به نام خدا

مبانی رایانش امن

دکتر موزرانی

تکلیف سوم

مهلت تحویل: ۱۴ خرداد ساعت ۲۳:۵۹

۱- با ذکر دلیل تعیین نماید کدام یک از موارد زیر درست و کدام یک نادرست است.

الف) مدل BLP از نظر کاربرد کاملا مناسب و بدون عیب است.

ب) در سیستمی که از مدل کنترل دسترسی ORCON استفاده می کند اگر کاربر A فایل f را ایجاد کرده و اجازه دسترسی آن را به کاربر B بدهد، آنگاه کاربر B می تواند فایل f را ویرایش و اجازه دسترسی به کل محتوای فایل جدید را در اختیار کاربر C قرار دهد.

ج) اگر در سیستمی از مدل Biba استفاده شود محرمانگی سیستم تضمین شده است.

۲- پاسخ سوالات زیر را با ذکر دلیل توضیح دهید.

الف) اگر یک Subject مشخص داشته باشیم برای تعیین آنکه Subj مورد نظر بر روی هر Obj چه مجوزهایی دارد از کدام روش یا روش های کنترل دسترسی می توان استفاده نمود؟

ب) یکی از راه‌های مقابله با Ring-Crossing Fault چیست؟

ج) اصل Fail-Safe Defaults چیست و در چه مواردی کاربرد دارد؟

۳- با توجه به primitive operation های مطرح شده در ویدئوهای درس ابتدا command نظیر هر یک از دستورات ۱ تا ۴ را تعریف کرده و سپس با استفاده از این command ها و همچنین با در نظر گرفتن ماتریس کنترل دسترسی زیر:

الف) با ذکر دلیل تعیین نمایید هر یک از command های اجرا شده در ماتریس مذکور تغییری ایجاد می کنند یا خیر.

ب) ماتریس کنترل دسترسی نهایی را مشخص کنید.

ج) لیست کنترل دسترسی و لیست قابلیت های نظیر ماتریس کنترل دسترسی نهایی را نیز تشکیل دهید.

۱) دستور Grant.read.file(Si, O, Sj) در صورتی که کاربر Si مالک فایل O باشد و خود نیز دسترسی خواندن بر روی فایل O را داشته باشد اجرا شده و اجازه خواندن از O به Sj داده می شود.
۲) دستور Grant.write.file(Si, O, Sj) در صورتی که کاربر Si مالک فایل O باشد و خود نیز دسترسی نوشتن بر روی فایل O را داشته باشد اجرا شده و اجازه نوشتن بر روی O به Sj داده می شود.
۳) دستور Revoc. execution.file(Si, O, Sj) در صورتی که کاربر Si مالک فایل O باشد اجرا شده و اجازه اجرای O از کاربر Sj سلب می شود.

۴) دستور Create.file (Si, O) اجرا شده و حقوق Owner, Read, Write, Execution بر روی O در اختیار کاربر Si قرار می گیرد.

	Obj1	Obj2	Obj3
Subj1	OWRX	R	RWX
Subj2	R	RW	R
Subj3	RW	ORW	OWRX

Command های اجرا شده به شرح زیر است:

- Create.file(Subj1, Obj4)
- Grant.write.file(Subj1, Obj3, Subj2)
- Grant.read.file(Subj1, Obj4, Subj2)
- Revoc.execution.file(Subj1, Obj3, Subj3)

۴- با توجه به سناریو تعریف شده در زیر و مدل BLP به سوالات با ذکر دلیل پاسخ دهید:

L(S1, O1) = {Confidential, {A, B}}

L(S2, O2) = {Top Secret, {B, C}}

L(S3, O3) = {Secret, {A}}

L(S4, O4) = {Unclassified}

الف) آیا S2 به O1 دسترسی خواندن و نوشتن دارد؟

ب) آیا S3 به O2 دسترسی خواندن و نوشتن دارد؟

ج) آیا S1 به O3 دسترسی خواندن و نوشتن دارد؟

د) در سناریو فوق جریان اطلاعات از پایین به بالا است یا برعکس؟

ه) شبکه lattice نظیر این مدل را رسم کنید.

حال سناریو زیر را برای مدل Biba در نظر گرفته و مجددا به سوالات الف تا د پاسخ دهید:

L(S1, O1) = {Very Trusted, {A, B}}

L(S2, O2) = {Trusted, {B, C}}

L(S3, O3) = {Slightly Trusted, {A}}

L(S4, O4) = {Untrusted}

۵- روش Shamir Threshold Scheme را در نظر بگیرید و به سوالات زیر پاسخ دهید:

الف) مزایا و معایب این روش را بیان کنید.

ب) اگر معادله $5024x^2 + 1234x + 1523$ را داشته باشیم مقدار threshold و secret را مشخص کنید. سپس t نقطه دلخواه از معادله را انتخاب کرده و نشان دهید با داشتن این t نقطه چگونه می توان به شی قفل شده دسترسی یافت.

۶- در سایت https://attackdefense.com آزمایشگاه های زیر را تکمیل کرده و برای هر آزمایش با ذکر توضیحات کامل از نحوه حل ویدئو تهیه کرده و لینک ویدئو را در پاسخنامه پیوست کنید.

https://attackdefense.com/challengedetails?cid=198

۷- در ویدئو های درس با دو روش کنترل دسترسی اجباری و تفویضی آشنا شدید. هدف از این سوال بررسی این دو روش در سیستم عامل ویندوز ۱۰ می باشد.

الف) کنترل دسترسی تفویضی (DAC)

در سیستم عامل ویندوز بدون استفاده از هیچ ابزاری میتوانید این نوع کنترل دسترسی را انجام دهید .این تنظیمات را میتوانید با راست کلیک کردن روی فایل، انتخاب گزینه properties و رفتن به تب security انجام دهید. مراحل زیر را انجام داده و نتایج بدست آمده ر گزارش کنید.

۱- یک کاربر جدید تحت عنوان User1 بسازید و سپس یک فایل متنی دلخواه را در مسیری مشترک میان کاربران (برای مثال دایرکتوری root در درایو C) قرار داده و سپس با استفاده از User1 محتویات فایل متنی را بخوانید. سپس فایل مورد نظر را در دایرکتوری Deocuments کاربر جاری خود قرار داده و مجددا تلاش کنید با استفاده از کاربر User1 آن را بخوانید.
در کدام حالت کاربر User1 اجازه خواندن فایل را در اختیار داشت؟ با توجه به نتایج بدست آمده توضیح دهید دسترسی های پیش فرض یک فایل بر چه اساسی تنظیم می شوند.

۲- در گام بعد کاری کنید که تمام دسترسی های پیش فرض بر روی ای فایل از بین رفته و به کاربر فعلی خود دسترسی خواندن و به کاربر User1 دسترسی نوشتن بر روی فایل را بدهید. سپس نتیجه را تست و گزارش کنید.

الف) کنترل دسترسی اجباری (MAC)

در سیستم عامل ویندوز سیستمی تحت عنوان windows integrity level یا WIL وجود دارد که می تواند مدل کنترل دسترسی برمبنای صحت را تا حدودی فراهم نماید. برای استفاده از این سیستم و تنظیم سطح صحت برنامه ها و فایل ها از ابزاری به نام chml استفاده کنید. این ابزار را می توانید از این لینک دانلود نمایید.

۱- یک فایل با محتوای دلخواه بسازید و سطح صحت این فایل را در سطح high تنظیم کرده سپس محتویات آن را بخوانید و یک متن جدید در آن بنویسید. نتایج را گزارش کنید.

۲- سیاست No Read Up را تنظیم و مرحله قبل را مجددا تکرار کرده و نتایج بدست آمده را گزارش کنید.

۳- برنامه ای به زبان c یا c++ بنویسید که فایل را خوانده و محتوای آن را چاپ کند سپس یک محتوای جدید در فایل بنویسد. ضمنا در صورتی که هر یک از عملیات های فوق ممکن نبود خطای مناسب نمایش دهید. برنامه را کامپایل کرده و به کمک فایل exe بدست آمده قسمت بعدی را انجام دهید.

۴- سطح صحت فایل متنی را در سطح medium و سطح صحت برنامه را در سطح low تنظیم کرده و عمل خواندن و نوشتن فایل را به کمک برنامه تست کرده و نتیجه را گزارش کنید.

لطفًا به نکات زیر توجه نمایید:

- در صورت وجود سوال و یا ابهام، می‌توانید به ایمیل های زیر پیام دهید:

Sara.br1378@gmail.com (سارا برادران)

ae.naderi@gmail.com (عاطفه نادری)

- فایل تکلیف را در سامانه تحویل دهید و به فرم name_stdnumber.zip باشد.
- به تکالیف مشابه نمره ای تعلق نخواهد گرفت.

سلامت و موفق باشید.