به نام خدا

تمرین سری اول امنیت پایگاه داده ها

نکات قابل توجه:

پاسخ خود را به صورت الکترونیکی به آدرس m.shahriyary@gmail.com یا shahriyary@ce.sharif.edu با عنوان DBSec:Assignment1 ارسال نمایید.

حل تمرین های درس باید به صورت فردی انجام پذیرد و پاسخ های گروهی به هیچ عنوان پذیرفته نیست.

به پاسخ هایی که رونوشت یکدیگر باشند، هیچ نمره ای تعلق نمی گیرد.

در صورت تاخیر در ارسال پاسخ، به ازای هر روز 25% نمره کل تمرین، جریمه احتساب می گردد.

در صورت استفاده از مرجعی خاص لطفا لیست مراجع در انتهای پاسخ آورده شود.

1 - هر یک از مفاهیم زیر را توضیح دهید:

الف) خطی مشی کنترل دسترسی

ب)مکانیزم کنترل دسترسی

ج)مدل کنترل دسترسی

د)Security through obscurity

2 - لیست کنترل دسترسی(Access list) با لیست قابلیت(capability list) را توضیح دهید و مزایا و معایت هر کدام چه می باشند؟

3 - سوالات زیر را بر اساس ماتریس کنترل دسترسی زیر پاسخ دهید:

	S_1	S_2	S_3	o_1	o_2	o_3
S_1				o, r, w, c		w, c
S_2				r	o, r	r
S_3				r	w, c	r, o

برای این سیستم دستورات زیر تعریف شده است:

```
command grant right(p, f, q, r)
    if r in a[p, f] and c in a[p, f]
    then
        enter r into a[q, f];
end
command delete right(p, f, q, r)
    if r in a[p, f] and o in a[p, f]
    then
        delete r from a[q, f];
end
```

command *grant ownership*(p, f, q)
if r, w, c, o **in** a[p, f] **and** r, w **in** a[q, f]
then
enter o **into** a[q, f];
end

اگر عملیات زیر به ترتیب در این سیستم اجرا شوند، ماتریس کنترل در هر مرحله از اجرا به چه صورت می باشد؟ لطفا ماتریس کنترل دسترسی را در هر مرحله بکشید و ماتریس به دست آمده را برای دستور بعدی به کار ببرید.

1. *grant right*(S1, O2, S3, r)
2. *grant right*(S2, O2, S3, r)
3. *grant ownership*(S2, O2, S3)
4. *grant right*(S1, O1, S3, w)
5. *grant ownership*(S1, O1, S3)
6. *delete right*(S3, O1, S1, w)
7. *delete right*(S3, O1, S1, r)
8. *grant right*(S3, O2, S1, w)
9. *grant right*(S1, O3, S3, w)
10. *grant right*(S1, O3, S2, w)
11. *grant ownership*(S3, O3, S2)

4- در سوال 3، فرض کنید در شرایطی که w در $a[S_2, O_k]$ قرار نداشته باشد که $k = 1, 2, 3$ آنگاه سیستم امن می باشد. آیا یک سری دستور وجود دارد که سیستم را غیر امن کند؟

5) دوباره سوال 3 را در نظر بگیرید. همانطور که می دانید مساله ایمنی در مدل HRU در حالت کلی تصمیم ناپذیر است. آیا در مورد سیستم بالا این موضوع صادق است؟ (توضیح دهید)

6) وحید می تواند در فایل X بنویسد و از فایل Y بخواند و همچنین می تواند فایل Z را اجرا کند. سعید می تواند X را بخواند و Y را هم بخواند و هم بنویسد ولی به Z دسترسی ندارد.
الف) لیست کنترل دسترسی(ACL)
ب) لیست قابلیت(Capablitiy list)
را برای هر یک بیان کنید.

7) به سوالات زیر پاسخ دهید:
الف) معایب مدل Take-grant را نام ببرید و توضیح دهید.
ب) مدل Acten چه عیب هایی از مدل Take-grant را برطرف می کند؟ چگونه؟ (همراه با مثال توضیح دهید).

8) با توجه به اینکه مدل HRU یک مدل عمومی برای مدل های کنترل دسترسی ماتریسی می باشد، پس باید بتوان مدل اخذ-اعطا(Take-Grant) را نیز با آن بیان نمود. مدل Take-Grant را با استفاده از مدل HRU بیان نمایید(برای این منظور باید دو عنصر اصلی مدل HRU یعنی مجموعه حقوق دسترسی(R) و مجموعه دستورات (C) را بر اساس مدل Take-Grant مشخص نمایید.

9) چه معیار هایی را برای ارزیابی یک مدل کنترل دسترسی پیشنهاد دهید. در مورد هر معیار توضیح کافی دهید و تعارض هر یک را با سایر معیارها بررسی کنید.

10) چرا در مدل های کنترل دسترسی اختیاری امکان وجود برنامه های خرابکار مانند اسب تراوا وجود دارد؟ برای این مشکل یک مثال بیاورید.

11) آیا می توان یک سیستم امنیتی را طراحی نمود که در آن هیچ گونه فرضی در خصوص اعتماد (trust) وجود نداشته باشد؟ با آوردن دلیل توضیح دهید.

12) سیاست کنترل دسترسی زیر را در نظر بگیرید:

- کارمندان می توانند به اطلاعات شخصی خود دسترسی یابند و آن را به روز رسانی نمایند(می توانند به حقوق خود دسترسی یابند)
- مدیران می توانند به اطلاعات شخصی(pd) و اطلاعات مرتبط با حقوق (sd) کارمندانشان دسترسی یابند و آن ها را بخوانند و به روز رسانی کنند.

الف) اگر بخواهیم که S_1 را مدیر S_2 قرار دهیم، دستورات مدل HRU را برای آن بیان نمایید .

(make-manager(S_1, S_2, pd, sd))

M:Manage R:Read W:write

ب)ماتریس کنترل دسترسی را بکشید.

13) به اعتقاد بسیاری از محققین "اطلاع از وجود یک داده" نیز نوعی "افشاء" محرمانگی محسوب می شود. در این خصوص وجود مفهوم جامعیت ارجاعی در پایگاه داده ها و نیاز به کلید خارجی چه مشکلات امنیتی را در امنیت پایگاه داده ها به دنبال دارد؟ چه راه حل هایی را پیشنهاد می کنید؟