ایجاد ارتباط امن تحت وب به وسیله مخفی سازی اطلاعات

شاهین جوانمردی **ابراهیم بهروزیان نژاد** **امین جوادی نسب**
دانشگاه آزاد اسلامی واحد شوشتر
E-mail:s.javanmardi@yahoo.com

چکیده:
پروتکل استگانوگرافی به کاربرانی که مایل به برقراری ارتباط امن باشند این امکان را میدهد کـه پیـام هـا یـشان را در داخـل پیامهای دیگر مخفی کنند. این پیام های مخفی در زمینه های مختلفی از سرگرمی رفته تا ارتباطات امن تجاری یا حتی دفاع ملی میتوانند مورد استفاده قرار گیرند.در این مقاله پروتکل استگانوگرافی تحت لایه کاربرد را بررسی می کنیم و شرح خـواهیم داد که چگونه میتوان پیامهایمان را در داخل پروتکل های رایج TCP\IP نظیر SSH مخفی کـرد , همچنـین مفهـوم ((حـافظ معنا)) را معرفی خواهیم کرد که به ما اطمینان میدهد بسته هایی که پیام هایمان را درداخل آنها مخفی میکنیم , بعد از عمـل مخفی سازی همچنان در چهارچوب و ساختار اولیه خود باقی خواهند ماند. حفاظت معنای قوی بـه مـا تـضمین میدهـد کـه معنای پیغامی که داخل بسته وجود دارد قبل و بعد از عمل پنهان سازی کـاملا یکـسان باشـد وهـیچ گونـه تغییـری نکنـد در صورتی که حفاظت معنای ضعیف دقت کمتری در حفظ معنای پیغام بسته ها دارد.

کلمات کلیدی: استگانوگرافی ، پروتکلهای لایه کاربرد، معنا

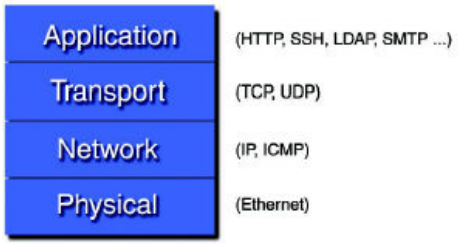
۱- مقدمه

واژه استگانوگرافی(steganography) برگرفتـه شـده از زبـان یونانی است و به معنی ((مخفی نگاری)) مـی باشـد کـه بـه عمل مخفی کـردن اطلاعـات درون اطلاعـاتی دیگـر اشـاره میکند.از لحاظ تاریخی موارد زیادی یافت میشود که از ایـده استگانوگرافی کلاسیک حتی قبل از مـیلاد مـسیح اسـتفاده کرده اند. در سالهای اخیر استگانوگرافی به صورت دیجیتـال مورد استفاده قرار میگیرد و رسانه های مورد اسـتفاده بـرای مخفـی سـازی عبارتنـد از :عکـس , مـتن , صـدا و ویـدئوی دیجیتال. تکامل تکنیک های استگانوگرافی موجب توجه بـه دو اصل ((امنیت)) و((قدرت)) در این روش ها شده است.
در گذشته امنیت اکثر سیستمهای استگانوگرافی متکـی بـر سرّ ی بودن سیـستم رمزکننـده بـود ولـی در حـال حاضـر امنیت این سیستمها به چگونگی مخفی نگهداشتن پیـام و- در صورت استفاده از کلیـد – چگـونگی مخفـی نگهداشـتن کلید بستگی دارد. پروتکل استگانوگرافی هنر مخفـی کـردن اطلاعات در "درون پیامها" و "پروتکل های کنترل شبکه که توسط برنامه های عادی استفاده می شوند" می باشد.

یک نکته قابل توجه در عمل پنهان سازی این است کـه آیـا روش ما حافظ معنا (semantics-preserving) می باشـد یـا خیر به این معنی که آیا پیـام حاصـل شـده بعـد از مخفـی کردن اطلاعات در درون آن همچنان مطابق ساختار پروتکل خود می باشد یا خیر. این خصوصیت تضمین میکند که اگـر پیام در هر نقطه ای در طول مسیر ترجمـه شـود نتیجـه ای معنی دار حاصل گردد . علاوه بـر ایـن موجـب میـشود کـه تشخیص پیامهایی که حاوی اطلاعات پنهان شده هـستند از بقیه پیامها غیر ممکن باشد.
استفاده از پروتکل استگانوگرافی به ما اجازه میدهد به جـای استفاده از کانالهای اختصاصی و مخفی از کنالهـای آشـکارو باز و عمومی برای انتقال پیامهایمان اسـتفاده کنـیم.مزایـای استفاده از پروتکل استگانوگرافی دسترسی به پهای باند بـالا برای انتقال پیامهای سرّی و استفاده و سـودبری از پروتکـل های پرکاربرد شبکه در جهت اهداف خودمان می باشد.
اکنون دو سطح حفاظت معنا را معرفی میکنیم که هـر دوی آنان اعلام میدارنـد پیامهـای حـاوی اطلاعـات پنهـان شـده منطبق بر ضوابط پروتکل خود می باشند.

سطح اول، حفاظت معنای ضعیف نام دارد که پیام حاوی اطلاعات مخفی باوجود تطبیق با ساختار پروتکل خود , دارای معنایی مفاوت نسبت به پیام اولیه(قبل از مخفی سازی اطلاعات) است.سطح دوم ، *حفاظت معنا ی قوی* نام دارد که پیام حاوی اطلاعات مخفی ,دقیقا دارای همان معنای پیام اولیه می باشد.

پروتکل های شبکه همان طور که در شکل ۱ نشان داده شده است به چندین لایه تقسیم میشوند.



شکل۱:لایه های پروتکل TCP\IP

لایه فیزیکی مسئول انتقال اطلاعات در سخت افزار شبکه می باشد (مثل کارت شبکه و ...) وبا ساختار بیت ها در سیم ها و کابل ها ارتباط دارد , بنابر این وابسته به تکنولوژی مورد استفاده درشبکه می باشد مانند اترنت و ۸۰۲,۱۱b بیسیم.لایه شبکه مسئول مسیریابی (Routing) است که همان لایه IP در پروتکل TCP\IP می باشد. لایه شبکه از دید کاربر پنهان است . لایه انتقال مسئول کنترل , تصحیح خطا, کنترل جریان و صحت انتقال می باشد. در پروتکل TCP\IP دو پروتکل پر کاربرد لایه انتقال عبارتند از: UDP و TCP .پروتکل های زیادی در لایه کاربرد TCP\IP وجود دارند مثل: SMTP, HTTP , FTP , SSH و ... که HTTP به تنهایی شامل ۷۰٪ ترافیک شبکه اینترنت میشود.

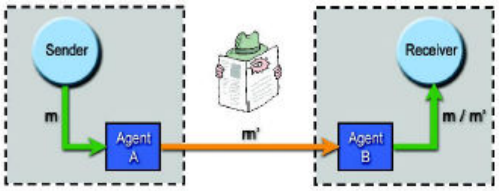
یک استگوسیستم امن(Secure stego-system) میتواند در مقابل مهاجمی که از سیستم مطلع باشد (یا حتی به آن مشکوک باشد)مقاومت کند یعنی اینکه دشمن به طور یقین نمیتواند از وجود ارتباط مطمئن شود.یک سیستم قوی میتواند در مقابل حملات فعال مقاومت کند.

ساده ترین راه مخفی کردن اطلاعات درون پیام ها , قرار دادن اطلاعات در فیلدهای استفاده نشده یا رزرو شده در سرآیند (Header) یا پی آیند (Tailer) پروتکل میباشد.این روش به راحتی توسط سیستم های ساده مهاجم یاب یا تحلیلگر ترافیک قابل کشف است.هرچند که با رمز کردن اطلاعات این عمل سخت تر به نظر میرسد اما باز هم این روش ضعیف است.

با توجه به اهداف و نکات مهم در برقراری یک ارتباط امن, درپروتکل استگانوگرافی ما توجه خود را به پروتکل های لایه شبکه و انتقال معطوف میکنیم , هرچند که بقیه لایه ها هم قابل بررسی هستند.به طور اخص دراین مقاله پروتکل SSH برای بررسی انتخاب شده است .

۲- ساختاری برای ارتباط مخفی

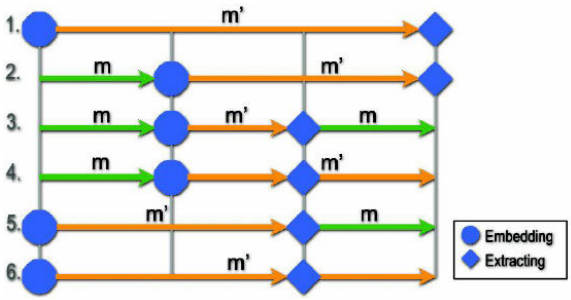
مدل ما برای پروتکل استگانوگرافی شامل دو مامور مخفی میباشد که در محیطی با حضور دشمن, میخواهند توسط ترافیک شبکه اینترنت ارتباطی مخفی برقرار کنند(شکل شماره۲).



شکل۲ : ساختاری برای ارتباط مخفی

مامور A و مامور B (همان آلیس و باب معروف!) میخواهند از مسیری که از قبل بین آنها یا دو پراسس ارتباطی به نام های Sender و Receiver وجود دارد استفاده کنند. فرض میکنیم آلیس می خواهد پیامی را به باب برساند وآنها در محیطی فعالیت میکنند که دشمن هم در آن حضور دارد .

بنابر این بر طبق اینکه آیا ماموران A وB همان Sender و Receiver هستند یا نه, دو سناریو میتوان تعریف کرد. سناریوی اول این که ماموران A وB همان Sender وReceiver هستند, ودقیقا مانند مدلهای استگانوگرافی کلاسیک تلاش میکنند که اطلاعات سرّ ی خود را در پیامهای معمولی شان مخفی کنند. در سناریوی دوم ماموران دیگر Sender وReceiver نیستند و جایی در طول یک مسیر ارتباطی قرار دارند و با دستکاری در پیامهای در حال عبور, اطلاعات سرّی خود را در آنها پنهان میکنند. با توجه به این دو سناریو یک پیام به ۶ حالت متفاوت میتواند توسط ماموران A وB تغییر داده شود(شکل شماره ۳).



شکل۳: مسیرهای پیام

در این حالات مامور A , اطلاعات سرّی را در پیام ها مخفی میکنـد و مـامور B , اطلاعـات پنهـان شـده را اسـتخراج مینماید.در شکل ۳ مامور A بـا دایـره ومـامور B بـا لـوزی نشان داده شده اند. قابل توجه است که برای مخفی کـرن و استخراج اطلاعات به کلید احتیاج است که در شکل نـشان داده نشده است.پیام اولیه با m و پیام حاوی اطلاعات مخفی با m' نمایش داده شده اند.

این ۶ حالت ممکنه عبارتند از:

۱. مـامور A بـه عنـوان Sender و مـامور B بـه عنـوان Receiver عمل میکند.پیام در طول مسیر m' است.

۲. مامور A به عنوان عنصر واسط (۱),در بین راه اطلاعـات را در پیام اولیه مخفی میکند و مامور B به عنوان Receiver عمل مینماید.پیام از Sender تـا مـامور A , m واز آنجـا تـا انتهای مسیر m' میباشد.

۳. هر دوی مـاموران A وB بـه عنـوان عنـصر واسـط عمـل مینمایند و مامور B پیام را بـه حالـت اولیـه آن برمیگردانـد .پیام از نقطه Sender تا محل مامور A , m , از مامور A تا مامور B , m' و از آنجا تا انتهای مـسیر مجـددا m میباشـد. قابل توجه است که هردو عملیات استخراج اطلاعـات پنهـان شده و بازگرداندن پیام بـه حالـت اولیـه در محـل مـامور B انجام میگیرد.

۴. هـر دو مـاموران A وB بـه عنـوان عنـصر واسـط عمـل مینمایند اما مامور B پیام را به حالت اولیه تبدیل نمیکند – پیام از محل Sender تا محل مامور A , m و از آنجا تا محل Receiver , m' میباشد.در حـالی کـه پیـام مخفـی شـده درمحل مامور B استخراج شده است.

۵. مامور A به عنوان Sender عمل میکنـد و مـامور B بـه عنوان عنصر واسط اطلاعات پنهان شده را استخراج کـرده و پیام را به حالت اولیه بر می گرداند. پیـام از نقطـه اولیـه تـا محـل مـامور B , m' و از انجـا تـا محـل Receiver , m میباشد.

۶. مامور A به عنوان Sender و مامور B بـه عنـوان عنـصر واسط عمل میکند اما مـامور B پـس از اسـتخراج اطلاعـات پیام را به حالت اولیه تبدیل نمیکند –پیام از ابتـدا تـا انتهـا m' میباشد اما مامور B در جایی قبـل از پایـان مـسیر پیـام مخفی را میگیرد.

همه سناریوهای بالا به صـورت عملـی مـورد اسـتفاده قـرار نمیگیرند اما از موارد ۱و۳ به صورت عملی استفاده میگـردد. تمامی مواردی که در آنها اطلاعـات پنهـان شـده اسـتخراج میشود اما پیام به حالت اولیه تبدیل نمیشود بسیار خطرناک هستند برای مثال در حالـت ۴ پیـامی کـه توسـط گیرنـده دریافت میشود کاملا با پیامی که فرسـتنده فرسـتاده اسـت متفاوت میباشد.

استفاده از ماموران به عنوان عناصر واسط در طـول مـسیر , مزایای فراوانی داد زیرا میتوان هر بـسته ای را کـه از مـسیر بین A و B میگذرد دستکاری کرد و از آن استفاده کـرد(بـه شرطی که برای انجام این کار از یک تابع حافظ معنا در لایه های انتقال و کاربرد استفاده شود).این ایده موجـب کـاهش شک تحلیلگر شبکه میگردد , زیرا زیرا از بسته هایی که یک مبدا و مقصد خاص دارند استفاده نمیـشود و ثانیـا از بـسته های یک پروتکل ثابت استفاده نمیشود و عـلاوه بـر امنیـت بیشتر به bit rate بالاتری نیـز دسترسـی پیـدا میکنـیم. در مدلهای ذکر شده بالا , یک موقعیت ایده آل ایـن اسـت کـه مامور A در آخـرین مـسیریاب داخـل دامنـه SENDER و مامور B بر روی اولین مسیر یاب خارج از دامنـه SENDER قرارگیرد. این روش موجب میشود که m' بـه مـدت حـداقل زمان ممکن بر روی سـیم قـرار گیـرد و احتمـال کـشف آن بسیار کاهش یابد.

۲-۱- مدل های تهاجم

نسبت به هدفیکه فرد مهاجم در نظـر دارد , حمـلات بـه دو دسته فعال و غیر فعال تقسیم میشوند . حملات غیر فعـال , ارتباط را برای کشف پیامهای حاوی اطلاعات مخفی بررسـی میکنند و در صورت توان پیام پنهان شده را پیدا کـرده و در صورت لزوم وجود پیام مخفی را برای شخص ثـالثی(Third party) اثبـات میکننـد.حمـلات فعـال تـلاش میکننـد کـه اطلاعات پنهان شده را از بین ببرند بدون اینکه تغییـر قابـل

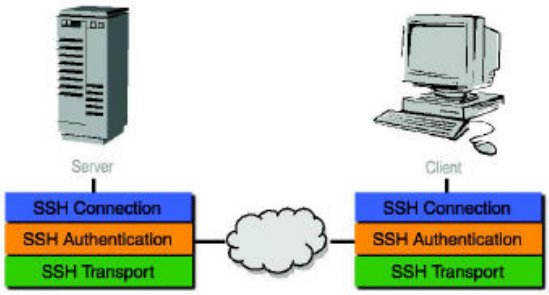
توجهی در بسته حامل آن ایجاد کنند یعنی اینکه از یک تابع حافظ معنای قوی استفاده میکنند .در بعضی موارد , حملات فعال بدون نیاز به کسب اطمینان در خصوص وجود اطلاعات پنهان شده در داخل پیام , تنها تغییر مناسبی را بر روی بیت های پیام های عبوری اعمال میکنند(مانند صفر کردن فیلد های استفاده نشده سرآیند).

سیستم های استگانوگرافی هر دو نوع حمله را مد نظر قرار میدهند .سیستم های finger printing وwatermarking بیشتر توجه خود را معطوف به حملات فعال میکنند در صورتی که stegosystem ها بیشتر با حملات غیر فعال مواجه می شوند.

۳- موضوع مورد بررسی :SSH

پروتکل SSH بر طبق تعریف IETF عبارتست از:

((*پروتکلی برای ورود امن و دیگر سرویس های امن شبکه در محیط یک شبکه نا امن*)). هدف اصلی این پروتکل فراهم کردن تشخیص هویت (authentication) , اطمینان(Confidentiality) و جامعیت(Integrity) برای سرور ها میباشد. برنامه های بسیاری اعم از تجاری و منبع باز برای SSH پیاده سازی شده است. آخرین ویرایش این پروتکل SSH۲ میباشد که به صورت گسترده در حال استفاده است و در این مقاله تحت بررسی قرار گرفته است.



شکل ۴ : معماری پروتکل SSH۲

همان گونه که در شکل ۴ نشان داده شده است پروتکل SSH از سه قسمت اصلی تشکیل شده است:

پروتکل لایه انتقال

این قسمت تشخیص هویت رمز نگاری شده را برای سرور فراهم میکند.و در صورت تقاضا امکان فشرده سازی هم دارد.معمولا بر روی یک اتصال TCP\IP بر برقرای ارتباط به پورت ۲۲ گوش می دهد.

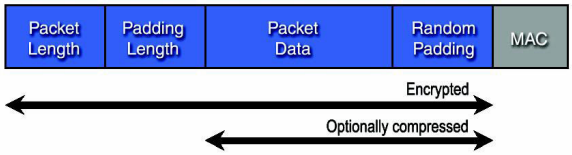
پروتکل تشخیص هویت کاربر

عمل تشخیص هویت کاربر را برای سرور انجام میدهد.بر روی لایه انتقال اجرامیشود.

پروتکل اتصال

تونل رمز شده را به چندین کانال منطقی تقسیم میکند .بر روی پروتکل تشخیص هویت کاربراجرا میشود . جلسات ورود دو طرفه , اجرای دستورات از راه دور, اتصلات TCP\IP و X۱۱ هدایت شده را نیز فراهم میسازد.

پروتکل لایه انتقال , یک پروتکل بسته باینری که همان بسته های پروتکل SSH میباشند را تولید میکند.مطابق شکل ۵ هر بسته از ۶ فیلد تشکیل شده است :



شکل۵ : بسته باینری پروتکل SSH۲

طول بسته

عددی فرم اکتد که نشانگر طول داده بسته است .بدون در نظر گرفتن MAC یا خود فیلد طول بسته

طول padding

عددی به فرم اکتد که نشانگر طول paddingمی باشد.

داده بسته

Payload یا محتوای واقعی پیام می باشد. اگر فشرده سازی در نظر گرفته شده باشد , این فیلد قابل فشرده شدن اشت.

padding تصادفی

یک مقدار تصادفی مثل مجموع طولهای طول *بسته + طول padding+ داده بسته*

کد تشخیص هویت پیام

(Message Authenticaton Code)

اگر تشخیص هویت پیام در نظر گرفته شده باشد , این فیلد شامل کد تشخیص هویت به صورت اکتد است.مقدار اولیه این فیلد قبل از عملیات تشخیص هویت , تهی میباشد.

کلاینت و سرور SSH ارتباط خود را با توافق بر سر یک نشست رمز نگاری شده آغاز میکنند , سپس هویت کلاینت توسط رمزعبور احراز میگردد. ایجاد یک نشست رمزنگاری شده شامل تبادل کلید ها و توافق بر سرآلگوریتم

ها(آلگوریتم تعویض کلید, آلگوریتم رمزنگاری, آلگوریتم تولید MAC ,آلگوریتم فشرده سازی) میباشد . عملیات تایید کلمه عبور دقیقا مشابه با سایر برنامه های ورود از راه دور می باشد با این برتری که به دلیل رمز نگاری شدن بسیار امن تر است.لو رفتن کلمه عبور تنها توسط برنامه های key-logging ممکن است.

دلیل اصلی انتخاب پروتکل SSH برای بررسی در این مقاله تصادفی بودن طول بسته های آن میباشد که فاکتور مثبتی برای مخفی کردن اطلاعات است.نکته دیگر این است که به دلیل رمز نگاری بودن پیامها در SSH بسیاری از مهاجمان به سراغ تحلیل محتوای آن نمیروند.

۳-۱- پتانسیل SSH برای مخفی کردن اطلاعات

مکان های زیادی در بسته ی SSH جهت مخفی کردن اطلاعات وجود دارد بدون اینکه خدشه ای به ساختار آن وارد شود.

تولید پیام مشابه MAC

همان طور که در شکل ۵ مشاهده شد در پروتکل SSH فیلد های زیر تعریف شده است:

uint۳۲	packet length
octet	padding length
octet[n۱]	payload; n۱ = packet length - padding length - ۱
octet[n۲]	random padding; n۲ = padding length
octet[m]	mac (message authentication code); m = mac length

که octed[m] حاوی MAC محاسبه شده است.به طور معمول MAC توسط آلگوریتم توافق شده MAC قبلی و با استفاده ازکلیدو شماره بسته و دیتای بسته (رمز نشده اما در صورت لزوم فشرده شده) محاسبه میشود. آلگوریتم های MAC تعریف شده تحت این پروتکل عبارتند از :

hmac- , hmac-md۵ , hmac-shal-۹۶ , hmac-shal md۵-۹۶ که طول MAC تولید شده بین ۱۲تا ۲۰ اکتد می باشد . بنا بر این تولید یک پیام شبیه MAC امکان فرستادن مامور B تا ۲۰ اکتد را فراهم میسازد .

تولید پیام مشابه padding تصادفی

این ایده دقیقا مشابه مورد قبل میباشد بااین تفاوت که اطلاعات را در فیلد padding تصادفی ذخیره میکند.

مخفی کردن اطلاعات تحت عنوان بخشی از مکانیزم تشخیص هویت

ساختار زیر مربوط به تقاضای تشخیص هویت میباشد که توسط پروتکل تشخیص هویت SSH ایجاد میشود:

octet	SSH_ MSG_ USERAUTH_ REQUEST
string	user name (in ISO-۱۰۶۴۶ UTF۸ encoding)
string	service name (US-ASCII)
string	method name (US-ASCII)
……	method-specific data

چهار فیلد اول قابل تغییر نیستند اما امکان مخفی کردن اطلاعات درون فیلد پنجم ممکن میباشد. ساختار پاسخ به تقاضای تشخیص هویت به این صورت است:

octet	SSH _MSG_ USERAUTH _FAILURE
string	authentications that can continue
boolean	partial success

که فیلد دوم لیستی از متد های تشخیص هویت میباشد که با کاما از هم جدا شده اند.

اگر سرور تقاضای تشخیص هویت را پذیرفت پاسخ آن به صورت زیر است:

octet	SSH _MSG_ USERAUTH _SUCCES

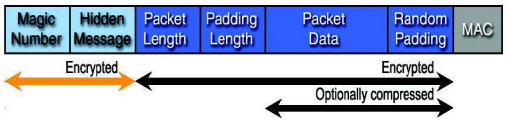
اکنون یک عملایت دست تکانی(Hand shake) بین کلاینت وسرور برای توافق بر سراستفاده متد استگانوگرافی مورد استفاده در تولید پیام مشابه MAC یا تولید پیام مشابه padding تصادفی تعریف میکنیم. برای انجام این کار از تعویض پارامترها در طول عملیات تشخیص هویت استفاده سودمی بریم. بنابراین ماموران A وB میتوانند ازفیلد method -specific data برای انجام این کار استفاده کنند. علاوه بر آن , در صورتی که در فیلد authentications that

can continue اطلاعات نادرستی برای سرور فرستاده شود, سرور ایجاد خطا نکرده وتنها این اطلاعات نادرست را دور می اندازد پس ماموران A وB از این فیلد هم میتوانند استفاده کنند.

نکته مثبت دیگری در باره استفاده از از مکانیزم تشخیص هویت برای مخفی کردن اطلاعات این است که چون فیلد های کاراکتری این بسته ها به صورت رمز شده در می آیند بنابر این تحلیل کنندگان ترافیک شبکه به آنها زیاد توجهی نمیکنند.

اضافه کردن قسمت های رمز شده اضافی به بسته

روشهای قبلی وقتی مؤثر هستند که ماموران به عنوان sender وreciever عمل کنند(تصویر ۲) . ولی این ایده که در باره آن صحبت خواهد شد مربوط به زمانی است که ماموران جایی در طول مسیر دو تولید کننده ترافیک SSH قرار داشته باشند. گرفتن بسته ها و اضافه کردن قسمتی که رمز نگاری شده به ابتدای قسمت رمزنگاری شده ی بسته ها یک راه حل میباشد همان طور که در شکل(۶) قابل مشاهده است. قسمت اضافه شده شامل در بخش است .یکی خود پیام مخفی و دیگری یک عدد ویژه که مامور B را از وجود پیام مخفی در بسته حامل آگاه میسازد.



شکل۶

این روش موجب می شود که دو مامور بتوانند هر جایی در طول مسیر قرار بگیرند و با یکدیگر ارتباط برقرار کنند ولی در انجام این کار باید دقیق بود و بسیار دقت کرد که موجب برانگیخته شدن شک تحلیلگر ترافیک نگردد. تحلیلگر ترافیک ممکن است به طویل تر بودن بسته های SSH از حد معمول شک کند و آنها را مورد بررسی قرار دهد که موجب لو رفتن کل روش میگردد. استاندارد پروتکل SSH بیان میدارد هرپیاده سازی ازاین پروتکل باید دارای بسته هایی با دیتای بسته (payload) فشرده نشده با طول مساوی یا کمتر از۳۲۷۶۸ اکتد وماکسیمم طول کل بسته(شامل طول بسته, طول padding , دیتای بسته, padding و MAC) برابربا ۳۵۰۰۰ اکتد باشد.بنابراین دامنه تغییر طول بسته ها بسیارگسترده می باشد. اکنون دو سوال مطرح میشود. اول اینکه طول قسمت اضافی چقدر باشد که تحلیلگر ترافیک به بسته ها مشکوک نشود؟ ثانیا اینکه ماموران درکجای مسیر قراربگیرند که تحلیلگر ترافیک متوجه تغییر طول بسته ها نگردد؟(یعنی اینکه دشمن قادر به در اختیار داشتن بسته اولیه و بسته حاوی اطلاعات مخفی و مقایسه آنها نباشد). بنا بر شرایط هر شبکه, به این سوالات می بایست پس از تحقیق فراوان پاسخ داد. نکته قابل توجه دیگر در این روش , انتخاب عدد ویژه میباشد.این عدد باید به شکل یک عدد ثابت با یک طول حد اقل باشد تا اولا طول بسته را افزایش ندهد و ثانیا احتمال وجود آن در محتوای بیه بسته کاهش یابد.آخرین نتکته در این روش این است که مامور B پس از استخراج اطلاعات پنهان شده در بسته , می بایست آن را به شکل اولیه تبدیل کند.

۴- نتیجه

در این مقاله پروتکلی حافظ معنا تحت لایه کاربرد با نام پروتکل استگانوگرافی را معرفی کردیم و روشهایی را برای پنهان کردن اطلاعات در پروتکل های لایه کاربرد شرح دادیم.

روش ما منافع فراوانی دارد:

به دلیل قابل اجرا بودن این روش برای محدوده وسیعی از پروتکل ها, میتوانیم پیام هارا در گستره زیادی از ترافیک شبکه در اینترنت پنهان کنیم.

استفاده از عناصر واسط موجب افزایش پهنای باند موجود و پیچیده شدن تحلیل ترافیک به دلیل انتخاب بسته از میان فرستنده وگیرندگان گسترده می شود.

حفاظت معنا به شدت موجب افزایش امنیت می گردد.

در گام های بعدی بر آن هستیم که این ایده ها را با پیاده سازی نرم افزاری به اجرا در آوریم و معایب ممکن را بر طرف سازیم و در نهایت این روش راروی بسته های HTTP پیاده کنیم.

مراجع

[۱] R. Anderson, editor. *Information Hiding: Proceedings of the First International Workshop*, Cambridge, U.K., May ۳۰-June ۰۱, ۱۹۹٦. Springer.

[۲] R. J. Anderson and F. A. Petitcolas. On the limits of steganography. *IEEE Journal of Selected Areas in Communications*, ۱٦(٤):٤٧٤–٤٨١, May ۱۹۹۸.

[۳] D. Aucsmit, editor. *Information Hiding: Proceedings of the Second International Workshop*, Portland, Oregon, U.S.A., April ۱٤-۱۷, ۱۹۹۸. Springer.

[٤] D. J. Barrett and R. Silverman. *SSH, The Secure*

Shell: The Definitive Guide. O'Reilly, ٢٠٠١.
[٥] L. Bowyer. Firewall bypass via protocol steganography. Network Penetration, ٢٠٠٢. Retrieved on January ٠٥, ٢٠٠٣ from the World Wide Web: http://www.networkpenetration.com/protocol steg.html.
[٦] C. Cachin. An information-theoretic model for steganography. In D. Aucsmith, editor, *Information Hiding: Proceedings of the Second International Workshop*, pages ٣٠٦–٣١٨, Portland, Oregon, U.S.A., April ١٤-١٧, ١٩٩٨. Springer.
[٧] S. J. Chapin and S. Ostermann. Information hiding through semantics-preserving application-layer protocol steganography. Technical report, Center for Systems Assurance, Syracuse University, October ٢٠٠٢.
[٨] T. Dunigan. Internet steganography. Technical report, Oak Ridge National Laboratory (Contract No. DEAC٠٥-٩٦OR٢٢٤٦٤), Oak Ridge, Tennessee, October ١٩٩٨. [ORNL/TM-limited distribution].
[٩] J. M. Ettinger. Steganalysis and game equilibria. In D. Aucsmith, editor, *Information Hiding: Proceedings of the Second International Workshop*, pages ٣١٩–٣٢٨, Portland, Oregon, U.S.A., April ١٤-١٧, ١٩٩٨.
[١٠] Norka B. Lucena, Douglas F. Calvert, James Pease, Steve J. Chapin
Semantics-Preserving Application-Layer Protocol Steganograph