بسم الله الرحمن الرحیم

مبانی رایانش امن

جلسه ۲

مجتبی خلیلی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان

امنیت (کامپیوتر) چیست؟

برقراری ویژگی‌ها یا اهدافی مشخص در یک سیستم،
با ملاحظاتی و با فرض وجود مهاجم

درباره امنیت

IUT-ECE

Mojtaba Khalili

امنیت، یک زنجیره است. ضعیف‌ترین اتصال، تعیین می‌کند چقدر امن هستیم.

مفاهیم پایه

◄ آسیب‌پذیری‌ها (Vulnerabilities):

نقطه ضعف‌های سیستم که ممکن از آنها برای ضربه زدن به سیستم استفاده شود. مثل احراز اصالت نشدن برای ورود به سیستم گلستان، پیاده سازی غلط یک پروتکل

◄ تهدید (Threat):

موقعیت یا شرایطی که پتانسیل ضربه زدن و ایجاد خسارت به دارایی‌های سیستم را دارد (هر چیزی که پتانسیل برهم زدن امنیت ما را دارد). مثلا تهدیدات طبیعی یا خطای انسانی یا خطر لو رفتن اطلاعات گلستان توسط یک فرد غیرمجاز

مفاهیم پایه

- حمله (Attack):

هر عملی برای بهره‌برداری از آسیب‌پذیری‌های سیستم به منظور اجرای یک تهدید. وارد سیستم گلستان دوستتان شده و اطلاعات او را ببینید/تغییر دهید.

فرد حمله کننده را attacker گوییم.

اگر حمله موفق باشد، گوییم یک compromise رخ داده است.

مهاجم/حمله کننده

- حمله کننده باید موارد زیر را داشته باشد:
  - ابزار: اغلب دسترسی به اینترنت کافیه!
  - شانس و فرصت: وجود آسیب پذیری در سیستم
  - انگیزه: ممکن است بسیار پیچیده باشد طوریکه ندانیم.

انگیزه مهاجم

- چالش فکری یا حس برتری
  - برای برخی شبیه بازی است. پیشنهاد به این افراد : CTF
- جاسوسی (دولتها یا شرکتها)
- مالی (رمز کارت اعتباری)
- انتقام (دزدیدن اطلاعات شخصی و باجگیری)
- نمایش قدرت (هک کردن یک سایت دولتی معروف)

پیامد حملات

- اعتبار و آبرو
- ضررهای مالی
- عواقب قانونی و حقوقی
- لو رفتن اطلاعات حساس سازمان
- عدم اعتماد مشتریان

مفاهیم پایه

- دفاع (Defence):

حذف یا کاهش آسیب‌پذیری‌ها. هدف ما نیز همین امر است که با شناخت تهدیدات و آسیب‌پذیری‌ها حاصل می‌شود.

- چگونه در مقابل تهدیدات دفاع کنیم؟

مفاهیم پایه

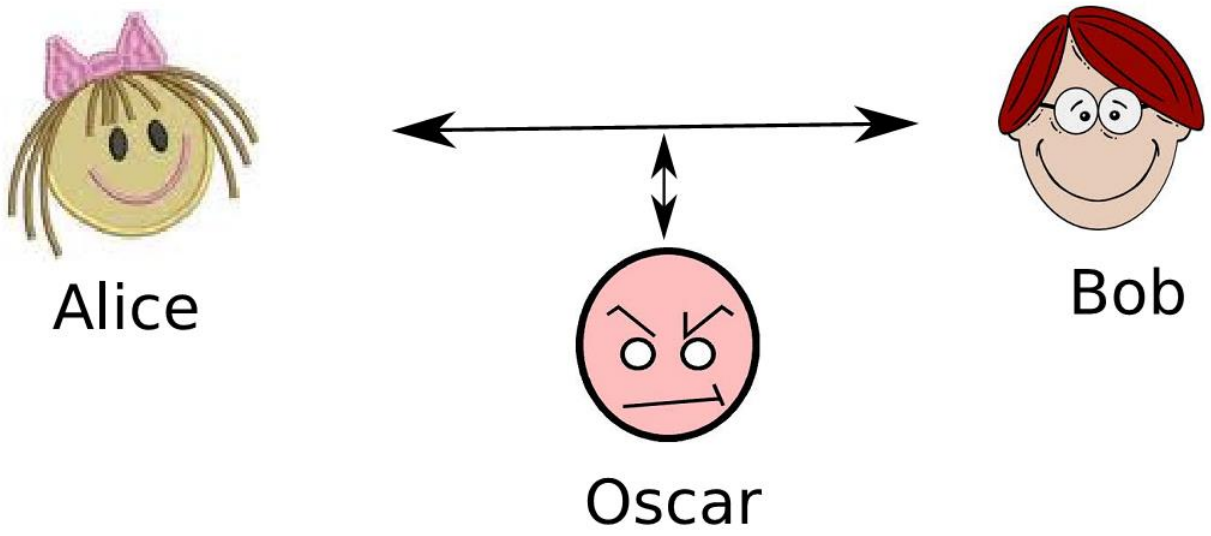
- برقراری ویژگی‌ها یا اهدافی مشخص؟

- منظورمان از ویژگی یا اهداف چیست؟

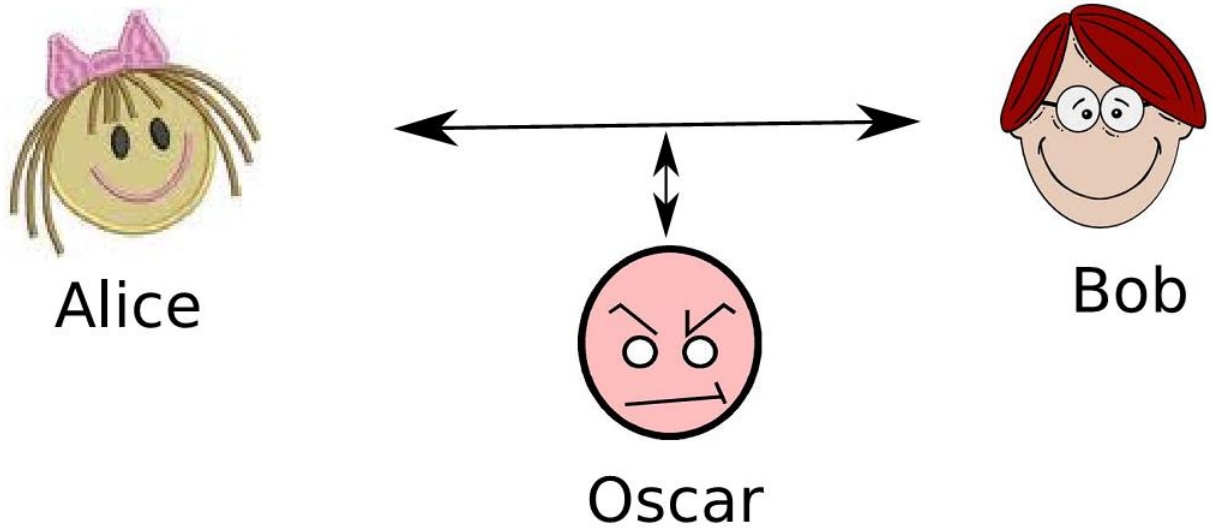
- خط مشی (policy): یک سیاست بیان می‌کند چه چیز مجاز و چه چیز غیرمجاز است.
- بعد از آن است که به سراغ ابزار و تکنیک ها میرویم.

مفاهیم پایه

- برقراری ویژگی‌ها یا اهدافی مشخص؟



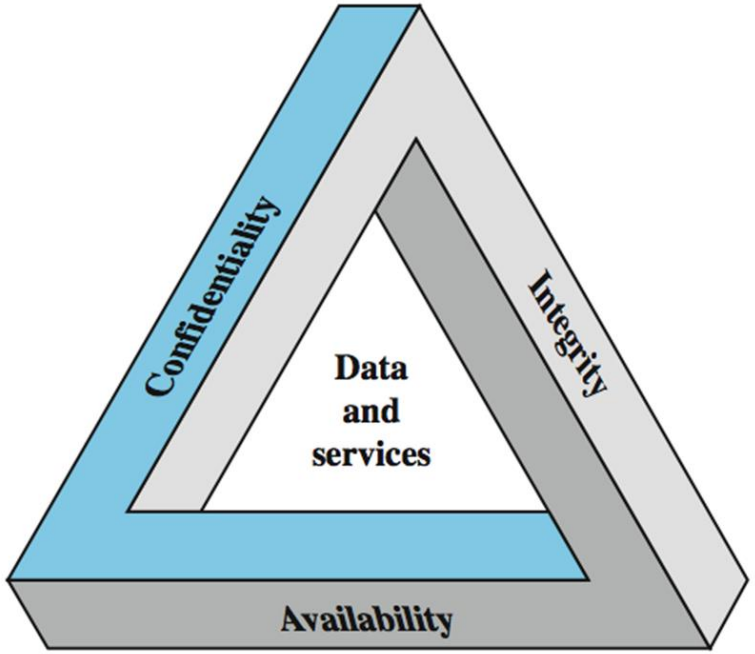
مفاهیم پایه



- حملات غیرفعال (Passive): نگاه میکند اما دست نمیزند؛ مثل شنود، تحلیل ترافیک
- حملات فعال (Active): نقاب‌زنی، جعل هویت، منع سرویس، تغییر پیام و ...

مفاهیم پایه

- برقراری ویژگی‌ها یا اهدافی مشخص؟



اهداف امنیتی

- در بحث‌های ما، در حالت کلی امنیت سه مورد را در بر میگیرد:

- **محرمانگی (Confidentiality)**: دسترسی به سیستم یا داده فقط به افراد مجاز داده شود.
- **صحت (Integrity)**: داده‌ای که دریافت می‌کنید، داده 'درست' باشد.
- **دسترس‌پذیری (Availability)**: به عنوان یک کاربر مجاز، هر زمان که خواستید به داده یا سیستم دسترسی داشته باشید.

اهداف امنیتی

- علاوه بر سه مورد گفته شده، دو هدف دیگر نیز روز به روز مهمتر میشوند:

- **احراز اصالت (Authentication)**: اینکه طرف مقابل همانی است که ادعا می‌کند.

- **انکارناپذیری (Non-repudiation)**: هیچ کس نتواند کاری که در شبکه انجام داده است را انکار کند.

مفاهیم پایه

- پس از تعیین خط مشی:

- راهکارها (mechanism): روش یا ابزاری برای اجرایی کردن سیاست‌ها (امضای دیجیتال، پروتکل احراز اصالت، استفاده از پسورد و ...)
- سرویس امنیتی (security service): بکار گرفتن راهکارهای امنیتی برای مقابله با حملات (سرویس احراز اصالت، محرمانگی داده، کنترل دسترسی، انکارناپذیری و ...)

انواع اطلاعات

- اطلاعات در یکی از سه شکل زیر هستند:
  - ذخیره شده: اطلاعاتی که در حافظه انسان، کاغذ یا کامپیوتر ذخیره شده اند.
  - در حال ارسال: به صورت فیزیکی یا الکترونیکی
  - در حال پردازش: به صورت فیزیکی یا الکترونیکی

اقدامات متقابل امنیتی در برابر حملات

- پیشگیری (Prevention)
- تشخیص (Detection)
- بازیابی (Recovery)

اقدامات متقابل امنیتی در برابر حملات

- پیشگیری:
  - هر فرد برای ورود به سیستم نیاز به احراز اصالت داشته باشد (Authentication)
  - دیواره آتش (Firewall)
  - رمزنگاری (Encryption, Signature, ...)
  - و ...

اقدامات متقابل امنیتی در برابر حملات

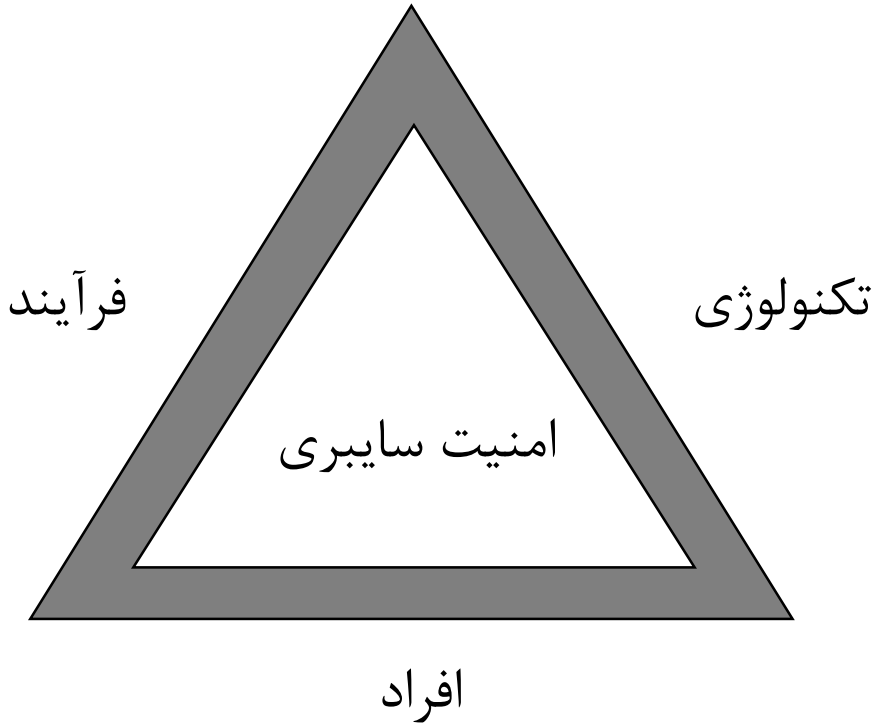
- تشخیص:
  - سیستم تشخیص نفوذ (IDS)
  - سیستم تله عسل (Honeypot)
  - و ...

اقدامات متقابل امنیتی در برابر حملات

- بازیابی:
  - سیستم‌ها و مکانیزم‌های پشتیبان‌گیری

مفاهیم پایه

- امنیت سایبری مسئله‌ای نیست که تنها با تکیه بر تکنولوژی قابل حل باشد بلکه شامل سه ضلع تکنولوژی، فرآیند و افراد است.



امنیت سیستم