دانشگاه صنعتی شریف
دانشکده مهندسی کامپیوتر

آزمایشگاه امنیت داده و شبکه
http://dnsl.ce.sharif.edu

درس ۱: مفاهیم و تعاریف اولیه

محمد صادق دوستی

فهرست مطالب

- **محتوا و جایگاه درس**
- ضرورت امنیت داده و شبکه
- مفاهیم اولیه
- دشواری برقراری امنیت
- انواع و ماهیت حملات
- خدمات امنیتی
- مدلهای امنیت شبکه

موضوعات تحت پوشش درس – ۱

- مقدمات
  - **درس ۱:** مفاهیم و تعاریف اولیه
  - **درس ۲:** ساز و کارهای تأمین امنیت
- اصول رمزنگاری
  - **درس ۳:** مفاهیم رمزنگاری و رمزنگاری سنتی
  - **درس ۴:** رمزنگاری متقارن (مدرن)
  - **درس ۵:** رمزنگاری نامتقارن (کلید عمومی)
  - **درس ۶:** کدهای تصدیق هویت پیام و توابع درهم‌ساز
  - **درس ۷:** امضای رقمی و زیرساخت کلید عمومی

موضوعات تحت پوشش درس – ۲

- پروتکلهای امنیتی
  - **درس ۸:** طراحی پروتکلهای رمزنگاری
  - **درس ۹:** پروتکل کربروس
  - **درس ۱۰:** امنیت رایانامه
  - **درس ۱۱:** SSL/TLS
  - **درس ۱۲:** IPsec

موضوعات تحت پوشش درس – ۳

- تجهیزات امنیتی
  - **درس ۱۳:** دیوار آتش
  - **درس ۱۴:** سیستم تشخیص نفوذ
- **درس ۱۵:** کنترل دسترسی
- **درس ۱۶:** کنترل دسترسی در سیستم عامل ویندوز
- **درس ۱۷:** ارزیابی امنیتی

سایر دروس امنیتی دانشکده – ۱

- امنیت شبکه پیشرفته (شماره درس: ۸۱۷-۴۰)

☜ الگوریتمهای داخلی دیوار آتش، سیستم تشخیص نفوذ، مقابله با حملات منع خدمت، تشخیص کرم و بات‌نت، تله عسل، مقابله با جاسوس‌افزار، فیشینگ، تحلیل ترافیک، گمنامی، امنیت مسیردهی، مقابله و کشف جرایم رایانه‌ای، امنیت شبکه بیسیم و VoIP

- توسعه امن نرم‌افزار (شماره درس: ۸۷۴-۴۰)

☜ چرخه تولید امن نرم‌افزار (تحلیل، طراحی، پیاده‌سازی، آزمون)، آزمون نفوذ، مهندسی معکوس، قفل شکنی

سایر دروس امنیتی دانشکده – ۲

- امنیت سخت‌افزار (شماره درس: ۸۴۳-۴۰)
  - ☜ حملات فیزیکی و مقاومت در برابر دستکاری، حملات کانال جانبی، اسب تروای سخت‌افزاری
- روشهای صوری در امنیت اطلاعات (شماره درس: ۸۷۳-۴۰)
  - ☜ توصیف، مدلسازی، و وارسی سیستمها و پروتکلهای امنیتی بر مبنای منطق

سایر دروس امنیتی دانشکده – ۳

- امنیت پایگاه داده (شماره درس: ۴۰-۷۳۴)

☜ مدلهای کنترل دسترسی (DAC، MAC، RBAC، ...) طراحی پایگاه داده امن، امنیت پایگاه داده آماری، پرس و جو روی داده رمز شده

- نظریه رمزنگاری (شماره درس: ۴۰-۶۷۵)

☜ مدل‌سازی، تعریف، ساخت و اثبات امنیت ساختارها و پروتکلهای امنیتی مبتنی بر نظریه پیچیدگی

سایر گروههای امنیت اطلاعات در دانشگاه شریف

- دانشکده مهندسی برق – پژوهشکده الکترونیک
  - دکتر عارف (امنیت و نظریه اطلاعات)
  - دکتر اقلیدس (امنیت پروتکل)
  - دکتر سلماسی‌زاده (رمزنگاری)
  - مهندس مهاجری (ریاضی رمز، امنیت پروتکل)
- دانشکده علوم ریاضی
  - دکتر دانشگر (رمزنگاری مبتنی بر نظریه پیچیدگی)
  - دکتر خزایی (رمزنگاری)

فهرست مطالب

- محتوا و جایگاه درس
- **ضرورت امنیت داده و شبکه**
- مفاهیم اولیه
- دشواری برقراری امنیت
- انواع و ماهیت حملات
- خدمات امنیتی
- مدلهای امنیت شبکه

امنیت چیست؟

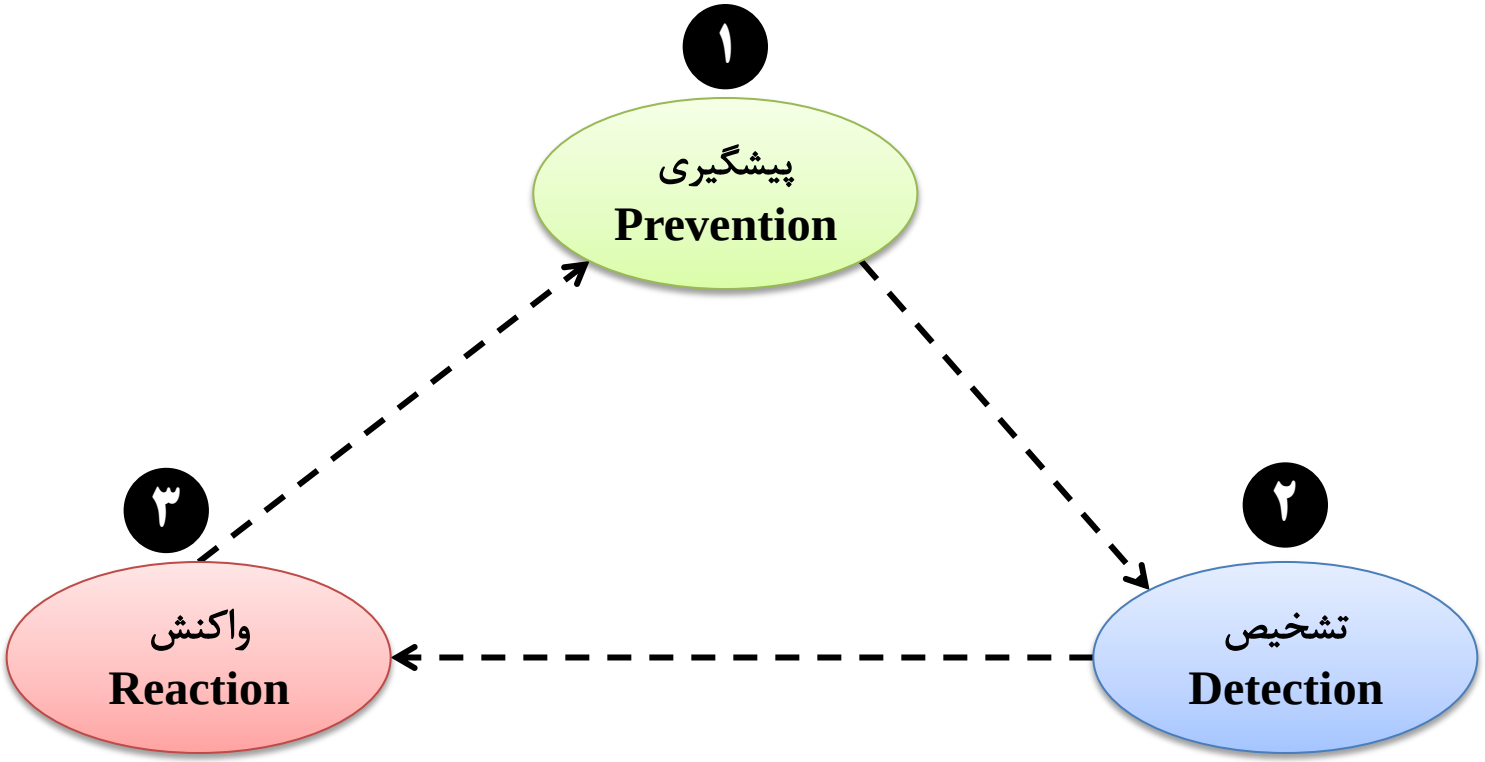
- **به طور غیر رسمی:** امنیت عبارت است از حفاظت از آنچه برای ما ارزشمند است.

- در برابر حملات عمدی
- در برابر نفوذ غیر عمدی

اقدامات امنیتی

- پیشگیری (Prevention)
  - جلوگیری از خسارت
- تشخیص و ردیابی (Detection & Tracing)
  - میزان خسارت
  - هویت دشمن
  - چگونگی حمله (زمان، مکان، دلایل حمله، نقاط ضعف و ...)
- واکنش (Reaction)
  - ترمیم، بازیابی و جبران خسارات
  - جلوگیری از حملات مجدد

اقدامات امنیتی



دو واژه‌ای که امروزه مفهوم متفاوتی دارند (۱)

- secure = se + cure

free from; without — care

- واژه secure در ریشه به معنی چیزی است که «نیازی به مراقبت ندارد».

☜ به عبارت دیگر، در گذشته وقتی چیزی secure می‌شد، آن قدر امن بود که دیگر نیازی به مراقبت و توجه نداشت.

- اما امروز می‌دانیم که برای امنیت، نیاز به توجه و مراقبت دائم است.

☜ امنیت به صورت set and forget **نیست**.

دو واژه‌ای که امروزه مفهوم متفاوتی دارند (۲)

- cryptography = crypto + graphy

hidden writing

امروزه رمزنگاری دیگر صرفاً به «مخفی نویسی» که معادل محرمانگی است نمی‌پردازد؛ بلکه دامنه وسیعی از خدمات را ارائه می‌کند که در این درس با آنها آشنا می‌شویم.

امنیت اطلاعات: گذشته و حال

امنیت اطلاعات سنتی

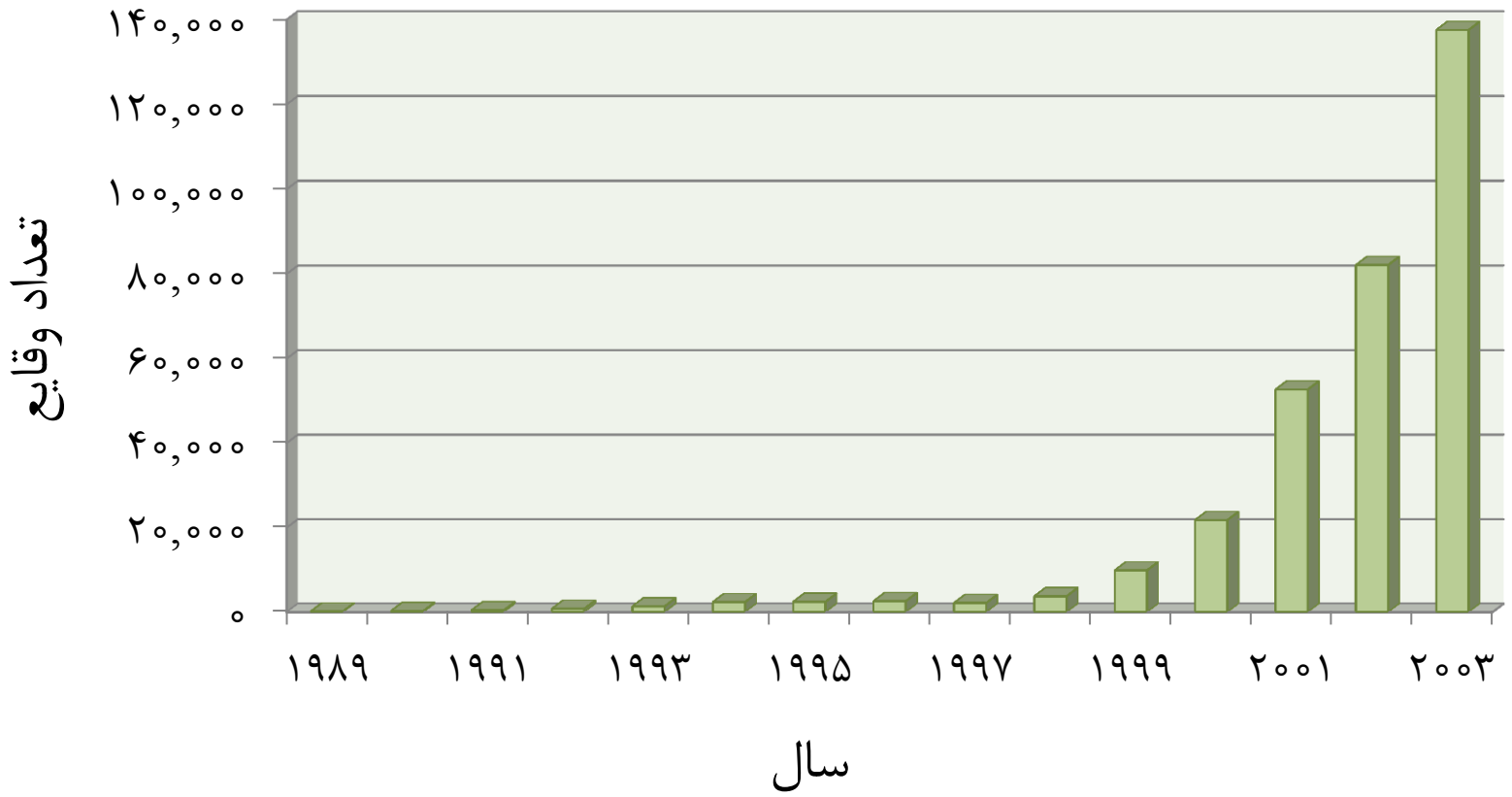
- نگهداری اطلاعات در قفسه‌های قفل‌دار
- نگهداری قفسه‌ها در مکان‌های امن
- استفاده از نگهبان
- استفاده از سیستم‌های الکترونیکی نظارت
- روشهای فیزیکی و مدیریتی

امنیت اطلاعات دنیای نوین

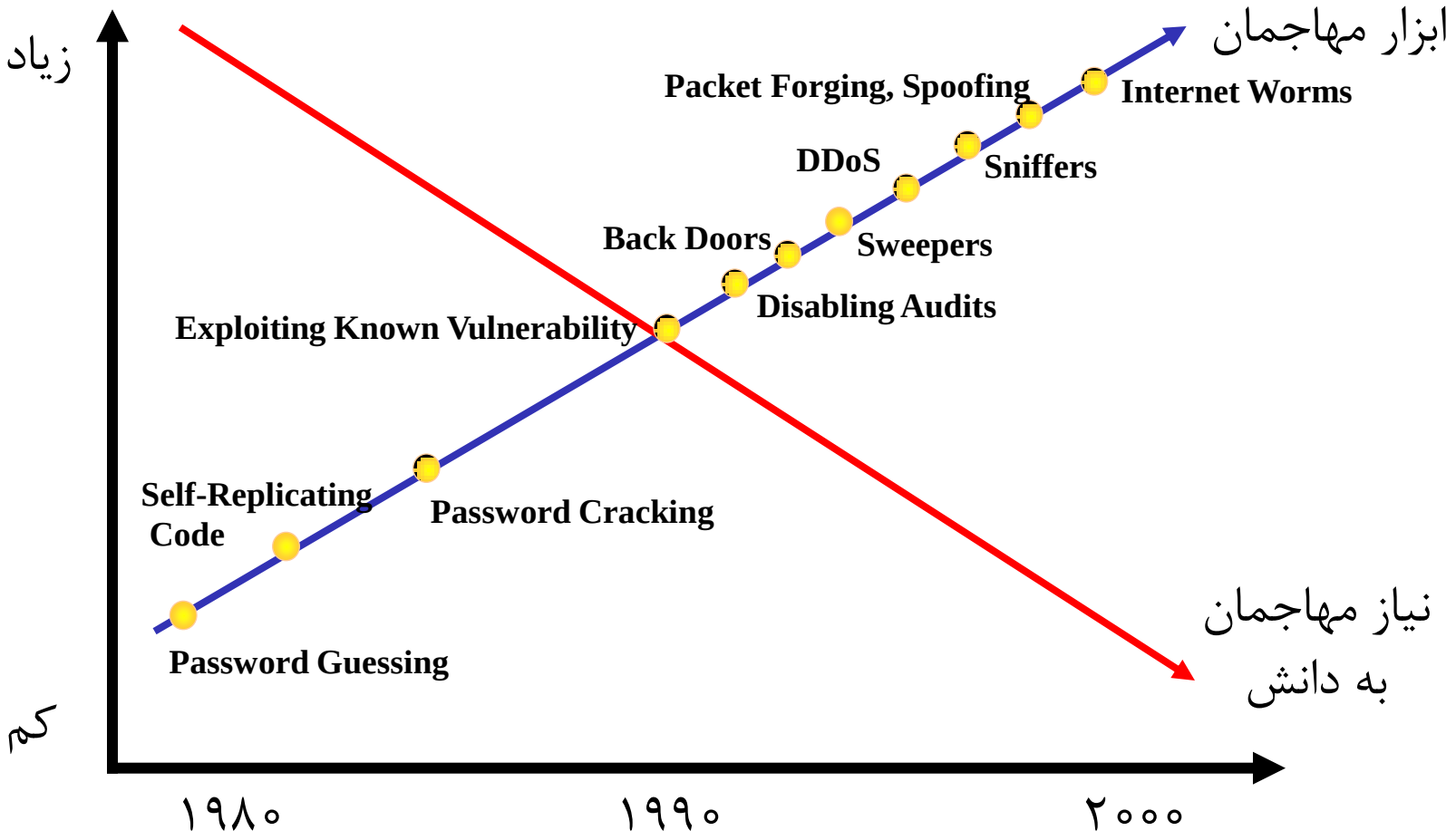
- نگهداری اطلاعات در کامپیوترها
- برقراری ارتباط شبکه‌ای بین کامپیوترها
- برقراری امنیت در کامپیوترها و شبکه‌ها

آمار منتشر شده توسط CERT

CERT: Computer Emergency Response Team



ابزار مهاجمان



نیازهای امنیتی: گذشته و حال

- از دو نمودار قبلی بخوبی پیداست:

☜ تعداد حملات علیه امنیت اطلاعات به طور قابل ملاحظه‌ای افزایش یافته است.

☜ امروزه تدارک حمله با در اختیار بودن ابزارهای فراوان در دسترس به دانش زیادی احتیاج ندارد (بر خلاف گذشته).

نگاهی به گزارش BIS انگلیس (۱)

میزان نفوذ به سازمانهای شرکت کننده در آمار

	۲۰۱۳	۲۰۱۴
سازمان بزرگ	٪۸۶	٪۸۱
سازمان کوچک	٪۶۴	٪۶۰

میزان نفوذ اندکی کاهش یافته است.

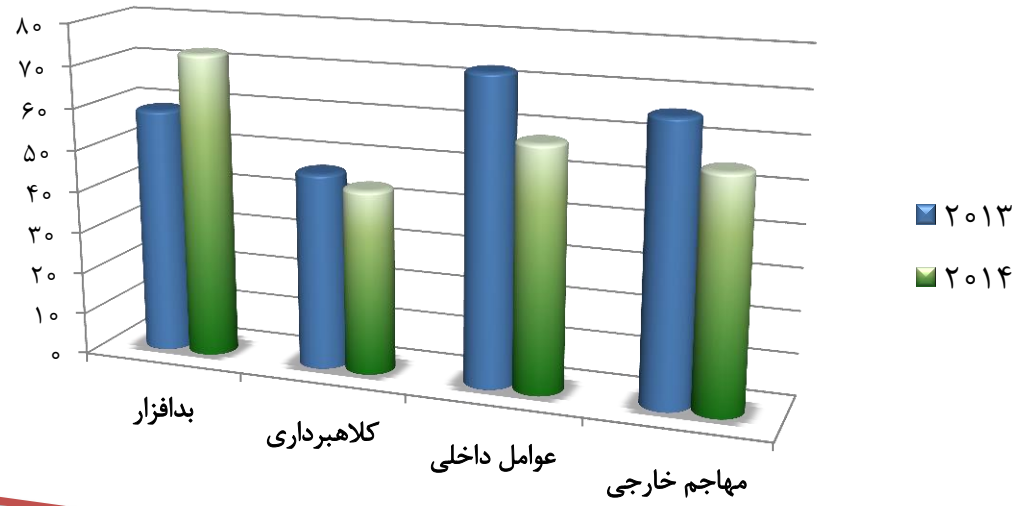
مخارج ناشی از بدترین نفوذ به سازمانهای شرکت کننده در آمار (هزار پوند)

	۲۰۱۳	۲۰۱۴
سازمان بزرگ	۴۵۰ تا ۸۵۰	۶۰۰ تا ۱۱۵۰
سازمان کوچک	۳۵ تا ۶۵	۶۵ تا ۱۱۵

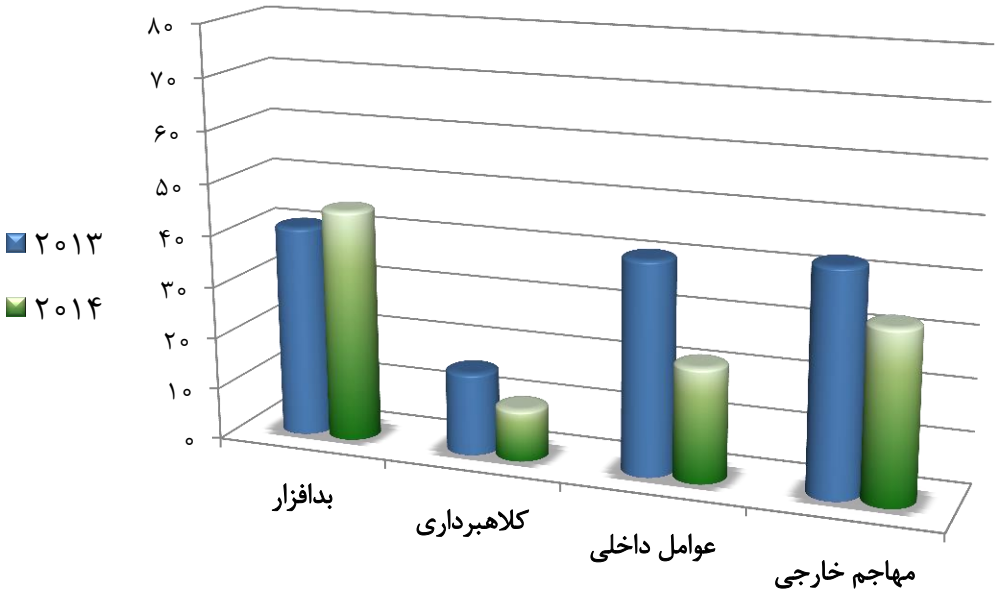
مخارج نفوذ تقریباً ۲ برابر شده است.

نگاهی به گزارش BIS انگلیس (۲)

سازمانهای بزرگ



سازمانهای کوچک

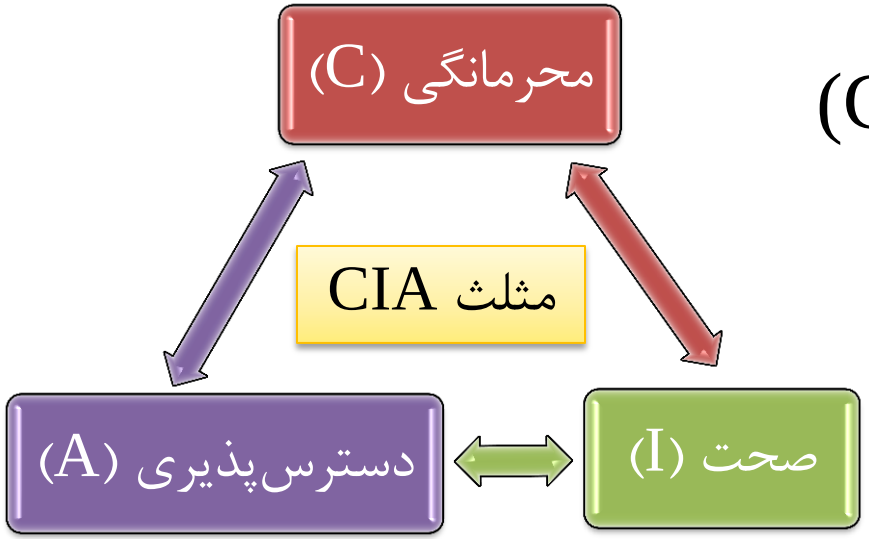


فهرست مطالب

- محتوا و جایگاه درس
- ضرورت امنیت داده و شبکه
- **مفاهیم اولیه**
- دشواری برقراری امنیت
- انواع و ماهیت حملات
- خدمات امنیتی
- مدلهای امنیت شبکه

مبانی امنیت داده‌ها

- **سه ویژگی اساسی:** محرمانگی، صحت و دسترس‌پذیری.



- محرمانگی (Confidentiality)
  - عدم افشای غیرمجاز داده‌ها
- صحت (Integrity)
  - «عدم امکان دستکاری» و/یا «امکان کشف دستکاری» داده‌ها توسط افراد یا نرم‌افزارهای غیرمجاز
- دسترس‌پذیری (Availability)
  - دسترسی به داده‌ها توسط افراد مجاز در «مکان و زمان» مجاز

محرمانگی

- محرمانگی داده (Data Confidentiality)

☜ اطمینان از اینکه داده‌های محرمانه و خصوصی برای افراد غیرمجاز فاش نمی‌شوند.

- حفظ حریم خصوصی (Privacy)

☜ اطمینان از اینکه افراد می‌توانند روی امکان و نحوه جمع‌آوری، ذخیره‌سازی و انتشار یا افشای داده‌های خصوصی خود توسط دیگران کنترل و تاثیر داشته باشند.

محرمانگی

- ساز و کارهای متداول:
  - رمزنگاری
  - کنترل دسترسی

صحت

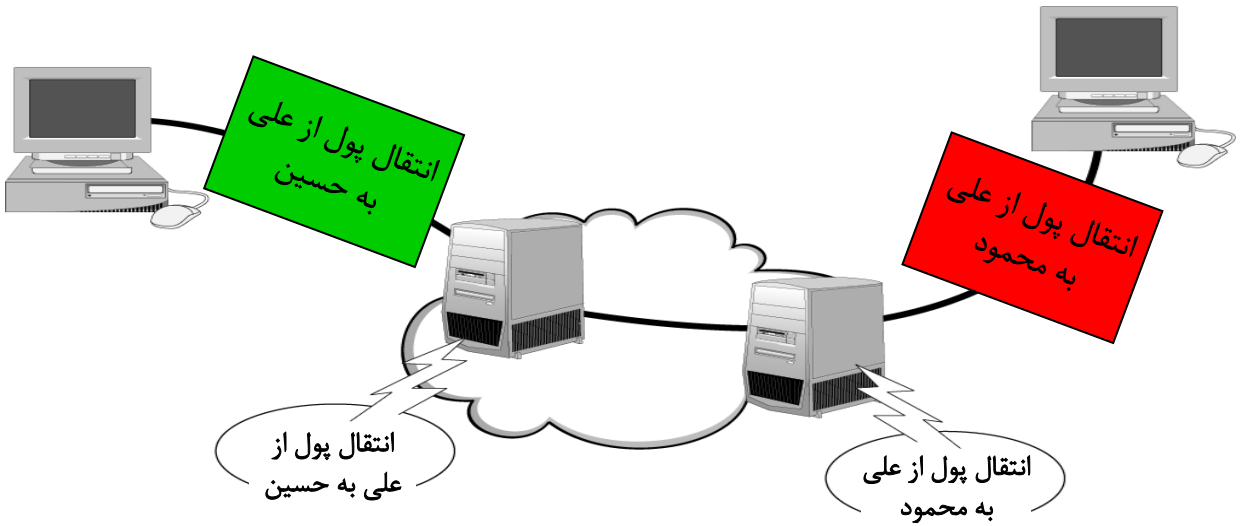
- صحت داده (Data Integrity)

☜اطمینان از اینکه داده‌ها و یا برنامه‌ها توسط افراد غیرمجاز تغییر نمی‌یابند، و در صورت تغییر ما متوجه خواهیم شد.

- صحت منبع (Origin Integrity)

☜اطمینان از درستی و صحت منبع (فرستنده) اطلاعات.

- ساز و کارهای متداول:
  - امضای دیجیتال
  - کد تصدیق هویت پیام
  - کنترل دسترسی



دسترس‌پذیری

- **تعریف:** دسترسی به داده‌ها و خدمت‌دهی به افراد مجاز در زمـان و مکان مجاز.

- **ساز و کارهای متداول:**

  - وجود پشتیبان
  - تکرار داده و خدمت
  - سیستم‌های پایش و توزیع بار

تعاریف و مفاهیم اولیه امنیت

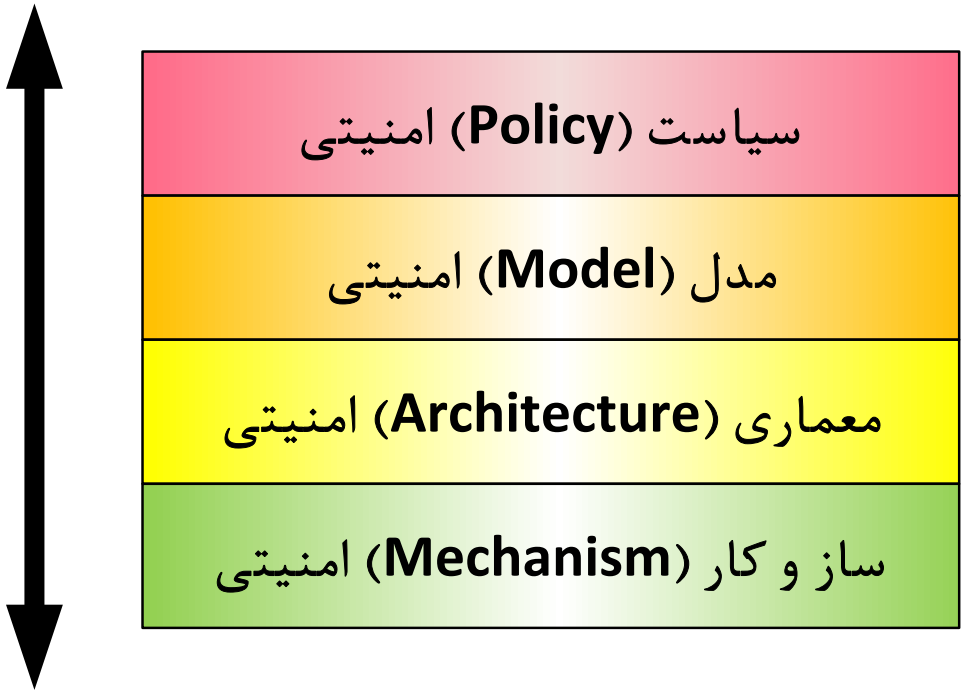
- انواع تعاریف امنیتی در مستندات و استانداردهای مختلف:

تعاریف مورد استفاده ما

- RFC 4949: واژگان امنیتی اینترنت، نسخه ۲
- ISO/IEC سری ۲۷۰۰۰ (مشهور به ISMS)
- NIST IR 7298 (واژه‌نامه اصطلاحات اساسی امنیت اطلاعات)
- واژگان ENISA
- واژگان ISACA
- ...

سطوح مختلف امنیت

چه خدمات امنیتی
باید فراهم شود؟



چگونه خدمات امنیتی
باید پیاده‌سازی شود؟

خدمات امنیتی

- خدمت امنیتی:
  - یک خدمت پردازشی یا ارتباطی از سیستم؛
  - جهت فراهم آوردن نوع مشخصی از محافظت برای منابع سیستم.
- **مثال:**
  - خدمت کنترل دسترسی
  - خدمت محرمانگی داده
  - خدمت تصدیق هویت موجودیت

ساز و کار امنیتی

- یک روش، فرآیند یا ابزار؛
- جهت پیاده‌سازی یک خدمت امنیتی؛
- که توسط یک سیستم یا درون آن فراهم می‌شود.
- **مثال:**
  - رمزنگاری
  - دیوار آتش

معماری امنیتی

- طرح و مجموعه‌ای از اصول که موارد زیر را توصیف می‌کند:
  - خدمات امنیتی که یک سیستم باید در جهت رفع نیاز کاربرانش فراهم آورد؛
  - اجزایی لازم جهت پیاده‌سازی خدمات امنیتی؛
  - سطوح کارایی مورد نیاز اجزا جهت تعامل با محیط تهدید.
- **مثال:**
  - معماری امنیتی مدل مرجع OSI (ISO 7499-2)

مدل امنیتی

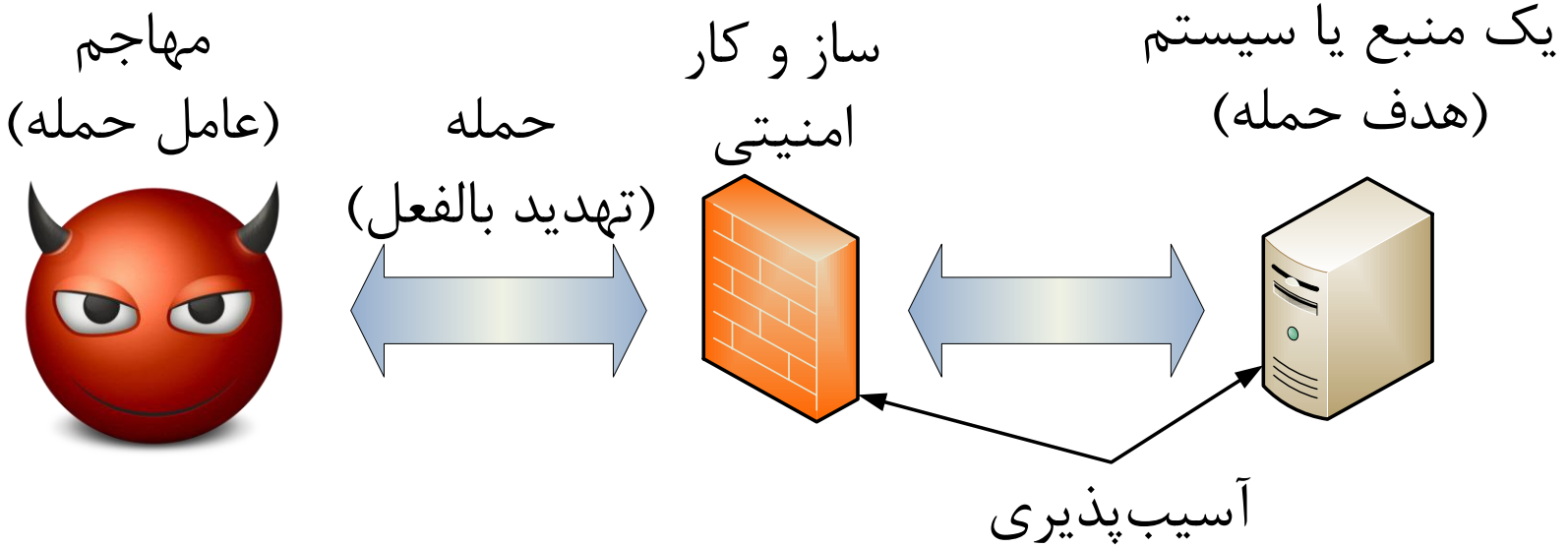
- توصیف ترسیمی؛
- از مجموعه موجودیتها و روابط آنها؛
- که به واسطه آنها خدمات امنیتی توسط یا درون سیستم فراهم می‌شود.
- **مثال:**
  - مدل کنترل دسترسی نقش-مبنا (RBAC)
  - مدل مهاجم (فعال / منفعل)

سیاست (خط مشی) امنیتی

- یک هدف، مسیر یا روش اقدام مشخص؛
- برای تعیین و جهت‌دهی به تصمیمات حال و آینده؛
- در رابطه با امنیت در یک سیستم.

- **مثال:**
  - سیاست امنیتی نصب نرم‌افزار
  - سیاست امنیتی ساخت گذرواژه
  - سیاست امنیتی دسترسی راه دور

آسیب‌پذیری، تهدید، حمله و مهاجم



آسیب‌پذیری (Vulnerability)

- نقصان یا ضعف؛
- در طراحی، پیاده‌سازی، یا عملیات و مدیریت سیستم؛
- که با سوء استفاده از آن می‌توان سیاست امنیتی سیستم را نقـض کرد.

CVE: Common Vulnerabilities and Exposures

- **مثال:**
  - آسیب‌پذیری خونریزی قلبی (HeartBleed) در OpenSSL
  - آسیب‌پذیری سر ریز بافر (Buffer Overflow)

تهدید (Threat)

- امکان بالقوه برای نقض امنیت.
- متناظر با هر آسیب‌پذیری، (حداقل) یک تهدید وجود دارد.
- می‌تواند عمدی یا غیر عمدی باشد.

☜ **عمدی:** امکان نقض امنیت توسط یک موجودیت هوشمند (فرد یا سازمان)

☜ **غیر عمدی:** امکان خطای انسانی، عملکرد ناصحیح ابزار، وقایع طبیعی (زلزله، سیل، آتش سوزی، و ...)

حمله و مهاجم

- حمله، بالفعل شدن یک تهدید توسط یک موجودیت هوشمند (مهاجم) است.
- هر تهدیدی منجر به حمله نمی‌شود.
- هر حمله‌ای الزاماً موفق نیست.

مهاجم و رخنه‌گر

- رخنه (Hack) در واقع به معنی کنکاش به منظور کشف حقایق و نحوه کار یک سیستم است.
- حمله (Attack) تلاش برای نفوذ به سیستمهای دیگران و در واقع رخنه خصمانه یا بدخواهانه است.

Malicious Hacker = Attacker

فهرست مطالب

- محتوا و جایگاه درس
- ضرورت امنیت داده و شبکه
- مفاهیم اولیه
- **دشواری برقراری امنیت**
- انواع و ماهیت حملات
- خدمات امنیتی
- مدلهای امنیت شبکه

دشواری برقراری امنیت

- امنیت معمولاً قربانی افزایش کارایی و مقیاس‌پذیری می‌شود.
- امنیت بالا هزینه‌بر است.
- کاربران عادی امنیت را به عنوان مانع در برابر انجام شدن کارها تلقی می‌کنند و از سیاستهای امنیتی پیروی نمی‌کنند.

دشواری برقراری امنیت

- اطلاعات و نرم‌افزارهای دور زدن امنیت به طور گسترده در اختیار هستند.
- برخی دور زدن امنیت را به عنوان یک مبارزه در نظر می‌گیرند و از انجام آن لذت می‌برند.
- ملاحظات امنیتی در هنگام طراحی‌های اولیه سیستم‌ها و شبکه‌ها در نظر گرفته نمی‌شود.

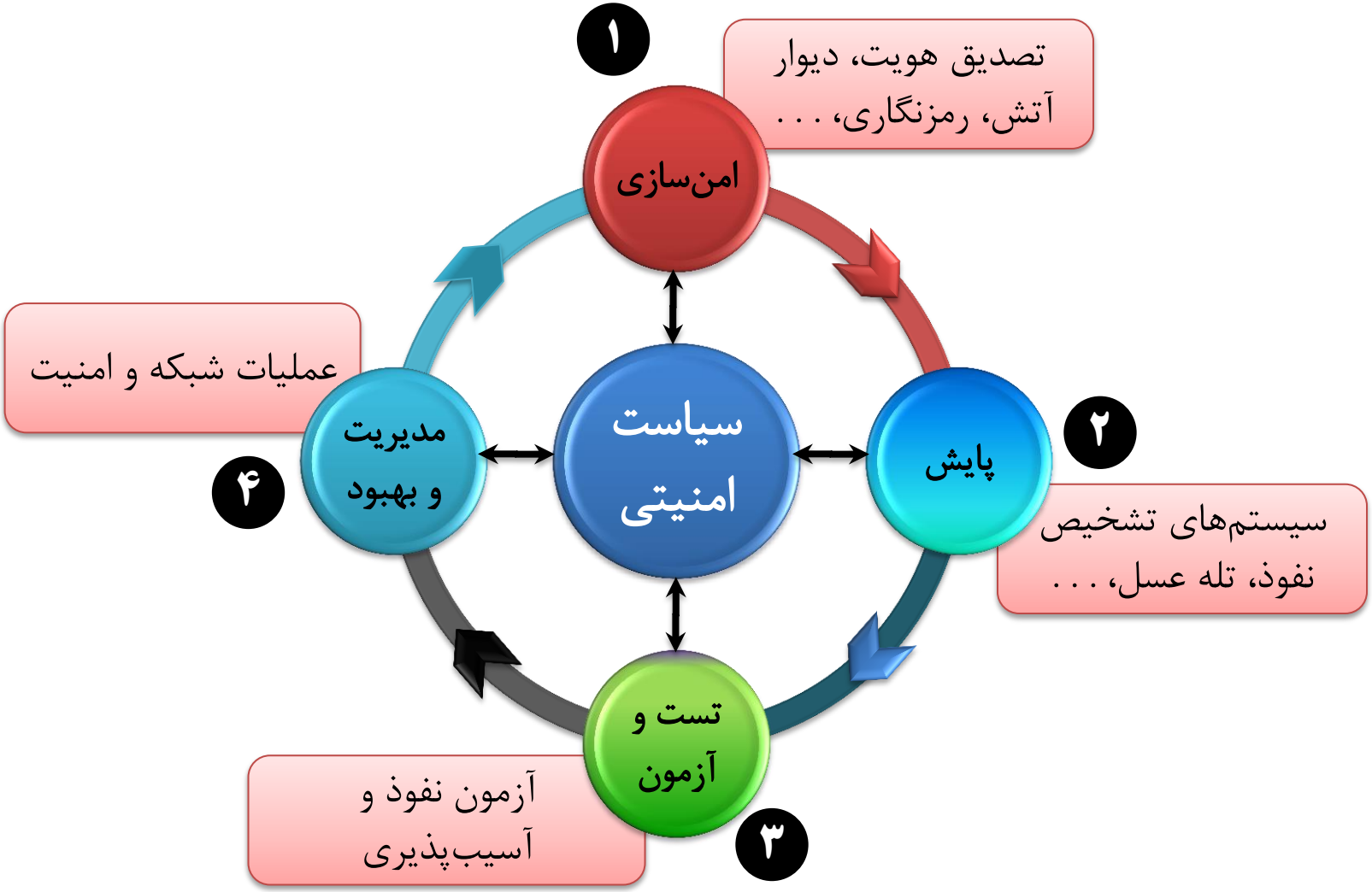
دلایل ناامنی شبکه‌ها

- ضعف فناوری (تحلیل، طراحی، پیاده‌سازی)
  - پروتکل، سیستم عامل، تجهیزات
- ضعف تنظیمات
  - رهاکردن تنظیمات پیش‌فرض، گذرواژه‌های نامناسب، عدم استفاده از رمزنگاری، راه‌اندازی خدمات اینترنت بدون اعمال تنظیمات لازم، ...
- ضعف سیاست‌گذاری
  - عدم وجود سیاست امنیتی
  - عدم وجود طرحی برای مقابله و بازیابی مخاطرات
  - نداشتن نظارت امنیتی مناسب (مدیریتی و فنی)

امن‌سازی

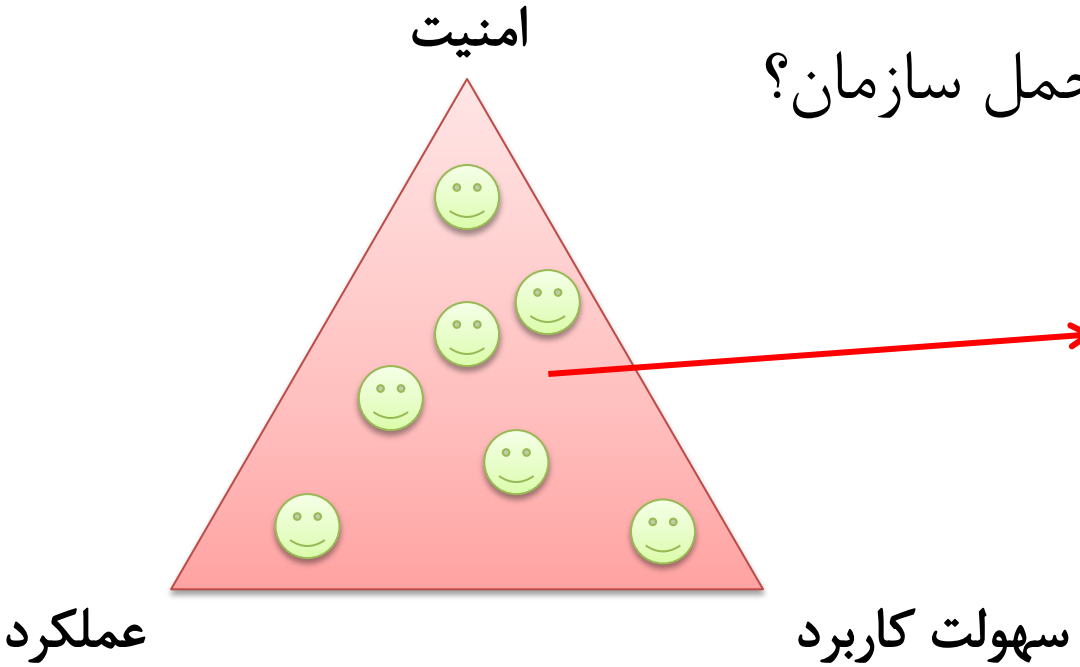
- گستره امنیت تمامی منابع سازمان است و نه تنها کارگزار اصلی.
- مسئله امنیت نیازمند نگرش مدیریتی است، نه صرفاً نگرش فنی.
- مهاجمین داخلی خطر بالقوه بیشتری دارند.
- مادام که انسانها امن فکر نکنند نمی‌توان تراکنش امن داشت.
- امن سازی یک فرآیند است نه یک وظیفه خاص و مقطعی.

چرخه ایجاد امنیت



راهبرد امنیت سازمانی

- مصالحه بین امنیت، عملکرد، و سهولت کاربرد.
- مصالحه بین امنیت و هزینه.
- میزان امنیت مورد انتظار کاربران؟
- میزان ناامنی قابل تحمل سازمان؟



فهرست مطالب

- محتوا و جایگاه درس
- ضرورت امنیت داده و شبکه
- مفاهیم اولیه
- دشواری برقراری امنیت
- **انواع و ماهیت حملات**
- خدمات امنیتی
- مدلهای امنیت شبکه

انواع حملات از نظر تاثیر

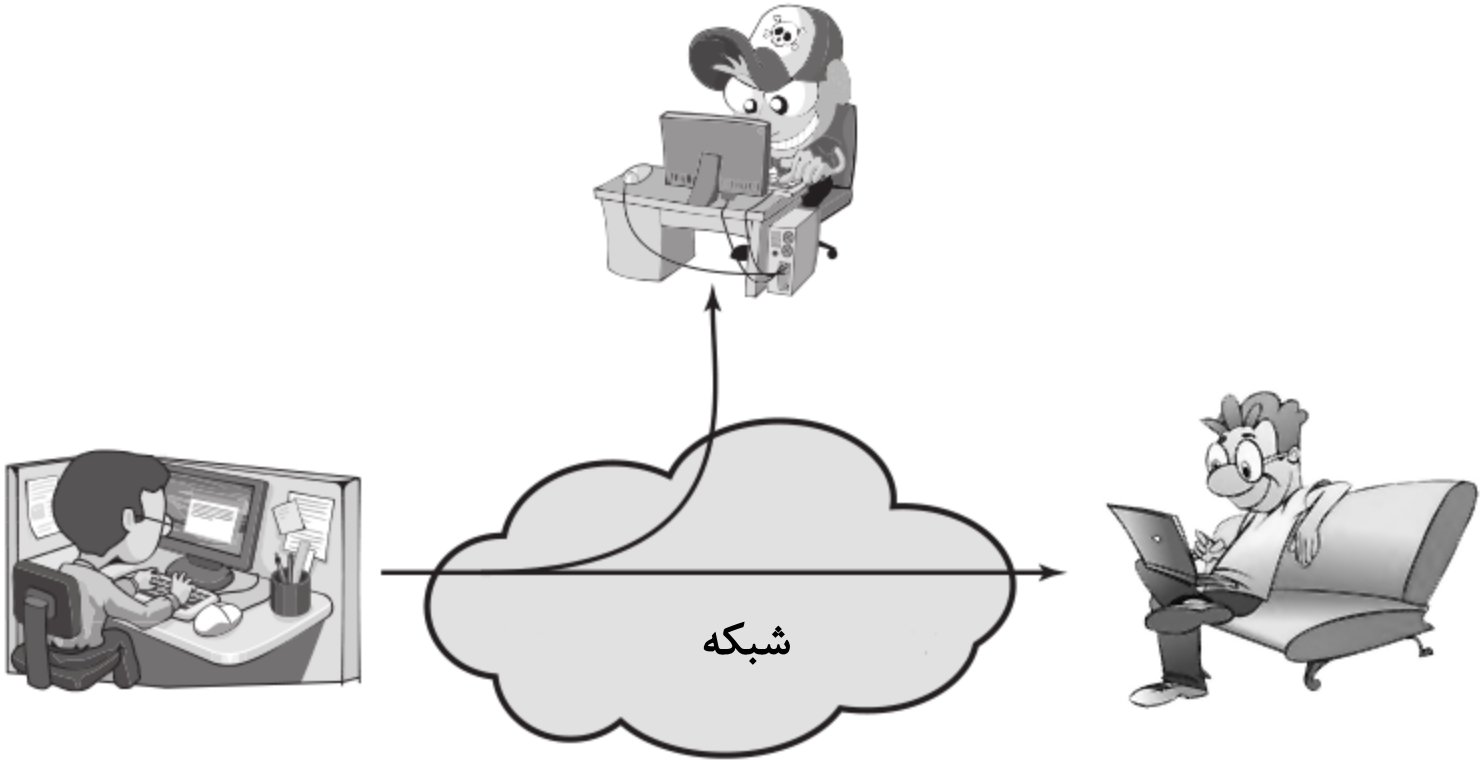
حملات فعال (Active)

- جعل هویت (Masquerade)
- ارسال دوباره پیغام (Replay)
- تغییر (Modification)
- منع خدمت (Denial of Service)

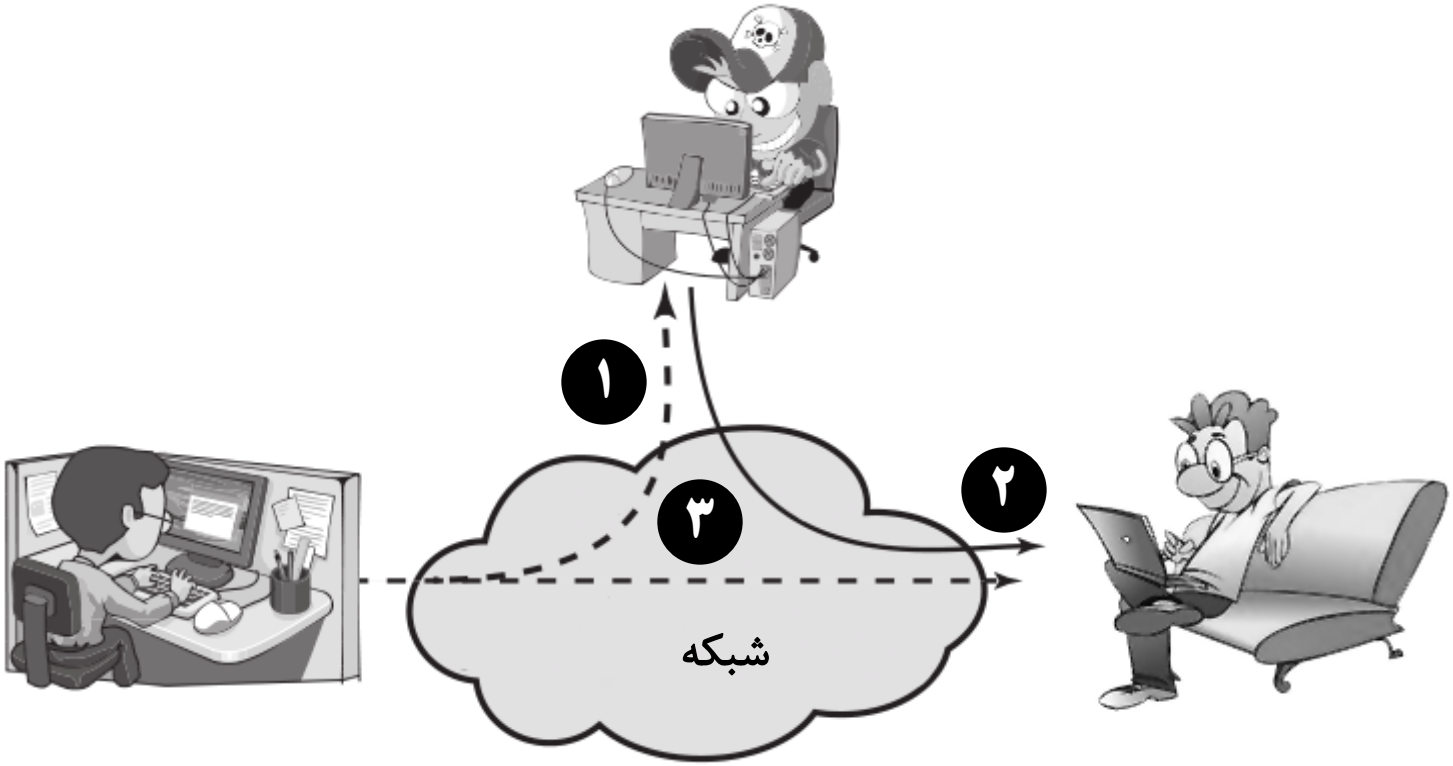
حملات منفعل (Passive)

- تحلیل ترافیک (Traffic Analysis)
- انتشار محتوای پیغام (Release of Message Contents)

حملات منفعل



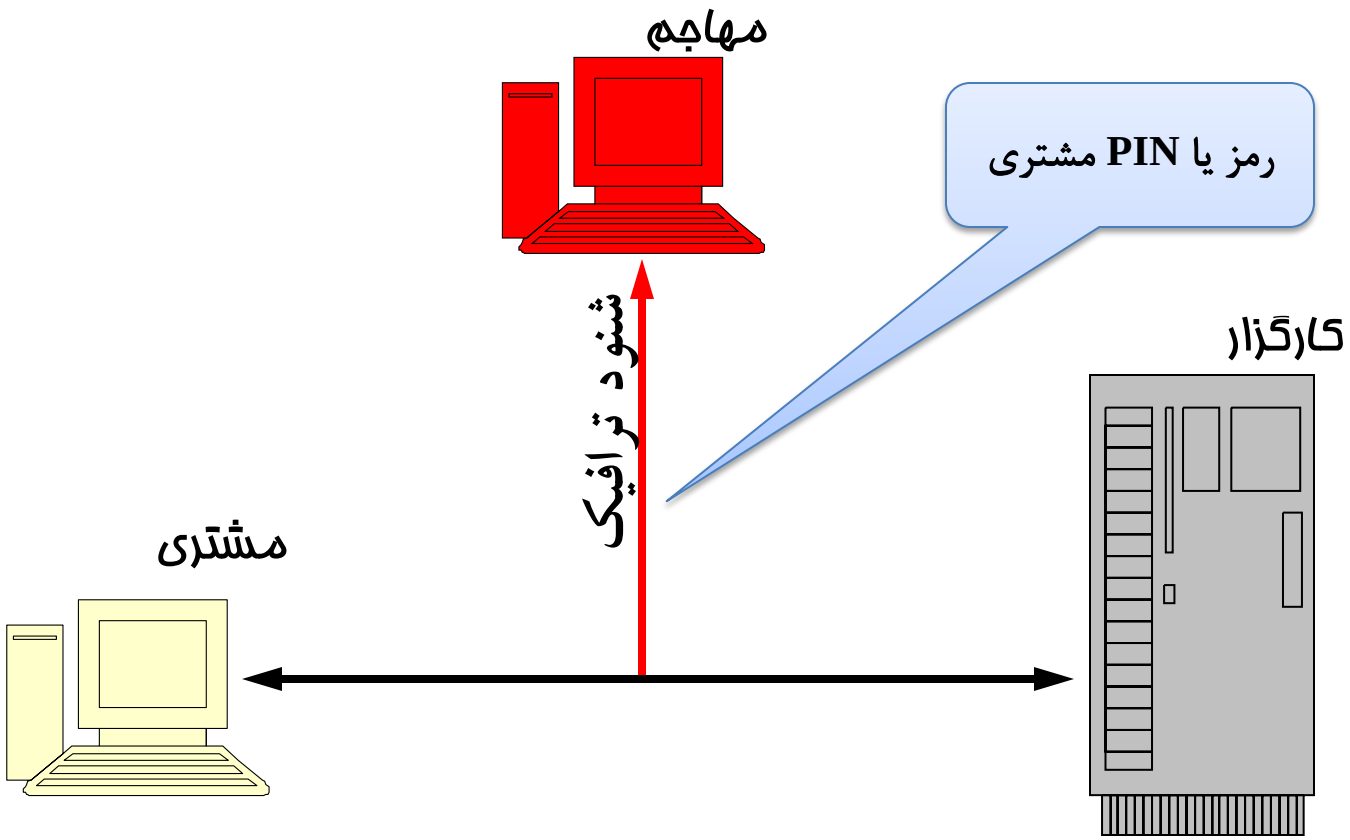
حملات فعال



حمله شنود یا استراق سمع – ۱

- **هدف:** نقض محرمانگی
- **نتیجه:** دسترسی غیرمجاز به داده‌های طبقه‌بندی شده
- راه‌های تحقق حمله:
  - اتصال فیزیکی به شبکه و دریافت بسته‌ها
  - دسترسی غیرمجاز به پایگاه‌داده‌ها
  - وجود ضعف و آسیب‌پذیری در سیستم کنترل دسترسی

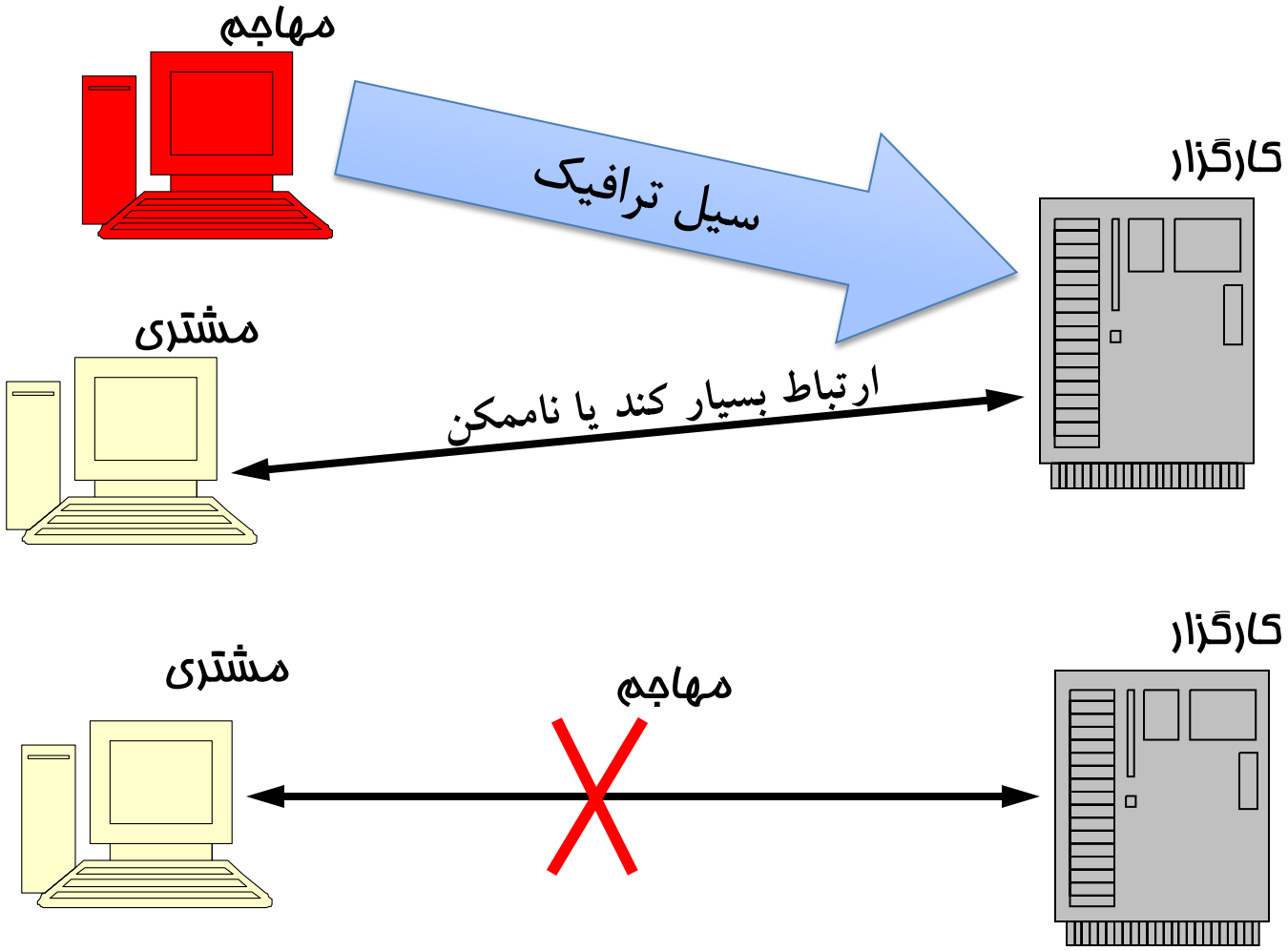
حمله شنود یا استراق سمع – ۲



حمله منع خدمت یا وقفه – ۱

- **هدف:** نقض دسترس‌پذیری
- **نتیجه حمله:** کاهش کارایی و یا عدم امکان دسترسی کاربران به شبکه و یا خدمات فراهم شده
- راه‌های تحقق حمله:
  - ارسال بسته و درخواست‌های مشکل‌دار
  - راه‌اندازی سیل ترافیکی
  - استفاده از ضعف‌ها و آسیب‌پذیری‌های نرم‌افزاری شبکه ویا خدمات

حمله منع خدمت یا وقفه – ۲

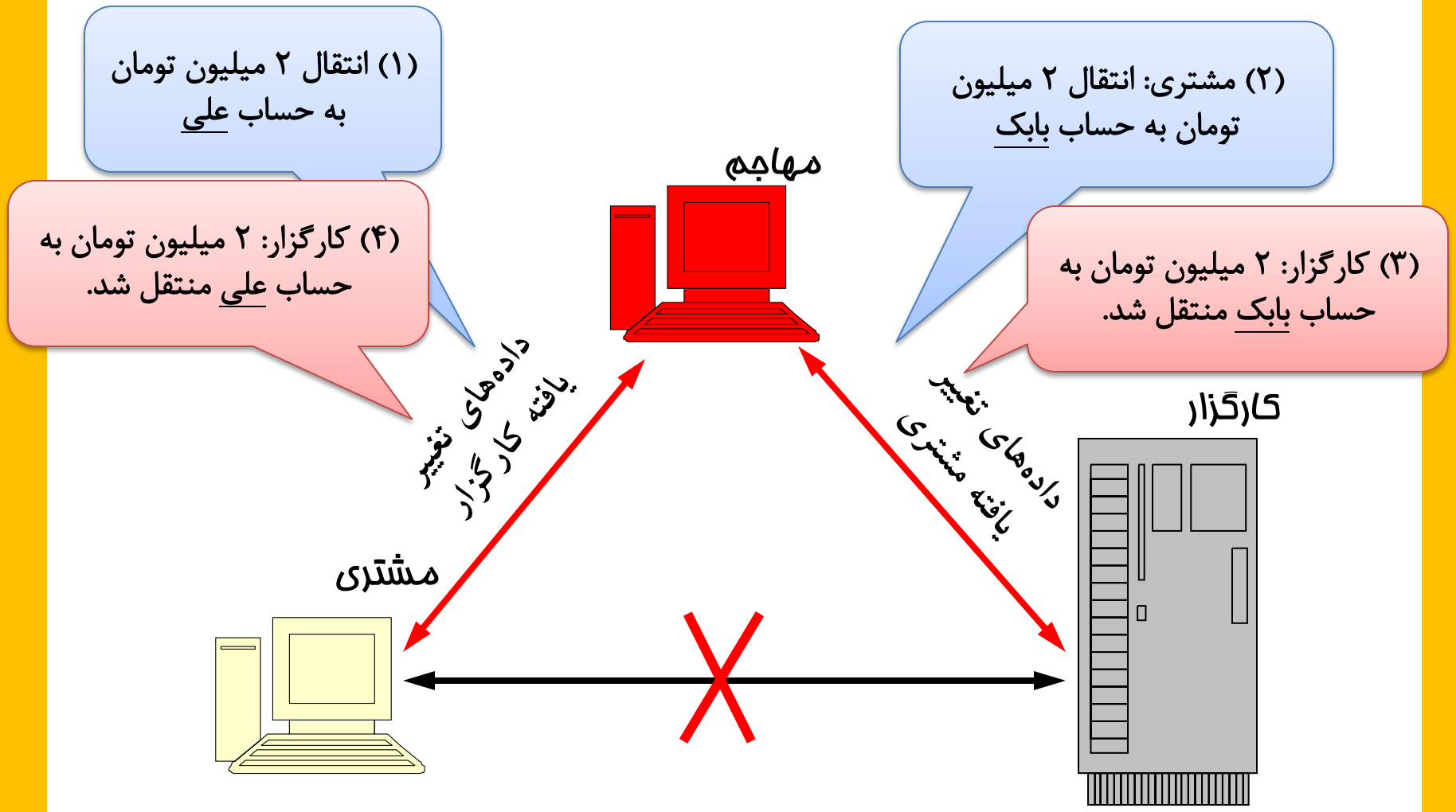


حمله تغییر یا دستکاری داده‌ها – ۱

- **هدف:** نقض صحت
- **نتیجه:** تغییر غیرمجاز داده‌های سیستم یا شبکه
- راه‌های تحقق حمله:
  - قرار گرفتن در مسیر شبکه و دستکاری و ارسال به گیرنده
  - دسترسی غیرمجاز به پایگاه‌داده‌ها و تغییر غیرمجاز در آن
  - وجود ضعف و آسیب‌پذیری در سیستم کنترل دسترسی و صحت

حمله تغییر یا دستکاری داده‌ها – ۲

- حمله مرد میانی (Man in the Middle)

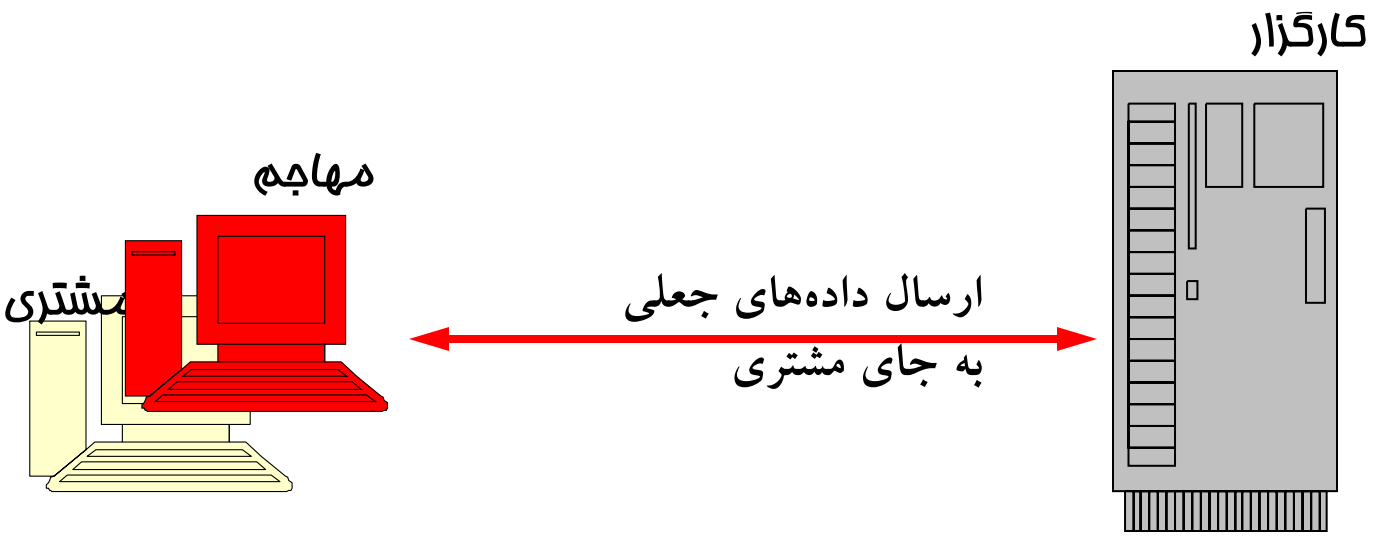


حمله جعل هویت – ۱

- **هدف:** نقض صحت
- **نتیجه:** جعل (یا اضافه کردن) پیام‌ها و داده‌هایی که می‌توانند مخرب یا منشأ سوءاستفاده باشند.
- راه‌های تحقق حمله:
  - اتصال فیزیکی به شبکه و دریافت بسته‌ها
  - بازارسال بسته‌های شنود شده پس از اِعمال تغییرات موردنیاز (ارسال بسته‌های جعلی)
  - وجود ضعف در ساز و کار تصدیق هویت و کنترل صحت

حمله جعل هویت – ۲

- حمله جعل مشتری یا کاربر (به طور مشابه جعل کارگزار)



فهرست مطالب

- محتوا و جایگاه درس
- ضرورت امنیت داده و شبکه
- مفاهیم اولیه
- دشواری برقراری امنیت
- انواع و ماهیت حملات
- **خدمات امنیتی**
- مدلهای امنیت شبکه

خدمات امنیتی – ۱

- محرمانگی داده‌ها (Data Confidentiality)
- صحت داده‌ها (Data Integrity)
- دسترس پذیری (Availability)

پیشتر آشنا شدیم

- تصدیق هویت (Authentication)
- کنترل دسترسی (Access Control)
- انکار ناپذیری (Non Repudiation)

خدمات امنیتی – ۲

- **تصدیق هویت**
  - **تصدیق هویت همتا (Peer):** کاربر همانی است که ادعا می‌کند.
  - **تصدیق هویت مبدأ (Origin) داده:** منبع داده همانی است که ادعا می‌کند.
- **کنترل دسترسی:** ممانعت از دسترسی غیر مجاز به منابع.
- **انکار ناپذیری:** عدم امکان انکار شرکت در یک ارتباط توسط هر یک از فرستنده یا گیرنده.

رابطه خدمات با ساز و کارهای امنیتی (استاندارد X.800)

نگاشت بر گرفته از کتاب درسی (Stallings)

SERVICE \ MECHANISM	Enchipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

نگاشت درست به نظر نمی‌رسد!

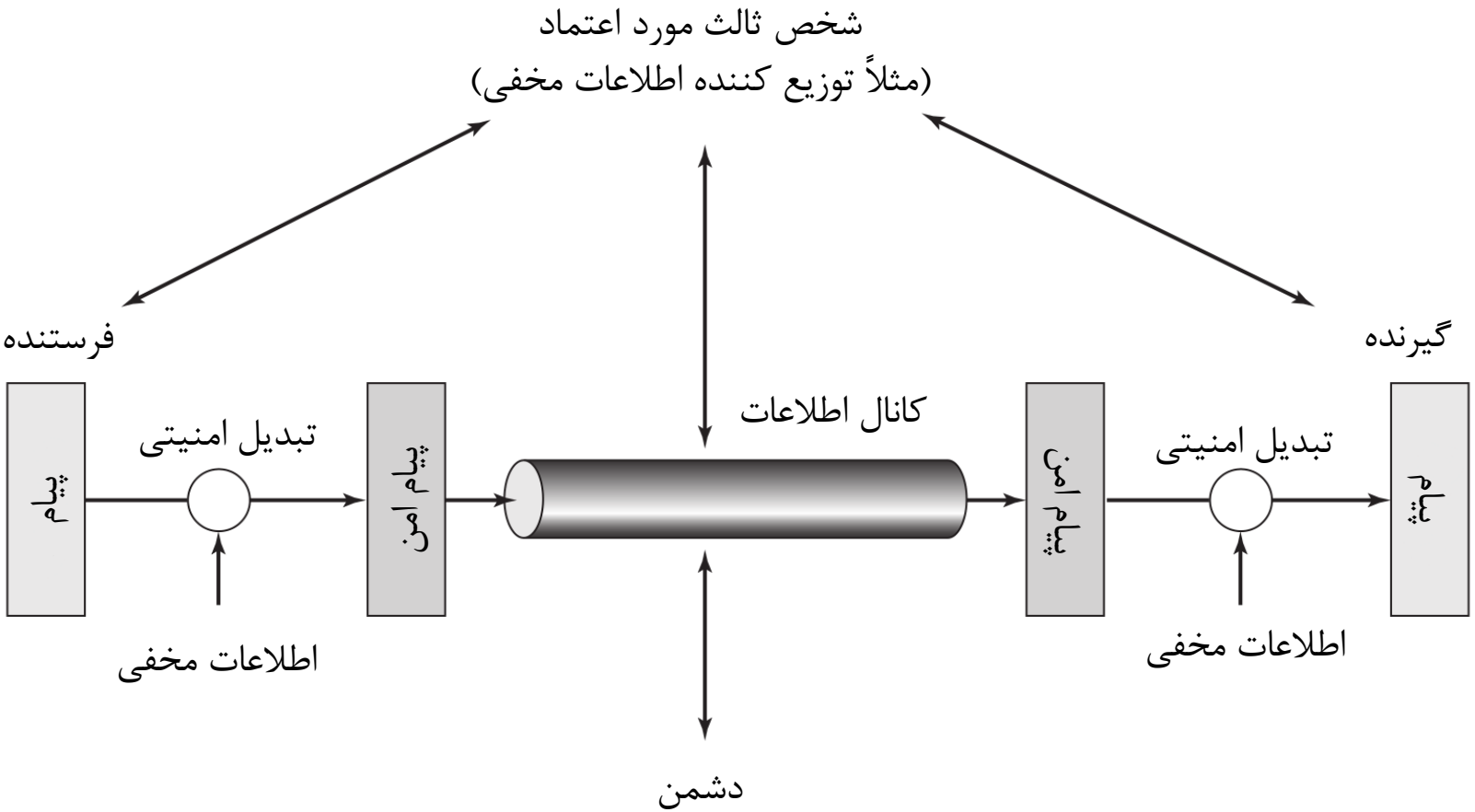
فهرست مطالب

- محتوا و جایگاه درس
- ضرورت امنیت داده و شبکه
- مفاهیم اولیه
- دشواری برقراری امنیت
- انواع و ماهیت حملات
- خدمات امنیتی
- **مدلهای امنیت شبکه**

مدل کلی در یک ارتباط امن

- سناریوی کلی در هر ارتباط امن:
  - **نیاز:** انتقال یک پیغام بین طرفین با استفاده از یک کانال ناامن (مثل شبکه اینترنت)
  - نیاز به تأمین خدمات محرمانگی، صحت، تصدیق هویت، و ...
- روشهای مورد استفاده عموما از دو مؤلفه زیر استفاده می‌کنند:
  - **تبدیل امنیتی:** جهت فراهم آوردن خدمات امنیتی مورد نیاز
  - **اطلاعات مخفی:** در تبدیل امنیتی مورد استفاده قرار می‌گیرند و به نحوی بین طرفین ارتباط به اشتراک گذاشته شده‌اند.

یک مدل نمونه برای ارتباط امن



تضمین خدمت امنیتی

- مدل فوق نشان می‌دهد که برای فراهم آمدن یک خدمت امنیتی خاص مجبوریم نیازهای زیر را فراهم کنیم:
  - طراحی الگوریتم مناسب برای انجام تبدیل امنیتی مورد نظر
  - تولید اطلاعات مخفی موردنیاز طرفین
  - استفاده از روش مناسب برای توزیع و توافق درباره اطلاعات مخفی
  - طراحی یک پروتکل مناسب برای ارتباط طرفین و تضمین خدمت امنیتی