



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



دانشگاه صنعتی شریف
دانشکده مهندسی کامپیوتر

درس ۱: مفاهیم و تعاریف اولیه

محمد صادق دوستی

- 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: امضاي رقمي و زيرساخت کلید عمومي

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 جاسوس افزار، فیشنینگ، تحلیل ترافیک، گمنامی، امنیت مسیردهی، مقابله و کشف جرایم رایانه‌ای، امنیت شبکه بی‌سیم و VoIP

□ توسعه امن نرم افزار (شماره درس: ۸۷۴-۴۰)

☞ چرخه تولید امن نرم افزار (تحلیل، طراحی، پیاده‌سازی، آزمون)، آزمون نفوذ، مهندسی معکوس، قفل شکنی

سایر دروس امنیتی دانشکده - ۲

□ امنیت سخت افزار (شماره درس: ۸۴۳-۴۰)

☞ حملات فیزیکی و مقاومت در برابر دستکاری، حملات کانال
جانبی، اسب تروای سخت افزاری

□ روش‌های صوری در امنیت اطلاعات (شماره درس: ۸۷۳-۴۰)

☞ توصیف، مدل‌سازی، و وارسی سیستمها و پروتکلهای امنیتی بر
مبانی منطق

سایر دروس امنیتی دانشکده - ۳

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

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

□ نظریه رمزنگاری (شماره درس: ۶۷۵-۴۰)

مدل سازی، 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)

- 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



اقدامات امنیتی

بَل از آنَق

□ پیشگیری (Prevention)

نقض نسخه

☞ جلوگیری از خسارت

جِن اَنَاق

□ تشخیص و ردیابی (Detection & Tracing)

☞ میزان خسارت

☞ هویت دشمن

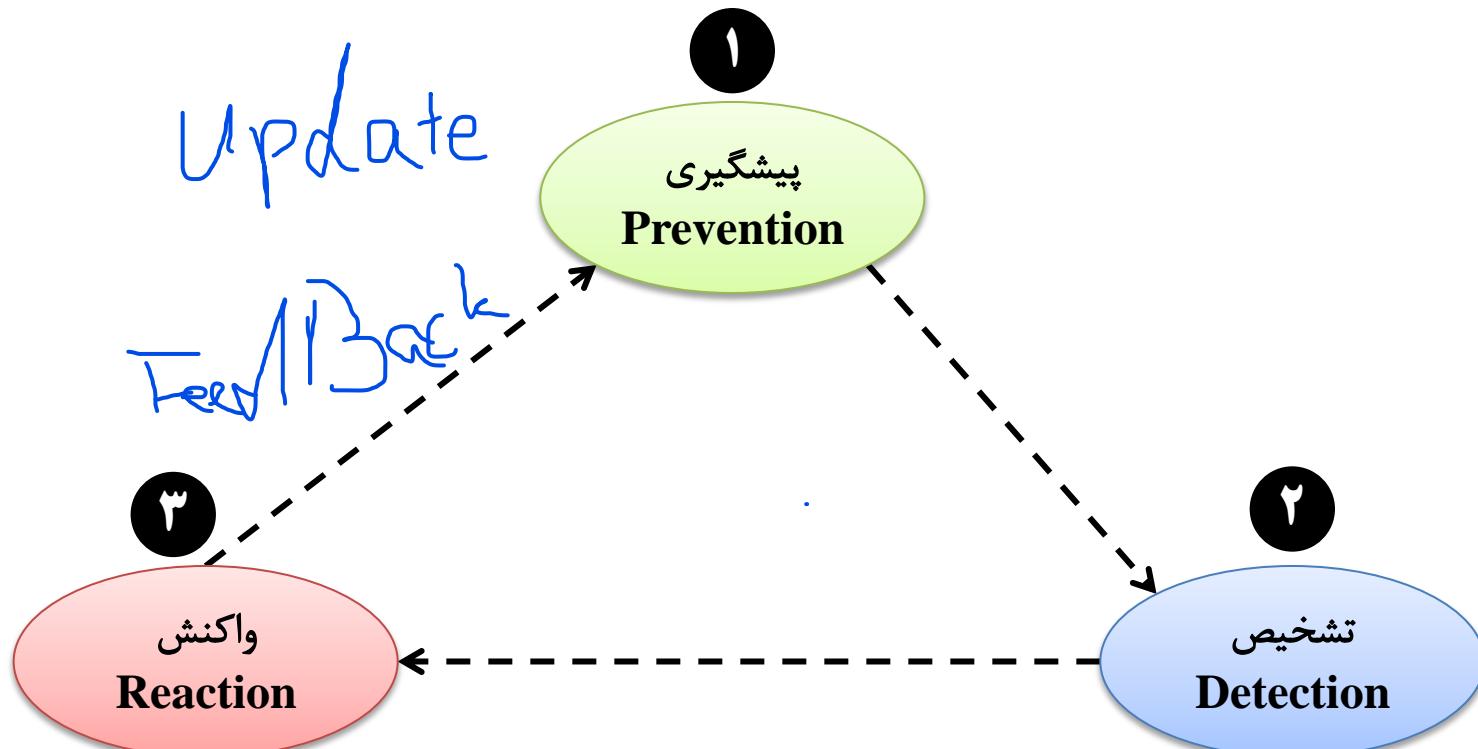
☞ چگونگی حمله (زمان، مکان، دلایل حمله، نقاط ضعف و ...)

بعد از افق

□ واکنش (Reaction)

☞ ترمیم، بازیابی و جبران خسارات

☞ جلوگیری از حملات مجدد



دو واژه‌ای که امروزه مفهوم متفاوتی دارند (۱)

□ secure = se + cure

بر اثربت
بِلَامْ،
free from; care
without

□ 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.

لیختنال / سلطه‌من

دو واژه‌ای که امروزه مفهوم متفاوتی دارند (۲)

□ cryptography = crypto + graphy
 hidden writing

پنهان نویسی



امروزه رمزنگاری دیگر صرفاً
به «مخفي نويسي» که معادل
محرمانگی است نمي پردازد؛
بلکه دامنه وسعيی از خدمات
را ارائه مي کند که در اين
درس با آنها آشنا مي شويم.

امنیت اطلاعات: گذشته و حال

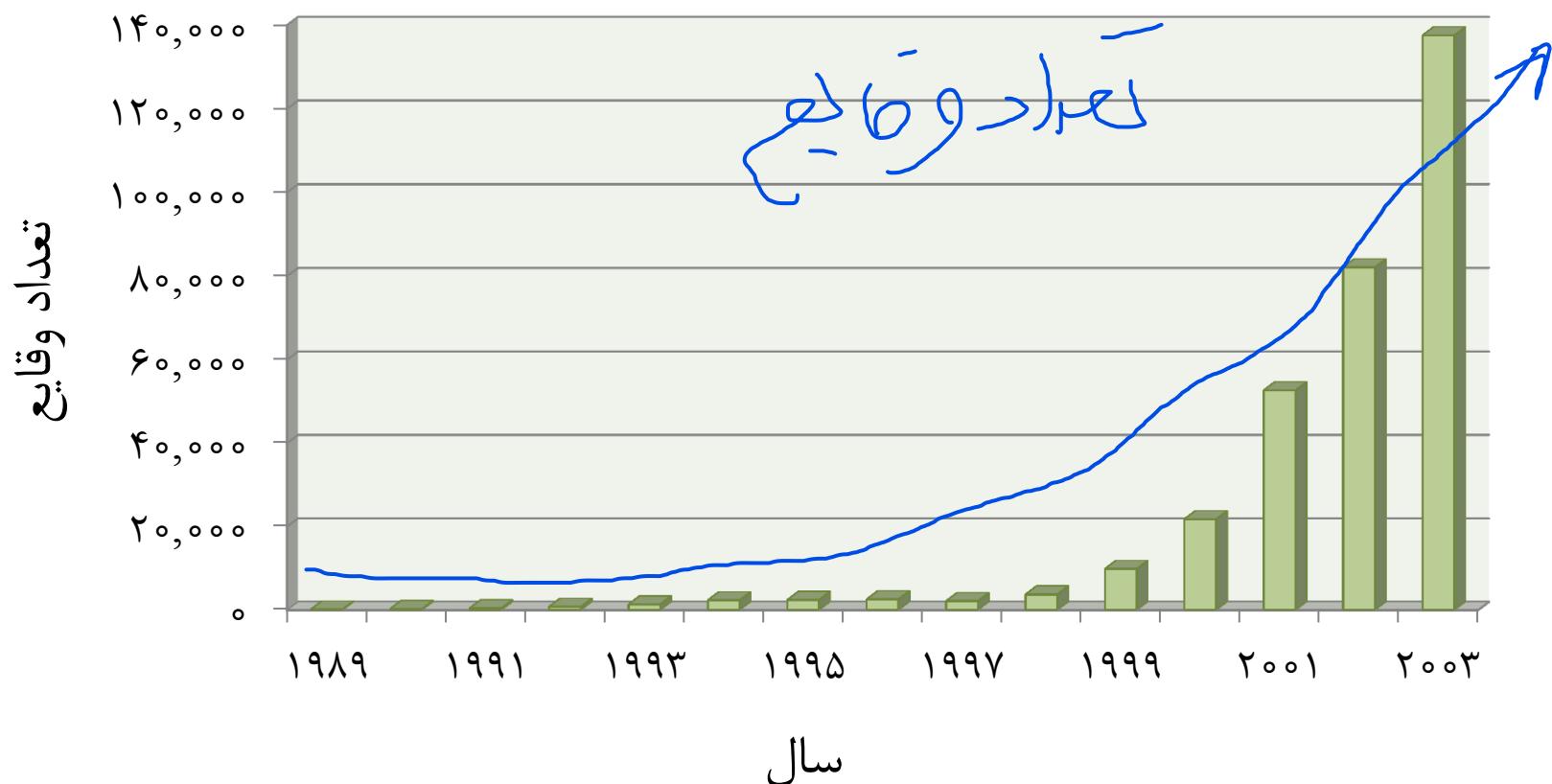
امنیت اطلاعات دنیای نوین لهم

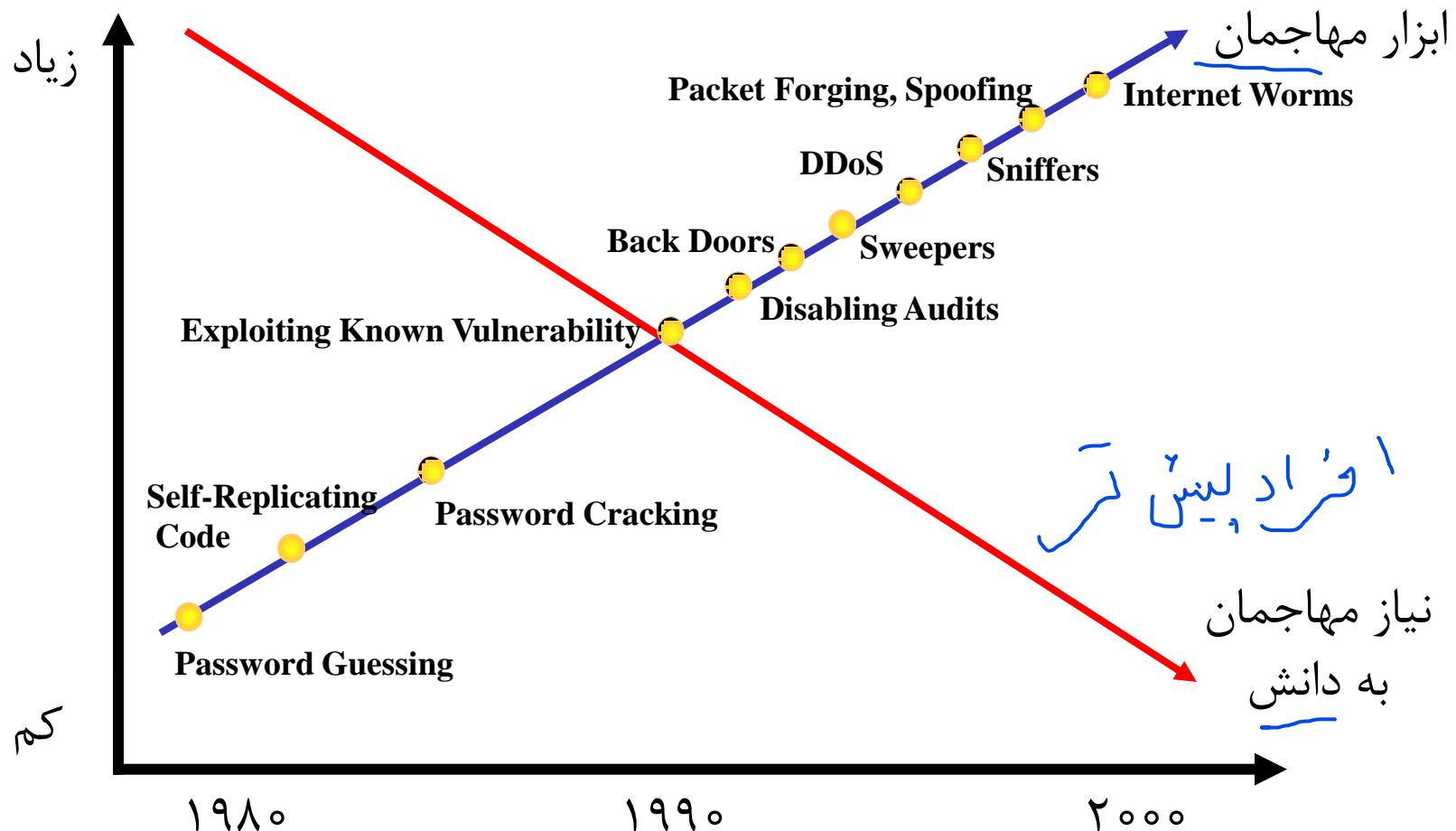
- نگهداری اطلاعات در کامپیوترها
- برقراری ارتباط شبکه‌ای بین کامپیوترها
- برقراری امنیت در کامپیوترها و شبکه‌ها

امنیت اطلاعات سنتی لهم

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

CERT: Computer Emergency Response Team





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 اندکی کاهش یافته است.

میزان نفوذ به سازمانهای شرکت کننده در آمار

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

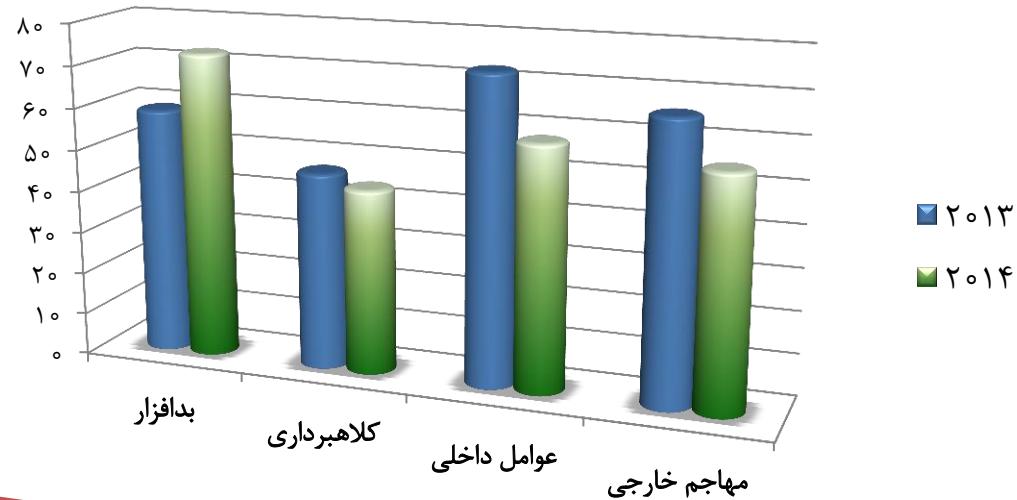
مخارج نفوذ تقریباً ۲ برابر شده است.

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

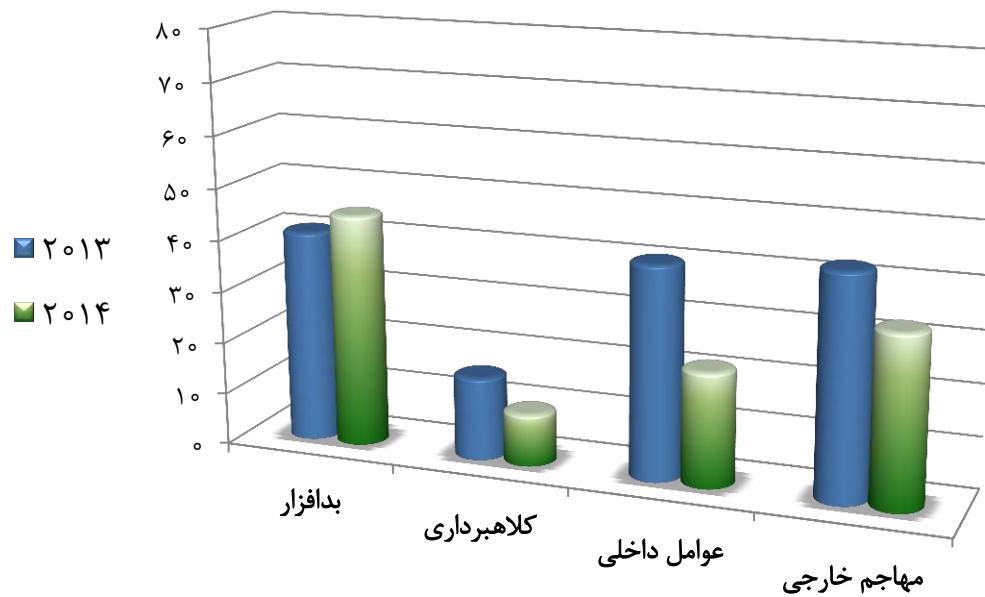
	۲۰۱۴	۲۰۱۳
سازمان بزرگ	۱۱۵۰	۴۵۰ تا ۶۰۰
سازمان کوچک	۱۱۵ تا ۶۵	۳۵ تا ۶۵

نگاهی به گزارش BIS انگلیس (۲)

سازمانهای بزرگ



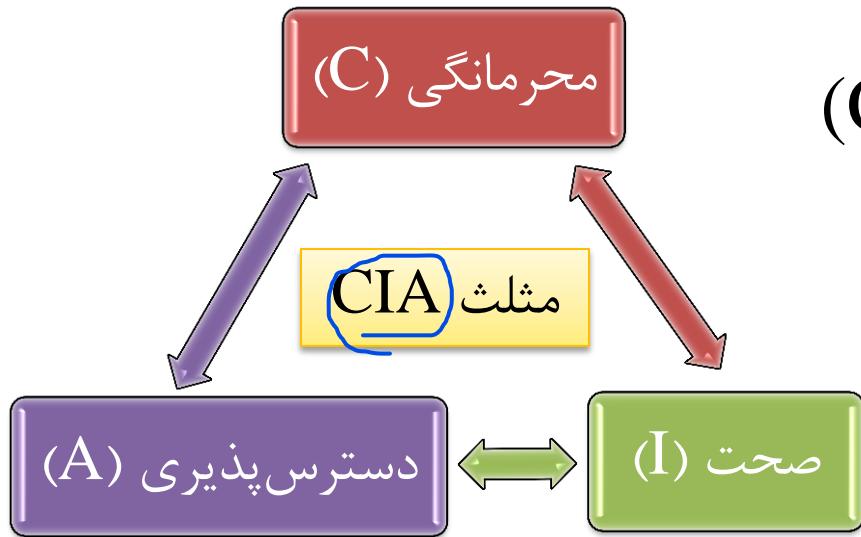
سازمانهای کوچک



- 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

لعله رنگ اساسی امنیت سه ویژگی اساسی: محرمانگی، صحت و دسترس پذیری.



□ محرمانگی (Confidentiality)

لعله رنگ امنیت عدم افشار غیرمجاز داده‌ها

□ صحت (Integrity)

لعله رنگ «عدم امکان دستکاری» و/یا «امکان کشف دستکاری» داده‌ها توسط افراد یا نرم‌افزارهای غیرمجاز

□ دسترس پذیری (Availability)

لعله رنگ امنیت داده‌ها توسط افراد مجاز در «مکان و زمان» مجاز

□ 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.

□ ساز و کارهای متداول:

رمزنگاری

کنترل دسترسی



□ 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)

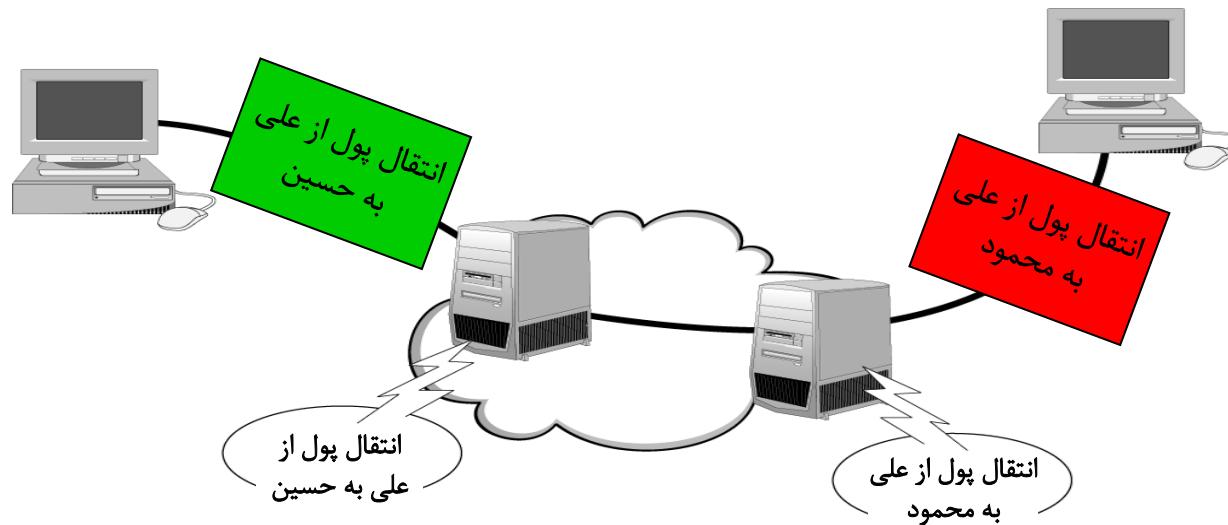
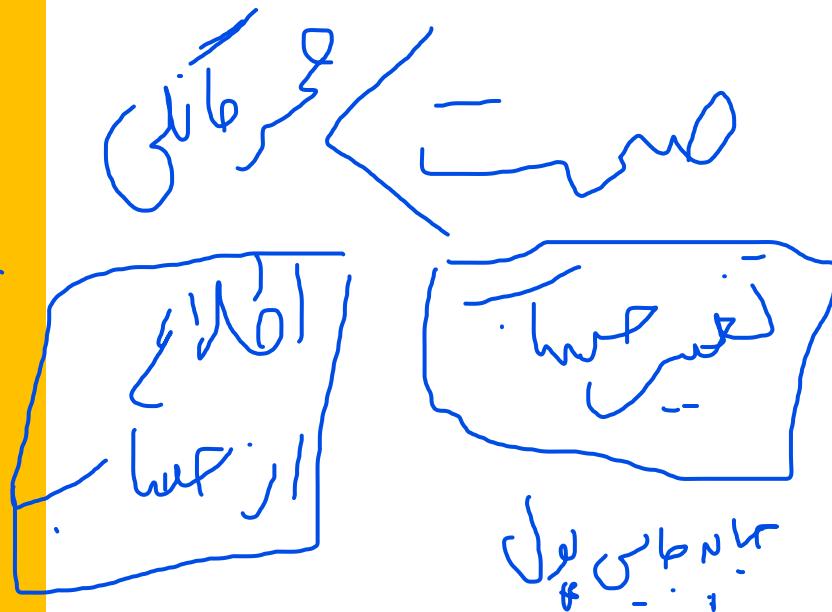
اطمینان از درستی و صحت منبع (فرستنده) اطلاعات.

□ ساز و کارهای متدال:

امضای دیجیتال

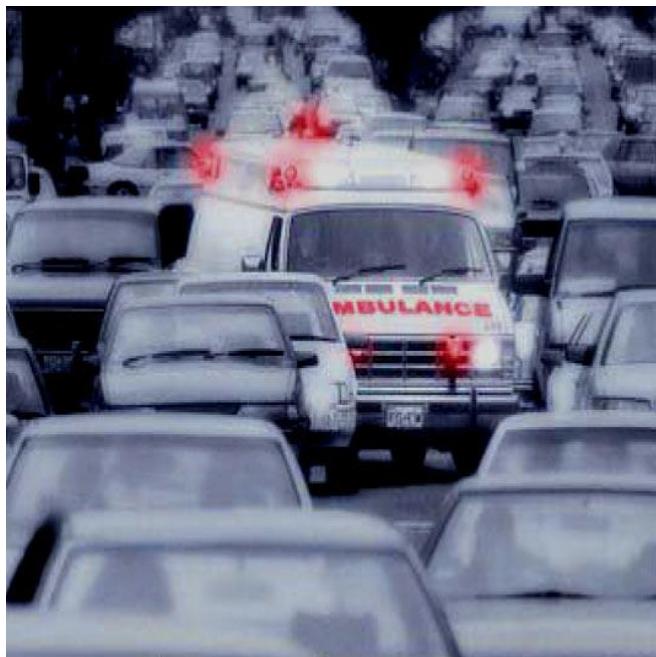
کد تصدیق هویت پیام

کنترل دسترسی



□ تعریف: دسترسی به داده‌ها و خدمت‌دهی به افراد مجاز در زمان و مکان مجاز.

کمترین مسافت
برقراریش سخت‌تر



□ ساز و کارهای متداول:

→ وجود پشتیبان

→ تکرار داده و خدمت

→ سیستم‌های پایش و توزیع بار

Dog →
آپلود فایل
در راه‌رانی زندگی
درینه است خانه‌ی داد

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 ۲۷۰۰۰ سری (مشهور به ISMS)

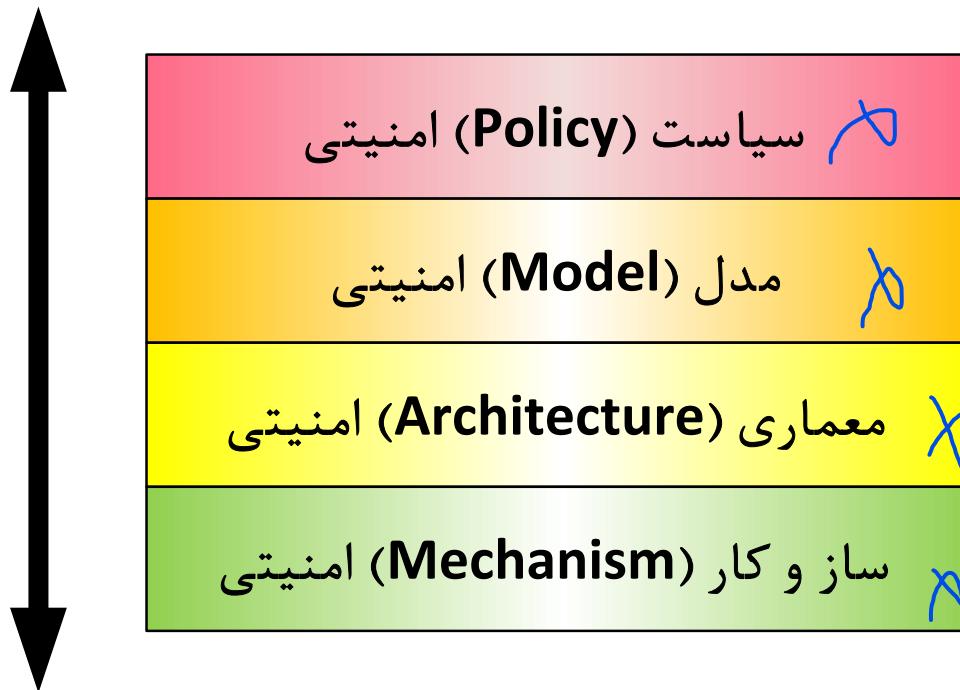
NIST IR 7298 (واژه‌نامه اصطلاحات اساسی امنیت اطلاعات)

ENISA واژگان

ISACA واژگان

...

چه خدمات امنیتی
باید فراهم شود؟



چگونه خدمات امنیتی
باید پیاده‌سازی شود؟

□ 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

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

□ مثال:

☞ رمزنگاری

☞ دیوار آتش

□ 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 تهديد.

□ مثال:

☞ معماری امنیتی مدل مرجع OSI (ISO 7499-2)

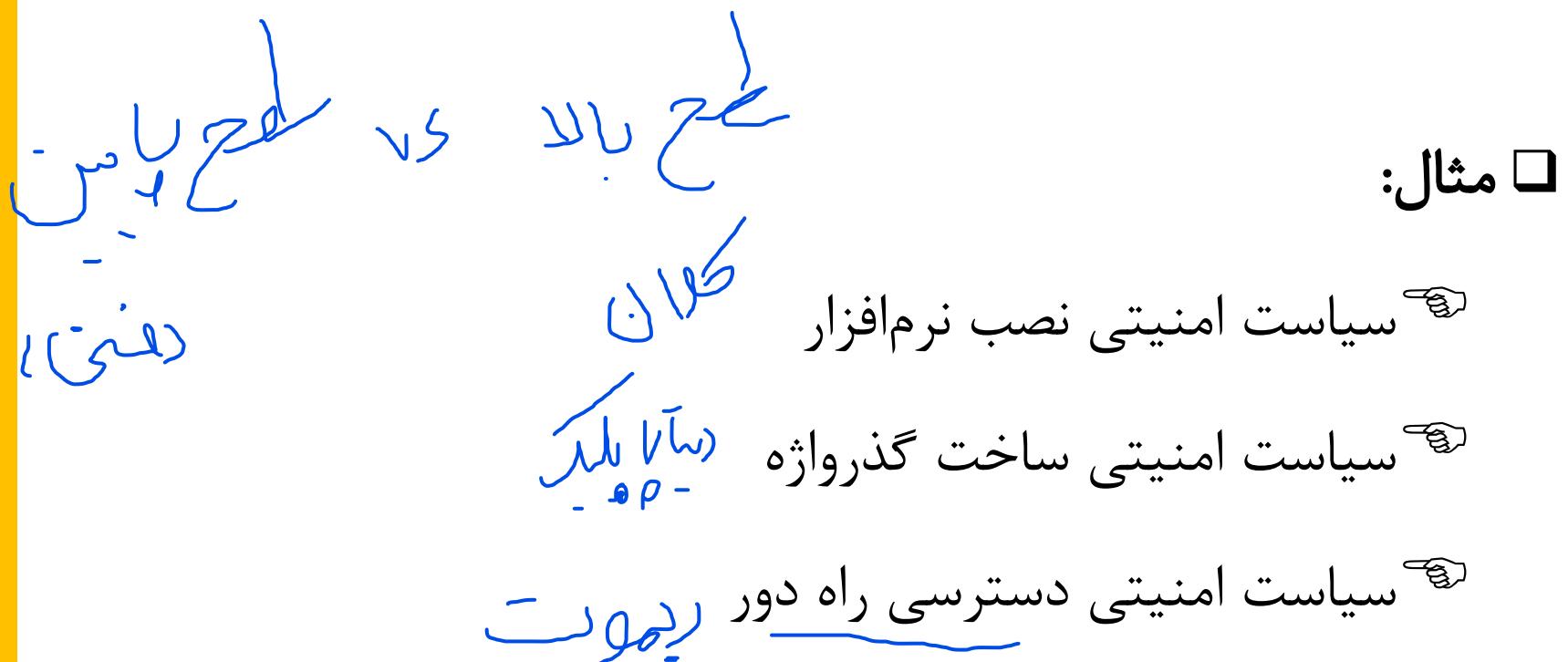
- توصیف ترسیمی؛
- از مجموعه موجودیتها و روابط آنها؛
- که به واسطه آنها خدمات امنیتی توسط یا درون سیستم فراهم می‌شود.
- مثال:

☞ مدل کنترل دسترسی نقش-مبنای (RBAC)

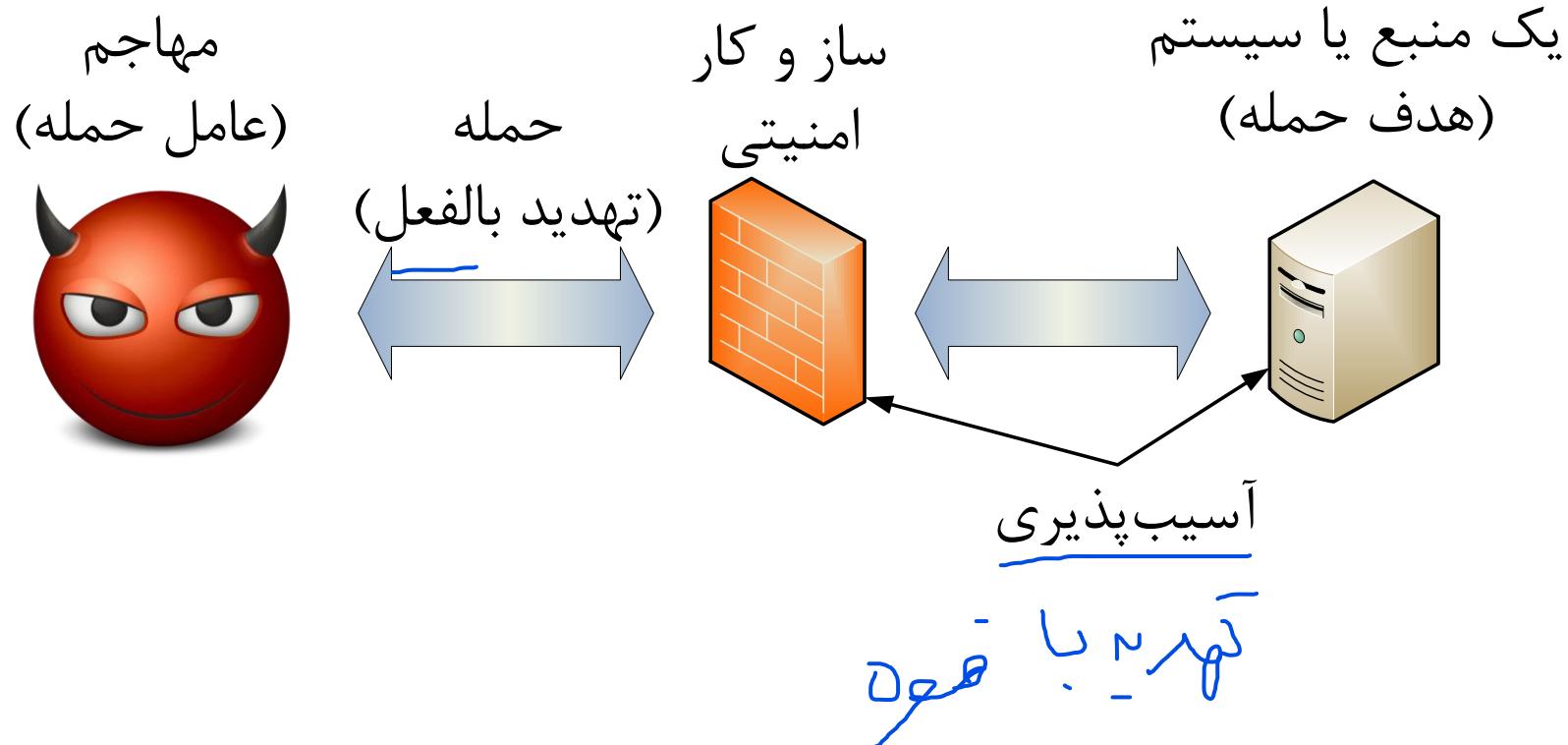
☞ مدل مهاجم (فعال / منفعل)

سیاست (خط مشی) امنیتی

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



آسیب‌پذیری، تهدید، حمله و مهاجم



آسیب‌پذیری (Vulnerability)

□ نقصان یا ضعف:

کالنگیل، استفاده
در طراحی، پیاده‌سازی، یا عملیات و مدیریت سیستم:

که با سوء استفاده از آن می‌توان سیاست امنیتی سیستم را نقض کرد.

شناخته شده

CVE: Common Vulnerabilities and Exposures

□ مثال:

آسیب‌پذیری خونریزی قلبی (HeartBleed) در OpenSSL

آسیب‌پذیری سر ریز بافر (Buffer Overflow)

در CVE نسبت به جمله‌ای روکیده دیگری که حفظ خواهد شد.

تهدید (Threat)

□ امکان بالقوه برای نقض امنیت.

□ متناظر با هر آسیب‌پذیری، (حداصل) یک تهدید وجود دارد.

□ می‌تواند عمدى یا غیر عمدى باشد.

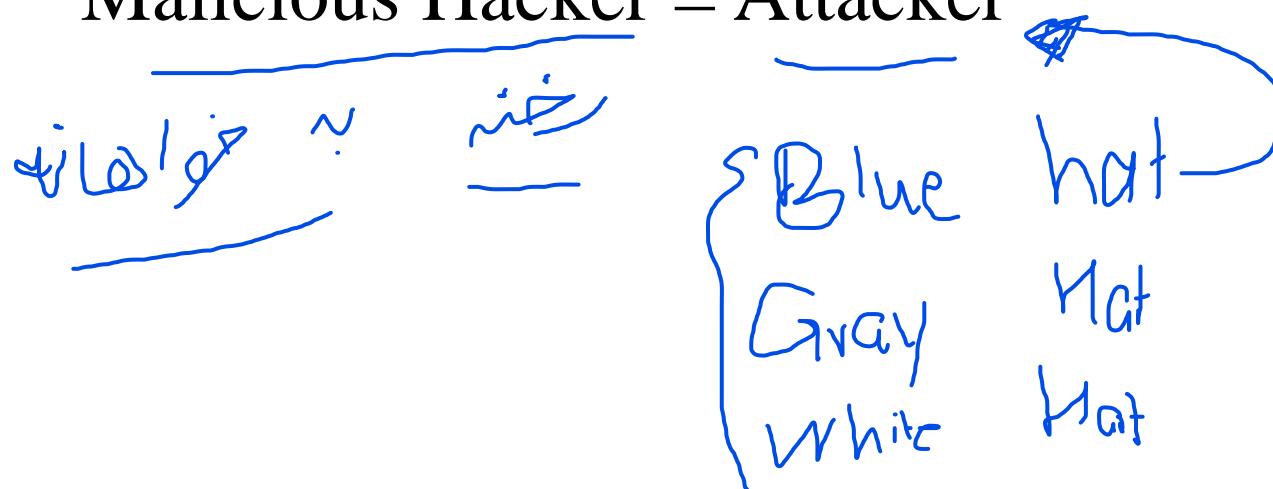
☞ عمدى: امکان نقض امنیت توسط یک موجودیت هوشمند (فرد یا سازمان)

☞ غیر عمدى: امکان خطای انسانی، عملکرد ناصحیح ابزار، وقایع طبیعی (زلزله، سیل، آتش سوزی، و ...)

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

- 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



- محتوا و جایگاه درس
- ضرورت امنیت داده و شبکه
- مفاهیم اولیه
- دشواری برقراری امنیت^۴
- انواع و ماهیت حملات
- خدمات امنیتی
- مدل‌های امنیت شبکه

دشواری برقراری امنیت

- امنیت معمولاً قربانی افزایش کارایی و مقیاس پذیری می شود.
- امنیت بالا هزینه بر است.
- کاربران عادی امنیت را به عنوان مانع در برابر انجام شدن کارها تلقی می کنند و از سیاستهای امنیتی پیروی نمی کنند.

لکن کی حل داشت می کنند

هزینه بالا

نقلاً کار باشد و مجاز

خواهی انسانی

پسند کنیست

دشواری برقراری امنیت

□ اطلاعات و نرم افزارهای 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.

فحلات کارهای کن

> نسبت نزد

دلایل نامنی شبکه‌ها

نمایش کاریش نمایش
کر->.

□ ضعف فناوری (تحلیل، طراحی، پیاده‌سازی)

پروتکل، سیستم عامل، تجهیزات

□ ضعف تنظیمات

رها کردن تنظیمات پیش‌فرض، گذرواژه‌های نامناسب، عدم استفاده از رمزگاری، راهاندازی خدمات اینترنت بدون اعمال تنظیمات لازم، ...

لبریز بیارن
یا نه!

□ ضعف سیاست‌گذاری

عدم وجود سیاست امنیتی

عدم وجود طرحی برای مقابله و بازیابی مخاطرات

نداشتن نظارت امنیتی مناسب (مدیریتی و فنی)

□ گستره امنیت تمامی منابع سازمان است و نه تنها کارگزار اصلی.

□ مسئله امنیت نیازمند نگرش مدیریتی است، نه صرفاً نگرش فنی.

سلیمان

فوج بالا

مهاجمین

□ مادام که انسانها امن فکر نکنند نمی‌توان تراکنش امن داشت.

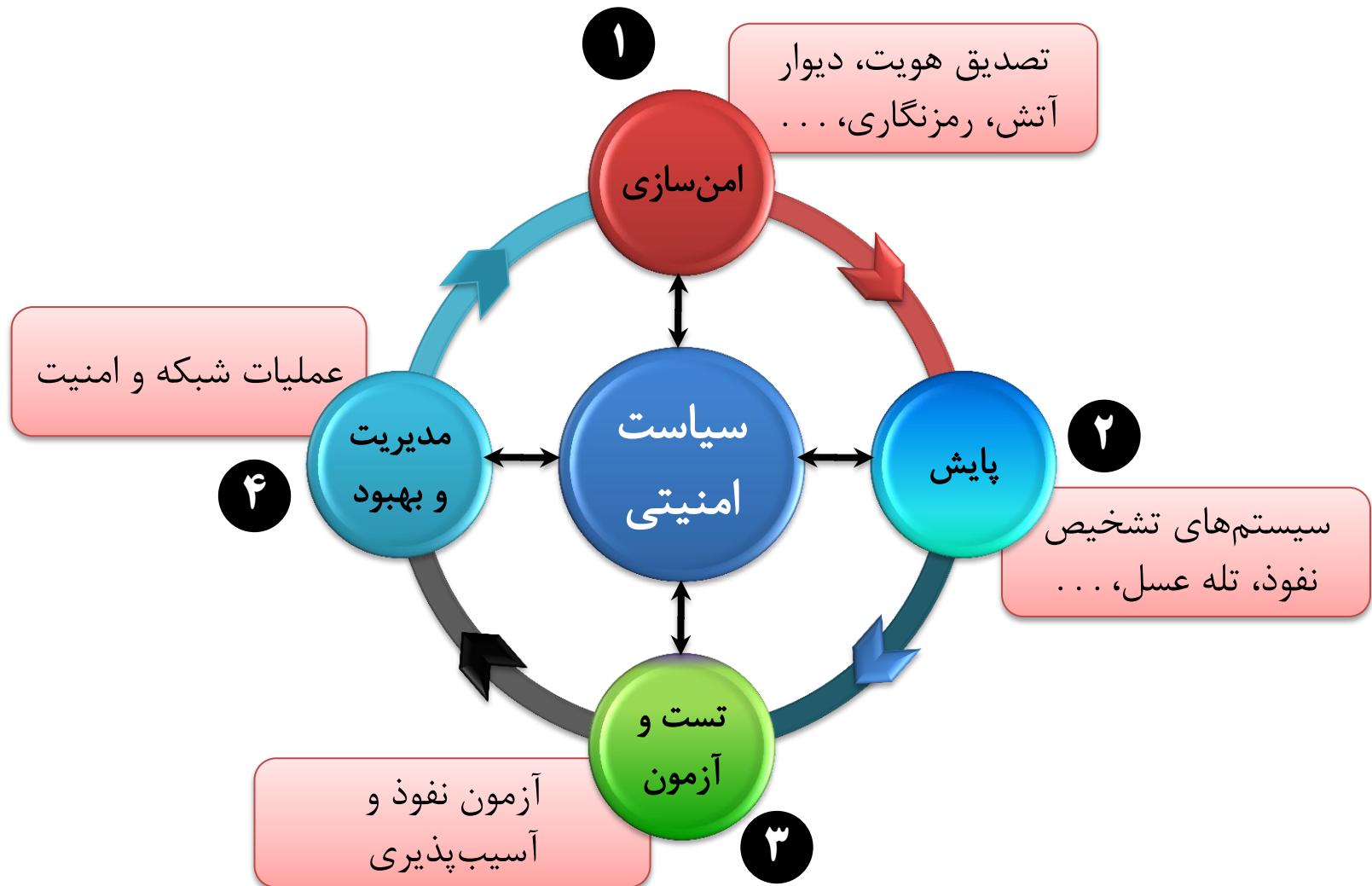
□ امن سازی یک فرآیند است نه یک وظیفه خاص و مقطوعی.

امنیت
فنی لنه قطعاً

مدیریتی (الول)

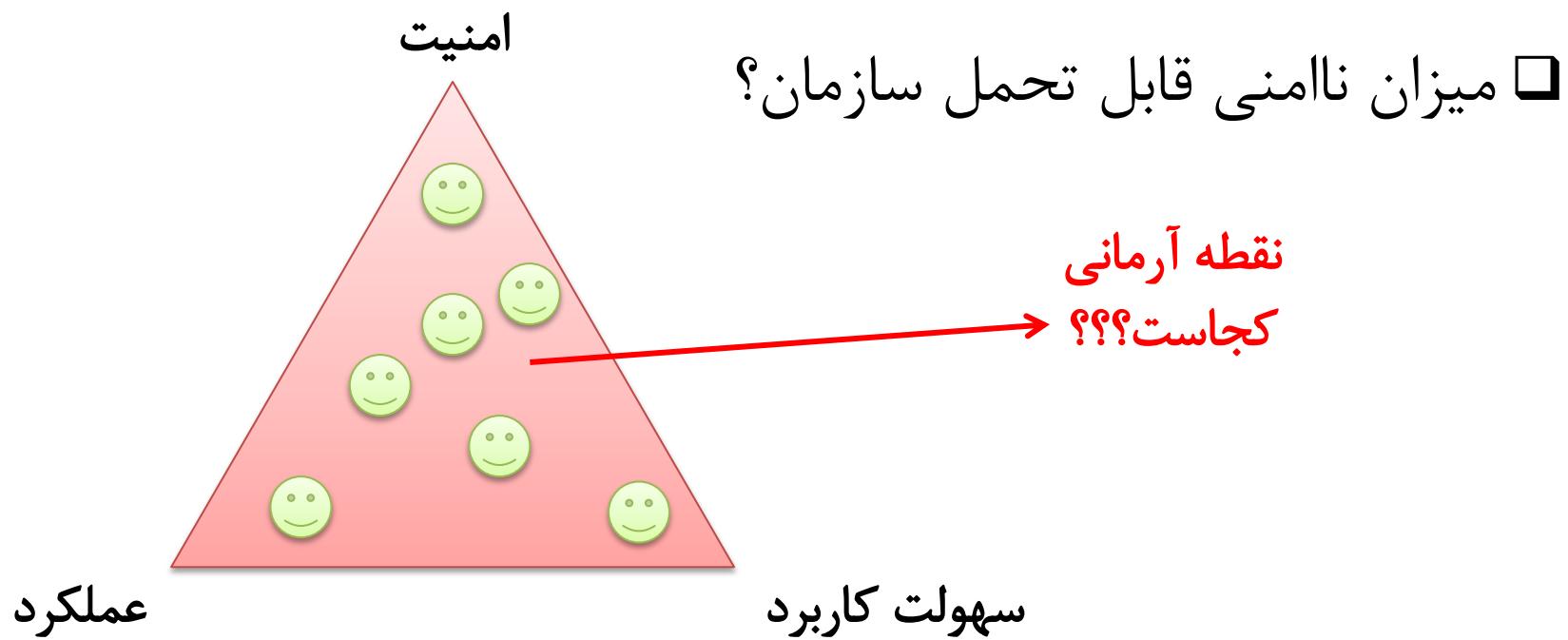
له هر چیز را باید دیدگوی

چرخه ایجاد امنیت



راهبرد امنیت سازمانی

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



- 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

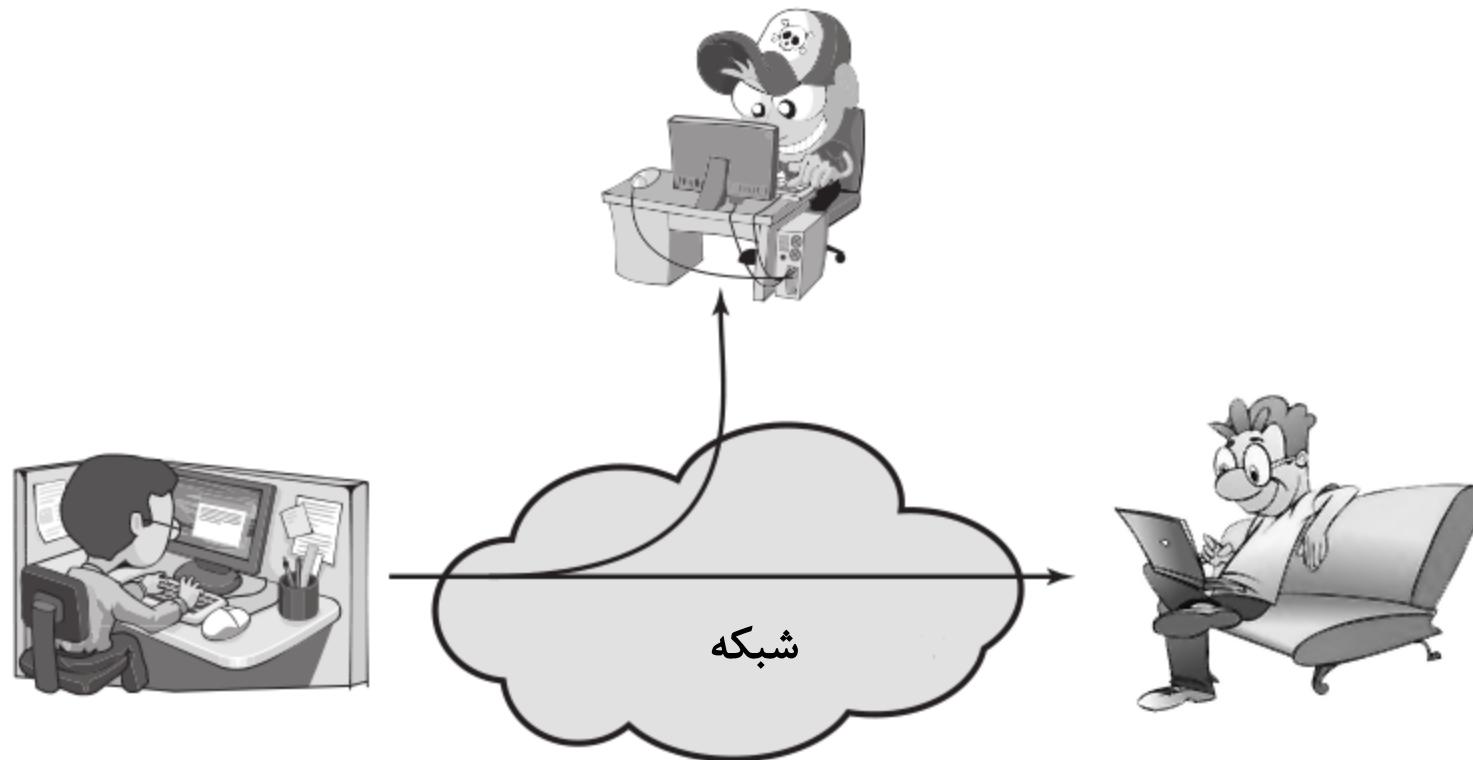
حملات منفعل (Passive)

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

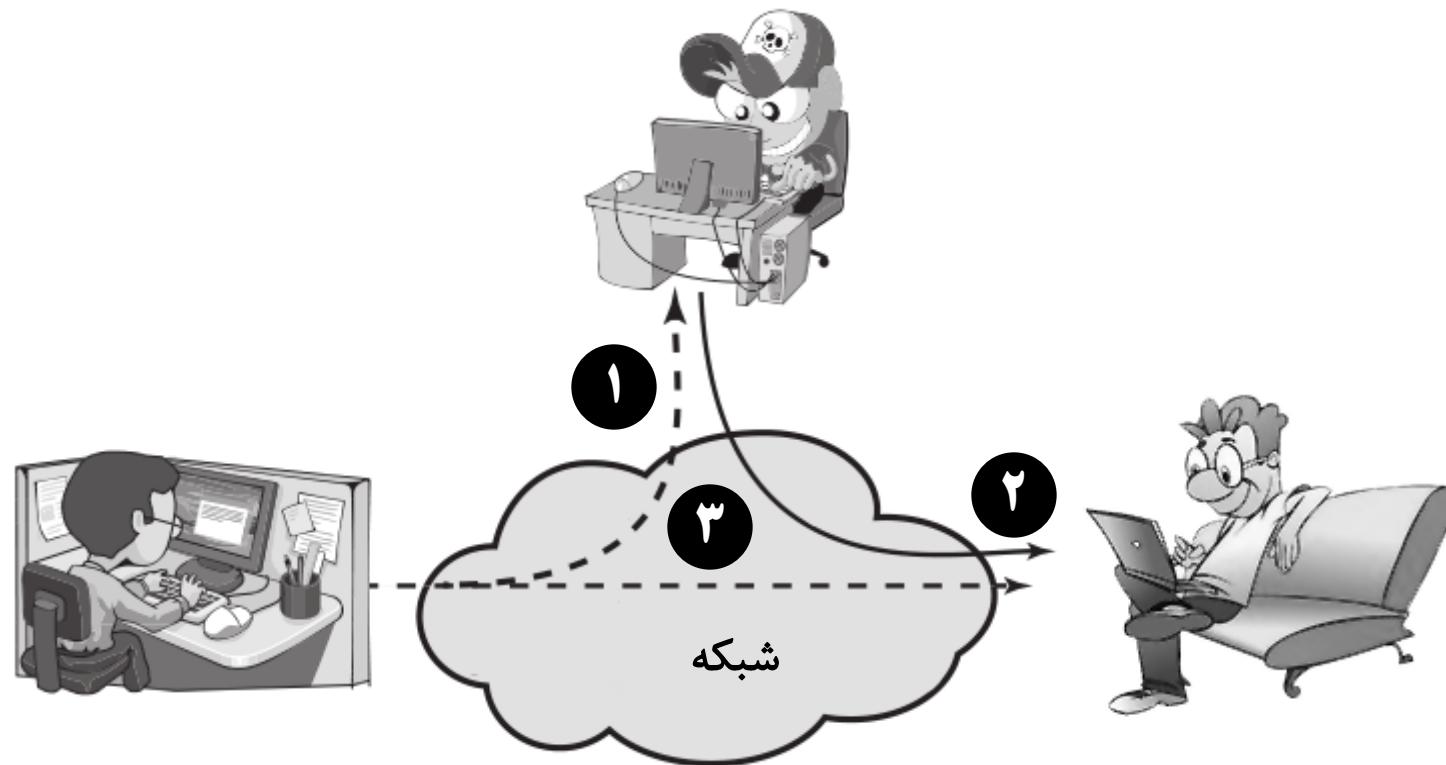
حملات فعال (Active)

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

حملات منفعل



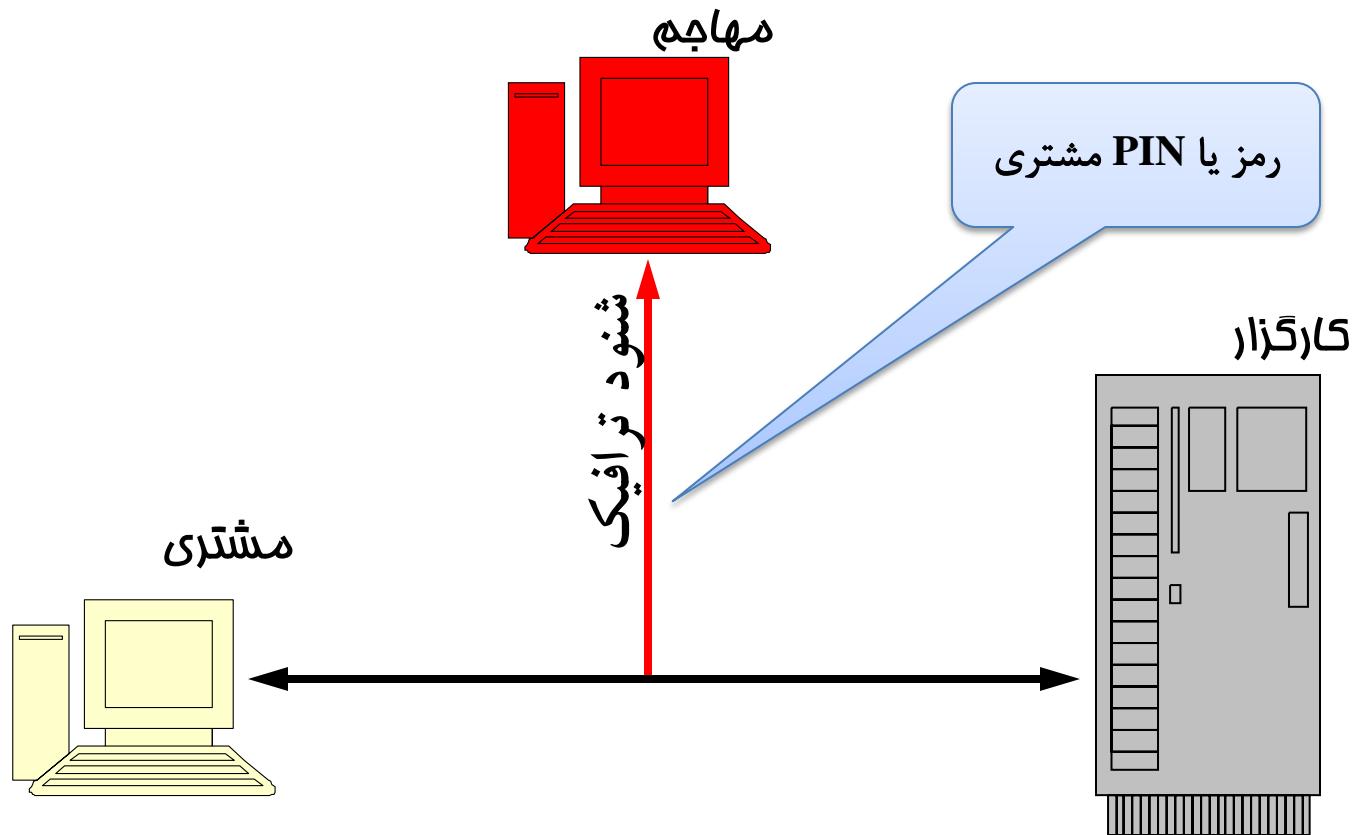
حملات فعال



حمله شنود یا استراق سمع - ۱

- هدف: نقض محترمانگی
- نتیجه: دسترسی غیرمجاز به داده‌های طبقه‌بندی شده
- راه‌های تحقق حمله:
 - ☞ اتصال فیزیکی به شبکه و دریافت بسته‌ها
 - ☞ دسترسی غیرمجاز به پایگاه داده‌ها
 - ☞ وجود ضعف و آسیب‌پذیری در سیستم کنترل دسترسی

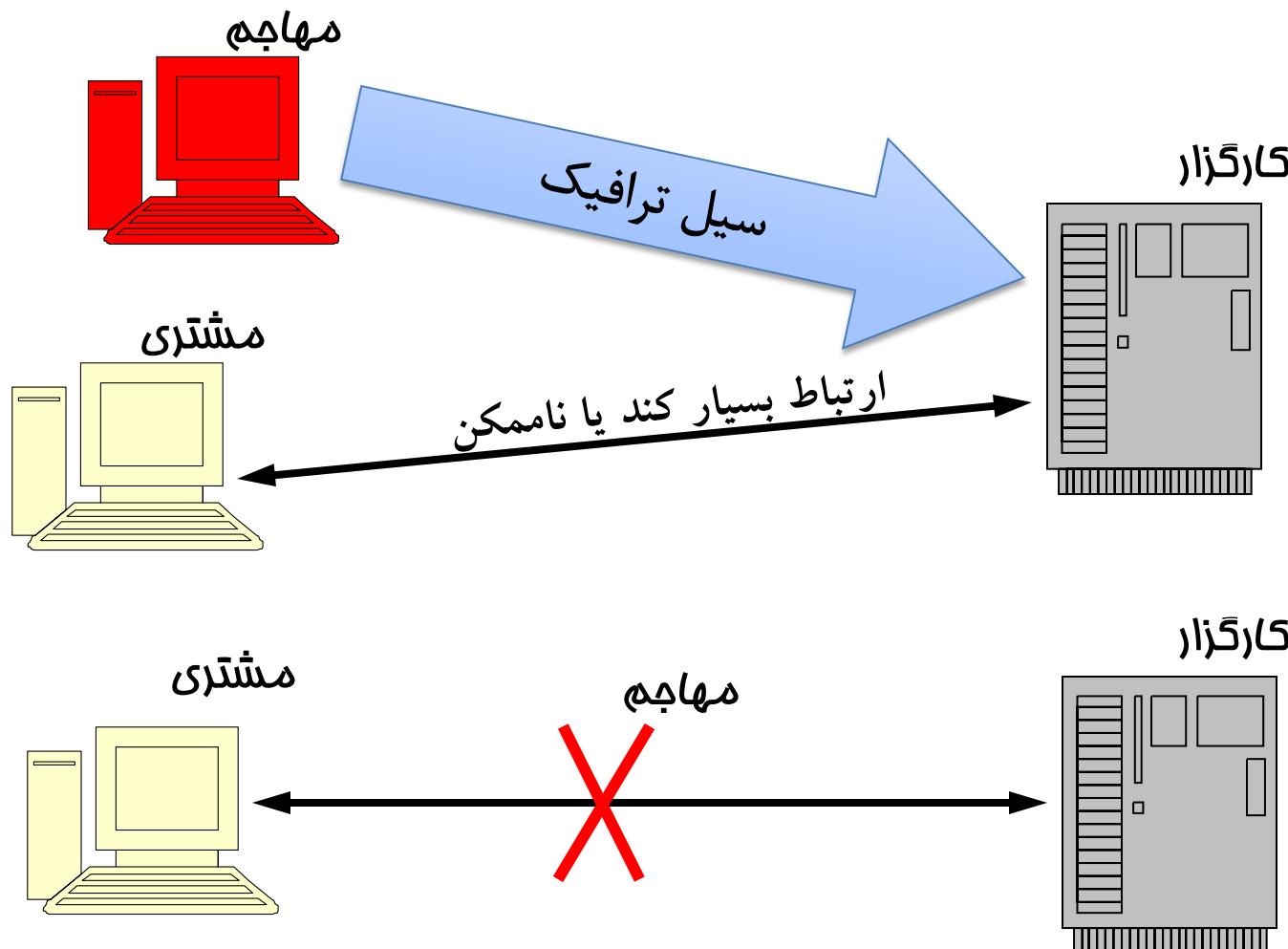
حمله شنود یا استراق سمع - ۲



حمله منع خدمت یا وقفه - ۱

- هدف: نقض دسترس پذیری
- 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 و یا 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

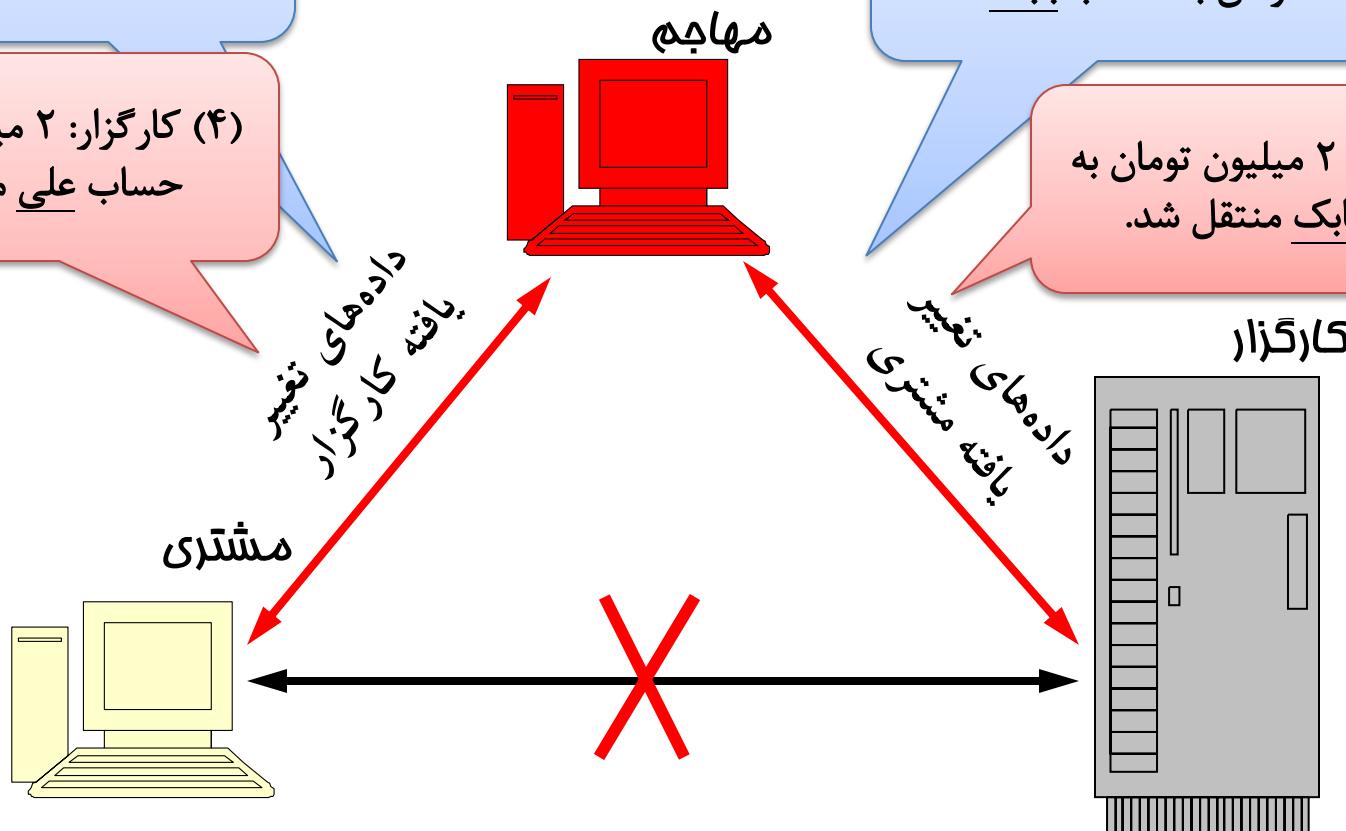
□ حمله مرد میانی (Man in the Middle) (MIM)

(۱) انتقال ۲ میلیون تومان
به حساب علی

(۴) کارگزار: ۲ میلیون تومان به
حساب علی منتقل شد.

(۲) مشتری: انتقال ۲ میلیون
تومان به حساب بابک

(۳) کارگزار: ۲ میلیون تومان به
حساب بابک منتقل شد.



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:

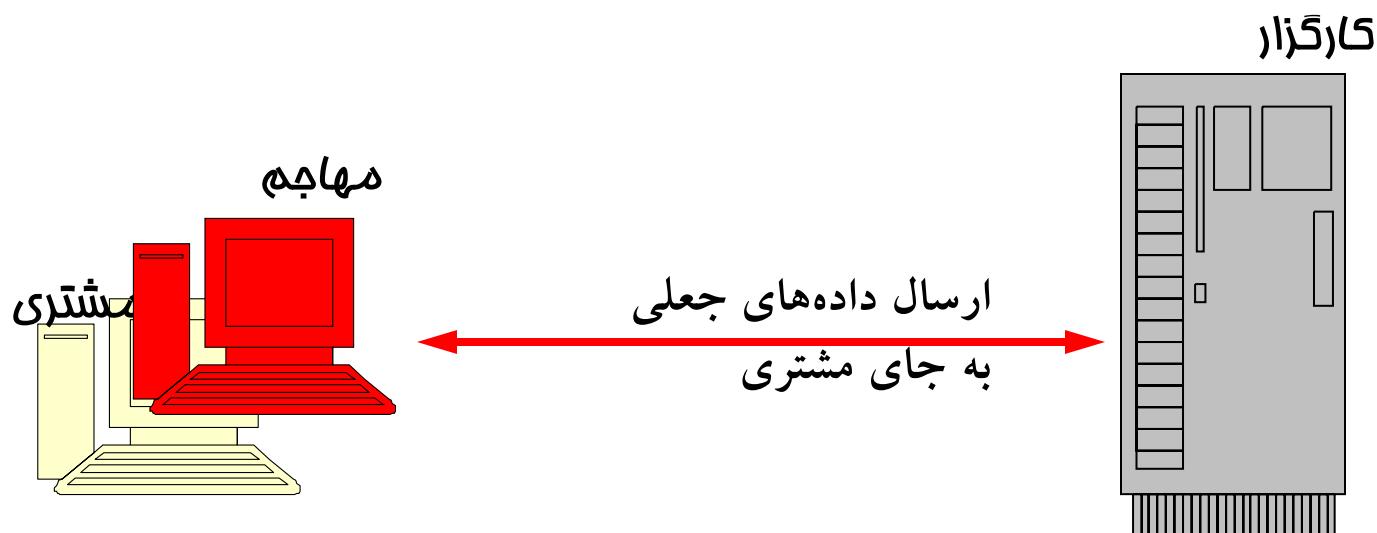
☞ اتصال فیزیکی به شبکه و دریافت بسته‌ها

☞ بازارسال بسته‌های شنود شده پس از اعمال 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)



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

پیشتر آشنا
شدیم

- محرمانگی داده‌ها (Data Confidentiality)
- صحت داده‌ها (Data Integrity)
- دسترس پذیری (Availability)
- تصدیق هویت (Authentication)
- کنترل دسترسی (Access Control)
- انکار ناپذیری (Non Repudiation)

□ 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
(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!

- محتوا و جایگاه درس

- ضرورت امنیت داده و شبکه

- مفاهیم اولیه

- دشواری برقراری امنیت

- انواع و ماهیت حملات

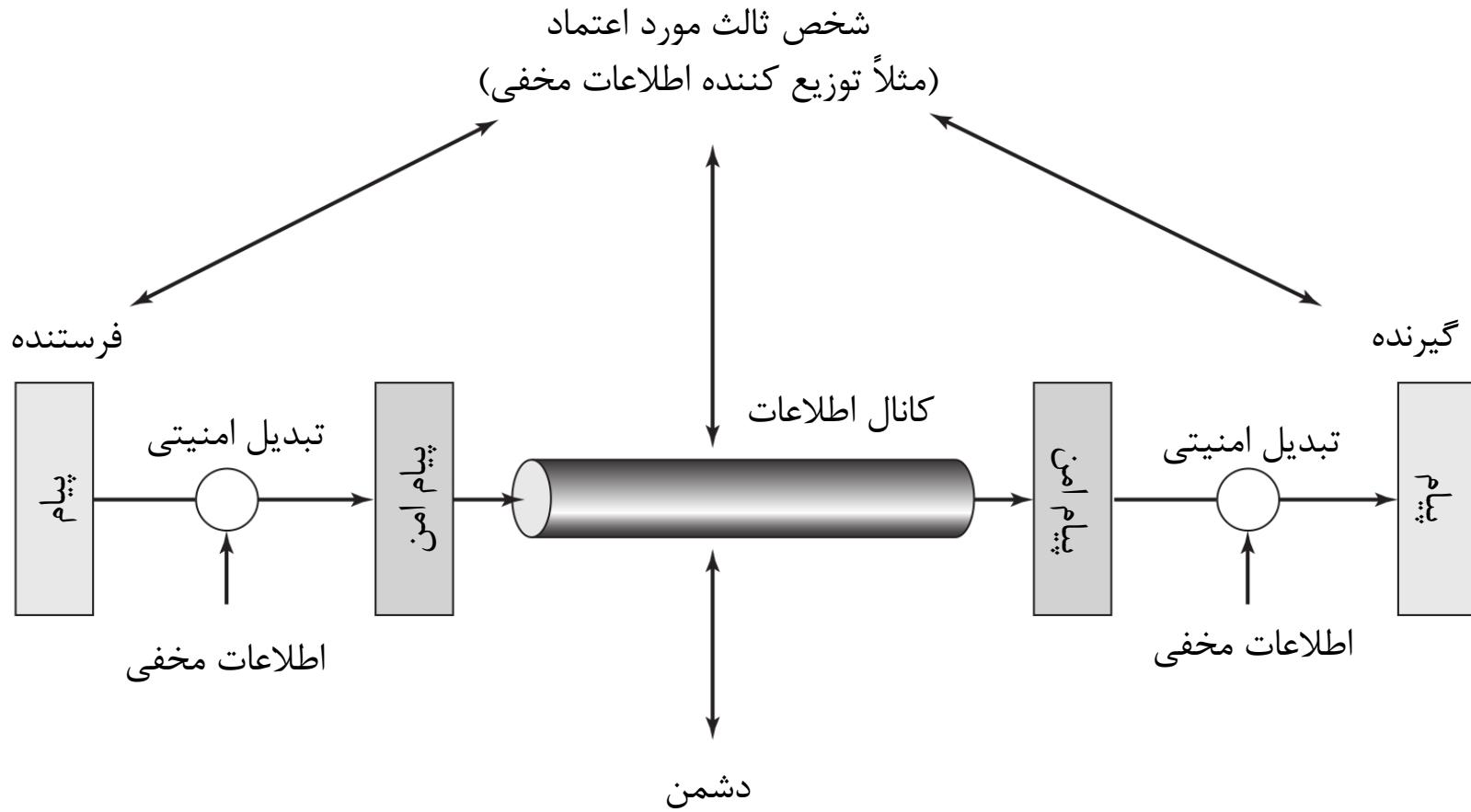
- خدمات امنیتی

- **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 نامن (مثل شبکه اینترنت)
 - ☞ نیاز به تأمین خدمات محترمانگی، صحت، تصدیق هویت، و ...
- روش‌های مورد استفاده عموماً 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



□ مدل فوق نشان مى دهد که برای فراهم آمدن یک خدمت امنيتي 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 تضمين خدمت امنيتي