بسمه تعالی

رمزنگاری
پروتکل امنیت لایه شبکه
IPsec

تهیه کننده:

سید محمد حسینی

۱۳۸۵/۲/۳۰

بخش دوم: رمزنگاری پروتکل امنیت در لایه شبکه IPsec

در گذر از لایه های OSI و رمزنگاری آنها به لایه سوم یعنی لایه مسیریابی می رسیم. جائیکه با پروتکل لایه شبکه یا IP برخورد می کنیم یعنی پروتکل (Internet Protocol). پیامهای پروتکلIP ،پکت یا بسته نامیده می شود. ما برای سهولت کار از همین آغاز به آن پکت می گوئیم. هر پکت دارای سرآیند(header) است که بطور مجزا روی شبکه ارسال و دریافت می شوند. در واقع در محل ارسال یک پیام ، یک پکت به پکت های مختلفی شکسته می شوند و سپس هر پکت با سرآیند هایش Paylaod شده،ارسال می گردد. در طرف دریافت کننده، بعد از دریافت پکت ها بهم وصل (assembeled) می شوند. و البته هر سرآیند از چندین فیلد تشکیل شده است که محتوای آن ها بیان کننده جزئیات راجع به آدرس ارسال کننده و دریافت کننده ،طول پکت و چیزهایی از این دست است. که بعداً راجع به آن بطور دقیق سخن خواهیم گفت.

IPsec, IKE .۱

وقتی ما ادعا می کنیم که روی IP دارم کار امنیتی می کنیم. پس قصد دارم راجع به تضمین محرمانگی (guarantee confidentially) احراز هویت(authenticity) و تمامیت اطلاعات (Integrity) ارسال و دریافت کارهایی انجام دهیم. بعد از اینکه ارائه دهنده آن یکسری اتغییرات روی این پرو تکل انجام داد. IPsec استاندارد شده توسط IETF پیاده سازی شد. و از آنجا یکی از اجزای ثابت IP نسخه جدید یعنی IPV6 گردید که قرار است تا چند سال آینده جانشینی IP فعلی گردد.

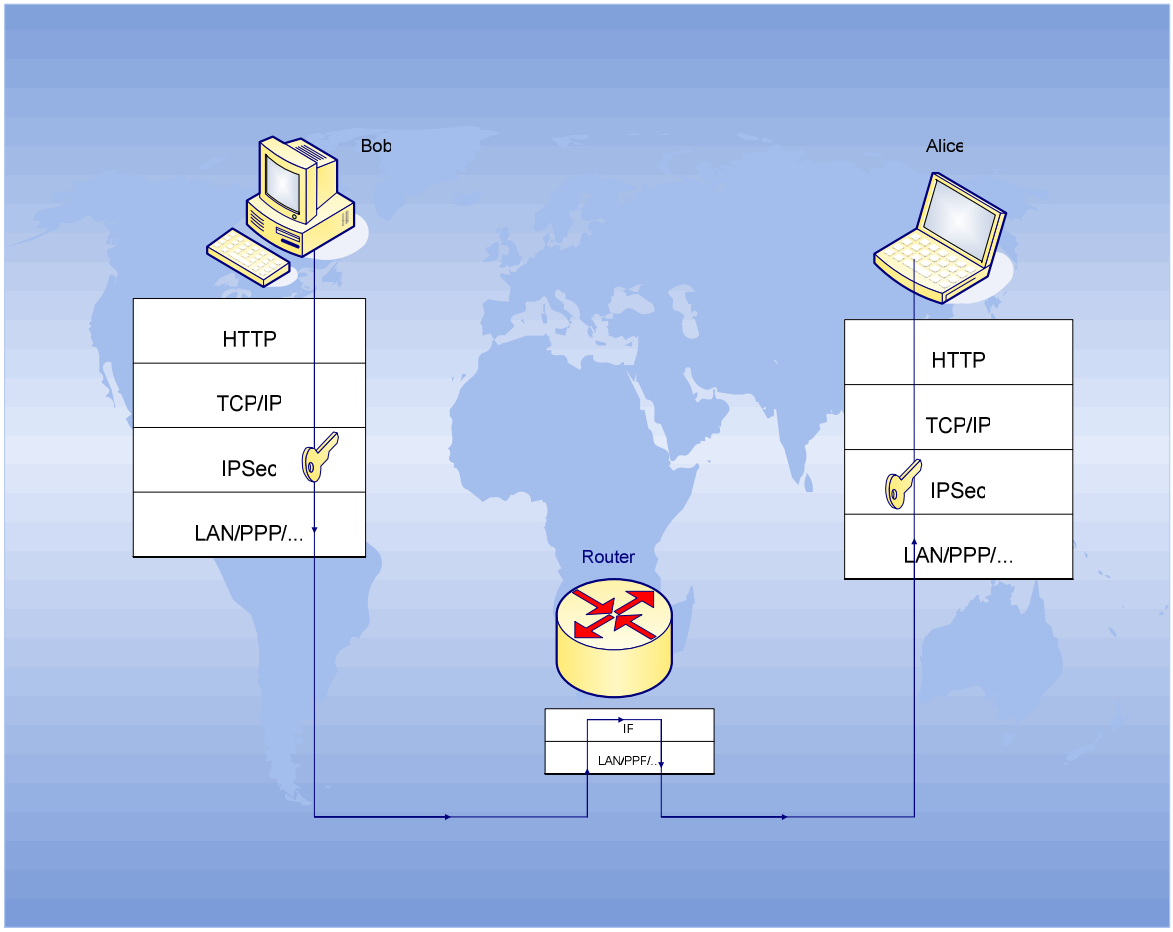
IPsec توانایی رمزنگاری پکت های IP با استفاده از ضمانت تمامیت داده ارسال و دریافت از طریق تابع درهم سازی کلیدهای عمومی [۱] فراهم می شود. برای ارتباطات مناسب امنیتی شرایطی لازم است که در صورت برآورده شدن این شرایط ما ارتباط امن خواهیم داشت. در این مورد داشتن یک کلید سری بین باب و آلیس[×] قابل انجام شدن است.

---

[۱]–Public key hash function

[*] در ادبیات امنیتي باب و الیس (Bob &Alice) طرفین ارسال ودریافت اطلاعات هستند که میخواهند یک جریان عادي وسالم تبادل اطلاعات داشته باشند.

امکانات IPsec ،نرم افزار های کاربردی رمزنگاری لایهٔ سوم مدل OSI باعث می شود ارتباط اینترنتی امن بین کاربران بوجود آید. همچنین تبادل کلید (Exchange key) نظارت و سازماندهی امنیت یکپارچه ای را بوجود می آورد.درحالیکه IPsec این موضوع رادر دورن



شکل ۱.امکانات رمزنگاری IPsec در لایه سوم مدل OSIنشان می دهد.

خود ندیده است، این موضوع توسط تبادل کلید اینترنتی(۱) یا IKE انجام می شود. هر چند IKE جزئی از اجزای IPsec نیست و بطور تنگاتنگی با IPsec در ارتباط است، با این وجود می تواند بخشی از این پروتکل گردد.

۲ . IPsec چیست:

اجازه دهید بدون در نظر گرفتنIKE به بررسی پروتکل IPsec بپردازیم. این پروتکل از دو جزء تشکیل یافته است. یک جزء آن رمزنگاری پکت های ارسال و دریافت را انجام می

دهد و موسوم به ESP یا Payload امنیت بسته بندی است. جزدیگر آن که سرآیند احراز هویت یا AH نام دارد، بعد از تدارک تمامیت اطلاعات و احراز هویت یک تابع درهم سازی کلید عمومی Public key hash function را بکار می گیرد. با این اوصاف باید بگوئیم IPsec اجزاء دقیق و مناسبی را بکار برده است.

۲-۱ ESP چیست :

اولین بخش IPsec همان ESP است . که مخفف Encapsulated security Payload بوده و توسط RFC۲۴۰۶ توصیف شده است. این جزء از IPsec رمزنگاری Payload های پکت های ارسال را انجام می دهد و همچنین در نسخه های جدیدتر این بخش، امکان تهیه تابع درهم سازی کلید عمومی دیده شده است. بیشترین فیلدهای سرآیند این بخش رمزنگاری نشده اند. چراکه روترها باید بتوانند آنها را بخوانند. ESP همچنین فیلدها سرآیند اضافی را در میان سایر فیلدهای اضافه کرده است ، چنانچه این فیلدها در IPV6 مورد استفاده قرار نگیرد این بخش جزء آخرین بخشها ؛یعنی قبل از شروع Payload بعدی قرار می گیرند و این قسمت خودش بطور مجزا رمز نگاری می شود.

ESP پروسه بکارگیری را تعریف نمی کند بدین معنی که پروسه رمزنگاری و تابع درهم سازی کلید عمومی هر چند در ESP مورد استفاده قرار می گیرد اما ESP توصیف این پروسه را بعهده ندارد.در RFC۲۴۰۵ روش بکارگیری ESP در حالت CBC همچون امکان پروسه رمزنگاری بیان شده است. در RFCشمارهٔ ۲۴۵۱، Triple DES و flowfish روشهای دیگری ارائه داده است. در RFC های ۲۸۵۷ و۲۴۰۷ و۲۴۵۴ ،از روشهاای دیگر می تواند استفاده کند.

مدل انتقال(Trasport Mode) :

ESP دو حالت دارد یک حالت همان حالت انتقال یا Transport Mode می باشد. در این روش ابتدا بخشهای پکت IP رمز شده و سپس بدون تغییر ارسال می شود. این بدین معناست که آنچه رمزنگاری شده درست بعد از اینکه توسط TCP یا UDP دست به دست ارسال شد بدون اینکه به اجزاء کوچکتر تقسیم شود بدون تغییر خواهد ماند.

حالت تونل (Tunnel Mode)

دراین روش کل پکت IPرمز نگاری ، سپس در بخشی از Payload **پکت IP بسته بندی می شود. زیرا در این روش، اولین فیلد پکت IP تا اندازه ای کوچک بوده و قابل خواندن می باشد. تا اینکه جلوی کوچکترین افشاسازی اطلاعات گرفته شود. این روش وقتی می تواند مورد استفاده قرار گیرد که بخشهایی از این پکت مانند آدرس ارسال و دریافت می باید غیر قابل خوانده شدن باشد. حالت تونل یکی از اصلی ترین بخشهای شبکه های اختصاصی مجازی (VPN) می باشد.**

۲-۲ . AH چیست:

AH سرآیند احراز هویت یا Authentication Header **دومین بخش IPsec است. این پروتکل توسط REC۲۴۰۲ توصیف شده است .AH یا سرآیند احزا هویت فیلد سرآیند زیادی برای نسبت دادن به زمینه ارسال و همچنین سرآیند های دیگری را برای پاسخ به تابع درهم سازی کلید عمومی ارسال شده تدارک می بیند. تابع درهم سازی کلید عمومی روی** Payload **ها فیلدهای IP پکت مورد استفاده قرار می گیرد. این موضوع هدف سرآیند احراز هویت را بیان می دارد. چون اگر آلیس بخواهد از طریق IP با باب ارتباط برقرار کند. بدون اینکه بتواند جاعلی را تشخیص دهد که دست به جعل پکت هایش می زند به کارش ادامه خواهد داد.**

همچنین باید توجه داشته باشیم بخشهایی از پکت که در طول انتقال پکت مقدارشان عوض می شود مثل Counter **ها نباید شامل حال توابع** hash **شود یعنی هیچ تغییری روی آن نباید انجام گردد. بنابراین فیلدهای غیر قابل تغییر تحت تابع درهم سازی کلید عمومی قرار می گیرند اما آدرسهای ارسال و دریافت از این قاعده مستثناء هستند.**

روش کار کلید وابسته توابع hash **به این شکل است که باب یک پکت به آلیس ارسال می دارد و سپس نتیجه کلید وابسته را محاسبه کرده و در AH می نویسد. آلیس هم همین کار را می کند یعنی پکتی به باب تهیه شده و فقط این دو از کلیدی که استفاده کرده اند با خبرند. جاعل هرگز نمیتواند تغییری در پکت بدهد پس به آن دسترسی نخواهد داشت.**

نکته قابل توجه اینکه حتی اگرچند متخصص احراز هویت روی AH specification **کار کنند نمی تواند مشخص کند که توابع** hash **رمزنگاری[۱] بکار گرفته است یا خیر.** RFC **ها**

[۱]- Cryptography hash function

که بکارگیری توابع hash رمزنگاری را در ESP تعیین می کنند صریحاً مـی گوینـد پروسـه رمزنگاری توابع hash همانطور که برای ESP ها وجود دارد برای AH هم وجود دارد. البته آلیس وباب توابـع دیگـر را نیـز مـی تواننـد بکـار گیرنـد بـشرط آنکـه هـر دو آن توابـع را پشتیبانی کنند اصولاً بجای تابع درهـم سـازی کلیـد عمـومی ، مـی تـوان از امـضاء دیجیتـالی استفاده کرد. زیرا امضاء دیجیتالی نسبتاً کُند هستند ولی بنظر می رسد خیلـی مناسـب لایـه کاربرد نباشند.

درست همانطور که ESP با دو حالت خودش می تواند کار کند،AH هم چنـین اسـت یعنـی روش کار مطابق با ESP است. یعنی در حالـت انتقـال (Transport mode) پکـت هـایIP موجود ، شکسته شده و درحالت تونل کل پکـت IP داخـل پکـت بزرگتـر Payload شـده و یک پکت IP جدیدی را می سازند.

۳ . IKE چیست؟

ابتدا بهتراست بحث راجع به ماهیت این موضوع داشته باشیم. قبلاً گفتیم که IPsec هر چنـد زمینه امنیت و ارتباط بین طرفین را حمایت و پشتیبانی می کند امـا مـدیریت و ایجـاد کننـده این امنیت نیست مطابق آنچه گفته شد آلیس و باب مـی پندارنـد IPsec دارای کلیـد سـری مشترک – کلید تبادلی – است در حالیکه چنین نیست. چنـین پروتکـل قدرتمنـدی تنهـا بـه شرایطی چنین محیط امنی را ایجاد می کند که با تشریک مساعی پروتکـل دیگـری کـه ایـن فاکتور مهم را برآورده می کننـد کـار کنـد و آن چیـزی نیـست مگـر IKE[۲] یـا تبـادل کلیـد اینترنتی که توسط IETF تهیه شده است.

۳-۱ . ضرورت IKE

این روزها مباحث زیادی حول و حوشIPsec بوجود آمده است . و در این مـورد اساسـاً دو دیدگاه وجود دارد. یکی از این دیدگاه حاکی از این است که IKE بیشترین انعطاف پذیری و غنی ترین پروتکل مؤثر در لایه هفتم است. از نظر این گـروه پروتکلهـای دیگـر یعنـی ISAKMP ، Oakley وSKEME نیز از اهمیت برخوردارند. دیـدگاه دیگـر نظـر پیچیـده

[۲] – Internet Key Exchange

دیگری را پیش می کشند. بنظر آنان ، باید از پروتکل مدیریت کلید ساده [1] یا (SKIP) در لایه سوم مدل OSI استفاد کرد بدون اینکه به عملیات تابعی زیاد استفاده کرد.بعد از مباحث طولانی در موضوعاتOakley-SKEHE; ISAKMP پیروز شد. با این وجود باید بگوئیم IKE خیلی پیچیده است و امکانات زیادی دارد.

۲-۳. ISAKMP چیست؟

بمنظور درک IKE ، یکی از بهترین موارد که آگاهی بیشتری از بقیهٔ در مورد امکانات و توانایی های IKE دارد همان ISAKMP است. این (پروتکل) مخفف Internet Security Association and key Management Protocol **است.و بعدها بایک وقفه، توسط مؤسسه NSA پیاده سازی شد و حال در ۲۴۰۸ RFC استاندارد شده است.**

پیامهای پروتکل ISAKMP

ISAKMP را یک پروتکل نباید بدانیم، بلکه یک مجموعهٔ meccano ، بهمراه پروتکل رمزنگاری است که می تواند همگردانی [2] شود.

بدین منظور ISAKMP قالبی برای پیامهای پروتکل که بتواند پروتکلها را تعیین کند تعریف کرده است. پیامهای پروتکل ISAKMP همیشه به لایه هفتم انتقال می یابد تا پروتکل UDP در لایه سوم مورد استفاده قرار گیرد. استفاده از این پروتکل نقطه عطفی در پیامهای پروتکل ISAKMP مانند هر پروتکل دیگری شامل سرآیندها و Payload هاست. برایPayload های ISAKMP ،۱۳ نوع کاملاً مختلف را تعریف میکند .انواع رمزنگاری داده ها می تواند بجای نوع Payload دیگر از مقادیر hash بوسیله یک امضاء دیجیتال تعیین شده در پیامهای پروتکل ISAKMP انتقال یابد.

در پیامهای پروتکل ISAKMP سرآیند آدرس ارسال کننده و دریافت کننده وجود ندارد ولی بوسیله لایه پایین UDP بارگذاری می شود. هر سرآیند ISAKMP دو فیلد برای cookie های ارسال و دریافت دارد. این سرآیندهای cookie مقادیر ۳۲ بیتی هستند. اما اگر او قبلاً خودش یک پیام ISAKMP را از باب دریافت کرده باشد بنابراین او

---

[1] - simple key Management protocol

[2] - compile

از cookie باب باخبر خواهد شد. پس او این cookie را به cookie های ارسال کننده اش اضافه خواهد نمود.یک cookie یک جواز همگردانی (compiled) برای باب است تا آنرا در یک مجمع امنیت مشخصی[1] (SA) جا دهد. علاوه بر این cookie ها می توانند از تهاجمات انکار سرویس جلوگیری کند.

اگر جاسوسی سعی داشته باشد تا آلیس را با ارسال پیامهای ISAKMP غلط سرریز کند، آلیس به سادگی می تواند همهٔ پیامها را بلافاصله فیلتر (پالایه) کند.

این cookie ها فقط هنگامی از کارمی فتد که جاسوس بخواهد ارتباط بین آلیس و باب را قطع کند. یعنی جاسوس سعی خواهد کرد Cookie ها را در میان راه بدوزد اما سادگی پیامهای ISAKMP به آلیس بیرون از این حیطه خواهد بود.

ISAKMP دو مرحله دارد

ISAKMP از دو مرحله تشکیل شده است. در اولین مرحله یک امنیت متمرکز و یکپارچه تشکیل می شود بدین معنی که بطور طبیعی (نرمال) یک الگوریتم متقارن برای اینکار بوجود می آید. امنیت متمرکز و یکپارچه ISAKMP-SA نامیده می شود. در مرحله دوم ISAKMP-SA برای تشکیل هر تعداد از امنیت یکپارچه بیشتر (بطور مثال در IPsec) بکار می رود. در این مرحله الگوریتم نا متقارن می تواند بطور طبیعی توزیع گردد (dispensed) چرا که بار کردن چنین الگوریتمی خیلی سنگین خواهد بود. عملکرد این دو مرحله باید خیلی استادانه انجام شود و آن خیلی جالب خواهد بود. در اولین مرحله می تواند با دقت توسط سیستم های عامل آلیس و باب انجام شود در دومین مرحله، آلیس و باب سریعاً می تواند بدون اینکه هزینه های الگوریتم نا متقارن را بپردازند،ارتباطی را بین هم بوجود آورند یا حتی این ارتباط را قطع کنند.

۲-۳ . IKE چگونه از ISAKMP استفاده می کند

[1] – specific security associate on: در پروتکل AH ، اطلاعات کپسوله کردن و بازگشائی پکت کپسوله شده ، با استفاده ازروشهای ذخیرهٔ سازی، کلیدهای سری،الگوریتم هاIP و آدرسها درگیر در تبادلات اینترنتی را ذخیره نمایند و بکار میگیرد. همهٔ این پارامترهای مورد نیاز جهت حفاظت دیتاگرامIP درجایی بنام مجمع امنیتی یا SA ها ذخیره می شوند. این مجمع امنیتی به نوبت در پایگاه دادهٔ مجمع امنیتی[15] یا (SAD) ذخیره می شوند.برای کسب اطلاعات بیشتربه مقا له نگارنده تحت عنوان پروتکل IPSecدر همین وب سایت مراجعه کنید.

ارتباط بین این دو خیلی ساده است.IKE یک پروتکل کاملاً هم بندی شده(assembled) از پیامهای پروتکل ISAKMP است که توسط IKE به دقت انجام می شود. در فاز اول ISAKMP-SA تشکیل می شود (بهمین علت می تواند IKE-SAنامیده شود،در مرحلهٔ دوم بر همین اساس،یک مجمع امنیت برای (IPsec SAها) تشکیل می شوند.انجام کامل IKE توسط دو پروتکل فوق الذکر اداره می شود.Qakleyو ,SKEME

یکی از مهمترین اجزای IKE همان کلید تبادل دیفن هیلمن[1] است، که برای ایجاد یک کلید سری بین آلیس و باب بکار می رود. (برای اینکه امنیت بیشتری را ارائه کند) و کلاً IKE پنج نوع مختلف کلید دیفن هیلمن را ارائه می کند. یعنی الیس و باب یا می توانند رویه کلاسیک که سه کلید به طول ۷۶۸ ، ۱۰۲۴ ویا ۱۶۸۰ بیت را بکار ببرد یا اینکه شِقِ دیگری که ممکن است دو نوع مختلف ECDH روی کلیدهای ۱۸۵ یا ۱۵۵ بیتی را بکار ببرد.

مرحله اول IKE (IKE Phase 1)

در اولین فاز پروتکل IKE، آلیس و باب Cookie را رد و بدل می کنند، روی پروسه ها و پارامترها مذاکره کرده و بطور دستی اجازه عبور و مرور را بهم می دهند و کلید تبادل دیفن هیلمن را برای تشکیل شدن اولیه یک IKE-SA را بوجود می آورند. IKE دو روش انجام یافتن این کارها را ارائه می کند.

۱- اولین روش همان حالت اصلی (main mode) است. در حالت اصلی، آلیس و باب به نوبت به یکدیگر شش پیام پروتکل ارسال می کنند.

- در اولین دو پیام پروتکلی، Cookie ها و پارامترها انتقال می یابد و این دو روی پروسه ها و پارامترها با هم مذاکره می کنند.
- سومین و چهارمین پیام، برای انتقال یک کلید تبادلی دیفن هیلمن بکار می رود.
- پنجمین و ششمین پیامها، احراز هویت و تمامیت کلیدهای دیفن هیلمن تبادلی مورد بررسی قرار میگیرد تا اعتماد فی مابین الیس و باب جلب شود، اگر آلیس و باب قبلاً یک کلید مشترک سری داشته باشند پس احراز هویت با بکارگیری کلید وابسته تابع hash انجام خواهد شد تا بتوانند کلید تبادلی دیفن هیلمن را بکار برند. این دو می توانند بجای استفاده از مقادیر hash، امضاء دیجیتالی برای هم ارسال کنند. که در واقع نوعی

1- Diffie – Hellman key exchange

کلید تبادلی از نوع دیفن هیلمن است. یک گواهینامه دیجیتالی نیز می تواند بهمراه امضاء دیجیتالی ارسال شود تا اجازه چک شدن امضاء ها را انجام دهد. روش دیگری که می تواند مورد استفاده قرار گیرد احراز هویتی است که باید با یک پروسه درخواست – پاسخ[۲] انجام گیرد. اگر آلیس و باب آنرا بکار گیرند، در پیامهای سوم و چهارمشان به طرف مقابل یک مقدار تصادفی (nonce) ارسال خواهند کرد، که سپس آنها کلید طرف مقابل رمز خواهد شد. این کلیدهای عمومی معمولاً یک کلید RSA یا حتی اجزای یک گواهینامه دیجیتالی می تواند باشد ، این گواهینامه دیجیتالی از یک سرور (ارائه کننده) گواهینامه دریافت می شود.

در پنجمین و ششمین پیام آنها به یکدیگر مقادیر hash کلید تصادفی را ارسال خواهند کرد. برای مرحله اول IKE که حالت اصلی آن است، همچنین حالت تهاجمی یا (aggressive mode) وجود دارد که حالت ساده تری است ولی تا حدودی کارآمد و موثر است. در این حالت اولین پیام آلیس ارسال یک Cookie به باب است. او پروسه ها و پارامترهای پیشنهادی خود را به همراه note مرز شده و کلید عمومی دفن هیلمن را بکار می برد. باب به آلیس جواب می دهد. جواب باب، همراه با Cookie او، پروسه های پذیرفته او، و کلید عمومی دیفن هیلمن مقادیر hash یا امضاء خواهد بود، نهایتاً آلیس به باب پیامهایی را ارسال می کند که ۱/۳ یا کمتر از پیامهای مرحله اول شامل موارد فوق خواهد بود.

در پایان مرحله اول، آلیس و باب یک مجمع امنیت خواهند داشت، علاوه بر آن یک کلید سری عمومی که آنها می توانند براساس ارتباطات IPsec بکار رود. چون نتیجه احراز هویت این خواهد بود که آنها شرکاء اصلی و واقعی خودشان را خواهند شناخت.

مرحله دوم IKE (IKE Phase 2)

در فاز دوم ISAKMP-SA ساخته شده در مرحله اول مورد استفاده قرار میگیرد. و نتیجه اش کلید سری عمومی است که آلیس و باب برای امنیت متمرکز بیشتر (IPsec SA) روی IPsec بکار می گیرند. علاوه بر اینکه دو حالت استفاده شده در مرحله اول (حالت اصلی و حالت تهاجمی)، IKE مشخص، حالتFurther که حالت سریع یا (quick mode) نامیده می شودرا خواهد داشت. در این حالت، آلیس ابتدا یک پیام پروتکلی به باب ارسال می کند، و دریافت

2- exchallange – response procedures

می کند جواب از خودش، دوباره آنرا به طرف مقابل ارسال می کند، بنابراین سه پیام وجـود خواهد داشت.

در حالت سریع، در الگوریتم نامتقارن آلیس و باب هر دو با هم نمی توانند هزینـه احـراز هویت و کلید تبادلی را یکجا داشته باشند. زیرا که هر دوی اینهـا قـبلاً در مرحلـه اول انجـام شده است. اگر ارسال بطرف مقابل بطور کمال امنیت اجـرا شـود، بـا ایـن وجـود یـک کلیـد تبادلی دیفن هیلمن می تواند انتقال یابد. پیامهای پروتکلی بیشتر علاوه بر پیامهای پروتکلـی در حالت اصلی، حالت تهـاجمی و حالـت سـریع، IKE دو نـوع پیـام پروتکلـی دیگـر را مهیـا می کند. اینها اساساً برای ایجادمجمع امنیت بکار می‌رود. یکی از این حالت ها پیامهای خطا و وضعیت را برای ارسال فعال می سـازد. کـاربرد دیگـری ایـن اسـت کـه آلـیس و بـاب روی پارامترهای جدید کلید تبادلی دیفن هیلمن با هم مذاکره و توافق کنند.

SKIP -۴

SKIP پروتکلی است که بعد از SKEME , Oakley , SAKMP توسط IETF معرفی شد. چـرا کـه ایـن پروتکـل اهمیـت خـودش را چنـد سـال حفـظ کـرده اسـت. ایـن پروتکـل توسـط شرکتMicrosystem ***SUN*** پیاده سازی شـده و مـشابه بـا IKE آن کلیـدهای تبـادلی دیفـن هیلمن را بکار می برد اما اینبار با رهیـافتی دیگـر. امـا SKIP اجـرای پروتکلهـای تبـادلی[۱] را پشتیبانی نمی کند. مطابق با SKIP ، هر پکت IP سرآیندهای مخصوصی الحاقی [۱] شامل همـه اطلاعات دریافتی مورد نیاز رمزنگاری در یک پکت داده یا برای چـک کـردن مقـادیر hash خواهد داشت. زیرا همه اطلاعات مرتبط شامل پکت های داده و امنیت یکپارچـه مـورد نیـاز نخواهند بود. بنابراین SKIP یک پروتکل بدون وضعیت [۲] است تا اینکه IKE اجرائـی اسـت شامل بسیاری از وضعیت ها خواهد بود. IKE در لایـه هفـتم مـدل OSI مـورد اسـتفاده قـرار میگیرد. تا کار SKIP کاملاً درلایه سوم انجام گیرد.

در مقایسه باOSKley , ISAKMP این پروتکـل بطـور کـاملاً شـفاهی پروتکـل کـم هزینـه است. در سطح IP، جائیکه پکت ها می توانند گم شوند، (یا توسط جاعلین) آشکار گردند، به خوبی درک [۳] می شوند. SKIP برای باب هم جالب خواهد بود چون می تواند پکت هـایش را

---

[۱] – exchange key

1- special header extensions

2- stateless Protocol [۲]

[۳]-Sense

برای الیس ارسال دارد و الیس کلید دیفن هیلمن یکسانی را برای باب مهیا می سازد. برای باب در این سطح به خوبی احساس می شود که بدون سرآیند روترها سرریز می‌شوند.
سادگی بیش از حد SKIP از اشکالات آن است. ارسال کاملاً سری یا مذاکره بر سر رمزنگاری پروسه ها در این پروتکل تعبیه نشده است. البته وقتی باب چیزی را ارسال می کند،که آلیس می تواند یک پروسه انتخاب نماید و اطلاعات را برای باب در سرآیند IP اش حمل نماید. اما در عوض آلیس نخواهد فهمید که آیا او از این رویه پشتیبانی خواهد کرد یا نه؟

۵- تشخیص بحران IPsec (Critical assessment of IPsec)

قرار گرفتن یکجای IKE , IPsec نمی تواند در حالت کلی بطور زمان به خود بگیرد. در سال ۱۹۹۹ نوشته ای در رابطه با حالت کنار هم بودن IPsec و IKE منتشر شد که توسط Ferguson ,Shiner انتشار یافت و این سند روی اینترنت هم قابل دسترسی است. در مقدمه این کتاب این دو ، حتی در مورد شک کردن این دو استاندارد طفره نرفتند آنها به جزئیات این دو پرداختند و در اینجا ما به مهمترین ایرادات این دو اشاره می کنیم.

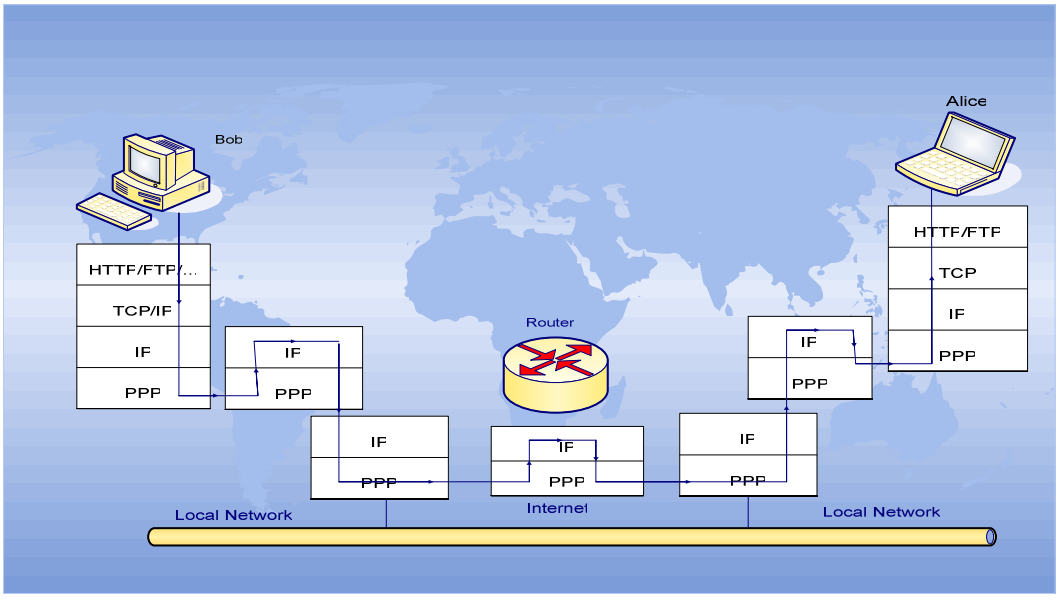
۱- مطابق با آنچه Ferguson , Shiner گفته اند، IKE , IPsec بسیار پیچیده و کامل هستند. متغیرهای زیاد، حالتهاو انواع مطمئن که هر شخصی نمی تواند راه نفوذ به آن را پیدا کند.در این دو پروتکل دیده شده است. این اصلی ترین نقدی است که دو نویسنده آنرا بیان کرده اند. این دو دیدگاهی دارند که می‌گوید "" بطور ویژه ای غیرممکن است اجرای IKE , IPsec بدون خطا شروع شود "" ،با اینکه این دو ایرادی به پیاده کنندگان این دو استاندارد ندارند ، این رویه برایشان پیاده شده است. زیرا IKE , IPsec توسط گروهی از افراد که دارای وابستگی و علایق کاملاً متفاوتی بودند و نتیجه نهایی آنها چیزی نبود مگر چیز درهم و برهمی از امری نادر و(غیر) قابل درک خاصی که از طریق مصالحه(و مسامحه) بوجود آمده بود و خیلی مغایر(آن چیز بود که انتظار) می رفت. Ferguson, Schiner این چنین اظهار نظر کردند که استانداردهای مهم نباید در یک Panel و یا بورد خیلی پیچیده پیاده شده باشند در حالیکه باید از گونهای هم بندی بوجود آیند، همانطوریکه AES چنین بوجود آمده است.

۲- اسناد موجود در مورد IKE , IPsec خیلی بد بدست می آید. علاوه بر اینکه مطابق RFCها که خیلی راحت خوانده نمی شوند، می باشد، شامل خطاها، از قلم افتاده ها، حتی

شامل تناقضات است. Ferguson, Shiner بعداً توضیح دادند که انصافاً هدف طراحی از این دو استاندارد خیلی اندک در این اسناد ذکر شده. پس شما مثل هر کسی که به آن اسناد رجوع کند درخواهید یافت که تشخیص اهمیت عملکرد آن متفاوت است.

۳- چند مغایرت در IPsec وجود دارد که خیلی عملکرد شبیه به هم دارند. IPsec دو مولفه دارد AH , ESP ؛ در جائیکه حالت تونل (Tunnel) و حالت انتقال (Transport mode) می تواند به ترتیب بکار رود. بنابراین ESP شامل عملکردهایی است که AH انجام میدهد. به راحتی، این نویسندگان اظهار نظر کردند که هر دوی AH و حالت انتقال Transport Mode نمی تواند با هم باشند برای ساده سازی و حل مشکل، این امر می باید رمزنگاری انتخابی باشد تا یک تابع درهم ساز کلید عمومی همیشه بکار برده شود.

IPsec , IKE خیلی غیر منطقی و یا غیرقابل درک هستند. بطور نمونه اگر رمزنگاری و تابع درهم سازی کلیدعمومی در IPsec بکار گرفته شده اند، تابع hash برای رمزنگاری متن بکار میرود. در یک زمان بسیاری از دیدگاههای فنی ، بحران را در این مورد نمی تواند ارائه کند. و این کاملاً مشخص است که این دو دارند برداشت مشخصی راجع به این دو استاندارد قضاوت می‌کنند، با این وجود در اسنادی که این دو نوشته اند تاکید کرده اند در حال حاضر شق دیگری برای کار در این زمینه وجود ندارد و ما باید بپذیریم که تاکنون بهترین استاندارد امنیتی در لایه سوم در میان همه استانداردهای رمزنگاری همین پروتکل یعنی IPsec میباشد.



شکل ۲: در این شکل می توانیم چگونگی استفاده از IPsec در تونل زنی VPN را ببینیم.

در این شکل پکت های IP بعد از اینکه در درون پکت های IP قرار میگیرند منتقل می شوند.

۶. شبکه های مجازی خصوصیبااستفاده IPsec

تونل زنی پروتکل لایه ۱ (Lay 2 Protocol Tunneling) **که معمولاً روی پروتکل نظیر به نظیر یا** PPP [1] **بکار می رود توسط پروتکلهای اینترنت لایه کاربرد همان** L2F , PPTP , L2TP **می باشد بکار میرود.بکارگیری تونلزنی می تواند یک شبکه محلی (**Intranet**) را به شبکه های دیگر یا یک کامپیوتر انتهایی متصل کند.همچنین این تونل زنی می تواند مرزهای** Intranet **و** Internet **را خیلی خوب حفظ کند.**

IPsec **همان نتایجی را که با بکارگیری روشهای توضیح داده شده بخش قبل بیان شده، داشته باشد. اما این روشها اساساً وقتی موثر خواهد بود که لایه های دیگر مدل** OSI **روی تونل زنی موثر باشند برهمین علت،** VPN **ترجیح می دهد تا از** IPsec **استفاده کند بدون اینکه از** L2TP , PPTP L2F **را بکار ببرد. در شکل ۲ چگونگی برقراری یک شبکه** VPN **با استفاده از** IPsec **تشریح شده است.** IPsec **در حالت تونل زنی برای پروتکل تونل بکار می رود و این روی دو شبکه اعمال می شود. مثلاً بین دو** LAN **یا بین یک کامپیوتر نهایی و یک شبکه (که به یک کامپیوتر انتهایی متصل است. اما بطور منطقی** IP (IPsec) **اینترانت و اینترنت هستند خیلی جدا از هم. تمام اطلاعات به اشتراک گذاشته شده بین دو سیستم که از قرارداد** IPsec **برای ایجاد و استفاده می کند از** SA **استفاده می کند. بطور خلاصه** IPsec **دربردارنده مفهوم کلید در یک رابطه یک‌طرفه است.**

1- Pear to Pear Protocol / Point – to – Point protocol