مفاهیم امنیت

سپهر مقیسه

دکتر شهریاری

9831103

پاییز 1401

1.

استفاده از روش two step authentication که ورود دومرحله است و در ملحه دوم کاربر حالا یا رمز عبور ارسالی به تلفن همراه یا ایمیل خود را وارد میکند و یا کد امنیتی ایجاد شده در برنامه تایید کد را وارد میکند.

روش دوم به تایید ip ورودی اشاره دارد که شرکت هایی مانند Spotify و گوگل از این کار استفاده میکنند به این صورت که اگر از ip کشوری متفاوت و مکانی متفاوت وارد شوید حتما با گزینه تایید هویت در ایمیل مواجه میشود

روش سوم: استفاده از کربروس - احراز هویت بر اساس رمز نگاری کلید مخفی )متقارن(

2.

امنیت- اطمینان-شفافیت-مقیاس پذیری

3.

در نسخه 5 می توان از هر الگوریتم متقارن استفاده کرد.

در نسخه 5 می توان از هر آدرس شبكه)مثلا OSI یا IP ( استفاده کرد

در نسخه 5 محدودیت زمان اعتبار بلیت ها وجود ندارد

4.

تا دو طرف ارتباط بتوانند ارتباط خود را مخفی و محرمانه نگه دارند.

هرزمان که کاربر جدیدی درخواستی به تایید کننده هویت میزند .سرور احراز هویت باید یک توکن جدید ایجاد کند و آن را میان هر دو گروه توزیع کند که به آن کلید جلسه گفته میشود.

به زبانی دیگر هنگامی که دو سیستم پایانی )میزبان، پایانهها، و غیره( تمایل به برقراری ارتباط

داشته باشند، آنها یک ارتباط منطقی برقرار میکنند )به عنوان مثال، مدار مجازی(.

5.

در تبادل کلید اکثر سیستم ها به این صورت عمل میکنند که یک سیستم کلید را ایجاد کرده و به سیستم دیگر ارسال میکند و به اصطلاحی سیستم دوم در تولید کلید دستی نداشته است و یا حتی تبادل کلید عمومی نیز تبادل کلید نامیده میشود. ولی در توافق کلید هردو بر سر کلید عمومی و خصوصی به توافق رسیده و کلیدی اشتراکی ایجاد میکنند.

6.

.به طور مثال با ورود به یک سایت یک جلسه ایجاد کردیم و حال هر بار با هر وسیله ای به ان "متصل" بشویم به جلسه دست پیدا میکنیم یعنی به یک جلسه میتوان از کانکشن های متعدد استفاده کنیم. مثال سایت کورسز که یک بار جلسه ایجاد میکنیم و با هر بار بستن و باز کردن سایت بدون نیاز به ورود به آن وارد میشویم به صورت خودکار.

7.

* Version-نسخه
* Serial number-سریال گواهی
* Signature algorithm- روش الگوریتم رمزی که صادر کننده توسط ان این گواهی را امضا میکند
* Issuer-صادر کننده
* Valid from-زمان شروع اعتبار گواهی
* Valid to- تا زمانی که گواهی اعتبار دارد
* Subject-اطلاعات کسی که این گواهی برایش صادر شده
* Public key-فیلد حاوی گواهی عمومی
* Extension-در این فیلد میتوان به تعداد دلخواه فیلد ایجاد کرد که هرکدام شناسه مشخص دارند

8.

در tls میتواند در پیام handshake باشد اما جداسازی ان باعث اسانی فهمیدن رفتار پروتکل میشود

جواب طولانی تر به این گونه است که پروتوکل ssl از پیام هایی استفاده میشود که برای هر رکورد منحصر به فرد کدگزاری شده اند.اما چند پیام یک نوع مانند handshake ها میتواند در یک رکورد جای بگیرد .از انجایی که change cipher spec روش کدگزاری را تغییر میدهد، باید یک رکورد جدید سریعا ایجاد شود تا تغییرات لحاظ شوند برای همین وقتی یک پروتکل برای این کار ایجاد میکنیم بعد از نوع جدید رکورد استفاده کنیم، ssl چاره ای جز تغییر روش کدگزاری ندارد و از رکورد بعدی با آن روش کدگزاری را انجام میدهد.

9.

الف)

Ssl تمامی ارتباطات را کدگزاری کرده. و این گونه فردی که ip spoofing را انجام میدهد نیاز به داشتن کلید کدگزاری کردن ssl دارد. حتی اگر این کلید را بدست اورد هر پکت اطلاعاتی در پروتکل ssl یک هشتگ بسیار سخت برای برگشت دارد که وظیفه دارد تا پکت را بدون دست خوردن ارسال کند.اگر این هشتگ ها دست خورده شوند سریعا به دو طرف خبرداده شده و ارتباط نا امن را قطع میکنند

ب)

به این صورت که کلاینت و سرور بر سر یک کلید جلسه توافق کرده . این کلید فرستاده نمیشود بلکه اطلاعات با این کلید کدگزاری شده و ارسال میشوند و به دلیل روشی که پروتوکل ssl کلید را به اشتراک میگذارد نمیتوان رمز را پیدا کرد.

10.

Session-identifier : یک دنباله بایتی که سرور انتخاب میکند تا جلسات فعال را پیدا کند.

Peer certificate: یک گواهی x.509 . این فیلد میتواند خالی باشد.

Compression method:روشی که داده را قبل از کدکردن فشرده میکند

Cipher spec: روش کدگزاری را مشخص میکند.یک کدگزاری روش هش نیز برای محاسبه مک استفاده میشود همچنین مقادیر کریپتوکرافیگی مانند اندازه هش را مشخص میکند.

Master secret: سکرت 49 بایتی که میان کلاینت و سرور به اشتراک گذاشته میشود

Is resumable: پرچمی که برای مشخص سازی این که ایا میتوان از نشست برای ایجاد اتصال های جدید استفاده کرد و یا خیر

11.

وقتی که میزبان A تمایل به برقرای ارتباط با میزبان B داشته باشد؛ یک بسته درخواست اتصال به KDC ارسال میکند. ارتباط بین A و KDC با استفاده از یک شاه کلید صورت میگیرد که تنها توسط A و KDC به اشتراک گذاشته شده است. اگر KDC درخواست اتصال را تأیید نماید، یک کلید جلسه منحصر بفرد را ایجاد کرده و کلید جلسه را با استفاده از کلید دائمی که با A به اشتراک گذاشته شده رمزگذاری نموده و کلید جلسه رمزگذاری شده را برای B ارسال می نماید. اکنون A و B میتوانند یک اتصال منطقی برای مبادله پیام و اطلاعات برقرار کنند. همه رمزگذاریها از کلید جلسه به طور موقت استفاده میکنند.

روش های توزیع کلید سری:

مبادله کلید با استفاده از رمز متقارن

مبادله کلید با استفاده از رمز کلید عمومی

مبادله پیام و کلید

پخش پیام و کلید

مبادله کلید دیفی-هلمن

پروتکل ایستگاه به ایستگاه

12.

یک پروتکل است که توسط RFC 2408 برای ایجاد Security association (**SA**) و کلیدهای رمزنگاری در یک محیط اینترنتی تعریف شده است. در دو فاز فعالیت خود را انجام میدهد. در فاز اول که ISAKMP SA نامیده می شود ابتدا توافقات امنیتی بین دو نقطه صورت می پذیرد. در فاز اول علاوه بر توافقات امنیتی، Key Management برای بحث رمزنگاری (تبادل کلید) و Authentication نیز انجام می شود.  در فاز دوم که IPSEC SA گفته می شود پروتکل Tunneling که می خواهیم استفاده نماییم از بین AH و ESP انتخاب می شود. در این فاز به صورت Optional می توانید Key Management را داشته باشید.

IKE یک پروتکل را با استفاده از بخشی از Oakley و بخشی از SKEME همراه با ISAKMP برای به دست آوردن مواد کلید دار معتبر برای استفاده با ISAKMP و سایر انجمن های امنیتی مانند AH و ESP برای IETF IPsec DOI توصیف می کند.

13.

برای مدیریت خودکار کلید ها،توزیع و تنظیمات آن ها از این پروتکل استفاده میشود. و به اصطلاح پروتکلی است که دو سرور بر آن برای ایجاد ipsec توافق میکنند.

14.

سایت اول:



چ



سایت دوم:





سایت سوم:





