

تمرینات از مبحث کنترل دسترسی اختیاری

امنیت پایگاه داده

مسعود نیازی

دستورات زیر در یک سیستم کنترل دسترسی HRU 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

ماتریس کنترل دسترسی بعد از اجرای هر یک از دستورات
زیر به چه صورتی خواهد بود؟

1. grant right(S2,O2,S3,r)
2. grant ownership(S2,O2,S3)
3. grant right(S1,O2,S3,r)
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)

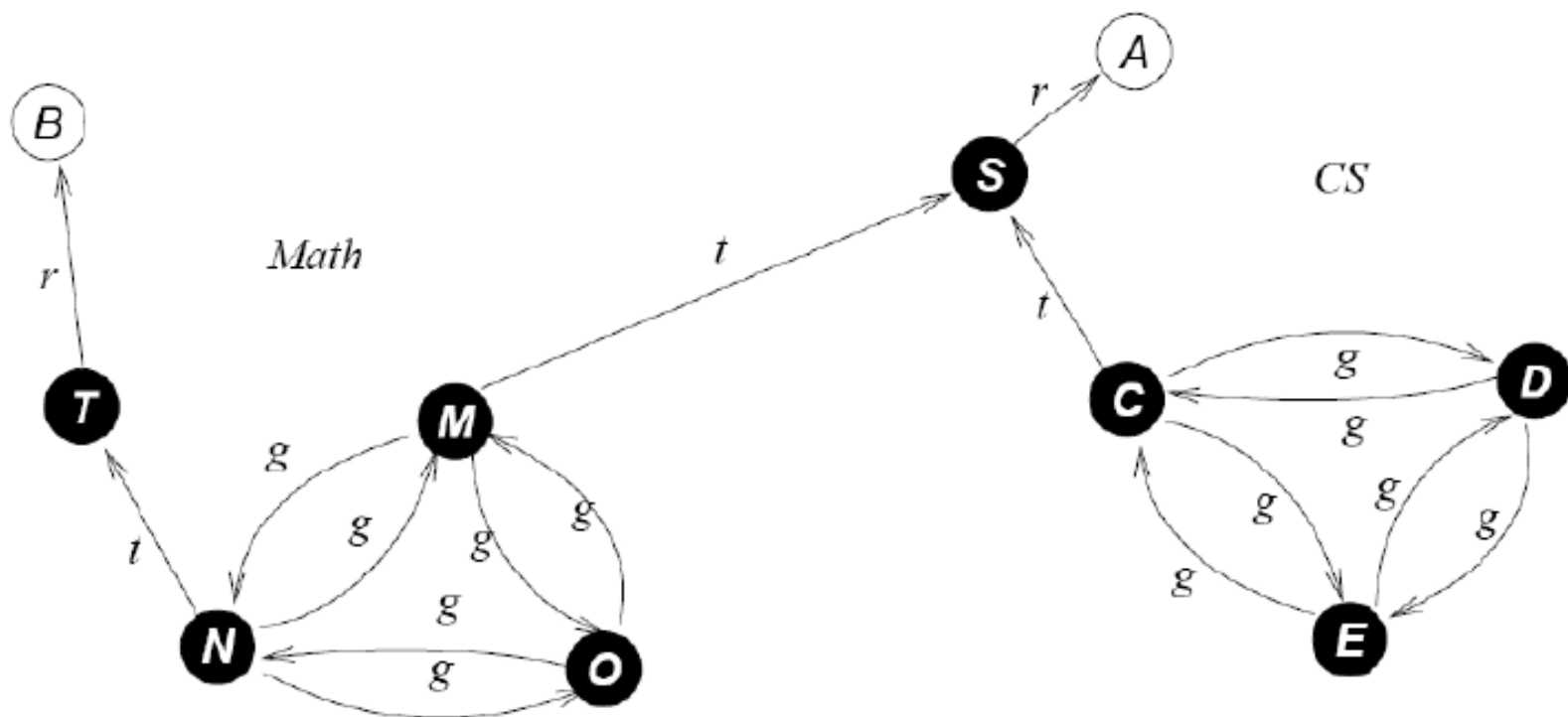
ماتریس کنترل دسترسی اولیه

	S1	S2	S3	O1	O2	O3
S1				o,r,w,c		w,c
S2				r	o,r	r
S3				r	w,c	r,o

سوال دوم

در دانشکده ای برای تسهیل در راهنمایی دانشجویان، استادان راهنما به کارهای دانشجو و درس های اخذ شده دسترسی دارند. استادان هم مجاز به رایزنی با دیگر اساتید در دانشکده خود درباره کارهای انجام شده در درس می باشند. فرض کنید برای ارزیابی سیستم (از نظر برآورده کردن نیازمندیهای کنترل دسترسی) از مدل Take-Grant استفاده شده است.

- در شکل دو دانشکده CS و Math وجود دارد. دانشجوی S درس هایی از M (استاد دانشکده Math) و C (استاد دانشکده CS) گرفته است. دانشجو تمرین A را برای درسی که توسط C تدریس می شود، انجام داده است. دانشجوی T هم درسی با آقای N گرفته است.



1. آیا سیستم نیازمندی های امنیتی (بیان شده در ابتدای مساله) را برآورده می کند؟ بطور خاص به سوال های زیر پاسخ دهید:

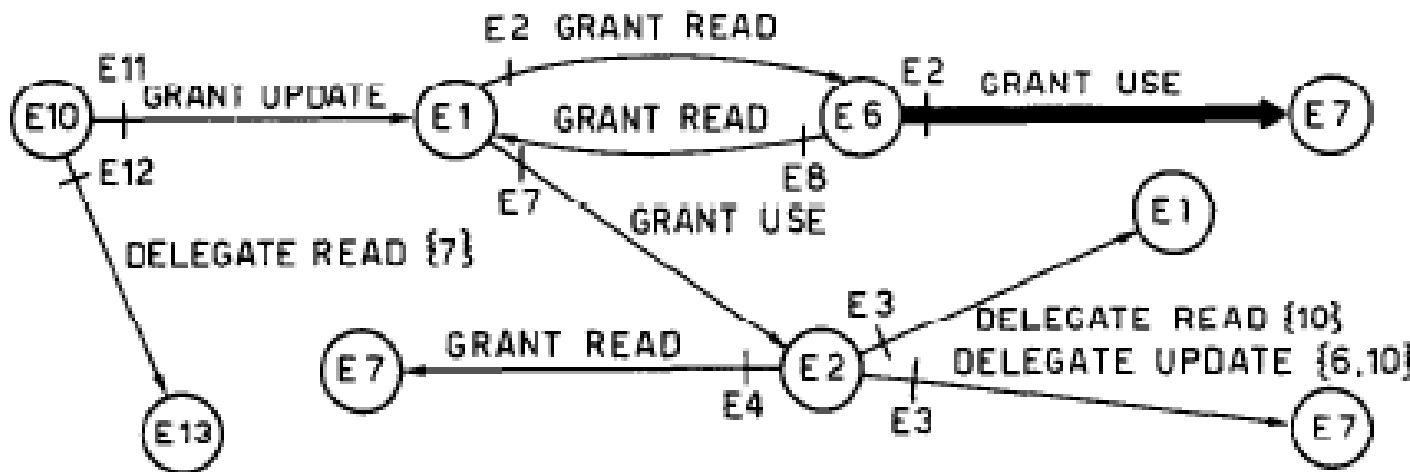
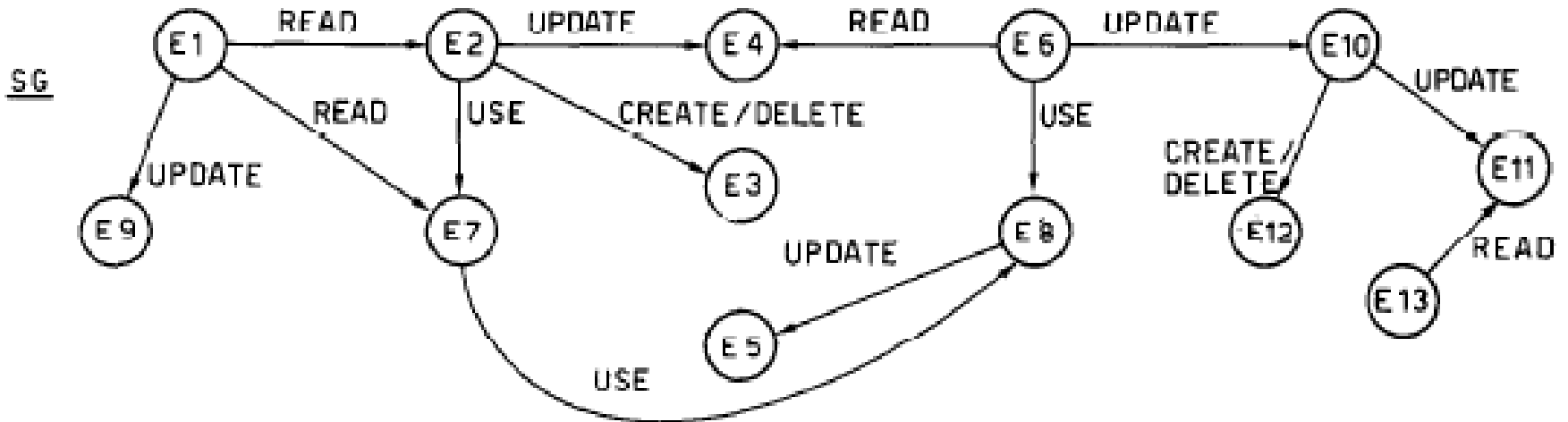
1. آیا C تمرین های A از S را می تواند بخواند؟

2. آیا C می تواند به دیگر استادان دانشکده CS اجازه مشاهده تمرین A را بدهد؟

3. آیا استادان دانشکده های دیگر از دسترسی به A منع می شوند؟

4. آیا استادان دانشکده CS هیچ وقت می توانند تمرین B از دانشجوی T را مشاهده کنند؟

ACTion-ENtity



Legend:

- E1 = user
- E2 = application program
- E3 = data file
- E4 = data record
- E5 = data file
- E6 = user
- E7 = application program
- E8 = peripheral
- E9 = data record
- E10 = application program
- E11 = record field
- E12 = record field
- E13 = user

ACTION-ENTITY

TABLE OF SECURITY CLASSES

E1	+ <u>UPDATE</u> - <u> </u>
⋮	
E3	+ <u> </u> - <u>CREATE/DELETE</u>
⋮	

با توجه به جدول مقابل به سوالات زیر پاسخ دهید:

1. موجودیتهای فقط فعال و فقط غیر فعال را پیدا کنید.
2. مجوزهای مستقیم و غیر مستقیم E1 را مشخص کنید.