


نام درس: امنیت پایگاه داده‌ها http://ce.sharif.edu/courses/84-85/2/ce925 نیم‌سال دوم ۸۴-۸۵ مدرس: دکتر جلیلی حل تمرین: حمید رضا شهریاری	باسمه تعالی تمرین سری اول موعده تحویل: ۸۵/۱/۲۶	 دانشگاه صنعتی شریف دانشکده‌ی مهندسی کامپیوتر
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------

- هر گونه کپی منجر به نمره صفر (کپی دهنده و کپی گیرنده) خواهد شد.
- پاسخها را حتی الامکان به صورت الکترونیکی به shahriari@mehr.sharif.edu بفرستید (Subject: [DBsec: Assignment1]). در غیر این صورت به صورت کاغذی در کلاس تحویل دهید.

۱. مثالی بیاورید که نقض محرمانگی منجر به نقض تمامیت (Integrity) می‌شود.
۲. سه رهیافت عمده در امنیت پیشگیری^۱، تشخیص^۲ و بازیابی^۳ است. یک مثال برای هر یک از گزاره های زیر ارائه کنید:

- a. پیشگیری از تشخیص و بازیابی مهمتر است.
- b. تشخیص از پیشگیری و بازیابی مهمتر است.
- c. بازیابی از تشخیص و پیشگیری مهمتر است.

۳. حمله SQL Injection که یک حمله متداول به پایگاه‌های داده‌ای است را شرح دهید. برای این کار می‌توانید به سایت‌های مرتبط مانند www.cert.org یا rr.sans.org مراجعه نمایید. توضیح شما باید شامل نحوه عملکرد، آسیب‌پذیری مورد سوءاستفاده، و نتیجه احتمالی حمله باشد.

	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

۴. ماتریس کنترل دسترسی زیر را در نظر گرفته و به پرسشهای بعدی پاسخ دهید: (حقوق موجود w : Write, r : Read, c : Control, o : Own هستند).

در این سیستم فقط دستورهای زیر تعریف شده‌اند:

```

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

```

¹ Prevention
² Detection
³ Recovery

```

command grant_ownership(p, f, q)
    if r,w, c, o in a[p, f] and r,w in a[q, f]
    then
        enter ointo a[q, f];
    end

```

a. ماتریس کنترل دسترسی بالا را پس از اجرای هر یک از دستورهای زیر نشان دهید. از ماتریس جدید

برای دستور بعدی استفاده نمایید.

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)

b. فرض کنید که اگر $w \notin a[S_2, O_k]$ ($k=1,2,3$) برقرار باشد، آنگاه سیستم امن است. آیا ترتیبی از

اجرای دستورها وجود دارد که سیستم را ناامن کند؟

c. Ruzzo, Harrison و Ullman ثابت کرده‌اند که «با داشتن یک حالت از سیستم حفاظتی، تعیین ایمن بودن سیستم برای یک حق خاص تصمیم‌ناپذیر است». پس چرا شما می‌توانید مساله b را برای حق

w پاسخ دهید؟

۵. در دانشکده‌ای برای تسهیل در راهنمایی دانشجویان، استادان راهنما به کارهای دانشجویی در دروسهای اخذ شده

دسترسی دارند. استادان هم مجاز به رایزنی با دیگر اساتید در دانشکده خود درباره کارهای انجام شده در

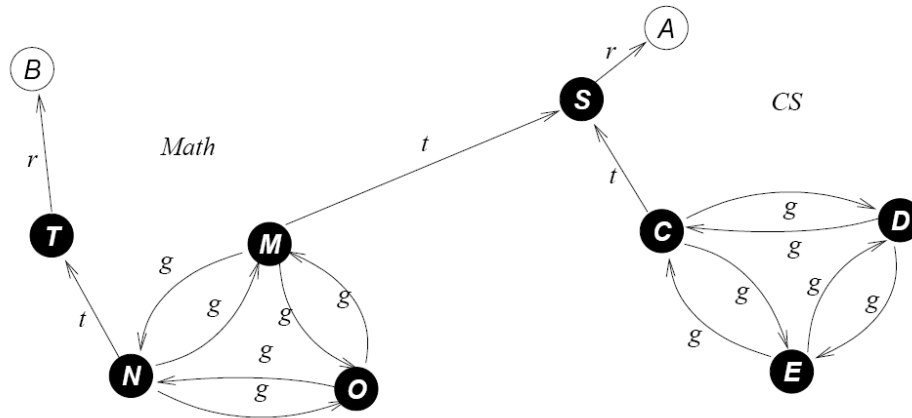
درس خود می‌باشند. فرض کنید برای ارزیابی سیستم (از نظر برآورده کردن نیازمندیهای کنترل دسترسی) از

مدل Take-Grant استفاده شده است. نمونه‌ای از آن در زیر نشان داده شده است: در شکل دو دانشکده CS و

Math وجود دارد. دانشجوی S درسهایی از M (استاد دانشکده Math) و C (استاد دانشکده CS) گرفته است.

دانشجو تمرین A را برای درس که توسط C تدریس می‌شود انجام داده است. دانشجوی T هم درسی با آقای

N گرفته است. (راسهای مشکی Subject/Object و راسهای سفید Object هستند).



آیا سیستم نیازمندیهای امنیتی (بیان شده در ابتدای مساله) را برآورده می‌کند؟ به طور خاص به سؤالهای زیر پاسخ دهید (برای پاسخهای زیر با ارائه یک دنباله از اعمال قواعد مدل Take-Grant دلیل بیاورید)

- آیا C تمرینهای A از S را می‌تواند بخواند؟
- آیا C می‌تواند به دیگر استادان دانشکده CS اجازه مشاهده تمرین A را بدهد؟
- آیا استادان در دانشکده‌های دیگر از دسترسی به A منع می‌شوند؟
- آیا استادان دانشکده CS هیچ وقت نمی‌توانند تمرین B از دانشجوی T را مشاهده کنند؟