کامپیوتر و اینترنت
اقتصادی ۲۴
پنجشنبه ۳۰ آبان ۱۳۸۷ - ۲۱ ذی القعده ۱۴۲۹ - ۲۰ نوامبر ۲۰۰۸ شماره ۲۹۶۶
Thursday, 20 Nov 2008, Number 2966

محصولی جدید از کسپرسکی عرضه خواهد شد

لابراتوار کسپرسکی در نظر دارد تا نسخه جدید محصولات شرکتی خود را در ابتدای سال ۲۰۰۹ میلادی به بازار عرضه نماید.

به گزارش ایتنا نسخه تحت شبکه آنتی‌ویروس کسپرسکی، جهت ایمن‌سازی ایستگاه‌های کاری، سرورهای فایل، سرورهای Mail و گذرگاه‌های اینترنتی محصولات متنوعی داراست. بزرگترین مزیت نسخه‌های تحت شبکه، نرم‌افزار مدیریت یک پارچه آنتی‌ویروس‌ها است. این نرم‌افزار به مدیر شبکه این امکان را می‌دهد تا علاوه بر نصب و بروزرسانی از راه دور آنتی‌ویروس‌ها بر روی سیستم‌های داخل شبکه، مدیریت کاملی بر عملکرد آنان داشته باشد و گزارشات متنوعی از روند کار آنها دریافت نماید. در نسخه جدید این محصول که در ابتدای سال ۲۰۰۹ میلادی به بازار ارائه خواهد شد، امکانات وسیع تری در اختیار کاربران قرار داده شده است و الگوریتم‌های پیشرفته‌تری جهت عملکرد هر چه بهتر نرم‌افزار افزوده شده است.

ویروس رایانه‌ای سه بیمارستان را به تعطیلی کشاند

سه بیمارستان در لندن به دنبال حمله یک ویروس رایانه‌ای ناچار شدند فعالیت بیش‌تر سیستم‌های رایانه‌ای خود را متوقف کنند.

به گزارش ایسنا، سیستم‌های رایانه‌ای بیمارستان‌های سنت بارتولومیو، رویال لندن و چست هاسپیتال عصر روز دوشنبه مورد حمله ویروس ناشناسی قرار گرفتند و با وجود به‌کارگیری تمهیدات لازم توسط بخش IT این بیمارستان‌ها آلودگی ویروس مذکور گسترده‌تر از حد انتظار بوده و مقامات این بیمارستان‌ها را واداشت به‌جز بخش‌های حساس مانند بخش تصادفات و اورژانس، کلیه سیستم‌های رایانه‌ای را ببندند. مدیران این بیمارستان‌ها پس از حمله این ویروس به‌دنبال افزایش ترافیک اطلاعات وضعیت فوق العاده اعلام کردند. به گفته سخنگوی یکی از این بیمارستان‌ها، بیماران اورژانسی به صورت دستی پذیرش شدند و بیماران دارای وضعیت وخیم نیز به بیمارستان‌های مجاور اعزام شدند تا در نتیجه کند بودن سیستم پذیرش دستی متحمل ناراحتی بیش‌تری نشوند.

مرورگرهای اینترنتی

بخش اول

اولین و مهمترین نیاز هر کاربر اینترنت در زمان اتصال به اینترنت استفاده نمودن از یک مرورگر وب می‌باشد.

بنابراین داشتن یک مرورگر سریع و در این حال با ثبات از ضروری ترین نیازهای هر کاربر اینترنت می‌باشد، به همین جهت در این مقاله قصد داریم شما را با ۶ تا از معروفترین مرورگرهای وب دنیا و تاریخچه آنها آشنا کنیم: مختصری از تاریخچه پیدایش مرورگرها:

با پیدایش سیستم عامل‌های همچون مایکروسافت ویندوز، دنیای کامپیوتر دچار تحولات زیادی شد من جمله کنار گذاشتن سیستم عامل‌های همچون داس که جز یکسری فرامین متنی و دانستن آنها کارایی بیشتری نداشت. با پیدایش ویندوز و حضور پنجره‌ها کار با کامپیوترها راحت‌تر گشته و امکانات استفاده از نرم‌افزارهای متعدد تر را در اختیار کاربران قرار می‌دهد. چیزی از پیدایش ویندوز نوپا نمی‌گذشت که سرو کله اینترنت بر روی کامپیوترهای شخصی یا همان PC باز شد. در ابتدا ویندوز چیزی تحت عنوان مروگر وب بر روی سیستم عامل خود نداشت و کاربران ویندوز جهت استفاده از اینترنت نیاز به نصب مرورگری به نام Netscape Browser که جهت استفاده در کامپیوترهای شخصی بود داشتند. این مرورگر سال‌ها توانست محبوبیت زیادی را در بین کاربران اینترنت به دست آورد تا اینکه شرکت مایکروسافت با ارائه اولین نسخه از مروگر خود به نام Internet Explorer بازار مرورگرهای وب را در اختیار خود قرار داد و شرکت AOL یا Netscape را به شدت شکست دهد. این روند همچنان ادامه داشت تا حدود سالهای ۲۰۰۱ - ۲۰۰۰ با افزایش کاربران اینترنت و استفاده انها از Internet Explorer به عنوان محبوبترین مرورگر وب و ظهور نسل جدید ویروس نویسان و کدهای مخرب Internet Explorer را به عنوان اولین هدف خود قرار می‌دادند. تنها اقدام مایکروسافت ارائه Patchهای متعددی برای این مشکلات بود که کارایی خوبی نداشتند اینجا بود که اولین جرقه‌های ارائه مروگرهای وب به ذهن شرکت‌های نرم‌افزاری دنیا رسید من جمله مهمترین این تحولات به جدا شدن ۲ شرکت قدیمی AOL و Mozilla که باهم به ارائه نرم‌افزار Netscape Browser می‌پرداختند اشاره نمود.

Microsoft Internet Explorer:

نامی آشنا برای تمام کاربران وب، راحت بودن و ساده بودن کار با این مرورگر و از همه مهمتر رایگان بودن این مرورگر از جمله مهمترین خصوصیات این مرورگر می‌توان نام برد که به پر کاربردترین مرورگر وب مبدل شده است.

مزایا:

داشتن قابلیت بستن پنجره‌های تبلیغاتی (pop-up blocker)، بالا بردن ضریب امنیتی مرورگر در سرویس پک ۲، پشتیبانی از قابلیت ActiveX

معایب: حفره‌های امنیتی متعدد، پشتیبانی نکردن از RSS (در نسخه‌های قدیمی)، تکنیکال ساپورت گران

نتیجه‌گیری: این مرورگر هم هنوز طرفداران زیادی را دارد اما به دلایل فوق و امنیت پایین در بسیاری از کشورها کنار گذاشته و از مرورگرهای دیگری استفاده می‌کنند. آخرین نسخه این محصول نسخه ۷ و Beta۸ می‌باشد.

Avant Browser:

یکی دیگر از مرورگرهایی که بر پایه اینترنت اکسپلورر کار می‌کند، نرم‌افزار فوق دارای سرعت بالا، پایداری، محیط کاربر پسند و ویژگی چند پنجره در یک پنجره می‌باشد. این مرورگر با پشتیبانی از ۳۹ زبان زنده دنیا در نوع خود بی نظیر است. این نرم‌افزار کاملاً رایگان می باشد و برای استفاده از آن هیچگونه محدودیتی وجود ندارد، به دور از هر گونه تبلیغ و یا نرم‌افزارهای جاسوسی می‌باشد.

مزایا: همان اینترنت اکسپلور با یکسری قابلیت‌های اضافه شده به آن مانند: ـ پشتیبانی از پوسته‌های مختلف برای جذاب تر شدن محیط کار برای کاربر ـ حالت همه صفحه واقعی با حذف دستگیره‌های پیمایش و مخفی کردن تسک بار ـ کنترل همزمان چندین پنجره باز برای متوقف کردن و بستن چندین پنجره ـ پشتیبانی کامل از تمامی امکانات اینترنت اکسپلورر همانند پذیرش کوکی ها، جاوا، فلش، پلیرها، اکتیو ایکس و . . . ـ بلوکه کردن پنجره‌های تبلیغاتی و . . .

معایب: حفره‌های امنیتی متعدد، پشتیبانی نکردن از RSS، تکنیکال ساپورت برای نسخه‌های دانلودی ندارد. نتیجه‌گیری: این مرورگر بازهم به دلیل استفاده از موتور اینترنت اکسپلور جهت کاوش وب دارای همان مشکلات اینترنت اکسپلور نیز می‌باشد.

articles.ir

پشت صحنه گوگل

بخش اول

قطعا، پشت صحنه سناریوهایی که مغزهای گوگل از اوایل دهه نود میلادی تا کنون بر پایه آنها، جهان دیجیتال را به تسخیر خود در آورده‌اند، به‌اندازه آگاهی از رفتار سازمانی این شرکت در خلق محصولات دیجیتالی، جذاب و خواندنی خواهد بود.

رانندگانی که به ریاضیات خود مطمئن بودند و در ترافیک همیشگی بزرگراه شماره ۱۰۱ که به «سیلیکون ولی» منتهی می‌شود، گیر می‌کردند، می‌توانستند وقت خود را با تامل در بیلبوردی که روی آن یک سؤال ریاضی نوشته شده بود، بگذرانند.

کسانی که می‌توانستند عدد موردنظر مسأله کننده را دریابند، در واقع مبنای یک الگوریتم طبیعی را می‌یافتند. تعداد کسانی که روی این معما کار کردند و از عهده حل آن برآمدند، به وب سایتی رهنمون شدند تا مسئله‌ای دیگر را حل کنند و پس از حل این معما هم، صفحه‌ای دیگر به روی آنها گشوده می‌شد که از آنها می‌خواست تا مشخصات و سوابق کاری خود را ارسال کنند. اگر بیلبوردی می‌توانست روح یک شرکت را به تصویر بکشد، همین بیلبورد بود، زیرا آگهی دهنده ناشناس شرکت گوگل بود که محصول اصلی و مهم آن محبوب‌ترین موتور جست‌وجوی اینترنتی در جهان است. با این شوخی جسورانه، با اشتغالات ذهنی ریاضی، سادگی و این اعتقاد مبتکرانه که گوگل منزلگاه نوابغ است، بیلبورد از شرکتی سخن می‌گفت که فکر می‌کند جایگاه درست و به‌حقی را به‌عنوان رهبر و پیشروی صنعت فناوری به‌دست آورده است، موقعیتی که در ۱۵ سال گذشته، مایکروسافت اشغال کرده بود.

لحن بیلبورد گوگلی بود، چیزی که کارفرماهای گوگل علاقه دارند، بگویند. سخنگوی شرکت می‌گوید که این صفت «گوگلی»، جهان وطنی، تواضع، تفاوت و تشخیص متعادلی را به ذهن متبادر می‌کند. نمایشی مناسب و زیبا از گوگلی بودن «googlyness» که در سخنرانی‌های لاس‌وگاس اجرا شد درحالی که روسای دیگر شرکت‌های فناوری به جایگاه سخنرانی در میان هیاهوی موسیقی راک و رقص نور وارد می‌شوند، گوگل کنسرت براندنبورگ شماره سه از باخ را پخش کرد، تا روسای شرکت به جایگاه وارد شوند. بیلبورد از این جهت گوگلی بوده، یعنی مانند صفحه اصلی گوگل، به‌لحاظ بصری به‌طور کامل ساده بود چنان که مراجعه کنندگان را درباره محتوای پیچیده آن به اشتباه می‌اندازد، یا اینکه، برای بیگانگان «گوگلی بودن»، به معنای آرزویی جسورانه و یک ماموریت است که شما را به پیشرفت جهان و یکی دانستن جهل با فضیلت فرا می‌خواند، عارضه اصلی این طرز فکر که در بیلبورد نشان داده شده است، بزرگ دانستن ریاضیات است.

علاقه به ریاضیات در گوگل، شاید از علاقه موسسان آن سرگئی برین و لری پیج ناشی می‌شود. برین که در روسیه متولد شده است پسر استاد آمار است و مادرش هم برای ناسا کار می‌کند و والدین لری پیج هر دو معلم رایانه هستند.

راز موفقیت گوگل که آن را محبوب‌ترین موتور جست‌وجو در جهان ساخته است، درک این موضوع است که بی‌نظمی در اینترنت یک نظم ضمنی ریاضی دارد. لری پیج و سرگئی برین با شمارش، تنظیم و ارزیابی ساختارهای ارتباطی توانستند نتایج جست‌وجو را به هم مربوط و نزدیک کنند، کاری که هیچ موتور جست‌وجوی دیگری نتوانسته بود انجام دهد.

تاکنون آنها این برتری را حفظ کرده‌اند. دانیل سولیوان، دبیر خبرنامه صنعتی آنلاین، گوگل را در صدر بهترین موتورهای جست‌وجو قرار داده است، پس از گوگل، یاهو (yahoo)، اسک (ASK) و MSN مایکروسافت در رتبه‌های دوم تا چهارم قرار دارند.

تعداد بازدیدکننده‌های گوگل به‌طور نسبی هر ماه نسبت به سال گذشته در همان ماه افزایش پیدا می‌کنند. به استثنای AOL که از ورودی اینترنتی مانند فناوری جست‌وجوی گوگل استفاده می‌کند، در ماه مارس گوگل میزبان نیمی از کل جست‌وجوگران اینترنتی بوده است، سهم گوگل به استثنای AOL از کل جست‌وجوگران ۴۳ درصد بود.

مهارت و توانایی ریاضی دلیل نیمی از موفقیت‌های گوگل است: توانایی تبدیل همه جست‌وجوها به پول. برعکس شرکت‌های نرم‌افزاری مانند مایکروسافت که بخش اعظم درآمد آن از محل لیسانس است،

گوگل در وهله اول یک بنگاه تبلیغاتی محسوب می‌شود. او آگهی‌های تبلیغاتی معمولی نمی‌فروشد. بلکه گوگل یک ژانر تبلیغاتی جدید و کارا به‌نام «پرداخت به ازای هر کلیک» ابداع کرده است. گوگل یک متن کوچک تبلیغاتی روی صفحات نتایج جست‌وجو قرار داده است، اما آگهی‌دهندگان فقط زمانی پول برای آن پرداخت می‌کنند که بازدیدکنندگان و کاربران اینترنتی به‌طور حتم روی آن متن کلیک کرده باشند و وارد آدرس آنها شده باشند. این سیستم روی صفحات نتایج جست‌وجو تا به‌حال خوب کار کرده و نیمی از درآمد گوگل را تامین کرده است، زیرا کلمات اصلی کاربران به گوگل اجازه می‌دهد تا آگهی‌های مناسب و مربوط به آن را روی صفحه قرار دهد.

اما در عین حال این سیستم روی دیگر صفحات وب مانند بلاگ‌ها و مقالات روزنامه هم که به‌عنوان بخشی از شبکه گوگل امضا می‌شوند، جواب داده است.

Keith H. Hammonds در مارچ ۲۰۰۳ در نشریه Fast، ۵ اصل مهم در پشت صحنه فعالیت‌های گوگل را در ارتقای کسب و کار در دنیای دیجیتال، با عنوان «آنها، این گونه رشد کردند»، این چنین معرفی می‌کند:

۱. قانون شماره یک: به کاربران بستگی دارد

در گوگل قانون مهمی وجود دارد، اگر ایده‌ای در سر داری که باعث بهبود نتیجه کار کاربران می‌شود، به ایده‌ات جامه عمل بپوشان. به استناد برخی برآوردها، گوگل میزبان سه چهارم جست‌وجوهای وب است. اما از آنجا که کامل نیست، تسلطش به‌اندازه کافی خوب نیست.

به همین دلیل گوگل باید تفسیر درستی از جست‌وجوی کاربران ترک و فنلاندی خود داشته باشد، آنهایی که عبارات جست‌وجویشان بیشتر به جملات شبیه است، و یا در زبان ژاپنی که بین کلمات هیچ فاصله‌ای وجود ندارد. گوگل نه تنها باید معنی تک تک کلمات جست‌وجو شده را درک کند، که ارتباط بین این کلمات با دیگر کلمات و ویژگی آن کلمات را به عنوان یک شیئ در صفحات وب نیز باید برای گوگل روشن شود. برای نمونه صفحاتی که عبارت جست‌وجو را به صورت پررنگ (bold) یا در گوشه بالا سمت راست نشان می‌دهند در لیست نتایج گوگل بالاتر از صفحاتی قرار خواهند گرفت که به آن اندازه، کلمه کلیدی را نمایان نکرده است.

گوگل هنوز یک محصول دارد و آن موتور جست‌وجویش است. افراد برای جست‌وجو در وب به گوگل سر می‌زنند، و هدف اصلی از صفحات اینترنتی این پایگاه ان است که مطمئن شود که کاربرانش از جست‌وجو دور نیافتاده‌اند. گوگل آنچه را که مردم مایل نیستند، به آنها نشان نمی‌دهد، چون در دراز مدت باعث شکست تجاری آنها خواهد شد.

گوگل خود را به شیوه سنتی در معرض فروش قرار نمی‌دهد. در عوض، گوگل مشاهده می‌کند و می‌شنود. گوگل ارقام ترافیک جست‌وجوها را مشاهده می‌کند و ایمیل‌های رسیده را می‌خواند. در واقع، ده کارمند تمام وقت در گوگل مشغول خواندن ایمیل‌های رسیده از طرف کاربران هستند، و آنها را به کارکنان مناسبی از گوگل ارجاع می‌دهند یا خود، به آنها پاسخ می‌دهد. مونیکا هنزینگر، مدیر بخش تحقیقات گوگل می‌گوید: تقریبا همه به بازخوردهای مخاطبان دسترسی دارند. ما همه می‌دانیم که بخش‌های مشکل سازکه کاربران از آنها گلابه دارند کدامند.

نتیجه این که، گوگل از چنین ادراک منحصر به فردی که از مخاطبان خود دارد خرسند است و نیز از صداقت و مخصوص خود. گوگل کار برجسته‌ای را مدیریت کرده است: خوش آمدن به مزاق کاربران حرفه‌ای خوگرفته به اینترنت، بدون آنکه گوگل کاربران مبتدی را از دست بدهد. گوگل حتی به رفتار کاری کاربرانی که عباراتی چون «amazon.com» را برای دسترسی به سایت Amazon.com جست‌وجو می‌کنند، دوست دارد و به کار آنها کنجکاو است. چون، همه چیز به کار کاربران گوگل، بستگی دارد.

گوگل می‌داند که چگونه کاری کند تا کاربران حرفه‌ای احساس خوبی داشته باشند. گوگل این کار را از ابتدای فعالیتش انجام داده است، هنگامی که لری و سرگئی، تکنولوژی گوگل را عرضه کردند. آنها از کاربران حرفه‌ای دعوت به عمل آوردند و به آنها احساسی بخشیدند که گویی در جای مخصوصی هستند.

barandeh24.com

اطلاعاتی در مورد حملات pharming

بخش اول

تهدیدهای جدیدی که هویت و اطلاعات کاربر را هدف قرار داده اند، رویکردهای جدید امنیتی را طلب می کند.

امروزه، حملات phishing ساده تر و کم خطرتر از تهدیدهای آنلاینی که در حال تجربه شدن هستند، به نظر می‌رسند.

حملات phishing به آسانی شناخته می‌شوند و می‌توان به سرعت آنها را از کار انداخت. جرائم سازمان یافته از این حد گذشته و پیچیدگی آنها به طرز چشم گیری افزایش یافته است. امروزه، کاربران با اشکال موذیانه تری از حمله مواجه می‌شوند و کشف و مقابله علیه آنها بسیار مشکل تر است.

گونه‌ای جدید از حمله

این گونه جدید حمله بعنوان pharming شناخته می‌شود. pharming بجای اینکه کاربر را گول بزند تا به یک ایمیل تقلبی پاسخ دهد تا او را به یک وب سایت جعلی هدایت کند، برای فریب دادن کاربر برای تسلیم هویت و اطلاعات حساسش، از روش‌های زیرکانه تری استفاده می‌کند.

این حملات از اسب‌های تروا (تروجان) برای نصب برنامه‌های کلیدخوان و برنامه‌های هدایت کننده استفاده می‌کنند تا به یک نفوذگر اجازه دهند کلمات عبور و شماره کارت‌های اعتباری را بدست آورد، بدون اینکه کاربر مجبور به انجام کاری غیرعادی باشد.

در اینجا دو مثال از چگونگی این حمله آورده شده است:

۱- کاربر یک ایمیل ظاهراً صحیح را باز می‌کند که او را تشویق می‌کند تا فایل الحاقی به ایمیل را باز کند.

این فایل الحاقی بصورت مخفیانه یک «کلیدخوان» (برنامه‌ای است که کلیدهایی را که توسط کاربر زده می‌شود، ثبت می‌کند) نصب می‌کند.

هنگامی که کاربر به بانک آنلاین خود سر می‌زند، کلیدخوان این را تشخیص می‌دهد و ورودی‌های صفحه کلید کاربر را هنگامی که وی اسم و کلمه عبور را تایپ می‌کند، ثبت می‌کند.

سپس این اطلاعات برای نفوذگر ارسال می‌شود تا برای دسترسی به حساب کاربر استفاده شود.

۲- یک کاربر ممکن است با دانلود کردن یک فایل یا مشاهده یک وب سایت که حاوی ActiveX control است، سهواً یک «هدایت کننده» (redirector) را روی سیستم خود نصب کند. این کار باعث می‌شود که فایل‌های موجود در سیستم دچار تغییراتی شود و هنگامی که کاربر به بانک آنلاین خود سر می‌زند، به وب سایت نفوذگر هدایت شود.

این عمل می‌تواند با مسموم کردن سرور DNS انجام گیرد که برای آدرس بانک آنلاین کاربر، IP وب سایت نفوذگر را می‌فرستد.

حملات پیچیده تر می‌توانند ارتباط را با بانک کاربر برقرار کنند و هنگامی که پروسه در حال انجام است، ترافیک عبوری بین کاربر و بانک (شامل کلمات عبور و اطلاعات شخصی) را مشاهده کنند.

در اصل نفوذگر خود را بین کاربران و بانک قرار می‌دهد.

از نظر تاریخی، رویکرد امنیتی که برای این نوع از حملات بکار گرفته شده است، مشابه مفهوم گارد مرزی (Boarder Guard) بوده است.

ورود موارد زیان رسان را به کامپیوتر متوقف کنید و جلوی کاربر را از رفتن به مکان‌های بد بگیرید. ابزارهایی مانند آنتی ویروس، ضدجاسوس، فایروال‌ها و تشخیص دهندگان نفوذ، همگی چنین رویکردی دارند. به هرحال، همچنانکه حملات به رشد خود ادامه می‌دهند و پیچیده تر می‌شوند، نمی‌توان از احتمال نصب شدن موفقیت آمیز یک کلیدخوان یا هدایت کننده علیرغم این گاردهای مرزی، غافل ماند.

برای سروکار داشتن با این احتمال، رویکرد متفاوت دیگری مورد نیاز است. علاوه بر ابزارهایی که ذکر آنها رفت، نیاز است که هویت و اطلاعات کاربران توسط محافظ شخصی (body guard) مراقبت شود. یعنی، نیاز است که هویت و اطلاعات شخص بدون در نظر گرفتن نوع حمله و جایی که اطلاعات کاربر به آنجا می‌رود، همواره امن باقی بماند. این نوع امنیت قابلیت‌های محافظ شخصی را برای هویت کاربر ایجاد می‌کند و اهمیتی ندارد که اطلاعات کاربر به کجا فرستاده می‌شود و کلیدخوان نصب شده است و یا اینکه نفوذگر می‌تواند ترافیک اینترنت را نظارت کند. دو قابلیت امنیتی وجود دارد که می‌تواند توانایی این محافظ شخصی را پیاده کند. اولی تصدیق هویت قوی (strong authentication) است.

امروزه، کاربران عموماً برای محافظت از هویتشان به یک کلمه عبور اطمینان می‌کنند، اما احتمال زیادی وجود دارد که کلمه عبور توسط کسی که نظاره گر login است، دزدیده شود. داشتن یک عامل اضافی برای تصدیق هویت، یعنی چیزی که کاربر باید بصورت فیزیکی داشته باشد علاوه بر آنچه که می‌داند، می‌تواند یک هویت آنلاین را در برابر حمله محافظت کند.

microrayaneh.com

تجهیزات و پیکربندی یک شبکه بی سیم

امروزه از شبکه‌های بدون کابل (Wireless) در ابعاد متفاوت و با اهداف مختلف، استفاده می‌شود.

برقراری یک تماس از طریق دستگاه موبایل، دریافت یک پیام بر روی دستگاه pager و دریافت نامه‌های الکترونیکی از طریق یک دستگاه PDA، نمونه هائی از کاربرد این نوع از شبکه‌ها می‌باشند. در همه موارد فوق، داده و یا صوت از طریق یک شبکه بدون کابل در اختیار سرویس گیرندگان قرار می‌گیرد. در صورتی که یک کاربر، برنامه و یا سازمان تمایل به ایجاد پتاسیل قابلیت حمل داده را داشته باشد، می‌تواند از شبکه‌های بدون کابل استفاده نماید. یک شبکه بدون کابل علاوه بر صرفه جوئی در زمان و هزینه کابل کشی، امکان بروز مسائل مرتبط با یک شبکه کابلی را نخواهد داشت. از شبکه‌های بدون کابل می‌توان در مکان عمومی، کتابخانه‌ها، هتل‌ها، رستوران‌ها و مدارس استفاده نمود. در همه مکان‌های فوق، می‌توان امکان دستیابی به اینترنت را نیز فراهم نمود. یکی از چالش‌های اصلی اینترنت بدون کابل، به کیفیت سرویس (QoS) ارائه شده برمی گردد. در صورتی که به هر دلیلی بر روی خط پارازیت ایجاد گردد، ممکن است ارتباط ایجاد شد ه قطع و یا امکان استفاده مطلوب از آن وجود نداشته باشد.

انواع شبکه‌های wireless

WLANS: Wireless Local Area Networks. شبکه‌های فوق، امکان دستیابی کاربران ساکن در یک منطقه محدود نظیر محوطه یک دانشگاه و یا کتابخانه را به شبکه و یا اینترنت، فراهم می‌نماید.

WPANS: Wireless Personal Area Networks. در شبکه‌های فوق، امکان ارتباط بین دستگاههای شخصی (نظیر laptop) در یک ناحیه محدود (حدود ۹۱۴ سانتی متر) فراهم می‌گردد. در این نوع شبکه‌ها از دو تکنولوژی متداول (Infra Red (IR و Bluetooth) IEEE 802.15)، استفاده می‌گردد.

WMANS: Wireless Metropolitan Area Networks. در شبکه‌های فوق، امکان ارتباط بین چندین شبکه موجود در یک شهر بزرگ فراهم می‌گردد. از شبکه‌های فوق، اغلب به عنوان شبکه‌های backup کابلی (مسی، فیبر نوری) استفاده می‌گردد.

WWANS: Wireless Wide Area Networks. در شبکه‌های فوق، امکان ارتباط بین شهرها و یا حتی کشورها و از طریق سیستم‌های ماهواره‌ای متفاوت فراهم می‌گردد. شبکه‌های فوق به سیستم‌های 2G (نسل دوم) معروف شده اند.

امنیت

برای پیاده سازی امنیت در شبکه‌های بدون کابل از سه روش متفاوت استفاده می‌شود:

WEP: Wired Equivalent Privacy. در روش فوق، هدف توقف ره گیری سیگنال‌های فرکانس رادیوئی توسط کاربران غیر مجاز بوده و برای شبکه‌های کوچک مناسب است. علت این امر به عدم وجود پروتکل خاصی به منظور مدیریت «کلید» بر می‌گردد. هر «کلید» می‌بایست به صورت دستی برای سرویس گیرندگان تعریف گردد. بدیهی است در صورت بزرگ بودن شبکه، فرآیند فوق از جمله عملیات وقت گیر برای هر مدیر شبکه خواهد بود. WEP، مبتنی بر الگوریتم رمزنگاری RC4 است که توسط RSA Data System ارائه شده است. در این رابطه همه سرویس گیرندگان و Aceess Point ها بگونه‌ای پیکربندی می‌گردند که از یک کلید مشابه برای رمزنگاری و رمزگشائی استفاده نمایند.

SSID: Service Set Identifier. روش فوق به منزله یک «رمزعبور» بوده که امکان تقسیم یک شبکه WLAN به چندین شبکه متفاوت دیگر که هر یک دارای یک شناسه منحصر بفرد می‌باشند را فراهم می‌نماید. شناسه‌های فوق، می‌بایست برای هر access point تعریف گردند. یک کامپیوتر سرویس گیرنده به منظور دستیابی به هر شبکه، می‌بایست بگونه‌ای پکربندی گردد که دارای شناسه SSID مربوط به شبکه مورد نظر باشد. در صورتی که شناسه کامپیوتر سرویس گیرنده با شناسه شبکه مورد نظر مطابقت نماید، امکان دستیابی به شبکه برای سرویس گیرنده فراهم می‌گردد.

فیلترینگ آدرس‌های MAC (Media Access Control): در روش فوق، لیستی از آدرس‌های MAC مربوط به کامپیوترهای سرویس گیرنده، برای یک Access Point تعریف می‌گردد. بدین ترتیب، صرفاً به کامپیوترهای فوق امکان دستیابی داده می‌شود. زمانی که یک کامپیوتر درخواستی را ایجاد می‌نماید، آدرس MAC آن با آدرس MAC موجود در Access Point مقایسه شده و در صورت مطابقت آنان با یکدیگر، امکان دستیابی فراهم می‌گردد. این روش از لحاظ امنیتی شرایط مناسبی را ارائه می‌نماید، ولی با توجه به این که می‌بایست هر یک از آدرس‌های MAC را برای هر Access point تعریف نمود، زمان زیادی صرف خواهد شد. استفاده از روش فوق، صرفاً در شبکه‌های کوچک بدون کابل پیشنهاد می‌گردد.

نویسنده: حمید باقری سلیمی