عنوان پروژه : IPSEC
جناب استاد فیروز بخت

تهیه کننده: فاطمه اروندی
شماره دانشجوئی : ۷۸۱۱۲۱۰۴۹۳
رشته : مهندسی کامپیوتر – نرم افزار

لغات کلیدی :
IPSEC , PROTOCOL , SECURITY , NETWORK , AH , ESP ,IPCOMP , DATA AUTHENTICATION , DATA INTEGRITY , DATA CONFIDENTIALTY-TRANSPORT , TUNNLE , IKE , ANTI – REPLY , SA , SPI , PER –SOCKET , PER-PACKET

email: ma_a602002@yahoo.com

پروژه درس انتقال داده

پائیز ۱۳۸۲

امنیت شبکه Ipsec

Ipsec Net work Security

ISpec یك بسته نرم افزاری از استانداردهاست که توسط گروه کار مهندسی اینترنت (IETF) سازمانی که مسئول

مطالعه مسائل فنی مربوط به اینترنت و ارائه راه حل به IAB یعنی هیئت معماری اینترنت است- ارائه شده است.

Ipsec امنیت را برای انتقال اطلاعات حساس بر روی شبکه های حفاظت نشده مثل اینترنت تامین می کند. Ipsec

روی لایه شبکه Network عمل می کند و بسته های IP را محافظت کرده و درستی آنها را تصدیق می کند.

Ipesc سرویس های امنیتی شبکه زیر را فراهم می آورد. این سرویس ها اختیاری هستند و عموما سیاست امنیتی

محلی ، استفاده از یك یا چند نمونه از این سرویسها را ایجاب می کند.

- Data Confidentiality (میزان محرمانه بودن از اطلاعات) : فرستنده Ipsec می تواند بسته ها را قبل از انتقال آنها بر روی شبکه رمزگذاری کند.
- Data Integrity (یکپارچگی اطلاعات) : گیرنده Ipsec می تواند صحت بسته های ارسالی از سوی فرستنده Ipsec را تایید کند تا مطمئن شود که اطلاعات در طول مسیر تغییرنکرده است.
- Data Orgin Authentication (تصدیق مبداء اطلاعات) : گیرنده Ipsec می تواند مبداء بسته های فرستاده شده را تصدیق کند، تا مطمئن شود که اطلاعات از کدام فرستنده، فرستاده شده است. این سرویس وابسته به سرویس Data Integrity است.
- Anty_Reply : گیرنده می تواند بسته های تکراری را تشخیص دهد و پس بفرستد. اطلاعات ، با وجود Ipsec می تواند روی یك شبکه عمومی فرستاده شوند بدون اینکه نگران باشیم که دیده می شوند یا تغییر می کنند یا درست عمل نکنند. این مسئله با برنامه های کاربردی مثل VPN ها، اینترنت ها، اکسترانت ها و دستیابی های کاربران راه دور را تواناتر می سازد. سرویسهای Ipsec شبیه سزویسهایی هستند. که توسط تکنولوژی رمزگذاری سیسکو در version 11.2 معرفی شده اند.اگرچه Ipsec یك راه حل امنیتی

نیرومندترو استانداردتر است . همچنین Ipsec سرویسهای تصدیق دیتا وغیرتکراری بودن را
علاوه بر میزان محرمیت داده پوشش میدهد در حالیکه CET تنها سرویس میزان محرمیت دیتا را پوشش میدهد .

مزایا : Ipsec و CET در مواردی مثل هم هستند :

۱- هر در تکنولوژی از بسته های حساس که در طول شبکه های محافظت نشده منتقل می شوند نگهداری و پشتیبانی می کنند .
۲- مثل CET سرویسهای امنیتی Ipsec در لایه شبکه عمل می کنند . بنابراین شما مجبور نیستید ایستگاههای کاری را تك تك بطور دستی چك کنید .

این مزایا تا حدود زیادی هزینه های اضافی را بر می گرداند . بجای تامین سرویسهای امنیتی و صف
کردن آنها و کنترل امنیت روی هر برنامه کاربردی بطور مجزا روی هر کامپیوتر اصلی شما می توانید براحتی زیرساخت و پیکربندی شبکه را برای تامین این سرویسهای امنیتی مورد نیاز تغییر دهید .

تفاوت Ipsec و CET:

۱ – چون Ipsec استاندارد است دستگاههای سیسکو می توانند بجای دستگاههای شبکه ای که برای تامین سرویسهای امنیتی Ipsec آماده شده اند عمل کنند . این دستگاهها می توانند شامل دستگاههای سیسکو و غیر سیسکو مثل کامپیوترهای شخصی (PC ها) و سرورها و سایر سیستمهای کامپیوتری باشند .
سیسکو و شرکایش که شرکت مایکروسافت نیز جزئی از آنهاست در حال برنامه ریزی هستند تا Ipsec را در
رنج وسیعی از Platform ها بهمراه نرم افزار CISCO IOS ، CISCO PIX FIREWALL ، ویندوز ۹۵
و NT عبور دهند . سیسکو به سرعت در حال استاندارد شدن است .
۲- یك کاربر می تواند با دفترش یك ارتباط مطمئن برقرار کند . برای مثال کاربر می تواند یك تانل Ipsec بوسیله یك فایروال جمعی برقرار کند و سرویسهای تصدیق کننده را تقاضا کند بدون اینکه به یك شبکه گسترده دسترسی یابد . تمام ترافیك اطلاعات بین کاربر و فایروال تائید خواهد شد . کاربر می تواند یك تانل Ipsec دیگر برقرار کند و سرویسهای خصوصی سازی داده را تقاضا کند . Ipsec همچنین از پروتکل IKE

(Internet Key Exchange) و گواهیهای دیجیتالی حمایت می کند . IKE سرویسهای مبادله و سرویسهای اشتقاق کلیدها را برای Ipsec تامین می کند . گواهیهای دیجیتالی به ابزار آلات اجازه می دهند تا به طور خودکار یکدیگر را تائید کنند بدون اینکه به طور دستی نیاز به تغییر کلیدها توسط تکنولوژی رمزگذاری سیسکو باشد .
این پشتیبانی ها اجازه میدند که Ipsec بهتر از CET ارزیابی شود و در بیشتر موارد ، برای کاربرد در شبکه های متوسط، بزرگ و در حال رشد ترجیح داده شود . جائی که ارتباطات مطمئن باید بین دستگاههای زیادی برقرار شود .

مقایسه Ipsec با تکنولوژی رمزگذاری سیسکو :

شما CET یا Ipsec ، کدام را پیاده سازی می کنید ؟ البته پاسخ شما به نیاز شما بستگی دارد . اگر به یك ارتباط رمزگذاری شده بین روترهای سیسکو نیاز دارید می توانید تکنولوژی رمزگذاری سیسکو را اجرا کنید که یك راه حل خیلی سریع و عمل کننده است . و اگر به یك راه حل بر پایه استاندارد و ارتباط چند جانبه با سرویسگیرهای راه دور نیاز دازید باید Ipsec را پیاده سازی کنبد . همچنین قادر خواهید بود که هر دو تکنولوژی را به طور همزمان در شبکه تان حتی بصورت همزمان بر روی همان دستگاهها پیکر بندی کنید . یك دستگاه سیسکو می تواند بصورت همزمان رمزگذاری سیسکو و Ipsec را داشته باشد .

استاندارد پشتیبانی شده بوسیله Ipsec :

DES : استاندارد رمزگذاری اطلاعات که برای رمزدار کردن بسته های اطلاعات بکار میرود. این Cisco Ios
استاندارد را با ۵۶ بیت DES_CBC با بردار مقداردهی صریح پیاده سازی میکند. CBC یا زنجیره سیاه رمزگذاری به یك بردار مقداردهی نیاز دارد . این بردار بطور صریح در بسته Ipsec داده می شود.برای سازگاری برگشت ، الگوریتم RFC 1829 از ESP DES_CBC را نیز پیاده سازی می کند.

MD5 : HMAC یك متغیر هش کلیدگذاری شده است و برای تصدیق صحت داده بکار میرود .

SHA : یك الگوریتم هش است . HMAC کلیدگذاری شده است و برای تصدیق صحت داده بکار میرود .

Ipsec در برگیرنده گروهی از پروتوکلهای زیر است :

۱- Authentication Header (AH) :درستی بسته ها را با اضافه کردن یك عدد check sum به بسته ها
ضمانت و تائید می کند . اگر شما بسته را با AH دریافت کنید و عملیات check sum موفقیت آمیز بود می توانید مطمئن باشید که شماو دستگاه های هم سطح peers (روترهای CET و...) یك کلیدرمز مشترك دارید و هیچ کس دیگری آن کلید را ندارد.و از دو مسئله مطمئن خواهید:

- مبدا بسته ، همان مبدا مورد نظر بوده است .

- بسته در طول انتقال تغییر نیافته است .

بر عکس پروتوکلهای دیگر ، AH کل بسته را از IP Header تا انتهای بسته ، پوشش میدهد .

۲- Encapculating Security Payload (ESP) : صحت و درستی بسته را با رمزگذاری بسته بوسیله الگوریتمهای رمزگذاری ، ضمانت و تائید می کند . هنگامی که شما بسته را ESP دریافت می کنید و بطور موفقیت آمیز آن را رمزگشایی می کنید می توانید مطمئن باشید که بسته در راه تغییر نکرده و دستگاههای مورد نظر و شما یك رمز مشترك دارید و کس دیگری آن را نمی داند .
۳- IP Payload Compression(IPCOMP) : سرویس رمزگذاری روی بسته را ESP تامین می کند در حالیکه تکنیك رمزگذاری به برخورد با فشرده سازی روی هم تمبیل دارد . (سازگار نیستند .) مثل فشرده سازی
IPCOMP.PPP قبل از رمزگذاری ESP راهی برای فشرده سازی ارائه می دهد . البته شما می توانید IPCOMP را در صورت تمایل بکار ببرید .
۴- Internet Key Exchange (IKE): همانطور که در بالا اشاره شد AH و ESP و IPCOMP در کد اصلی پیاده سازی می شوند . IKE به صورت یك پروسس Daemon در محیط کاربری پیاده سازی می شوند .
بخش اصلی و محیط کاربری با به کار بردن جدول مدیریت کلیدها ، کار خود را انجام میدهند .
IKE کاملاً اختیاری است . شما می توانید به صورت دستی کلیدهای رمز را برای ESP/AH پیکربندی کنید . البته توجه داشته باشید که برای ابد ، شما نمی توانید آن کلید رمز زا بکار ببرید . در این صورت بار ترافیکی شما ، خیلی
زیاد می شود . بطوریکه کلیدها متراکم می شوند .
توجه داشته باشید که امنیت IPSEC به محرمانه بودن کلیدهای رمز بستگی دارد . اگر آنها متراکم شده باشند Ipsec مدت زیادی امن نخواهد بود . نسبت سطح دسترسی ها ، برای پیکربندی فایلها ، فایلهای پایگاه داده کلیدهاو
هر چیز دیگری که منجر به نشت اطلاعات می شود مراقب باشید .

Userland programs IKE daemon

AF-INET{6}socket PF-Key Socket

Kernel / user boundary

Transport layer , tcp / udp Key Management table

Key information

IP input / out logic

Network drivers (Ethernet)←----------→ AH / ESP / IPCOMP logic

مود انتقال و تانل:

Transport mode & Tunnle mode

AH ، ESP و IPCOMP دو مود عملیاتی دارند : مود انتقال و مود تانل
مود انتقال يك ارتباط عادی را بین دستگاههای هم سطح peers رمزگذاری می کند . مود تانل بسته ها را به هدر
Ipv4/v6 تبدیل و بسته بندی می کند. مود تانل برای استفاده در gateway های vpn طراحی شده است .

[[transport mode]]

my host==========peer,s host
transport mode

packet :[ip:me->peer]ESP Payload

←----------→encrypted
[[tunnel mode]] tunnel mode

my host -------my VPN gateway========== peer,s vpn gateway-------peers host

packets on (a) : [ip:me -> peer] payload

packets on (b) :[ip :mygw ->peergw]esp [ip:me -> peer] payload←→ encrypted

packets on (c) :[ip:me -> peer]payload

سیاست مدیریت Ipsec :

فکر کنید که کرنل می داند چگونه بسته ها را از نظر امنیت تامین کند . اما نمی داند که کدام بسته به امنیت نیاز دارد . ما باید به او بگوئیم که کدام بسته نیاز دارد تا امنیتش تامین شود . سیاست پیکربندی Ipsec این اجازه را به ما می دهد که چنین عملی را انجام دهیم . سیاست Ipsec بر این است که می تواند به دو صورت per-packet و به صورت per-socket پیکربندی شود :

الف : per – packet : کاملاً مثل فیلترهایی روی بسته ها در بخش اصلی پیکر بندی کی شود . شما می توانید چنین معین کنید : رمزگذاری کن بسته های خارج شده را اگر به ۲۴. ۱ . ۱. ۱۰ فرستاده می شوند .
این ، وقتی شما یك روتر Ipsec را اجرا می کنید خوب عمل می کند .

ب : per – socket : بوسیله set socket برای یك سوکت مطمئن پیکربندی می شود . شما می توانید معین کنید که کدام بسته های خارج شده از این سوکت را رمز گذاری کن . وقتی شما برنامه خدمتگزار هوشمند Ipsec را اجرا می کنبد per – socket بخوبی عمل میکند .
Ipsec تصمیم می گیرد که کدام یك از پروتوکلهای Ipsec (AH ، ESP یا IPCOMP) بر روی یك بسته اعمال می شوند .همچنین شما می توانید یك یا چند پروتکل را ، بیش از یکبار روی یك بسته اعمال کنید .

پیکر بندی هسته Ipsec :

۱- در فایل پیکربندی کرنل بخش زیر را فعال کنید و یك هسته جدید بسازید :

```
Options  Ipsec
Options Ipsec-ESP
```

۲- مثل همیشه یك کرنل جدید بسازید .
۳- کرنل جدید را جایگزین کنید و سیستم را دوباره راه اندازی کنید .

محیط کاری کاربر ، پشتیبانی Ipsec را بطور پیش فرض دارد و ایجاد دوباره محیط کاری کاربر الزامی نیست .

مثال پیکربندی :رمزگذاری HOST _TO_HOST
اگر شما می خواهید رمزگذاری (مود انتقال) host-to-host را با پیکربندی کلیدهای رمز بصورت دستی اجرا کنید پیکربندی زیر کافیست . set key را برای پیکربندی کلیدهای دستی بکار می بریم .

```
# !/bin/sh

#

#packet will look like this : Ipv4 ESP Payload

# the node is on 10.1.1.1, peer is on 20.1.1.1

setkey –c << EOF

add 10.1.1.1 20.1.1.1 esp 9876-Edes-cbc “hogehogehogehogehogehoge”;

add 20.1.1.1 10.1.1.1 esp 1000 –e 3des-cbc oxdeadbeafdeadbeafdeadbeaf

spdadd 10.1.1.1 20.1.1.1 any –p out ipsec esp/transport//use;
```

درخط اول کلیدهای رمز را برای استفاده ESP می سازیم . اعداد دهدهی به ۴ کلمه به نام SPI (Security Parameter Index) تفکیك می شوند . مقادیر به بسته ESP متصل می شوند . به طرف دیگر یعنی گیرنده اجازه داده می شود که کلید رمز بسته را چك کند . اعداد باید از یك تا نود باشند .

-از ۱۰,۱,۱,۱ تا ۲۰,۱,۱,۱ الگوریتم 3DES-CBC را بکار می بریم . با کلید رمز hogehogehogehoge .بار
ترافیك بوسیله SPI 9876 شناسایی می شود .

- و از ۲۰,۱,۱,۱ تا ۱۰,۱,۱,۱ الگوریتم 3DES-CBC را با کلید رمز oxdeadbeafdeadbeafdeadbeef بکار می بریم .

خط آهر حالت per- packet را برای نود پیاده سازی می کند . با این پیکر یندی نود ۱۰,۱,۱,۱ بسته ها را به دستگاه ۲۰,۱,۱,۱ می فرستد و هر وقت که در کرنل کلید رمز پیکربندی شود رمزگذاری می شود .
این پیکر بندی مانع از رمز گشائی بسته ها ئی که از ۲۰,۱,۱,۱ به ۱۰,۱,۱,۱ رسیده اند نمی شوند .اگر بخواهید که بسته های رمز گذاری نشده را برگردانید خط زیر را کی توانید اضافه کنید :

Spdadd 20.1.1.1 10.1.1.1 any –p in ipsec esp /transport//require ;

در طرف دیگر یعنی ۲۰,۱,۱,۱ پیکر بندی مثل همین است . توجه داشته باشید که آدرسها باید در خط "spdadd "
آورده شوند نه در خط "add" .

#!/bin/sh

#

packet will look like this : IPV4 ESP Payload

the node is on 20.1.1.1 , peer is on 10.1.1.1 setkey –c << EOF

add 10.1.1.1 20.1.1.1 esp 9876 –E 3des-cbc"hogehogehogehogehoge";

add 20.1.1.1 10.1.1.1 esp 10000 –E 3des-cbc
oxdeadbeafdeadbeafdeadbeafdeadbeaf

spdadd 20.1.1.1 10.1.1.1 any –p out ipsec esp/transport//use;

EOF

مثال بالا، کلیدهای رمزی که توسط اشخاص قابل خواندن هستند بکار برده شدند . اگرچه بکار بردن آنهاد لسرد
کننده است . چون آنها تراکم پذیر تر از کلیدهای باینری هستند . بنابراین بکار بردن کلیدهای باینری برای این عملیات بهتر است .

الگوریتم دیگر rijndeal-cbc است که کلیدها می توانند ۱۲۸ ، ۱۹۲ ، ۱۵۶ بیت باشند . در ادامه یك الگوریتم با ۱۲۸ بیت کلید رمز را می بینید .

#!/bin/sh\

#

#packet will look like this :IPV4 ESP Payload

#the node is on 10.1.1.1 ,peer is on 20.1.1.1

```
#rijndeal – cbc with 128 bit key

setkey –c<< eof

add 10.1.1.1   20.1.1.1 esp 9876 –E rijndeal-cbc “hogehogehogehogehoge”

add 20.1.1.1   10.1.1.1 esp 10000 –E rijndeal-cbc
oxdeadbeafdeadbeafdeadbeafdeadbeaf

spdadd 10.1.1.1  20.1.1.1  any –p out ipsec esp / transport//use;

EOF
```

لیست لغات :

۱-anti- reply یك سرویس امنیتی که گیرنده می تواند بسته های قدیمی یا تکراری را پس بفرستد . بجای اینکه خودش را از برخورد بسته های تکراری محافظت کند .
سرویس Ipsec این سرویس اختیاری را تامین می کند . البته با استفاده از یك ترکیب کننده اعداد ترتیبی و با بکار بردن سرویس تصدیق صحت اطلاعات . Cisci IOS Ipsec این سرویس را همزمان که سرویس تصدیق آن را تامین می کند پیاده سازی می کند بجز موارد زیر :

الف : RFC 1828 برای این سرویس پشتیبانی نمی شود .

ب: این سرویس برای ارتباط امنیتی برقرار شده دستی ، قابل دسترس نیست .

۲- تصدیق صحت اطلاعات
Data Authentication
جامعیت داده (Data Intergrity) که چك می کند که اطلاعات تغییر نکرده باشد .
چك می کمد که دیتا واقعاً از کدام فرستنده ؤ فرستاده شده است .
۳- Data Confidentiality : یك سرویس امنیتی برای جائی که اطلاعات محافظت شده ، قابل دیدن نباشد .
۴- Data Flow : تجمع داده ای که بوسیله ترکیبی از آدرس یا مالك مبدا ، آدرس یا مالك مقصد ، IP پروتکل بعدی و پورت مبدا و مقصد مشخص می شود . جائی که فیلد پروتکل و پورت می توانند هر مقداری داشته باشند .
۵- Peer : در این مقاله ، ثثق به جفت دستگاههای هم سطحی گفته می شود که در Ipsec شرکت می کنند .
۶- SA : Security Association شرح چگونگی استفاده یك یا چند موجودیت از سرویسهای امنیتی در متن یك

پروتکل امنیتی خاص مثل AH یا ESP است .
SA هم با IKE و هم بصورت دستی پیکربندی می شود . SA ها بدون جهت هستند و برای هر پروتکل امنیتی
یگانه اند . پس وقتی SA ها برای Ipsec تعیین و برقرار می شوند . (همزمان)
اگر SA با IKE پیاده سازی شود که این مربوط به زمانی است که SA مورد نیاز است و بعد از یك دوره زمانی یا حجمی از ترافیك منقضی می شوند . اگر SA دستی پیاده سازی شود به محض اینکه پیکربندی مورد
لزوم کامل شود ایجاد شده ولی هیچگاه منقضی نمی شوند .
۷- SPI عددی است که شامل یك IP و یك پروتکل امنیتی است که به تنهایی یك ارتباط امنیتی خاص را مشخص می کند. وقتی IKE برای برقراری ارتباط امن بکار می رود، SPI برای هر ارتباط امن یك عدد مشتق شدهٔ تصادفی و ساختگی است. بدون IKE، SPI می تواند به طور دستی هم تنظیم شود.
۸- Transform : لیست انتقال یك پروتکل امنیتی ESP یا AH با الگوریتم متناظرش. برای مثال یك لیست انتقال یك پروتکل AH با الگورتیم HMAC_MD5 است. لیست انتقال دیگر، پروتکل ESP با الکوریتم رمزگذاری ۵۶ بیتی DES است و الگوریتم تصحیح HMAC_SHA می باشد.
۹- تانل : در این متن یك مسیر ارتباطی مطمئن بین دو جفت دستگاه هم سطح مثل دو روتر است و ربطی به کاربرد IPSEC در مود تانل ندارد.

مروری بر عملکرد IPSEC

به زبان ساده، IPSEC از تانلهای بین دو دستگاه هم سطح مانند دو روتر نگه داری می کند. شما مشخص می کنید که کدام بسته ها نیاز به توجه و مراقبت دارند و باید در تانلهای مطمئن و امن فرستاده شوند و نیز شما مشخص می کنید که کدام پارامترها باید برای نگهداری از این بسته های حساس بکار روند. وقتی Peer های IPSEC این بسته های حساس را می بینند تانل مطمئن و مناسب را تنظیم می کنند و بسته را درون آن به سوی طرف دیگر می فرستند. تانلها مجموعه ای از ارتباطات امن هستند که بین جفت دستگاههای هم سطح ISPEC برقرار شده اند. این تانلها معلوم می کنند که کدام پروتکلها و الگورتیمها باید برای این بسته های حساس تقاضا شوند و نیز موضوع کلیدها را برای استفاده peers تعیین می کنند. تانلها بی جهت هستند و بر ای هر پروتکل امنیتی مثل AH یا ESP برقرار شده اند. شما با Ipsec مشخص می کنید که کدام ترافیك باید بین این دستگاهها نگهداری شوند که البته این کار را بوسیله پیکربندی لیستهای دستیابی Access List و خواستن این لیستها برای برقراری ارتباط بوسیله مجموعه نقشه های رمزگذاری شده انجام می دهید.