دانشگاه صنعتی امیرکبیر
دانشکده مهندسی کامپیوتر

دکتر حمیدرضا شهریاری

مهدی نیکوقدم

پاییز 1402

نکته1: جواب تمرینات صرفا برای افزایش اطلاعات دانشجویان قرار داده شده است. برای سوالات ممکن است جواب‌های مختلفی درست باشد. در نتیجه در صورتی که مشاهده کردید که جواب تمرینات شما با پاسخی که قرار داده شده است دقیقا مشابه نیست نگران نباشید! همان‌طوری که گفته شد برای سوالات جواب‌های مختلفی جواب صحیح است و این پاسخ‌ها تنها پاسخ‌های صحیح نمی‌باشد. همان‌طوری که از اول ترم در پایین تمامی تمرینات نوشته شده است هدف افزایش یادگیری شماست و همین که دانشجو تلاشی در راستای به دست آوردن جواب کرده باشد ارزشمند است.

نکته2: جواب برخی سوالات به طور کامل نوشته شده است. برخی سوالات نیز با توجه به اینکه حالت تحقیقاتی داشته‌اند آورده نشده است. همچنین با توجه به این موضوع که برخی دانشجویان جواب‌های واقعا جالبی به سوالات داده‌اند. پاسخ آن‌ها به عنوان یک نمونه در این فایل آورده شده است تا نحوه پاسخگویی به سوالات را مشاهده کنید و بتوانید نحوه تفکر و فکر دیگر دوستانتون رو ببینین.

1.سه روش که می‌تواند امنیت اعتبارسنجی کاربر در یک محیط توزیع شده را بهبود دهد بیان کنید؟

نمونه اول

Public Key Infrastructure (PKI): در PKI از کلید عمومی برای ایمن سازی ارتباطات استفاده می‌شود و هر کاربر یک کلید عمومی و یک کلید خصوصی دارد که از کلید عمومی برای رمزگذاری داده ها و از کلید خصوصی برای رمزگشایی داده ها استفاده می‌شود.

Single Sign-On (SSO) with Federation: SSO به کاربران اجازه می‌دهد تا با یک مجموعه از اعتبارنامه ها به چندین برنامه یا خدمات دسترسی داشته باشند.

Multi-Factor Authentication: در این حالت یک لایه امنیتی بیشتر اضافه می‌شود که نیاز است کاربر قبل از گرفتن دسترسی از این مراحل امنیتی عبور کند.

نمونه دوم

1. رمزگذاری تیکت با استفاده از کلیدی که از کانال امن با کاربر مبادله شده است.
2. در نظر گرفتن طول عمر مناسب برای تیکت، جهت کاهش احتمال حمله man in the middle و replay
3. استفاده از زیرساخت کلید عمومی

به طور کلی راه‌ها و روش‌های احرازهویت و اعتبارسنجی، بستگی به فاکتورهای احرازهویت دارد. که می‌تواند تک فاکتوره، دو فاکتوره یا سه فاکتوره(احرازهویت مولتی فاکتور) باشد. توضیحات در سر کلاس حل تمرین داده خواهد شد.

2. چهار نیازی که برای Kerberos تعریف شده است کدامند؟

Secure

حفظ ارکان امنیت برای کارفرمایان و کارگزاران

Reliable

قابل اتکا (توزیع شده)، بدون وابستگی به مرکزی خاص (Distributed)

Transparent

شفافیت، از لحاظ پوشیده و نامعلوم بودن پیچیدگی و اتفاقات پشت صحنه برای کاربر

Scalable

پشتیبانی از تعداد زیادی سرور و کلاینت

3. تفاوت‌های بین ورژن 4 و Kerberos 5 در چیست؟

۱. در کربروس ۴ تنها می‌توان از الگوریتم رمزنگاری **DES** استفاده نمود؛ ولی در کربروس ۵، استفاده هر الگوریتم متقارنی ممکن می‌باشد.

۲. کربروس ۴ وابسته به پشته **IP** است، در حالی که در کربروس ۵ می‌توان از هر آدرس شبکه‌ای با پشته‌های دیگر استفاده نمود.

۳. در کربروس ۴، زمان استفاده از بلیط‌ها محدود است، ولی در کربروس ۵ چنین محدودیتی وجود ندارد.

۴. در کربروس ۴، امکان انتقال اعتبار یک کاربر به یک سرور دیگر وجود ندارد، ولی این مساله در کربروس ۵ رفع شده است و امکان آن به وجود آمده است.

۵. در کربروس ۴، با افزایش تعداد قلمروها (**Realm**ها)، تعداد کلیدها به صورت تصاعدی افزایش می‌باشد؛ ولی این مشکل در کربروس ۵ حل شده است.

4. هدف از استفاده کلید جلسه در Kerberos چیست؟

نمونه اول

اگر از یک کلید متقارن برای کلیه‌ی ارتباطات استفاده شود ممکن است آن کلید شنود شده و یا به طریقی هک شود. با استفاده از کلید جلسه، برای هر جلسه یک کلید خاص داریم و بدین ترتیب احتمال شنود و سوءاستفاده از کلید خیلی کم و تقریبا محال می‌شود. بدین ترتیب در صورت دستیابی به یک کلید جلسه، فقط آن جلسه فاش می‌شود و جلسات دیگر امن باقی می‌ماند.

نمونه دوم

در Kerbros دو کلید جلسه وجود دارد:

۱) **کلید جلسه میان Client و TGS**: این کلید برای رمزنگاری متقارن بین Client و TGS استفاده می‌شود. در مرحله ۴ پروتکل، TGS بلیت استفاده از سرویس را به کمک این کلید رمزگذاری کرده و برای Client ارسال می‌کند. از این رو، اگر کسی این پیام را شنود کند، چون به کلید جلسه دسترسی ندارد، نمی‌تواند بلیت را استخراج کند. پس تنها کاربر واقعی می‌تواند به بلیت دست پیدا کند.

۲) **کلید جلسه میان Client و Server**: این کلید در مرحله ۶ پروتکل Kerbros، جهت احراز هویت کارگزار استفاده می‌شود. همچنین از این کلید برای رمزگذاری داده‌های جابه‌جا شده میان Client و Server استفاده می‌شود.

5.تفاوت بین توافق کلید و تبادل کلید در چیست؟ کدام سربار کمتری دارند؟ در چه زمانی از توافق کلید و در چه زمانی از تبادل کلید استفاده می‌کنیم؟

در الگوریتم‌های توافق کلید (Key agreement) مشابه آنچه در Diffie Helmann استفاده می‌شود، هر دو طرف مکالمه در ساخت کلید مشارکت می‌کنند، ما در تبادل کلید/انتقال کلید (Key exchange/Key transport) مشابه RSA Key Exchange در TLS، کلید توسط یک طرف احراز شده مکالمه ساخته شده و به طرف دیگر ارسال می‌شود.
اگر هیچ گونه اقدام امنیتی دیگری مثل احراز اصالت در نظر نگیریم، و فقط توافق کلید را با تبادل آن مقایسه کنیم، در تبادل کلید، به دلیل وجود چند مرتبه رمزگذاری (متقارن اگر یک master key قبلا به اشتراک گذاشته شده، یا نامتقارن در حالت عمومی) عملیات بیشتر در یک طرف انجام می‌شود و طرف دیگر تنها رمزگشایی می‌کند، همچنین الگوریتم‌های رمزگذاری نامتقارن پیچیدگی محاسباتی بیشتری دارند.
بنابراین توافق کلید سربار کمتری خواهد داشت.
در تبادل کلید، ویژگی‌های امنیتی مانند Forward Secrecy را از دست می‌دهیم.

6.پارامترهایی که حالت Session را تعریف می‌کنند را بیان کرده و مختصرا توضیح دهید. تفاوت بین کلید عمومی خصوصی و کلید جلسه را بیان کنید.

پارامترهای یک جلسه (Session) در دنیای امنیت، عموما شامل

- یک کلید جلسه، جهت حفظ محرمانگی مکالمات همان جلسه
- طرفین جلسه، چه کسانی در جلسه شرکت دارند (می‌توانند در مکالمات شرکت کنند)
- طول اعتبار جلسه، اینکه قبل از نیاز به احراز دوباره، تا چه مدت می‌توان به شکل فعلی (از کلید فعلی) برای جلسه استفاده کرد
- تفاوت کلیدهای خصوصی، عمومی و جلسه، در این است که کلیدهای خصوصی و عمومی، یک جفت کلید برای رمزگذاری نامتقارن و عموما احراز اصالت هستند، ولی کلید جلسه، عموما کلیدی است که از طریق کلیدهای عمومی و خصوصی با حفظ محرمانگی و احراز اصالت، بین طرفین مکالمه منتقل می‌شود (یا سر آن به توافق می‌رسند) و متقارن است تا سربار محاسباتی کمتری در طول مکالمه داشته باشیم.

7. تعریف شما از مرکز توزیع کلید چیست و راه‌های ممکن برای توزیع یک کلید سری بین دو واحد را نام ببرید.

مرکز توزیع کلید، مرکزی است که واحدها به آن اعتماد دارند و از طریق کانالی امن، قبلا کلیدی (که می‌تواند در قالب رمز عبور باشد) با آن مبادله کرده‌اند، و این مرکزی قابل اعتماد و مشترک میان واحدها، با کلیدی که با واحدها در اختیار دارد، آنها را احراز کرده و داده‌های جلسه (مانند کلید سری) را میان آنها به صورت امن منتقل می‌کند تا میان واحدها ارتباطی امن برقرار شود.
برای توزیع کلید سری بین دو واحد، در صورتی که واحدها از استانداردی مانند X.509 پشتیبانی کنند، می‌توانند گواهی یکدیگر را احراز کرده و بین خود با رمزگذاری نامتقارن کلید سری منتقل کنند
در صورت وجود مرکز تولید کلید نیز می‌توانند برای ارتباط با یکدیگر از آن مرکز درخواست ایجاد ارتباط کنند.

8. به لینک https://sslcheck.cert.ir/fa/ و یا https://sslcheck.certcc.ir مراجعه کنید و بعد از مطالعه و فهم مسئله‌ای که هدف سایت است، 3 سایت را به دلخواه از نظر امنیتی بررسی کنید و نتایج را به صورت اسکرین در PDF قرار دهید.

حذف!

9. چگونه می‌توان از رمزنگاری کلید عمومی برای توزیع یک کلید مخفی استفاده کرد؟

یکی از روش‌های مرسوم با استفاده از الگوریتم دیفی هلمن صورت می‌گیرد. توضیحات مربوط به الگوریتم در اسلاید ۶۲ تا ۶۵

10. الگوریتم دیفی هلمن را با عدد اول q=11 و ریشه ابتدایی a=2 در نظر بگیرید.
الف. اگر کاربر کلید عمومی A و Ya=9 را داشته باشد کلید اختصاصی Xa کدام است؟
ب. اگر کاربر B کلید عمومی برابر ۳ داشته باشد، کلید سری مشترک kچیست؟

الف)

$$Y_A = a^{X_A} \bmod q \rightarrow 9 = 2^{X_A} \bmod 11 \rightarrow X_A = 6$$

ب)

$$K_{AB} = (Y_B)^{X_A} \bmod q \rightarrow K_{AB} = 3^6 \bmod 11 = 3$$