

madsage
IRan Education
Research
NETwork
(IRERNET)

شبکه آموزشی - پژوهشی مادیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است

مادیج

شبکه آموزشی - پژوهشی ایران

madsg.com
مادیج



porta. Lorem ipsum
dolor mauris e
goma. Lorem ipsum.



یادداشت‌های امن و آلمان

امنیت داده و شبکه

مفاهیم و تعاریف اولیه

مرتضی امینی - نیمسال اول ۹۰-۹۱



فهرست مطالب

- محتوای درس
- ضرورت امنیت داده و شبکه
- مفاهیم اولیه
- دشواری برقراری امنیت
- انواع و ماهیت حملات
- سرویس های امنیتی
- مدل های امنیت شبکه



آنچه این درس بررسی می کند

□ این درس مفاهیم زیر را در بر می گیرد:

■ تهدیدهای امنیتی

■ نیازهای امنیتی

■ خدمات امنیتی

■ مکانیزمها و پروتکل های امنیتی

□ برای داده هایی که بر روی کامپیوترها ذخیره شده و یا بر روی

شبکه انتقال داده می شوند.



موضوعات تحت پوشش درس

- تهدیدات امنیتی
- رمزنگاری مقدماتی
- مکانیزم‌های پیشگیری
- مکانیزم‌های تشخیص
- مبانی طراحی پروتکل‌های امن
- مبانی پروتکل‌های امنیت شبکه



موضوعات خارج از محدوده پوشش درس

- رمزنگاری پیشرفته
- روشهای هک و نفوذ
- اصول نظری در امنیت اطلاعات
- ...



فهرست مطالب

- محتوای درس
- ضرورت امنیت**
- مفاهیم اولیه
- دشواری برقراری امنیت
- سرویس های امنیتی
- انواع و ماهیت حملات
- مدل های امنیت شبکه



امنیت چیست؟

□ امنیت به (طور غیر رسمی) عبارتست از حفاظت از آنچه برای ما ارزشمند است.

■ در برابر حملات عمدی

■ در برابر حملات غیر عمدی





اقدامات امنیتی

□ پیشگیری (Prevention):

■ جلوگیری از خسارت

□ ردیابی (Tracing):

■ تشخیص (Detection)

□ میزان خسارت

□ هویت دشمن

□ کیفیت حمله (زمان، مکان، دلایل حمله، نقاط ضعف...)

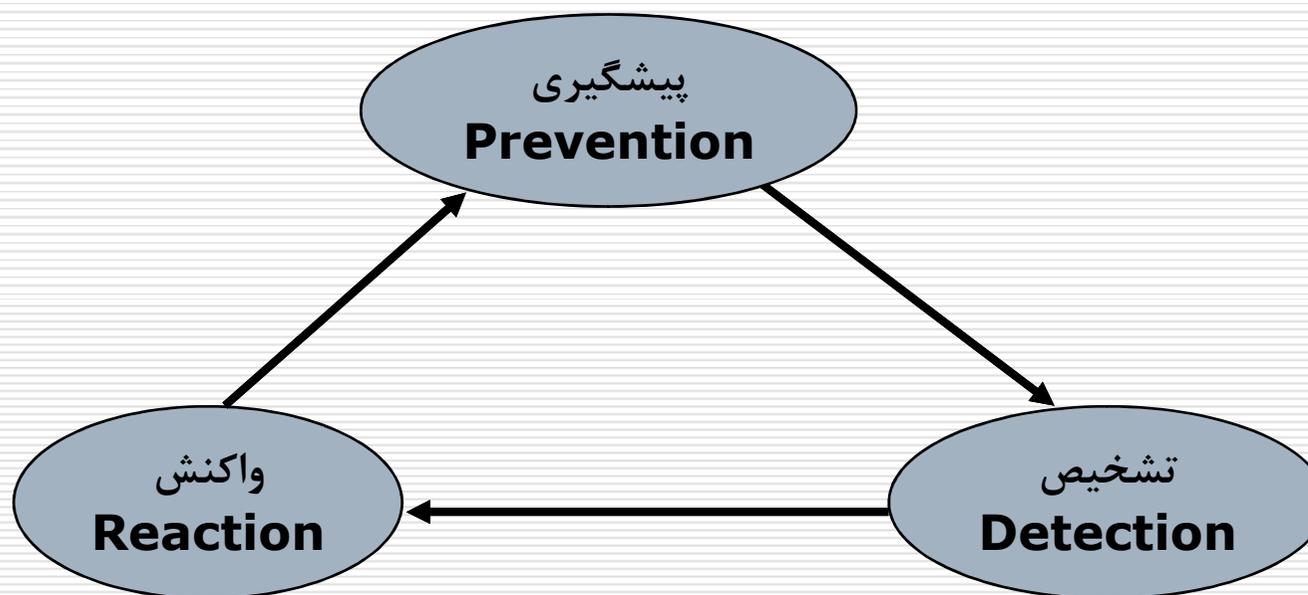
□ واکنش (Reaction):

■ ترمیم، بازیابی و جبران خسارات

■ جلوگیری از حملات مجدد



اقدامات امنیتی





امنیت اطلاعات: گذشته و حال

امنیت اطلاعات در دنیای نوین

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

امنیت اطلاعات سنتی

- نگهداری اطلاعات در قفسه‌های قفل دار
- نگهداری قفسه‌ها در مکان‌های امن
- استفاده از نگهبان
- استفاده از سیستم‌های الکترونیکی نظارت
- به طور کلی: روشهای فیزیکی و مدیریتی



نیازهای امنیتی

□ بنابراین :

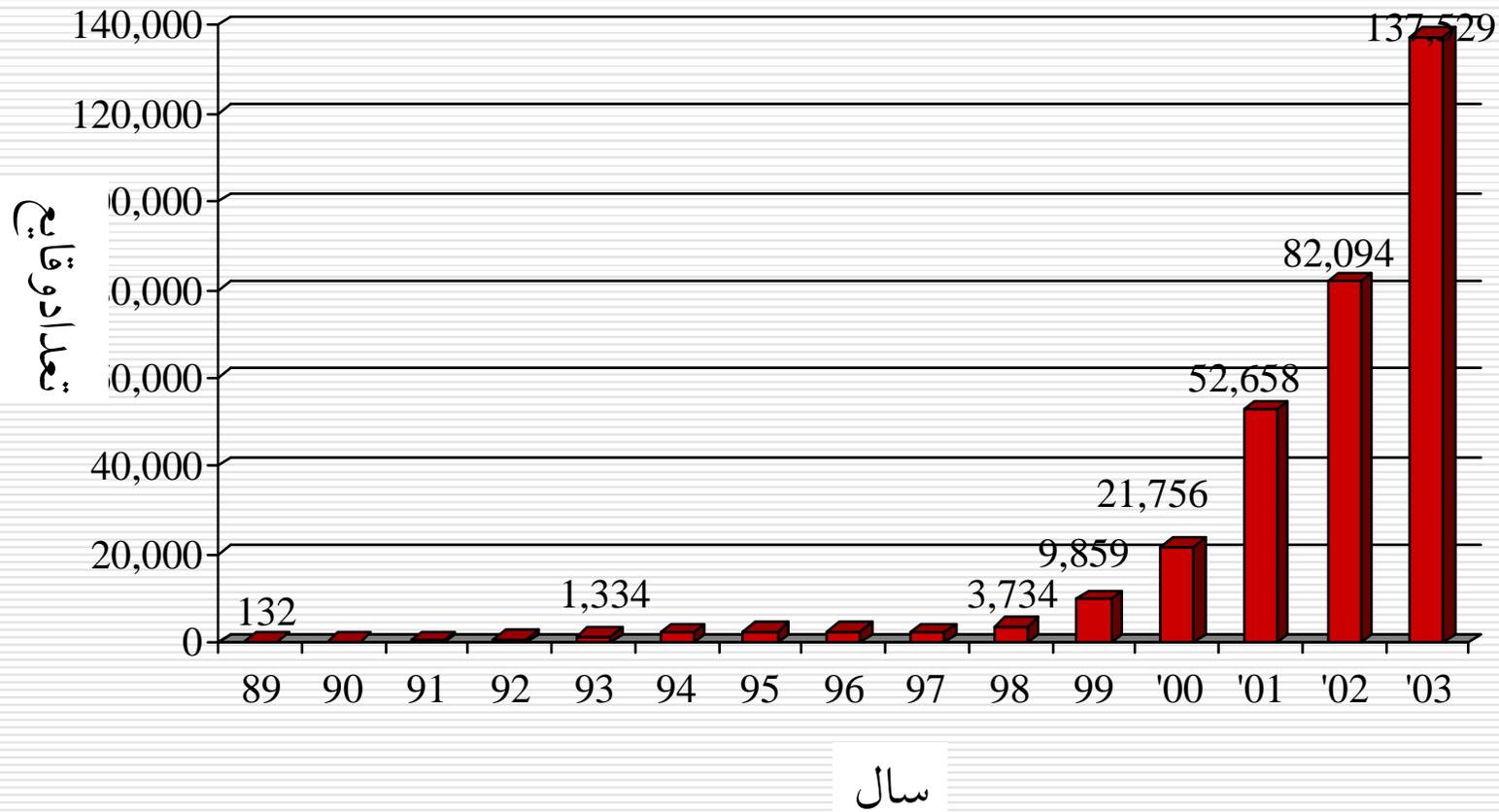
■ در گذشته، امنیت با حضور فیزیکی و نظارتی تامین می شد،

ولی

■ امروزه از ابزارهای خودکار و مکانیزم‌های هوشمند برای حفاظت از داده ها استفاده می شود.

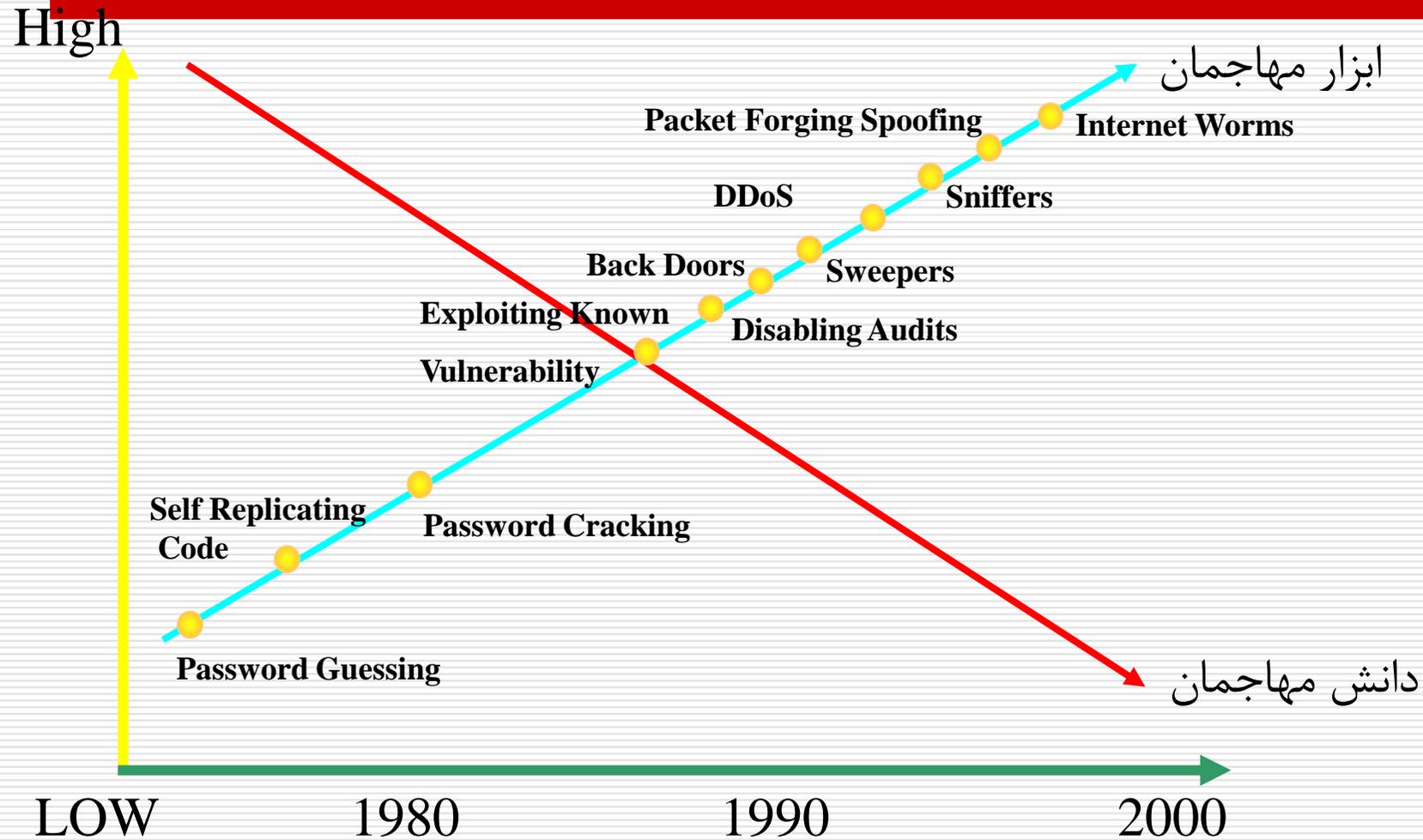
آمار منتشر شده توسط آپا

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).



فهرست مطالب

- محتوای درس
- ضرورت امنیت
- مفاهیم اولیه
- دشواری برقراری امنیت
- سرویس های امنیتی
- انواع و ماهیت حملات
- مدل های امنیت شبکه



مبانی امنیت داده‌ها

امنیت داده‌ها: مبتنی است بر تحقق سه ویژگی محرمانگی، جامعیت و دسترس پذیری.



✓ محرمانگی (Confidentiality)

- عدم افشای غیرمجاز داده‌ها

✓ صحت (Integrity)

- عدم دستکاری داده‌ها توسط افراد یا نرم‌افزارهای غیرمجاز

✓ دسترس پذیری (Availability)

- دسترسی به داده‌ها توسط افراد مجاز در هر مکان و در هر زمان



محرمانگی

□ **تعریف:** عدم افشای غیرمجاز داده‌ها

□ **مکانیزم متداول:** رمزنگاری و کنترل دسترسی





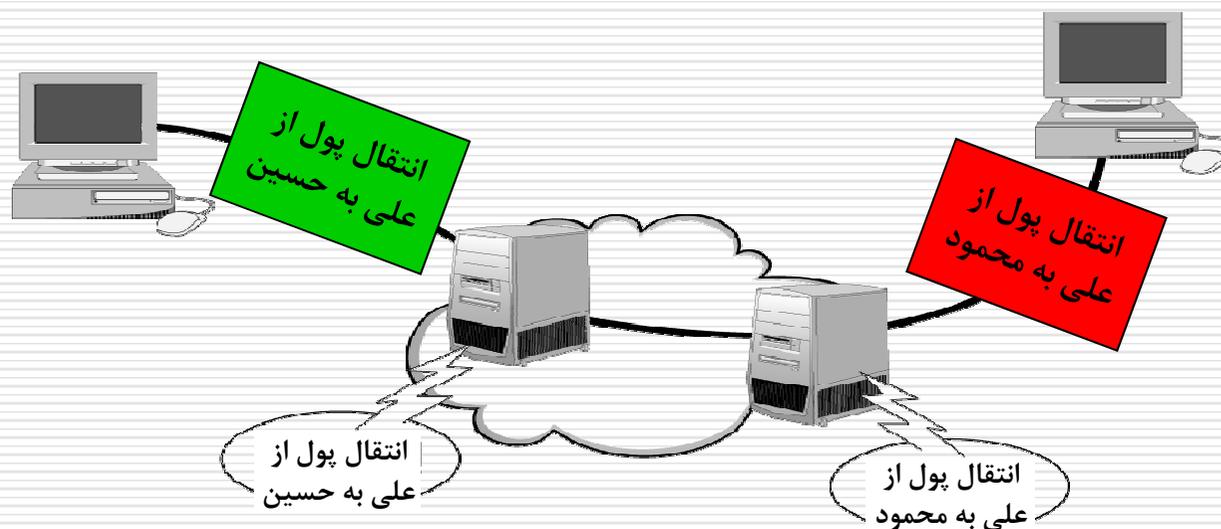
صحت

□ **تعریف:** عدم دستکاری داده‌ها توسط افراد یا نرم‌افزارهای غیرمجاز

■ **صحت منبع (Origin Integrity)**

■ **صحت داده (Data Integrity)**

□ **مکانیزم متداول:** امضای دیجیتال، کد احراز پیام، کنترل دسترسی





دسترسی پذیری

- **تعریف:** دسترسی به داده‌ها و سرویس‌دهی به افراد مجاز در هر مکان و در هر زمان.
- **مکانیزم متداول:** تهیه پشتیبان و نصب سیستم‌های محافظ مناسب





دلایل ناامنی شبکه‌ها

❑ ضعف فناوری

- پروتکل، سیستم عامل، تجهیزات

❑ ضعف تنظیمات

- رهاکردن تنظیمات پیش فرض، گذرواژه‌های نامناسب، عدم استفاده از رمزنگاری، راه‌اندازی سرویس‌های اینترنت بدون اعمال تنظیمات لازم، ...

❑ ضعف سیاست‌گذاری مدیریتی

- عدم وجود سیاست امنیتی
- عدم وجود طرحی برای مقابله و بازیابی مخاطرات
- نداشتن نظارت امنیتی مناسب (مدیریتی و فنی)

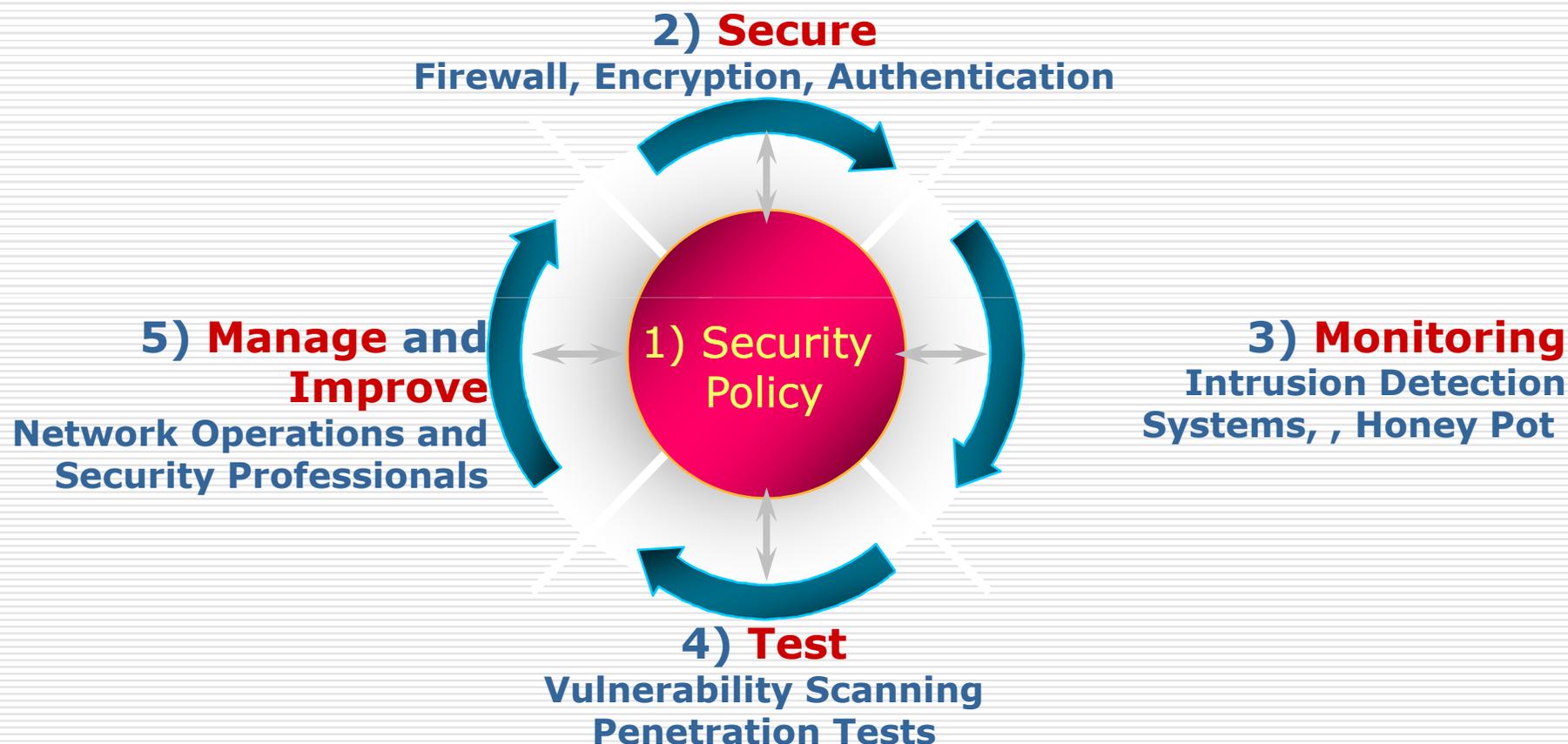


امن سازی

- گستره امنیت تمامی منابع سازمان است و نه تنها کارگزار اصلی.
- نگرش **مدیریتی** به مسئله امنیت لازم است و نه نگرش فنی.
- مهاجمین داخلی و مجاز 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 حلقه پایان ناپذیر است





خط‌مشی (سیاست) امنیتی

□ خط‌مشی (سیاست) امنیتی (Security Policy): نیازمندیهای امنیتی یک سازمان و یا یک سیستم اطلاعاتی / ارتباطی را بیان می‌نماید.

□ در تعریف سیاست‌های امنیتی:

- باید بدانید تا چه اندازه و در چه نقاطی نیاز به اقدامات محافظتی دارید.
- باید مشخص شود که چه نوع اطلاعاتی در سازمان وجود دارد و هر یک تا چه حد قابل دسترسی برای هر یک از افراد سازمان است.
- باید بدانید چه افرادی، چه مسئولیت‌هایی در اجرای اقدامات محافظتی سازمان دارند.
- ارتباط این افراد با کاربران عادی سازمان چگونه بوده و چه راهنمایی و آموزش‌هایی در مواقع خطر و بروز ویروس باید به آنان ارائه کنند.



تعاریف و مفاهیم اولیه (از Bishop)

- **حمله (Attack):** تلاش عمدی برای رخنه در یک سیستم یا سوء استفاده از آن.
- **ریخنه (Breach):** نقض سیاست امنیتی یک سیستم
- **نفوذ (Intrusion):** فرایند حمله و رخنه ناشی از آن
- **آسیب پذیری (Vulnerability):** هر گونه نقطه ضعف در توصیف، طراحی، پیاده سازی، پیکربندی، اجرا که بتوان از آن سوءاستفاده کرده و سیاستهای امنیتی سیستم را نقض کرد.



تعاریف و مفاهیم اولیه

□ مهاجم و هکر (Attacker and Hacker)

■ هک (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 هک خصمانه است.

Malicious Hacker = Attacker



تعاریف و مفاهیم اولیه (از Stallings)

- **حمله امنیتی (Security Attack):** عملی که امنیت اطلاعات سازمان را نقض می کند.
- **مکانیزم امنیتی (Security Mechanism):** روش در نظر گرفته شده برای تشخیص، جلوگیری و بازیابی از حملات. هر مکانیزم امنیتی در واقع یکی از روشهای پیاده سازی یک سیاست امنیتی است.
- **سرویس امنیتی (Security Service):** سرویس های تضمین کننده امنیت با استفاده از مکانیزم های بالا.

- سیاست امنیتی با مکانیزم امنیتی چه تفاوتی دارد.
ر.س : ارتباط آنها با هم بیان شد
sadoddin, 1/8/2005



تعاریف و مفاهیم اولیه

- آسیب‌پذیری (**Vulnerability**): درز یا رخنه شناخته‌شده و یا مشکوک در طراحی یا عملکرد سخت‌افزار یا نرم‌افزار یک سیستم که موجب نفوذ در آن سیستم می‌گردد.

- نفوذ (**Intrusion**): هر مجموعه از اعمال که هدف آن نقض **محرمانگی**، **صحت** و یا **دسترسی‌پذیری** یک منبع باشد.

- **حمله (Attack)**: به یک نفوذ عمدی در یک سیستم اطلاعاتی / ارتباطی، حمله گفته می‌شود (معمولاً با بهره‌گیری از آسیب‌پذیری‌های موجود).



تعاریف و مفاهیم اولیه

□ **مکانیزم امنیتی (Security Mechanism):** به هر روش، ابزار و یا رویه‌ای که برای اعمال یک سیاست امنیتی به کار می‌رود، یک مکانیزم امنیتی گویند.

□ **سرویس امنیتی (Security Service):** به سرویس‌های تضمین‌کننده امنیت در یک سیستم و یا شبکه گفته می‌شود.



فهرست مطالب

- محتوای درس
- ضرورت امنیت
- مفاهیم اولیه
- دشواری برقراری امنیت
- سرویس های امنیتی
- انواع و ماهیت حملات
- مدل های امنیت شبکه



دشواری برقراری امنیت

- تعامل پروتکلها پیچیدگی را افزایش داده و امنیت را تهدید می کند.
- 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.



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 می گیرند و

از انجام آن لذت می برند.

□ ملاحظات امنیتی در هنگام طراحی های اولیه سیستم ها و

شبکه ها در نظر گرفته نمی شود.



فهرست مطالب

- محتوای درس
- ضرورت امنیت
- مفاهیم اولیه
- دشواری برقراری امنیت
- سرویس های امنیتی**
- انواع و ماهیت حملات
- مدل های امنیت شبکه



سرویس‌های امنیتی

- حفظ صحت داده‌ها (Integrity)
- حفظ محرمانگی داده‌ها (Confidentiality)
- احراز اصالت (Authentication)
- کنترل دسترسی (Access Control)
- عدم انکار (Non-repudiation)
- دسترس پذیری (Availability)



سرویس‌های امنیتی

□ **حفظ صحت داده‌ها:** اطمینان از اینکه آنچه رسیده همان است که فرستاده شده.

- کد احراز هویت پیام (MAC)
- امضاء

□ **حفظ محرمانگی داده‌ها:** اطمینان از اینکه تنها کاربران مورد نظر قادر به درک پیامها است.

- رمزنگاری



سرویس های امنیتی

□ **احراز اصالت:** اطمینان از این که کاربر همانی است که ادعا می کند.

■ کنترل هویت

□ **کنترل دسترسی:** کاربر تنها به منابع مقرر شده حق دسترسی دارد.

■ مجازشماری هم نامیده می شود (هر چند که چندان درست نیست).



سرویس های امنیتی

- **عدم انکار:** عدم امکان انکار دریافت یا ارسال توسط گیرنده و فرستنده
■ امضاء
- **دسترس پذیری:** در دسترس بودن به موقع خدمات برای کاربران مجاز



فهرست مطالب

- محتوای درس
- ضرورت امنیت
- مفاهیم اولیه
- دشواری برقراری امنیت
- سرویس های امنیتی
- انواع و ماهیت حملات
- مدل های امنیت شبکه



انواع حملات

انواع حملات بر حسب نتیجه:

- **وقفه (Interruption):** اختلال در شبکه و تبادل اطلاعات
- **استراق سمع (Interception/Eavesdropping):** دسترسی غیرمجاز به داده‌های طبقه‌بندی شده با شنود از شبکه
- **دستکاری داده‌ها (Modification):** تغییر غیرمجاز داده‌های سیستم یا شبکه
- **جعل (افزودن) اطلاعات (Fabrication):** اضافه کردن داده‌هایی که می‌توانند مخرب یا منشأ سوء استفاده باشند.



انواع حملات (ادامه)

انواع حملات از نظر تاثیر:



حملات فعال (Active):

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

حملات غیرفعال (Passive):

- ✦ استراق سمع (Eavesdropping)
- ✦ انتشار پیغام (Release of message)



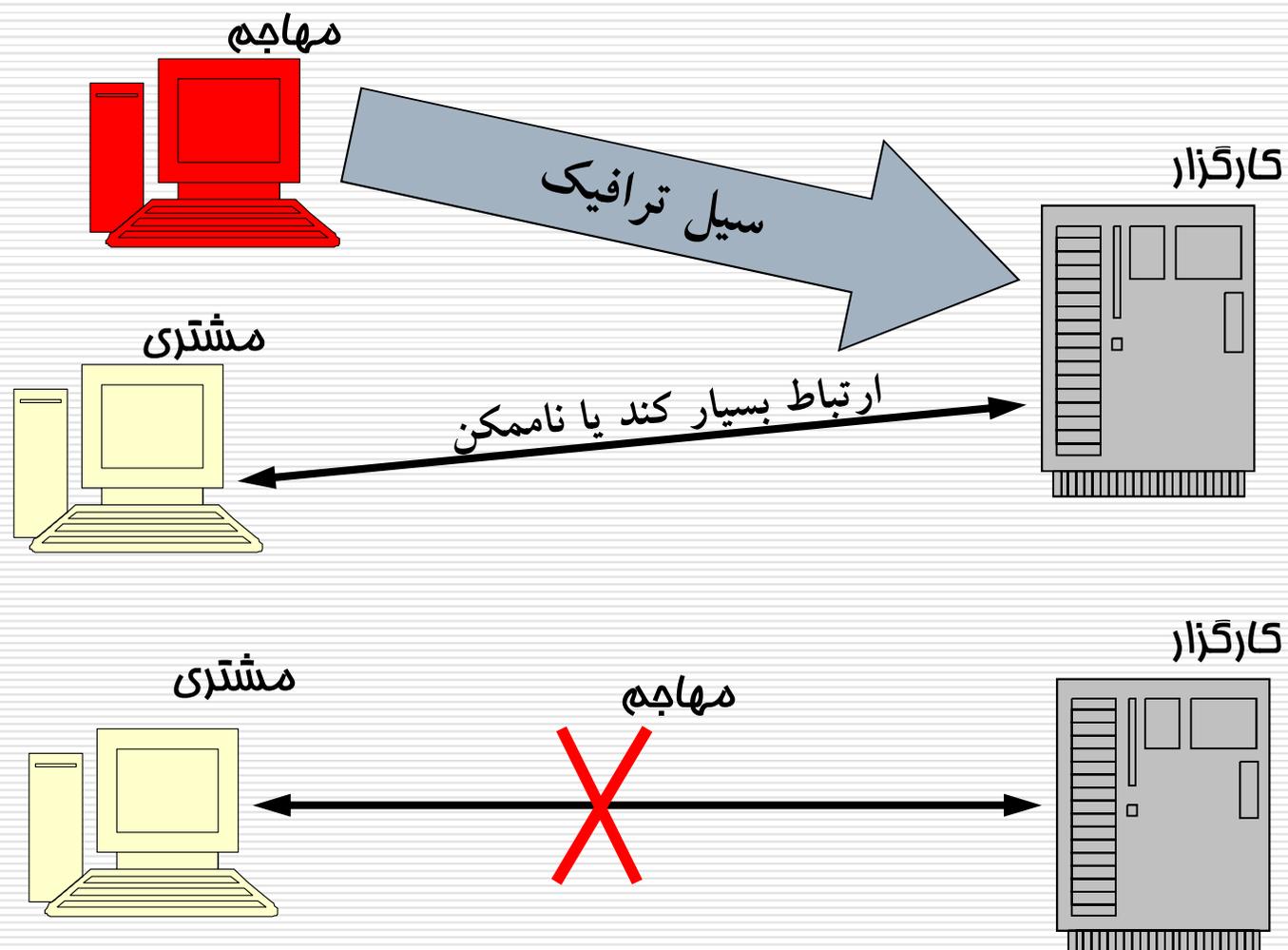
Sniffer



حمله وقفه

- هدف: نقض دسترس پذیری
- نتیجه حمله: کاهش کارایی و یا عدم امکان دسترسی کاربران به شبکه و یا سرویس های فراهم شده
- راه های تحقق حمله:
 - ارسال بسته و درخواست های مشکل دار
 - راه اندازی سیل ترافیکی
 - استفاده از ضعف ها و آسیب پذیری های نرم افزاری شبکه و یا سرویس ها

حمله وقفه (ادامه)



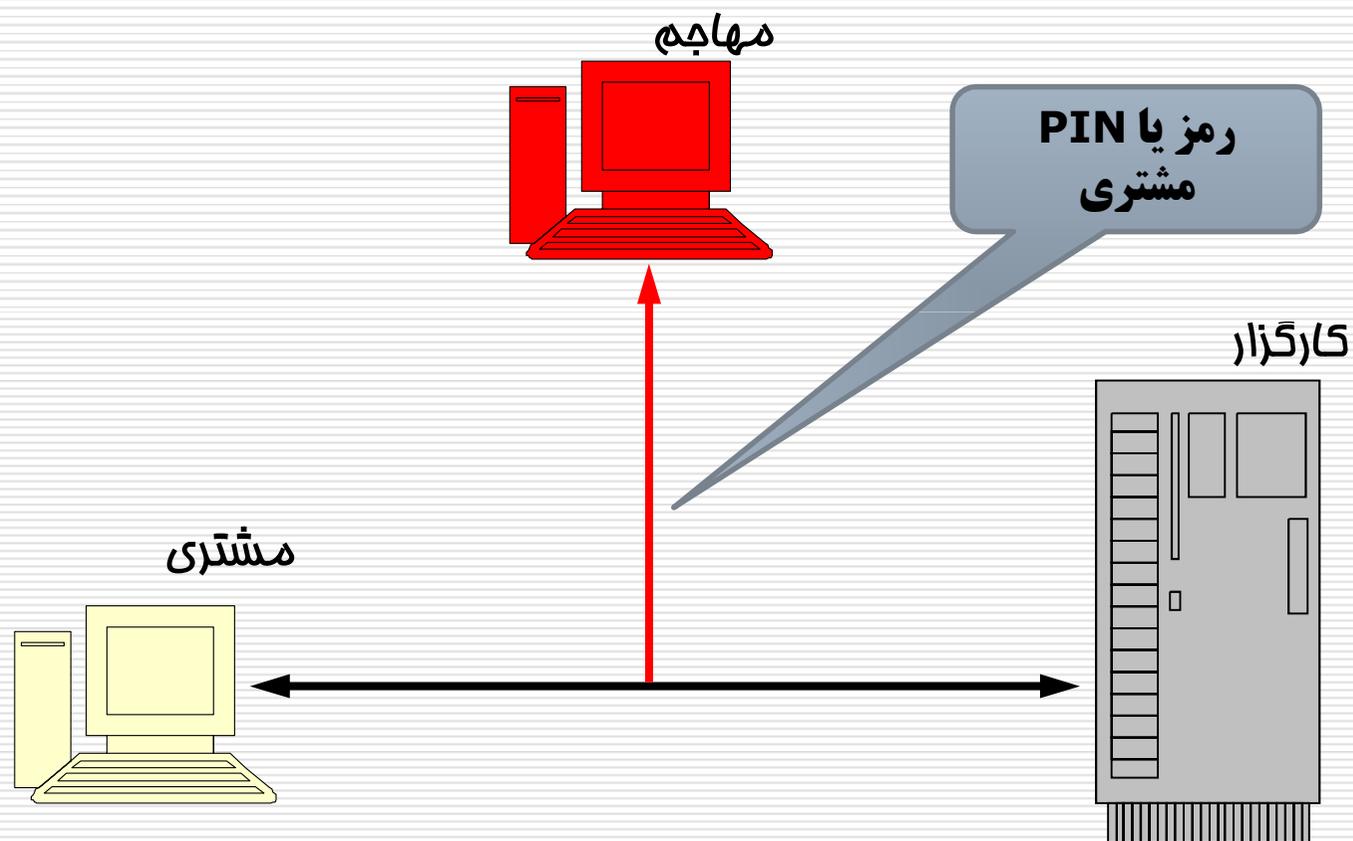


حمله شنود یا استراق سمع

- 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 (ادامه)





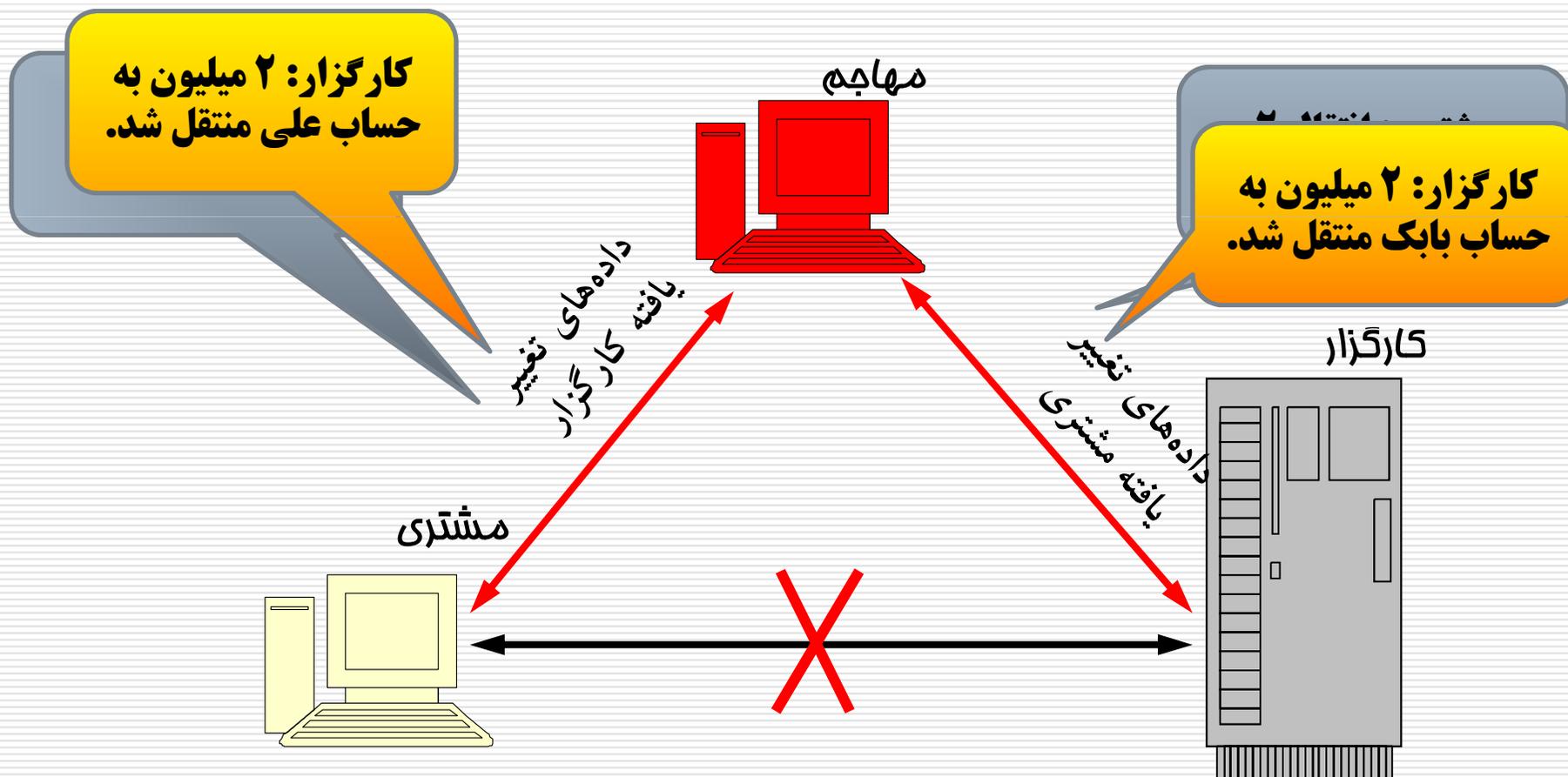
حمله دستکاری داده‌ها

- 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 پایگاه داده‌ها و تغییر غیرمجاز در آن
 - وجود ضعف و آسیب‌پذیری در سیستم کنترل دسترسی و صحت



حمله دستکاری داده‌ها

□ حمله مرد میانی (Man in the Middle)





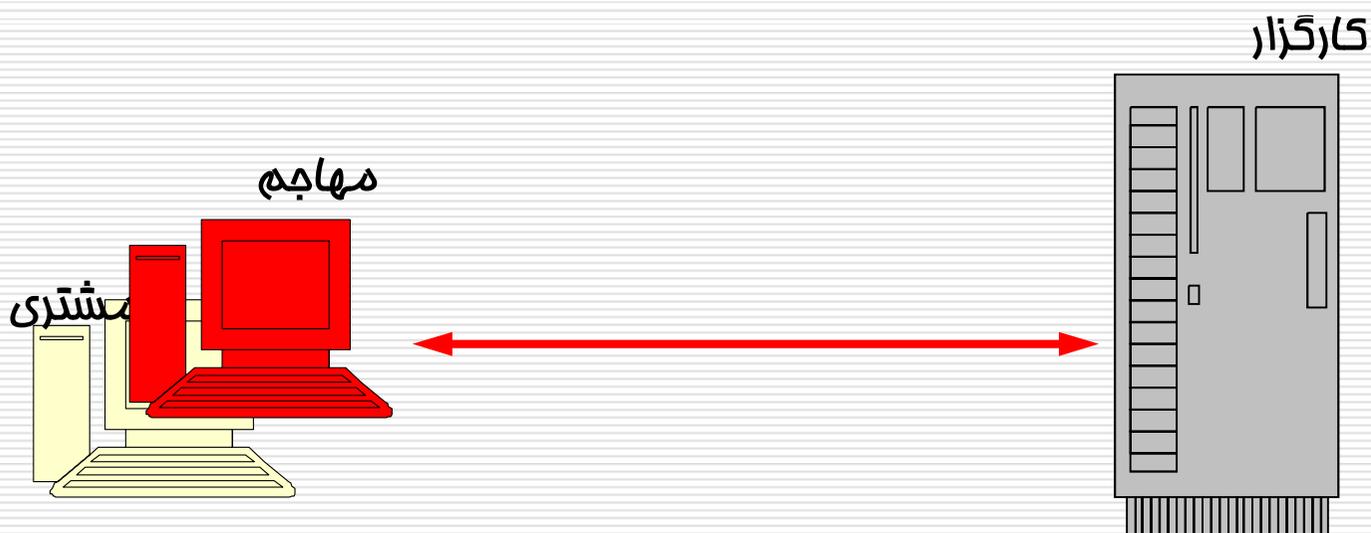
حمله جعل اطلاعات

- 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 مکانیزم احراز هویت و کنترل صحت



حمله جعل اطلاعات (ادامه)

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





فهرست مطالب

- محتوای درس
- ضرورت امنیت
- مفاهیم اولیه
- دشواری برقراری امنیت
- سرویس های امنیتی
- انواع و ماهیت حملات
- مدل‌های امنیت شبکه



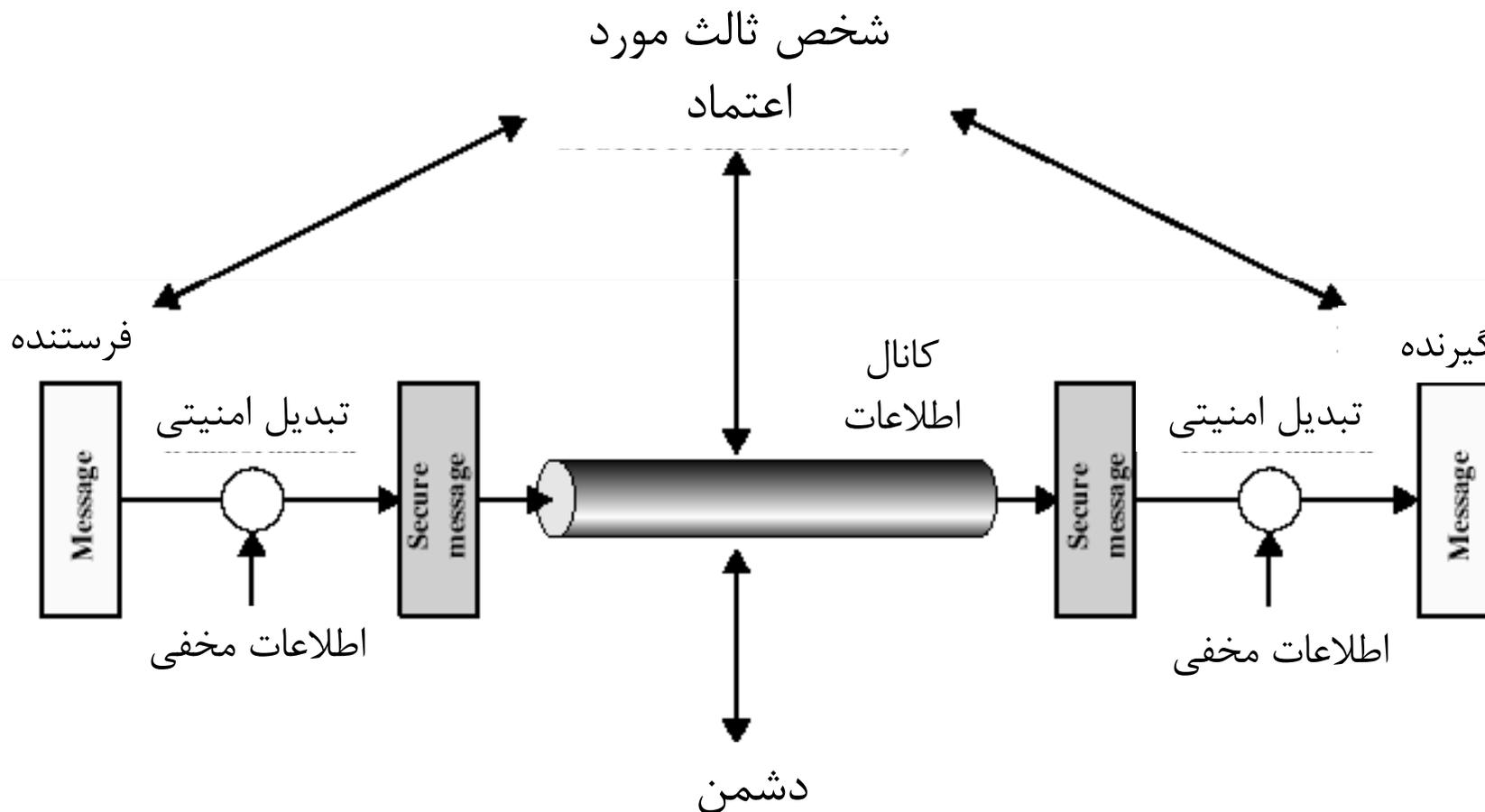
مدل کلی در یک ارتباط امن

□ سناریوی کلی در هر ارتباط امن:

- نیاز انتقال یک پیغام بین طرفین با استفاده از یک کانال ناامن (مثل شبکه اینترنت)
- نیاز به تامین سرویس‌های محرمانگی، صحت و احراز اصالت در انتقال پیام
- تکنیک‌های مورد استفاده عموماً از دو مولفه زیر استفاده می‌کنند:
 - تبدیل امنیتی: جهت فراهم آوردن سرویس‌های امنیتی موردنیاز
 - اطلاعات مخفی: که در تبدیل فوق مورد استفاده قرار می‌گیرند و نحوی بین طرفین ارتباط به اشتراک گذاشته شده‌اند.



یک مدل نمونه برای ارتباط امن





تضمین سرویس امنیتی

- مدل فوق نشان می دهد که برای فراهم آمدن یک سرویس امنیتی خاص مجبوریم نیازهای زیر را فراهم کنیم:
- طراحی الگوریتم مناسب برای انجام تبدیل امنیتی موردنظر
- 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 سرویس امنیتی

- منظور از شرایط استفاده صریحتر بیان گردد (باید نرم افزاری نصب شود، تجهیزاتی خریداری گردد، اطلاعاتی را باید کسی تولید نماید و ...)
ر.س : اضافه شد.

- شرایط طرفین ارتباطی نیز بیان گردد. (بیشتر جهت تعیین تفاوت با مدل بعدی)
ر.س : به جز شرایط ذکر شده، به نظر نمی رسد که شرط دیگری لازم باشد
sadoddin, 1/8/2005



پایان

مرکز امنیت داده و شبکه شریف

<http://dnsl.ce.sharif.edu>

پست الکترونیکی

m_amani@ce.sharif.edu

شبکه آموزشی - پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است



madsg.com
مادسیج

IRan Education & Research NETwork
(IRERNET)

