امنیت اطلاعات

فصل اول

مفاهیم امنیت اطلاعات

مقدمه

- ضرورت برقراری امنیت اطلاعات با توجه به رشد روزافزون به کارگیری فناوری اطلاعات
  - بانکداری الکترونیکی
  - دولت الکترونیکی
    - رای گیری الکترونیکی
  - آموزش الکترونیکی
  - بهداشت الکترونیکی
  - ...

جرایم الکترونیکی

- اولین بار در سال 1988 روبرت موریس اولین کرم کامپیوتری را نوشت
- در سال 1994 کلاهبرداری یک گروه روسی 10/4 میلیون دلار به Citibank ضرر زد
- در سال 1996 وب سایت CIA هک شد!
- در سال 1998 در آستانه جنگ امریکا و عراق دو نوجوان کالیفرنیایی بهمراه مربی 18 ساله اسراییلی خود به سیستم رایانه ای پنتاگون حمله کردند!
- پس از سال 2000 هرسال بیش از یک میلیون حمله امنیتی

انواع رخدادهای ناخوشایند برای اطلاعات:

- دسترسی غیرمجاز به داده ها
- افشای اطلاعات محرمانه
- از دسترس خارج شدن خدمات یک سرویس دهنده
- تغییر مخفیانه در داده ها
- سرقت داده ها
- نابود شدن داده ها
- جعل داده ها
- اختلال در عملکرد صحیح ماشین کاربران
- و هر نوع تعرض به حریم داده های یک ماشین

امنیت داده ها

- امنیت داده ها عبارتست از مجموعه تمهیدات و روش هایی که در یکی از بندهای زیر قرار گیرد:
  - تمهیداتی که اطمینان می دهند رخدادهای ناخوشایند هرگز اتفاق نمی افتند
  - تمهیداتی که احتمال وقوع رخدادهای خطرناک را کم می کند
  - تمهیداتی که نقاط حساس و استراتژیک را در سطح شبکه توزیع می کند
  - تمهیداتی که اجازه می دهند به محض وقوع رخدادهای خطرناک، شرایط در اسرع وقت و با کمترین هزینه به شکل عادی برگردد.

تمهیدات امنیتی، شمشیر دولب!

- هرچه تمهیدات امنیتی دقیق تر و مفصل تر اجرا شوند:
  - دسترسی افراد مجاز به منابع شبکه دشوارتر و دست و پاگیرتر می شود
  - هزینه پیاده سازی و نگهداری سیستم را بالا می برد.
- پس تمهیدات امنیتی در هر سیستم باید به قدر لازم باشد

اصطلاحات امنیتی

- تهدید امنیتی (Security Threat)
  - هر عامل که بطور بالقوه بتواند منجر به رخدادی خطرناک شود
    - تهدیدهای طبیعی
    - تهدیدات غیر عمدی
    - تهدیدات عمدی : هرگونه اقدام برنامه ریزی شده جهت افشا ، نابودی یا تغییر در داده های حیاتی شبکه یاایجاد اختلال در خدمات معمول سرویس دهنده ها
- حمله (Attack)
  - هرگاه یک تهدید عمدی از حالت بالقوه به حالت بالفعل درآید ، یک حمله رخ داده است.

اصطلاحات امنیتی(ادامه)

- آسیب یا خسارت (Harm)
  - اثرات احتمالی ناشی از یک حمله مانند دستکاری یا از بین رفتن منابع شبکه.
- نقطه آسیب پذیر (Vulnerability)
  - هرگونه ضعف یا اشکال یک مولفه از سیستم در مقابل تهدیدات احتمالی که بتواند منجر به حمله شود.
- میزان خطر (Risk)
  - تخمینی از احتمال وقوع یک حمله

اصطلاحات امنیتی(ادامه)

- مکانیزم امنیتی (Security Mechanism)
  - هر روش یا الگوریتمی که برای تشخیص یا پیشگیری از وقوع حمله یا برگشت به وضعیت معمولی (پس از وقوع حمله) طراحی می شود
    - هیچ مکانیزم واحدی که بتواند امنیت داده ها را کاملاً تضمین کند وجود ندارد
- سرویس های امنیتی (Security Services)
  - پیاده سازی هرنوع مکانیزم امنیتی و ارائه آن به کاربران بطوری که میزان خطر (Risk) را به حداقل برساند.

سرویس های امنیتی

- محرمانگی (Confidentiality)
- احراز هویت (Authentication)
- جامعیت (Integrity)
- عدم انکار (Non-Repudiation)
- کنترل دسترسی (Access Control)

سرویس های امنیتی- محرمانگی

- مجموعه مکانیزمهایی که تضمین می کند داده های مهم کاربران از دسترس افراد بیگانه دور نگاه داشته شود

- محرمانگی دو جنبه دارد
  - محرمانگی محتوای داده ها
  - محرمانگی ترافیک

سرویس های امنیتی- احراز هویت

- مجموعه مکانیزمهایی که این امکان را فراهم می کند که بتوان مبداء (صاحب) واقعی یک پیام ، سند یا عملیات را بدون هیچ تردیدی مشخص کرد

- احراز هویت دو جنبه مهم دارد
  - احراز هویت پیام
  - احراز هویت کاربر

سرویس های امنیتی- جامعیت داده ها

- مجموعه مکانیزمهایی که از هرگونه تحریف، دستکاری، تکرار یا حذف داده ها پیشگیری می کند یا حداقل باعث کشف چنین اقداماتی می شود

سرویس های امنیتی – عدم انکار

- مجموعه مکانیزمهایی که باعث می شود فرستنده و گیرنده پیام نتوانند بترتیب ارسال و دریافت پیام را انکار کنند.

  - عدم انکار مبدا
  - عدم انکار مقصد

سرویس های امنیتی- کنترل دسترسی

- مکانیزمهایی که دسترسی به کوچکترین منابع اشتراکی شبکه را تحت کنترل در آورده و هر منبع را بر اساس سطح مجوز کاربران در اختیار آنها قرار می دهد.

حملات امنیتی

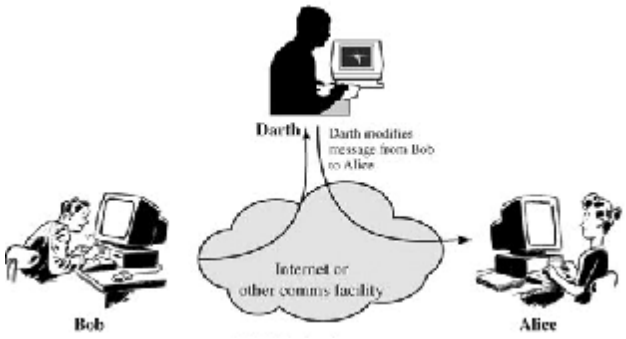
- استراق سمع (Interception)
- تغییر داده ها (Modification)
- جعل (Fabrication)
- وقفه (Interrruption)

حملات امنیتی – استراق سمع

- شخص غیرمجاز نسخه ای از داده های در حال جریان بین مبدا و مقصد را به نفع خود شنود کند

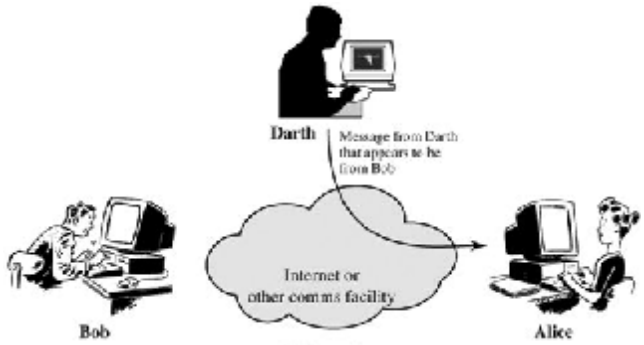
حملات امنیتی- تغییر داده ها

- داده های در حال جریان بین مبدا و مقصد توسط شخص غیرمجاز به هر نحوی دستکاری یا تحریف شوند.



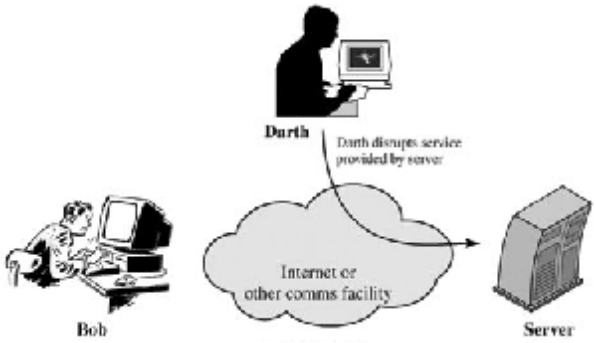
حملات امنیتی - جعل

- شخص غیرمجاز اقدام به تولید پیام ساختگی کرده و ارسال آنرا به شخص مجاز دیگری نسبت می دهد



حملات امنیتی - وقفه

- کسی بتواند سیستم یا سرویسی را در شبکه از کار بیندازد



دسته بندی حملات امنیتی

- حملات فعال
  - در جریان طبیعی انتقال اطلاعات از مبدا به مقصد تغییر ایجاد می کنند
    - جعل، تغییر، وقفه
- حملات غیر فعال
  - در جریان طبیعی انتقال اطلاعات از مبدا به مقصد تغییر ایجاد نمی کنند
    - استراق سمع