یا ذاالامن والامان

امنیت داده و شبکه

مفاهیم و تعاریف اولیه

مرتضی امینی - نیمسال اول ۹۰-۸۹

مرکز امنیت داده و شبکه شریف
http://dnsl.sharif.edu

فهرست مطالب

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

آنچه این درس بررسی می‌کند

- این درس مفاهیم زیر را در بر می‌گیرد:
  - تهدیدهای امنیتی
  - نیازهای امنیتی
  - خدمات امنیتی
  - مکانیزم‌ها و پروتکل‌های امنیتی
- برای داده‌هایی که بر روی کامپیوترها ذخیره شده و یا بر روی شبکه انتقال داده می‌شوند.

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
- مدلهای امنیت شبکه

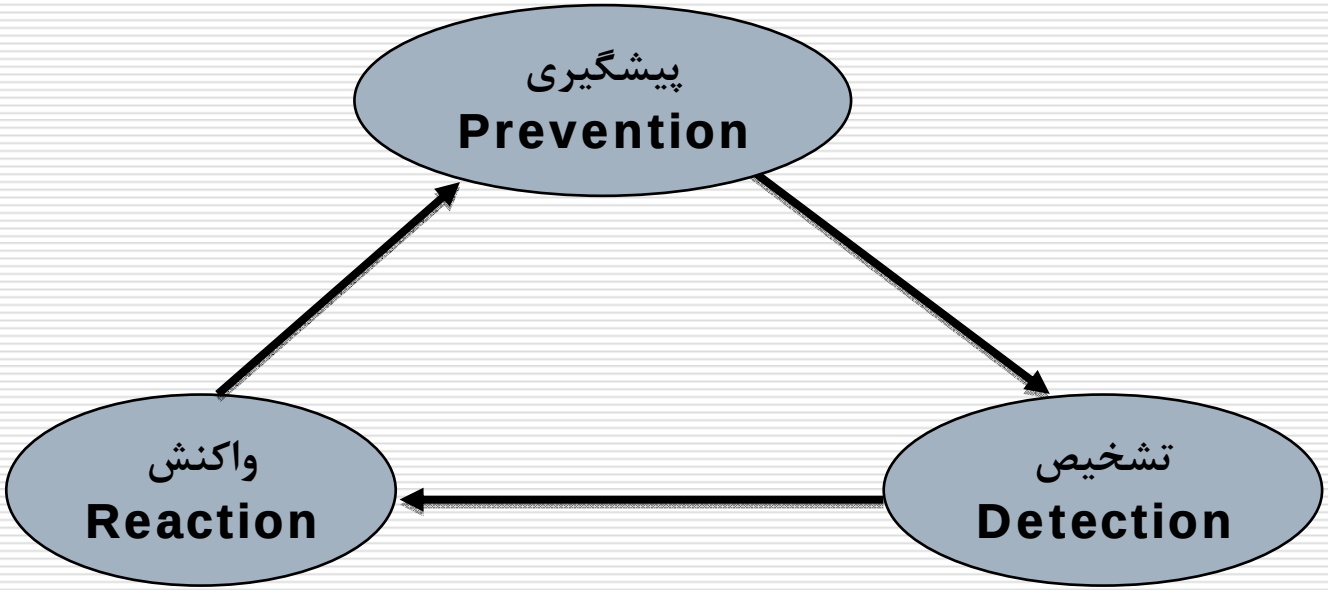
امنیت چیست؟

- امنیت به (طور غیر رسمی) عبارتست از حفاظت از آنچه برای ما ارزشمند است.
  - در برابر حملات عمدی
  - در برابر حملات غیرعمدی

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 سنتی

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

امنیت اطلاعات در دنیای نوین

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

نیازهای امنیتی

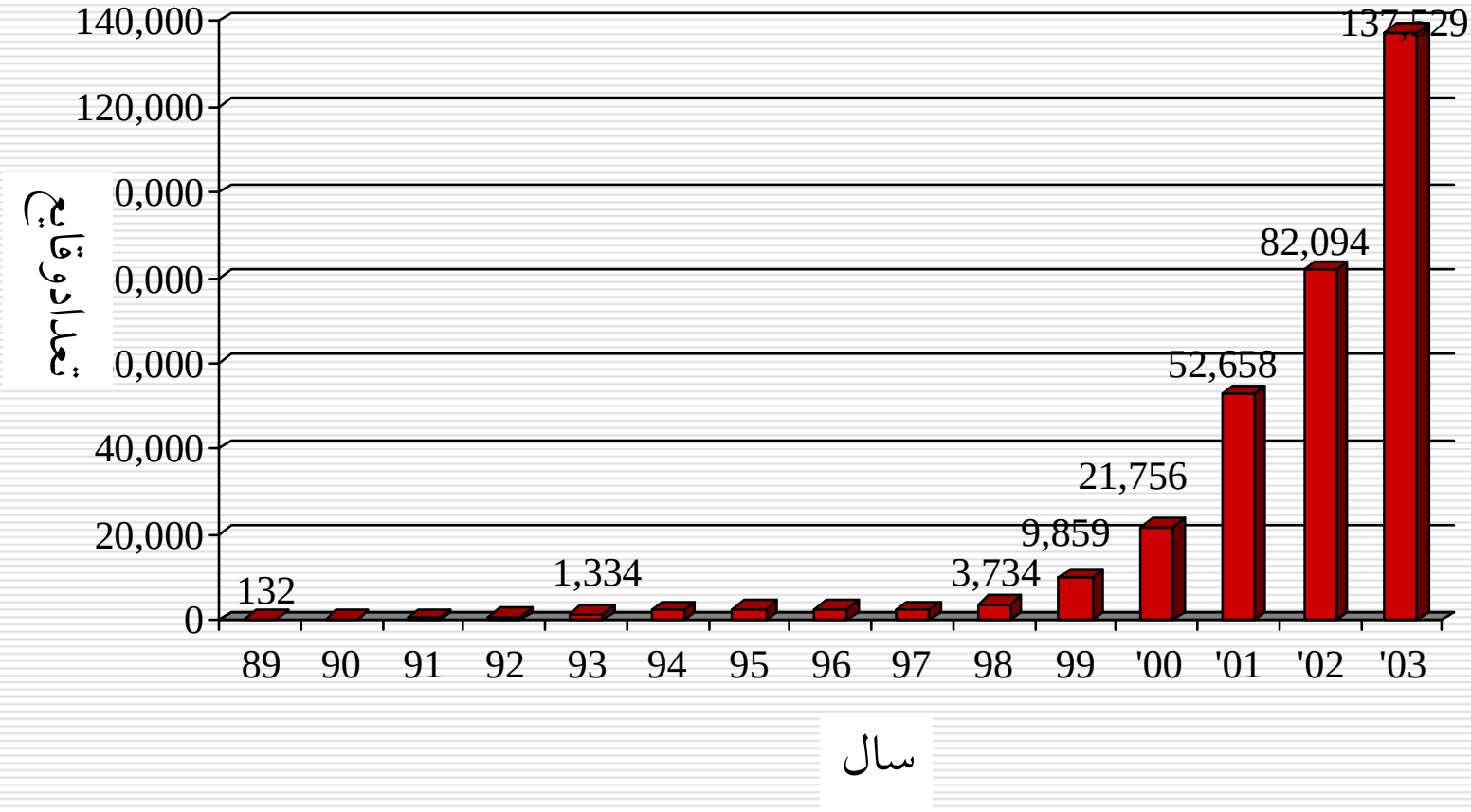
- بنابراین :
  - در گذشته، امنیت با حضور فیزیکی و نظارتی تامین می‌شد،

ولی

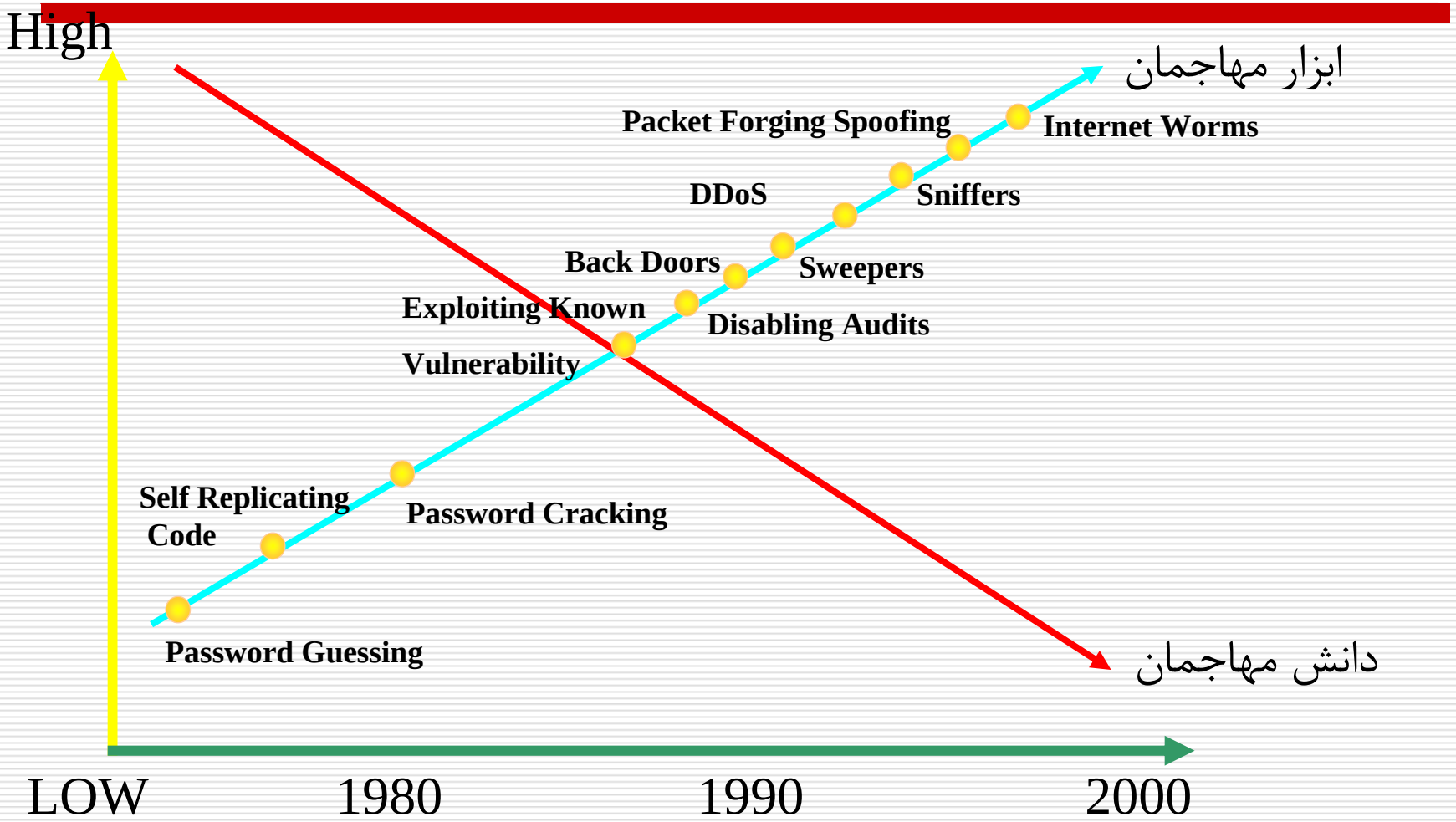
  - امروزه از ابزارهای خودکار و مکانیزم‌های هوشمند برای حفاظت از داده ها استفاده می‌شود.

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

مبانی امنیت داده‌ها

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

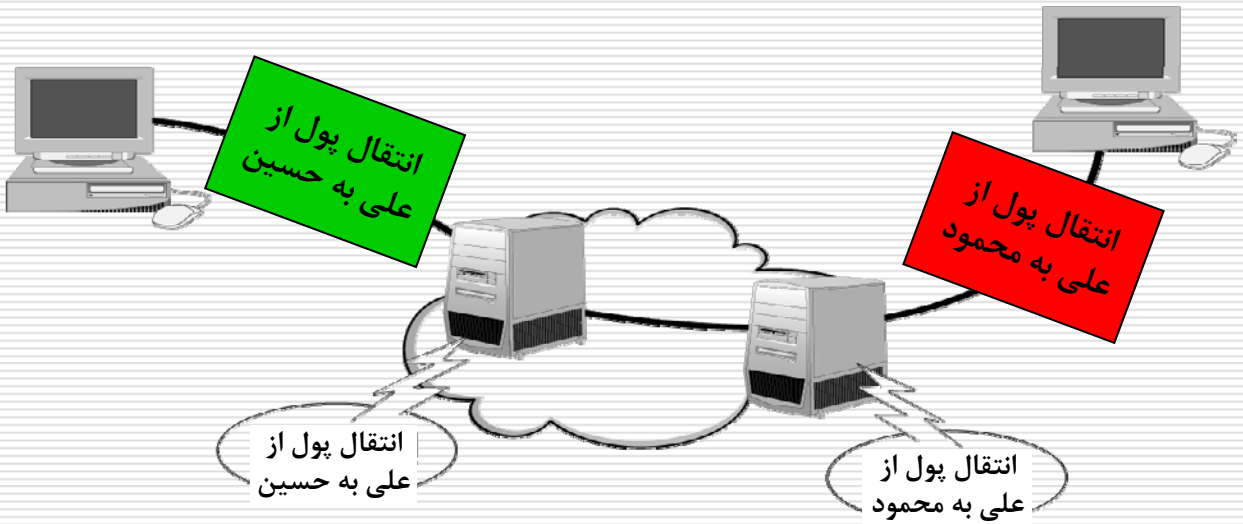
- ✓ **محرمانگی (Confidentiality)**
  - عدم افشای غیرمجاز داده‌ها
- ✓ **صحت (Integrity)**
  - عدم دستکاری داده‌ها توسط افراد یا نرم‌افزارهای غیرمجاز
- ✓ **دسترس‌پذیری (Availability)**
  - دسترسی به داده هاتوسط افراد مجاز در هر مکان و در هرزمان

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



دسترس‌پذیری

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

دلایل ناامنی شبکه‌ها

ضعف فناوری

- پروتکل، سیستم عامل، تجهیزات

ضعف تنظیمات

- رهاکردن تنظیمات پیش‌فرض، گذرواژه‌های نامناسب، عدم استفاده از رمزنگاری، راه‌اندازی سرویس‌های 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)

دلایل ناامنی شبکه‌ها

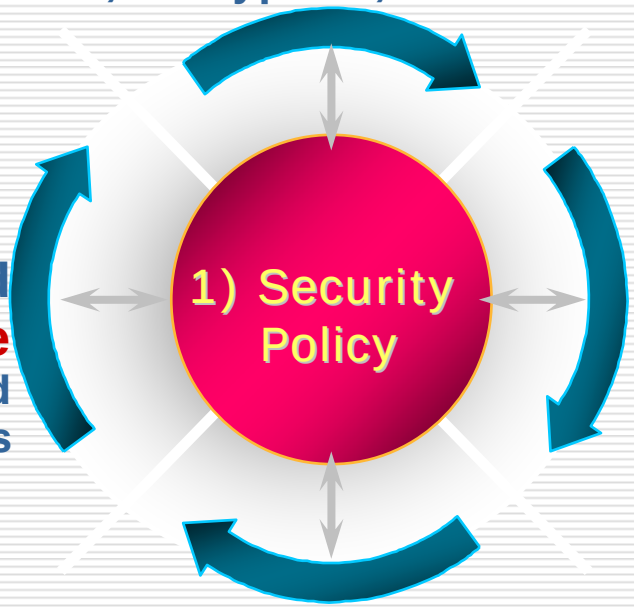
- ضعف فناوری
  - پروتکل، سیستم عامل، تجهیزات
-
-

ضعف مدیریتی

امن‌سازی

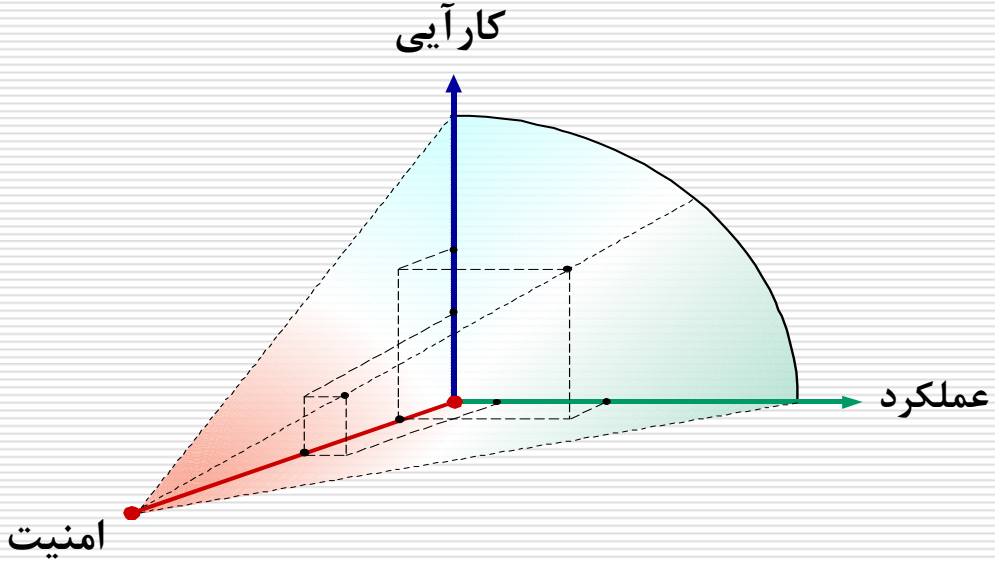
- گستره امنیت تمامی منابع سازمان است و نه تنها کارگزار اصلی.
- نگرش مدیریتی به مسئلهٔ امنیت لازم است و نه نگرش فنی.
- مهاجمین داخلی و مجاز خطر بالقوهٔ بیشتری دارند.
- مادام که انسان‌ها امن فکر نکنند نمی‌توان تراکنش امن داشت.
- امن‌سازی یک فرآیند است نه یک وظیفه خاص و مقطعی.

چرخه ایجاد امنیت حلقه پایان ناپذیر است



استراتژی امنیت سازمانی

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



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 مسؤولیت‌هایی 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 حمله 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.
- **رخنه (Breach):** نقض سیاست امنیتی یک سیستم
- **نفوذ (Intrusion):** فرایند حمله و رخنه ناشی از آن
- **آسیب‌پذیری (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 نحوهٔ 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 درنظرگرفته شده برای تشخیص، جلوگیری و بازیابی از حملات. هر مکانیزم امنیتی در واقع یکی از روشهای پیاده‌سازی یک سیاست امنیتی است.
- **سرویس امنیتی (Security Service)**: سرویس‌های تضمین کننده امنیت با استفاده از مکانیزم‌های بالا.

s26 - 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 رخنهٔ 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 دسترس‌پذیری 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 تضمین‌کنندهٔ 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
- مدلهای امنیت شبکه

دشواری برقراری امنیت

- تعامل پروتکلها پیچیدگی را افزایش داده و امنیت را تهدید می‌کند.
- امنیت معمولاً قربانی افزایش کارآیی و مقیاس پذیری 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.

فهرست مطالب

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

سرویس‌های امنیتی

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

سرویس‌های امنیتی

- **حفظ صحت داده‌ها (Integrity)** : اطمینان از اینکه آنچه رسیده همان است که فرستاده شده.
  - کد احراز هویت پیام (MAC)
  - امضاء

- **حفظ محرمانگی داده‌ها(Confidentiality)** : اطمینان از اینکه تنها کاربران مورد نظر قادر به درک پیامها است.
  - رمزنگاری

سرویس های امنیتی

- **احراز اصالت (Authentication)** : اطمینان از این که کاربر همانی است که ادعا می‌کند.
  - کنترل هویت

- **کنترل دسترسی (Access Control)** : کاربر تنها به منابع مقرر شده حق دسترسی دارد.
  - مجازشماری هم نامیده می‌شود (هر چند که چندان درست نیست).

سرویس های امنیتی

- **عدم‌انکار (Non-Repudiation)** : عدم امکان انکار دریافت یا ارسال توسط گیرنده و فرستنده
  - امضاء

- **دسترس پذیری (Availability)** : 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**
- مدلهای 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)

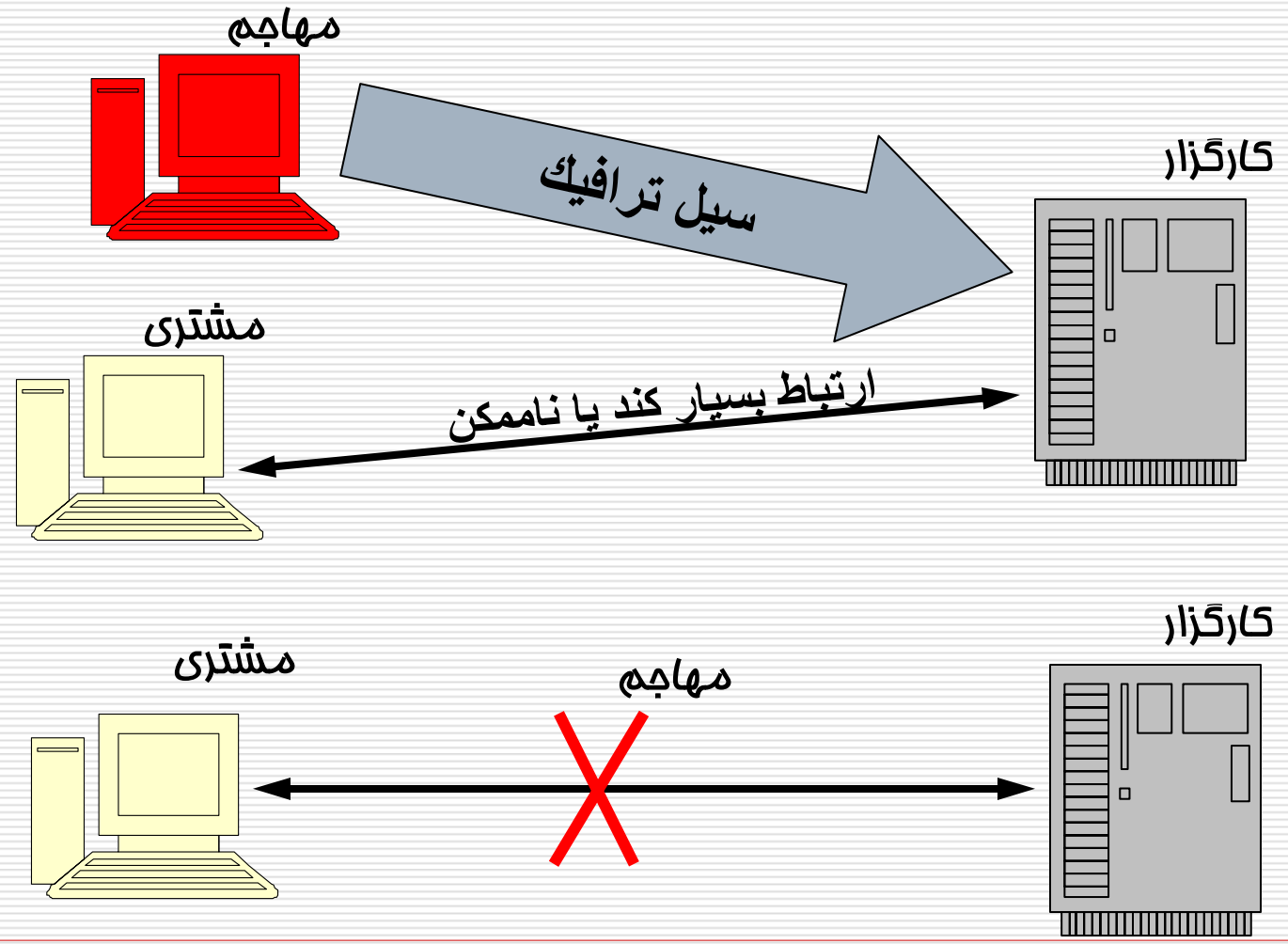
انواع حملات از نظر تاثیر:

- **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)

حمله وقفه

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

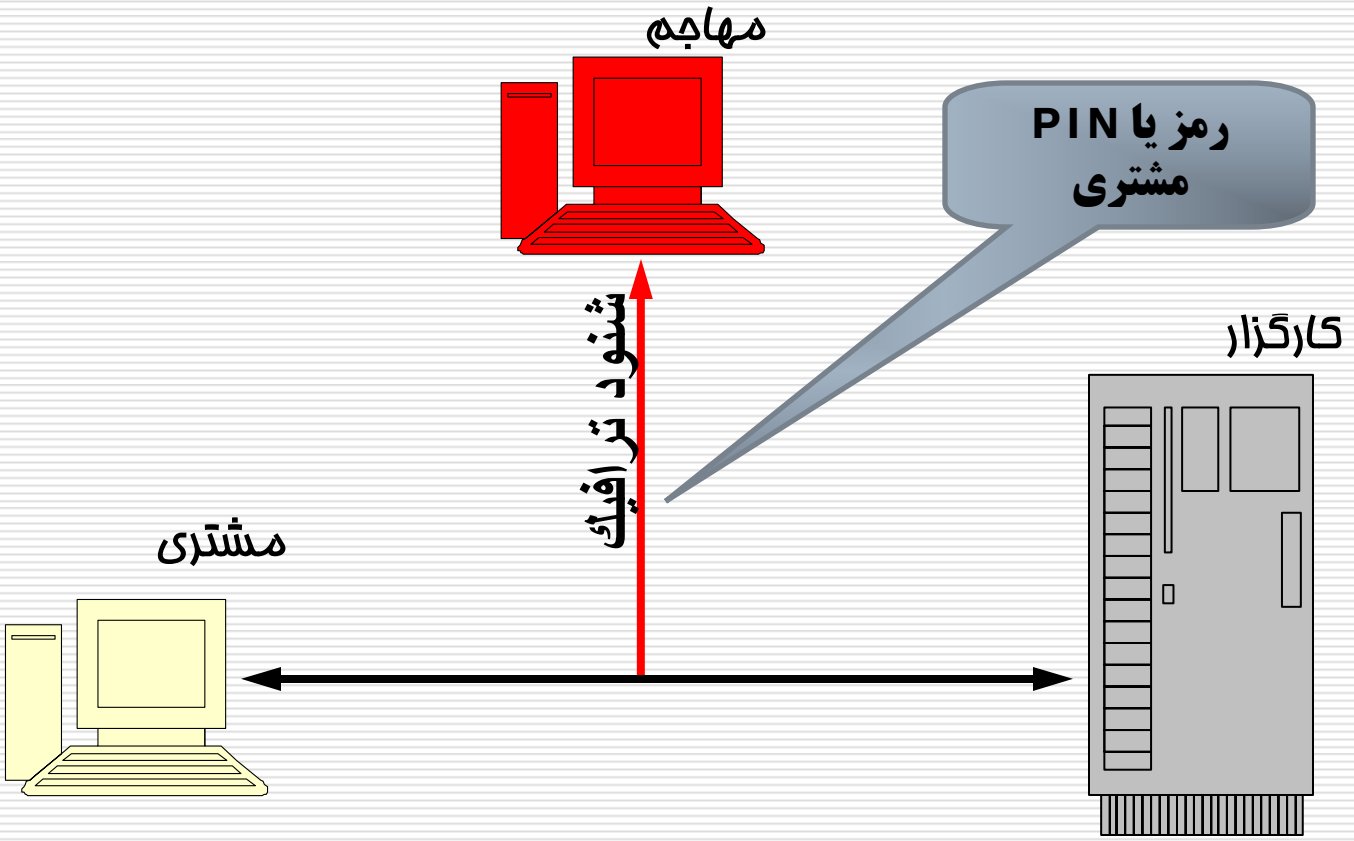
حمله وقفه (ادامه)



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)

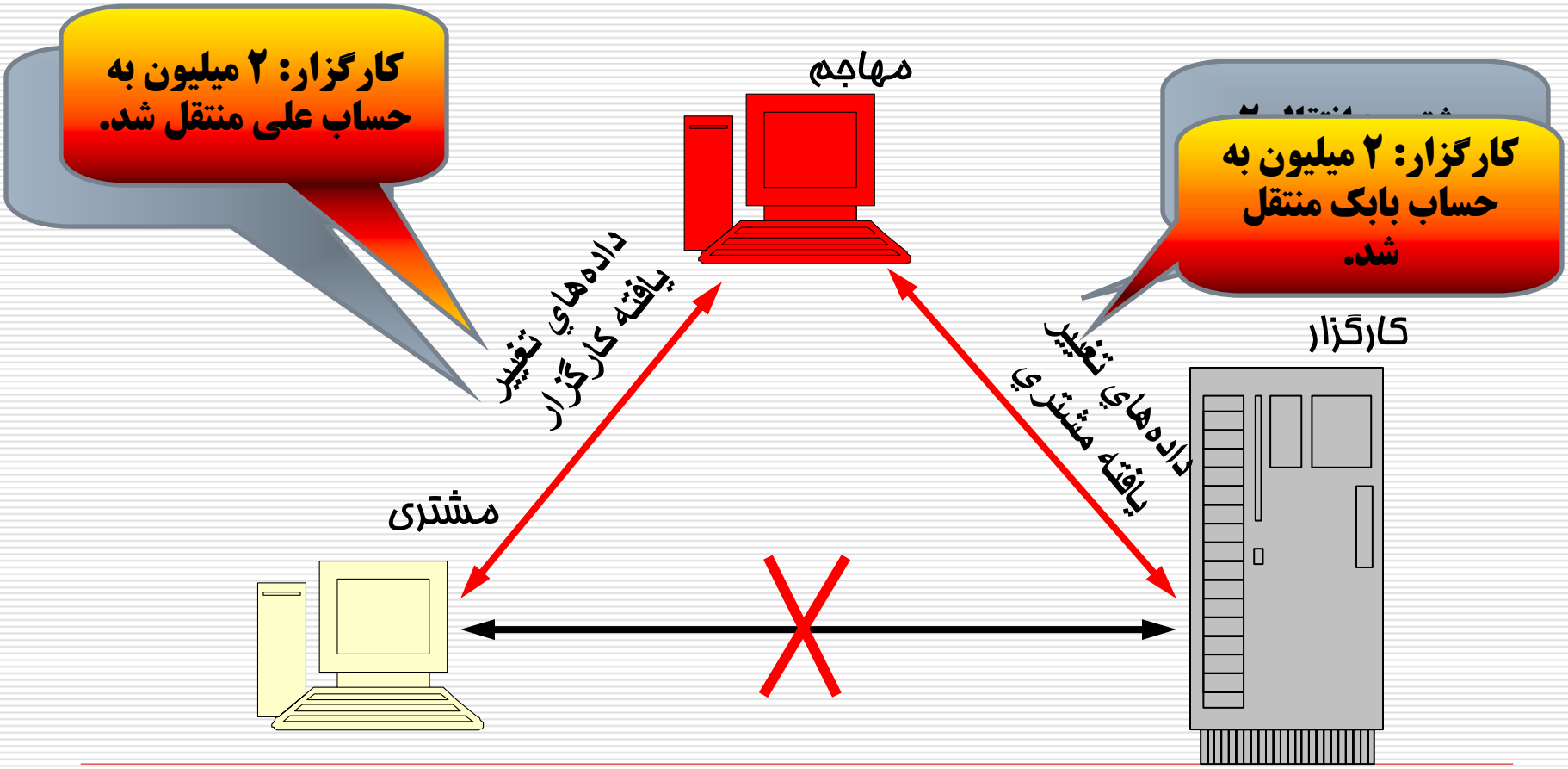


حمله دستکاری داده‌ها

- 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 پایگاه‌داده‌ها 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)

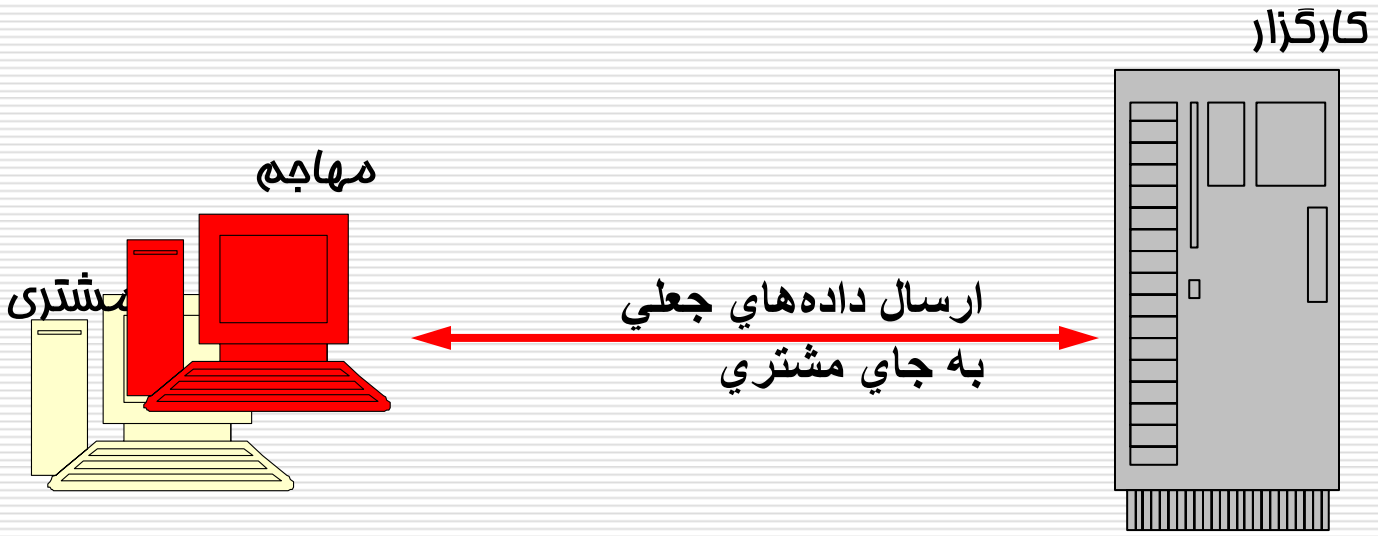


حمله جعل اطلاعات

- 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 اِعمال 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)



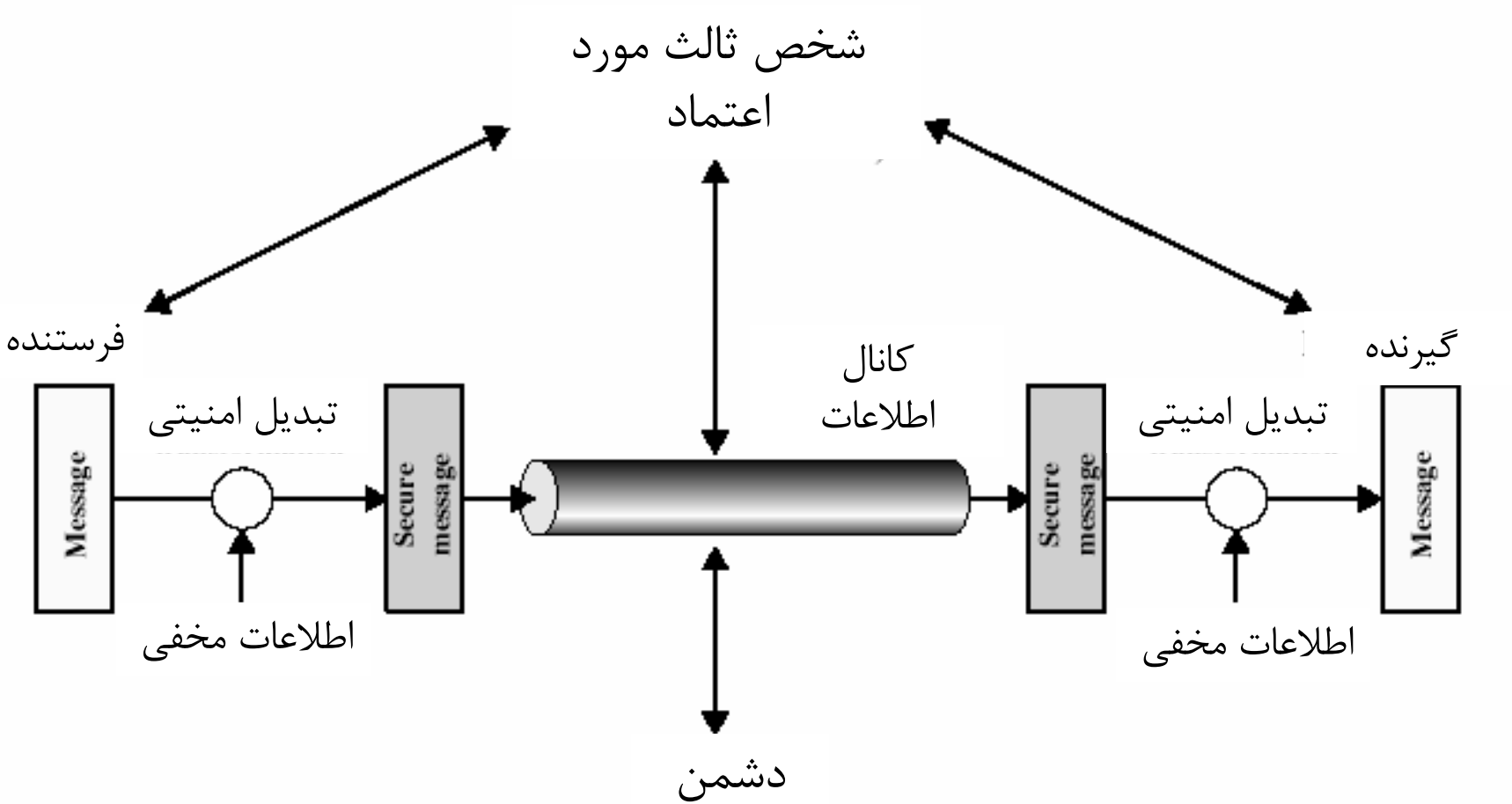
فهرست مطالب

- 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 عموما از دو مولفه زیر استفاده می‌کنند:
  - تبدیل امنیتی : جهت فراهم آوردن سرویس های امنیتی موردنیاز
  - اطلاعات مخفی : که در تبدیل فوق مورداستفاده قرار می‌گیرند و به نحوی بین طرفین ارتباط به اشتراک گذاشته شده‌اند.

یک مدل نمونه برای ارتباط امن



تضمین سرویس امنیتی

- مدل فوق نشان می‌دهد 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

Slide 53

s16

- 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

Details on the Course

Administrivia

- Website:
  - sharif.edu/~kharrazi/courses/40817-901k/
  - You are expected to check the website regularly
- Mailing List
  - Register for it
  - Registration link will be on the website

Administrivia

- References:
  - Cryptography and Network Security Principles and Practices, Fourth Edition, by William Stallings
  - Computer Security, by Matt Bishop

Administrivia

- Grading (tentatively)
  - 30% Homework
  - 30% Midterm
  - 40% Final

Policies

- Late Homework
  - One day late will cost you 25%, two days 50%, and three days 75%.
  - No homework will be accepted after the third day.
- Cellphones: Please turn them off before entering class.
- Cheating and Copying
  - First time you are caught you will get a zero for the task at hand.
  - Second time you are caught you will fail the course.
  - Providing your homework to someone else, is considered cheating on your behalf as well.

پایان

مرکز امنیت شبکه شریف

http://nsc.sharif.edu

پست الکترونیکی

m_amini@ce.sharif.edu