معرفی نرم افزار

Acresso InstallShield 2009 Professional v15

برای نصب برنامه ها و نرم افزارهای مختلف کاربران از فایل های Installer استفاده می کنند که به وسیله این installerها کاربران فایل ها و اجزای مورد نیاز نرم افزار مورد نظر خود را بر روی سیستم نصب می کنند.

بسیاری از نرم افزارها برای انجام عملیات های مختلف و اجرای درست نیاز به فایل های سیستمی در کنار خود دارند که وقتی برنامه نویسان نرم افزار خود را آماده ارائه به کاربران می کنند با ایجاد فایل های setup فایل های سیستمی مورد نیاز را نیز برای قرار گرفتن در کنار نرم افزار اصلی در درون فایل های setup قرار می دهند تا به صورت خودکار در هنگام نصب این فایل ها نیز در کنار نرم افزار کپی شده و یا حتی در صورت نیاز تغییرات سیستم نیز توسط همین فایل های نصبی تنظیم شده است بر روی سیستم اعمال شود.

برای ساخت فایل های setup نرم افزارهای بسیاری را می توان یافت و حتی بسیاری از برنامه نویسان خود اقدام به نوشتن این فایل ها می کنند اما سازگاری آن ها با همه سیستم ها همیشه یکسان نیست و به همین علت امروزه حتی بسیاری از شرکت های بزرگ تولید کننده نرم افزار سعی بر این دارند تا از برنامه های سازنده setup استفاده نمایند که در گذشته امتحان خود را به درستی پس داده اند.

InstallShieldنام یکی از معروفترین برنامه های تولید کننده فایل های setup می باشد که نسخه جدید آن برای سال ۲۰۰۹ میلادی به تازگی ارائه شده است و به کمک آن برنامه نویسان و کاربران مختلف قادر خواهند بود تا اقدام به ساختinstaller های حرفه ای با تمام نیازهای مورد نظر خود در این زمینه نمایند.

این نرم افزار به صورت کاملا حرفه ای ابزاری را در اختیار برنامه نویسان قرار می دهد تا به کمک آن یک Installer قدرتمند و بدون نقص را برای نرم افزارهای خود ایجاد نمایند.

از ویژگی های این نرم افزار می توان به قابلیت پشتیبانی از چیدن زبان مختلف برای ساخت فایلsetup ، پشتیبانی از قابلیت مدیریت قرار دادن اسکریپت کدها در فایلsetup ، دارای ۴ ابزار مخصوص برای ساخت فایل های setup با فرمتMSI ، پشتیبانی از Windows Installer 4.5 ، پشتیبانی از فایل هایVisual Studio 2008 ، قابلیت استفاده از ویژگی های NET Framework 3.5.و . . . اشاره نمود. این نرم افزار محصولی از شرکت Acresso Software می باشد.

Corel Painter X v10

هنر کمپانی Corel آماده سازی نرم افزار های گرافیکی بوده است. نرم افزار هایی فوق العاده کاربردی که کابران را به تحسین این محصولات وامی دارد.

شاید بتوان با اطمینان اعلام کرد که بزرگترین شرکت در ساخت نرم افزار های طراحی و نقاشی Corel است. چندین نرم افزار که هرکدام خصوصیات مختص به خود را دارند می توانند سلیقه کابران را به نقاشی های زنده تبدیل کنند.

یکی از محصولات بسیار معروف شرکت Corel به نام Corel Painter X v10 قدرتمندترین نرم افزار ایجاد نقاشی های طبیعی و تصاویر گرافیکی دنیا است. نرم افزاری بسیار کامل و غنی از امکانات فوق العاده که به نوعی قلم نقاش برای نقاشی به شمار می رود.

در یک کلام باید این طور بیان کرد که طرحی که کاربر بخواهد به سادگی می تواند با Corel Painter انجام دهد. محیط کاربری نرم افزار بسیار زیبا و در عین حال بسیار کارا می باشد. این محیط نرم افزاری با توجه به آن چه که از Corel سراغ داریم بسیار عادی و طبیعی است. براش ها و افکت های موجود در Corel Painter عصای دست کاربران برای نقاشی و تصویرسازی بهتر است. براش هایی سه بعدی و بسیار زیبا که برای هر سلیقه و هدفی براشی خاص دارد.

با Corel Painter می توان حتی انیمیشن هایی با فرمت های نظیر GIF و AVI تولید نمود.

ترکیب بندی رنگ ها برای ویرایش تصاویر بسیار آسان و در عین حال فوق العاده زیبا است.

به سادگی می توان رنگ ها را برای به دست آوردن رنگ مورد نظر در جعبه ای ترکیب و رنگ مورد نظر را بدست آورد. نکته ای که اکثر کاربران حرفه ای بدان توجه دارند این است که یک نرم افزار گرافیکی چه سرعتی در زمان لود و ذخیره سازی تصاویر دارد؟ در جواب این کاربران باید بیان نمود که Corel Painter سرعتی بسیار بالاتر در زمان ذخیره سازی و لود کردن نسبت به نرم افزار های مشابه دارد. این سرعت تقریبا در زمان باز کردن عکس ها ۳۵ درصد و در زمان ذخیره سازی عددی معادل ۲۰۰ درصد است.

ضمن این که Corel Painter هم با پشتیبانی از اکثر فرمت های تصویری به قدرت خود تا اندازه زیادی افزوده است. بد نیست بدانید این ابزار با این همه امکانات فوق العاده با محصول بسیار معروف کمپانی Adobe یعنی Adobe PhotoShop نیز سازگاری کامل هم دارد و می توان به سادگی تصاویر را میان این دو نرم افزار جابه جا نمود.

قابلیت های کلیدی نرم افزار Corel Painter X v10:

- محیطی ساده در عین کارآیی فوق العاده
- ترکیب رنگ ها به سادگی برای بدست آوردن رنگ مورد نظر
- سازگاری کامل با نرم افزار بسیار معروف Adobe PhotoShop
- افکت های بسیار زیبا و متنوع
- براش هایی سه بعدی و متعدد
- سرعت بسیار بالا در لود و ذخیره سازی تصاویر
- پشتیبانی از اکثر فرمت های تصویری موجود
- سرعت بسیار بالا در بازیابی و ذخیره سازی تصاویر
- طراحی انیمیشن و ذخیره سازی با فرمت های GIF و AVI
- تغییر سایز، رنگ، متون و چرخش و . . . به سادگی و با وجود ابزارهای بسیار کامل
- پشتیبان گیری از تصاویر ویرایش شده به صورت اتوماتیک
- از بین بردن رنگ قرمز موجود در عکس ها

kamyabonline.com

تکنولوژی در تلفن های سلولی

بخش پایانی

نسل جدید:

تلفن های سلولی دیجیتالی مشابه نوع آنالوگ اما متفاوت از آن کار می کنند و قادر به ایجاد کانال های ارتباطی بیشتر و با کیفیت مطلوب تری هستند. این سامانه ها اطلاعات مورد تبادل را به صورت ۰ و ۱ و فشرده شده ارسال و دریافت می کنند به این دلیل حجم سیگنال اشغالی در شبکه دیجیتالی توسط هر گوشی برابر ۱/۳ تا ۱/۱۰ سامانه آنالوگ است.

فناوری دسترسی سلولی:

سه نوع روش معمول جهت انتقال اطلاعات توسط شبکه های تلفن سلولی عبارتنداز:

دسترسی چندگانه تقسیم بسامدی (FDMA): که هر تماس را برروی یک بسامد مجزا قرار می دهد.

دسترسی چندگانه تقسیم زمانی (TDMA): هر تماس را به بخشی از یک زمان روی یک بسامد واگذار می کند.

دسترسی چندگانه تقسیم کدی (CDMA): که به هر تماس یک کد منحصر اختصاص داده و به کل طیف پخش می کند.

در قسمت اول هر یک از این سه روش عبارت «دسترسی چندگانه» را می بینیم، این بدین مفهوم است که هر سلول امکان برقراری ارتباط بیش از یک نفر را در یک زمان فراهم می آورد.

۱) FDMA :

در این روش کل طیف بسامد به چندین کانال تقسیم می شود، این روش اکثراً جهت سامانه های آنالوگ به کار می رود ولی قابلیت طراحی به صورت دیجیتال را نیز دارد، اما جهت سامانه های دیجیتالی کارآیی موثر نخواهد داشت.

۲) TDMA :

از یک پهنای باند نازک ۳۰khz کیلوهرتز و به طول ۶/۷ میلی ثانیه جهت تقسیم زمان به سه بخش استفاده می کند. هر مکالمه ۱/۳ حجم زمانی معمول را در این حالت اشغال نموده و موجب فشرده سازی و افزایش بهره وری می گردد و باعث افزایش تعداد کانال های هر سلول خواهد شد. این سامانه در باندهای ۹۰۰ و ۱۸۰۰ مگاهرتز در اروپا و آسیا و نیز ۱۹۰۰ مگاهرتز در آمریکا مورد استفاده قرار دارد. متأسفانه باند ۱۹۰۰ (Gsm) که در آمریکا کاربرد دارد با سامانه های جهانی همساز نیست.

۳) CDMA :

یک تفاوت کلی با سامانه TDMA دارد. در این روش بعد از تبدیل سیگنال ها به دیجیتال آن ها را بر روی کل پهنای باند موجود انتشار می دهند و همچنین به هر تماس و سیگنال یک کد منحصر به فرد اختصاص می دهند. در این حالت گیرنده نیز جهت بازیابی اطلاعات از کد مشابه مختص هر تلفن استفاده می نماید. بازده این سامانه ۸ الی ۱۰ برابر سامانه های آنالوگ (AMPS) است و ظرفیت را به میزان چشم گیری افزایش خواهد داد.

مختل کننده تلفن همراه:

وسیله ای است که با ارسال سیگنال های همسان با بسامد کار تلفن و با ایجاد تناوب های نامنظم، با توانی بیشتر از یک تلفن سلولی، مانع ارتباط بین گوشی و BTS سلول خواهد شد و ایجاد ارتباط و مکالمه را غیر ممکن می سازد.

این وسیله غالباً در مواردی که استفاده از تلفن همراه مخاطرات امنیتی در بردارد به کار می رود، مثلاً در مکان هایی مانند مراکز نظامی، تالارهای همایش و جلسات مهم از نظر حفظ امنیت، این وسایل می توانند ثابت و یا قابل حمل باشند.

تقویت کننده تلفن همراه:

این دستگاه وسیله ای است که قادر است سیگنال های بسامدی مربوط به تلفن همراه را که از طرف سلول (BTS) پخش می شود، حتی اگر بسیار ضعیف باشند، به طوری که گوشی تلفن قادر به تشخیص و دریافت آن ها نباشد، دریافت نموده و پس از تقویت دوباره ارسال نماید، این وسایل تقریباً شبیه تکرار کننده های رادیویی عمل می کنند. تقویت کننده ها معمولاً در نقاطی که سیگنال ها بسیار ضعیف اند (نقاط کور) مورد استفاده قرار می گیرند. همچنین می توان از آن ها جهت انتقال گستره سیگنال مثلاً انتقال سیگنال تا چندین طبقه زیرزمین ساختمان که در حالت عادی امکان پذیر نیست و یا مسیرهای مترو زیرزمین استفاده نمود.

gigapars.com

مایکروسافت هشدار داد

افزایش حمله از راه مرورگرهای اینترنت

بر اساس گزارش امنیتی مایکروسافت، حملات روی سیستم های عامل ممکن است نسبت به سال گذشته کاهش یافته باشد اما حمله به برنامه ها، موارد بدافزاری و نرم افزارهای ناخواسته در حال افزایش بوده و ۹۰ درصد از آسیب پذیری ها را تشکیل می دهند.

به گزارش ایسنا، بر اساس جدیدترین ارزیابی غول نرم افزاری از تهدیدها و آسیب پذیری ها، میزان نرم افزارهای مخرب و ناخواسته برداشته شده از رایانه ها در نیمه نخست سال جاری ۴۳ درصد افزایش یافت.

همچنین ۳۰ درصد از نرم افزارهای مخرب مبتنی بر تروژان و به شکل یک ورم یا ویروس رایانه ای و در قالب برنامه دیگری مخفی شده بودند و داده ها را پاک کرده، فایل ها را خراب و خود را پس از غیرفعال شدن مجددا نصب می کردند.

بر اساس گزارش مایکروسافت، بالاترین درصد حملات مبتنی بر مرورگرها با ۵۰ درصد مربوط به چین بوده و آمریکا با ۲۳ درصد به دنبال این کشور قرار گرفت.

میزان آلودگی ۶/۶ درصد چین که ۴۱ درصد نسبت به نیمه نخست سال ۲۰۰۷ افزایش یافت اندکی بالاتر از پیش بینی کارشناسان صنعت بود.

پژوهش مایکروسافت نشان می دهد در حالی که کارشناسان امنیتی به طراحی نرم افزار و سیستم های عامل برای مقابله با حملات ادامه می دهند مشکلات و تهدیدهای متوجه کاربران اداری و خانگی در حال تحول هستند.

مایکروسافت به مصرف کنندگان و شرکت ها پیشنهاد می کند به روزرسانی های نرم افزاری را به صورت مداوم بررسی و مورد استفاده قرار داده و برنامه های آنتی ویروس و ضد جاسوس افزار را برای افزودن یک لایه امنیتی دیگر نصب کنند.

سیستم های دفاعی در برابر حملات اینترنتی

بخش پایانی

ازدحام بسته های UDP

در این روش شخص مهاجم بسته های بدون استفاده ای از یک پورت UDP به پورت دیگر UDP روی کامپیوتر مقصد منتقل می کند و از آنجائیکه پروتکل UDP وابسته به ارتباط نیست (Connection Less)، ازدحام بسته های UDP، مشکل ساز می شود.

بمباران سرور به وسیله نامه های الکترونیکی:

این روش اغلب به وسیله کاربران غیرحرفه ای استفاده می شود و در آن شخص مهاجم هزاران نامه الکترونیکی را به یک آدرس خاص می فرستد و باعث سرریز نامه ها می شود. در این روش وقتی تعداد نامه های الکترونیکی از حدمجاز سرورهای SMTP تجاوز کند، باعث از کار افتادن سرور شده و سایر کاربران ISP از ادامه کار عاجز می شوند. این نوع حملات به آسانی قابل ردیابی هستند و با یافتن IP مبدا نامه های الکترونیکی، می توان به سایر اطلاعات موردنیاز دست یافت و جلوی حملات را گرفت.

باز شدن صفحات اینترنتی به صورت پشت سر هم:

این نوع از حملات نیز به وسیله کاربران غیرحرفه ای صورت می پذیرد. در این روش مهاجمان با برنامه های کوچک به صورت تکراری بعضی از صفحات اینترنتی را مرتبا و پشت سر هم فراخوانی می کنند. این عمل نیز باعث اشغال بسیار زیاد پهنای باند سرورها می شود و کاربران دیگر را از ادامه کار باز می دارد.

جهت رفع این مشکل باید مدیران شبکه به هر کاربر فقط امکان برقراری یک ارتباط را بدهند تا چنین مشکلاتی ایجاد نشود.

جلوگیری از سرویس دهی سرورهای غیرمتمرکز:

این نوع از حملات از جمله رایج ترین حملات اینترنتی است که در آن هزاران یا ده ها هزار کامپیوتر آسیب خواهد دید.

اغلب این حملات بدین صورت است که فایلی در کامپیوترهای آسیب دیده می نشیند و منتظر دستور فرد مهاجم می ماند، وقتی که شخص مهاجم دستور ازدحام بسته های کنترل پیام ها را می دهد، به سرعت بسته های ICMP روی کامپیوترهای مختلف پخش شده و باعث از کارافتادن کامپیوترهای راه دور می شوند.

امروزه امکانات و برنامه های زیادی برای این نوع حملات وجود دارد؛ به گونه ای که ارتشی از فایل های جست وجوگر، سرویس ها و پورت های سرور را جست وجو می کنند تا نقاط ضعف آنها را پیدا کنند و به صورت گروهی حملاتی را به سرورهای مختلف انجام دهند.

حل این مشکل به وسیله ایمن سازی تک تک کامپیوترها ممکن نیست زیرا فیلترکردن و یا دنبال کردن ترافیک حملات به علت شباهت آنها با ترافیک واقعی شبکه، بسیار دشوار است. از آنجائیکه همواره تعداد بسیار زیادی از کامپیوترهای ناامن روی اینترنت وجود دارد، این کامپیوترها محل بسیار مناسبی برای ایجاد حملات جدید هستند.

از آنجائیکه حمله به سیستم های غیرمتمرکز منجر به بروز مشکلات بسیار جدی می شود، بنابراین برای جلوگیری از آنها باید اصول خاصی در نظر گرفته شود:

۱- استفاده از راهکارهای غیرمتمرکز برای سیستم های غیرمتمرکز.

۲- اجتناب از راهکارهای مضر برای کاربران قانونی.

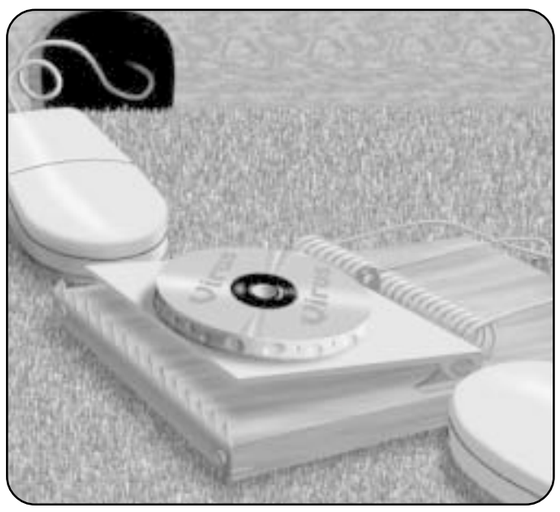
۳- ایمن سازی سیستم در مقابل تهدیدات داخلی و خارجی

۴- طراحی سیستم های عملی برای هماهنگی با مشکلات واقعی.

۵- ارائه راه حل های قابل اجرا در محیط های کوچک و تعمیم آنها به کل سیستم ها.

راه حل هایی که برای حملات غیرمتمرکز ارائه می شود، اغلب به صورت محدودکردن سرویس ها و یا قطع آنها هستند که مشکلاتی جدی برای فعایت های قانونی ایجاد می کنند.

اما در اصل باید برای جلوگیری از این حملات، گره هایی را که دچار مشکل شده اند، شناسایی و آنها را ایزوله کرد و یا از شبکه بیرون انداخت و این عملیات باید به ترتیبی صورت پذیرد که بهترین نتیجه حاصل شود.



DefCOMیکی از سیستم های دفاعی در برابر این حملات است که از چندین گره امنیتی غیرمتجانس تشکیل شده است. این گره ها ترافیک شبکه را بررسی کرده و سپس نرخ مناسب ترافیک در شبکه را برای جلوگیری از ترافیک تقلبی مشخص می کنند.

درصورت حمله، کامپیوتر قربانی پیام خطر می دهد و کامپیوتر امنیتی آن را به همه کامپیوترهای امنیتی دیگر می فرستد تا همه در حالت تدافعی قرار گیرند.

از این به بعد کامپیوترهای امنیتی پیام های بین خود را با برچسب خاصی می فرستند تا ارتباطی امن بین خودشان برقرار شود؛ بدین ترتیب ریشه حمله را پیدا می کنند. در این ارتباط داده های شبکه با ۳ نوع برچسب متفاوت ارسال و دریافت می شوند:

۱- ترافیک بدون برچسب که ترکیبی از داده های خوب و بد است.

۲- ترافیک کنترل شده که با نرخ پایین مبادله می شود.

۳- ترافیک قانونی که ترافیک مجاز شبکه است.

بررسی روش های مختلف حملات اینترنتی و راهکارهای مقابله با آنها نشان می دهد که امکان برطرف کردن کامل آنها وجود ندارد و آنچه که مدیران شبکه ها قادر به انجام آنها هستند، بررسی چگونگی حملات اینترنتی است تا تدابیری را جهت جلوگیری از تکرار آنها بیندیشند.

jonoobiha.com

خوانندگان محترم

شما می توانید مقالات و یادداشت های خود را به پست الکترونیکیAbrar_ eq_it @ yahoo.com ارسال نمایید.

دانستنی ها

IPSecچیست؟

IP SecurityیاIPSec رشته ای از پروتکل هاست که برای ایجاد VPN مورد استفاده قرارمی گیرند. مطابق با تعریف IETF (Internet Engineering Task Force) پروتکل IPSec به این شکل تعریف می شود:

یک پروتکل امنیتی در لایه شبکه تا خدمات امنیتی رمزنگاری را تامین کند. خدماتی که به صورت منعطفی به پشتیبانی ترکیبی از تایید هویت، جامعیت، کنترل دسترسی و محرمانگی بپردازد.

در اکثر سناریوها مورد استفاده، IPSec به شما امکان می دهد تا یک تونل رمزشده را بین دو شبکه خصوصی ایجاد کنید. همچنین امکان تأیید هویت دو سر تونل را نیز برای شما فراهم می کند. اما IPSec تنها به ترافیک مبتنی بر IP اجازه بسته بندی و رمزنگاری می دهد و درصورتی که ترافیک غیر IP نیز در شبکه وجود داشته باشد، باید از پروتکل دیگری مانند GRE در کنار IPSec استفاده کرد.

IPSecبه استاندارد de facto در صنعت برای ساخت VPNتبدیل شده است. بسیاری از فروشندگان تجهیزات شبکه، IPSec را پیاده سازی کرده اند و بنابراین امکان کار با انواع مختلف تجهیزات از شرکتهای مختلف، IPSec را به یک انتخاب خوب برای ساخت VPN مبدل کرده است.

انواع IPSec VPN

شیوه های مختلفی برای دسته بندی IPSec VPN وجود دارد اما از نظر طراحی، IPSec برای حل دو مسأله مورد استفاده قرار می گیرد:

۱- اتصال یکپارچه دو شبکه خصوصی و ایجاد یک شبکه مجازی خصوصی

۲- توسعه یک شبکه خصوصی برای دسترسی کاربران از راه دور به آن شبکه به عنوان بخشی از شبکه امن

بر همین اساس، IPSec VPNها را نیز می توان به دو دسته اصلی تقسیم کرد:

۱- پیاده سازی LAN-to-LAN IPSec

این عبارت معمولا برای توصیف یک تونل IPSec بین دو شبکه محلی به کار می رود. در این حالت دو شبکه محلی با کمک تونل IPSec و از طریق یک شبکه عمومی با هم ارتباط برقرار می کنند به گونه ای که کاربران هر شبکه محلی به منابع شبکه محلی دیگر، به عنوان عضوی از آن شبکه، دسترسی دارند. IPSec به شما امکان می دهد که تعریف کنید چه داده ای و چگونه باید رمزنگاری شود.

۲- پیاده سازی Remote-Access Client IPSec

این نوع از VPNها زمانی ایجاد می شوند که یک کاربر از راه دور و با استفاده از IPSec client نصب شده بر روی رایانه اش، به یک روتر IPSec یا Access server متصل می شود. معمولا این رایانه های دسترسی از راه دور به یک شبکه عمومی یا اینترنت و با کمک روش dialup یا روشهای مشابه متصل می شوند. زمانی که این رایانه به اینترنت یا شبکه عمومی متصل می شود، IPSec client موجود بر روی آن می تواند یک تونل رمز شده را بر روی شبکه عمومی ایجاد کند که مقصد آن یک دستگاه پایانی IPSec، مانند یک روتر، که بر لبه شبکه خصوصی مورد نظر که کاربر قصد ورود به آن را دارد، باشد.

در روش اول تعداد پایانه های IPSec محدود است اما با کمک روش دوم می توان تعداد پایانه ها را به ده ها هزار رساند که برای پیاده سازی های بزرگ مناسب است.

ساختار IPSec

IPSecبرای ایجاد یک بستر امن یکپارچه، سه پروتکل را با هم ترکیب می کند:

۱- پروتکل مبادله کلید اینترنتی (Internet Key Exchange یا IKE)

این پروتکل مسئول طی کردن مشخصه های تونل IPSec بین دو طرف است. وظایف این پروتکل عبارتند از:

- طی کردن پارامترهای پروتکل
- مبادله کلیدهای عمومی
- تایید هویت هر دو طرف
- مدیریت کلیدها پس از مبادله

IKEمشکل پیاده سازی های دستی و غیر قابل تغییر IPSecرا با خودکار کردن کل پردازه مبادله کلید حل می کند. این امر یکی از نیازهای حیاتیIPSec است IKE .خود از سه پروتکل تشکیل می شود:

SKEME- مکانیزمی را برای استفاده از رمزنگاری کلید عمومی در جهت تأیید هویت تامین می کند.

Oakley- مکانیزم مبتنی بر حالتی را برای رسیدن به یک کلید رمزنگاری، بین دو پایانه IPSec تامین می کند.

ISAKMP- معماری تبادل پیغام را شامل قالب بسته ها و حالت گذار تعریف می کند.

IKE به عنوان استاندارد RFC 2409 تعریف شده است. با وجودی که IKE کارایی و عملکرد خوبی را برایIPSec تأمین می کند، اما بعضی کمبودها در ساختار آن باعث شده است تا پیاده سازی آن مشکل باشد، بنابراین سعی شده است تا تغییراتی در آن اعمال شود و استاندارد جدیدی ارائه شود کهIKE v2نام خواهد داشت.

۲- پروتکل Encapsulating Security Payload یا ESP

این پروتکل امکان رمزنگاری، تأیید هویت و تأمین امنیت داده را فراهم می کند.

۳- پروتکل سرآیند تأیید هویت (Authentication Header یا AH)

این پروتکل برای تأیید هویت و تأمین امنیت داده به کار می رود.

microrayaneh.com