امنیت شبکه

جلسه چهارم: توزیع کلید و احراز هویت کاربر

تهیه و تنظیم: دکتر آرش حبیبی لشکری

منبع: کتاب اصول و مبانی امنیت شبکه (استانداردها و کاربردها)

اولین نسخه: دی 1393
بروزرسانی: دی 1393

فهرست:

- توزیع کلید با استفاده از رمزنگاری متقارن
- Kerberos 4 , 5
- گفتگوی ساده برای احراز هویت
- توزیع کلید با استفاده از رمزنگاری نامتقارن
  - گواهینامه‌های کلید- عمومی
  - پخش کلیدهای محرمانه با کلید- عمومی
- گواهینامه‌های X.509

توزیع کلید با استفاده از رمزنگاری متقارن

توزیع کلید متقارن با استفاده از رمزنگاری متقارن

برای اینکه رمزنگاری متقارن انجام شود باید دو طرف مبادله یک کلید مشابه را به اشتراک بگذارند و این کلید باید از دسترسی دیگران نیز محافظت شود. توزیع کلید می‌تواند از راههای متعددی بدست آید. برای دو طرف A و B گزینه‌های زیر وجود دارد:

1. یک کلید می‌تواند توسط A انتخاب شود و به روشهای فیزیکی به B ارسال کند
2. شخص سوم می‌تواند کلید را انتخاب کند و به روشهای فیزیکی به B و A ارسال نماید
3. اگر A و B پیشتر و به تازگی از یک کلید استفاده می‌کردند، هر طرف می‌تواند کلید جدید را به طرف مقابل ارسال نماید در حالیکه از کلید قدیمی برای رمزگذاری استفاده می‌نماید.
4. اگر هر کدام از A و B یک اتصال رمز شده به شخص سوم C داشته باشند، آنگاه Cمی‌تواند کلید را با استفاده از لینک رمزگذاری شده به A و B ارسال نماید.

توزیع کلید متقارن با استفاده از رمزنگاری متقارن (ادامه)

که در اینجا برای تهیه کلید رمزنگاری تنها گزینه 4 ترجیح داده می‌شود. برای گزینه 4 دو نوع کلید در اصل استفاده می‌شود:

کلید جلسه: 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).

کلید دائم :کلید دائمی کلیدی است که بین اشخاص به منظور توزیع کلیدهای جلسه استفاده می‌شود.

با اینحال عنصر ضروری گزینه 4 یک مرکز توزیع کلید یاKDC است که یک کلید جلسه یکبار - مصرف برای آن ارتباط فراهم می‌نماید. عملیات مرکز توزیع کلید به شرح زیر می‌باشد:

1. 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.

2. اگرKDC 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 می‌نماید.

3. 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.

Kerberos

در واقع Kerberos برای توزیع کلید و خدمات احراز هویت کاربر در MIT توسعه یافته شده است.
مشکلی که Kerberos درباره آن سخن گفته این است که:

یک محیط باز توزیع شده را فرض کنید که در آن کاربران در ایستگاه های کاری

مایل به دسترسی به خدمات بر روی سرویس‌های توزیع شده در سراسر شبکه هستند.

حال می‌خواهیم سرویس‌دهنده‌ها قادر به محدودکردن دسترسی به کاربران مجاز و

تصدیق درخواست خدمات آنها باشند.

در این محیط، یک ایستگاه کاری نمی‌تواند برای شناسایی کاربرانش در درستی به خدمات شبکه اعتماد داشته باشد. چرا که به طور خاص سه تهدید زیر وجود خواهد داشت:

1. یک کاربر ممکن است به یک ایستگاه کاری خاص دسترسی داشته باشد و تظاهر نماید که کاربر دیگری از آن ایستگاه کاری می‌باشد.

2. یک کاربر ممکن است آدرس شبکه ایستگاه‌های کاری را تغییر دهد به طوری که بنظر می‌رسد درخواستها از ایستگاه‌های کاری که هویتشان جعل شده است، ارسال گردیده‌اند.

3. یک کاربر ممکن است تبادل اطلاعات را استراق سمع نماید و از یک حمله بازپخش برای به دست آوردن ورودی به یک سرویس‌دهنده و یا مختل کردن سرویس استفاده نماید.

Kerberos

در هر یک از این 3 مورد، یک کاربر غیر مجاز ممکن است قادر به دسترسی به سرویسها و داده‌هایی باشد که مجوز دسترسی به آنها را ندارد. به جای ایجاد پروتکل‌های احراز هویت در هر سرویس‌دهنده بطور جداگانه، در واقع Kerberos سرویس‌دهنده احراز هویت متمرکزی که تابعی برای تایید هویت کاربران برای سرویس‌دهنده‌ها و سرویس‌های مختلف است، را برای کاربران فراهم می‌کند.

بطور انحصاری Kerberos بر پایه رمزنگاری متقارن طراحی شده و از رمزنگاری کلید عمومی استفاده نمی‌کند.

دو نسخه از Kerberos بیشتر از سایر موارد مورد استفاده قرار می‌گیرند:

نسخه 4 که هنوز هم وجود دارد، اگر چه کم کم از رده خارج می‌شود.

نسخه 5 که برخی از کمبودهای امنیتی نسخه 4 را اصلاح کرده و به عنوان یک استاندارد پیشنهادی برای اینترنت صادر شده است.

Kerberos4

نسخه 4 از Kerberos در اصل از پروتکل DES با عنوان یک پروتکل دقیق برای سرویس احراز هویت استفاده می‌نماید.

در یک محیط شبکه محافظت نشده، هر سرویس‌گیرنده می‌تواند به هر سرویس‌دهنده برای دریافت سرویس درخواستی را ارسال نماید. جعل هویت خطر امنیتی آشکار اینگونه محیطهاست. مهاجم می‌تواند وانمود نماید که یک مشتری دیگری است و دسترسی غیر مجاز به ماشین سرویس‌دهنده پیدا نماید. . برای مقابله با این تهدید، سرویس‌دهنده باید قادر به تایید هویت سرویس‌گیرنده‌ای که درخواست سرویس نموده-است، باشد (بار عملیاتی سنگین روی سرویس دهنده).

یک جایگزین خوب برای این امر استفاده از سرویس دهنده احراز هویت است تا بتواند کلمه ورودی تمام کاربران را پیدا کند و در یک پایگاه داده مرکزی ذخیره نماید. علاوه بر این، سرویس‌دهنده احراز هویت یک کلید مخفی منحصر به فرد را با هرکدام از این سرویس دهنده‌ها نیز به اشتراک می‌گذارد.

گفتگوی ساده برای احراز هویت

گفتگوی فرضی در یک سناریوی نمونه:

کاربر در یک ایستگاه کاری درخواست دسترسی به سرویس دهنده V را می‌کند.

سرویس‌گیرنده ماژول C در ایستگاه کاری کاربر، رمزعبور کاربر را درخواست نموده و سپس یک پیام خصوصی به سرویس‌دهنده احراز هویت که شامل شناسه کاربر، شناسه سرویس‌دهنده و رمزعبور کاربر است، ارسال می‌نماید.

سرویس‌دهنده احراز هویت پایگاه داده خود را چک نموده تا ببیند که آیا کاربر رمز عبور مناسب برای این شناسه کاربری تدارک دیده است یا خیر و آیا کاربر مجاز به دسترسی به سرویس دهنده V است.

اگر هر دو آزمون به تصویب رسید، سرویس‌دهنده احراز هویت کاربر را به عنوان کاربر معتبر پذیرفته و اکنون سرویس‌دهنده باید متقاعد شود که این کاربر معتبر است.

(1) C ->AS:$ID_c||P_c||ID_v$

(2) AS -> C:Ticket

(3) C -> V:IDc||Ticket

Ticket = $E(K_v, [ID_c||AD_c||ID_v])$

راه حل: سرویس دهنده یک بلیط که شامل شناسه کاربر و آدرس شبکه و شناسه سرویس‌دهنده است، را ایجاد می‌نماید. این بلیط با استفاده از کلیدهای مخفی که توسط سرویس‌دهنده احراز هویت و خود سرویس‌دهنده به اشتراک گذاشته شده، رمزگذاری می‌گردد. این بلیط به C باز فرستاده می‌شود. از آنجایی که بلیط رمزگذاری شده است لذا نمی‌تواند توسط C و یا مهاجم تغییر یابد.

گفت و گوی ایمن‌تر برای احراز هویت

سناریو قبلی برخی از مشکلات احراز هویت در محیط شبکه باز را حل می‌نماید اما دو مشکل اساسی هنوز باقی می مانند:

- اول اینکه باید تعداد دفعاتی را که کاربر رمزورود خود را وارد می‌نماید به حداقل رساند.

- دوم اینکه سناریوی پیشین شامل انتقال عبارت اصلی رمز عبور آن هم بصورت رمزنشده [پیام (1)] است. یک استراق سمع ساده می‌تواند رمز عبور را ربوده و از هر سرویسی که قربانی به آن دسترسی دارد، استفاده نماید.

برای حل این مشکلات اضافی، یک طرح معرفی می‌کنیم که از رمزهای عبور متن ساده و یک سرویس دهنده جدید استفاده می‌نماید و با عنوان سرویس دهنده اعطای بلیط یا TGS شناخته می‌شود.

گفت و گوی امن‌تر برای احراز هویت (ادامه)

سناریوی جدید به شرح زیر است:

یکبار برقراری جلسه به ازاء هر کاربر:

(1) $C \rightarrow AS: ID_c || ID_{tgs}$

(2) $AS \rightarrow C: E(K_c, Ticket_{tgs})$

یک بار برای هر نوع خدمات:

(3) $C \rightarrow TGS: ID_c || ID_v || Ticket_{tgs}$

(4) $TGS \rightarrow C: Ticket_v$

و یکبار به ازاء هر جلسه:

(5) $C \rightarrow V: ID_c || Ticket_v$

$Ticket_{tgs} = E(K_{tgs}, [ID_c || AD_c || ID_{tgs} || TS_1 || Lifetime_1])$

$Ticket_v = E(K_v, [ID_c || AD_c || ID_v || TS_2 || Lifetime_2])$

سرویس جدید یا همان TGS بلیطهایی را به کاربران ارائه می‌کند که توسط AS تصدیق شده باشد. بنابراین در ابتدا کاربران درخواست یک TGS برای تایید از AS می‌کنند. ماژول مشتری در ایستگاه کاری کاربر این بلیط را ذخیره نموده و هر زمان کاربری نیاز به دسترسی به یکی از سرویس‌های جدید داشته باشد، مشتری به TGS درخواست می‌دهد از بلیط برای احراز هویتش استفاده نماید. سپس TGS بلیط را برای یک سرویس خاص تایید می‌کند.

گفت و گوی ایمن‌تر برای احراز هویت (ادامه)

جزئیات :

1. مشتری یک بلیط تایید از جانب کاربر با ارسال شناسه کاربری به AS، همراه با شناسه TGS، برای استفاده از خدمات TGS درخواست می‌کند.

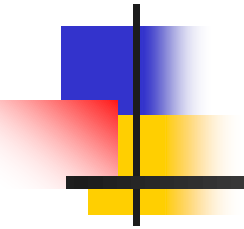
2. آنگاه AS از یک بلیط رمزگذاری شده برای پاسخگویی که در AS ذخیره شده است، استفاده می‌کند. هنگامی که این پاسخ به مشتری می‌رسد، مشتری رمز عبور کاربر را گرفته، کلید را تولید کرده و تلاش می‌کند تا پیام دریافتی را رمزگشایی نماید. در صورتی که رمز عبور صحیح فراهم شود، بلیط با موفقیت بازیافت می‌شود.

3. مشتری یک سرویس برای بلیط واگذاری – بلیطها از طرف کاربر درخواست می‌کند. برای این منظور، مشتری یک پیام به TGS شامل شناسه کاربر، شناسه سرویس مورد نظر و بلیط واگذاری - بلیطها ارسال خواهد نمود.

4. حال TGS بلیط عبور را با استفاده از کلید مشترکی که تنها بین AS و TGS تحت عنوان K_{tgs} وجود دارد، رمزگشایی نموده و موفقیت رمزگشایی را با وجود شناسه خود تایید خواهد نمود. آنگاه بررسی می‌کند تا مطمئن شود که طول عمر بلیط به پایان نرسیده باشد. سپس شناسه کاربر و آدرس شبکه را با اطلاعات ورودی کاربر برای تأیید هویت او مقایسه خواهد کرد. در صورتی که کاربر مجاز به دسترسی به سرویس دهنده V باشد آنگاه TGS یک بلیط برای دسترسی به سرویسها به او اعطا می‌نماید.

5. مشتری دسترسی به یک سرویس را از طرف کاربردرخواست می‌کند. برای این منظور، مشتری پیامی برای سرویس‌دهنده حاوی شناسه کاربر و بلیط اجازه واگذاری خدمات منتقل می‌نماید. سرویس‌دهنده با استفاده از محتویات بلیط هویت وی را اعتبار سنجی می‌نماید.

لذا ین سناریو جدید هر دو شرط مربوط به یک پرس و جوی رمز عبور در هر جلسه را بر آورده ساخته و از رمز عبور کاربر نیز محافظت خواهد نمود.



Kerberos 4 , 5

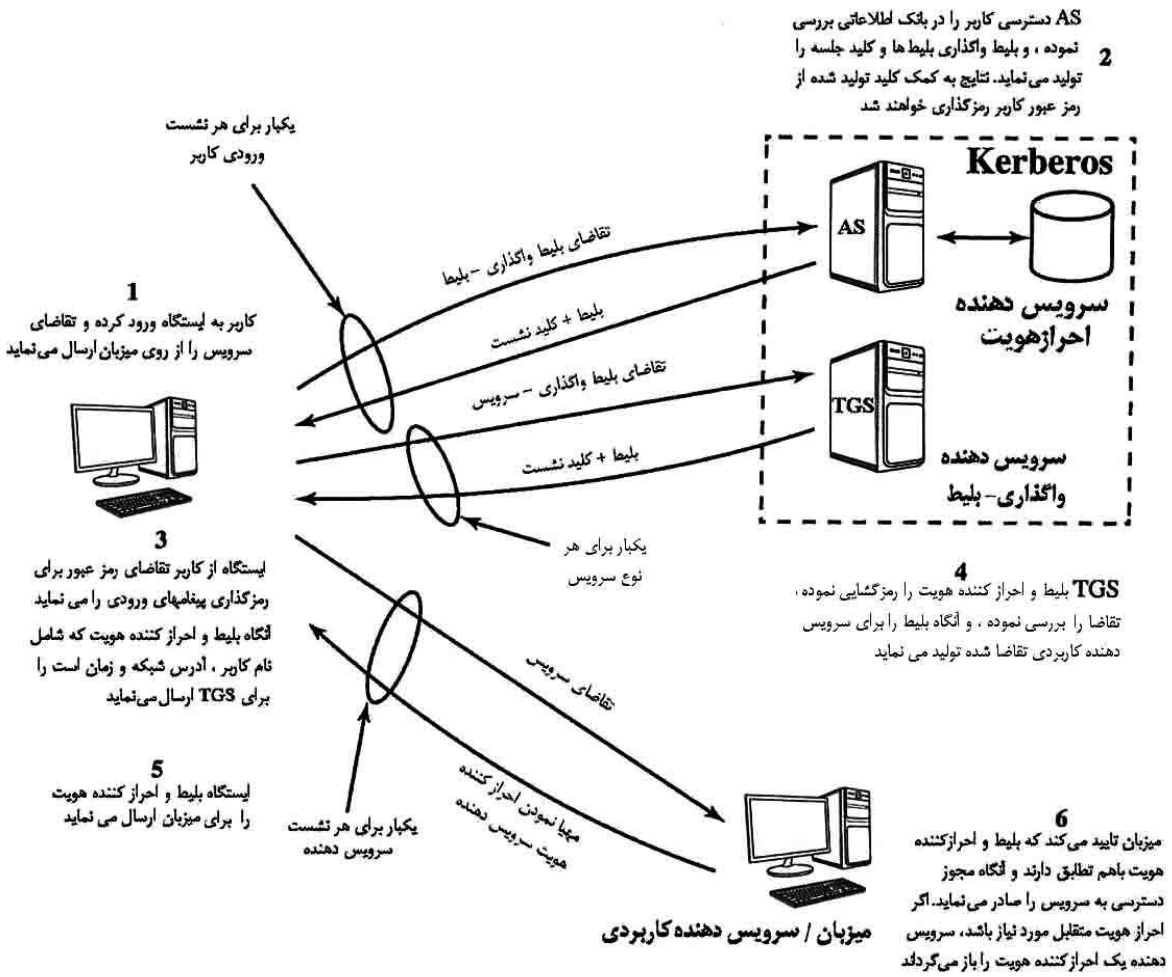
Kerberos 4

اما دو مشکل همچنان باقی می‌ماند:

اول اینکه طول عمر مربوط به بلیط واگذاری - بلیطها است. اگر طول عمر این بلیط بسیار کوتاه باشد (به عنوان مثال، چند دقیقه)، آنگاه کاربر بطور مکرر برای رمز عبور فراخوانده خواهد شد. اگر طول عمر طولانی باشد (به عنوان مثال، چند ساعت)، آنگاه مهاجم فرصت بیشتری برای پاسخ خواهد داشت. یعنی مهاجم می‌تواند شبکه را استراق سمع نموده و یک کپی از بلیط TG را گرفته و صبر نماید تا کاربر مشروع خارج شود. سپس مهاجم می‌تواند آدرس شبکه کاربر مشروع را جعل نموده و پیام مرحله (3) را برای TGS ارسال نماید.

دوم آن که باید شروطی برای سرویس‌دهنده‌ها وجود داشته باشد که هویتشان را برای کاربران اثبات نمایند. بدون چنین احراز هویتی، مهاجم می‌تواند تنظیمات را طوری بهم‌ریخته و تغییردهد که پیام‌ها به سرویس‌دهنده دیگری هدایت شوند. از آن پس سرویس‌دهنده کاذب می‌تواند در یک موقعیت به عنوان یک سرویس‌دهنده واقعی عمل نموده و هر گونه اطلاعات را از کاربر گرفته و از رسیدن سرویس واقعی به کاربر جلوگیری نماید.

Kerberos 4


AS دسترسی کاربر را در بانک اطلاعاتی بررسی
نموده ، و بلیط واگذاری بلیط ها و کلید جلسه را
تولید می‌نماید. نتایج به کمک کلید تولید شده از
رمز عبور کاربر رمزگذاری خواهند شد
2
یکبار برای هر نشست
ورودی کاربر
Kerberos
AS
سرویس دهنده
احرازهویت
تقاضای بلیط واگذاری - بلیط
بلیط + کلید نشست
تقاضای بلیط واگذاری - سرویس
بلیط + کلید نشست
TGS
سرویس دهنده
واگذاری- بلیط
1
کاربر به ایستگاه ورود کرده و تقاضای
سرویس را از روی میزبان ارسال می‌نماید
یکبار برای هر
نوع سرویس
3
ایستگاه از کاربر تقاضای رمز عبور برای
رمزگذاری پیغامهای ورودی را می نماید
آنگاه بلیط و احراز کننده هویت که شامل
نام کاربر ، آدرس شبکه و زمان است را
برای TGS ارسال می‌نماید
4
TGS بلیط و احراز کننده هویت را رمزگشایی نموده ،
تقاضا را بررسی نموده ، و آنگاه بلیط را برای سرویس
دهنده کاربردی تقاضا شده تولید می نماید
تقاضای سرویس
مبنا نمودن احراز کننده
هویت سرویس دهنده
5
ایستگاه بلیط و احراز کننده هویت
را برای میزبان ارسال می نماید
یکبار برای هر نشست
سرویس دهنده
میزبان / سرویس دهنده کاربردی
6
میزبان تایید می‌کند که بلیط و احرازکننده
هویت باهم تطابق دارند و آنگاه مجوز
دسترسی به سرویس را صادر می‌نماید. اگر
احراز هویت متقابل مورد نیاز باشد، سرویس
دهنده یک احرازکننده هویت را باز می‌گرداند

Kerberos 4

الف) احراز هویت برای مبادله سرویس دهنده جهت به دست آوردن بلیط واگذاری – بلیط

(1) C -> AS $ID_c||ID_{tgs}||TS_1$

(2) AS -> C $E(K_c, [K_{c,tgs}||ID_{tgs}||TS_2||Lifetime_2||Ticket_{tgs}])$

$Ticket_{tgs}=E(K_{tgs},[K_{c,tgs}||ID_C||AD_C||TS_2||Lifetime_2])$

ب) بلیط واگذاری تبادل خدمات برای به دست آوردن بلیط TS

(3) C -> TGS $ID_v||Ticket_{tgs}||Authenticator_c$

(4) TGS -> C $E(K_{c,tgs},[K_{c,v}||ID_v||TS_4||Ticket_v])$

$Ticket_{tgs}=E(K_{tgs},[(K_{c,tgs}||ID_C||AD_C||ID_{tgs}||TS_2||Lifetime_2])$

$Ticket_v=E(K_v, [K_{c,v}||ID_C||AD_C||ID_v||TS_4||Lifetime_4])$

$Authenticator_c=E(K_{c,tgs},[ID_C||AD_C||TS_3])$

پ) تبادل احراز هویت سرویس‌گیرنده/ سرویس‌دهنده برای به دست آوردن سرویسها

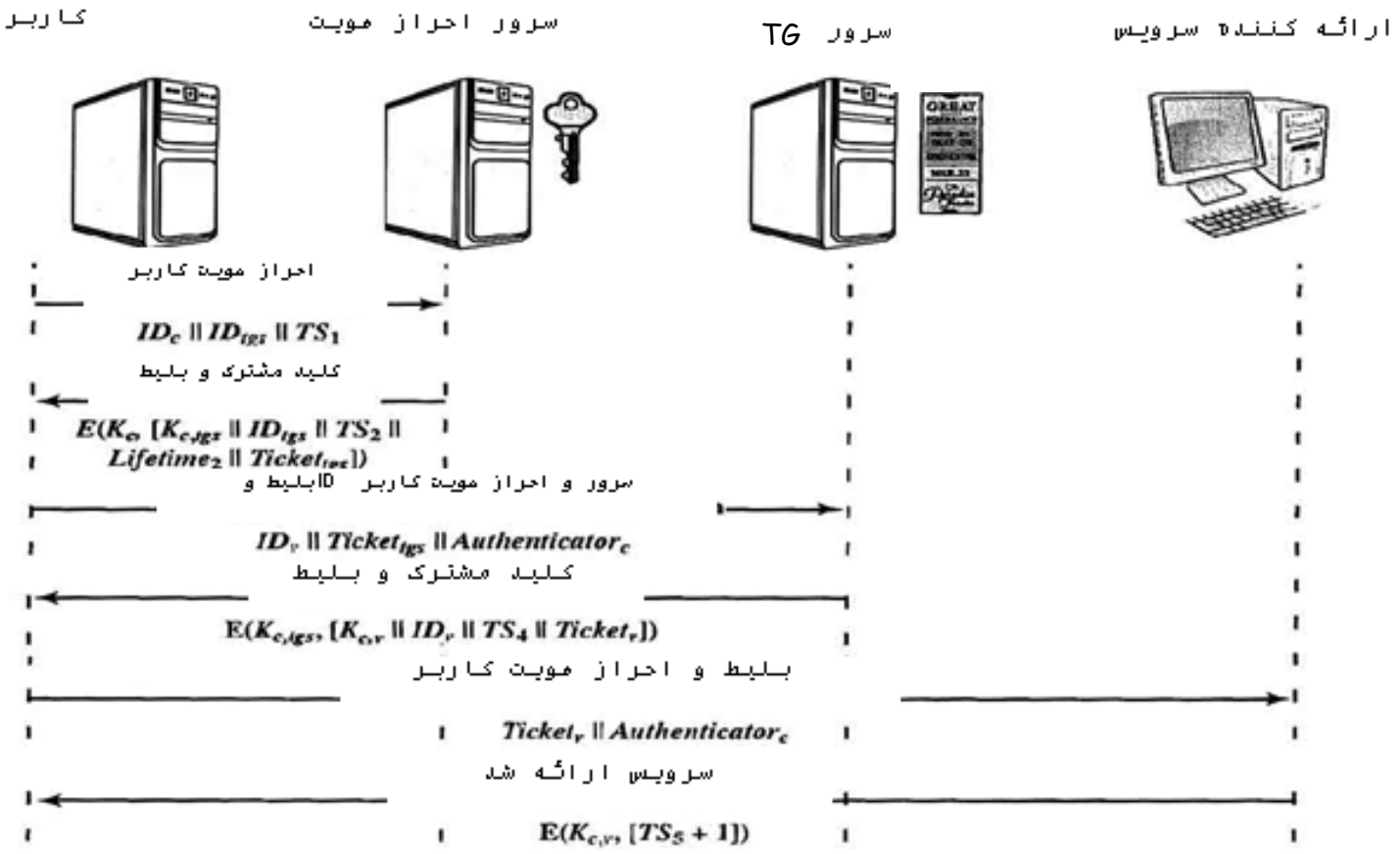
(5) C -> V $Ticket_v||Authenticator_c$

(6) V -> C $E(K_{c,v}, [TS_5+1])$(For mutual authentication)

$Ticket_v = E(K_v,[K_{c,v}||ID_C||AD_C||ID_v||TS_4||Lifetime_4])$

$Authenticator_c= E(K_{c,v}[ID_C||AD_C||TS_s])$

تبادلات Kerberos 4



مقایسه نسخ 4 و 5

۱. وابستگی به سیستم رمزنگاری: نسخه 4 نیاز به استفاده از DES دارد. در نسخه 5، متن رمزشده بوسیله یک شناسه نوع- رمزنگاری برچسب گذاری شده و هر روش دیگر رمزنگاری ممکن است مورد استفاده قرار گیرد.

۲. وابستگی به پروتکل اینترنت: نسخه 4نیاز به استفاده از پروتکل آدرس اینترنتی (IP) دارد. انواع دیگر آدرسها، مانند آدرس شبکه ISOبا این نسخه سازگار نیستند. در نسخه ۵ آدرس شبکه با یک برچسب نوع و طول همراه است که اجازه می‌دهد تا هر نوع آدرس‌دهی شبکه‌ای مورد استفاده قرار گیرد.

۳. ترتیب بایتهای یک پیام: در نسخه 4، فرستنده پیام روش مرتب سازی پیام خود را انتخاب نموده و پیام را برچسب گذاری می‌نماید تا کم ارزشترین بایت موجود در پایین‌ترین آدرس و یا پرارزشترین بایت موجود در پایین‌ترین آدرس را مشخص سازد. در نسخه 5، تمام ساختارهای پیام از "نشانه‌گذاری گرامری انتزاعی نسخه (ASN.1)" و "قوانین رمزگذاری عمومی (BER)" که مرتب سازی بایتها را بدون ابهام فراهم می‌کنند، استفاده می‌نمایند.

۴. طول عمر بلیط :مقادیر طول عمر در نسخه 4 در یک مقدار 8 بیتی در واحدهای پنج دقیقه‌ای از زمان کدگذاری می‌شود. بنابراین، حداکثر طول عمری که می‌توان بیان کرد عبارت از $2^8*5=1208$دقیقه (کمی بیش از 21 ساعت) خواهد بود که ممکن است کافی نباشد . در نسخه 5، بلیطها شامل یک زمان آغاز و پایان آشکار است که اجازه می‌دهد تا بلیط طول عمر دلخواه خود را داشته باشد.

۵. انتقال احراز هویت: نسخه 4 اجازه نمی‌دهد که اعتبار صادر شده برای یک مشتری به برخی از میزبانهای دیگر فرستاده شود و توسط برخی از سرویس‌گیرنده‌های دیگر استفاده می‌شود. این قابلیت باعث می‌شود تا یک سرویس‌گیرنده به یک سرویس‌دهنده دسترسی یافته و آن سرویس‌دهنده به سرویس‌دهنده دیگر به نمایندگی از سرویس‌گیرنده دسترسی یابد. نسخه 5این قابلیت را نیز فراهم نموده است.

۶. احراز هویت بین قلمرو: در نسخه 4، قابلیت همکاری میان N قلمرو نیازمند درحدود N^2 رابطه Kerberos- به- Kerberos بود. در نسخه 5 از یک روش نوینی پشتیبانی می‌شود که نیازمند تعداد روابط کمتری است.

توزیع کلید با استفاده از رمزنگاری نامتقارن

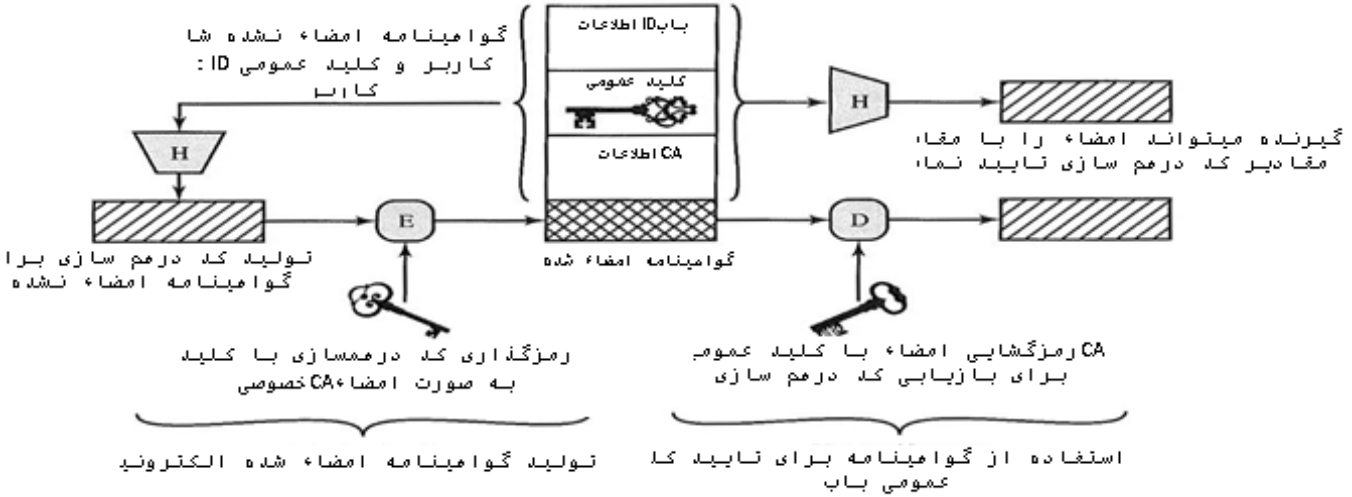
توزیع کلید با استفاده از رمزنگاری نامتقارن

یکی از نقش‌های عمده رمزنگاری کلید- عمومی رسیدگی به مشکل توزیع کلیدهاست. در واقع دو جنبه متمایز برای استفاده از رمزنگاری کلید- عمومی در این زمینه وجود دارد:

1. توزیع کلیدهای- عمومی
2. استفاده از رمزگذاری کلید- عمومی برای پخش کلیدهای محرمانه

گواهینامه‌های کلید- عمومی

دیدگاه رمزنگاری کلید- عمومی این است که کلید- عمومی در اصل عمومی است. بنابراین، اگر برخی از الگوریتم‌های کلید - عمومی مانند RSA به طور گسترده پذیرفته شده باشند آنگاه هر شرکت‌کننده می‌تواند کلید عمومی خود را به هر یک از شرکت‌کنندگان دیگر ارسال نموده یا در جامعه بزرگتری کلید را پخش نماید. اگر چه این روش مناسب است، اما یک ضعف عمده نیز دارد. هرکس می‌تواند چنین اعلان عمومی را جعل نماید.



برخی از کاربران می‌توانند تظاهر کنند که کاربر A هستند و کلید- عمومی را به یکی دیگر از شرکت کنندگان ارسال نموده و یا این کلید- عمومی را پخش نمایند. تا زمانی که کاربرA جعل سند را کشف نکرده و به دیگر شرکت‌کنندگان هشدار نداده باشد، جعل‌کننده قادر به خواندن تمام پیام‌های رمزگذاری شده به مقصد A بوده و می‌تواند از کلید جعلی برای احراز هویت خود استفاده نماید. راه حل این مشکل استفاده از گواهینامه کلید- عمومی است.

پخش کلیدهای محرمانه با کلید- عمومی

با رمزنگاری رایج، یک نیاز بنیادی برای ارتباط دو بخش بطور امن این است که آنها یک کلید مخفی را به- اشتراک بگذارند. یک روش، استفاده از الگوریتم دیفی- هلمن برای تبادل کلیدهاست.

هنگامی که باب به برقراری ارتباط با آلیس تمایل داشته باشد، باب می‌بایست کارهای زیر را انجام دهد:

1. آماده کردن یک پیام
2. رمزگذاری آن پیام با استفاده از رمزگذاری مناسب با یک کلید جلسه رایج یک بارمصرف
3. رمزگذاری کلید جلسه با استفاده از رمزنگاری کلید- عمومی با کلید عمومی آلیس
4. اضافه نمودن کلید جلسه رمزگذاری شده به پیام و ارسال آن به آلیس

فقط آلیس قادر به رمزگشایی کلید جلسه و درنتیجه بازیابی پیام اصلی خواهد بود. اگر باب کلید عمومی آلیس را با استفاده از گواهی کلید- عمومی آلیس به دست آورد، آنگاه باب مطمئن خواهد بود که این کلید معتبر است.

گواهینامه‌های X.509

سازمان ITU-T استاندارد X.509 را بعنوان بخشی از مجموعه توصیه‌های X.500 معرفی می‌نماید که معرف یک سرویس دایرکتوری است. دایرکتوری، در اینجا بواقع، یک سرویس‌دهنده و یا مجموعه توزیع‌شده از سرویس‌دهنده‌هاست که یک پایگاه داده از اطلاعات مربوط به کاربران را حفظ می‌نماید.

این اطلاعات شامل نگاشت نام کاربر به آدرس شبکه و همچنین دیگر ویژگی‌ها و اطلاعات مربوط به کاربران است.

استاندارد X.509 یک چارچوب برای ارائه خدمات احراز هویت توسط دایرکتوری X.500 برای کاربرانش تعریف می‌نماید.

این دایرکتوری ممکن است به عنوان یک انبار از گواهی کلید- عمومی بکار گرفته شود. هر گواهینامه شامل کلید عمومی یک کاربر بوده و توسط کلید خصوصی یک تاییدکننده گواهینامه مورد اعتماد نیز امضاء شده است.

علاوه بر این، X.509 پروتکل‌های احراز هویت جایگزین بر اساس استفاده از گواهینامه‌های کلید- عمومی را نیز تعریف می‌نماید.

استاندارد X.509بر پایه رمزنگاری کلید- عمومی و امضاهای الکترونیکی بنا نهاده شده است. استاندارد استفاده از الگوریتم خاصی را دستور نداده است ولی الگوریتم RSA را توصیه نموده است.

سوالات مرتبط

1. روشهایی که کلیدهای مخفی می‌توانند بین دو بخش ارتباطی توزیع شوند را بیان نمایید؟
2. تفاوت بین کلید اصلی و کلید جلسه در چیست؟
3. منظور از یک مرکز توزیع کلید چیست؟
4. یک محیط سرویس‌دهی کامل Kerberos شامل چه موجودیتهایی می‌باشد؟
5. در مفهوم Kerberos، یک realm یا ناحیه چیست؟
6. تفاوتهای اصلی نسخه های چهارم و پنجم Kerberos در چیست؟
7. منظور از nonce چیست؟
8. دوکاربرد متفاوت رمزنگاری کلید- عمومی در ارتباط با توزیع کلیدها کدامند؟
9. اجزاء اصلی یک دایرکتوری یا شاخه کلید عمومی کدامند؟
10. گواهینامه کلید- عمومی چیست؟
11. نیازمندیهای استفاده از یک طرح گواهینامه کلید- عمومی کدامند؟
12. هدف از استاندارد X.509 چیست؟

خلاصه: توزیع کلید با استفاده از رمزنگاری متقارن، Kerberos 4 , 5، گفتگوی ساده برای احراز هویت، توزیع کلید با استفاده از رمزنگاری نامتقارن، گواهینامه‌های کلید- عمومی، پخش کلیدهای محرمانه با کلید- عمومی، گواهینامه‌های X.509

جلسه بعدی:
امنیت لایه انتقال

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.