دانشکده علوم ریاضی و آمار

مدرس: دکتر مجتبی رفیعی

نیمسال دوم ۱۴۰۰-۱۴۰۱

رمزنگاری

جلسه ۳ رمزنگاری

نگارنده: صبا عبدی

۲۷ بهمن ۱۴۰۰

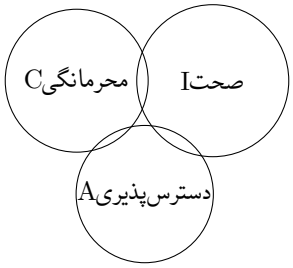
فهرست مطالب

۱ مفهوم سه گانه امنیت

در امنیت اطلاعات، تمامی ویژگی های امنیتی (از جمله ویژگی‌های ذکر شده در مباحث قبلی) در یک مفهومی برنامه سه گانه امنیت (Security Triad) خلاصه می‌شود:

- محرمانگی (Confidentiality)، عدم افشای غیرمجاز داده ها،
- صحت یا جامعیت (Integrity)، عدم دستکاری دادهها توسط افراد یا نرم افزارهای غیرمجاز،
- دسترس پذیری (Arailability)، دسترسی به دادهها توسط افراد مجاز در هر مکان و در هر زمان.

که به طور معمول به سه گانه امنیت CIA معروف است.



نکته: جنس دسترس‌پذیری متفاوت از جنس محرمانگی و صحت است و بیشتر مباحث تکنیکی و فنی مدنظر هست برخلاف محرمانگی و صحت که نیازمند عمق نظری است.

۲ مکانیزم های امنیتی

برای تامین ویژگی های امنیتی ذکر شده در بالا، نیازمند بهره گیری از مکانیزم ها (یا ساز و کارهای) امنیتی هستیم. این مکانیزم‌ها در ادامه آورده شده‌اند و بهتر است.
برای فهم کامل آنها به طور همزمان معادل فضای فیزیکی و فضای سایبری آن را در نظر بگیرید.

* مکانیزم های هشداردهنده
  - فضای فیزیکی: نصب تابلو، حفاظت
  - فضای سایبری: پیام هشدار و...
* مکانیزم های پیشگیرانه:
  - فضای فیزیکی: دیوارکشی، قفل و کلید
  - فضای سایبری: رمز کردن داده، کنترل دسترسی، دیواره آتش (firenall)
* مکانیزم های تشخیصی:
  - فضای فیزیکی: دوربین، دزدگیر، نگهبان.
  - فضای سایبری: نظارت مداوم سامانه، حسابرسی و...
* مکانیزم‌های ترمیم و بازیابی
  - فضای فیزیکی: بیمه کردن خانه و...
  - فضای سایبری: نسخه های پشتیبان و...

در این درس به مکانیزم های امنیتی پیشگیرانه و تشخیص که بیشتر تمرکزشان روی مفاهیم رمزنگاری است، می پردازیم. با این حال سعی می‌شود دیگر ابزارهای امنیتی نیز با توجه به محدودیت زمانی نیمسال تحصیلی، تا حد مناسبی پوشش داده شود.

۳ تعریف غیررسمی امنیت

یک تعریف غیررسمی از امنیت که در فضای سایبری و فضای فیزیکی مطرح است:

"امنیت عبارت است از حفاظت دارایی‌های ما در برابر حملات (Attack) عمدی (Intentional) یا نفوذ (Intrusion) غیرعمدی (Unintentional)".

در ادامه نمونه‌هایی ازدارایی‌های در محیط‌های مختلف آورده شده است.

- دارایی در محیط فیزیکی (Physical space): ایده و نوآوری تولید یک محصول، املاک، پول و...
- دارایی در محیط سایبری (Cyber space): در قالب داده (Data) است و می تواند همه دارایی های فیزیکی را در خود جای دهد.

۴ امن

واژه امن (Secure) در ریشه به معنی چیزی است که "نیاز به مراقبت ندارد". به عبارت دیگر، در گذشته وقتی چیزی امن فرض می شد بدین معنا بود که دیگر نیاز به مراقبت و توجه ندارد. در واقع امنیت به صورت "تنظیم کردن و فراموش کردن" set and forget در نظر گرفته می‌شد.

۵ امنیت اطلاعات سنتی در مقابل امنیت اطلاعات در دنیای نوین

- سنتی:
  ۱ نگهداری اطلاعات در قفسه‌های قفل‌دار،
  ۲ نگهداری قفسه ها در مکان‌های امن،
  ۳ استفاده از نگهبان،
  ۴ استفاده از سیستم الکترونیکی نظارت.
- دنیای نوین:
  ۱ نگهداری اطلاعات در کامپیوترها،
  ۲ برقراری ارتباط شبکه‌ای بین کامپیوترها،
  ۳ برقراری امنیت در کامپیوترها و شبکه ها.

۶ ضرورت و اهمیت امنیت

هدف از این بخش آن است که بتوانیم تا حدودی مطالب و منابعی که برای توجیه اهمیت امنیت لازم است را فرا گرفته و بتوانیم در آینده مدیران سازمانها را در این‌باره متقاعد کنیم.
برخی منابع قابل استفاده در این رابطه در ادامه فهرست شده‌اند:

۱ اطلاعات منتشر شده توسط مراکز رسیدگی به حوادث امنیتی (CERT)،
۲ توجیه گذر زمان و افزایش دانش مهاجمان،
۳ شرح و توجیه اهداف حملات:
- رخنه های (Breach) امنیتی در سازمان های با مقیاس های مختلف،
- انواع حوادث امنیتی در سازمانها،
- متوسط هزینه‌های تحمیل شده به سازمان‌ها.

۴ شرح جزئی‌تر برخی حوادث امنیتی که فراوانی بیشتری دارند:

۱ حملات منع سرویس،

۲ توزیع سایت‌های فیشینگ (Fishing)،

۳ توزیع سیستم های آلوده به بدافزار ،

۴ توزیع سایت‌های آلوده ساز .

۵ ذکر جنگ های سایبری (مشابه جنگ های واقعی):

- جنگ عراق و آمریکا در کویت (۱۹۹۱)،
- حمله اسرائیل به تاسیسات هسته‌ای ایران (۲۰۱۰)،
- حمله به وزارت خارجه ایران (۲۰۱۱).

۱.۶ مراکز رسیدگی به حوادث امنیتی (CERT)

CERT که مخفف Computer Emergency Response Team می‌باشد، به گروه‌های تخصصی که برای مدیریت رخدادهای امنیتی است، اطلاق می شود. به طور معمل، این گروه‌ها در دو قالب فعالیت می‌کنند:

- به صورت یک بخش از سازمان و در واقع وابسته به سازمان (سازمانی)،
- به صورت مستقل و در قالب خدمات به دیگر سازمان‌ها (ملی)،

به عنوان مثال مرکز ماهر (مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای)، به عنوان بخشی از سازمان فناوری اطلاعات ایران زیر نظر وزارت ارتباطات و فناوری اطلاعات به عنوان یک CERT در مقیاس کشوری فعالیت می کند.
گزارش‌های ارائه شده توسط این مراکز گویای آن است که حوادث امنیتی به صورت فزاینده‌ای روز به روز در حال افزایش است.
نکته: برخی از نرم افزارهای پر استفاده با مقیاس بالایی از کاربران مثل ویندوز، ممکن است با پیدایش یک باگ امنیتی یا رفع آن، تعداد زیادی از حوادث امنیتی به یکباره به ترتیب افزایش یا کاهش یابد. بنابراین ممکن است یک سال مشخص نسبت به سال مشخص دیگر نوسان محسوسی را از حیث حوادث امنیتی تجربه کند.

۲.۶ گذر زمان و افزایش دانش مهاجمان

رشد تکنولوژی سبب شده تا:

- حجم زیادی از اطلاعات به طور فزآینده‌ای تولید شود،
- ابزارهای تخصصی برای مدیریت و نگهداری و استفاده از داده ها تولید و در دسترس باشد،
- نیازمندی هرچه بیشتر سازمان ها و افراد به یکدیگر برای پیشبرد اهداف خود و در نتیجه تعاملات افزایش یافته است.

همه این موارد سبب شده است تا تهدیدات شکل جدیدی به خود بگیرد. در گذشته به سبب دسترسی محدودتر به داده، ابزارها و ارتباطات، تهدیدات به مراتب کمتری مطرح بود و تنها افراد متخصص امکان نفوذ و حمله داشتند. با این حال، امروزه افراد با دانش کم با بهره‌گیری از ابزارها می توانند به راحتی به سیستم ها حمله و تهدیدات جدی را بر آنها تحمیل کنند.

جمع بندی: افزایش دسترسی به داده + افزایش ابزارها = رشد تهدیدات و حملات