امنیت در شبکه با نگرشي به شبکه هاي بیسیم

شرکت فنـاوري اطلاعات
دفتر تحقـیق و توسعه
گروه مطالـعاتي امنیت

محقق وگردآورنده
مـهدي منـصوري

سرپرست تحقیق
مهنـدس آقامیرزایي

اداره کل توسعه و مهندسي

اسفندمذار ۱۳۸۴

فهرست

عنوان | صفحه

مقدمه:

اينترنت يك شبكة عظيم اطلاع‌رساني و يك بانك وسيع اطلاعاتي است كه در آينده نزديك دسترسي به آن براي تك‌تك افراد ممكن خواهد شد. كارشناسان ارتباطات، بهرهگيري از اين شبكه را يك ضرورت در عصر اطلاعات مي‌دانند.
اين شبكه كه از هزاران شبكه كوچكتر تشكيل شده، فارغ از مرزهاي جغرافيايي، سراسر جهان را به هم مرتبط ساخته است. طبق آخرين آمار بيش از ششصد ميليون رايانه از تمام نقاط جهان در اين شبكة گسترده به يكديگر متصل شده‌اند كه اطلاعات بي‌شماري را در تمامي زمينه‌ها از هر سنخ و نوعي به اشتراك گذاشته‌اند. گفته مي‌شود نزديك به يكصد ميليارد صفحه اطلاعات با موضوعات گوناگون از سوي افراد حقيقي و حقوقي روي اين شبكه قرار داده شده است.
اين اطلاعات با سرعت تمام در بزرگراههاي اطلاعاتي بين كاربران رد و بدل مي‌شود و تقريباً هيچ گونه محدوديت و كنترلي بر وارد كردن يا دريافت كردن داده‌ها اعمال نمي‌شود. حمايت از جريان آزاد اطلاعات، گسترش روزافزون فنآوري اطلاعات و بسترسازي براي اتصال به شبكه‌هاي اطلاع‌رساني شعار دولتهاست. اين در حالي است كه گستردگي و تنوع اطلاعات آلوده روي اينترنت، موجب بروز نگراني در بين كشورهاي مختلف شده است. انتشار تصاوير مستهجن، ايجاد پايگاههايي با مضامين پورنوگرافي و سايتهاي سوءاستفاده از كودكان و انواع قاچاق در كشورهاي پيشرفته صنعتي بخصوص در خاستگاه اين شبكة جهاني يعني آمريكا، كارشناسان اجتماعي را بشدت نگران كرده، به گونه‌اي كه هيأت حاكمه را مجبور به تصويب قوانيني مبني بر كنترل اين شبكه در سطح آمريكا نموده است. هشدار، جريمه و بازداشت براي برپاكنندگان پايگاههاي مخرب و فسادانگيز تدابيري است كه كشورهاي مختلف جهان براي مقابله با آثار سوء اينترنت اتخاذ كرده‌اند.
ترس و بيم از تخريب مباني اخلاقي و اجتماعي، ناشي از هجوم اطلاعات آلوده و مخرب از طريق اينترنت، واكنشي منطقي است، زيرا هر جامعه‌اي چهارچوبهاي اطلاعاتي خاص خود را دارد و طبيعي است كه هر نوع اطلاعاتي كه اين حد و مرزها را بشكند مي‌تواند سلامت و امنيت جامعه را به خطر اندازد. علي‌الرغم وجود جنبه‌اي مثبت شبكه‌هاي جهاني، سوء استفاده از اين شبكه‌هاي رايانه‌اي توسط افراد بزهكار، امنيت ملي را در كشورهاي مختلف با خطر روبرو ساخته است. از اين رو بكارگيري فيلترها و فاير والهاي مختلف براي پيشگيري از نفوذ داده‌هاي مخرب و مضر و گزينش اطلاعات سالم در اين شبكه‌ها رو به افزايش است. خوشبختانه با وجود هياهوي بسياري كه شبكة اينترنت را غيرقابل كنترل معرفي مي‌كند، فناوري لازم براي كنترل اين شبكه و انتخاب اطلاعات سالم روبه گسترش وتكامل است

۱-امنيت شبكه‌هاي اطلاعاتي و ارتباطي

۱-۱: اهميت امنيت شبكه :

چنانچه به اهميت شبكه‌هاي اطلاعاتي (الكترونيكي) و نقش اساسي آن دريافت اجتماعي آينده پي برده باشيم، اهميت امنيت اين شبكه‌ها مشخص مي‌گردد. اگر امنيت شبكه برقرار نگردد، مزيتهاي فراوان آن نيز به خوبي حاصل نخواهد شد و پول و تجارت الكترونيك، خدمات به كاربران خاص، اطلاعات شخصي، اطلاعاتي عمومي و نشريات الكترونيك همه و همه در معرض دستكاري و سوءاستفاده‌هاي مادي و معنوي هستند. همچنين دستكاري اطلاعات- به عنوان زيربناي فكري ملت‌ها توسط گروههاي سازماندهي شده بين‌المللي، به نوعي مختل ساختن امنيت ملي و تهاجم عليه دولت‌ها و تهديدي ملي محسوب مي‌شود. براي كشور ما كه بسياري از نرم‌افزارهاي پايه از قبيل سيستم عامل و نرم‌افزارهاي كاربردي و اينترنتي، از طريق واسطه‌ها و شركتهاي خارجي تهيه مي‌شود، بيم نفوذ از طريق راههاي مخفي وجود دارد. اكنون كه كه بانكها و بسياري از نهادها و دستگاههاي ديگر از طريق شبكة به فعاليت مي‌پردازند، جلوگيري از نفوذ عوامل مخرب در شبكه بصورت مسئله‌اي استراتژيك درخواهد آمد كه نپرداختن به آن باعث ايراد خساراتي خواهد شد كه بعضاً جبران‌ناپذير خواهد بود. چنانچه يك پيغام خاص، مثلاً از طرف شركت مايكروسافت، به كليه سايتهاي ايراني ارسال شود و سيستم عاملها در واكنش به اين پيغام سيستمها را خراب كنند و از كار بيندازند، چه ضررهاي هنگفتي به امنيت و اقتصاد مملكت وارد خواهد شد؟ نكته جالب اينكه بزرگترين شركت توليد نرم‌افزارهاي امنيت شبكه، شركت چك پوينت است كه شعبة اصلي آن در اسرائيل مي‌باشد. مسأله امنيت شبكة براي كشورها، مسأله‌اي استراتژيك است؛ بنابراين كشور ما نيز بايد به آخرين تكنولوژيهاي امنيت شبكه مجهز شود و از آنجايي كه اين تكنولوژيها به صورت محصولات نرم‌افزاري قابل خريداري نيستند، پس مي‌بايست محققين كشور اين مهم را بدست بگيرند و در آن فعاليت نمايند.
امروزه اينترنت آنقدر قابل دسترس شده كه هركس بدون توجه به محل زندگي، مليت، شغل و زمان ميتواند به آن راه يابد و از آن بهره ببرد. همين سهولت دسترسي آن را در معرض خطراتي چون گم شدن، ربوده شدن، مخدوش شدن يا سوءاستفاده از اطلاعات موجود در آن قرار مي‌دهد. اگر اطلاعات روي كاغذ چاپ شده بود و در قفسه‌اي از اتاقهاي محفوظ اداره مربوطه نگهداري مي‌شد، براي دسترسي به آنها افراد غيرمجاز مي‌بايست از حصارهاي مختلف عبور مي‌كردند، اما اكنون چند اشاره به كليدهاي رايانه‌اي براي اين منظور كافي است..

۱-۲: سابقه امنيت شبكه

اينترنت در سال ۱۹۶۹ بصورت شبكه‌هاي بنام آرپانت كه مربوط به وزارت دفاع آمريكا بود راه‌اندازي شد. هدف اين بود كه با استفاده از رايانه‌هاي متصل به هم، شرايطي ايجاد شود كه حتي اگر، بخشهاي عمده‌اي از سيستم اطلاعاتي به هر دليلي از كار بيفتد، كل شبكه بتواند به

كار خود ادامه دهد، تا اين اطلاعات حفظ شود. از همان ابتدا، فكر ايجاد شبكه، براي جلوگيري از اثرات مخرب حملات اطلاعاتي بود.
در سال ۱۹۷۱ تعدادي از رايانه‌هاي دانشگاهها و مراكز دولتي به اين شبكه متصل شدند و محققين از اين طريق شروع به تبادل اطلاعات كردند.
با بروز رخدادهاي غيرمنتظره در اطلاعات، توجه به مسأله امنيت بيش از پيش اوج گرفت.
در سال ۱۹۸۸، آرپانت براي اولين بار با يك حادثه امنيتي سراسري در شبكه، مواجه شد كه بعداً، «كرم موريس» نام گرفت. رابرت موريس كه يك دانشجو در نيويورك بود، برنامه‌هايي نوشت كه مي‌توانست به يك رايانه‌اي ديگر راه يابد و در آن تكثير شود و به همين ترتيب به رايانه‌هاي ديگر هم نفوذ كند و بصورت هندسي تكثير شود. آن زمان ۸۸۰۰۰ رايانه به اين شبكه وصل بود. اين برنامه سبب شد طي مدت كوتاهي ده درصد از رايانه‌هاي متصل به شبكه در آمريكا از كار بيفتد.
به دنبال اين حادثه، بنياد مقابله با حوادث امنيتي (IRST) شكل گرفت كه در هماهنگي فعاليتهاي مقابله با حملات ضد امنيتي، آموزش و تجهيز شبكه‌ها و روشهاي پيشگيرانه نقش مؤثري داشت. با رايج‌تر شدن و استفاده عام از اينترنت، مسأله امنيت خود را بهتر و بيشتر نشان داد. از جمله اين حوادث، اختلال در امنيت شبكه، WINK/OILS WORM در سال ۱۹۸۹، Sniff packet در سال ۱۹۹۴ بود كه مورد اخير از طريق پست الكترونيك منتشر مي‌شد و باعث افشاي اطلاعات مربوط به اسامي شماره رمز كاربران مي‌شد. از آن زمان حملات امنيتي- اطلاعاتي به شبكه‌ها و شبكه جهاني روزبه‌روز افزايش يافته است.
گرچه اينترنت در ابتدا، با هدف آموزشي و تحقيقاتي گسترش يافت، امروزه كاربردهاي تجاري، پزشكي، ارتباطي و شخصي فراواني پيدا كرده است كه ضرورت افزايش ضريب اطمينان آن را بيش از پيش روشن نموده است.

۲- جرائم رايانه‌اي و اينترنتي

ويژگي برجسته فناوري اطلاعات، تأثيري است كه بر تكامل فناوري ارتباطات راه دور گذاشته و خواهد گذاشت. ارتباطات كلاسيك همچون انتقال صداي انسان، جاي خود را، به مقادير وسيعي از داده‌ها، صوت، متن، موزيك، تصاوير ثابت و متحرك داده است. اين تبادل و تكامل نه تنها بين انسانها بلكه مابين انسانها و رايانه‌ها، و همچنين بين خود رايانه‌ها نيز وجود دارد. استفاده وسيع از پست الكترونيك، و دستيابي به اطلاعات از طريق وب‌سايتهاي متعدد در اينترنت نمونه‌هايي از اين پيشرفتها مي‌باشد كه جامعه را بطور پيچيده‌اي دگرگون ساخته‌اند. سهولت در دسترسي و جستجوي اطلاعات موجود در سيستمهاي رايانه‌اي توأم با امكانات عملي نامحدود در مبادله و توزيع اطلاعات، بدون توجه به فواصل جغرافيايي، منجر به رشد سرسام‌آور مقدار اطلاعات موجود در آگاهي كه مي‌توان از آن بدست آورد، شده است. اين اطلاعات موجب افزايش تغييرات اجتماعي و اقتصادي پيش‌بيني نشده گرديده است. اما پيشرفتهاي مذكور جنبة خطرناكي نيز دارد كه پيدايش انواع جرايم و همچنين بهره‌برداري از فناوري جديد در ارتكاب جرايم بخشي از آن به شمار مي‌رود. بعلاوه عواقب و پيامدهاي رفتار مجرمانه مي‌تواند خيلي بيشتر از قبل و دور از تصور باشد چون كه محدوديتهاي جغرافيايي يا مرزهاي ملي آن را محدود نمي‌كنند. فناوري جديد مفاهيم قانوني موجود را دچار چالشهايي ساخته است. اطلاعات و ارتباطات راه دور به راحت‌ترين وجه در جهان جريان پيدا كرده و مرزها ديگر موانعي بر سر اين جريان به شمار نمي‌روند. جنايتكاران غالباً در مكانهايي به غير از جاههايي كه آثار و نتايج اعمال آنها ظاهر مي‌شود، قرار دارند. سوءاستفاده گسترده مجرمين، به ويژه گروههاي جنايتكار سازمان نيافته از فناوري اطلاعات سبب گشته است كه سياستگذاران جنايي اغلب كشورهاي جهان با استفاده از ابزارهاي سياست جنايي درصدد مقابله با آنها برآيند. تصويب كنوانسيون جرايم رايانه‌اي در اواخر سال ۲۰۰۱ و امضاي آن توسط ۳۰ كشور پيشرفته، تصويب قوانين مبارزه با اين جرايم توسط قانون‌گذاران داخلي و تشكيل واحدهاي مبارزه با آن در سازمان پليس بيشتر كشورهاي پيشرفته و تجهيز آنها به جديدترين سخت‌افزارها و نرم‌افزارهاي كشف اين گونه جرايم و جذب و بكارگيري بهترين متخصصين در واحدهاي مذكور، بخشي از اقدامات مقابله‌اي را تشكيل مي‌دهد.

۲-۱: پيدايش جرايم رايانه‌اي

در مورد زمان دقيق پيدايش جرم رايانه‌اي نمي‌توان اظهارنظر قطعي كرد. اين جرم زائيده تكنولوژي اطلاعاتي و انفورماتيكي است، بنابراين بطور منظم بعد از گذشت مدت كوتاهي از شيوع و كاربرد تكنولوژي اطلاعات، باب سوءاستفاده نيز قابل طرح است. شيوع استعمال اين تكنولوژي و برابري كاربران آن حداقل در چند كشور مطرح جهان بصورت گسترده، امكان بررسي اولين مورد را دشوار مي‌سازد. در نهايت آن چه مبرهن است اينكه در جامعه آمريكا رويس موجب شد براي اولين بار اذهان متوجه سوءاستفاده‌هاي رايانه‌اي شود.

۲-۲: قضيه رويس

آلدون رويس حسابدار يك شركت بود. چون به گمان وي، شركت حق او را پايمال كرده بود،

بنابراين با تهيه برنامه‌اي، قسمتي از پولهاي شركت را اختلاس كرد. انگيزة رويس در اين كار انتقامگيري بود.
مكانيزم كار بدين گونه بود كه شركت محل كار وي يك عمدهفروش ميوه و سبزي بود. محصولات متنوعي را از كشاورزان مي‌خريد و با استفاده از تجهيزات خود از قبيل كاميونها، انبار و بسته‌بندي و سرويس‌دهي به گروه هاي فروشندگان، آنها را عرضه مي‌كرد. به دليل وضعيت خاص اين شغل، قيمتها در نوسان بود و ارزيابي امور تنها مي‌توانست از عهدة رايانه برآيد تا كنترل محاسبات اين شركت عظيم را عهده‌دار شود. كليه امور حسابرسي و ممیزي اسناد و مدارك و صورت حسابها به صورت اطلاعات مضبوط در نوارهاي الكترونيكي بود.
رويس در برنامه‌ها، دستورالعمل‌هاي اضافي را گنجانده بود و قيمت كالاها را با ظرافت خاصي تغيير مي‌داد. با تنظيم درآمد اجناس وي مبلغي را كاهش مي‌داد و مبالغ حاصله را به حسابهاي مخصوص واريز مي‌كرد. بعد در زمانهاي خاص چكي به نام يكي از هفده شركت جعلي و ساختگي خودش صادر و مقداري از مبالغ را برداشت مي‌كرد. بدين ترتيب وي توانست در مدت ۶ سال بيش از يك ميليون دلار برداشت كند. اما او بر سر راه خودش مشكلي داشت و آن اين بود كه مكانيسمي براي توقف عملكرد سيستم نمي‌توانست بينديشد. بنابراين در نهايت خود را به مراجع قضايي معرفي و به جرم خود اعتراض كرد و به مدت ده سال به زندان محكوم شد. از اين جا بود كه مبحث جديدي به نام جرم رايانه‌اي ايجاد شد.

۲-۳: تعريف جرم رايانه‌اي

تاكنون تعريفهاي گوناگوني از جرم رايانه‌اي از سوي سازمانها، متخصصان و برخي قوانين ارائه شده كه وجود تفاوت در آنها بيانگر ابهامات موجود در ماهيت و تعريف اين جرائم است. جرم رايانه‌اي يا جرم در فضاي مجازي (ساير جرايم) داراي دو معني و مفهوم است. در تعريف مضيق، جرم رايانه‌اي صرفاً عبارت از جرايمي است كه در فضاي سايبر رخ مي‌دهد. از اين نظر جرايمي مثل هرزنگاري، افترا، آزار و اذيت سوءاستفاده از پست الكترونيك و ساير جرايمي كه در آنها رايانه به عنوان ابزار و وسيله ارتكاب جرم بكار گرفته مي‌شود، در زمرة جرم رايانه‌اي قرار نمي‌گيرند.
در تعريف موسع از جرم رايانه‌اي هر فعل و ترك فعلي كه در اينترنت يا از طريق آن يا با اينترنت يا از طريق اتصال به اينترنت، چه بطور مستقيم يا غيرمستقيم رخ مي‌دهد و قانون آن را ممنوع كرده و براي آن مجازات در نظر گرفته شده است جرم رايانه‌اي ناميده مي‌شود. براين اساس اينگونه جرايم را مي‌توان به سه دسته تقسيم نمود:
دسته اول: جرايمي هستند كه در آنها رايانه و تجهيزات جانبي آن موضوع جرم واقع مي‌شوند. مانند سرقت، تخريب و غيره
دسته دوم: جرايمي هستند كه در آنها رايانه به عنوان ابزار وسيله توسط مجرم براي ارتكاب جرم بكار گرفته مي‌شود.
دسته سوم: جرايمي هستند كه مي‌توان آنها را جرايم رايانه‌اي محض ناميد. اين نو ع از جرايم كاملاً با جرايم كلاسيك تفاوت دارند و در دنياي مجازي به وقوع مي‌پيوندند اما آثار آنها در دنياي واقعي ظاهر مي‌شود. مانند دسترسي غيرمجاز به سيستم‌هاي رايانه‌اي.

۲-۴: طبقه‌بندي جرايم رايانه‌اي

طبقه‌بندي‌هاي مختلفي از جرايم رايانه‌اي توسط مراجع مختلف انجام گرفته است. براي آشنايي شما با آنها موارد مهم بشرح زير اكتفا مي‌شود.

۲-۴-۱: طبقه‌بندي OECDB

در سال ۱۹۸۳ «او.اي.سي.دي.بي» مطالعه امكان پذيري اعمال بين‌المللي و هماهنگي قوانين كيفري را به منظور حل مسئله جرم يا سوءاستفاده‌هاي رايانه‌اي متعهد شد. اين سازمان در سال ۱۹۸۶ گزارشي تحت عنوان جرم رايانه‌اي، تحليل سياستهاي قانوني منتشر ساخت كه به بررسي قوانين موجود و پيشنهادهاي اصلاحي چند كشور عضو پرداخته و فهرست حداقل سوءاستفاده‌هايي را پيشنهاد كرده بود كه كشورهاي مختلف بايد با استفاده از قوانين كيفري، مشمول ممنوعيت و مجازات قرار دهند. بدين گونه اولين تقسيم‌بندي از جرايم رايانه‌اي در سال ۱۹۸۶ ارائه شد و طي آن پنج دسته اعمال را مجرمانه تلقي كرد و پيشنهاد كرد در قوانين ماهوي ذكر شود. اين پنج دسته عبارتند از:

الف: ورود، تغيير، پاك كردن و يا متوقف‌سازي داده‌هاي رايانه‌اي و برنامه‌هاي رايانه‌اي كه بطور ارادي با قصد انتقال غيرقانوني وجوه يا هر چيز باارزش ديگر صورت گرفته باشد.

ب: ورود، تغيير، پاك كردن، و يا متوقف‌سازي داده‌هاي رايانه‌اي و برنامه‌هاي رايانه‌اي كه بصورت عمدي و به قصد ارتكاب جعل صورت گرفته باشند. يا هرگونه مداخله ديگر در سيستمهاي رايانه‌اي كه بصورت عمدي و با قصد جلوگيري از عملكرد سيستم رايانه‌اي و يا ارتباطات صورت گرفته باشد.

ج: ورود، تغيير، پاك كردن و متوقف‌سازي داده‌هاي رايانه‌اي و يا برنامه‌هاي رايانه‌اي.

د: تجاوز به حقوق انحصاري مالك يك برنامة رايانه‌اي حفاظت شده با قصد بهره‌برداري تجاري از برنامه‌ها و ارائه آن به بازار.

ه- دستيابي يا شنود در يك سيستم رايانه‌اي و يا ارتباطي كه آگاهانه و بدون كسب مجوز از فرد مسئول سيستم مزبور يا تخطي از تدابير امنيتي و چه با هدف غير شرافتمندانه و يا موضوع صورت گرفته باشد.

۲-۴-۲: طبقه‌بندي شوراي اروپا:

كميتة منتخب جرايم رايانه‌اي شوراي اروپا، پس از بررسي نظرات «او.اي.سي.دي.بي» و نيز بررسي هاي حقوقي- فني دو ليست تحت عناوين ليست حداقل و ليست اختياري را به كميته وزراء پيشنهاد داد و آنان نيز تصويب كردند. اين ليستها بدين شرح هستند:

- ليست اختياري:

الف: كلاهبرداري رايانه‌اي
ب: جعل رايانه‌اي

ج: خسارت زدن به داده‌هاي رايانه‌اي يا برنامه‌هاي رايانه‌اي
د: دستيابي غيرمجاز
ه: ايجاد مجدد و غيرمجاز يك برنامة رايانه‌اي حمايت شده
و: ايجاد مجدد غيرمجاز يك توپوگرافي.
- ليست اختياري:
الف: تغيير داده‌هاي رايانه‌اي و يا برنامه‌هاي رايانه‌اي
ب: جاسوسي رايانه‌اي
ج: استفاده غيرمجاز از رايانه
د: استفاده غيرمجاز از برنامة رايانه‌اي حمايت شده.

۲-۴-۳: طبقه‌بندي اينترپول:

سالهاست كه اينترپول در مبارزه با جرايم مرتبط با فناوري اطلاعات فعال مي‌باشد. اين سازمان با بهره‌گيري از كارشناسان و متخصصين كشورهاي عضو اقدام به تشكيل گروههاي كاري در اين زمينه كرده است. رؤساي واحدهاي مبارزه با جرايم رايانه‌اي كشورهاي باتجربه عضو سازمان در اين گروه كاري گردهم آمده‌اند.
گروههاي كاري منطقه‌اي در اروپا، آسيا، آمريكا و آفريقا مشغول به كارند. و زير نظر كميتة راهبردي جرايم فناوري اطلاعات، مستقر در دبيرخانة كل اينترپول فعاليت مي‌نمايند.
گروه كاري اروپايي اينترپول با حضور كارشناسان هلند، اسپانيا، بلژيك، فنلاند، فرانسه، آلمان، ايتاليا، سوئد و انگليس در سال ۱۹۹۰ تشكيل شد. اين گروهها هر سال سه بار تشكيل جلسه مي‌دهند و در ژانويه سال ۲۰۰۱ سي‌امين گردهمايي آن در دبيرخانه كل تشكيل گرديد.
تهيه كتابچة راهنماي پي‌جويي جرايم رايانه‌اي، كتاب و سي‌دي راهنماي جرايم رايانه‌اي، تشكيل دوره‌هاي آموزشي براي نيروهاي پليس در طول ۵ سال گذشته، تشكيل سيستم اعلام خطر كه مركب از سيستمهاي پاسخگوي شبانه‌روزي، نقاط تماس دائمي شبانه‌روزي، تبادل پيام بين‌المللي در قالب فرمهاي استاندارد در زمينة جرايم رايانه‌اي واقعه مي‌باشد و انجام چندين پروژه تحقيقاتي پيرامون موضوعات مرتبط با جرايم رايانه‌اي از جمله اقدامات گروه كاري مذكور مي‌باشد. گروه كار آمريكايي جرايم مرتبط با تكنولوژي اطلاعات مركب از كارشناسان و متخصصين كشورهاي كانادا، ايالات متحده، آرژانتين، شيلي، كلمبيا، جامائيكا و باهاماست.
گروه كاري آفريقايي جرايم مرتبط با تكنولوژي اطلاعات مركب از كارشناسان آفريقاي جنوبي، زيمبابوه، نامبيا، تانزانيا، اوگاندا، بوتسوانا، سوازيلند، زنگبار، لسوتو و رواندا در ژوئن سال ۱۹۹۸ تشكيل گرديد. آنها كارشان را با برگزاري يك دوره آموزشي آغاز نمودند و دومين دوره آموزشي آنها با مساعدت مالي سفارتخانه‌هاي انگليس برگزار شد.
گروه كاري جنوب اقيانوس آرام، و آسيا در نوامبر سال ۲۰۰۰ در هند تشكيل شد و كارشناساني از كشورهاي استراليا، چين، هنگ كنگ، هند، ژاپن، نپال، و سريلانكا عضو آن هستند. اين گروه كاري با الگو قرار دادن كميته راهبردي جرايم مربوط به فناوري اطلاعات به منظور ايجاد و هماهنگي ميان اقدامات گروههاي كاري منطقه‌اي در محل دبيرخانه كل اينترپول تشكيل گرديده است.
سازمان پليس جنايي بين‌المللي جرايم رايانه‌اي را به شرح زير طبقه‌بندي كرده است:

۱: دستيابي غيرمجاز
۱-۱: نفوذغيرمجاز
۱-۲: شنود غيرمجاز
۱-۳: سرقت زمان رايانه
۲: تغيير دادههاي رايانهاي
۲-۱: بمب منطقي
۲-۲: اسب تروا
۲-۳: ويروس رايانهاي
۲-۴: كرم رايانهاي
۳: كلاهبرداري رايانهاي
۳-۱: صندوقهاي پرداخت
۳-۲: جعل رايانهاي
۳-۳: ماشينهاي بازي
۳-۴: دستكاريها در مرحله ورودي/ خروجي
۳-۵: ابزار پرداخت (نقطه فروش)
۳-۶: سوءاستفاده تلفني
۴: تكثير غيرمجاز
۴-۱: بازيهاي رايانهاي
۴-۲: نرمافزارهاي ديگر
۴-۳: توپوگرافي نيمه هادي
۵: سابوتاژ رايانهاي
۵-۱: سختافزار
۵-۲: نرمافزار
۶: ساير جرائم رايانهاي
۶-۱: سيستمهاي تابلوي اعلانات الكترونيك
۶-۲: سرقت اسرار تجاري
۶-۳: ساير موضوعات قابل تعقيب

۲-۴-۴: طبقهبندي در كنوانسيون جرايم سايبرنتيك

اين كنوانسيون در اواخر سال ۲۰۰۱ به امضاي ۳۰ كشور پيشرفته رسيده است و داراي وظايف زيادر مي باشد:

الف :هماهنگ كردن اركان تشكيل دهنده جرم در حقوق جزاي ماهوي داخلي كشورها و مسائل مربوطه در بخش جرايم سايبراسپيس.

ب: فراهم آوردن اختيارات لازم آيين دادرسي كيفري داخلي براي پي‌جويي و تعقيب چنين جرائمي علاوه بر جرايم ديگر كه با استفاده از سيستمهاي رايانه‌اي ارتكاب مي‌يابند.

ج: تدوين سيستم سريع و مؤثر همكاري بين‌المللي

كنوانسيون بين‌المللي جرايم رايانه‌اي بوداپست (۲۰۰۱) جرم را موارد زير تعريف نموده است:

۱- نفوذ غيرمجاز به سيستمهاي رايانه‌اي
۲- شنود غيرمجاز اطلاعات و ارتباطات رايانه‌اي
۳- اخلال در داده‌هاي رايانه‌اي
۴- اخلال در سيستمهاي رايانه‌اي
۵- جعل رايانه‌اي
۶- كلاهبرداري رايانه‌اي
۷- سوءاستفاده از ابزارهاي رايانه‌اي
۸- هرزنگاري كودكان
۹- تكثير غيرمجاز نرم‌افزارهاي رايانه‌اي و نقض حقوق ادبي و هنري

۲-۵: شش نشانه از خرابكاران شبكه‌اي

۱: در صورت نفوذ يك خرابكار به شبكة شما ممكن است حساب بانكي‌تان تغيير كند.
۲: خرابكاران شبكه‌اي آن قدر تلاش مي‌كنند تا بالاخره موفق به ورود به اينترانت شما شوند. لازم به ذكر است كه در برخي موارد در صورتيكه يك خرابكار بتواند به حساب بانكي شما نفوذ كند فايل آن بطور خودكار بسته نمي‌شود.
۳: گاهي اوقات خرابكاران براي نفوذ به يك رايانه ناچارند كد جديدي به آن وارد كنند. براي اين كار لازم است رايانه دوباره راه‌اندازي شود. بنابراين راه‌اندازيهاي مجدد رايانه، كه بطور غيرمنتظره انجام مي‌شود، مي‌تواند نشانه‌اي از نفوذ خرابكاران شبكه‌اي به رايانه شما باشد.
۴: بعضي اوقات خرابكاران شبكه‌اي تنها با حذف بخشهايي از يك فايل مي‌توانند راه نفوذ خود در آن را مخفي نگه دارند. بنابراين قسمتهاي حذف شده از يك فايل مي‌تواند نشان‌دهندة مسير نفوذ خرابكاران شبكه‌اي به يك فايل از رايانه باشد.
۵: گاهي با اين كه انتظار مي‌رود ارتباط بين دو رايانه از طريق شبكه، در زمانهايي مشخص، بسيار كم باشد ترافيك زيادي در آن مسير ملاحظه مي‌شود. چه بسا خرابكاران شبكه‌اي در حال تلاش براي نفوذ به آن سيستمها باشند و همين امر موجب ترافيك سنگين بين آنها شود.
۶: بخشهايي در سيستم هر شركت وجود دارد كه جدا از بقيه سيستم بوده و تنها افراد معدودي به آن دسترسي دارند، گاهي مي‌توان خرابكاران شبكه‌اي را در چنين بخشهايي پيدا كرد.

۳ـ منشأ ضعف امنيتي در شبكه‌هاي بي‌سيم و خطرات معمول

خطر معمول در كليه‌ي شبكه‌هاي بي‌سيم مستقل از پروتكل و تكنولوژي مورد نظر، بر مزيت اصلي اين تكنولوژي كه همان پويايي ساختار، مبتني بر استفاده از سيگنال‌هاي راديويي به‌جاي سيم و كابل، استوار است. با استفاده از اين سيگنال‌ها و در واقع بدون مرز ساختن پوشش ساختار شبكه، نفوذگران قادرند در صورت شكستن موانع امنيتي نه‌چندان قدرتمند اين شبكه‌ها، خود را به‌عنوان عضوي از اين شبكه‌ها جازده و در صورت تحقق اين امر، امكان دست‌يابي به اطلاعات حياتي، حمله به سرويس دهندگان سازمان و مجموعه، تخريب اطلاعات، ايجاد اختلال در ارتباطات گره‌هاي شبكه با يكديگر، توليد داده‌هاي غيرواقعي و گمراه‌كننده، سوءاستفاده از پهناي‌باند مؤثر شبكه و ديگر فعاليت‌هاي مخرب وجود دارد. در مجموع، در تمامي دسته‌هاي شبكه‌هاي بي‌سيم، از ديد امنيتي حقايقي مشترک صادق است :

- تمامي ضعف‌هاي امنيتي موجود در شبكه‌هاي سيمي، در مورد شبكه‌هاي بي‌سيم نيز صدق مي‌كند. در واقع نه تنها هيچ جنبه‌يي چه از لحاظ طراحي و چه از لحاظ ساختاري، خاص شبكه‌هاي بي‌سيم وجود ندارد كه سطح بالاتري از امنيت منطقي را ايجاد كند، بلكه همان گونه كه ذكر شد مخاطرات ويژه‌اي را نيز موجب است.

- نفوذگران، با گذر از تدابير امنيتي موجود، مي‌توانند به‌راحتي به منابع اطلاعاتي موجود بر روي سيستم‌هاي رايانه‌اي دست يابند.

- اطلاعات حياتي‌يي كه يا رمز نشده‌اند و يا با روشي با امنيت پايين رمز شده‌اند، و ميان دو گره در شبكه‌هاي بي‌سيم در حال انتقال مي‌باشند، مي‌توانند توسط نفوذگران سرقت شده يا تغيير يابند.

- حمله‌هاي DoS به تجهيزات و سيستم‌هاي بي‌سيم بسيار متداول است.

- نفوذگران با سرقت كدهاي عبور و ديگر عناصر امنيتي مشابه كاربران مجاز در شبكه‌هاي بي‌سيم، مي‌توانند به شبكه‌ي مورد نظر بدون هيچ مانعي متصل گردند.

- با سرقت عناصر امنيتي، يک نفوذگر مي‌تواند رفتار يک كاربر را پايش كند. از اين طريق مي‌توان به اطلاعات حساس ديگري نيز دست يافت.

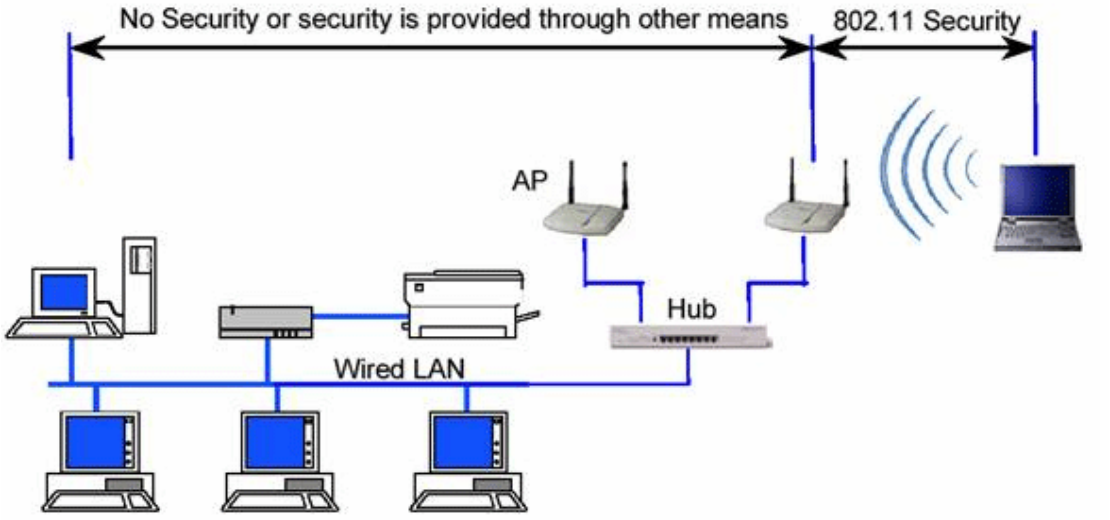
- كامپيوترهاي قابل حمل و جيبي، كه امكان و اجازه‌ي استفاده از شبكه‌ي بي‌سيم را دارند، به‌راحتي قابل سرقت هستند. با سرقت چنين سخت افزارهايي، مي‌توان اولين قدم براي نفوذ به شبكه را برداشت.

- يک نفوذگر مي‌تواند از نقاط مشترک ميان يک شبكه‌ي بي‌سيم در يک سازمان و شبكه‌ي سيمي آن (كه در اغلب موارد شبكه‌ي اصلي و حساس‌تري محسوب مي‌گردد) استفاده كرده و با نفوذ به شبكه‌ي بي‌سيم عملاً راهي براي دست‌يابي به منابع شبكه‌ي سيمي نيز بيابد.

- در سطحي ديگر، با نفوذ به عناصر كنترل كننده‌ي يک شبكه‌ي بي‌سيم، امكان ايجاد اختلال در عملكرد شبكه نيز وجود دارد.

۳-۱امنیت و پروتکلWEP

در اين قسمت بررسي روش‌ها و استانداردهاي امن‌سازي شبكه‌هاي محلي بي‌سيم مبتني بر استاندارد IEEE 802.11 را آغاز مي‌كنيم. با طرح قابليت‌هاي امنيتي اين استاندارد، مي‌توان از محدوديت‌هاي آن آگاه شد و اين استاندارد و كاربرد را براي موارد خاص و مناسب مورد استفاده قرار داد. استاندارد ۸۰۲,۱۱ سرويس‌هاي مجزا و مشخصي را براي تأمين يک محيط امن بي‌سيم در اختيار قرار مي‌دهد. اين سرويس‌ها اغلب توسط پروتكل WEP (Wired Equivalent Privacy) تأمين مي‌گردند و وظيفه‌ي آن‌ها امن‌سازي ارتباط ميان مخدوم‌ها و نقاط دسترسي بي‌سيم است. درک لايه‌اي كه اين پروتكل به امن‌سازي آن مي‌پردازد اهميت ويژه‌اي دارد، به عبارت ديگر اين پروتكل كل ارتباط را امن نكرده و به لايه‌هاي ديگر، غير از لايه‌ي ارتباطي بي‌سيم كه مبتني بر استاندارد ۸۰۲,۱۱ است، كاري ندارد. اين بدان معني است كه استفاده از WEP در يک شبكه‌ي بي‌سيم به‌معني استفاده از قابليت دروني استاندارد شبكه‌هاي محلي بي‌سيم است و ضامن امنيت كل ارتباط نيست زيرا امكان قصور از ديگر اصول امنيتي در سطوح بالاتر ارتباطي وجود دارد.



شكل ۱

شكل ۱ محدوده‌ی عملكرد استانداردهای امنیتی ۸۰۲,۱۱ (خصوصاً WEP) را نشان می‌دهد.

۳-۲قابليت‌ها و ابعاد امنيتي استاندارد ۸۰۲,۱۱

در حال حاضر عملاً تنها پروتكلي كه امنيت اطلاعات و ارتباطات را در شبكه‌هاي بي‌سيم بر اساس استاندارد ۸۰۲,۱۱ فراهم مي‌كند WEP است. اين پروتكل با وجود قابليت‌هايي كه دارد، نوع استفاده از آن همواره امكان نفوذ به شبكه‌هاي بي‌سيم را به نحوي، ولو سخت و پيچيده، فراهم مي‌كند. نكته‌يي كه بايد به‌خاطر داشت اين‌ست كه اغلب حملات موفق صورت گرفته در مورد شبكه‌هاي محلي بي‌سيم، ريشه در پيكربندي ناصحيح WEP در شبكه دارد. به عبارت ديگر اين پروتكل در صورت پيكربندي صحيح درصد بالايي از حملات را ناكام مي‌گذارد، هرچند كه في‌نفسه دچار نواقص و ايرادهايي نيز هست. بسياري از حملاتي كه بر روي شبكه‌هاي بي‌سيم انجام مي‌گيرد از سويي است كه نقاط دسترسي با شبكه‌ي سيمي داراي اشتراک هستند. به عبارت ديگر نفوذگران بعضاً با استفاده از راه‌هاي ارتباطي ديگري كه بر روي مخدوم‌ها و سخت‌افزارهاي بي‌سيم، خصوصاً مخدوم‌هاي

بي‌سيم، وجود دارد، به شبكه‌ي بي‌سيم نفوذ مي‌كنند كه اين مقوله نشان دهنده‌ي اشتراكي هرچند جزيي ميان امنيت در شبكه‌هاي سيمي و بي‌سيي است كه از نظر ساختاري و فيزيكي با يكديگر اشتراك دارند.

سه قابليت و سرويس پايه توسط IEEE براي شبكه‌هاي محلي بي‌سيم تعريف مي‌گردد :

· Authentication
· Confidentiality
· Integrity

3-2-1Authentication

هدف اصلي WEP ايجاد امكاني براي احراز هويت مخدوم بي‌سيم است. اين عمل كه در واقع كنترل دسترسي به شبكه‌ي بي‌سيم است. اين مكانيزم سعي دارد كه امكان اتصال مخدوم‌هايي را كه مجاز نيستند به شبكه متصل شوند از بين ببرد.

3-2-2-Confidentiality:

محرمانگي هدف ديگر WEP است. اين بُعد از سرويس‌ها و خدمات WEP با هدف ايجاد امنيتي در حدود سطوح شبكه‌هاي سيمي طراحي شده است. سياست اين بخش از WEP جلوگيري از سرقت اطلاعات در حال انتقال بر روي شبكه‌ي محلي بي‌سيم است.

3-2-3Integrity:

هدف سوم از سرويس‌ها و قابليت‌هاي WEP طراحي سياستي است كه تضمين كند پيام‌ها و اطلاعات در حال تبادل در شبكه، خصوصاً ميان مخدوم‌هاي بي‌سيم و نقاط دسترسي، در حين انتقال دچار تغيير نمي‌گردند. اين قابليت در تمامي استانداردها، بسترها و شبكه‌هاي ارتباطاتي ديگر نيز كموبيش وجود دارد.

۳-۳-خدمات ايستگاهي:

بر اساس اين استاندارد خدمات خاصي در ايستگاه‌هاي كاري پيادەسازي مي‌شوند. در حقيقت تمام ايستگاه‌هاي كاري موجود در يك شبكه محلي مبتني بر ۸۰۲,۱۱ و نيز نقاط دسترسي موظف هستند كه خدمات ايستگاهي را فراهم نمايند. با توجه به اينكه امنيت فيزيكي به منظور جلوگيري از دسترسي غير مجاز بر خلاف شبكه‌هاي سيمي، در شبكه‌هاي بي‌سيم قابل اعمال نيست استاندارد ۸۰۲,۱۱ خدمات هويت سنجي را به منظور كنترل دسترسي به شبكه تعريف مي‌نمايد.

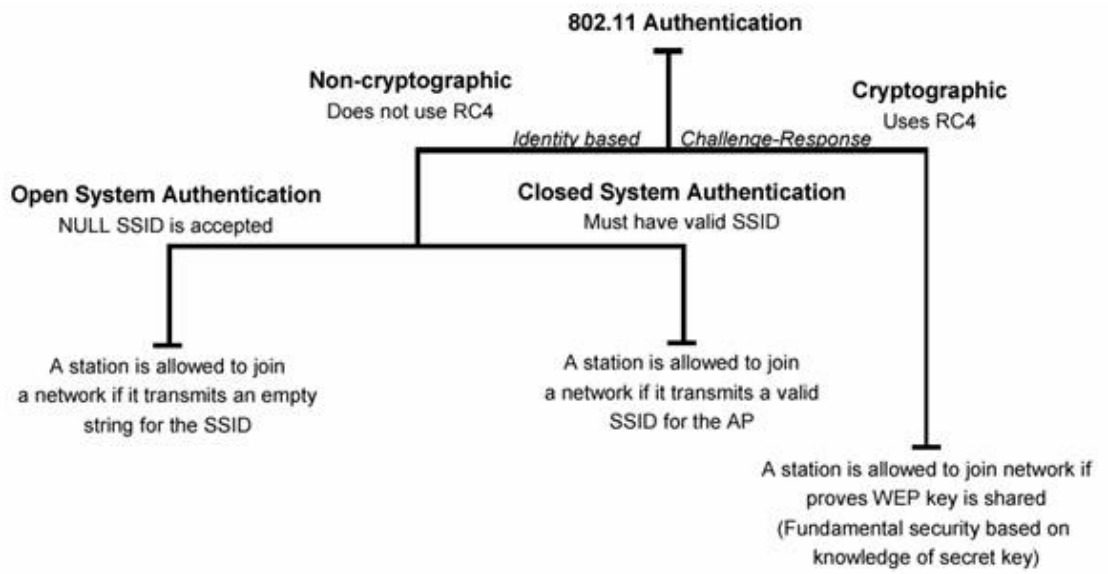
۳-۳-۱-هویت سنجی :

سرويس هويت سنجي به ايستگاه كاري امكان مي‌دهد كه ايستگاه ديگري را شناسايي نمايد. قبل از اثبات هويت ايستگاه كاري، آن ايستگاه مجاز نيست كه از شبكه بي‌سيم براي تبادل داده استفاده نمايد. در يك تقسيم بندي كلي ۸۰۲,۱۱ دو گونه خدمت هويت سنجي را تعريف مي‌كند:

Non-Cryptographic System Authentication-
Shared Key Authentication -

روش اول، متد پيش فرض است و يك فرآيند دو مرحله‌اي است. در ابتدا ايستگاهي كه مي‌خواهد توسط ايستگاه ديگر شناسايي و هويت سنجي شود يك فريم مديريتي هويت سنجي شامل شناسه ايستگاه فرستنده، ارسال مي‌كند. ايستگاه گيرنده نيز فريمي در پاسخ مي‌فرستد كه آيا فرستنده را مي‌شناسد يا خير. روش دوم كمي پيچيده‌تر است و فرض مي‌كند كه هر ايستگاه از طريق يك كانال مستقل و امن، يك كليد مشترك سّري دريافت كرده است. ايستگاه‌هاي كاري با استفاده از اين كليد مشترك و با بهره‌گيري از پروتكلي موسوم به WEP اقدام به هويت سنجي يكديگر مي‌نمايند. يكي ديگر از خدمات ايستگاهي خاتمه ارتباط يا خاتمه هويت سنجي است. با استفاده از اين خدمت، دسترسي ايستگاهي كه سابقاً مجاز به استفاده از شبكه بوده است، قطع مي‌گردد.
در يك شبكه بي‌سيم، تمام ايستگاه‌هاي كاري و ساير تجهيزات قادر هستند ترافيك داده‌اي را "بشنوند" – در واقع ترافيك در بستر امواج مبادله مي‌شود كه توسط تمام ايستگاه‌هاي كاري قابل دريافت است. اين ويژگي سطح امنيتي يك ارتباط بي‌سيم را تحت تأثير قرار مي‌دهد. به همين دليل در استاندارد ۸۰۲,۱۱ پروتكلي موسوم به WEP تعبيه شده است كه برروي تمام فريم‌هاي داده و برخي فريم‌هاي مديريتي و هويت سنجي اعمال مي‌شود. اين استاندارد در پي آن است تا با استفاده از اين الگوريتم سطح اختفاء وپوشش را معادل با شبكه‌هاي سيمي نمايد.

همانگونه كه كطرح شد استاندارد ۸۰۲,۱۱ دو روش براي احراز هويت كاربراني كه درخواست اتصال به شبكه‌ي بي‌سيم را به نقاط دسترسي ارسال مي‌كنند، دارد كه يک روش بر مبناي رمزنگاري‌ست و ديگري از رمزنگاري استفاده نمي‌كند.
شكل زير شَمايي از فرايند Authentication را در اين شبكه‌ها نشان مي‌دهد :



شكل 2

همان‌گونه كه در شكل ۲ نيز نشان داده شده است، يک روش از رمزنگاري RC4 استفاده مي‌كند و روش ديگر از هيچ تكنيک رمزنگاري‌اي استفاده نمي‌كند.

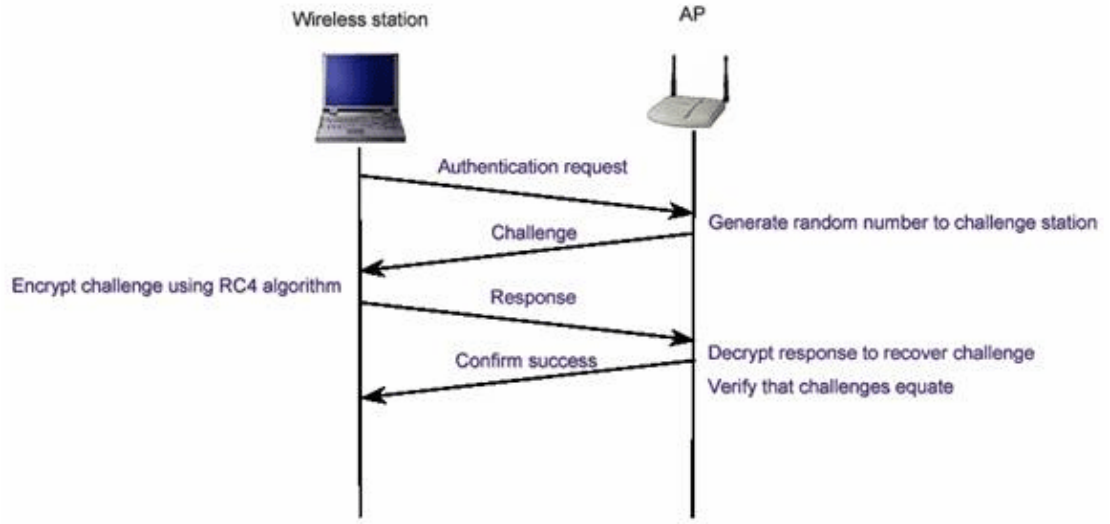
Authentication-3-3-1-1 بدون رمزنگاري (Non-Cryptographic System Authentication)

در روشي كه مبتني بر رمزنگاري نيست، دو روش براي تشخيص هويت مخدوم وجود دارد. در هر دو روش مخدوم متقاضي پيوستن به شبكه، درخواست ارسال هويت از سوي نقطه‌ي دسترسي را با پيامي حاوي يک SSID (Service Set Identifier) پاسخ مي‌دهد. در روش اول كه به Open System Authentication موسوم است، يک SSID خالي نيز براي دريافت اجازه‌ي اتصال به شبكه كفايت مي‌كند. در واقع در اين روش تمامي مخدوم‌هايي كه تقاضاي پيوستن به شبكه را به نقاط دسترسي ارسال مي‌كنند با پاسخ مثبت روبه‌رو مي‌شوند و تنها آدرس آن‌ها توسط نقطه‌ي دسترسي نگاهداري مي‌شود. به‌همين دليل به اين روش Authentication NULL نيز اطلاق مي‌شود.
در روش دوم از اين نوع، بازهم يک SSID به نقطه‌ي دسترسي ارسال مي‌گردد با اين تفاوت كه اجازه‌ي اتصال به شبكه تنها در صورتي از سوي نقطه‌ي دسترسي صادر مي‌گردد كه SSIDي ارسال شده جزو SSIDهاي مجاز براي دسترسي به شبكه باشند. اين روش به Authentication System Closed موسوم است.
نكته‌يي كه در اين ميان اهميت بسياري دارد، توجه به سطح امنيتي‌است كه اين روش در اختيار ما مي‌گذارد. اين دو روش عملاً روش امني از احراز هويت را ارايه نمي‌دهند و عملاً تنها راهي براي آگاهي نسبي و نه قطعي از هويت درخواست‌كننده هستند. با اين وصف از آن‌جايي‌كه امنيت در اين حالات تضمين شده نيست و معمولاً حملات موفق بسياري، حتي توسط نفوذگران كم‌تجربه و مبتدي، به شبكه‌هايي كه بر اساس اين روش‌ها عمل مي‌كنند، رخ مي‌دهد، لذا اين دو روش تنها در حالتي كاربرد دارند كه يا شبكه‌اي در حال ايجاد است كه حاوي اطلاعات حياتي نيست، يا احتمال رخداد حمله به آن بسيار كم است. هرچند كه با توجه

پوشش نسبتاً گسترده‌ي يک شبکه‌ي بي‌سيم – که مانند شبکه‌هاي سيمي امکان محدودسازي دسترسي به صورت فيزيکي بسيار دشوار است – اطمينان از شانس پايين رخدادن حملات نيز خود تضميني ندارد!

2-1-3-3-Authentication با رمزنگاري RC4 (shared key) (authentication

اين روش که به روش «کليد مشترک» نيز موسوم است، تکنيکي کلاسيک است که بر اساس آن، پس از اطمينان از اينکه مخدوم از کليدي سري آگاه است، هويتش تأييد مي‌شود. شکل ۳ زير اين روش را نشان مي‌دهد :



شکل 3

در اين روش، نقطه‌ي دسترسي (AP) يک رشته‌ي تصادفي توليد کرده و آن‌را به مخدوم مي‌فرستد. مخدوم اين رشته‌ي تصادفي را با کليدي از پيش تعيين شده (که کليد WEP نيز ناميده مي‌شود) رمز مي‌کند و حاصل را براي نقطه‌ي دسترسي ارسال مي‌کند. نقطه‌ي دسترسي به روش معکوس پيام دريافتي را رمزگشايي کرده و با رشته‌ي ارسال شده مقايسه مي‌کند. در صورت همساني اين دو پيام، نقطه‌ي دسترسي از اينکه مخدوم کليد صحيحي را در اختيار دارد اطمينان حاصل مي‌کند. روش رمزنگاري و رمزگشايي در اين تبادل روش RC4 است. در اين ميان با فرض اينکه رمزنگاري RC4 را روشي کاملاً مطمئن بدانيم، دو خطر در کمين اين روش است :

الف) در اين روش تنها نقطه‌ي دسترسي‌ست که از هويت مخدوم اطمينان حاصل مي‌کند. به بيان ديگر مخدوم هيچ دليلي در اختيار ندارد که بداند نقطه‌ي دسترسي‌يي که با آن در حال تبادل داده‌هاي رمزي است نقطه‌ي دسترسي اصلي‌ست.

ب) تمامي روش‌هايي که مانند اين روش بر پايه‌ي سئوال و جواب بين دو طرف، با هدف احراز هويت يا تبادل اطلاعات حياتي، قرار دارند با حملاتي تحت عنوان man-in-the-middle در خطر هستند. در اين دسته از حملات نفوذگر ميان دو طرف قرار مي‌گيرد و به‌گونه‌اي هريک از دو طرف را گمراه مي‌کند.

۳-۳-۲-اختفا اطلاعات (سرويس Privacy يا Confidentiality)

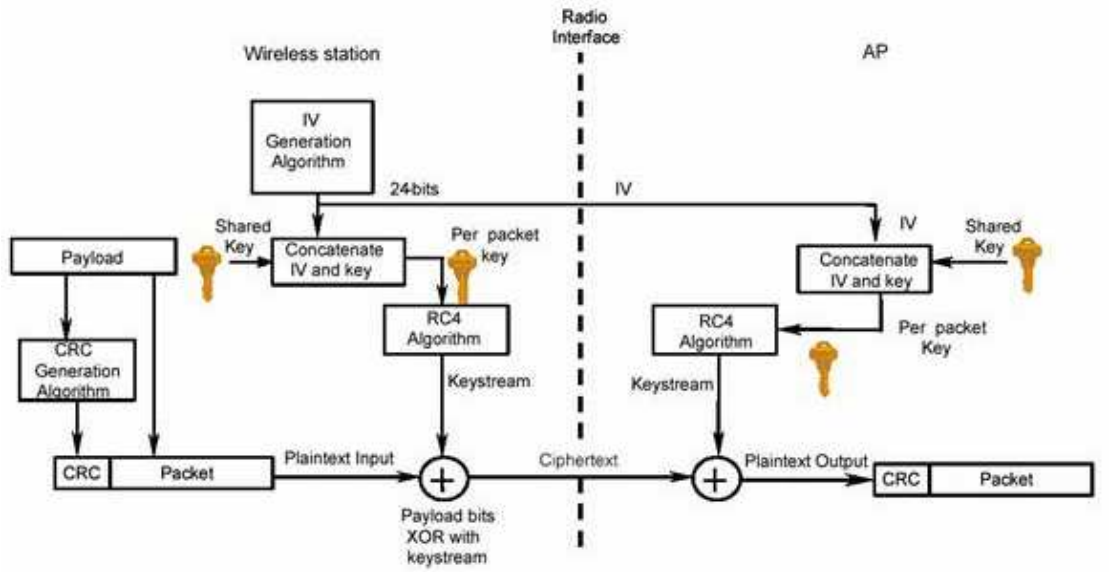
اين سرويس كه در حوزه‌هاي ديگر امنيتي اغلب به عنوان Confidentiality از آن ياد مي‌گردد به‌معناي حفظ امنيت و محرمانه نگاه‌داشتن اطلاعات كاربر يا گره‌هاي در حال تبادل اطلاعات با يكديگر است. براي رعايت محرمانگی عموماً از تكنيك‌هاي رمزنگاري استفاده مي‌گردد، به‌گونه‌يي‌كه در صورت شنود اطلاعات در حال تبادل، اين اطلاعات بدون داشتن كليدهاي رمز، قابل رمزگشايي نبوده و لذا براي شنودگر غيرقابل سوء استفاده است.

در استاندارد b۸۰۲,۱۱، از تكنيك‌هاي رمزنگاري WEP استفاده مي‌گردد كه برپايه‌ي RC4 است. RC4 يک الگوريتم رمزنگاري متقارن است كه در آن يک رشته‌ي نيمه تصادفي توليد مي‌گردد و توسط آن كل داده رمز مي‌شود. اين رمزنگاري بر روي تمام بسته‌ي اطلاعاتي پياده مي‌شود. به‌بيان ديگر داده‌هاي تمامي لايه‌هاي بالايي اتصال بي‌سيم نيز توسط اين روش رمز مي‌گردند، از IP گرفته تا لايه‌هاي بالاتري مانند HTTP. از آنجايي كه اين روش عملاً اصلي‌ترين بخش از اعمال سياست‌هاي امنيتي در شبكه‌هاي محلي بي‌سيم مبتني بر استاندارد b۸۰۲,۱۱ است، معمولاً به كل پروسه‌ي امن‌سازي اطلاعات در اين استاندارد به‌اختصار WEP گفته مي‌شود.

كليدهاي WEP اندازه‌هايي از ۴۰ بيت تا ۱۰۴ بيت مي‌توانند داشته باشند. اين كليدها با IV (مخفف Initialization Vector يا بردار اوليه) ۲۴ بيتي تركيب شده و يک كليد ۱۲۸ بيتي RC4 را تشكيل مي‌دهند. طبيعتاً هرچه اندازه‌ي كليد بزرگ‌تر باشد امنيت اطلاعات بالاتر است. تحقيقات نشان مي‌دهد كه استفاده از كليدهايي با اندازه‌ي ۸۰ بيت يا بالاتر عملاً استفاده از تكنيک brute-force را براي شكستن رمز غيرممكن مي‌كند. به عبارت ديگر تعداد كليدهاي ممكن براي اندازه‌ي ۸۰ بيت (كه تعدد آن‌ها از مرتبه‌ي ۲۴ است) به اندازه‌يي بالاست كه قدرت پردازش سيستم‌هاي رايانه‌يي كنوني براي شكستن كليدي مفروض در زماني معقول كفايت نمي‌كند.

هرچند كه در حال حاضر اكثر شبكه‌هاي محلي بي‌سيم از كليدهاي ۴۰ بيتي براي رمزكردن بسته‌هاي اطلاعاتي استفاده مي‌كنند ولي نكته‌يي كه اخيراً، بر اساس يک سري آزمايشات به دست آمده است، اين‌ست كه روش تأمين محرمانگی توسط WEP در مقابل حملات ديگري، غير از استفاده از روش brute-force، نيز آسيب‌پذير است و اين آسيب‌پذيري ارتباطي به اندازه‌ي كليد استفاده شده ندارد.

نمايي از روش استفاده شده توسط WEP براي تضمين محرمانگي در شكل۴ نمايش داده شده است :



شكل 4

۳-۳-۳-حفظ صحت اطلاعات (Integrity) :

مقصود از Integrity صحت اطلاعات در حين تبادل است و سياست‌هاي امنيتي‌اي كه Integrity را تضمين مي‌كنند روش‌هايي هستند كه امكان تغيير اطلاعات در حين تبادل را به كمترين ميزان تقليل مي‌دهند.

در استاندارد b۸۰۲,۱۱ نيز سرويس و روشي استفاده مي‌شود كه توسط آن امكان تغيير اطلاعات در حال تبادل ميان مخدوم‌هاي بي‌سيم و نقاط دسترسي كم مي‌شود. روش مورد نظر استفاده از يک كد CRC است. همان‌طور كه در شكل قبل نيز نشان داده شده است، يک CRC-32 قبل از رمزشدن بسته توليد مي‌شود. در سمت گيرنده، پس از رمزگشايي، CRC داده‌هاي رمزگشايي شده مجدداً محاسبه شده و با CRC نوشته شده در بسته مقايسه مي‌گردد كه هرگونه اختلاف ميان دو CRC به‌معناي تغيير محتويات بسته در حين تبادل است. متأسفانه اين روش نيز مانند روش رمزنگاري توسط RC4، مستقل از اندازه‌ي كليد امنيتي مورد استفاده، در مقابل برخي از حملات شناخته شده آسيب‌پذير است.

۳-۴ضعف‌هاي اوليه‌ي امنيتيWEP

متأسفانه استاندارد b۸۰۲,۱۱ هيچ مكانيزمي براي مديريت كليدهاي امنيتي ندارد و عملاً تمامي عملياتي كه براي حفظ امنيت كليدها انجام مي‌گيرد بايد توسط كساني كه شبكه‌ي بي‌سيم را نصب مي‌كنند به‌صورت دستي پيادسازي گردد. از آنجايي كه اين بخش از امنيت يكي از معضل‌هاي اساسي در مبحث رمزنگاري است، با اين ضعف عملاً روش‌هاي متعددي براي حمله به شبكه‌هاي بي‌سيم قابل تصور است. سهل انگاري‌هاي انجام‌شده از سوي كاربران و مديران شبكه مانند تغييرندادن كليد به‌صورت مداوم، لودادن كليد، استفاده از كليدهاي تكراري يا كليدهاي پيش فرض كارخانه و ديگر بي توجهي ها نتيجه يي جز درصد نسبتاً بالايي از حملات موفق به شبكه‌هاي بي‌سيم ندارد. اين مشكل از شبكه‌هاي بزرگ‌تر بيش‌تر خود را نشان مي‌دهد. حتي با فرض تلاش براي جلوگيري از رخداد چنين سهل‌انگاري‌هايي، زماني كه تعداد مخدوم‌هاي شبكه از حدي مي‌گذرد عملاً كنترل‌كردن اين تعداد بالا بسيار دشوار شده و گهگاه خطاهايي در گوشه و كنار اين شبكه‌ي نسبتاً بزرگ رخ مي دهد كه همان باعث رخنه در كل شبكه مي‌شود.

پايه‌ي امنيت در استاندارد ۸۰۲,۱۱ بر اساس پروتكل WEP استوار است. WEP در حالت استاندارد بر اساس كليدهاي ۴۰ بيتي براي رمزنگاري توسط الگوريتم RC4 استفاده مي‌شود، هرچند كه برخي از توليدكنندگان نگارش‌هاي خاصي از WEP را با كليدهايي با تعداد بيت‌هاي بيش‌تر پيادسازي كرده‌اند.
نكته‌يي كه در اين ميان اهميت دارد قائل شدن تمايز ميان نسبت بالارفتن امنيت و اندازه‌ي كليدهاست. با وجود آن كه با بالارفتن اندازه‌ي كليد (تا ۱۰۴ بيت) امنيت بالاتر مي‌رود، ولي از آن‌جاكه اين كليدها توسط كاربران و بر اساس يک كلمه‌ي عبور تعيين مي‌شود، تضميني نيست كه اين اندازه تماماً استفاده شود. از سوي ديگر همان‌طور كه در قسمت‌هاي پيشين نيز ذكر شد، دست‌يابي به اين كليدها فرايند چندان سختي نيست، كه در آن صورت ديگر اندازه‌ي كليد اهميتي ندارد.

متخصصان امنيت بررسي‌هاي بسياري را براي تعيين حفره‌هاي امنيتي اين استاندارد انجام داده‌اند كه در اين راستا خطراتي كه ناشي از حملاتي متنوع، شامل حملات غيرفعال و فعال است، تحليل شده است.

حاصل بررسي‌هاي انجام شده فهرستي از ضعف‌هاي اوليه‌ي اين پروتكل است :

۱. استفاده از كليدهاي ثابت WEP(Initialization Vector -IV)
۲.استفاده از CRC رمزنشده

۳-۴-۱-استفاده از كليدهاي ثابتWEP :

يكي از ابتدايي‌ترين ضعف‌ها كه عموماً در بسياري از شبكه‌هاي محلي بي‌سيم وجود دارد استفاده از كليدهاي مشابه توسط كاربران براي مدت زمان نسبتاً زياد است. اين ضعف به دليل نبود يک مكانيزم مديريت كليد رخ مي‌دهد. براي مثال اگر يک كامپيوتر كيفي يا جيبي كه از يک كليد خاص استفاده مي‌كند به سرقت برود يا براي مدت زماني در دسترس نفوذگر باشد، كليد آن به‌راحتي لو رفته و با توجه به تشابه كليد ميان بسياري از ايستگاه‌هاي كاري عملاً استفاده از تمامي اين ايستگاه‌ها ناامن است.
از سوي ديگر با توجه به مشابه بودن كليد، در هر لحظه كانال‌هاي ارتباطي زيادي توسط يک حمله نفوذپذير هستند.

Initialization Vector – IV:

اين بردار كه يک فيلد ۲۴ بيتي است در قسمت قبل معرفي شده است. اين بردار به صورت متني ساده فرستاده مي شود. از آن‌جايي‌كه كليدي كه براي رمزنگاري مورد استفاده قرار مي‌گيرد بر اساس IV توليد مي شود، محدوده‌ي IV عملاً نشان‌دهنده‌ي احتمال تكرار آن و در نتيجه احتمال توليد كليدهاي مشابه است. به عبارت ديگر در صورتي كه IV كوتاه باشد در مدت زمان كمي مي‌توان به كليدهاي مشابه دست يافت.
اين ضعف در شبكه‌هاي شلوغ به مشكلي حاد مبدل مي‌شود. خصوصاً اگر از كارت شبكه‌ي استفاده شده مطمئن نباشيم. بسياري از كارت‌هاي شبكه از IVهاي ثابت استفاده مي‌كنند و بسياري از كارت‌هاي شبكه‌ي يک توليد كننده‌ي واحد IVهاي مشابه دارند. اين خطر به‌همراه ترافيک بالا در يک شبكه‌ي شلوغ احتمال تكرار IV در مدت زماني كوتاه را بالاتر مي‌برد و در نتيجه كافي است نفوذگر در مدت زماني معين به ثبت داده‌هاي رمز شده‌ي شبكه بپردازد و IVهاي بسته‌هاي اطلاعاتي را ذخيره كند. با ايجاد بانكي از IVهاي استفاده شده در يک

شبکه‌ي شلوغ احتمال بالايي براي نفوذ به آن شبکه در مدت زماني نه چندان طولاني وجود خواهد داشت.

ضعف در الگوريتم:

از آن‌جايي‌که IV در تمامي بسته‌هاي تکرار مي‌شود و بر اساس آن کليد توليد مي‌شود، نفوذگر مي‌تواند با تحليل و آناليز تعداد نسبتاً زيادي از IVها و بسته‌هاي رمزشده بر اساس کليد توليد شده بر مبناي آن IV، به کليد اصلي دست پيدا کند. اين فرايند عملي زمان بر است ولي از آن‌جاکه احتمال موفقيت در آن وجود دارد لذا به عنوان ضعفي براي اين پروتکل محسوب مي‌گردد.

۳-۴-۲-استفاده ازCRC رمز نشده :

در پروتکل WEP، کد CRC رمز نمي‌شود. لذا بسته‌هاي تأييدي که از سوي نقاط دسترسی بي‌سيم به‌سوي گيرنده ارسال مي‌شود بر اساس يک CRC رمزنشده ارسال مي‌گردد و تنها در صورتي که نقطه‌ي دسترسی از صحت بسته اطمينان حاصل کند تأييد آن را مي‌فرستد. اين ضعف اين امکان را فراهم مي‌کند که نفوذگر براي رمزگشايي يک بسته، محتواي آن را تغيير دهد و CRC را نيز به دليل اين که رمز نشده است، به‌راحتي عوض کند و منتظر عکس‌العمل نقطه‌ي دسترسی بماند که آيا بسته‌ي تأييد را صادر مي کند يا خير.

ضعف‌هاي بيان شده از مهم‌ترين ضعف‌هاي شبکه‌هاي بي‌سيم مبتني بر پروتکل WEP هستند. نکته‌يي که در مورد ضعف‌هاي فوق بايد به آن اشاره کرد اين است که در ميان اين ضعف‌ها تنها يکي از آن‌ها به ضعف در الگوريتم رمزنگاري باز مي‌گردد و لذا با تغيير الگوريتم رمزنگاري تنها اين ضعف است که برطرف مي‌گردد و بقيه‌ي مشکلات امنيتي کماکان به قوت خود باقي هستند.

جدول۵ ضعف‌هاي امنيتي پروتکل WEP را به‌اختصار جمع‌بندي 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.

جدول۵

۴ ـمؤلفه‌هاي امنيتي در بلوتوث

بلوتوث از پروتكلهاي تشخيص هويت، احراز صلاحيت و رمزنگاري؛ مدهاي امنيت از جمله امنيت در سطح پيوند؛ كنترل دسترسي جداگانه براي دستگاهها و سرويس‌ها؛ و استفاده از انواع شناسه بستگي به نوع دستگاه، حمايت مي‌كند.
امنيت در سطح پيوند تكنيك‌هايي را براي ساختن يک لايه پيوند امن فراهم مي‌كند. در اين تكنيكها با رمزنگاري و تشخيص هويت در سطح پيوند، پيوند امني بين دستگاههاي بلوتوث فراهم مي‌شود.
رمزنگاري و احراز هويت در بلوتوث براساس يک كليد پيوندي صورت مي‌گيرد كه بين هر دو دستگاه مرتبط با هم وجود دارد. براي توليد اين كليد اولين باري كه دو دستگاه در صدد ارتباط با يكديگر بر مي‌آيند، متد Pairing فراخوانده مي‌شود كه توسط آن دو دستگاه هويت يكديگر را احراز كرده و يک كليد مشترک براي برقراري پيوند ايجاد مي‌نمايند. همچنين دستگاهها براي ارتباط با هم از يک عدد هويت شخصي در زمان مقداردهي اوليه ارتباط استفاده مي‌كنند. اين عدد در واقع مانند يک رمز عبور براي ارتباط با يک دستگاه بلوتوث عمل مي‌كند.
علاوه بر اين بلوتوث از تكنيكي به نام برش فركانس استفاده مي‌كند. در اين روش فركانس ارتباطي بين دو دستگاه براساس الگوی توافقي بين خودشان در محدوده فركانس مجاز ۱۶۰۰ بار در ثانيه، عوض مي‌شود تا علاوه بر اينكه نويز كمتري در ارتباطات ايجاد شود دست يافتن به داده واقعي رد و بدل شده بين دو دستگاه براي هكرها هم دشوار شود.

۴-۱خطرات امنيتي:

موارد و آسيب‌پذيريهاي امنيتي در بلوتوث وجود دارند كه باعث مي‌شوند كاربران ترجيح دهند علاوه بر تدابير امنيتي پيش فرض بلوتوث اقدامات امنيتي بيشتري براي امن كردن شبكه خود بكاربرند. با اينكه استاندارد شبكه‌هاي بلوتوث بستري امن را فراهم مي‌سازد اما بسياري از دستگاه هاي اين شبكه با رعايت نكردن اين استاندارد نواقص خطرناكي در احراز هويت و مكانيزم‌هاي انتقال اطلاعات خود دارند كه شبكه را ناامن مي‌سازد.
جدول ۶ برخي از نكات امنيتي شبكه‌هاي بلوتوث را كه بايد مورد توجه قرار بگيرد توضيح مي‌دهد.

مورد	توضيحات
عدم احراز صلاحيت كاربر	بلوتوس احراز صلاحيت دستگاهها را فراهم مي‌كند نه كاربران
استراق سمع ناشي از اشتراك‌گذاری كد پيوندی	در هنگام ساخته شدن يک لينک كد پيوندی آن پيوند بين دستگاهها رد و بدل مي‌شود كه اين ممكن است امكان دزديده شدن آن را فراهم آورد.
فراهم نبودن امنيت End toEnd	فقط پيوندهای بين دو دستگاه مجاور رمزگذاری و احراز هويت مي‌شوند و در هر نقطه ميانی مسير عمليات رمزگشايی صورت مي‌گيرد. امنيت بين مبدأ و مقصد اصلی بايد به وسيل يک كاربردی جدا از استاندارد بلوتوس تأمين گردد.

جدول 6 برخی از نکات امنیتی شبکه‌های بلوتوس

ليستي از مهمترين آسيبها و حملات كه در شبكه‌هاي بلوتوث وجود دارد به شرح زير است:

- استراق سمع شبكه از طريق يک دستگاه هک شده درون شبكه شبكه‌هاي بلوتوث در برابر حملات منع سرويس آسيب‌پذيرند. هكرها مي‌توانند به وسيله دستگاههايي كه قادرند امواجي در فركانس ۲,۴ GHz بفرستند، ترافيک كاذب در شبكه بوجود آورند.
- حمله SNARF
- حملات در پشتي
- حمله Blue Jacking كه بسيار شبيه حمله سرريز در شبكه‌هاي معمولي است.
- آسيب‌پذيري كاربر مجاز شبكه

۴-۲مقابله با خطرات:

۴-۲-۱اقدامات مديريتي:

مديران شبكه‌ها با سياستگذاري و وضع قوانيني، نحوه استفاده كاربران از شبكه و مسئوليت‌هاي آنان را مشخص كنند.

۴-۲-۲پيكربندي درست شبكه:

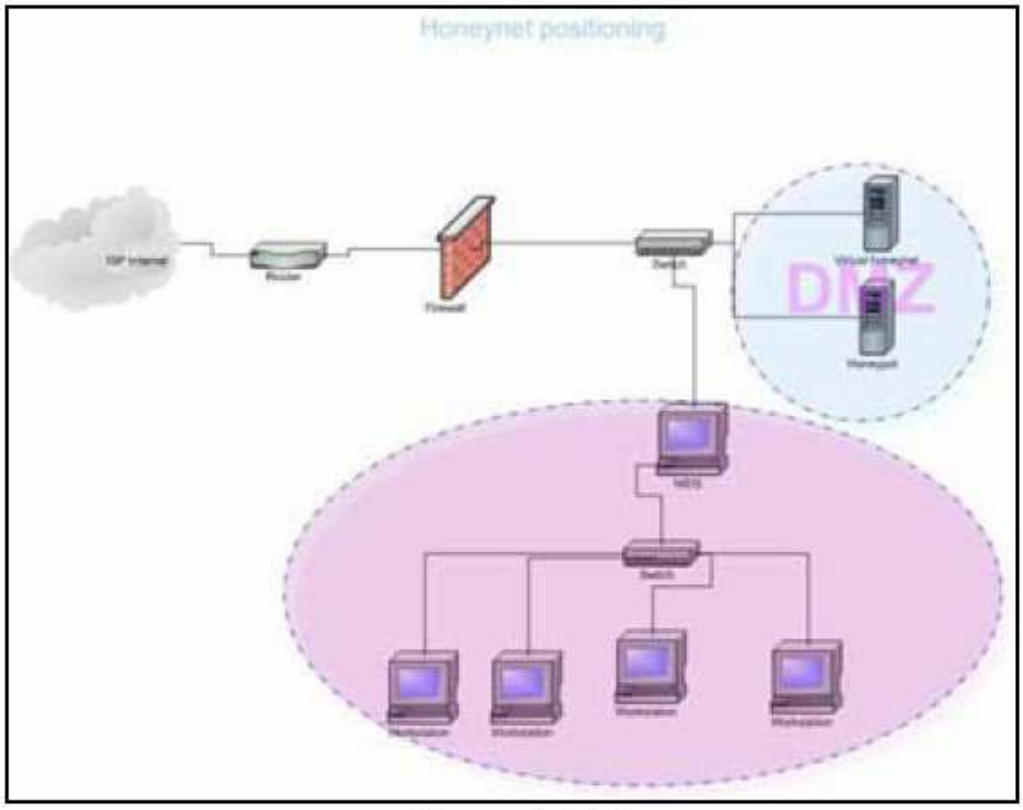
مديران شبكه‌ها بايد اطمينان پيدا كنند كه تمام دستگاهها از كد هويت شخصي براي احراز هويت استفاده مي‌كنند. همچنين در لايه كاربرد حفاظت برنامه‌ها بايد با كلمه عبور تأمين گردد.

۴-۲-۳نظارت اضافي بر شبكه:

بعضي برنامه‌هاي كاربردي توليد شده‌اند كه امنيت شبكه‌هاي بلوتوث را كنترل مي‌كنند و امنيت بيشتري را براي اين شبكه‌ها فراهم مي‌آورند. يكي از اين برنامه‌ها Blue Watch مي‌باشد كه براي محيط ويندوز طراحي شده است.

۵-HoneyPotتدبيري نو براي مقابله با خرابكاران

Honeypot يكي از ابزارهائي است كه متخصصين برخورد با هكرها و مديران شبكه از آن براي شناسايي و به دام انداختن هكرها ونفوذگران استفاده مي كنند.اين وسيله از اين بعد كه ميتواند اطلاعات بسيار دقيق و مفيدي از هكر و نحوه ي هک كردن را در اختيار مديران شبكه قرار دهد بسيار مورد توجه است به گونه اي كه تحقيقات گسترده اي در جهت ارتقا كارامدي اين وسيله در حال انجام است.



شكل ۷ هانيپوت در شبكه

۵-۱-تعريفHoneypot :

يک منبع سيستم اطلاعاتي مي باشد كه بر روي خود اطلاعات كاذب وغير واقعي دارد وبا استفاده از ارزش واطلاعات كاذب خود سعي در كشف وجمع آوري اطلاعات و فعاليت هاي غيرمجاز و غير قانوني بر روي شبكه مي كند.به زبان ساده Honeypot يک سيستم يا سيستمهاي كامپيوتري متصل به شبكه و يا اينترنت است كه داراي اطلاعات كاذب بر روي خود مي باشد و از عمد در شبكه قرار مي گيرد تا به عنوان يک تله عمل كرده و مورد تهاجم يک هكر يا نفوذگر (Attacker) قرار بگيرد و با استفاده از اين اطلاعات آنها را فريب داده و اطلاعاتي از نحوه ي ورود آنها به شبكه و اهدافي كه در شبكه دنبال مي كنند جمع آوري كند.

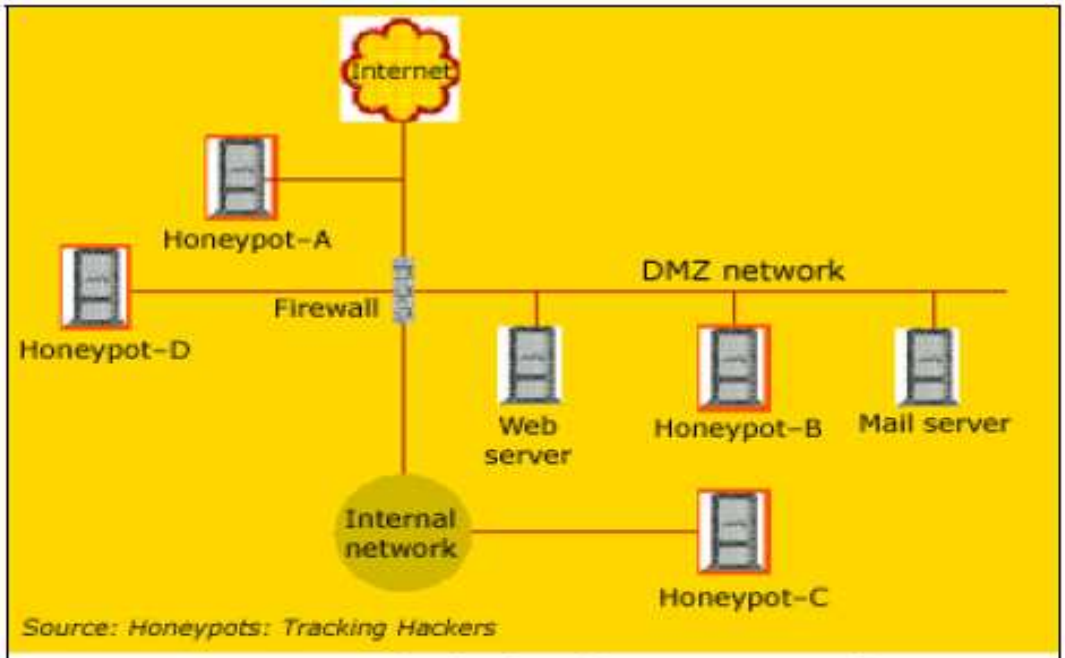


Figure 8. Honeypots can be deployed from a variety of locations. This diagram shows four different possible locations. The optimum location for deployment depends on an array of factors, such as the type of information the organization is interested in gathering, and the level of risk that organization can tolerate to obtain the maximum amount of data.

شکل ۸ شبکه‌ای از هانیپوت ها

۵-۲-نحوه تشخيص حمله و شروع عملكرد Honeypot :

در مسير منتهي به Honeypot نبايد هيچ ترافيكي ايجاد شود يعني هر گونه ارتباطي با Honeypot فعاليت غيرمجاز و غير قانوني محسوب شده و مي تواند يک دزدي ، حمله و يا سرقت محسوب شود.

۵-۳-مزاياي Honeypot :

۱- جمع آوري بسته هاي اطلاعاتي كم حجم ولي با ارزش :

Honeypot ها حجم كوچكي از اطلاعات را جمع آوري مي كنند .مثلاً به جاي ثبت روزانه GB۱ داده توسط ساير تكنولوژي هاي برقراري امنيت اطلاعات ، Honeypot مثلاً MB۱ اطلاعات جمع آوري مي كند ولي چون مطمئن هستيم كه اطلاعاتي كه يک Honeypot جمع آوري مي كند مربوط به فعاليتي غير مجاز است در نتيجه اين اطلاعات بسيار مفيد بوده و تجزيه و تحليل حجم كوچكي ازاطلاعات آسان و ارزان است.

۲- ابزارها و تاكتيكها ي جديد :

Honeypot ها طراحي شده اند تا هر چيزي كه به سمتشان منتهي مي شود ثبت كنند بنابراين Honeypot مي تواند ابزارها و تاكتيكهايي جديد را كه هكرها به كمک آنها به سيستم حمله مي كنند را ثبت كند.

۳- نياز به كمترين سخت افزار براي پياده سازي :

در يک كامپيوتر Pentium كه داراي MBRAM۱۲۸ است قابل پياده سازي است.

۴- قابل پياده سازي در محيط هاي IPV6 و رمز شده :

بر خلاف اغلب تكنولوژيهاي امنيت (مثل سيستمهايIDS) كه در محيط هاي رمز شده بخوبي كارنمي كنند Honeypot به راحتي قابل پياده سازي در اين محيط ها است و در اين محيط ها به خوبي كار مي كند.

۵- سادگي :

Honeypot ها بسيار ساده اند زيرا الگوريتم پيچيده اي ندارند كه بخواهند توسعه يابند جداول حالت ندارند كه نياز به پشتيباني داشته باشند.

۶-شناسايي نقاط ضعف سيستم :

مدير سيستم مي تواند با مشاهده تكنيک ها و روشهاي استفاده شده توسط نفوذگر بفهمد كه سيستم چگونه شكسته مي شود و نقاط آسيب پذير سيستم را شناسايي و نسبت به ترميم آنها اقدام كند.هدف اصلي يكHoneypot شبيه سازي يک شبكه است كه نفوذگران سعي مي كنند به آن وارد شوند اطلاعاتي كه بعد از حمله به يكHoneypot به دست مي آيد مي تواند براي كشف آسيب پذيري هاي شبكه فعلي و رفع آنها استفاده شود.

۵-۴-تقسيم بندي Honeypot از نظر كاربرد :

۱)Honeypot Production
۲)Research Honeypot

۵-۴-۱Production Honeypot :

اين نوع سيستم وقتي كه سازمان مي خواهد شبكه و سيستم هايش را با كشف و مسدود كردن نفوذگران حفاظت كند و نفوذگر را از طريق قانون در دادگاه مورد پيگيرد قرار دهد مورد استفاده قرار مي گيرد.
Honeypot هايي كه كاربرد Production دارند به سه طريق مي توانند در برابر حملات از شبكه محافظت كنند .

۱)به روش Prevention (پيشگيري)
۲)به روش Detection (كشف يا شناسايي)
۳)به روش Response (پاسخ)

۵-۴-۱-۱- Prevention :

در بعضي از حملات نفوذگران با استفاده از ابزارهايي رنجي از شبكه ها را پويش مي كنند تا آسيب پذيري سرورهاي موجود در شبكه راشناسايي كنند اين ابزارها پس از پيدا كردن آسيب پذيريهاي موجود در سيستم به اين سيستمها حمله مي كنند در روش پيشگيريHoneypot سرعت اين گونه حملات را كند مي كند و حتي بعضي اوقات آنها را متوقف نيز مي كند به اين دسته از Honeypotها،Honeypotهاي چسبنده (Sticky) مي گويند در اين روش Honeypot هنگام پويش توسط نفوذگر نسبت به آدرسهايي كه در شبكه موجودنيست واكنش نشان ميدهد Labrea Tarpit جزو اين دسته از Haneypot ها است . به طور كلي هدف پيشگيري (Prevention) كند كردن سرعت عمليات نفوذگر و توقف حمله است.

۵-۴-۱-۲-Detection (كشف يا شناسايي) :

وظيفه اش عمل كشف و شناسايي ناتواني هاي بخش پيشگيري است كشف يک حمله كار بسيارمشكلي است. وقتي يک حمله شناسايي شود مي توان خيلي سريع به آن واكنش نشان دادو آن را متوقف و يا حداقل اثرش را كم كرد مي توان از تكنولوژيهاي امنيتي مثل IDSو فايلهاي ثبت وقايع(Log) در مرحله شناسايي استفاده كرد ولي بدليل اينكه اين تكنولوژي ها داده هاي زيادي را ثبت مي كنند تجزيه و تحليل آنها زمانبر است و بسياري از اين داده ها غير مفيد بوده و در شناسايي نفوذگر و اهدافش ما را كمک نمي كنند و در محيط هاي رمز شده نيز بخوبي كار نمي كنند.Honeypot ها در كشف و رديابي يک حمله نسبت به تكنولوژيهاي مذكور برتري دارند.Honeypotها داده هاي كم و با درجه اطمينان درستي بالاتري جمع آوري مي كنند كه تجزيه و تحليل آنها آسان بوده و ارزش بيشتري دارند. همچنين Honeypotها در محيط هاي رمز شده نيز مي توانند بخوبي كار كنند.

۵-۴-۱-۳-Response (پاسخ) :

يكي از چالشهايي كه هر سازماني مي تواند با آن روبرو شود اين است كه بعد از شناسايي و كشف حمله چگونه به آن پاسخ دهد معمولا در پاسخ مناسب به يک حمله دو مشكل وجود دارد. اول اينكه اكثر سيستمهايي كه مورد حمله قرار گرفته اند را نمي توان بخاطر تجزيه و تحليل مناسب از كار انداخت زيرا online بودن آنها امري ضروري و حياتي است دوم اينكه حتي اگر سيستم را نيز از كار بياندازيم به دليل وجود كثرت داده ها در سيستم تشخيص داده هاي متعلق به نقوذگر آسان نيست. بنابراين استفاده از Honeypot در چنين سازماني اين امكان را فراهم مي كند كه درمواقع لزوم براي تجزيه وتحليل كامل داده ها آنها را از شبكه خارج كنيم بدليل اينكه Honeypot هميشه فعاليتهاي غير قانوني و بد انديشانه را ذخيره مي كند بنابراين مطمئن هستيم كه اطلاعات موجود در آنها مربوط به يک هكر و يا يک نفوذگر است و به همين دليل است كه تجزيه وتحليل يكHoneypot هك شده بسيار آسانتر از يک سيستم واقعي است ودر نتيجه مي توان در برابر حمله پاسخ سريع ومؤثري داد.

۵-۴-۲-Research Honeypot :

ايـن نـوع سيسـتم وقتـي كـه سـازمان مـي خواهـد فقـط امنيـت شـبكه وسيسـتمهاي خـود را بـا آموختن روشهاي نفوذ، منشأ نفوذ، ابزارها و Exploit هاي مورد استفاده نفوذگر مستحكم تر كند، استفاده مي شود.

۵-۵-تقسيم بندي Honeypot از نظر ميزان تعامل با نفوذگر :

Honeypot ها از لحاظ ميزان تعامل ودرگيري با نفوذگر به سه دسته تقسيم مي شود.

1)Low Interaction Honeypots (Honeypot هاي با تعامل كم)
2)Medium Interaction Honeypots (Honeypot هاي با تعامل متوسط)
3)High Interaction Honeypots (Honeypot هاي با تعامل بالا)

Interaction نوع ارتباطي كه تفوذگر با Honeypot دارد را مشخص مي كند.

۵-۵-۱-Low Interaction Honeypots :

ارتبـاط وفعـاليتي محـدود بـا نفـوذگر دارنـد ومعمـولاً بـا سرويسـها وسيسـتم عاملهـاي شـبيه سـازي شده كـار مـي كنند وسطح فعاليت نفوذگر را محدود بـه سطوح شبيه سـازي شده مـي كننـد. بـه عنـوان مثـال Low Interaction honeypot مـي توانـد شـامل يک WindowsServer2000 به همراه سرويسهاي مثل Telnet و FTP باشد. يک نفوذگر مي تواند ابتدا با استفاده از Telnet روي Honeypot نـوع سيستم عامل آن را تشخيص داده سپس با حدس زدن رمز عبور و يا بـا هر روش ديگري وارد شبكه شود بدون اينكـه اطـلاع داشـته باشـد كـه در يـک Honeypot گرفتـار شـده اسـت. بـر اسـاس فعـاليتي كـه نفـوذگر در Honeypot انجـام مـي دهـد.Honeypot مـي توانـد اطلاعـات زيـر را جمـع آوري كـرده و در اختيار متخصص شبكه قرار دهد.

۱) زمان نفوذ نفوذگر و يا هكر به سيستم
۲) پروتكلي كه از آن استفاده كرده
۳) آدرس FTP مبدا ومقصد

در اين نوع Honeypot ، نفوذگر نمي تواند هيچ گونه ارتباطي با سيستم عامل برقرار كندو اين مسأله ميزان خطر را كاهش ميدهد چون پيچيدگيهاي سيستم عامل حذف مي شود وبـه دليل اينكـه مـا سطح فعاليت نفوذگر را محدود كرده ايم بنـابراين اعمـالي كـه نفوذگرانجام مـي دهد محـدود شـده ودر نتيجـه Honeypot اطلاعـات محـدودي را مـي توانـد ثبـت كنـد. ايـن نـوع Honeypot فقط قادر به شناسايي حمله هاي شناخته شده است ونمي تواند حمله هـاي ناشناخته را تشخيص دهد. سادگي نگهداري وتوسعه Honeypot كم واكنش همچنين پايين بودن ريسـک خطـــر آن از نقـــاط قـــوت Honeypot كـــم واكـــنش محســـوب مـــي شـــود. ازاين Honeypotها ميتوان براي اهداف Production استفاده كرد.

HoneyPot-2-5-5 با تعامل متوسط(HoneyPot Medium Intraction) :

Honeypot با تعامل متوسط در مقايسه با Honeypot نوع كم واكنش امكان بيشتري براي تعامل با نفوذگر فراهم مي كند ولي هنوز هم نفوذگر هيچ ارتباطي با سيستم عامل نداردDaemonهاي جعلي فراهم شده پيشرفته ترند و دانش بيشتري راجع به سرويسهاي ارائه شده دارند. در اين حالت ميزان خطر افزايش مي يابد. احتمال اينكه نفوذگر يک حفره امنيتي يا يک نقطه آسيب پذيري پيدا كند بيشتر است زيرا پيچيدگي Honeypot افزايش مي يابدو نفوذگر امكان بيشتري براي ارتباط با سيستم وبررسي آن دارد و راحت تر فريب مي خورد. همچنين با توجه به تعامل بيشتر، امكان انجام حمله هاي پيچيده تري وجود دارد كه مي توان با ثبت و آناليز كردن آنها به نتايج دلخواه دست يافت. همانطوري كه گفته شد نفوذگر هيچ ارتباطي با سيستم عامل ندارد و در سطح برنامه هاي كاربردي فعاليت مي كند. توسعه يک Honeypot با تعامل متوسط كاري پيچيده و زمانبر است. بايد دقت شود كه تمام Daemonهاي جعلي تا جايي كه ممكن است ايمن شوند. نسخه هاي توسعه يافته اين سرويسها نبايد داراي همان آسيب پذيري هاي نسخه هاي واقعي باشند زيرا اين اصلي ترين دليل جايگزيني آنها با نسخه هاي جعلي است. كسي كه مي خواهد چنين سيستمي را طراحي و پياده سازي كند، بايد از دانش خوبي در مورد پروتكلها، سرويسها و برنامه هاي كاربردي ارائه شده برخوردار باشد ازاين Honeypotها ميتوان هم براي اهداف دسته Research و هم براي اهداف دسته Production استفاده كرد.

۵-۵-۳-High Interaction Honeypot :

يكي از اهداف نفوذگرامكان دسترسي به اطلاعات در ماشيني كه به اينترنت وصل است مي باشد اين نوع Honeypot چنين امكاني را در اختيار نفوذگر قرار مي دهد. به محض اينكه نفوذگر اين امكان را پيدا كند كار اصلي او شروع مي شود در اين نوع Honeypot ما يک سيستم واقعي را در اختيار نفوذگر قرار مي دهيم و هيچ چيزي شبيه سازي شده نيست و نفوذگر با سيستم عامل واقعي و شبكه واقعي سرو كار دارد و ميزان دسترسي وي به شبكه بيشتر است در نتيجه ميزان عملي كه مي تواند انجام دهد بيشتر شده و Honeypot مي تواندفعاليت بيشتري از نفوذگر و اهداف مورد نظر وي جمع آوري كند.ازاين Honeypotها ميتوان براي اهداف دسته Research استفاده كرد.

۵-۵-۳-۱- مزاياي استفاده از High Interaction Honeypot :

متخصص شبكه با تجزبه و تحليل اطلاعات Honeypot مي تواند اطلاعات زير را در مورد نفوذگر بدست آورد.

- نفوذگران بيشتر از چه ابزارها و Exploit هايي استفاده مي كنند
- از چه كشورهايي هستند
- به دنبال چه نقاط آسيب پذيري هستند
- ميزان دانش آنها درمورد نفوذگري
- جمع آوري اطلاعات واسناد زياد براي تحليل
- به دليل وسيع بودن سطح فعاليت نفوذگر اغلب اين نوع Honeypot ها رفتارهايي ازفردنفوذگررا به مانشان مي دهند كه ما انتظارنداشته ايم ويا نمي توانسته ايم حدس بزنيم.

۵-۵-۳-۲- معایب استفاده از High Interaction Honeypot :

- طراحي ، مديريت ونگهداري آن فوق العاده زمانبر است.
- سيستم بايد دائماً تحت نظرباشد درغير اين صورت نه تنها هيچ كمكي نمي كند بلكه خودش به عنوان يک نقطه خطريا حفره امنيتي مطرح مي شود.
- داراي ريسک بالازيرا نفوذگر يک سيستم واقعي رادراختيار دارد وممكن است به سيستم هاي اصلي شبكه صدمه بزند .بنابراين هيچ سيستمي بر روي شبكه را نمي توان امن در نظر گرفت .

نتیجه :

تا کنون شاهد چگونگی عملکردسیستم های مختلف امنیتی در شبکه های بی سیم ونقاط قوت و ضعف آن هابوده ایم.در ضمن این نکته نیز به عنوان واقیعت پذیرفته واثبات شده است که اگر خرابکاران یک گام جلوتر از مدیران شبکه نباشند حداقل در سطحي همگام با آنانند و در زمینه ي اطلاعات فني و تکنیک هاي نفوذ این خرابکاران هستند که داراي معلوماتي بیشتر هستند زیرا و در غیر این صورت دیگر هیچ گونه خرابکاري صورت نمي گرفت و یا احتمال آن به صفر مي رسید . امري که با وجود پیشرفت هاي بسیار در زمینه امنیت شبکه هنوز نیز نا ممکن به نظر مي رسد.از همین رو می باید به دنبال سیستم امنیتی جدید و کارآمد بود که علاوه بر کاربردهای تعریف شده برای یک سیستم امنیتی بتواند مدیران شبکه را با روش های جدید و کشف نشده ی نفوذ در شبکه آشنا کند وامکانی برای چاره اندیشی برای مقابله باخرابکاران را فراهم نماید. لذا نیارمند ایجاد یک نظام امنیتی جدید برای حفاظت از شبکه هستیم که دربردارنده ی خصوصیات فوق باشد. چنین سیستمی که چندی نیزنیست که از ابداع آن می گذرد اختصارا ظرف عسل(HoneyPoy) نام گرفته است.

مزایاو برتری های این سیستم در فصل پنج کاملا توضیح داده شده است و تنها نکته باقی مانده چگونگی کاربری این سیستم در شبکه های بیسیم است. همانگونه که گفته شد به علت این که در این سیستم نیازمند یک دستگاه رایانه به عنوان ظرف عسل(HoneyPot) هستیم تا هکرها را به سمت خود جذب کرده و اطلاعات لازم را جمع آوري نماید پس نباید انتظار داشت که یک کاربر عادي که تنها از یک دستگاه رایانه استفاده مي نماید یا مدیر یک شبکه کوچک محلي عادي با تعدادمحدودي رایانه از جمله استفاده کنندگان این سیستم باشند.این مکانیزم امنیتي معمولا در شبکه هاي محلي بزرگ و یا شبکه هایي که از نظر امنیتي بسیار مورد اهمیت هستند مورد استفاده قرار مي گیرد وظرق عسل نیز معمولا می باید به صورت بلافصل به Router متصل مي گردد تا در دسترس ترین ماشین از دید خرابکاران تلقي شود و بتواند اطلاعات مورد تیاز را به راحتی جمع آوری کند.

کلمه های کلیدی

- شبکه های بیسیم(Wireless Networks)
- شبکه های کابلی
- کیفیت سرویس(Quality Of Service)
- فرکانس رادیویی(Radio Frequency)

- BS : Base Station
- DSL : Digital Subscriber Line
- ETSI : European Telecommunication Standards Institute
- IEEE : Institute of Electric and Electronic Engineers
- MAC : Media Access Control address
- MAN : Metropolitan Area Network
- PAN : Personal Area Network(شبکه ی محلی شخصی)
- WAN : Wide Area Network
- WLAN : Wireless Local Area Network
- WMAN : Wireless Metropolitan Area Network
- OFDM : Orthogonal Frequency Division Multiplexing
- OFDMA : Orthogonal Frequency Division Multiple Access
- VOIP : Voice Over Internet Protocol
- Wi-Fi : Wireless Fidelity
- WIMAX : Worldwide Interoperability for Microwave Access
- DSSS : Direct Sequence Spread Spectrum
- FHSS : Frequency Hopping Spread Spectrum
- FSK : Frequency Shift Keying
- IAPP : Inter Access Point Protocol
- ISM : Industrial Scientific and Medical
- DCF : Distribute Coordination Function
- PCF : Point Coordination Function
- CSMA/CA : Carrier Sense Multiple Access With Collision Avoidance
- BSS : Basic Service Set
- ESS : Extended Service Set
- IBSS : Independent Basic Service Set
- BSSI : Basic Service Set Infrastructure
- PCMCIA : Personal Computer Memory Card International Association
- PCI : Peripheral Component Interconnect
- SSID : Service Set Identifier
- EAP : Extensible Authentication Protocol
- LEAP : Light Extensible Authentication protocol
- SNMP : Service of Network Management Protocol

- IR : Infra Red
- SS : Spread Spectrum
- DCF : Distribution Coordination Function
- PCF : Point Coordination Function
- CCK : Complementary Code Keying
- WEAC : Wireless Ethernet Communication Alliance
- EIRP : Equivalent Isotropically Radiate Power
- PBCC : packet Binary Convolutional Code
- UNII : Unlicensed National Information Infrastructure
- QAM : Quadrate Amplitude Modulation
- Vendor Proprietary (درانحصارفروشنده)
- Ethernet
- Encryption
- Ad Hoc
- Infrastructure
- Peer to Peer
- Bluetooth
- Router
- Broad Band
- WEP : Wired Equivalent Privacy
- Access Point(نقطه ی دسترسی)
- Client(سرویس گیرنده)
- Master-Slave
- Pico net
- Scatter net
- Link Level Security Mode(امنیت در سطح پیوند)
- Identifier(شناسه)
- Link Key(کلید پیوندی)
- Personal Information Number(عدد هویت شخصی)
- Frequency Happing(برش فرکانسی)

منابع و مراجع :

- **Pahlavan, Kaveh.Wireless Network. New York : Prentice Hall,1999**
- **Peikari, Cyrus. Maximum Wireless Security.Sams,**
- **Tanenbaum, Andrew S. Computer Networks. New Jersey : Prentice Hall, 2003**
- **Steve Cap. 802.11: Leaving the Wire Behind. IEEE Internet Computing, January-February 2002**
- **http://www.Amoltk.com/**
- **http://www.ieee802.org/11/**
- **http://www.ee.ed.ac.uk/~acmc/OFDMTut.html/**
- **http://www.wireles.per.nl/telelearn/ofdm/**
- **http://www.farda-tech.com/**
- **http://www.itc.ir/**
- **http://www.intel.com/**
- **http://www.ostadonline.com/**
- **http://www.fa.wikipedia.com/**
- **http://www4.irandoc.ac.ir/full-text/full-art.htm**
- **http://www.vikiit.com/cms/mambo/**
- **http://www.cisco.com/**
- **http://www.persiantools.com/**
- **http://www.websecurity.ir/**
- **http://www.srtelecom.com/**
- **http://www.motorola.canopywireless.com/kbase/**
- **http://www.sgnec.net/**