دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

Department of
Computer Engineering

به نام خداوند جان و خرد

تمرین تحویلی اول

درس مبانی امنیت اطلاعات

امیرفاضل کوزه گر کالجی

۹۹۳۱۰۹۹

سوال اول:

- امنیت به طور غیر رسمی، عبارت است از حفاظت در برابر آنچه برای ما ارزشمند است. (چه در برابر حملات عمدی و چه در برابر حملات غیر عمدی)
- سازمان NIST، امنیت را به صورت زیر تعریف کرده است:
  - حفاظت از سیستم های اطلاعاتی به منظور حفظ **صحت**، **دسترسی پذیری**، و **محرمانگی** مربوط به منابع سیستم. سیستم ها می‌توانند شامل سخت افزار، نرم افزار،firmware، داده ها و اطلاعات و ارتباطات باشند.
- از طرف دیگر در کتاب network security essentials، computer security، به شکل زیر تعریف شده است:
  - "حفاظتی که به یک سیستم اطلاعاتی داده می‌شود، به منظور دست‌یابی به یک سری اهداف قابل اجرا، از جمله، صحت، در دسترس بودن، و محرمانگی منابع اطلاعات" همانند مورد قبل.

سوال دوم:

حمله، یک اقدام یا تلاش برای نقض امنیت است. با این‌حال، تهدید، یک عامل بالقوه برای نقض امنیت است و شامل هیچ گونه عملی نمی‌شود. از طرف دیگر، آسیب پذیری نیز، به معنی وجود یک ضعف درون خود سیستم ما است که ممکن است از آن سو استفاده شده و امنیت سیستم نقض شود.

سوال سوم:

حملات غیرفعال :: در این گونه حملات، اطلاعاتی از سیستم جمع آوری نمی‌شود.

حملات فعال :: حملاتی که در آن سعی می‌شود منابع یا رفتار سیستم تغییر کند.

به‌نظر من، تشخیص حملات غیرفعال، سخت تر می‌باشد. زیرا که تاثیری روی سیستم ایجاد نمی‌کنیم و کسی به تغییر نحوه کارکرد سیستم توجهی نمی کند و شخص حمله کننده، می تواند به طور پنهان و دور از ایجاد سر و صدا، شنود اطلاعات کند.

سوال چهارم:

حملات غیر فعال	حملات فعال
شنود	جعل هویت
	تکرار
	منع سرویس
	دستکاری

در حمله شنود، فقط داده های رد و بدل شده دریافت می‌شوند.

اما در دیگر نوع از حملات، شخص مهاجم درون سیستم ارتباط اطلاعات، دست می برد و به وضوح تغییراتی را در روند اجرای آن اعمال می‌کند.

سوال پنجم:

به وضوح مشخص است که privacy، جامع ترین موضوع نامبرده است زیرا که تمام هدف و تلاش این درس حول این موضوع می‌چرخد.

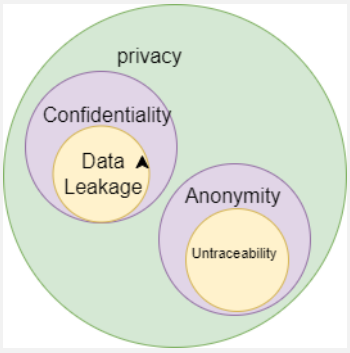
در ادامه محرمانگی یا confidentiality را داریم که یکی از زیرمجموعه های کلیدی privacy حساب می‌شود.

Data leakeage به نوعی از زیرشاخه های محرمانگی محسوب می‌شود. این مورد به لو رفتن اطلاعات به صورت عدم احراز هویت شده یا اتفاقی می‌پردازد.

یکی دیگر از زیرمجموعه های privacy، ناشناس ماندن یا anonymity می‌باشد.

Untracebility یا داشتن قابلیت عدم رهگیری، از زیرمجموعه های ناشناس ماندن است.

به طور بصری، می‌توان پاسخ این سوال را به شکل زیر نمایش داد:



سوال ششم:

در DES، جایگشت ها، جایگشت های گسترشی، حایگشت های انتخابی، چرخش کلید و جایگشت انتخاب کلید، به صورت یکسان و بدن توجه به ورودی خود رفتار می‌کنند. یعنی، برایشان مهم نیست ورودی، خود ورودی باشد یا بیت تکمیل شده آن(bitwise complement). پس اگر ورودی را در ابتدا، یک بیت مکمل کنیم، در انتها نیز، خروجی یک بیت مکمل خواهد شد.

حال، جایگشت گسترشی یا expansion permutation ، را به صورت یک تابع با نام EP() در نظر خواهیم گرفت. از کلید، چشم پوشی خواهیم کرد(در ادامه خواهیم دید چرا):

می‌خواهیم ثابت کنیم EP(A') = EP'(A)

می دانیم که A' = A XOR ۱

و برای XOR کردن دو متغیر داریم:

A XOR B = 1 XOR A XOR 1 XOR B = A' XOR B'

پس اگر C خروجی EP(A, K) باشد، لزوما خروجی EP(A', K') نیز معادل C می‌شود و در مرحله جایگشت،

هیچ کدام از ورودی و کلید، مکمل نمی‌شوند.