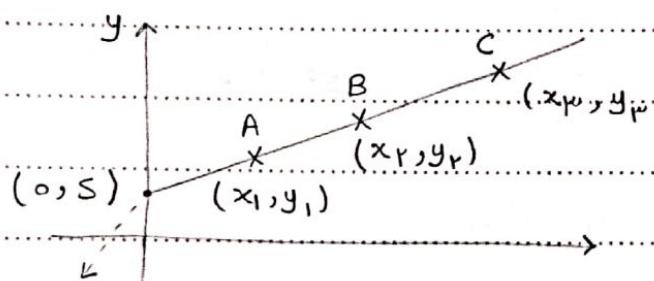


سی ایز بیم

۱۷  
← سیم لردن راز پلاس رازی راسن ۴. بقیر تقسیم بردیم و اون ۳.

و تقریباً می باشد تا این راز ساخته شده و بی بعفونی و قتایهم نیاز نشست. لذا همچو باستاد رازه



m.out.of.n ... m ≤ h ...

محل برخورد با

هر ۲ قسم از ۳ تقریب من تواند اون راز را

محور یعنی میگزیند اون

راز

لے طبقه میں ← توی یعنی میگزیند اون

### Access control

فقط ۳ ←

۱۸  
← راه ارتباطیں الین و باب پلاس الین وارد بیسی سیستم و از مریق سیستم با باب

در ارتباط باس

۱۹  
← الین کو من خواهد دارد دارد system بسی هد فس الین کو از منابع Access control.

سیستم استفاده کنند ← آن سرگار دانس الین مفتوح میگزیند ←

۲۰  
آیا تو واقعاً همین کوئی کی میگزیند؟ ۲- حالات وارد سرگار به چه منابع تابعه میگزیند  
کی تو نه دلسته سن دانس باسی

← یعنی ایجاد کردن دسترسی دارندگان (Authentication) و محدودیت دادن برای دسترسی (Authorization).

- لے تو یہ این سیمی دسترسی محدودیت میں سے ہے۔
- اس سیمی محدودیت میں محدودیت میں سے یہ یہ ہے کہ کسی کو اپنے با اون سمع کا خلاف نہ کرنے کا اعلان کرو۔

← Authentication تو یہ Subject

- System → تو External Entity
- لے ملے ہوئنے دارد ملکا حوصلہ میں داری ہے۔
- جس طبقہ سے اس کا دامدیں ملکے میں ہوئے۔
- هر سفاریوں کی identity یعنی ملکا وہی داری ہے۔
- لے تو اس کا subject identity یعنی داری ہے۔
- لے تو اس کا subject identity یعنی داری ہے۔

- Authorization و Authentication کو بھی کام کا ابھام کہا جاتا ہے۔
- میں دیہم اپنے کہ identity کو میں زیر دشائیں کر دیں۔
- بچہ زدن این ہماری فلسفہ کے subject کے کہہ دیں۔
- احم از اعمالت است۔

- طیوری کی ایسا کہ لفڑی این identity را داری دیں۔

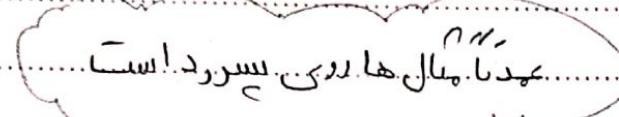
- یعنی اطلاعاتی رابطہ system بدهے۔ این اطلاعاتی ۳ حالات میں داری ہے۔

- 1. what the Entity know? \*
- 2. Who has? \*
- 3. What is? \*

- موجودیت ہی میں دونہ؟ \*
- داری کے کیا ہے؟ \*
- چیز کیا ہے؟ \*

\* سیستم ازایین من ریهون کتاب بعدی یا پیر هنریه است یا بیهوده است

له یعنی داشتن ولن امتنان خلی خالی بالا نمیست

  $\rightarrow$   $A \rightarrow$  Authentication

همین اطلاعات لغ طبری فراهم من کنه مثل سوردس

$\hookrightarrow a \in A$

$\rightarrow C \in C$

$C \rightarrow$  Complementary information  
 یعنی داشته باشد یا نداشته باشد. هر چندی سخنیم این ادعا درست است یا ن است من هایم باید از طبری خود را در خصیره کنیم سوں اون اطلاعات لغ دخیره من کنیم مسنه اون اطلاعات تکمیلی

$F \rightarrow$  complementation function  $\rightarrow A \rightarrow F$

$F(a) = h(a) = c$   $\rightarrow F: A \rightarrow C$  بعده مجموعه  $C$  من برداشت

$L \rightarrow$  Authentication function  $\rightarrow$  سود است از نماین استفاده من سود لغ طبری داره من فرسته دهاید مقابله کنیم با  $C$ . لغ سخنیم ادعا درست یا ن است خواهد بود و  $\{True, False\}$  است این مجموعه دخیره  $\rightarrow$  لغ این طبری داده است لغ مسلسله بود و بین

$S \rightarrow$  Selection function  $\rightarrow$  یعنی از چه چیزی مثلا سورد را انتخاب کنیم

.15.

قرار میں لیمہ با مو جو دیتھاں خارجی در لیمہ استے۔ این مو جو دیتھاں خارجی د

الزاماً طابعه يعني انسان نيسن مملكة ان موحد يبيت خارجي على System ديلم باس يدا

(...Authentication System... (برائی پھنسی) با سند تعریف میں ... (Authenticatiون

10

لیلیا، میر دلیلیست، لرزو، میا، میلیا، میلیلیست

نلہے۔ علاوہ بن موصود یستھا ہیں لہ ماں این سسٹم را عمر احمد لرد بیم لہ باہماں مار لے۔

موجودیت‌های هم‌هسته‌ای از تعریف اقرا و نسبت با این system در آن دارد.

نگه داشت. همچو مودعیت هایی ل.ب.....system طرد من لشکر ستر سیسون ب.ج. اولن حیرزهای

سیستمی سسٹم system.....

.20 .

\*بلسمی، طاریم، داریم، لامن، تو، لتبای، سیستم، Bob، Alice، Dr. لشکریان، وینا، بابی، بیری، ها

هم دریم لوبن هوایم با این System طریق هم Trudy

هدف از این اعمالت چه؟ بحث‌منابع یاداران است لوح‌داریم و برای محققان

از این منابع از احراز احتاله استفاده می‌کنیم.

پس ایجا میسری منابع داریم که به اون طایران لاصود مون در تعریف قائم باهای خارجی مارکت

اچاره می دیم از این منابع ببره هند پس و به اون طایران که نیز خواهیم این امانته

۵. نیز دیم و همین مور سفع دسترسی لرخی منابع متفاوت است

لے باعث ایجاد انتیه درای ریت فعل افرادی سرد چه و اسی Study  
و یا چه و اسی افرادی که سفع دسترسی این دارند ← و اسی همین از  
آخر از احوالات استفاده می کنیم که اتفاق بالا نوقشت

۱۰ طوی system تغیر هر طایر subject تعریف ای لشیم که با استفاده از این subject

است لع مسخن لشیم که احوالات ملیم د هر طایر چن هست و هر کدام از طایرها

۱۵ چه سفع دسترسی دارند ← تغیر هر طایر مجاز subject تعریف ای دیم

\* طوی system احوالات دیم ای لشیم و به میسری منانیزم نیاز داریم ←

با ای تامولن ای لع میلا تعریف ای دیم مله بالا رایر اورده می لشیم

۲۰ A ← مجموعه ای است لع طایران از طوی اون می تون ملا بسور دسون لع اتفاق لشیم

← اینه مجموعه می باشد راه راح سیستم ای لع ملا ب سور د حداقل ۲۴ رقمی باشد

که مجموعه A باعث می شود فعالیت بورد هم تعیین لشیم ملا ای بر بیم عدد ۲۴ رقمی باشد

عَفَّانِي... سُورَد... هَا مِلْسَه... يَا بِلَّا ازِنْ... يَا الْغَنَّامِ... ٢٥٩... صَرْفَنِي... طَرَالْمَرْ تَلْدِيمِي... عَفَّانِي.

سسورڈ ۴۵۰ میلینے سے مقام سے میں فناہیں لیں۔ فناہیں طلبیں۔

فَعَالَىٰ لِسْرُورٍ... وَ

مِنْ طَهْ

$$P(\Theta | Y) = P$$

.....  
४८

...P.....

اسسته آیا این موضوع را من تو نمیرم برای فعالیت سیوردهم بلبیر؟

صفاتي

لے لوی طبیعه حون طبیعه لندو مر اسسته باید محسشوی طامل طبیعه انجام بدهیم دلی توی مقنای

ل سور د. الیفورسی. لستیسته. یعنی می‌ایم اون. لسور د. همان که. احتیاں. استفاده می‌شون. تو. لطف مادر

لیست اسے را بala گی لیسے قرار من دلیم و این باعث میں سر یعنی بہ جواب بوللائیں

نہیں۔ مفتاہیں، سورج، و فقہائیں، ملیل، حقیقت از نعمتیں، باہمیں برابر بساں، سماں، مہاجم براک

الله سورد. لا إله إلا الله. لا ستر، لا مطير! سرت.

...عادل هر لدام از subject ها میباشند. ای دختره من لستم.

نایاب... استی... لوری... A. اصل... ملکه... بابه... C. بیرللر

از محروم و توافق است. لامن توانیم استفاده نماییم و  $C = f(a)$  می‌شود.

ابن C را داده چه می کردیم  $\times \in C$

E.C

بله  $\leftarrow$  فضای A و فضای C من تونه متفاوت است با سه یا متفاوت نباشد

زمانی متفاوت نبین  $\text{لهم } \text{لله } \text{يعني}$

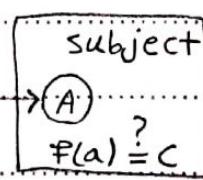
زمانی با هم برابر می‌باشند

نامن زمانی جزوی دخیره نموده

لئے در این حالته بده حون الـ sy stem بیرون فتد دسته مهام، مهام را  
هئی اطلاعات را داره و بدی دو میکنی هم این است لئے ادمیان اطلاعات ملیت را داره  
و ما این را همین فوایم هم F را به عنوان فراخ sy stem یعنی جزوی تقدیر  
من کنیم لئے ۲.۱ مقاوم بالا بروند

L  $\leftarrow$  خوب یعنی True است یا False

A L(a)



لئے فرض من کنیم قبل رحیمه

سده و اولن طریکه واسه

من لنه اینه که این Authentication

L را با استفاده از ه فراخوانی

من لنه  $\leftarrow$  توی این حالته سورد

را از مامن کنیم و توی sy stem برسی

من لنه لجه آیا  $f(a) = c$  با  $c$  دخیره

لوده یعنی هست یا نه و بر اساس نتیجه

بها باز خورد من ده

ک... ← برای ایجاد و تغییر A می بیم از کمن دیم له سلا بیل سوردی را برای اولین.

بلد ایجاد لئیم یا ایله روئ بزنامه اینزی سمه له بعد ازین مدن له روئی یعنی لردیم از ها بخواهد سورد را بعومن لئیم

← مابه عنوان فراخ system باید این هتا رالحاف لئیم

\* بطورت plain همان سوردی له طریقی ده را دخیره لئیم ← توی مفعه قبل نوشته

10... ← اربوی سبله طوبه A را بعون هیچ رمز نهاری یعنی سنه ← حلہ replay attack

یعنی ولدی داده تم افندی السن را لد ادمین است سورد من لنه و من بنتی السن با ادمین

و (a) L وارد سین Trudy میاد با این ادعا له ادمین است میاد (a) L له السن دی

داد را وارد من لنه ← حلہ replay attack

20... ند! سنه با سیم که این سامن له داره ارسان میسنه و دریا فست من لنه از عمر خدا موجودیت

خارجی ای این هیام بی هیام جدید است یا قبل ارسان سمه و هن داره نظر او میسنه

و این چیز جدیدی بناسه حلہ له لفته را من خوریم

\* ای F میا هس بآسه ← مزیت = ای system سفیم سد سورد ملدی ببوریت هایم

دستے مجاہم نیستے۔ ہیں مجاہم میں تو نہ ہو۔ این صورتے چل لئے ہیں دیلسٹری:

یعنی مجاہم system را سفیر کر دے۔ میں دونہ ہسپن۔ دخیرہ سہیں اون لیست

ڈاؤن بلیہ۔ لہ براں A۔ این ہسکہ د براں B۔ این ہسپن۔ بھیں صورتے وظاری کوئی لئے

این لہ بیلہ دیلسٹری درستے میں لئے۔ جیسا میں لئے ہیں کہا این پسوردی لہ لیست کر دیں

ہسپن کہدا با اون حسابی لہ لقیم بیلی میں سے ہے چلہ دیلسٹری نوع ایا چلہ دیلسٹری

گ ملاں ہے۔ وقتی لہ مجاہم ترنسٹر system را سفیر کنے۔ یعنی دستے میں داسٹے باسٹے ب

وچلہ دیلسٹری انلائیں ہے وقتی کہ مجاہم system را سفیر کر دے۔ دارہ ہیں تعامل و صرابی

کھیں کیمہ از تابع لادارہ است میں لئے یعنی دعاواہ چلہ دیلسٹری رالڈ اسٹے د دونہ دونہ

سردھا راست میں لئے لہ یسینہ کی صواب... True... است و دارد system میں کے

در این حالت یعنی موفق سدھے ہے۔ ایجاد موقیت و وقتی لہ ہے لہ سایں لئے با اون لہ

دخیرہ سہیں بیلی یسینہ

original unix ..... ← ۸.۶.۱.۱. اصلی سوردمون است.

۸.۸.۲. بست طراحت اصلی داریم ← یعنی ۷.۸.۱. است. اینجا طراحت هایی که می توانیم برای ۱۹۷۴ سسی بینی.

\* اینجا بد جز salt که تاماً هفتم است. یعنی طراحت های اصلی را می توانیم انخاب لفظی

← سی سوردم ۸.۶.۱.۱. اصلی است. له مقایی سوردم ۸.۷.۱. حلقه

مقایی سورد یا مقایی  $A \rightarrow 9.9.x^{14} \rightarrow$

10

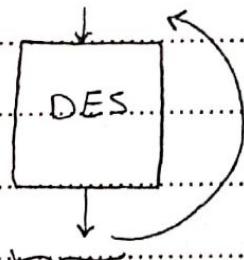
۸.۶.۱.۱. اصلی له ۷.۸.۱. است. ←  $8x7 = 56$

لے مقایی طبی دی DES ← سی اینجا برای.

دھیره سورد از سوردم بعنوان طبی.

استفاده می کنیم.

(۴۴ بست تاماً هفتم بسی ده) ۰۰۰ ۰۰۰ ←



۲۵ بار این تغییر میدهیم. بعد از آن

?

۲۵ دور این طراحت از الغایی ۴۴ تایی داریم + ۸.۶.۱.۱.

این طراحت بدهی داده می دیم. از این ۲۵ طراحت استفاده می کنیم برای این DES او خوبی که می فواد تغییرات

بله.

نکته → توی DES مقشیت expand E ( ) را متناظر با اون ۸.۶.۱.۱. ده اون اول.

DANIAL

DP

41

و اسے حرمہ ایک سستے میں لئتے ہوئے ...  $E \rightarrow$  Unix ...  $\leftarrow$  راتغیر سے دن ... = > پس باتا۔

طرالتر ... E. راتغیر دادیم

و اسے تامولفہ برائی سیستم ...  $\leftarrow$  otherway بالیں

A  $\rightarrow$  طرالتر اسلی

C  $\rightarrow$  (ستم ۱۳۰۰ تایی)

F  $\rightarrow$  DES  $\rightarrow$  F. ۹۹ جایلست  $\rightarrow$   $F \in F$  ...  $\therefore L \in F$  ۹۰

L  $\rightarrow$  توابع ... su

S  $\rightarrow$  password  $\leftarrow$  (برائی ایجاد و تغیر سیورڈ) ۱۵

اسسیب بندی میں ہائی طبقہ ملبوڑ

اسنان ہاتا ۸ سو روڈ میں تو نن حلقہ لئتے ہیں اور اس سیورڈ کے لئے لام است پس بسیست

از ۸ سو روڈ باید بلن  $\rightarrow$  کوئی این باعٹ کیسیجاں بیرون ہاں تو نسیست

پس بنی از اسسیب بندی میں طبقہ ملبوڑ  $\leftarrow$  تو نسیست سدن است

لے راھنماار  $\rightarrow$  الرمیں حوالہم لتو نسیم خود اون طبقہ عبور لتو نسیم بلہ ہمچیں چڑیا لتو نسیم

1.  $t : \underline{x} \rightarrow A$   
 جیزی لے ایسی طریقہ من نویسی پر  
 ملائیں تابع ترا صفت لئیم۔
2. اسے بندی کریں۔  
 سوڈردن سے جو اون موقع لے طبے۔ عبور را دار دیں لئیم وچے
3. اون موقع لے دارہ تویں سبلے ارسال من سہ من توں در یعنی ملک ریزد بالسے
4. ملک M.I.T.M. من نوعی از جملہ است۔ Man in the Browser
5. اور Trudy توکی میوریٹ ببر بیاد طریقہ من توں جملہ را انجام بدھ۔
6. اون نوع جملہ دیلیسٹری داریم۔ بیک لیسٹ از میسر دھا دیست کر دیم بچتیں لے جائیں من کسی اپنے اس بیسٹری دیست کر دیم حالابجہ اموریت من توں کسی جملہ کیم۔ اون نوع ایڈن افلائیں
7. و فتن کے کیک دیسٹری کردہ جیزی لے مور دھمن F و C است  
 ملائیں گوئی یعنی حسست میں افتادہ وہن داریم ریز من زنیں تاوارد گوئی سبیم
8. اون نوع ایڈن سے بچے جنمیں لئے اونے بچا جنمیں بچا جنمیں لئے سے بچا جنمیں داریم ایضاً دونہ دوں ہو اور دی لے تویں دیلیسٹری است را باہمیست من لئے وہ من بلیں
9. True یا False کہ داریم این است کہ جو تعدادی من توں بزرگ
10. والر بیسٹری سک ایسا طبے تابع لئے یعنی بعد زمان تا جیزی واپسی من داریم

16

• جملہ دلیل منی

• نوع ۱ → آنلائین → F و C

• لے برای اینلہ چلوی جملہ نوع ۱ بلیں سی سعی میں لسیم F و C را پہم لئیں ← جو بارہنے

• کردن غایلی کو داردیم ترسنے C را دیکھ رہا ہے میں لسیم و بالیساں F سعی میں لسیم اسر ہماں

• تقدیم کر دلی ہنوز سمع دسترسیں کو تونہ C را بخونہ ← ہس سعی میں لسیم محرمانگی

C را حقف لسیم

• نوع ۲ → آنلائین ← L

• لے برای اینلہ چلوی جملہ نوع ۲ بلیں لیں

• ← لیعنی بعد از اینلہ چند بار رہنے را زدیم یعنی بازہ رہانی مارانے ← Back off

• میں حادہ و بعد دوبارہ اجازہ میں دہ رہنے را وارد لسیم ← Back off بھیں ملورت

• است میلانہ بطورت نہایی باسہ ← یعنی مکام system کیسے بازہ رہانی بے انتہا X

• را در تقریبی لیں وہ بار بار طوبی تلاش میں کند X را بتوان میں دسترنہ ملا لے

۱۰. سن داریم <sup>۱۰</sup> و <sup>۱۰</sup> حین میں باری کے داری، دارہ بلاسٹ من لئے من سے۔ ← این طریقے میں

واسطہ میاجم ہز لیہ برسے تا اینلے لفیرفت بسے.....

۱۱. ← یعنی مرتب ارتباط را قطع لئیم و این باعکسی من سے ادن Disconnection..... ← ۱۱.

چلے کور دیلے واسطہ میاجم لفیرفت

۱۲. ← میں میں طریقہ میں دا ستم کے این عیر فعال سے و نیاز بیٹھا مامور Disabling..... ← ۱۲.

۱۳. امنیت داریم کے این فعال لئے و فرمسن با کے Disconnection. توی مامور امنیتی است.....

لے ای خدا مامور امنیتی نیاز نیست

۱۴. ← زفارہ میاجم را تقلیل لئیم ← خنی از سکریٹ ہائی بزرگ دین طریقہ Jailing..... ← ۱۴.

من لست بامراحت hakey pat.....

۱۵. تا لستن میں خود جم طریقہ

لے یعنی میاجم توی این system من جزو و مجموعہ توی.....

۱۶. ← اسی بندیری طبیعہ میں دارند hakey pot.....

ادامہ اسی بندیری طبیعہ میں دارند ←

۱۷. اسلام داریم ← ۱۔ بخا مر سیاری سادہ ← حد سی اسادہ میں سادہ

۱۸. ← یعنی میں سوردی وال تقابی لئے تحدی سی سادہ است

DANIAL

۲۰- از نیازمندی عبور نوی حیند system استفاده من کنند.

۲۱- نقویین نظر دن طبیعه عبور

راهنما ر مقابله با نایابی بالاین:

راهنما اسئال اول  $\leftarrow$  برای نیازمندی محدودیت انتساب طبیعه عبور را برداشند و

(۱۵) آنرا  $\leftarrow$  انتساب صبور نظر فی بودند

۲۲- از ۳۲۸۹ طبیعه عبور ما  $\leftarrow$

۳۲۸۹  $\leftarrow$  طبیعه عبور ما  $\leftarrow$  ۷۲ طبیعه  $\leftarrow$  ۲

$\leftarrow$  ۳  $\leftarrow$  ۴۹۴

$\leftarrow$  طبیعه  $\leftarrow$  رالترم فرمود

این سیوردهای خوبی لست

ملئے راهنمایس  $\leftarrow$  proactive password selection  $\leftarrow$  مولفه ک ملئے

سی باید ک رایج حوری صراحت بلنیم له قوانین انتساب طبیعه عبور را بصورت احیانی

توس بذریم:

همین حیزابی ل داسطه عبور تعیین من کنیم اینه ل حداقل مول طبیعه عبور صیدر

باشه  $\leftarrow$   $\frac{p}{\sim} \rightarrow$  TG

سؤال امتحانی

قابل اول  $\leftarrow$

P. ← احتمال موافقیت مهاصب در بازدیدمان مسخن.

۷. → تعداد واحد های زمانی ل. حدس طی. عبور در آن انتقام من سرگرد

۶- تعداد حدس‌های هم‌دریل و اندزمانی.

N ← بقداد طماست علوں مکلن

• عَالِيَّونَ د. و. م.  $\rightarrow$  اذ هر دسته طارالمت. انتخابی. حداقل بیس طاراللّم  $\rightarrow$  یعنی اذ هر دسته.

طَارَ الْمَرْءُ بِنَدِ طَارَ الْمَرْءُ أَصْبَأَ لَوْهٍ سَعْوَدَ بِنَدِ اَرْبَيْ

مانون سوم → همان موری که مهاجم من تونیس دیلسنری اماده شد. بالله مسامح... .

من بتوانم بی دیلیسنسن آماده لشیم و اجازه دادیم به طایفه اندیوی اولن دیلیسنسن ...

طهہ. علورین. رائیتھا بے لئے. ← طہہ. علور دد. دیلسٹری. سا۔ سد

بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِيْمِ

20.....

• pass.wor.d → Arash.۱۲۳ ..... ← این نیم تونه بلطفه

مانون...لتخیم...← هبستنی...با...pass...word...aging...← برای...تعویض...نامه...دن...طیه...عبور...<sup>25</sup>

را هدایت مون... password... است... یعنی... رمزگشایی... را تعیین کنیم... له طالب میور...

سنه طبیعه عبوریکن... را تعیین بده... نکته... سورد چهاری قبیل... را دقت کنید من لئنیه له براي...

و سورد جدید از آنها استفاده نکن... لئن توانه بی سورد... یا ۴۵ با سورد قبلی  
را در قیمه لذ این دست مرلح system...  
است که حقدر سختی باشد.

الله هم سورد ها را دقت کنید  
لئنی چی؟

همانی از اندروون ←

سورد از طرالله های الغایبین... ۹۶ تایی... انفایب من سنه

۱۵ هماجم در هر یافته... ۴۰ حدس من رته

من حواهیم احتیال حدس هونق دری باره... ۴۵... ۳۳... روزه... ۱... باسک

حداقل مول password... چیست؟ ←  $s = ?$

$$N > \frac{TG}{P} = \frac{(340 \times 24 \times 90 \times 40) \times 10^4}{0.01} = 9,31 \times 10^{11}$$

ک... ← حداقل مول

$$\rightarrow \sum_{i=1}^{99} s^i \geq N \rightarrow s \geq 4$$

Saltig... ← لَسْتَ تَعَاذُنِي بِطَهَّ عَبُورٍ افْتَأْمَنْ مِنْ لَنْيِمْ

لَهُ طَرِيرًا زِيلًا طَهَّ عَبُورٌ تَوْيِنْ ... system... هَامِنْ مُخْلِفٌ اسْتَقَادَهُ مِنْ لَنْهُ وَبِرَاهِي إِيْلَهَ اهْنِيْتِ.

مَا بِهِ اندَانَهُ اونْ صَنْعِيْنَ تَرِيْنَهُ لَهُمْ سَهَّ مِيَاهِمْ تَالِكَ افْتَأْمَنْ مِنْ لَنْيِمْ ← مِلَامِنْ دَوْنِيْمْ طَارِيرَه

لَوْنِ حِينَتَاهَا سَامَانَهُ سَتَ نَامِمْ لَرِدَهُ وَيَسِنْ ازَاهِنْ سَامَانَهُهَا هَادِهَ سَدَهُ وَالْرَّدَاهِنْ حَالَتْ هَهِنْ مُورِي

لَسْلُورِدْ رَادِقَيْرِه لَرِدَهُ بَوْدِيْرْ وَهِنَّهُ حِيزْ تَعَاذُنِي بِهِسْ افْتَأْمَنْ لَرِدَهُ بَاسِيْرْ وَهَقَنْ لَهُ اونْ سَامَانَهُ

هَهِنْ سَهَّ لَسْلُورِدْهَا بَغَيْرِهِ سَهَّ مَاهِيْرْ دَاهِيْرْ وَهِنَّهُ ازَاهِنْ دَدَ سَامَانَهُهَايِيْ دَيلِرْ اسْتَقَادَهُ لَهُ

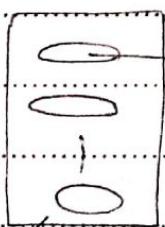
← سِنْ بِرَاهِيْ دَفعَ مَسْلَلَنْ سَيْلَهُ لَسْتَهُ تَعَاذُنِي بِهِ طَهَّ عَبُورٍ افْتَأْمَنْ مِنْ لَنْيِمْ لَهُ لَفَسْ سَكَ

رَادَادَهُ

دَكَ رَاعِيْهُ لَغَيْرِهِ سَهَّ غَاسِ دَحِيمَهُ مِنْ لَنْيِمْ ← هَسْ سَكَ رَانَهُهِنْ دَارِيْهُ → نَلَهَهُ

هَدَفَسْ ← طَاهِيْهِمْ رَاسْتَهُهِنْ لَهُنَّهُ يَعْنِيْ الرَّهَاهِيْمْ مَوْنَقْ سَهَّيْلَهُ سَامَانَهُاهِنْ رَابِسَلَهُ

نَلَونَهُ اونْ اَهْلَهُعَاتَهُ رَابِهَعَزَانْ دَيلِسْتَهُ مِنْ اسْتَقَادَهُ لَنْهُ وَبَقِيَهُ حَابَهَا اَرْسَنْ اسْتَقَادَهُ لَنْهُ ...  
Salt...



اَهْرَهَيَادَهُ Salt لَهُرَاهِنْ دَيلِسْتَهُ مِنْ

بَذَهِيْهُمْ آيَاهَنْ هَهِرَهُ طَاهِيْهِمْ سَخَتَهُهِسْمُ؟ بَلَهُ

نَلَهَهُ ← بَهَاهِيْهِ هَهَ طَارِيرَهُ Salt دَارِيْهُ

وَبِلَهْ بَعْدَ اِدَ طَرِيرَى لَهْ دَارِيْمْ تَاهْ كَبِيْرَى مَالِهِ مَنْ لَهْ

...original\_unix... اد.

۸. طرالتر اسلن داست لوه طید DES برامون آماده من کرد

DES<sub>a</sub>(.....)

طائی کو تویی DES انعام می ده اینکو اون قسم است expand لتوس نسیار

۲۰ دلستیم. و من لعنت که لدایم می‌انداشتم. ۲۱ سیا تکر اور لسنه تبا بیاد توی این ۴۸ سی روسیا

النقاوٰت ساٹ

۹۰۹۴... است DES... را توجه به E... → حاصلست های ... داریم. حاصلست داریم F →

→ سـ salt ... اسـ استـ لـ بوـئـيـ ۲ـ بـاـطـ رـالـمـ دـقـمـ هـمـ لـردـ

ملئے۔ بعد از ۲۵ تاریخی لہجتے۔ ضروری نہیں رائے دینے میں لئے یعنی انتظامی امور

راہنمائی تو یعنی نظردن کا عبور password... است... وہ... aging

وہ... aging... password... رائے دینے کا باہمی نہیں لئے یعنی رائے دینے کا حکم فراریں دیں:

ایسے۔ اتفاق یا بیسا۔ فدادیں۔ داسنے باسیں۔ ملا جائے سہ۔ وہ دلیں این اتفاق انہما۔

حوالسن سیورد۔ رائے دینے کا

سیں نہیں۔ سیورد۔ رائے دینے کا

یا

لے۔ ۲۔ براسان۔ یا۔ فدا۔ خاص من

ملئے۔ مو معنی لہ۔ بعثت ابر میں حوابیں بلیں سیورد۔ رائے دینے کا لہ۔ ہستے۔ بوئی ہیں

اصلام۔ لرد نسہ۔ چون۔ الرہمن۔ موقع لہ۔ طبیر۔ وارد۔ سد۔ بلیں سیورد۔ ہستے۔ مدققی سد۔ طبیر۔

احمد۔ ایسا۔ سیورد۔ صنعت۔ اتفاق۔ میں کہ۔ در۔ این۔ مو معنی۔

ملئے۔ طا۔ اسر۔ aging... password... اتفاق۔ لرد۔ بلیں۔ بہ۔ سیسی۔ وون۔ طبیر۔ سیزدیون

کرم میں اللہ

17

نَلَهٌ ← بَوْيٌ فَرِهُولٌ اندِرسون بَلَسْرِنٌ فَرِصْبِيَاْتٌ دَالِيمٌ ازْجَلَهٌ فَرِمَنْ مِنْ لَسْبِرٌ طَابِيرْ هَبِرْدَ

۵۰ ندوم داده طبق عبور اختیاب می‌کند. یعنی مثلاً اگر از این فرمول ۶ بدست اورده باشد

• مجموعه سیوان صراحی system... مدت تابعیز بسیار اختلافی داشته باشند.

ط. والقر. باسنه ← سـن فـرضـنـيـاـسـ اـيـهـ لـهـ طـارـبـرـدـارـهـ دـنـدـمـ طـبـ عـورـ رـاـلـتـخـاـسـ بـيـ لـهـ

ملحق دویسی ایضاً معرفت نمی‌شود.

\* سهل آیه دال ..... password aging ..... این است. لام هم طبق عبور را پلیبا راستفاده ننماییم

لیز بیو مخفی استفاده از این پسورد می‌تواند وقتی از

لے با ط ری بر سیند بودن مسلسلی ندارد طبقه عبور این طبقه معتبر  
گذار ناچار است

\* میتا روک سیاحدہ سعائی دا رہ :

۲۰ ای. بی. لسست. انلسن ملست. از طبق عوره‌های اصرفت دا. سه با سیم

ملاس طه عور ..... Arash ۱۴۳ سایم ملاس سایم

..... ۲۵ و آن طبقه معلوم سست. لتفهم میباشد. part a ۹.VII ۸۰ و ..... شهر بارگاه با اون طبقه معتبر وارد میشود.

Subject:

page: ( )

Year : Month : Day : ( )

اون طبقه عبر ناچیز بود سه و نیوی ارتباط مالک باریم یعنی است یعنی

حضرت احمد؟ اند چیزی لست داشته باشد اینجا ماجد است سه

5 حسین استانی اولاده ← شاهزاده ای ← شفیع ترسب

۲ ← همانکه ارتباط برقراری نمایم طبقه عبور را بروز کنیم (او افسوسانی مبتدا و  
طبقه عبور) ۱۰

اسناس ← انتخاب طبقه عبور ضعیفی ← (این همراه)

۱۵ ← ال ارتباط مفعه استوی طبقه بنشیم ← مجموع اسلام صورت بدلیله  
بلال الله عن

۳ ← از باتابع بی مرغ و استفاده از میل همس ماناسن ها

۴ ← ( دنباله ای از طبقه عبور بتن بر پیشتابع بی مرغ و )

۲۰ ← این شبیه بودایی قلب بزرگی دارد

۲۵ → LAMPART عس

الس طبقه عبور خودس را به عنوان Initial seed انتخاب می کند

Alice → K: initial seed

P4CO طبقه عبور

Alice ← → Bob  $h, h^r$  اسن و باب برو توافق من استناراز جو تابع های معرفه وی

اسناده لش و همین موردنی با عدد صیغه  $h$

Alice:  $K_1 = h(K)$  این اور آسن و ماسن من لند

$K_r = h(K_1) = h(h(K)) = h^r(K)$  یعنی بار از K حس رفته

$$K_n = h^n(K)$$

$$pw_0 = K_n = h^n(K)$$

$$pw_1 = K_{n-1} = h^{n-1}(K)$$

$$pw_i = K_{n-i} = h^{n-i}(K)$$

از K پس دینالای انطباقات بور ایجاد نهاد

Alice ←  $h, n$  → Bob  $h^n(K)$  معداً موافق توافق

Counter

i	user			password
1		;	;	;
Alice	n	i	w:a	$h^n(K)$
		!	!	!

این جدول باب اسن

25

Subject:

Year: Month: Day: ۲۱

page: ( )

داره این وسیع ارتباط را سودمند نماید Trudy

طی بررسی نامین ارتباط اینارو من فرسته

$$i, pw_i = h^{n-i}(K)$$

تویی نامین ارتباط باب

حالات باب حیز زایی نبایش سید میباشد

اینارو دخیره میکند

i Alice ? (?)

اینارو لیس فرستاده

$$(pw_i) ? h(pw_{i-1}) ??$$

10

$i+1$  counter الگویی هادرس بود  $pw_{i-1} = h(pw_i)$

مثال ص ۵۹

و سورد پسر که  $pw_i$  = < یعنی این کتاب بولن میشون

واسه ارتباط بعدي

\* Trudy:  $pw_i = h^{n-i}(K) \rightarrow$  خواهد پرسید بیاره  $pw_{i+1}$

لایز سودمند ننماید

$$h^{n-(i+1)}(K) - h^{n-i-1}(K)$$

20

ایام تونه از  $pw_{i+1}$  سربر سر؟ خیر، چون تابع مایل اصراف بود

تلخ سی سی بیشتری من تونه سورد  $pw_{i+1}$  سر را بسی بیاره از بیرون و بر عاس همسایه مانلسن

بله

25

اسنخاچهی replay attack داری یعنی آسیس را دستور لانے تو نه سامدی-Trudy

لنه ومه وقت خواست خودش فرسته

نله ← اسنخاچهی نسخه اونسان حمله تازی سام باس

نله ← الارون طرد عوری اون طاری را در بین عنوان initial seed استفاده من لنه خلی

ساده باس همچو این تئرنری دیلیسٹری بزرگ ایجاد لنه و کهاراحدس برخواز هر کدام

از کهاراحدس دنباله ای ایجاد لنه و وقتی طرد را در هر قسم ای فرسته الربا (K) <sup>10</sup>

بنی اس حس من ننه طرد K بوده <sup>\*</sup> initial seed من ننه طرد صنعتی استخاب بس

نسل دیلیسٹری آنرا داری متن طرد حاسابتی اون مراج براید از قبل انجام بده <sup>15</sup>

اسنخاچهی بسته اس

نله ← سب ایجاد همچو کو اس جو K را استخاب بی که لنه لجه بالا را در بس <sup>\*</sup>

یعنی اسیں باید K را استخاب لنه او از دیلیسٹری بناس <sup>20</sup>

Subject:

Year : Month : Day : ( )

page: ( )

بُو طَبَرْ بَابِرْ اَعْتَادَ لَدَرْ ← zero Trust

لَهُ اَنْ اَنْفَادِيْ لَوْتَى نَزَقِيْ اَمْلَقِيْ اَمْسِيْ سَابِقِيْ اَذْمَعِيْنَ تَرِيْنَ حَلَّةَ تَحْمِيرِ اَسْتَ

سَبِّ بَعْدِيْلَوْمِ اَزْ تَحْمِيرِ هَالِيْنِ تَرِيْنِ اَعْتَادَ لَسِيْ ← مَوْلَاتَوْيِيْنِ System 5

صَعِيْنَ تَرِيْنَ حَلَّةَ طَبَرِ اَسْتَ

نَلَّهَ ← بَوْسِيْنِ system هَالِيْ اَهِ اَزْ اَصْمَالِيْسِ بَشْنِ بَرَطْبَرْ بُورِرِ system هَالِيْ اَخْرِ اَصْمَالِيْسِ

10

صَعِيْنَاهِمِيْنِ لَنِ

نَلَّهَ ← system هَالِيْ اَهِ اَزْ اَصْمَالِيْسِ قَوْيِيْ system هَالِيْ خَسَّتَنِ اَجْبَتِيْ بَشْنِ بَرَطْبَرِ

15

challenge response

لَوْيِيْ اَهِ اَنْ اَصْمَالِيْسِ مَوْيِيْ طَبِرِيْ بَحِيْ اَيْلَهِ لَانْ جَوْدَسِ رَبِّيْمِ فَادِيلِهِ اَرَادَهِ لَهِ بَادِ

صَفَّا سُونِ مَنِ دَهَلَ اَنِيْنِ رَازِ اَطَاهِرِهِ مَنِ الْرَّايْجِ الْرَّمَاهِيْنِ K مَنِ دَاهِيْرِ K رَا رَاهِهِ

20

Alice Bob ← دَهِيْرِ بَالْمَدْرَفِ مَنِ السُّونِ مَنِ دَهِيْرِ اَزِ K اَطَاهِرِهِ K مَنِ دَاهِيْرِ K مَنِ دَاهِيْرِ

25

بیتی برای زیر آفاین  $\leftarrow$  challenge response \*

بیتی این از ملائم (مختصر)  $\leftarrow$

Alice Authentication  $\rightarrow$  Bob  
 $\leftarrow$  challenge

$MACK(\text{challenge})$

مسنون

↓

این کسی را نمی‌داند که از این کس و این کتاب استفاده می‌کند

آنچه بقیه طبق امن بتوافق هم فرستید می‌باشد  $\leftarrow$  جو حس را

جای این جای خود را این سیستم به ازانته اون  $\leftarrow$  این سیستم را داریم

استفاده از لذت  $\leftarrow$  هنچ تصور  $\leftarrow$  Trudy من تونه طلب را بسیاره و خود شر جای این

جا بهتر

$K \rightarrow \dots \rightarrow h^{n-i}(K) \rightarrow \dots \rightarrow h^n(K)$   $\leftarrow$  پادخواری

$\leftarrow pw_i \leftarrow \dots \leftarrow pw_0$

$$pw_0 = h^n(K)$$

$$pw_i = h^{n-i}(K)$$

$$\frac{1}{pw_i} = h^{n-i}(K)$$

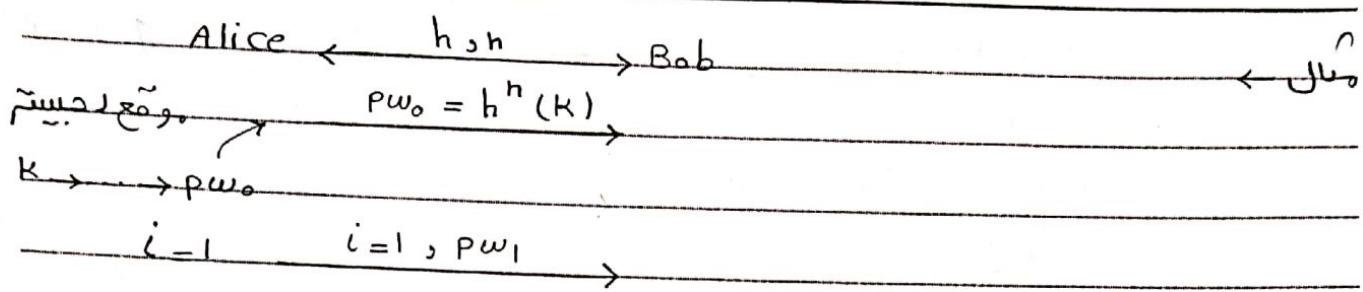
20

25

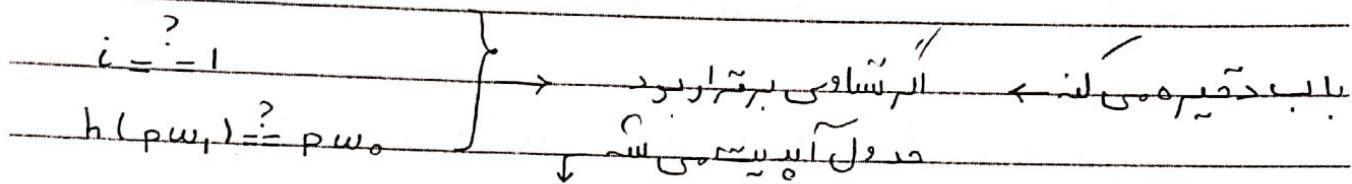
Subject:

Year : Month : Day : ( )

page : ( )



5

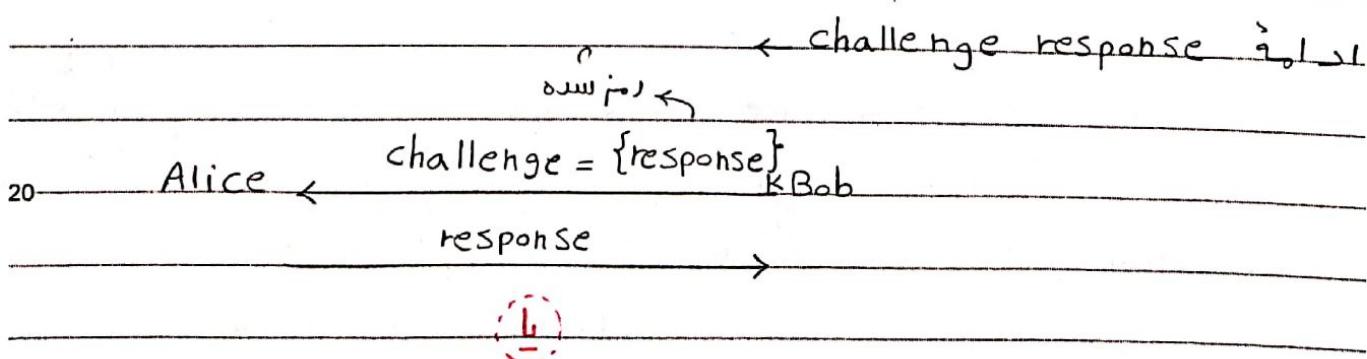


10

Alice	$h,h$	$r$	$p_{w_1}$
	:	:	:

15

18



25

Alice  $\xleftarrow{\text{challenge}}$  Bob

$\text{response} = \{\text{challenge}\}_K$

1

در درس

Alice Authentication → Bob

challenge ←

$$MAC_K(\text{challenge}) = \{\text{challenge}\}_K$$

(یا)

از پی ۱ ایجاد می شود

Trudy ← اسلاسیس می خواهد چند سوالی ایجاد نماید

الرخود شرمنی ایجاد نماید تا باید طبق رابطه این را اثبات کند

امنیت برای ایس بواندازه اون الگوریتم را زی استفاده می کند

اگر بخواهد خود شرمنی باید جایز نباشد احراز اصلیت باید تایید شود ←

و احراز اصلیت ۲ مرحله دارد

برای حمله replay attack باید نشان دهد که یک تأثیر نداشت ← سی ار ناری

سلام مسخن بنامه های replay را من خوبیم

1 → nonce : number used once ← تأثیر نداشت

challenge ← اینها این چیزی که بوداریم بعنوان

ارسال می کنیم و قدری باشند اینها یکبار این استفاده شده و برای

قابل استین سیستم Trudy

2 → Time stamp

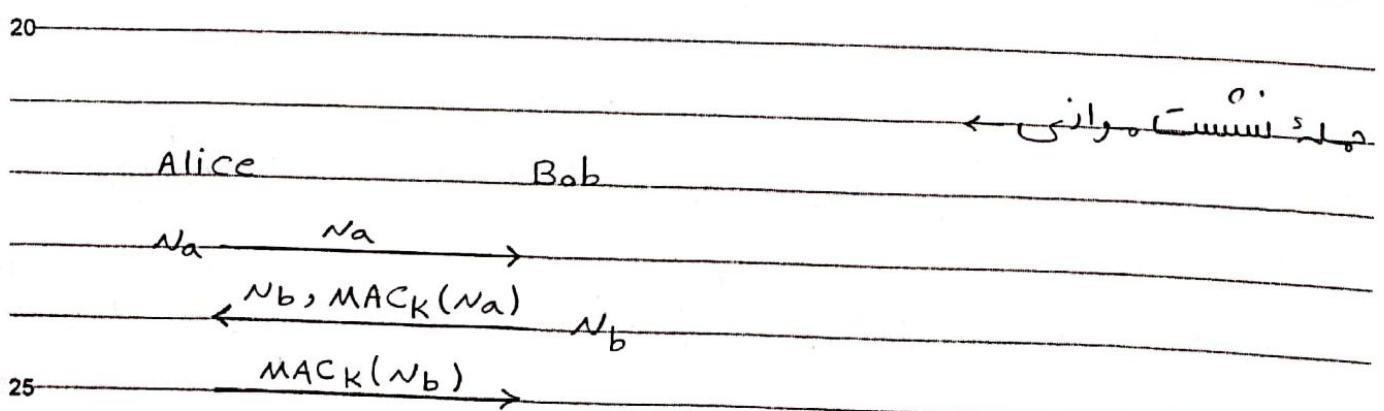
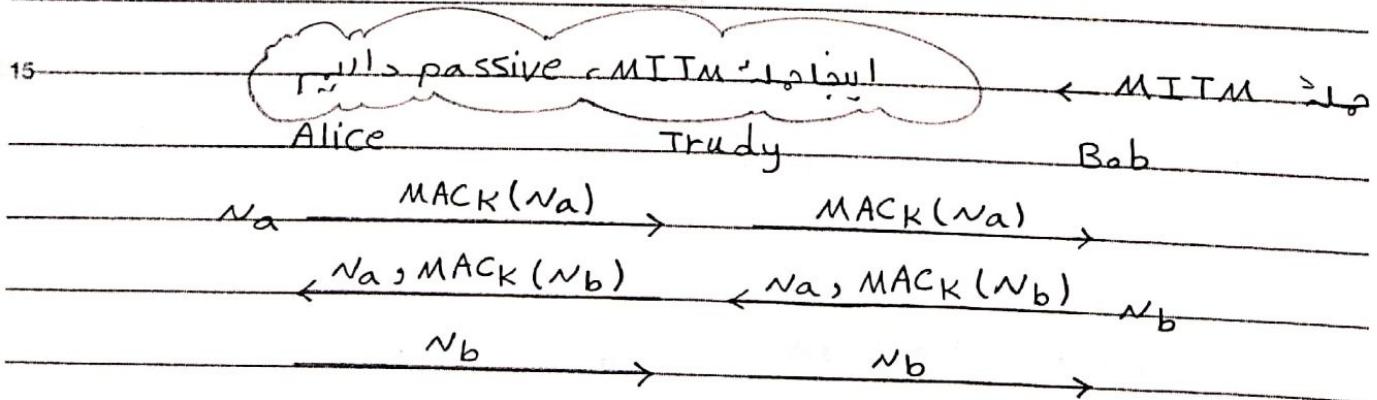
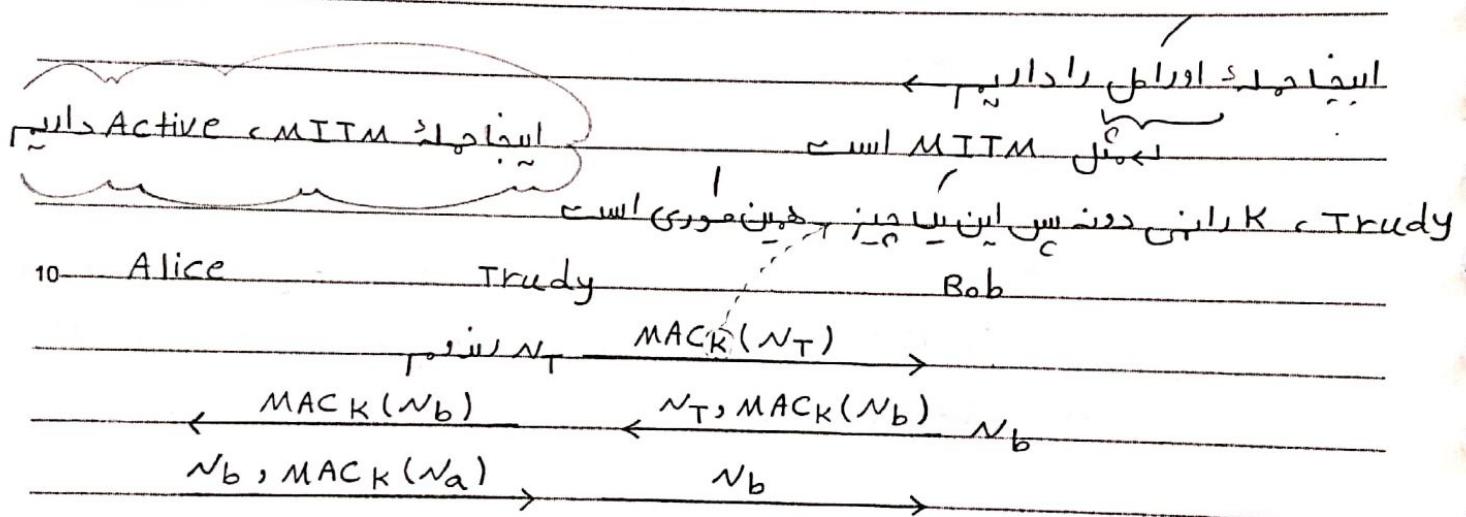
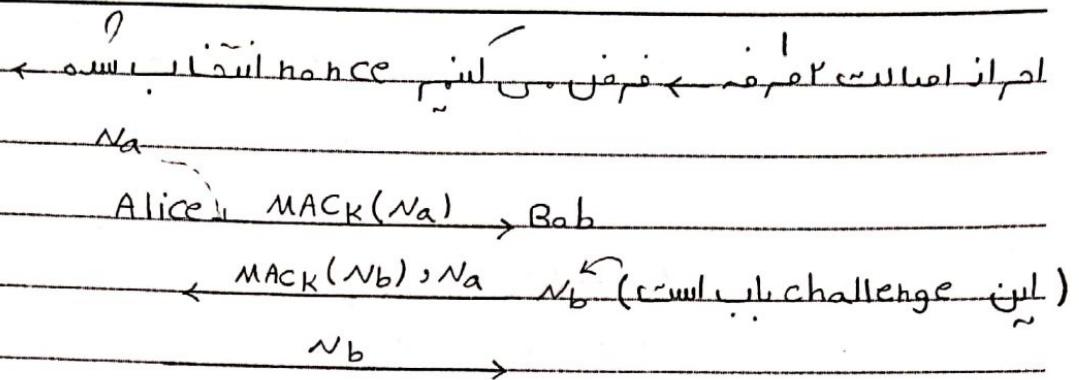
25

3 → counter

Subject:

Year: Month: Day: ( )

page: ( )



Alice

Attacker

$n_a$

$n_a$

$n_a' = n_b$

$MACK(n_a), n_a'$

$MACK(n_a), n_a'$

$MACK(n_a')$

$MACK(n_a')$

الرسالة مسورة بـ  $n_a$   
الرسالة مسورة بـ  $n_b$

Alice

Bob

$AIB|n_a$

$n_a$

رسالة من Alice و مت خواست

$n_b, MACK(BIA|n_a|n_b)$

$MACK(A|n_b)$

باب اتصال بـ Bob، ولكن هـ

رسالة من Alice

19

$\bar{n}_i \rightarrow \{M\}_K = MACK(M)$

Alice

$n_a$

Bob

$\{BIA|n_a|n_b\}_K, n_b$

$\{A|n_b\}_K$

\*

ردود فعل

20

لین \* جمهوری جلوی چه اور اطلاع را من لیم؟ توی \* حالت فاس اس س و ردیف رمز response

سند اس س ولی توی چه اور اطلاع حالت امنیتی نبود و response رمز لسا میس بود

25

توی حمله اور اطلاع Trudy بناز بخطی نداشت و من امد پابیک رمز که ردیف رمز

Subject:

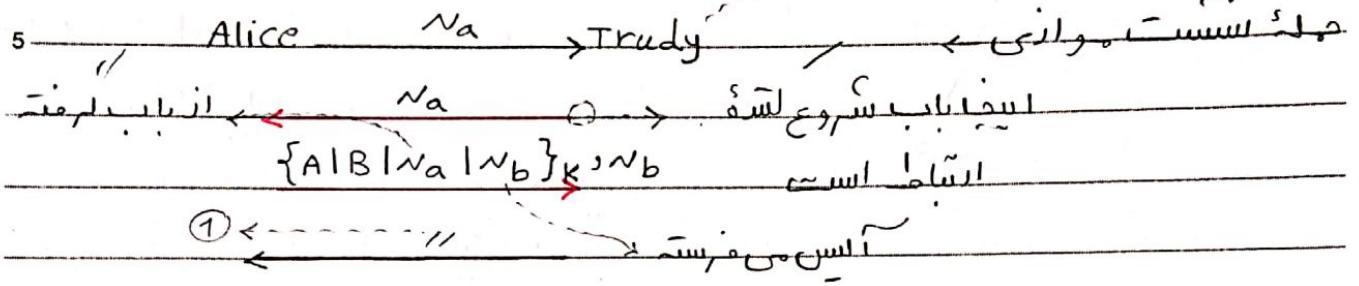
Year: Month: Day: ( )

page: ( )

لیکن تویی مشترک داریم، سه مادر، پایامبر، پیغمبر اسلام. با این هایی مخاطب از هم

افتخار خواهد بود.

Bob



لین \* حکمی جلوی مخاطب داشت. واری را من لیرد؟ حق؟ تویی قسمت ۱) باشید

$\{BIA|Na|Nb\}_K$  را داشته باشید. ولی تویی مخاطب داشت. اینجا بالا سو

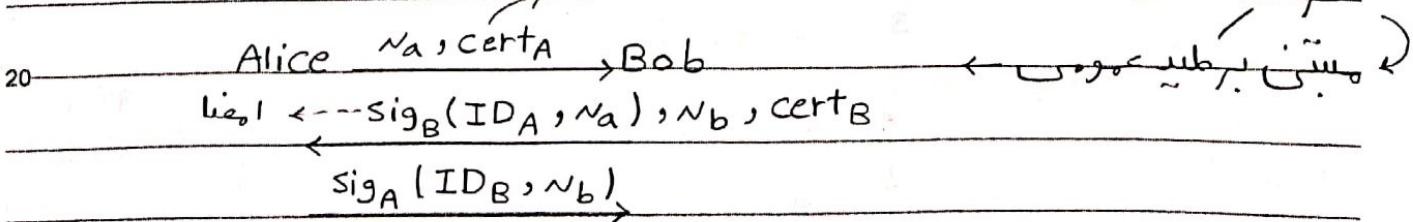
داریم و آلسین می خواست. این درست است.

تویی قسمت ۲) را داشت. سه مرندس

لین چوتھا \* با افتخار خودن پایامبر هایی مخاطب جلوی مخاطب داشت. اور این و نیز

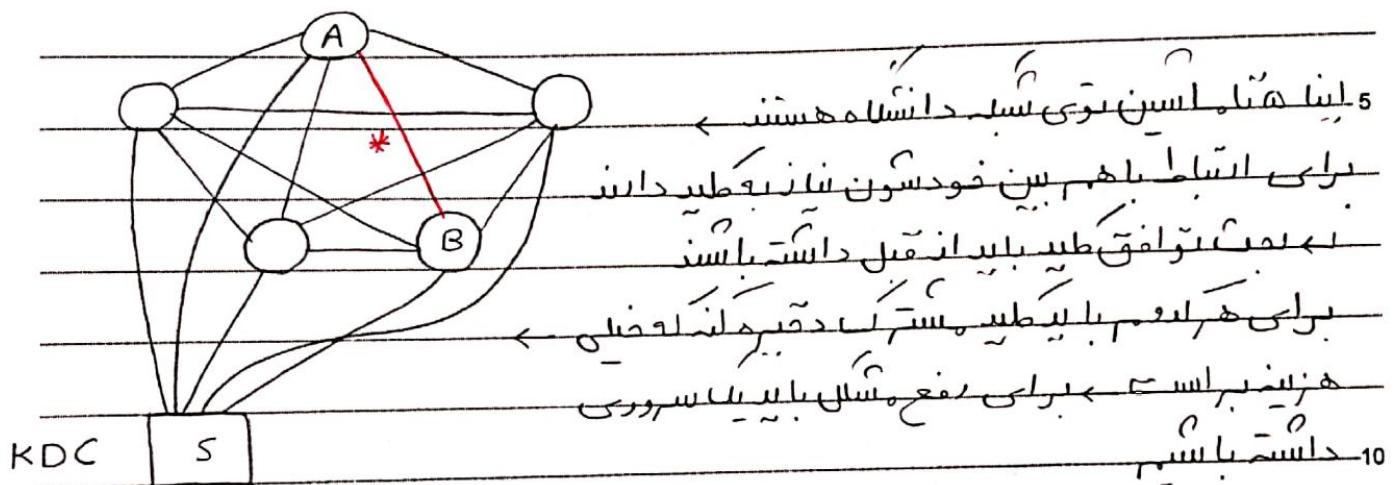
واری را من لیرد.

certificate



25

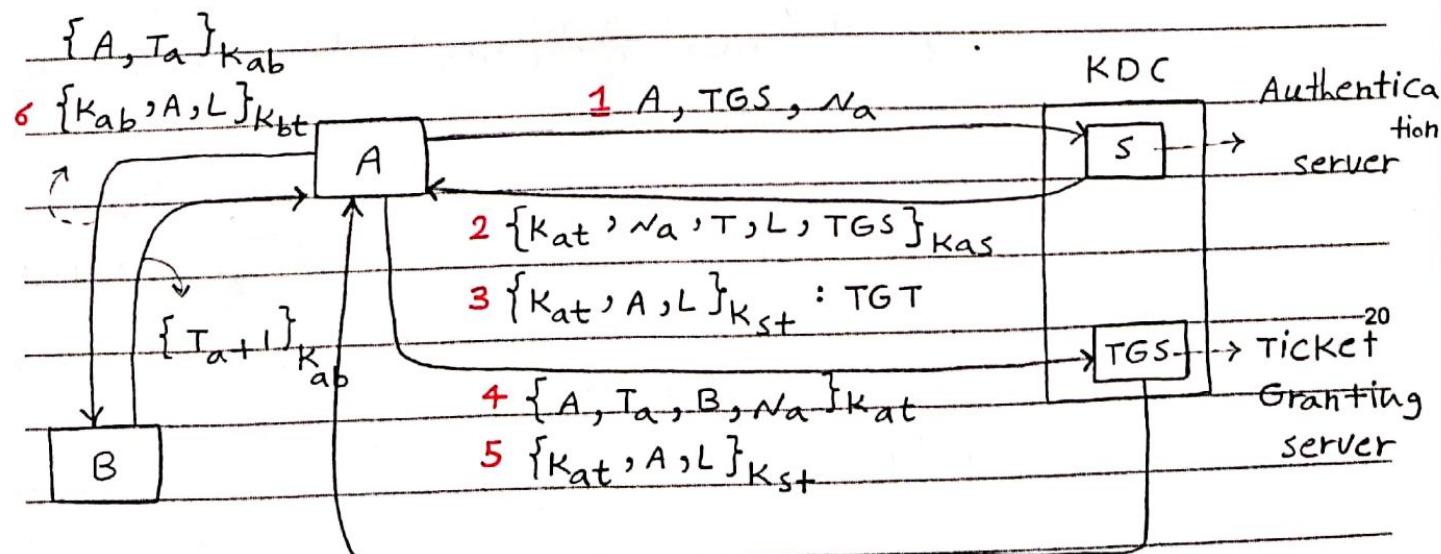
ویرایش اول  
برام از اطلاعاتی برخواهد که درین دسترسی را داشته باشد  
Auditing & Authorization



Key distribution center

این بوجاطبی داده و اس انتها \* یعنی  
ده ایس ایس، A, B تهیی طبی داده

اینجا طبی توان استفاده من لازم



Subject:

Year : Month : Day : ( )

page: ( )

نحوی :

TGS , S ← داریم server تیک بوتل برگوس  
 Authorization ایجنا ← → Authentication ایجنا مس

5

الس من خود با درسته ماسو و ناچ مالی اس اس ← 1  
 من خود شدیتی هر کس ایش بعید باب طرلنہ

Time stamp = T | TGS = طبیعتی ایس و KAT ← 2

10

ک، A و رزیں لنهان حا طبیعتی است کر = Kas | Time stamp = T ←

A بن تونہ ایزبانس لنه ← 3  
 KAT = باین رمزیں اردن |

TGT یعنی تیک اس کو صدی بوج TGS و ایش تیک هائی دیلیمی لیمی ← 4

A جل Time stamp =  $T_A$  ← 4

TGS اول ایزبانس لنه تابو 4 برس بعین KAT دار و بادھس 4 رابانی لنه ← 5

20

از این فریم و ایس توک طرفی توسی کام کام ایمان ایس اس اس ←

توک این باب مطمئن سیمی ایس تیک TGS ایش مجوز دسترسی ایس رفتیم ← 6

25

کو توک زیر بایس ایس اخ باب ←

page: ( )

Subject: \_\_\_\_\_  
Year: \_\_\_\_\_ Month: \_\_\_\_\_ Day: ( )

نکته ← بالاستفاده از این تبلیغاتی لامپ دیوبوطران بعد از ترنی دستال اشیاء

جملاتی لتفاق افتادن تبلیغاتی بوده اس س

5

10

15

20

25

20

اچ ان ایکالر با استفاده از Biometric قدرتمندی دارد

5 \* قدرتمندی رنگ های ابر نانست یا Finger print

بصورت انسانی optical

10 دستگاه های آنست استفاده از دستگاه های الکترونیک است اتفاقات بارهای الکترونیک

حلقه های ابر نانست را جاسوسی کنند

دستگاه های ابر نانست و این را برای این برای این

15  Approximation matching از graph matching algorithm

استفاده از اثبات ایمنی با این است

20 برای Voice استفاده از لیز:

(independent) این مستقل اس

verbal info verification این speaker verification

25 دستگاه های مخصوص این است

(dependent) این دستگاه است speaker این به

Speaker's voice characteristics این دستگاه است Speaker recognition

30 این دستگاه دارد این دستگاه دارد این دستگاه دارد

PAYCO این دستگاه دارد این دستگاه دارد

یعنی درین های مصالح ادن سنتل را در میاره

3 Iris (عینی) ← عینی هر لمس اللوی خاصی دارم که این اللو را برمی دارند

Eyes

5 Retina (سلی) ← این های خونی آنست جسم است

لکله = ایست سبلیه بود است ← عورلای تویی جاهای خیلی ایشی از این می باشد

4 Face ← زاویه های صورت را از ازانه بیری می کشد

10 5 Key strokes ← الکترونیک هر اس تاپ می کند

لکه بصری است ایشان با داینامیک تونه بیس لکه ← یعنی این اللو را بجهوی درس بیارن لکه یا است ایشان است یا

15 یعنی بلامتنی را برو → داینامیک

اطبیعت دن دن ان

تاسیک ان ← این اللو ایزود بیار و از این استفاده میکنیں خود طبیعت دارد طارو

دقیقت امن ده

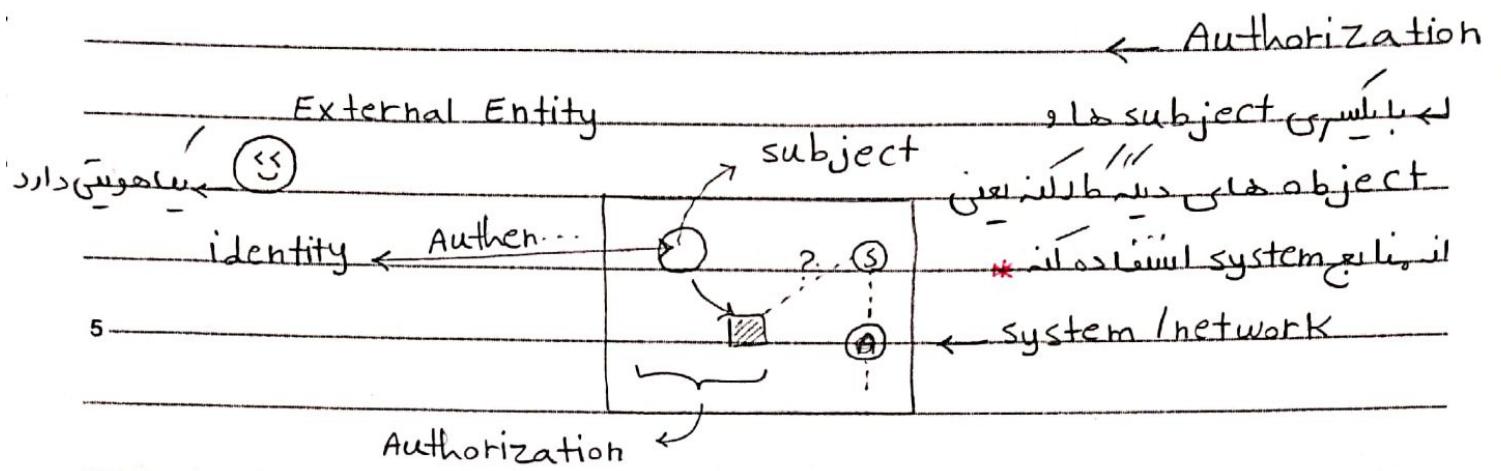
20 Key strokes براکی است فراج سردهم استفاده می کشد از

لکه ← این Biometric ها را در لذاری بوس دیگر استفاده می کنیم یعنی بصریست از ای

25 از این استفاده کنیم دون خود سرن بعتنای این نیست

replay attack

PAYCO



\* بالون خوبی تویی Authentication لیکن system

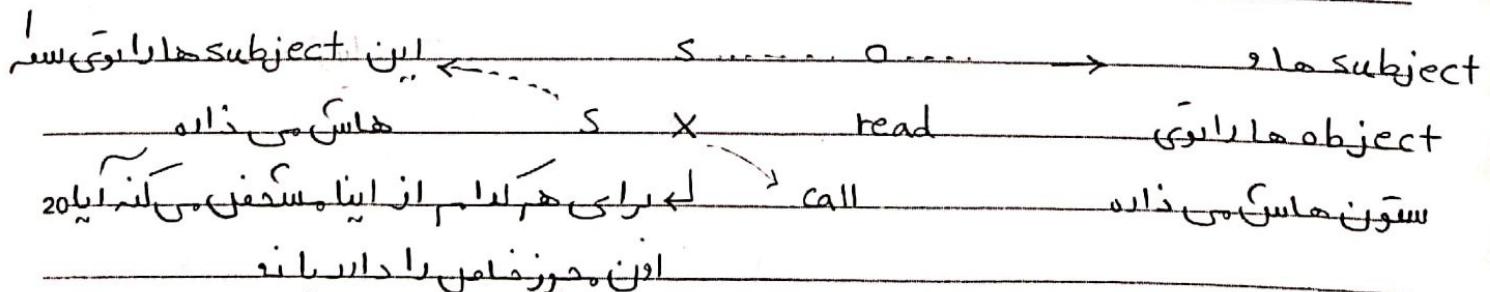
این باید یه ماتریس باشد اینکه subject و object را که همچوں منابع

امور داشتند از آنها برای وصول دسترسی داشتند.

لینک ماتریسی Civil Authorization

15-

اساس خوبی از ماتریسی داریم از Access control



25-

او نفسی فعال ندارد

$a[s, o] \in R$   $\rightarrow$  صور

ج

file 1 file 2 process1 process2

process1 r/w/lawnh r r/w/x/lawnh w 5

process2 append r/lawnh r r/w/x/lawnh

نحوه بالا استفاده از access control matrix باشد این سیستم را عینک نامی نماییم

10

حق خواهی دارند این اسیستم به این نامی باشید Authorization

نحوه درون خارجی درون خارجی system و system ill باشد این متن معتبر است

نحوه درون خارجی درون خارجی object و subject باشد این معتبر است

15

حق خواهی دارند این اسیستم را درون خواهی نماییم

w r d ایجاد  $\leftarrow$  r w "

20

sub dir. دسترسی به فایل ها و  $\leftarrow$  r x w

دیافت سیستم  $\leftarrow$  process و حق  $\leftarrow$  process

25

w ارسال  $\leftarrow$  r w w

process قابلیت اجرایی  $\leftarrow$  r x w

PAYCO



3 → Enter r into  $a[5,0]$  → محوّي اول فهرست درایم و دوک است اینجا می‌توانیم ۵ را بگذاریم.

٤ → Delete r into  $a[s, o]$  → حوز این را فتح کنید

5 → Destroy subject s → ۵ سعی و سخون امید را حذف کن

سُوْنَ تَفْهِمْ هَرَاجِمْ تَكْنِ

Command create\_file(p, f)

create object #;

enter a into  $a[p, f]$ ;

✓ R II ✓ ;

11      w      11      11      ;

ehd

: مولودی، علیم، شیخ و child ، patient ، الکترونیک process ← جه.

command parent process (p, q)

create subject q ;

enter o into a[p, q];

N r II II ;

N      w      u      u      ;

" r " a[ q , p ] ;

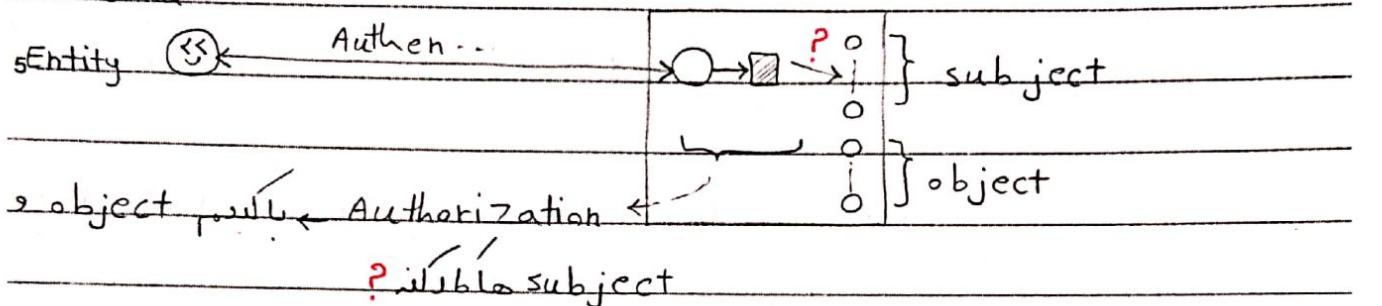
N      W      H      H      i

chd

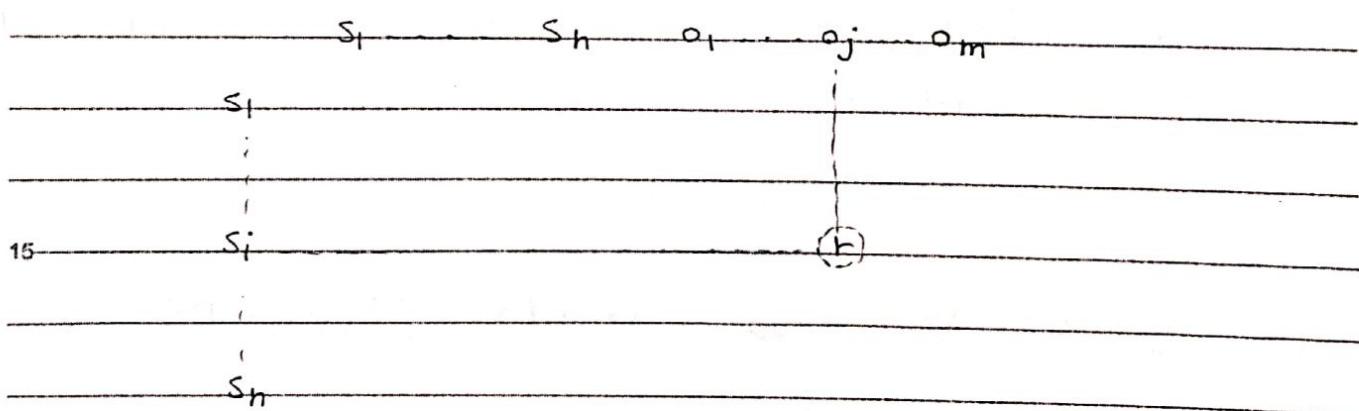
21

پایه اداری

External



\* بعکوکم میں از این حاصل توند دسترسی داشت باشید / ماتریس نظریه اداری



process مفعال است ← مدل یعنی مانع از تغییر احتمالی داره ← subject

object ← غیر مفعال است ← یعنی قابلی ایجاد رخواهی هم ندارد ←

ACM → ACM

commands → مدل این است که وقت این طبقه ایجاد احتمالی

حالات این بسیجی این دلیل برای این دستورات این اموری باشد پرسیم

PAYCO

او بعده اسیستنایین نزدیک

لے یعنی درجیان امر ای این دستورات کی حق دسترسی نہست بدالنا

5 نسل ← الہ نہست حق دسترسی داسنے باسیں بینی حالت غیر ایین میں لیز ← بارے

اصلہ این انفاق نیو فنڈ سیاست ہائی اہمیت اعمال میں لئے

grant / revoke ← DAC ← → طبق سسن  
داری

MAC ← → 10 بارے یعنی تفاصیل و  
امسٹ کا توڑسی دھمنی

RBAC ← → اہمیت داری

لے توئی این فرماں بینی برائی میں نفس

علیٰ داری بارے سرکن حقوق دسترسی

میں دیکھیں

15

توئی DAC ہر لسی بالترتیب بمعنی دنہایی لتوئی system کو تعین کر دیں ہر لسی میں ترہ

حقوق دسترسی کو داری میں بالترتیب اون سرایعی لتوئی مہندھن داری میں توئی بیاد این مقرر

دسترسی را برو یعنی اعمال انجام یا اذکون میں بلیہ

سیاست DAC داری میں لیز

توئی primitive command <sup>hd</sup> عالمی conditional command میں ذاریہ

25

لگائی اون سطح پر فرماں برد مایاں دستورات primitive داری میں لشیں

Year :      Month :      Day :      ( )

عمل الرياح وسس ماس فايل فبايس حق خواندن را پس process دید، اعمالی ز

command grant read file (p, f, q)

if own in  $a[p, f]$  then  $\leftarrow s[p, f]$  الـ  $s$  دار

5 حق خواشن الابوی افغانو < ; enter r into a [q, f]

end اُن

لله ← لوئي دستورس، ام بتونز، استفاده باشی، ولی سرمه و لیکن اینها

ملائكة امر  $\leftarrow$  امر hat دال الله يناس  $\rightarrow$  دليل من تزكيه بدل این حالات بعدی آندرس افتد  $\rightarrow$  عزم

A

A'

## Commands

silicium LA

لـ لعن حق دسترس راست من ده دیگران دهد

15--

مثال از and بـ حق من دارم و رسـ حق و دادـ اسـ بالـ لـ لونـ

command grant read file2 (p, f, q)

جست اسوسیتی های اسلامی با هم می شوند

if  $r$  in  $a[p, f]$  and  $c$  in  $a[p, f]$  then

enter  $r$  into  $a[q, \#]$ ;

25 end

Command grant read file2 (p, f, q)

if r in a[p, f] then

enter r into a[q, f];

end

Command grant-read file3 (p, f, q)

if  $c$  in  $a[p, f]$  then

enter  $r$  into  $a[q, f]$ ;

-end-

-10

البروسوم حق تباقق راداسنه باس براند حق ترابه روسمه واعمالن

safe

ili → A

$\rightarrow A' \rightarrow$

2

## Command

unsafe

-15

۱۰۷ مادری این طمندستون

~~unilcuid safe A~~

من است او با معنیت باید این آداب اطهار لفظی روش این هست یاده

نَلَّةٌ تَأْدِي مُلَّا طَهْرٌ مُنْدَسٌ سَادِمْهُ دَالِيرٌ حُونَ الْبَحِيمَهُ اَسْ لَسْنَ بَرْقَى حَالَتْ دَرْخَتْ كَه

دال

inland is a view of the desert in the south of Egypt at the time of the Exodus 25

Subject:

Year :      Month :      Day :      ( )

page:( )

عن باقی عبادت ہن تو نہ تاری این ہستیا جانسی

لهم وَقْتُكَ لِي حَالَتْ أَسْأَدَ اللَّهِ تَبَرِّعَانِي أَسْتَأْمِنُ أَنْ أَنْقَالَ أَوْ أَسْتَأْنِحَاتَ

داره بودن فرق multi operational بودن با main conditional

- undesirable long-term initial operation in  $\leftarrow$   $\rightarrow$

10-

الى ادى اول است multi operational

۱۵- میل: این سهمهای درایه‌های مختلف ماتریس باشند از این است

if r in a[p, f] then

"c" a [q, f] "

وَالْمُؤْمِنُونَ هُوَ الْأَوَّلُونَ مَا تَرَسَّعَ بِهِمْ سَبَقَهُمْ أُولَئِكَ هُمُ الْمُنْتَصِرُونَ

20 if  $r$  in  $a[p, f]$  then

N C N

5

نَالِينْ سِيِّسْ وَلِمَانْ تُوْرِيْ بَاهِمْهُلْ

سے ملکیت سے لے کر بے داری از ماں اس توک سے طہر نہ تھا

25

append حق

محسوسیاتی دار دار مجهود و توقیع دار  $\leftarrow$  **کل**  
 modify  $\leftarrow$  own حق

با خواسته ای این را ایجاد کنید و این را در اینجا ذکر نمایم

5

با خواسته ای  $\leftarrow$  **کل**

Command revok all rights (p, f, q)

create sub tmp;  $\rightarrow$  ایجاد در **کل** subject باش

enter r in a[tmp, f];

if o in a[q, f] then

delete r from a[tmp, f];

if m in a[p, f] and r in a[tmp, f] then

delete r from a[q, f];

destroy sub tmp;

end

15

کل  $\leftarrow$  **کل**  $\leftarrow$  **کل**

hal

C:\multioperations  $\leftarrow$

20

25

حق ایشنس دستورز ←

command grant exec ( $p, f, q$ )

if  $a$  in  $a[p, f]$  then

5 enter  $x$  into  $a[q, f]$ ;

end

command modify right ( $q, f$ )

if  $x$  in  $a[q, f]$  then

enter  $w$  into  $a[q, f]$ ;

10 end

→ ام رای فایل اف آیس دام بباب می ده

\*Command grant exec (Alice, f1, Bob) ← فرمان این آیس دستورز

رای فایل هن اف اد، آرد و باب می دستور

15

→ من نه = > این پستیشن خواسته command modify right (Bob, f1);

جون اتفاق که افتاد این بود او توی سایریوی آیس من خواست حق نوشت ب

20 باب به مری باب ایخا این حق را خودش بخودش داد بخاطر دستور \*

بله ← این ماتریس اندایر تغییر من لبر خیلی از درایه ها صفحه است

25 حکم و زیاد معقول این که بین نیس سیس برای این حافظه است

استفاده از بروکس لیزنلایری من لش:

1 → Authorization table

1

2 → Access control list (ACL)

2

3 → capabilities

اوی ابروں از این استفاده کنند 35

داری table میں 1

Alice	own	file1	---
"	r	"	
"	w	"	
!	!	!	
Bob	own	file1	
"	r	file1	
!	!	!	

لستہ ایکسٹریس سارے ایکسٹریس 10

جذبہ

اچھوڑتے ایکسٹریس دیکھو 2 15

object میں ۔ ACL میں

file1 .

Alice	Bob
own	
r	
w	
!	
.	

ایساں سوچنے والے

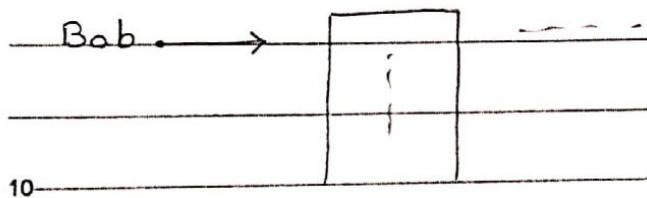
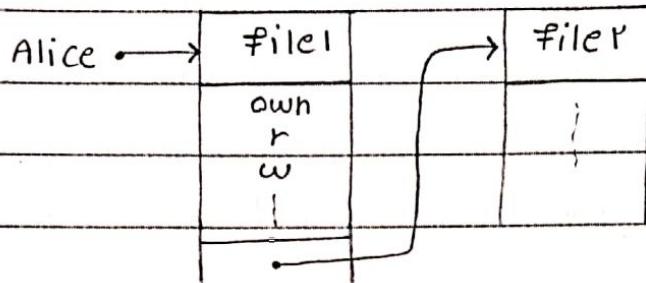
اکسٹریس 20

file2 .

!	---
!	
!	
!	

25

بر اساس سه راه کی ماتریس اس سی ۳ ←



22

مسکن نهاد داده لینک های همچ لشتری برای جریان اطلاعات ندارد

15 از نشانه طبق سینه است اونقدر سختی از نشانه

\* سایر مسابقات تری امتحان بیان

هم ا است مالکیتی داریم بواسر مادرلت کو ادمین owner این مالک ا است و اجازه خوانش ادمین این دارم فقط

object

هم ای مالکیتی است از هم مالکیتی و اسون

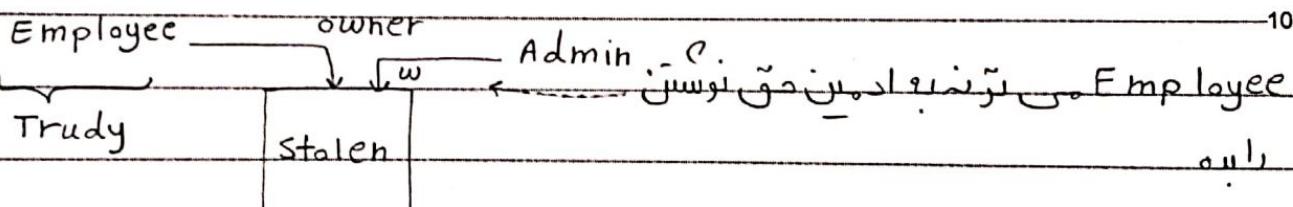
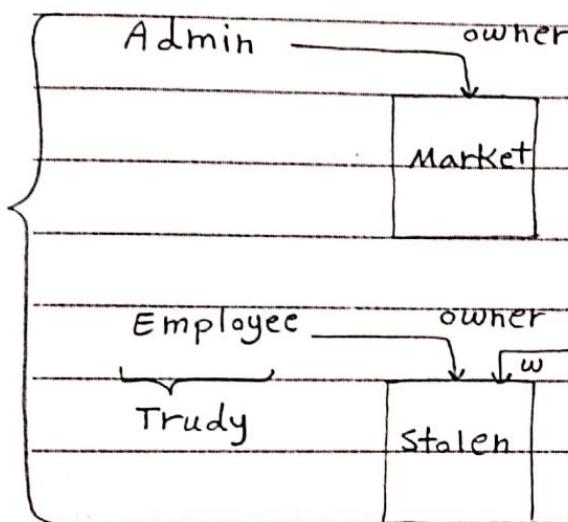
و

و سطرهایی می خواهد اطلاعات مالک را درست بخواهد و توی سیستم MAC هاست و فوچن

پیش املاعاتی که از مارکت بدست آوردیں خود رئی سازمان های لفتسی بفروض

کامپانیایی فایلی بواسطه staleh درست. لذت

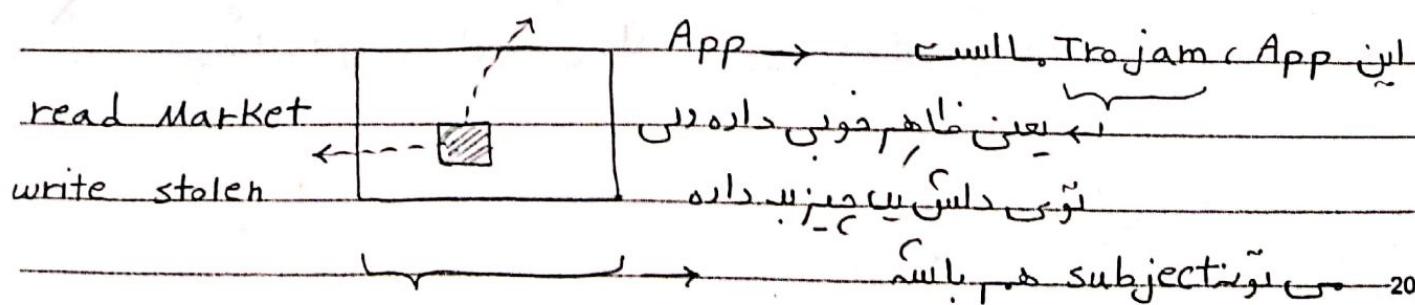
لارسی owner باشد تو نعمت تو ستن را بودیران به



این متن object هستند ولی

با قرار دادن subject ها باشند

لذت خواه



لذت App توسعه دهنده را در دست داشت تردد دارد برای ادمین لذت

ظاهرش اینکه همچنان با این فایل مارکت نزدیکی در واقعیت رئی این قسم است

لذت خواه از مارکت خونه و بوی staleh من تو سی هون این برنامه مردی هست

Subject:

Year: Month: Day: ( )

page: ( )

لادین ام اس بلن  $\leftarrow$  س لریانی خوانن از مارکت مارکت

جون اس اس هرچوئی او واس نو سس دامی تونه  
 $\leftarrow$  جون اس اس هرچوئی او واس نو سس دامی تونه

بچونه  $\leftarrow$  س ام ال ام ات مس اس ای بی اس تی س ار د  $\leftarrow$  مسلمه دی جریان ام ال ام ات

لترلی نالیم هین اس تی با سعی این سال راحل لشیر

هدف از MAC  $\leftarrow$  جریان ام ال ام ات را بوقتی لترل لشیر

10

1  $\rightarrow$  BLP  $\leftarrow$  این باید واس های داری  $\leftarrow$  واس ۳ تا مدل پادم سازی  $\leftarrow$  MAC

2  $\rightarrow$  Biba  $\leftarrow$  استهان داره ای اسی س

3  $\rightarrow$  Dinh  $\leftarrow$  لیزون لیز

15 نله  $\leftarrow$  توی MAC سعوح دسترسی لغرنام لشیر و ک توی ناسی

نله  $\leftarrow$  برای ه سویقین category object subject سفح امیتی

↓ Access class  $\leftarrow$  لشیر این

20

Access class = ( security level , category )

1 = { TS, S, C, U }  $\leftarrow$  میل  $\rightarrow$  { Army, nuclear } =  
Top secret  $\leftarrow$   $\rightarrow$  unclassified

25 secret  $\leftarrow$   $\rightarrow$  confidential

PAYCO \*  $\leftarrow$  از ۱ و پیش از ۲ انتخاب می لشیر  
نیمه جو عوای  $\leftarrow$  subject object

\* → Access Class → levels EL

یعنی یا بنتی ام تو نه باس سه یا هر ۲ یا بینی از  $\subseteq$  است

برای ایجاد محتوا در اینجا کلیک کنید ۵

set is a well partially ordered class. Access class  $\leftarrow$  الـ

لـمـعـنـهـاـفـرـمـوـعـرـالـلـلـهـبـالـعـتـقـسـيـ  
لـمـعـنـهـاـفـرـمـوـعـرـالـلـلـهـبـالـعـتـقـسـيـ

To set:  $\forall a, b \in S$   $a R b$  or  $b R a$   
 $\downarrow$   
 set  $\leftarrow \exists c \forall b_0 \in S$

رايِ مُتّسی با هم دارند

nuclear      Army      Access class il  $\leftarrow$  JI!

و سطح اس از پیش طاس های بالاتر می شود.

$\langle TS, \phi \rangle$

$\left\langle S_n \mid n \in A \right\rangle$

A diagram illustrating a geometric construction. A horizontal line is intersected by a transversal line. From the point of intersection, a vertical dashed line is drawn downwards. The angle between the transversal line and the vertical dashed line is labeled 'L'. The angle between the vertical dashed line and the second ray of the V-shape is labeled 'X'.

$\langle s, \phi \rangle$

ادام و دارد

Subject:

Year : Month : Day : ( )

page: ( )

نوات من قبل ←

$\geq \triangleq$  Dominance :  $c_1, c_r \in AC$  ← خصوصیات دارای طالع

$$5 \quad \begin{aligned} (c_r \geq c_1) &\leftarrow c_1 \geq c_r \text{ iff } = \\ &\quad \sqrt{\text{لهم }} \quad \swarrow \text{ وفقه } \end{aligned} \quad \begin{cases} SL(c_1) \geq SL(c_r) \\ cat(c_r) \subseteq cat(c_1) \end{cases}$$

طایعه از AC بسته است ←

$$10 \quad AC : \langle \underline{SL}, \underline{cat} \rangle \rightarrow |AC| = l \times r^c$$

نحوی اعداد از AC باشند ←

نحوی نتایج من قبل ← ۱۹ تا بود

۱۵ نحوی نتایج من قبل و متناسب با این طاس نیز نتوی متناسب باشد

نحوی داده ایانه (همان را با این طاس نیز نتوی متناسب باشد)

نحوی نتایج من قبل و متناسب با این طاس نیز نتوی متناسب باشد

از خواص داده ایانه ← Dominance

greatest lower bound :  $\forall x, y \in AC \exists z \in AC$  و درست

$z \leq x$  and  $z \leq y$

1 → BLP → confidentiality

2 → Biba → Integrity

3 → Diah → C + I

object واسو subject اقران من لب و AC راه

میزان حساست میں سے

## اہم ترین اور داریں

ان بالا رَى هاربِي تُرْنِي بَرْزِنِي ← no read up

اے خواہن وہیں اسٹ  $\leftarrow$  No write down  $\rightarrow$  اے خواہن وہیں تونی بوسی

$Ac: < \{ TS, s, e, u \}, \{ manager, Employee \} >$

Ac<sub>admin</sub> = < TS, { manager } >

AC<sub>Trudy</sub> = < S, {Employee} >

Trudy 20 بوده‌ان حق دسترسی روشن ناید و متن افتخاری App از ارالت

کلوب های امنیتی (اجانشوداره) و ل وقتی می خواهد از stolen stok لایوسسیستم کی بپرس اجازه

میں دھونے والے stalen پاسن رہاست

نَلَهَ ← مِنْ تَوْنَرَائِي نُولَسَنْ باسْمَحْ دَسْتَسْ يَاْسِنْ تَرْ وَارْدِبَسْ (جُونْ بَالَاتَّهْمِي تَوْنَبَا

سماح دسترسی بایسین تر و روکیده آن) در این حالت اولی نویسنده و دو دیگر دلی

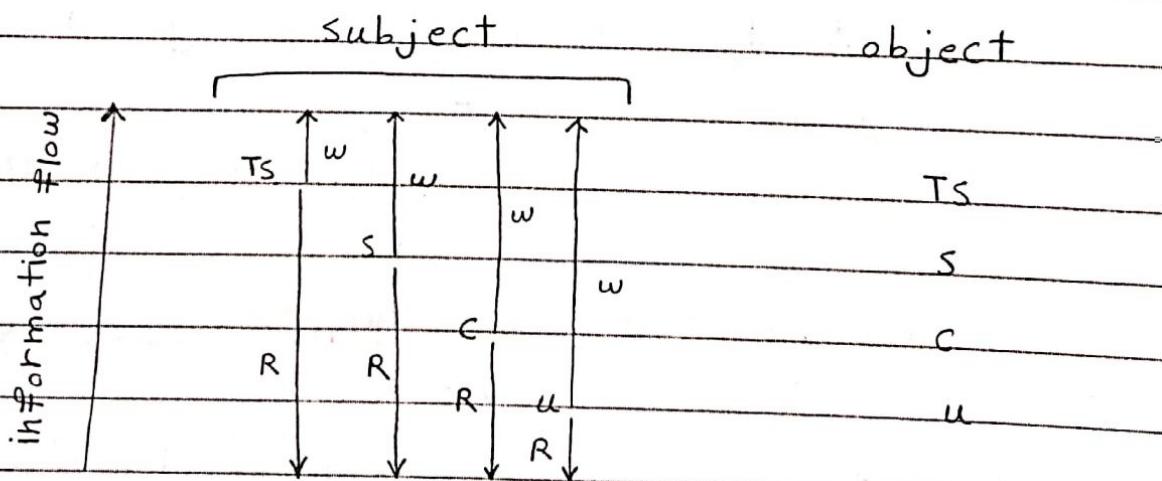
زنانه ایوب هر زان ادمین تویی سمعن دسترسی secret

رَاجِلُ الشَّرِّ وَرَاجِلُ ابْسُورْدِ، لِمَنْ مَا رَأَتْ حُجَّونَ بِالْأَتَاسِتْ حَوْانَهُنَّ

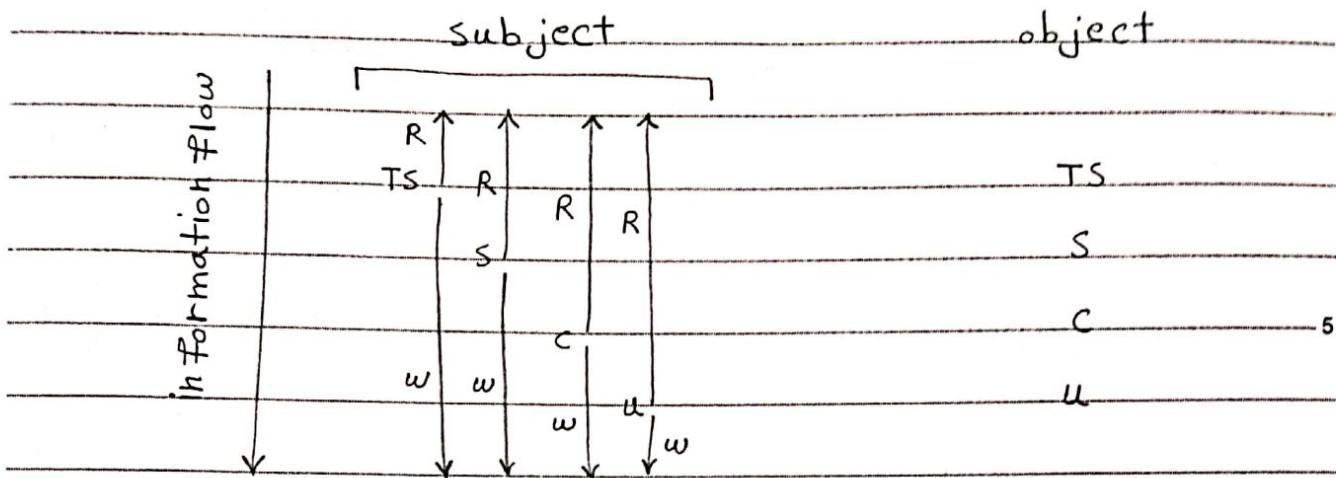
نَّيَّارَ ← نَوْعِي لِنْ حَالَتِ رَا إِمَالَانْ زَارَيْرَ

10-

خوانن رامددوس من لئن



No read down ← Biba جایز  
No write up



Integrity داریم، اینا نکته

-10

نامہ GLB کی طرف اسے عمل تونس میں قبول کر دیا گی۔

## ازیاسن دارہ می خونہ

دلل فعل خواستن  $\leftarrow$  الـ subject  $\rightarrow$  الـ object  
 $\approx$  لـ خواسته بـ و از  $\approx$  s

امض السواد وللآلئ از سعف بالا ایش بخوبی تقدیر کنی من آنکه

law watermark for subject ← → ملکون اول

برای یک چیز خواستن می‌توانیم نوشته شده باشد، object

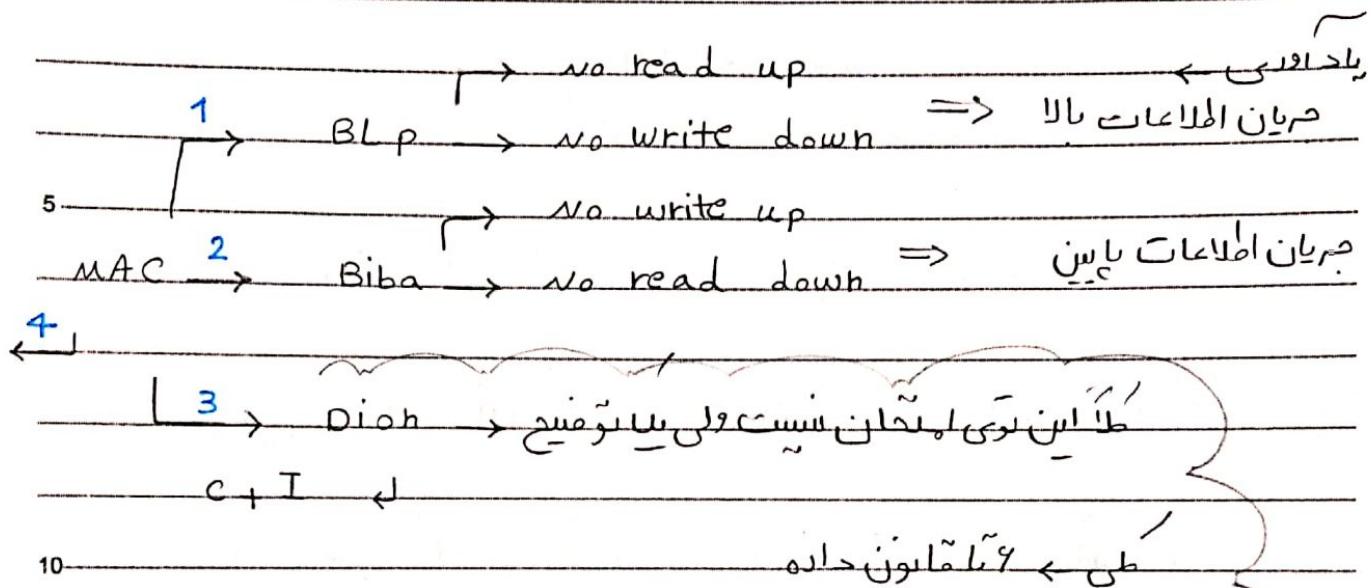
-20

۷. تونس ← الـ کـ رـ اـ لوـی ۵ بـ لـ زـ سـ بـ سـ عـ حـ وـ اـ نـ اـ زـ

رسود میں GLB (5,0)

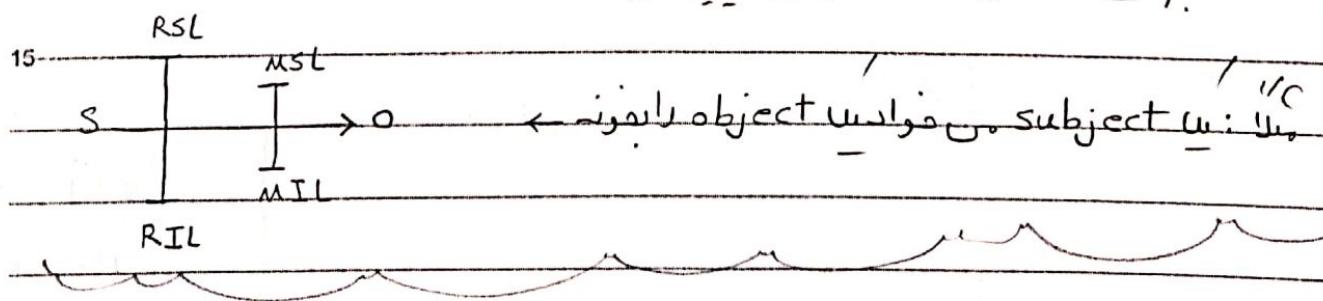
Low watermark for object ← مالوز دار ← 25

23



RTI و RSL میادین محدود مقربین از subject برای هر دویں دارند.

برای object دویں دلیل تعین میں لذت میں



نکته کوئی Biba میں BLP کامن لفڑی، برای نوشش حاصل متفاوتی نہیں با

سچ دسترسی حاصل متفاوت وارد ہے کوئی Biba این ورد راند بیریم و Biba از این

لکھ محدود ترمیم میں کوئی افادہ بیان محدودیت را برداشت و ۲۳ ماہون لذا سچ

PAYCO نوادران طرح ایامی کرد جو یعنی میں سو سچ دسترسی لمحہ میں

یعنی از وظایفی مثلی system استفاده می‌کنند و براساس این احتمالاتی

لپ تاپ دستگیره کرده می‌باشد تغییرات لیبره

Subject:

Year : Month : Day : ( )

page: ( )

History Based ↑

پی ساقه تاریخی سلسله ایتی خارج

Hierarchical structure \*

Co + Int

4 → CWM = Chinese wall Model

بر طبق برداشت از Dinh

5

فرضیه ای این همین تاسیسات تلقیب داری بعده خواهد شد و ساده ای را دارد

استخراج اینی برای کارهای محدود است A هست و اس اس اس ای او داری ساخت

10 تلقیب اتفاق نمود ساده باش (اینی خواهد شد)

دندانه ای ای

هدف = اجازه نیست املاک اداره را نزدیکی این احتمالات این وسیله نیست

A

استخراجی x

B

استخراجی صفر x

این اینها

هم تغایر نمی‌کنند

نافع دارند

15

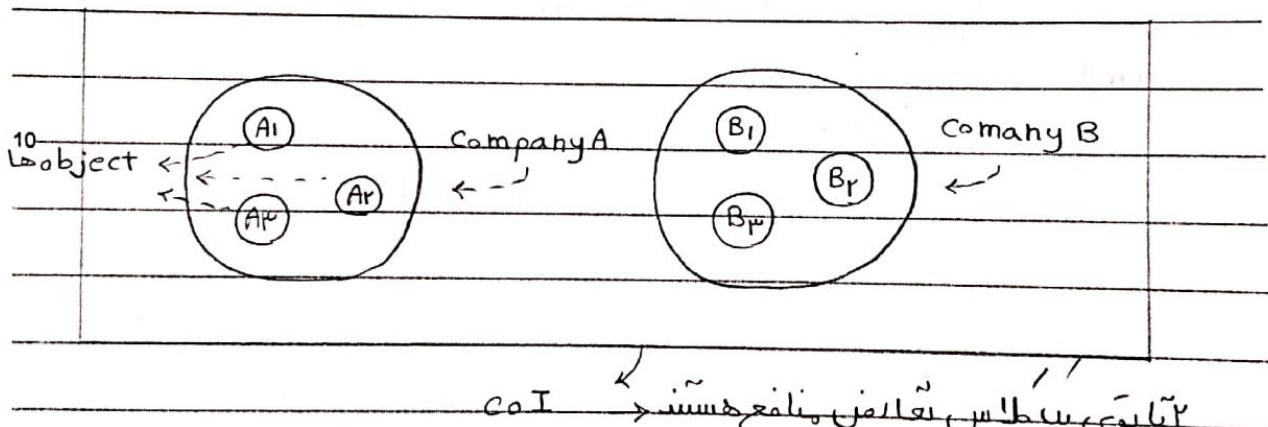
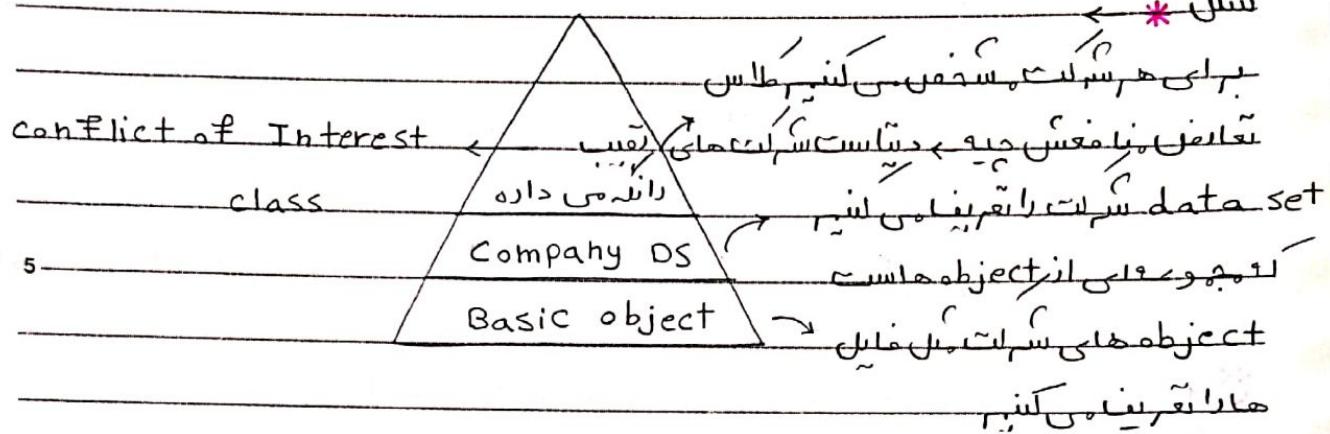
20

نکته دلیل این سیاست باید می‌کند همان مدل BLP است

+ no write up ←

پرسی متابلیت جدید ←

PAYCO



آنکه این دو سیستم متعارض هستند

\* آنکه اون واسوتوشن خواهد بود زیرا

جوابی از است استقیم

20.1)  $\rightarrow$  simple property  $\rightarrow$  خواهش خواهش است

$s \cdot \text{read}$  بازخواهید

$\rightarrow s$  can read off either:

1-  $\exists o' \text{ s.t. } s \xrightarrow{o'} \text{ read}$  برای هر سیستم مسخره می‌کنیم طلاس می‌خواهد  
بعنوان قبلاً از دیتابیس ساخته شده بودیم که از اینه باشیم اما از اینه باشیم این داریم یعنی هدف هاست

company  
dataset

=  $CD(o)$

PAYCO 2-  $H^o \in PR(s) \rightarrow COI(o') + COI(o)$   
که جزو هدف هایی نیز از خواهد

حکایت از مسیر خود را بخواهید

2 → property → هدف نوشت اسے

$s \xrightarrow{\text{write}} o$  باید

→  $s$  می‌تواند بفرمایش را بخواهد

1 the simple property permits  $s$  to read  $o$

↓ ←  $s$  می‌تواند  $o$  را بازخواند

(and)

2 for all 'object  $o'$ '

$s$  can read  $o' \rightarrow CD(o') = CD(o)$



\* ملک امتحان بیاد

Alice → A, C ساده سری

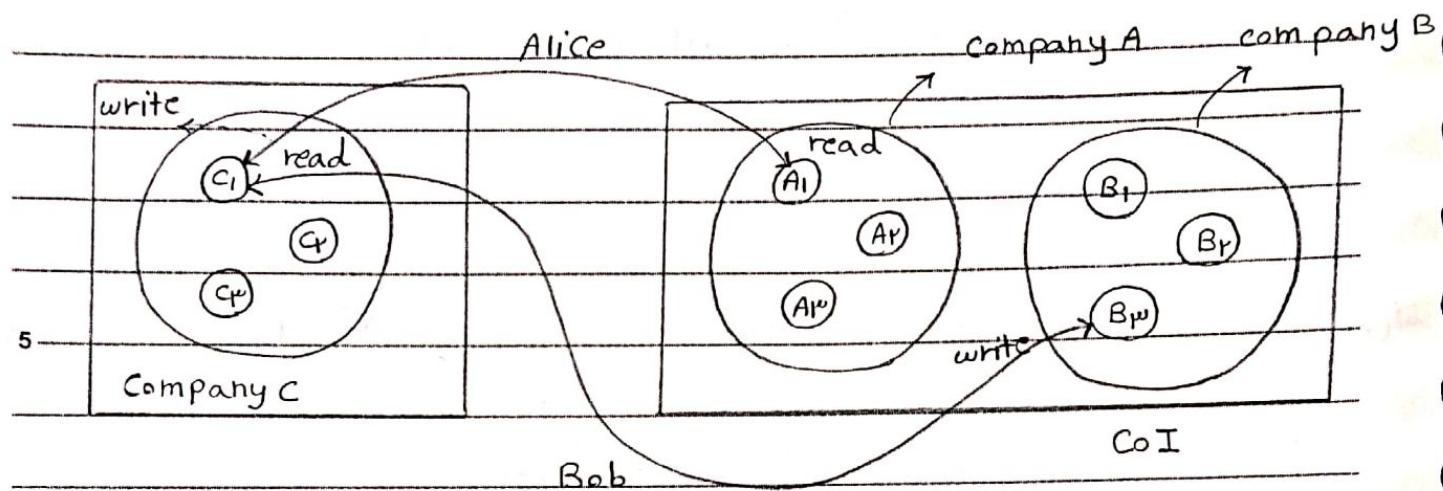
غرض داشت

Bob → C, B //

الروبوت 20 را در آنسته باسیم ← آلس اجازه A را در دس از Alice خون

والی این نویسی غایب + از اعمت خونه والی سی

نیست خود مستقر داریم



لایهای امنیتی مبتنی بر تاریخ History Based

از این نظر، داده‌ها در سیستم امنیتی مبتنی بر تاریخ، بازدید و ویرایش می‌توانند انجام شوند.

System

RBAC - Role Based Access Control

RBAC را که امنیتی از این قرار دارد، می‌گویند.

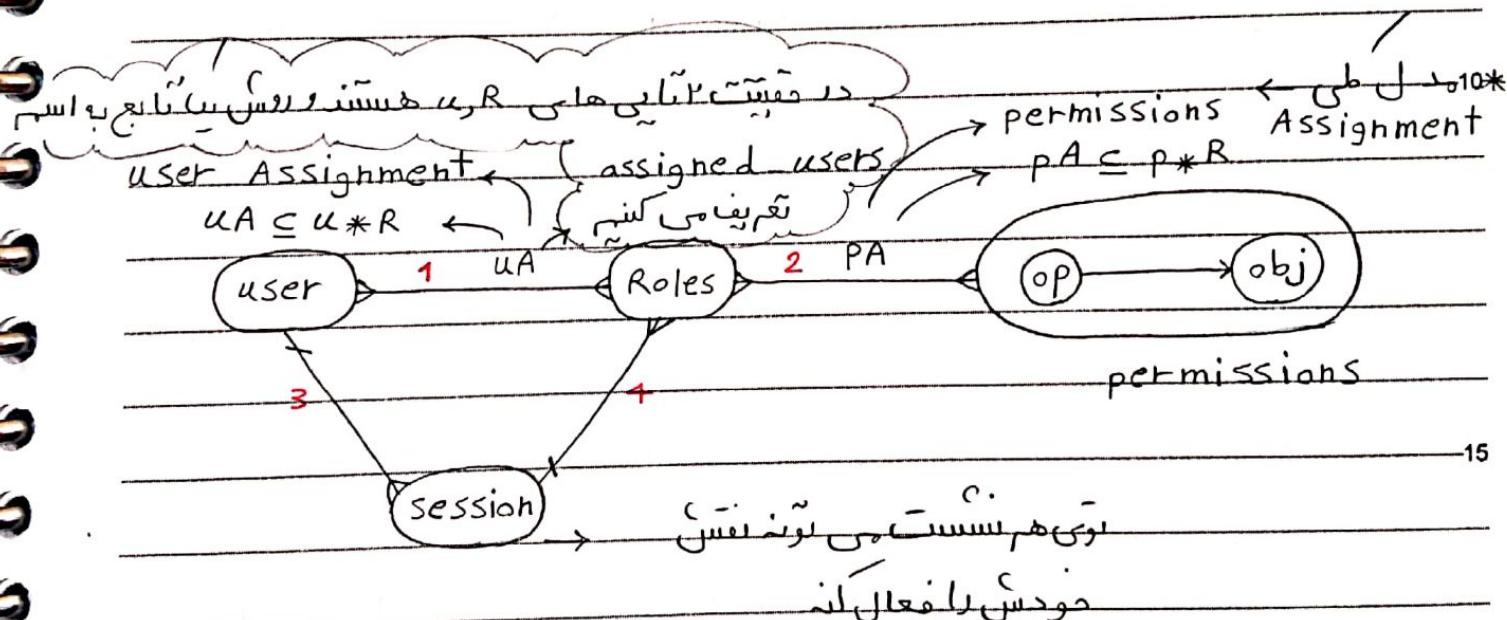
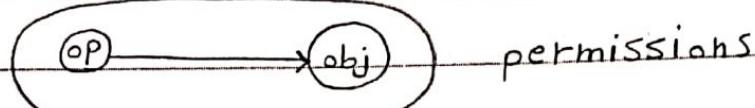
1 → least privilege → حداقل امتیاز بدهید، هر کسی بدانندنی باشد  
دسترسی بیش از آنکه لازم باشد را نداشته باشد.

2 → separation of duty → این فناوری از هر کسی اطمینان می‌آورد که یک فرمان را تنفيذ نمایند و خواهش نداشتن آن را تأمین نمایند.

3 → Abstraction → این فناوری از هر کسی اطمینان می‌آورد که یک فرمان را تنفيذ نمایند و خواهش نداشتن آن را تأمین نمایند.

\* میزبانی امنیتی مدل واسطه RBAC داریم

( باسی user ترین subject هست )  $\rightarrow$  user  $\leftarrow$  طبقان  
 Roles  $\leftarrow$  نفس ها  
 جو زیرا مجوزها را تقدیر نمی کنند  $\leftarrow$  object  $\rightarrow$  operation  $\leftarrow$  مجوزها ۱۵



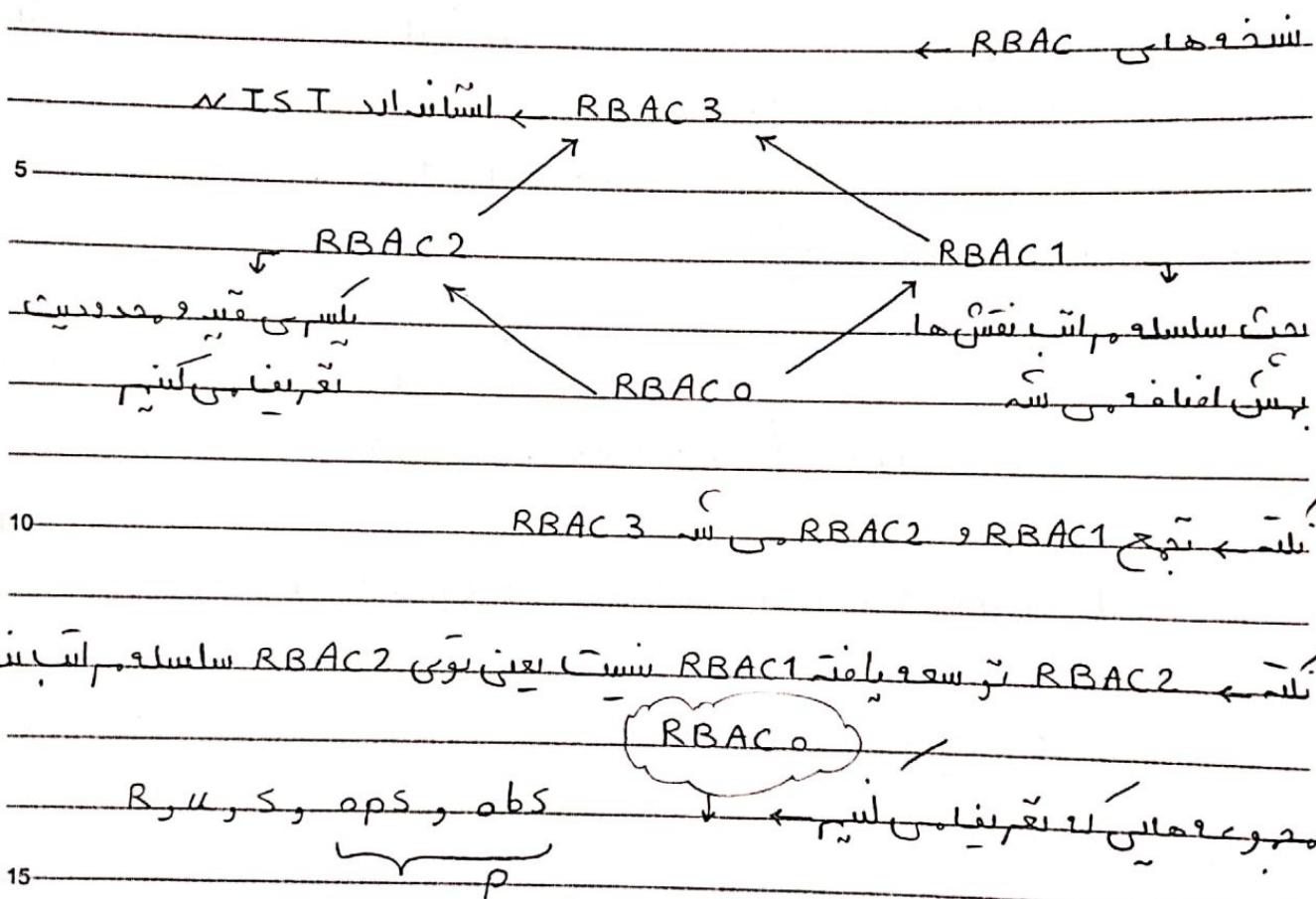
۱- طبقان تونه چندین نقش داشته باشد و هر چندی تونه بجهنین طایر اختیام

۲- آنکه رایج نباشد و جزو  $C$  باشد

۳- هر طایر چندی تونه مفعال آن و لی هر session مال طایر است.

۴- تونه هر طایر چندی تونه مفعال آن و همچنین تونه ملکه  $session$  را داشته باشد.

سؤال اصلی توپ طبر، توپ هر سیستم چه جزوی دارد؟ \*



همه نیازی اینجا واقع سوال اصلی \*

$\text{assigned\_users}(r) = \{ u \in U \mid \langle u, r \rangle \in \text{UA} \}$

ایعنی نیش توب جو کاربری  
دارد میتواند است

$\text{assigned\_permissions}(r) = \{ p \in P \mid \langle p, r \rangle \in \text{PA} \}$

ایعنی نیش توک امتحان بار سئون دارد و در آن این سوال میاد \*

24

نکته اینست که دری امتحان فرمای ایزبرون میم  
 $\text{assigned\_users} : R \rightarrow P(u)$   
 $=$   
 $\rightarrow$  small powerset این یعنی مجموعه ای از زیرمجموعه های  $u$

لیستی از داده هایی که خود را باس بتوانیم  
 $\text{assigned\_users}(r) = \{ u \in U \mid \langle u, r \rangle \in UA \}$

$\text{assigned\_permissions}(r) = \{ p \in P \mid \langle p, r \rangle \in PA \}$

$\text{user\_sessions} = U \rightarrow P(S)$   
 یعنی خروجی چند تاست  
 $\rightarrow$  جو موادی هستند که در آن خروجی می باشند

$\text{session\_user} = S \rightarrow U$   
 یعنی خروجی یعنی است  
 $\rightarrow$  جو موادی هستند که در آن خروجی می باشند

التباه! بین این دو

$\forall s \in S, \forall u \in U \text{ s.t. } \text{session\_user}(s) = u \leftrightarrow s \in \text{sessions}(u)$   
 این دو اثبات برای این اتفاق است  
 این دو اثبات برای این اتفاق است

Subject:

Year : Month : Day : ( )

page: ( )

session roles :  $S \rightarrow P(R)$

دسترسی طبق زیر مجموعه ای از نقش های خود را فعال می کند

الایام session roles , UA

5

uses session roles(s)  $\{ r \in R \mid \langle session\_user(s), r \rangle \in UA \}$

این بودن user برای این دوست از مسافری شیوه (وقتی هم  
نقش ها سر مغلل نمی باشند)

اصل مقادیر  $\leftarrow$  تویی سیستم جو مجوزهای داره:

با این طرز توزیع یک طبقه اداری مجموعه مجوزهای داره

available session permissions(s) =  $\sqcup_{i=1}^n assigned\ permission(r_i)$   
 $\leftarrow$  اجتناب

نیز session roles(s)

15

نامه سلسله توک RBACo  $\leftarrow$  یعنی جو لیسی باشد این نقش ها

را بطریق آن به داشته و ممکن است این معرفت نداشته باشد

باید داری  $\leftarrow$  Super user یا اون سطحی که این طبقه مجموعه دارد و در

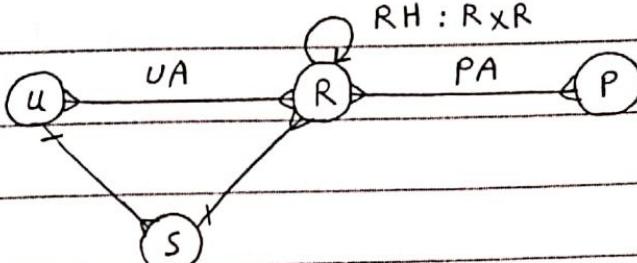
نقش ها بودن

25

سلسله امنیتی و RBAC 1

سلسله امنیتی و RBAC 2

RH : RXR



5

مدیر خودسی طارمی manager

است

\* جوزهای انسانی

طیران از بالا برو

6

کارکردی کارگردان Employee

جواہر است

پاسن است

7

دسترسی را مدیر به Employee

اینست برخوازان

حروف امیر طاری کو مدیر

دسترسی پاسن را مدیر به Employee

\* بواری می برمیس

15

توکن RBAC 0 Manager

Manager :  $P_1 + P_2$

$\frac{1}{\text{بسی}} \cdot \frac{1}{\text{جوزهای می باشد}}$

جنون طارمی دارد

مدیریت دارد

20

موقعیتی که این را برو

Manager اختیاری نیز

25

Subject:

Year : Month : Day : ( )

page: ( )

RBAC1 ← جوزهای ایجاد و مدیریت اقران من ایز ← P<sub>1</sub> ←

← سیستم این

حالات استراحت را

دهی مادر Manager!

5

\* RBAC1 ← جوزهای نزدیکی ها ← سیستم ← P<sub>1</sub> ←

P<sub>1</sub> ← خدمت ←

لار، کارکردی، اراده است باشند، که نزدیکی باشد:

این بخش جزو ایجاد جوزهای ایجاد است.

دستورات طبقه ای ایجاد کردن ←

15

\* RBAC1 ← داده های RH روش ایجاد است.

General RH →

سیستم تونیباش، درجه های RH

20 Limited RH →

project manager

Tester

programmer

← +

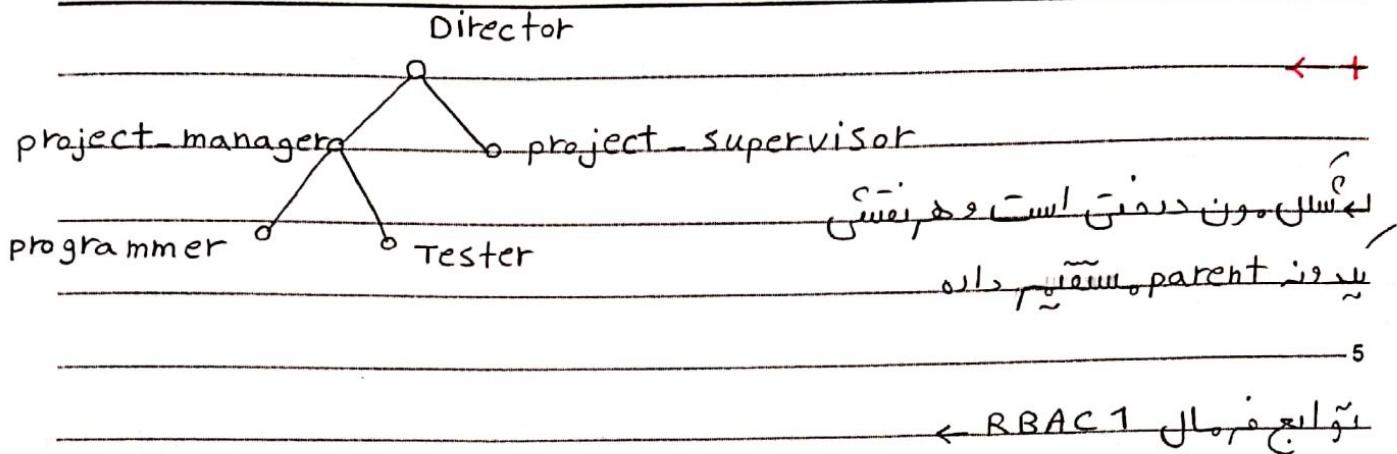
25

project member

جزءی از پروژه ایجاد شود

PAYCO

ایران



$$RH \subseteq R \times R$$

↪ partially ordered

با این نکادسون می دهم ← رابطه انتشاری :

$r_1 \geq r_2 \rightarrow \text{authorized permissions}(r_1) \subseteq \text{authorized permissions}(r_2)$

جوزهای معرفی و معرفی بعنوان است ←

$r_1 \geq r_2 \rightarrow \text{authorized users}(r_1) \subseteq \text{authorized users}(r_2)$

$\{Alice\} \subseteq \{Alice, Bob, Dave\}$

و ↪

Alice ↪ Bob, Dave

20

Subject:

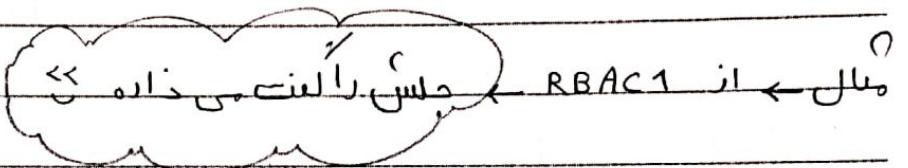
Year : Month : Day : ( )

page: ( )

authorized users(r) = { user |  $\exists r'$ ,  $r' \leq r \wedge \langle u, r' \rangle \in UA$ }  
 Authorized users (r) = مجموعه کاربرانی که دارد  $r'$  را که  $r'$  را که دارد.

authorized permissions(r) = { p |  $\exists r'$ ,  $r' \leq r \wedge \langle p, r' \rangle \in PA$ }

5



طريقان  $\rightarrow u = \{Alice, Bob, Dave\}$

نقش  $\rightarrow R = \{$  directory, project manager, programmer, Tester, ...  $\}$

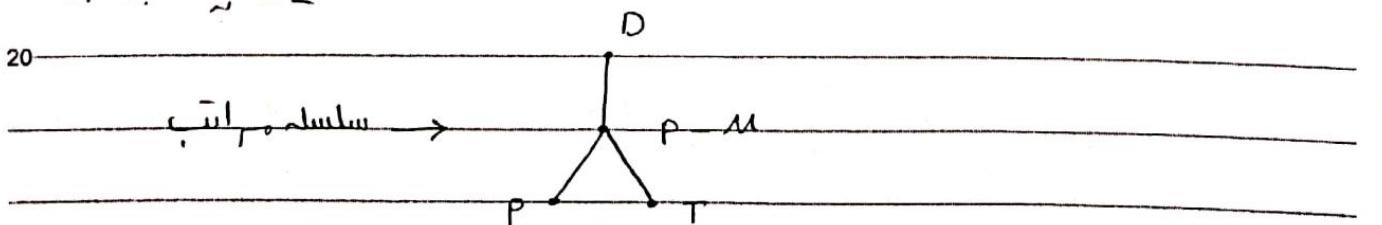
$P = \{P_1, P_2, \dots, P_q\}$  خواستن فایل (1)  $\rightarrow P_1: r \rightarrow file1$   
 $P_r: w \rightarrow \dots$   
;

15  
UA:  $\{ \langle Alice, p_m \rangle, \langle Bob, D \rangle, \dots \}$

بین Alice و D

PA:  $\{ \langle P_1, p_m \rangle, \langle P_2, p_m \rangle, \dots, \langle P_n, D \rangle \}$

میان پیوندی بین P و D



sessions roles ( $S_1$ ) =  $\{p_m\}$ , user sessions (Alice) =  $\{S_1\}$

25  
(RBAC1, RBAC0)  $\rightarrow$  آیا آلس میتواند file2 را بخواهد؟ (بافرضیه)

p, e available session permissions (S.)

RBAC0

RBAC1

لئے این محدودیتیں باہم مطابق ہیں

RBAC2  
constrained RBAC1

محدودیتیں و معاویتیں

نئی کارکردگیاں سے م جدا ہیں ← separation of Duty

ناساز طریقہ نئی کارکردگیاں سے م جدا ہیں → SoD

متنافر ترقیاتیں کیں

بوجھ موریں محدودیتیں لئیں: SoD

لئے این اختیارات سے

1 → static SoD → UA وقوع سے؟

2 → Dynamic SoD → موقع برقراری سے؟

برائے این محدودیتیں رابطہ برابر نہیں: SSoD میں

$\langle \underline{sr}, \underline{n} \rangle$ ,  $rs \subseteq R$

$SSoD \subseteq P(R) \times N$

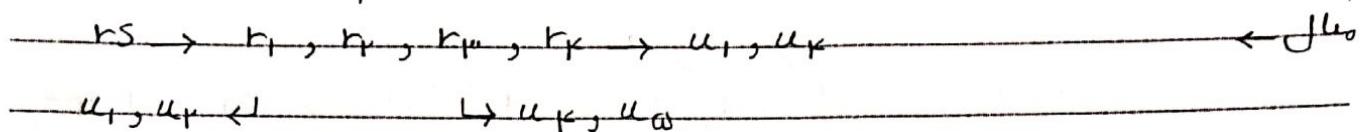
role set  $\hookrightarrow$  یہ کام دعیے

$\langle rs, n \rangle \in SSoD$ ,  $\forall t \subseteq rs$ ,  $|t| \geq n \Rightarrow n$  assigned users  
 اسے  $\leftarrow ret$  PAYCO =  $\emptyset$

Subject:

Year: Month: Day: ( )

page: ( )



$n = p$

5

$t_i \in \{R_1, R_2, R_3\} \rightarrow n \text{ assigned users}(r) = \emptyset$

re  $t_i$

لیست

اگر  $t_i$  ای این مجموعه نباشد

برازماید

10

برازماید همچو  $t_i$  را با  $R_1, R_2, R_3$  مقایل کنید، اگر باسیز است، باید در رابطه با  $t_i$  اسود شود

برازماید  $t_i = \{R_1, R_2\}$  را با  $t_i = \{R_1, R_2, R_3\}$  مقایل کنید، اگر باسیز است، باید در رابطه با  $t_i$  اسود شود

15

برازماید  $t_i = \{R_1, R_2, R_3\}$  را با  $t_i = \{R_1, R_2, R_3, R_4\}$  مقایل کنید، اگر باسیز است، باید در رابطه با  $t_i$  اسود شود

برازماید  $t_i = \{R_1, R_2, R_3, R_4\}$  را با  $t_i = \{R_1, R_2, R_3, R_4, R_5\}$  مقایل کنید، اگر باسیز است، باید در رابطه با  $t_i$  اسود شود

DSoD معرفی

20

$DSoD \subseteq P(R) \times S$

$\forall \langle RS, n \rangle \in DSoD, \forall s \in S, 1 \leq \text{session\_roles}(s) \cap RS \leq n$

کارشناسی اور دسترسی مفعال شده

اجزء و نسبت های متنافر

25

حالاتِ تعداد نسبتی از بزرگی توانی بلند ← Granularity

حالاتِ تعداد نسبتی از بزرگی توانی کوتاه ←

5

10

15

20

25