دانشگاه صنعتی اصفهان
مبانی رایانش امن (نیمسال دوم ۱۳۹۹)

سوالات پایانی فصل اول

مریم سعیدمهر
شماره دانشجویی : ۹۶۲۹۳۷۳

نسترن عشوری
شماره دانشجویی : ۹۶۳۱۷۹۳

1

1. Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.

a. John copies Mary's homework. → **Confidentiality**

b. Paul crashes Linda's system. → **Availability**

c. Carol changes the amount of Angelo's check from $100 to $1,000. → **Integrity**

d. Gina forges Roger's signature on a deed. → **Integrity**

e. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name. → **Availability**

f. Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number. → **Confidentiality and availability**

g. Henry spoofs Julie's IP address to gain access to her computer. → **Confidentiality, integrity, availability**

2

3. The aphorism "security through obscurity" suggests that hiding information provides some level of security. Give an example of a situation in which hiding information does not add appreciably to the security of a system. Then give an example of a situation in which it does. →

- برای مثال در موردی که برای رمزنگاری پیام ها از الگوریتم substitution (جایگذاری هر حرف با حرف دیگر) و یا الگوریتم shift cipher استفاده شود ،پنهان کردن رمز چندان به امنیت ارسال پیام کمک نمیکند چرا که سایر مولفه های امنیتی ضعیف بوده و به ترتیب با یک آنالیز آماری حروف و امتحان تمام حالت ها (حمله bruteforce) برای دو الگوریتم فوق میتوان به راحتی به متن اصلی پی برد.
- برای مثال پنهان کردن پسورد حساب ایمیل یک کاربر نقش به سزایی در حفظ امنیت اطلاعات شخصی ایفا میکند.

3

4. Give an example of a situation in which a compromise of confidentiality leads to a compromise in integrity. → برای مثال از بین رفت محرمانگی رمزبانکی و شماره کارت نظیر آن، موجب آن میشود که سارق بتواند از حساب فرد برداشت کرده و یا حتی برخی اطلاعات کاربر را تغییر داده و موجب از بین رفتن صحت دیتا و تغییرات احراز شده شود.

4

5. Show that the three security services—confidentiality, integrity, and availability—are sufficient to deal with the threats of disclosure, disruption, deception, and usurpation. →

- disclosure : هرجور دسترسی غیرمجاز به اطلاعات هست و وقتی confidentiality رعایت شود مهاجم نمیتواند به اطلاعات محرمانه دسترسی داشته باشد.
- disruption : این تهدید دقیقا در مقابل معنای availability قرار میگیرد و به معنای قطع دسترسی به سرویس یا منابع است پس اگر هرلحظه availability تضمین شود این دسته حملات نمیتوانند کاری از پیش ببرند.
- deception : به معنای پذیرش دیتاهای غلط توسط قربانی است و اگر Integrity رعایت شود هم صحت اطلاعات مورد تایید است هم شخصی که اطلاعات را میدهد احراز هویت شده است.
- usurpation : اگر availability را تضمین کنیم مهاجم نمیتواند بخشی را که در کنترل گرفته را از دسترس کاربران مجاز خارج کند و اگر Integrity نیز رعایت شود دستکاری نیز نمیتواند صورت بگیرد.

5

7. For each of the following statements, give an example of a situation in which the statement is true.

a. Prevention is more important than detection and recovery. → در سیستم های خیلی امنیتی مثل سازمان های اطلاعاتی کشور ها، پیشگیری از حملات و دزدیده شدن اطلاعات، مهم تر از بازیابی یا کشف است.

b. Detection is more important than prevention and recovery. → وقتی هزینه ای که برای یافتن حمله ها باید بشود کمتر از هزینه ی پیشگیری از حملات است، کشف حملات مهم تر است. به طور مثال در سرور وبسایت هایی مثل wikipedia و ... همواره خطر حملات DOS هست و نمیتوان به شکل محسوس از وقوع آنها جلوگیری کرد ولی تشخیص رخدادن حمله به عنوان اولین قدمم بسیار مهم است.

c. Recovery is more important than prevention and detection. → سایتی که اطلاعاتی از کاربران داشته (برای لاگین یا ...) و به هر دلیلی مورد حمله واقع شده و اطلاعات از دیتابیس پاک شده. در این حالت بازیابی مهم تر است.

6

8. Is it possible to design and implement a system in which no assumptions about trust are made? Why or why not? → با توجه به دنیای امروز و اهمیتی که داده ها دارند، برای هیچ سیستمی نمی شود هیچ مورد امنیتی در نظر نگرفت.

7

9. Policy restricts the use of electronic mail on a particular system to faculty and staff. Students cannot send or receive electronic mail on that host.Classify the following mechanisms as secure, precise, or broad.

a. The electronic mail sending and receiving programs are disabled. → **Secure**

b. As each letter is sent or received, the system looks up the sender (or recipient) in a database. If that party is listed as faculty or staff, the mail is processed. Otherwise, it is rejected. (Assume that the database entries are correct.) → **Precise**

c. The electronic mail sending programs ask the user if he or she is a student. If so, the mail is refused. The electronic mail receiving programs are disabled. → **Broad**

8

14. A respected computer scientist has said that no computer can ever be made perfectly secure. Why might she have said this? → به این دلیل که سیستم های کامپیوتری نه هر روز بلکه هر ساعت به روز می شوند و هر بار حملات و آسیب پذیری های جدید تری رخ میدهد و هیچ گاه نمی توان گفت سیستمی کاملا امن است.

9

17. The police and the public defender share a computer. What security problems does this present? Do you feel it is a reasonable cost-saving measure to have all public agencies share the same (set of) computers? → با نفوذ به یکی کار دیگری نیز تمام است و به نوعی single point of failure داریم. این که این روش cost-saving است صحیحه ولی با توجه به نکته فوق و ریسک بالای آن روش معقولی نیست.

10

20. For many years, industries and financial institutions hired people who broke into their systems once those people were released from prison. Now, such a conviction tends to prevent such people from being hired. Why do you think attitudes on this issue changed? Do you think they changed for the better or for the worse? → این مجرم ها به دلیل مهارتی که دارند استخدام می شوند چون کسانی هستند که توانسته اند به برترین سیستم های امنیتی نفوذ کنند. اما به قاطعیت نمی شود گفت استخدام این ها خوب است یا نه. از طرفی نیروهای ماهری هستند و از طرف دیگر، جرم کرده اند و ممکن است به هر دلیلی دوباره مرتکب آن بشوند.