جزوه درس فناوری اطلاعات (IT)

دبیرستان دوره اول سینا

اردیبهشت ۱۴۰۰

۱- امنیت چیست و چرا امنیت اطلاعات برای ما اهمیت دارد ؟

امنیت به (طور غیر رسمی) عبارتست از حفاظت از آنچه براي ما ارزشمند است. از آنجایی که اطلاعات ذخیره شده در دیوایس های ما (تلفن همراه هوشمند، تبلت، کامپیوتر و ...) از اهمیت بالایی برخوردار هست، امن نگه داشتن آن نیز برای ما دارای اهمیت می باشد.

۲- اقدامات امنیتی شامل چه مواردیست ؟ فقط نام ببرید.

پیشگیری، ردیابی، واکنش

۳- منظور از پیشگیری (Prevention) در اقدامات امنیتی چیست ؟

پیشگیری از بروز حملات امنیتی به منظور جلوگیری از خسارت وارد شده به سیستم را پیشگیری گویند.

۴- منظور از تشخیص (Detection) در اقدامات امنیتی چیست ؟

پس از بروز حمله امنیتی نوبت به مرحله ی تشخیص می باشد، تشخیص در اقدامات امنیتی شامل بررسی میزان خسارت، هویت دشمن و کیفیت حمله از نظر زمان، مکان، دلایل حمله، نقاط ضعف و ... می باشد.

۵- منظور از واکنش (Reaction) در اقدامات امنیتی چیست ؟

به اقداماتی که موجب بازیابی و جبران خسارات و جلوگیری از حملات مجدد توسط نفوذگران به سیستم شود واکنش گویند.

۶- تفاوت برقرار کردن امنیت اطلاعات از گذشته تا به امروز دچار چه تحولاتی شده است ؟

امنیت اطلاعات در گذشته امنیت با حضور فیزیکي و نظارتي تامین میشد، به این منظور که اطلاعات به صورت فیزیکی در اتاقی امن با وجود موارد امنیتی مانند انواع قفل ها، حفاظ ها و نگهبانان امن می بود.

اما در دنیای نوین امروزه، امنیت اطلاعات توسط سیستم های امنیتی در کامپوتر ها و شبکه با استفاده از ابزارهای خودکار و مکانیزم های هوشمند براي حفاظت از داده ها استفاده می شود.

۷- چرا با وجود پیشرفت تکنولوژی در سال های جدید آمار حملات امنیتی نیز بیشتر شده است ؟

با رشد تکنولوژی و بیشتر شدن ابزار های برنامه نویسی، ایجاد حملات امنیتی برای افراد تازه کار نیز ممکن شده است چرا که این ابزار ها کار را ساده تر کردند و استفاده از آن ها (برخلاف گذشته) نیاز به دانش برنامه نویسی پیشرفته ای ندارد، از این رو حفظ امنیت در تمام سطوح مورد اهمیت است.

۸- مفاهیم زیر را تعریف کنید.

حمله (Attack): تلاش عمدي براي رخنه در يك سيستم يا سوء استفاده از آن.

رخنه (Breach) : نقض سياست امنيتي يك سيستم(منظور از سیاست امنیتی بایدها و نبایدهای سیستم است).

نفوذ (Intrusion) : فرايند حمله و رخنه ناشي از آن

آسيب‌پذيري (Vulnerability) : هر گونه نقطه ضعف در طراحی، پیاده سازی، پیکربندی و اجرا یک سیستم که بتوان از آن سوء استفاده کرد و سیاستهای امنیتی آن سیستم را نقض کرد.

هک (Hack): در واقع به معني نفوذ به سيستم و جستجو در آن به منظور كشف حقايق و نحوه كار آن سيستم است.

سیاست امنیتی (Security Policy): تعیین می کند که از جنبه امنیتی چه کارهایی مجاز و چه کارهایی غیرمجاز است.

مکانیزم امنیتی (Security Mechanism): روش در نظرگرفته شده براي تشخيص، پيشگيری و واكنش به حملات امنيتی

۹- سرویس های امنیتی شامل چه مواردی هستند ؟ توضیح دهید.

حفظ صحت داده (Integrity) : اطمینان از اینکه آنچه رسیده (پیام) بدون دستکاری بوده و دقیقا پیامی است که فرستنده ارسال کرده است.

حفظ محرمانگي داده‌ها (Confidentiality) : اطمینان از اینکه تنها کاربران مورد نظر (فرستنده و گیرنده) قادر به مشاهده پيام ها مي باشند.

هویت شناسی، احراز هویت (Authentication) : اطمینان از این که کاربر همانی است که ادعا می کند. (هویت فرستنده مورد تایید می باشد)

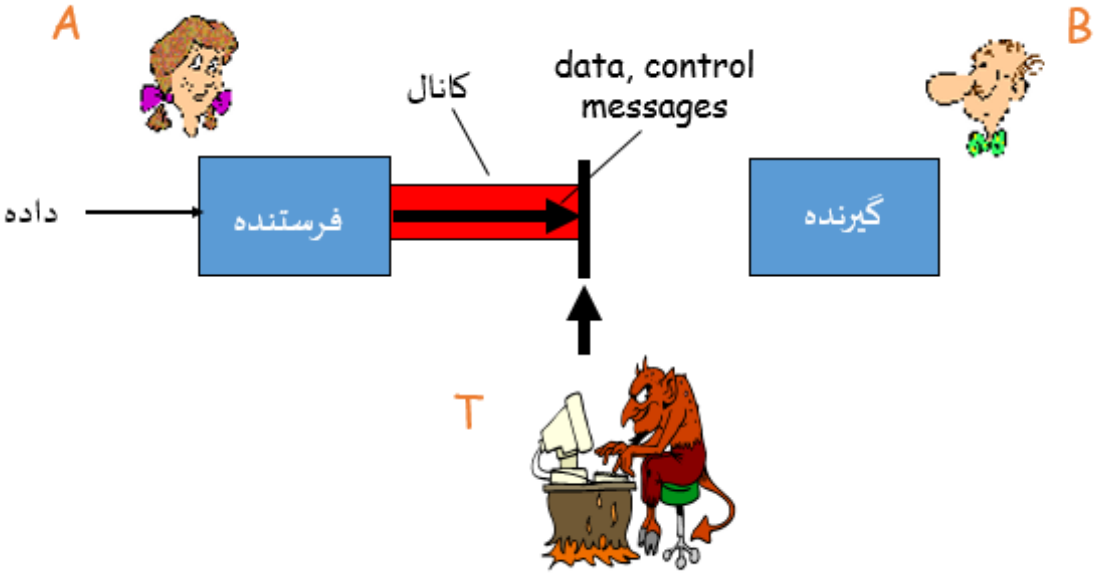
مجازشناسی (Authorization) : کاربر تنها به امکانات مشخص شده ی خود حق دسترسی دارد.

عدم‌انکار (Non-repudiation) : اطمینان از اینکه دریافت یا ارسال پیام توسط گیرنده و فرستنده قابل انکار نباشد.

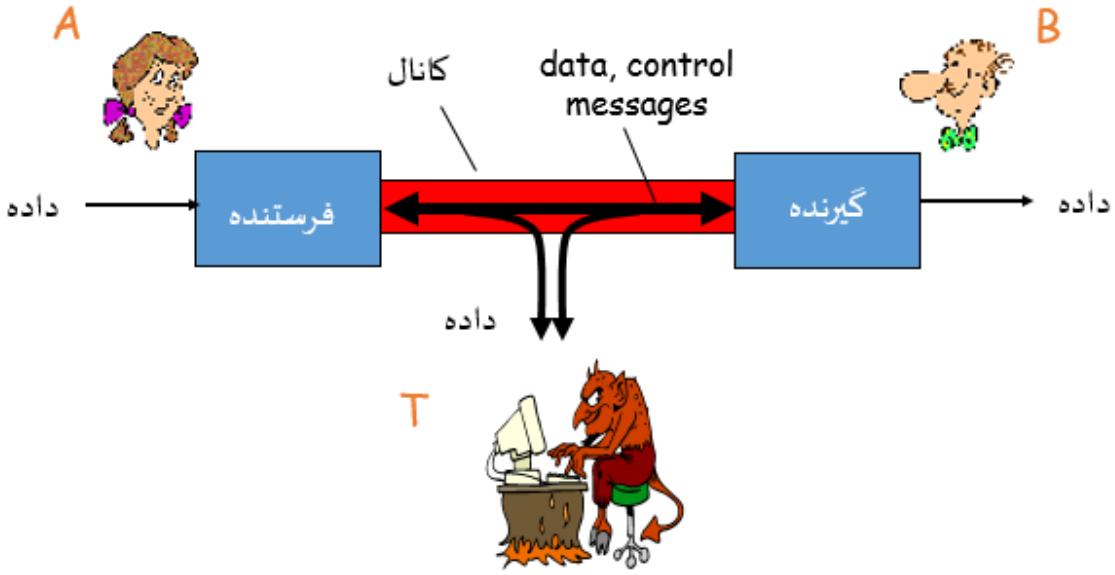
دسترس پذیری (Availability) : در دسترس بودن سرویس مد نظر برای انجام کار کاربران

۱۰- انواع حملات بر حسب نحوه عملکرد را نام برده و توضیح دهید.

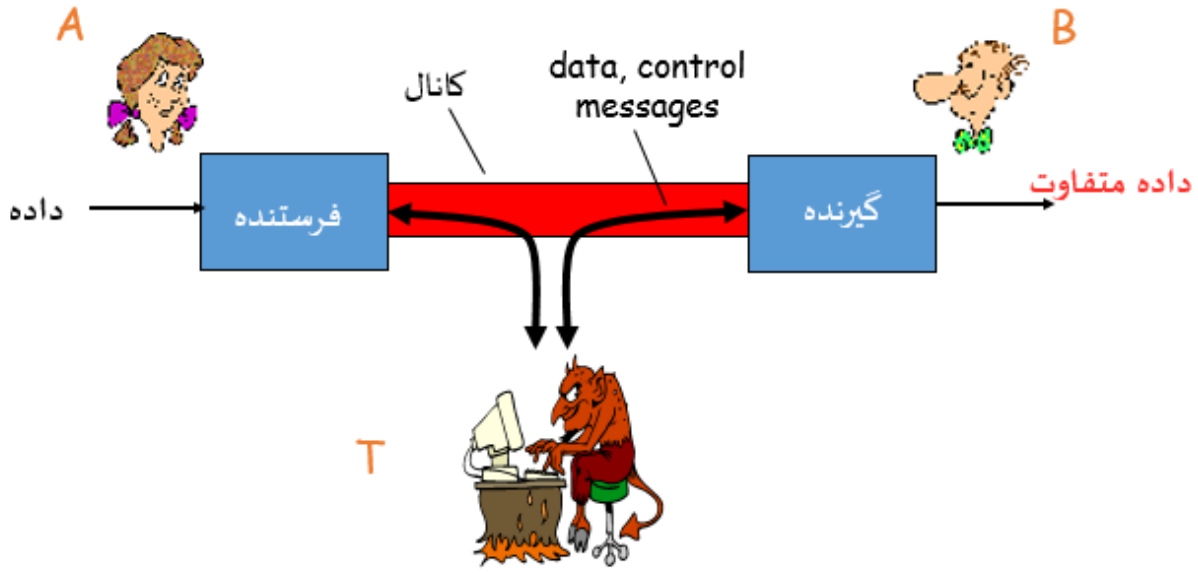
وقفه (Interruption) : اختلال در شبکه و سرویس ارتباطی



شنود (Interception) : استراق سمع ارتباطات شخصی یا مخفی سایرین



دستکاري داده‌ها (Modification) : تغییر غیرمجاز داده‌های ارسالی و یا دریافتی



جعل اطلاعات (Fabrication) : ارسال داده توسط کاربران غیرمجاز با جعل هویت کاربران مجاز