دانشکده مهندسی کامپیوتر - دانشگاه صنعتی اصفهان
نیمسال دوم تحصیلی ۱۴۰۳-۱۴۰۴

تکلیف دوم رایانش امن

دکتر خلیلی - علیرضا میرزائی - مهدی آقاجانیان

۱. TLS/SSL

۱.۱. سوال اول

۱.۱.۱. با توجه به فرآیند Handshake در TLS/SSL، مراحل اصلی تولید و ارسال کلیدهای رمزنگاری و احراز هویت بین کلاینت و سرور را توضیح دهید. نقش هر یک از پیام‌های اصلی Handshake (مانند ClientHello, ServerHello, ...) در این فرآیند چیست؟

۱.۱.۲. با بهره گیری از مفاهیم تولید MAC و رمزگذاری در TLS Record Protocol، یک روش ساده‌تر و جدید برای تضمین همزمان محرمانگی و یکپارچگی (صحت) یک بلوک داده طراحی کنید. توضیح بدهید که چگونه با استفاده از یک کلید مشترک از پیش تعیین شده، می‌توانید داده اصلی را رمزگذاری کرده و سپس یک کد احراز هویت پیام (همان MAC) برای داده رمزگذاری شده (یا داده اصلی، با ذکر دلیل انتخاب) تولید و به آن اضافه کنید تا گیرنده بتواند دو شرط Integrity و Privacy را تضمین شده داشته باشد.

۱.۱.۳. تفاوت‌های کلیدی بین نسخه‌های مختلف پروتکل TLS/SSL (مانند SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 و TLS 1.3) چیست؟ TLS 1.3 چه بهبودهای مهمی نسبت به نسخه‌های قبلی ارائه داده و این بهبودها چگونه بر امنیت و کارایی ارتباطات برقرار شده بر این بستر تأثیر می‌گذارند؟

۱.۲. مدیریت و توزیع گواهی‌ها در اینترنت

درباره‌ی سازوکارهای توزیع و بررسی وضعیت ابطال گواهی‌ها در لیست پایین، در اینترنت تحقیق کنید و سپس به سوالات زیر پاسخ دهید

- CRL (Certificate Revocation List)
- OCSP (Online Certificate Status Protocol)
- CT (Certificate Transparency)

۱.۲.۱. تفاوت اصلی بین CRL و OCSP چیست و OCSP چه مشکلی را در فرآیند بررسی وضعیت ابطال گواهی‌ها حل می‌کند؟

۱.۲.۲. OCSP با چه چالش‌ها و مشکلاتی مواجه بود؟ OCSP Stapling و OCSP Must-Staple چگونه این مشکلات را برطرف کردند و چه مزایایی نسبت به OCSP ساده ارائه می‌دهند؟

۱.۲.۳. با توجه به ساختار PKI و نقش CA ها، توضیح دهید که چگونه هویت خود CA ها در اینترنت تأیید می‌شود و (مرورگر) کاربران چگونه به کلید عمومی COMهای ریشه (Root CAs) اعتماد می‌کنند؟

۱.۳. بخش امتیازی

۱.۳.۱. درباره‌ی یکی از حمله‌های POODLE, BEAST یا Heartbleed تحقیق کنید (دوتا از این حملات در تکلیف عملی شما نیز استفاده شده اند). این حمله چه تاثیرات احتمالی روی سیستم‌های نفوذ شده داشت، به کدام بخش از فرآیند کار TLS حمله می‌کرد و چگونه از آن جلوگیری شد؟

۱.۳.۲. برای یک شرکت با شبکه داخلی شامل ۱۰۰ سرور، یک سیستم مناسب برای توزیع و مدیریت گواهی‌های دیجیتال طراحی کنید. در طراحی خود، ملاحظات معقولی مانند در دسترس بودن (Availability)، سرعت دریافت و ابطال گواهی‌ها را در نظر بگیرید. (راهنمایی: می‌توانید از تحقیق درباره‌ی LDAP directories مانند Active Directory Certificate Services یا از مکانیزم OCSP با کمی بهبود، برای این سوال استفاده کنید.)

۲. Blockchain/BitCoin

۲.۱. تحقیق کنید difficulty هم اکنون در بیت کوین چقدر است؟ این میزان سختی نشان دهنده چند صفر در جلوی target است؟

۲.۲. وبسایت‌هایی وجود دارند که به کمک آنها می توانید وضعیت فعلی و تاریخچه تراکنش هاو دیگر اطلاعات مفید مربوط به بیت کوین را در آنها ببینید[1] [2] [3]. بر این اساس به سوالات زیر پاسخ دهید:

۲.۲.۱. چه میزان از توان شبکه دست mining pool هاست؟

۲.۲.۲. بزرگترین mining pool کیست و چند درصد توان شبکه را دارد؟ به نظر شما این موضوع به امنیت بیت‌کوین آسیبی می‌زند؟

۲.۲.۳. اندازه تقریبی هر بلاک در این هفته چقدر است؟

[1] btscan.org
[2] blockchair.com/bitcoin
[3] blockchain.com

۳. Kerberos

۳.۱. سوال ۱: پروتکل Kerberos و تکامل آن

۳.۱.۱. پروتکل Kerberos از نسخه اولیه تا نسخه ۵ که در کلاس مطرح شده است، تغییرات قابل توجهی داشته است. این تغییرات شامل افزودن ماژول‌های جدید و بهبود امنیت و کارایی پروتکل بوده است. سه تفاوت اصلی بین Kerberos نسخه ۴ و نسخه ۵ را توضیح دهید.

۳.۱.۲. در نسخه ۵ پروتکل Kerberos، ماژول PKINIT اضافه شده است. هدف و دلیل از اضافه کردن این ماژول چیست و به نظر شما چه مشکلی از نسخه‌های قبلی را، چه از لحاظ امنیتی چه از لحاظ عملی، حل می‌کند؟

۳.۲. جریان درخواست

۳.۲.۱. با استفاده از نمادهای رسمی مشابه کتاب، جریان پیام‌های رد و بدل شده بین کلاینت Alice، سرور احراز هویت و TGS را برای دسترسی به سرویسی به نام Bob بنویسید. تمام کلیدهای رمزنگاری، تابع‌های هش و داده‌های رمزشده را به شکل متغیر در پیام ها مشخص کنید.

۳.۲.۲. در مدل‌سازی خود، توضیح دهید که چرا تیکت TGT با کلید KDC رمزگذاری می‌شود و چگونه این کار به امنیت پروتکل کمک می‌کند. همچنین توضیح دهید که چرا تیکت دسترسی به Bob، به Alice ارسال می‌شود و نه مستقیماً به Bob.

۳.۳. حمله Golden Ticket در Kerberos

توضیحات: یکی از حملات مشهور علیه پروتکل Kerberos، حمله Golden Ticket است. این حمله به مهاجمان امکان می‌دهد دسترسی طولانی‌مدت و بدون محدودیت به شبکه را به دست آورند و عملا برای مدت زیادی در سیستم با دسترسی مناسب بتوانند کار کنند.

۳.۳.۱. حمله Golden Ticket چگونه انجام می‌شود؟ مراحل اصلی این حمله را با جزئیات تشریح کنید و توضیح دهید که مهاجم به چه اطلاعاتی نیاز دارد تا این حمله را با موفقیت اجرا کند.

۳.۳.۲. این حمله به کدام بخش از معماری Kerberos هدف قرار می‌دهد و چرا این بخش نقطه ضعف محسوب می‌شود؟

۳.۳.۳. دو راهکار مشخص برای مقابله با این حمله را پیشنهاد دهید و مزایا و معایب هر راهکار را بیان کنید.

۳.۴. سوالات مربوط به آماده شدن برای تکلیف عملی

قبل از انجام بخش عملی پیاده‌سازی Kerberos، به سوالات زیر پاسخ دهید:

الف) هماهنگ‌سازی زمان (Time Synchronization) چه نقشی در امنیت پروتکل Kerberos ایفا می‌کند؟ توضیح دهید که چرا عدم هماهنگی ساعت بین کلاینت، سرور احراز هویت و سرویس‌دهنده می‌تواند باعث شکست در احراز هویت شود.

ب) فرآیند عملکرد دستورات kinit و klist در محیط Kerberos چیست و هر کدام چه اطلاعاتی را نشان می‌دهند؟ توضیح دهید که چگونه این دستورات به عیب‌یابی مشکلات احراز هویت کمک می‌کنند.

سوالات عملی

1. Kerberos Challenge:

i. راه‌اندازی Realm:

- یک MIT Kerberos KDC و admin server روی یک میزبان Linux (VM، WSL2 یا هر محیط دلخواه) نصب و یک realm (مثلاً EXAMPLE.COM) ایجاد کنید.

ii. ساخت Principals:

- حداقل یک user principal بسازید.
- یک service principal ایجاد کرده و کلید آن را در یک keytab قرار دهید.

iii. ادغام Service:

- یک network service (مثل web با Apache، SSH یا SMB) را با Kerberos محافظت کنید.
- از یک کلاینت Kerberos-aware پس از گرفتن ticket به سرویس وصل شوید.

iv. Break & Fix

- دو خطای متفاوت Kerberos (مانند clock skew، ticket expiration یا name mismatch) را عمداً ایجاد و سپس رفع کنید.

v. گزارش ویدیویی:

- ویدئویی حداکثر ۵ دقیقه‌ای که مراحل بالا و توضیحات رفع خطا را نشان می‌دهد.
- توضیح کوتاه درباره realm و سرویس.
- گرفتن ticket (klist)
- دسترسی موفق به سرویس با Kerberos

2. TLS Hardening Challenge

i. وضعیت اولیه:

- روی Apache یا Nginx یک سایت HTTPS (با self-signed) راه‌اندازی کنید.
- با یک TLS scanner (مثل testssl.sh یا sslyze) پروتکل‌ها و cipher suites پیش‌فرض را ثبت کنید.

ii. سخت‌سازی:

- تنظیم کنید که فقط TLS 1.3 / TLS 1.2 فعال باشد.
- تمام cipher و پروتکل ضعیف (3DES، RC4، TLS 1.0/1.1، SSLv3 و CBC) را حذف کنید.
- اخطارهای باقی‌مانده اسکنر (small DH parameters، Compression و ...) را نیز برطرف کنید.

iii. راستی‌آزمایی:

- دوباره همان scanner را اجرا کنید تا مطمئن شوید پروتکل‌ها و cipherهای قدیمی حذف شده و اخطار بحرانی وجود ندارد.

iv. گزارش ویدیویی:

- ویدئویی حداکثر ۵ دقیقه‌ای که تغییرات، نتایج اسکن و توضیحات دلایل سخت‌سازی را نشان می‌دهد.
- هر آیتم ناامن حذف‌شده و دلیل ناامن‌بودن
- بلاک نهایی تنظیمات TLS.

در صورت بروز مشکل یا سوال درباره سوال ها، ترجیحا در گروه درس و در صورت الزام در این یا این آدرس در تلگرام سوالات خود را بپرسید.

موفق باشید.