دهنده‌های مورد اطمینان شبکه معطوف شده است، ولی گونه‌ای از حمله‌ی فیزیکی کماکان دارای خطری بحرانی است.

عمل شنود بر روی سیم‌های مسی، چه در انواع Coax و چه در زوج‌های تابیده، هم‌اکنون نیز از راه‌های نفوذ به شمار می‌آیند. با استفاده از شنود می‌توان اطلاعات بدست آمده از تلاش‌های دیگر برای نفوذ در سیستم‌های کامپیوتری را گسترش داد و به جمع‌بندی مناسبی برای حمله رسید. هرچند که می‌توان سیم‌ها را نیز به گونه‌ای مورد محافظت قرار داد تا کمترین احتمال برای شنود و یا حتی تخریب فیزیکی وجود داشته باشد، ولی در حال حاضر، امن ترین روش ارتباطی در لایه‌ی فیزیکی، استفاده از فیبرهای نوری است. در این روش به دلیل نبود سیگنال‌های الکتریکی، هیچگونه تشعشعی از نوع الکترومغناطیسی وجود ندارد، لذا امکان استفاده از روش‌های معمول شنود به پایین‌ترین حد خود نسبت به استفاده از سیم در ارتباطات می‌شود.

13-1-5 – منابع تغذیه

از آنجاکه داده‌های شناور در شبکه به منزله‌ی خون در رگهای ارتباطی شبکه هستند و جریان آنها بدون وجود منابع تغذیه، که با فعال نگاه‌داشتن نقاط شبکه موجب برقراری این جریان هستند، غیر ممکن است، لذا چگونگی چینش و نوع منابع تغذیه و قدرت آنها نقش به سزایی در این میان بازی می‌کنند. در این مقوله توجه به دو نکته زیر از بالاترین اهمیت برخوردار است :

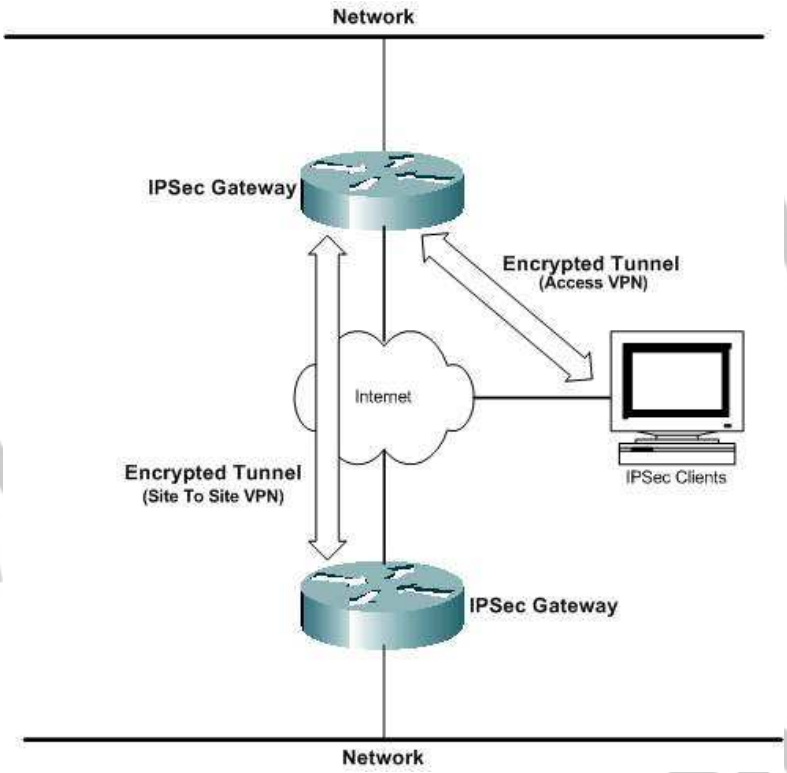
- طراحی صحیح منابع تغذیه در شبکه بر اساس محل استقرار تجهیزات شبکه. این طراحی باید به گونه‌ای باشد که تمامی تجهیزات فعال شبکه، برق مورد نیاز خود را بدون آنکه به شبکه‌ی تامین فشار بیش‌اندازه‌ای (که باعث ایجاد اختلال در عملکرد منابع تغذیه شود) وارد شود، بدست آورند.
- وجود منبع یا منابع تغذیه پشتیبان به گونه‌ای که تعداد و یا نیروی پشتیبانی آنها به نحوی باشد که نه تنها برای تغذیه کل شبکه در مواقع نیاز به منابع تغذیه پشتیبان کفایت کند، بلکه امکان تامین افزونگی مورد نیاز برای تعدادی از تجهیزات بحرانی درون شبکه را به صورت منفرد فراهم کند.

13-1-6 – عوامل محیطی

یکی از نکات بسیار مهم در امن سازی فیزیکی تجهیزات و منابع شبکه، امنیت در برار عوامل محیطی است. نفوذگران در برخی از موارد با تاثیرگذاری بر روی این عوامل، باعث ایجاد اختلال در عملکرد شبکه می‌شوند. از مهمترین عواملی در هنگام بررسی امنیتی یک شبکه رایانه‌ای باید درنظر گرفت می‌توان به دوعامل زیر اشاره کرد :

- احتمال حریق (که عموماً غیر طبیعی است و منشآ انسانی دارد)
- زلزله، طوفان و دیگر بلایای طبیعی

با وجود آنکه احتمال رخداد برخی از این عوامل، مانند حریق، را می‌توان تا حدود زیادی محدود نمود، ولی تنها راه حل عملی و قطعی برای مقابله با چنین وقایعی، با هدف جلوگیری در اختلال کلی در عملکرد شبکه، وجود یک سیستم کامل پشتیبان برای کل شبکه است. تنها با استفاده از چنین سیستم پشتیبانی است که می‌توان از عدم اختلال در شبکه در صورت بروز چنین وقعایعی اطمینان حاصل کرد.



13-2 – امنیت منطقی

امنیت منطقی به معنای استفاده از روش‌هایی برای پایین آوردن خطرات حملات منطقی و نرم‌افزاری بر ضد تجهیزات شبکه است. برای مثال حمله به مسیریاب‌ها و سوئیچ‌های شبکه بخش مهمی از این گونه حملات را تشکیل می‌دهند. در این بخش به عوامل و مواردی که در اینگونه حملات و ضد حملات مورد نظر قرار می‌گیرند می‌پردازیم.

13-2-1 – امنیت مسیریاب‌ها

حملات ضد امنیتی منطقی برای مسیریاب‌ها و دیگر تجهیزات فعال شبکه، مانند سوئیچ‌ها، را می‌توان به سه دسته‌ی اصلی تقسیم نمود :

- حمله برای غیرفعال سازی کامل
- حمله به قصد دستیابی به سطح کنترل
- حمله برای ایجاد نقص در سرویس‌دهی

طبیعی است که راه‌ها و نکاتی که در این زمینه ذکر می‌شوند مستقیماً به امنیت این عناصر به تنهایی مربوط بوده و از امنیت دیگر مسیرهای ولو مرتبط با این تجهیزات منفک هستند. لذا تأمین امنیت تجهیزات فعال شبکه به معنای تآمین قطعی امنیت کلی شبکه نیست، هرچند که عملاً مهمترین جنبه‌ی آنرا تشکیل می‌دهد.

13-2-2 – مدیریت پیکربندی

یکی از مهمترین نکات در امینت تجهیزات، نگاهداری نسخ پشتیبان از پرونده‌ها مختص پیکربندی است. از این پرونده‌ها که در حافظه‌های گوناگون این تجهیزات نگاهداری می‌شوند، می‌توان در فواصل زمانی مرتب یا تصادفی، و یا زمانی که پیکربندی تجهیزات تغییر می‌یابند، نسخه پشتیبان تهیه کرد.

با وجود نسخ پشتیبان، منطبق با آخرین تغییرات اعمال شده در تجهیزات، در هنگام رخداد اختلال در کارایی تجهزات، که می‌تواند منجر به ایجاد اختلال در کل شبکه شود، در کوتاه‌ترین زمان ممکن می‌توان با جایگزینی آخرین پیکربندی، وضعیت فعال شبکه را به آخرین حالت بی‌نقص پیش از اختلال بازگرداند. طبیعی است که در صورت بروز حملات علیه بیش از یک سخت‌افزار، باید پیکربندی تمامی تجهیزات تغییریافته را بازیابی نمود.

نرم‌افزارهای خاصی برای هر دسته از تجهیزات مورد استفاده وجود دارند که قابلیت تهیه نسخ پشتیبان را فاصله‌های زمانی متغیر دارا می‌باشند. با استفاده از این نرم‌افزارها احتمال حملاتی که به سبب تآخیر در ایجاد پشتیبان بر اثر تعلل عوامل انسانی پدید می‌آید به کمترین حد ممکن می‌رسد.

13-2-3 – کنترل دسترسی به تجهیزات

دو راه اصلی برای کنترل تجهزات فعال وجود دارد :

- کنترل از راه دور
- کنترل از طریق درگاه کنسول

در روش اول می‌توان با اعمال محدودیت در امکان پیکربندی و دسترسی به تجهیزات از آدرس‌هایی خاص یا استانداردها و پروتکل‌های خاص، احتمال حملات را پایین آورد.

در مورد روش دوم، با وجود آنکه به نظر می‌رسد استفاده از چنین درگاهی نیاز به دسترسی فیزکی مستقیم به تجهیزات دارد، ولی دو روش معمول برای دسترسی به تجهیزات فعال بدون داشتن دسترسی مستقیم وجود دارد. لذا در صورت عدم کنترل این نوع دسترسی، ایجاد محدودیت‌ها در روش اول عملاً امنیت تجهیزات را تآمین نمی‌کند.

برای ایجاد امنیت در روش دوم باید از عدم اتصال مجازی درگاه کنسول به هریک از تجهیزات داخلی مسیریاب، که امکان دسترسی از راه‌دور دارند، اطمینان حاصل نمود.

13-2-4 – امن سازی دسترسی

علاوه بر پیکربندی تجهیزات برای استفاده از Authentication، یکی دیگر از روش‌های معمول امن‌سازی دسترسی، استفاده از کانال رمز شده در حین ارتباط است. یکی از ابزار معمول در این روش SSH(Secur Shell) است. SSH ارتباطات فعال را رمز کرده و احتمال شنود و تغییر در ارتباط که از معمول‌ترین روش‌های حمله هستند را به حداقل می‌رساند.

از دیگر روش‌های معمول می‌توان به استفاده از کانال‌های VPN مبتنی بر IPsec اشاره نمود. این روش نسبت به روش استفاده از SSH روشی با قابلیت اطمینان بالاتر است، به گونه‌ای که اغلب تولیدکنندگان تجهیزات فعال شبکه، خصوصاً تولید کنندگان مسیریاب‌ها، این روش را مرجح می‌دانند.

13-2-5 – مدیریت رمزهای عبور

مناسب‌ترین محل برای ذخیره رمزهای عبور بر روی خادم Authentication است. هرچند که در بسیاری از موارد لازم است که بسیاری از این رموز بر روی خود سخت‌افزار نگاه‌داری شوند. در این صورت مهم‌ترین نکته به یاد داشتن فعال کردن سیستم رمزنگاری رموز بر روی مسیریاب یا دیگر سخت‌افزارهای مشابه است.

13-3 – ملزومات و مشکلات امنیتی ارائه دهندگان خدمات

زمانی که سخن از ارائه دهندگان خدمات و ملزومات امنیتی آنها به میان می‌آید، مقصود شبکه‌های بزرگی است که خود به شبکه‌های رایانه‌ای کوچکتر خدماتی ارائه می‌دهند. به عبارت دیگر این شبکه‌های بزرگ هستند که با پیوستن به یکدیگر، عملاً شبکه‌ی جهانی اینترنت کنونی را شکل می‌دهند. با وجود آنکه غالب اصول امنیتی در شبکه‌های کوچکتر رعایت می‌شود، ولی با توجه به حساسیت انتقال داده در این اندازه، ملزومات امنیتی خاصی برای این قبیل شبکه‌ها مطرح هستند.

13-3-1 – قابلیت‌های امنیتی

ملزومات مذکور را می‌توان، تنها با ذکر عناوین، به شرح زیر فهرست نمود :

۱ – قابلیت بازداری از حمله و اعمال تدابیر صحیح برای دفع حملات

۲ – وجود امکان بررسی ترافیک شبکه، با هدف تشخیص بسته‌هایی که به قصد حمله بر روی شبکه ارسال می‌شوند. از آنجاییکه شبکه‌های بزرگتر نقطه تلاقی مسیرهای متعدد ترافیک بر روی شبکه هستند، با استفاده از سیستم‌های IDS بر روی آنها، می‌توان به بالاترین بخت برای تشخیص حملات دست یافت.

۳ – قابلیت تشخیص منبع حملات. با وجود آنکه راه‌هایی از قبیل سرقت آدرس و استفاده از سیستم‌های دیگر از راه دور، برای حمله کننده و نفوذگر، وجود دارند که تشخیص منبع اصلی حمله را دشوار می‌نمایند، ولی استفاده از سیستم‌های ردیابی، کمک شایانی برای دست یافتن و یا محدود ساختن بازه‌ی مشکوک به وجود منبع اصلی می‌نماید. بیشترین تأثیر این مکانیزم زمانی است که حملاتی از نوع DoS از سوی نفوذگران انجام می‌گردد.

13-3-2 – مشکلات اعمال ملزومات امنیتی

با وجود لزوم وجود قابلیت‌هایی که بطور اجمالی مورد اشاره قرار گرفتند، پیاده‌سازی و اعمال آنها همواره آسان نیست.

یکی از معمول‌ترین مشکلات، پیاده‌سازی IDS است. خطر یا ترافیکی که برای یک دسته از کاربران به عنوان حمله تعبیر می‌شود، برای دسته‌ای دیگر به عنوان جریان عادی داده است. لذا تشخیص این دو جریان از یکدیگر بر پیچیدگی IDS افزوده و در اولین گام از کارایی و سرعت پردازش ترافیک و بسته‌های اطلاعاتی خواهد کاست. برای جبران این کاهش سرعت تنها می‌توان متوسل به تجهیزات گران‌تر و اعمال سیاست‌های امنیتی پیچیده‌تر شد.

با این وجود، با هرچه بیشتر حساس شدن ترافیک و جریان‌های داده و افزایش کاربران، و مهاجرت کاربردهای متداول بر روی شبکه‌های کوچکی که خود به شبکه‌های بزرگتر ارائه دهنده خدمات متصل هستند، تضمین امنیت، از اولین انتظاراتی است که از اینگونه شبکه‌ها می‌توان داشت.

فهرست منابع مورد استفاده

۱) Internet

۲) Bulbrook Dale – مترجم مهرداد توانا- سال ۱۳۸۳- برنامه نویسی سیستمهای بی سیم و موبایل WAP-

انتشارات روزنه.

۳) محسنیان‌راد، مهدی. (۱۳۷۶). انتقاد در مطبوعات ایران. مرکز مطالعات و تحقیقات رسانه‌ها، انتشار محدود.

۴) مولانا، حمید. (۱۳۷۹). جریان بین‌المللی اطلاعات. ترجمهٔ یونس شکرخواه. تهران: مرکز مطالعات

۵) رابرت، ماندل. (۱۳۷۷). چهره متغیر امنیت ملی. تهران: پژوهشکده مطالعات راهبردی.