sooraac.ir

یا ذاالامن والامان

امنیت داده و شبکه

مفاهیم و تعاریف اولیه

شرکت و آموزشگاه فنی و حرفه‌ای سورا

www.sooraac.ir

sooraac.ir

فهرست مطالب

- محتوای درس
- ضرورت امنیت داده و شبکه
- مفاهیم اولیه
- دشواری برقراری امنیت
- انواع و ماهیت حملات
- سرویس‌های 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.

sooraac.ir

موضوعات تحت پوشش درس

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

sooraac.ir

فهرست مطالب

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

امنیت چیست؟

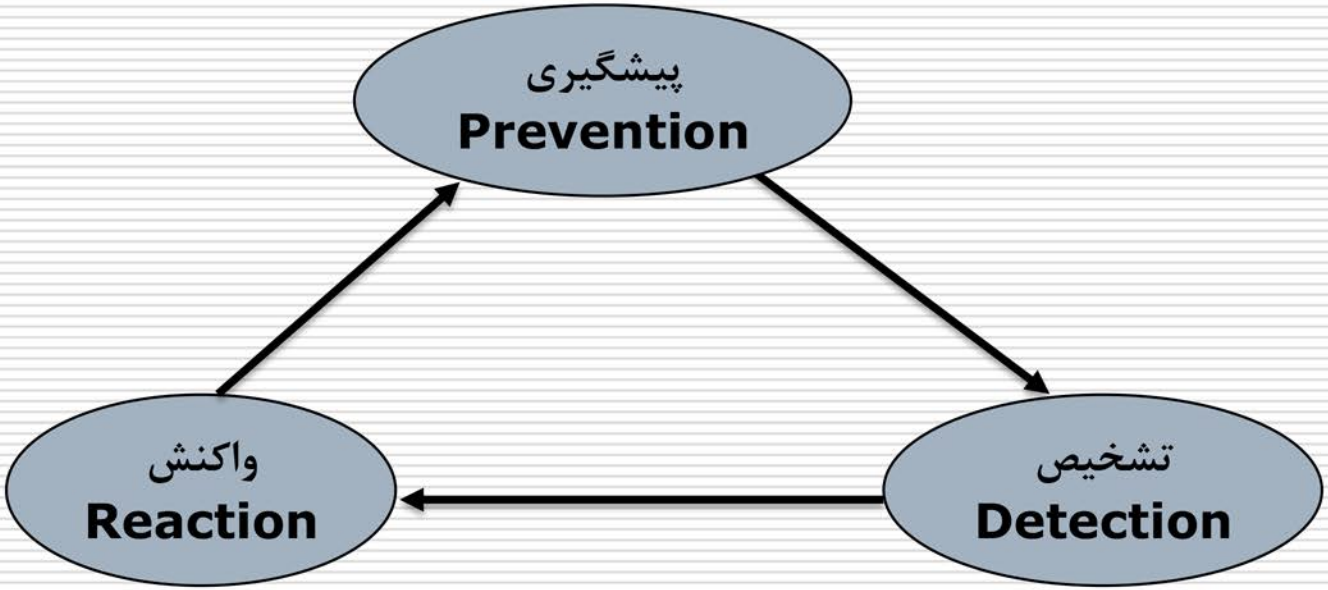
- امنیت به (طور غیر رسمی) عبارتست از حفاظت از آنچه برای ما ارزشمند است.
  - در برابر حملات عمدی
  - در برابر نفوذ غیرعمدی

اقدامات امنیتی

- **پیشگیری (Prevention):**
  - جلوگیری از خسارت
- **تشخیص و ردیابی (Detection & 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

sooraac.ir

اقدامات امنیتی



sooraac.ir

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

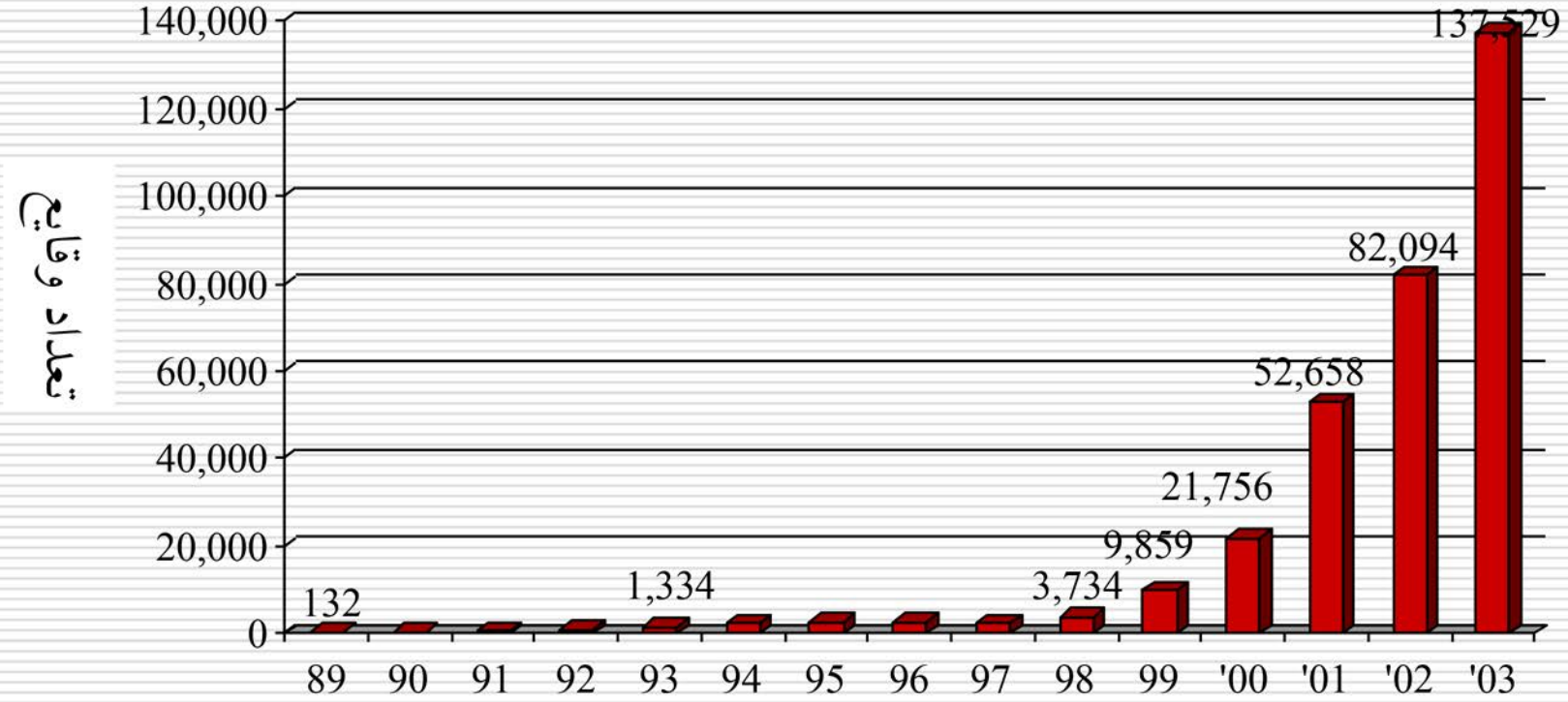
- بنابراین :
  - در گذشته، امنیت با حضور فیزیکی و نظارتی تامین می‌شد،

ولی

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

sooraac.ir

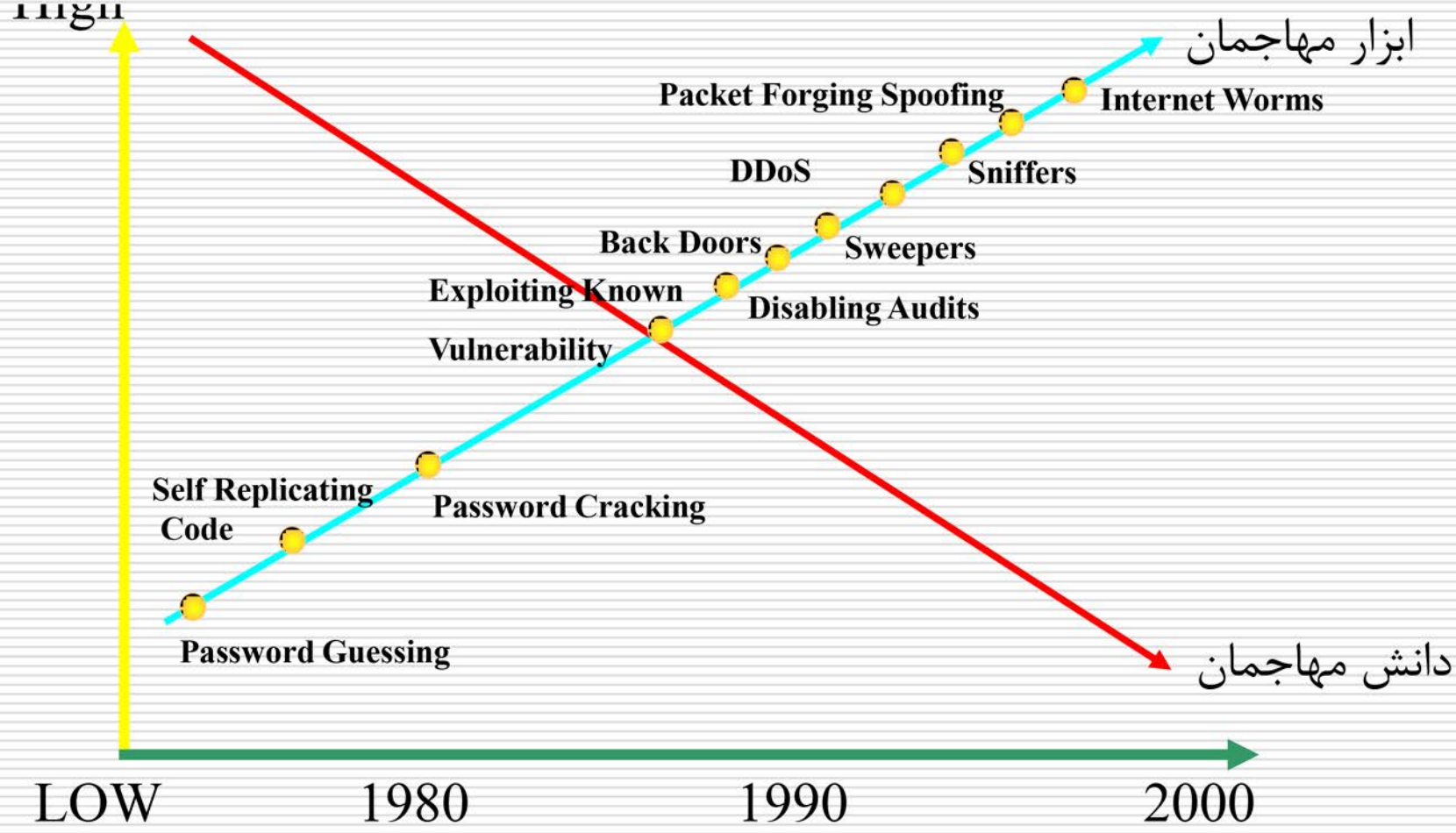
آمار منتشر شده توسط CERT



CERT (Computer Emergency Response Team)

sooraac.ir

ابزار مهاجمان



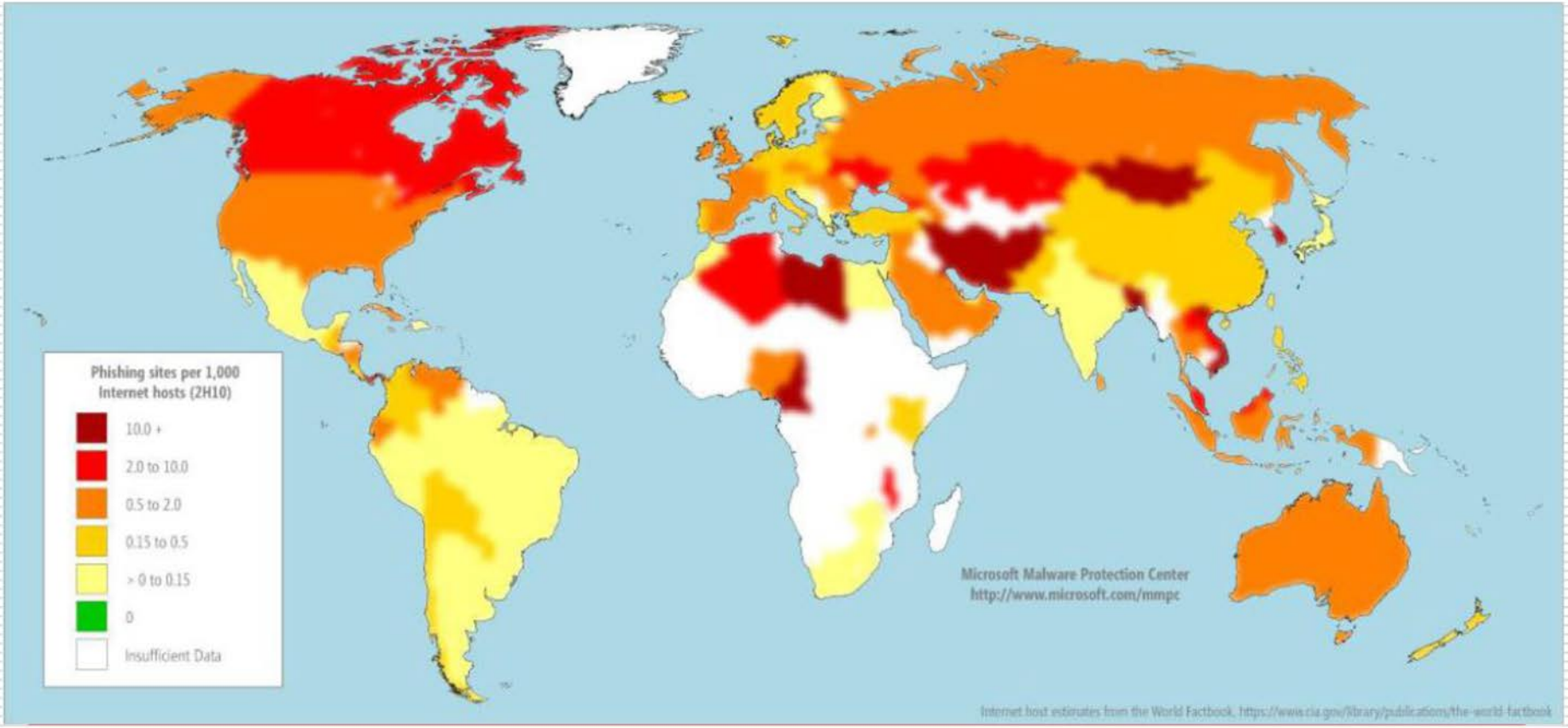
نیازهای امنیتی: گذشته و حال

- 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).

sooraac.ir

توزیع سایت‌های فیشینگ (۱)

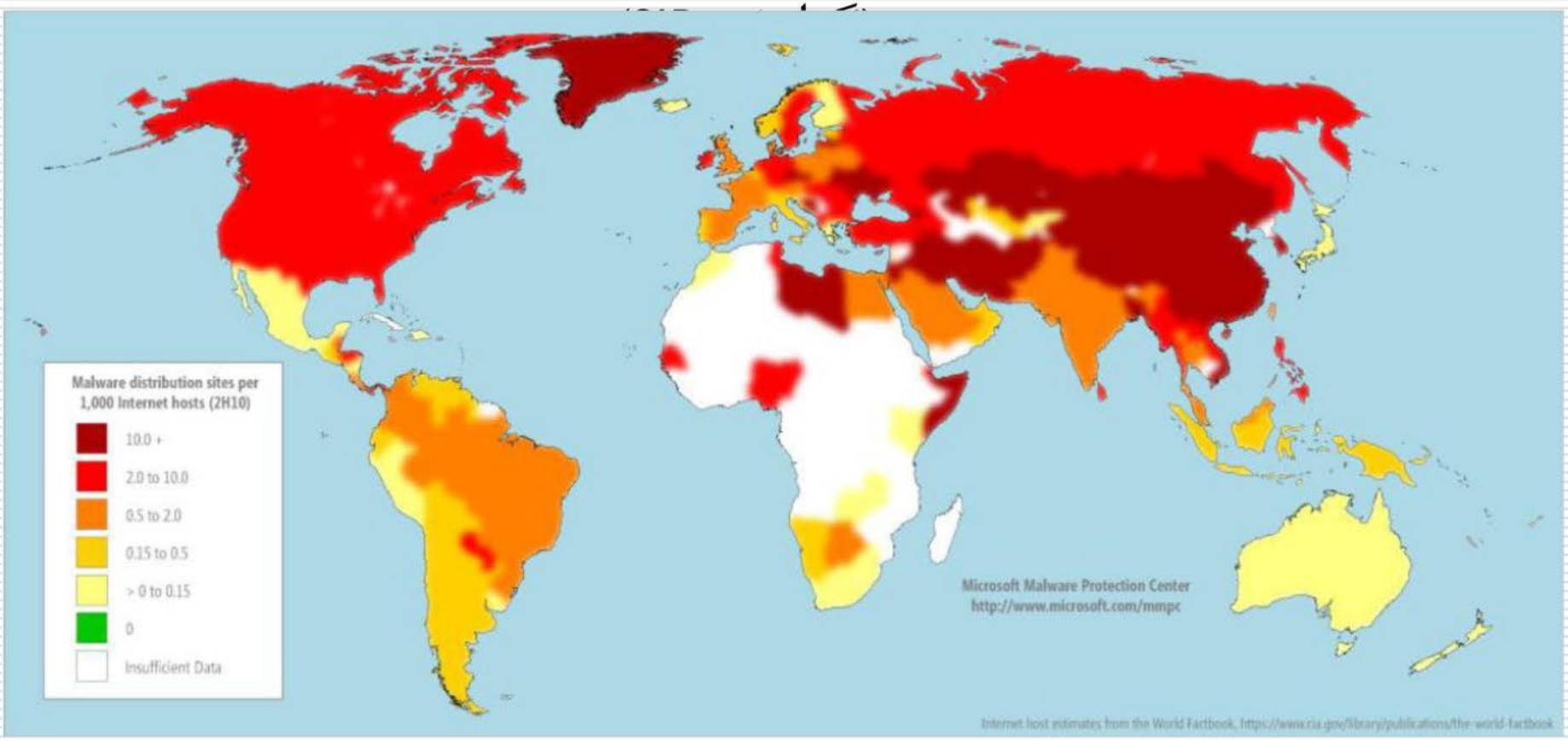
توزیع سایت‌های فیشینگ در دنیا در ۶ ماه دوم ۲۰۱۰ (گزارش SIR)



sooraac.ir

توزیع سیستم‌های آلوده (۱)

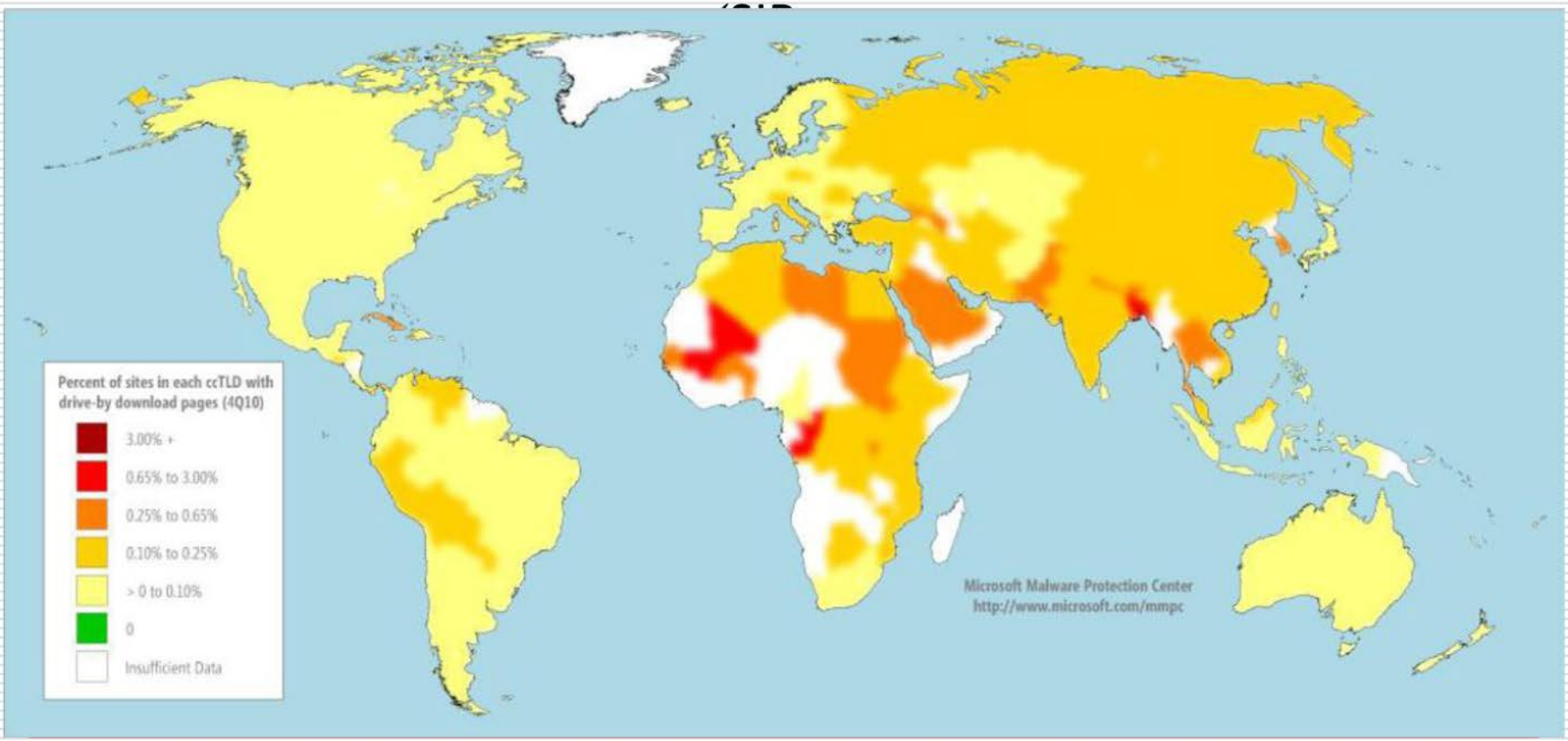
توزیع سیستم‌های آلوده به بدافزار در دنیا در ۳ ماهه دوم ۲۰۱۰



sooraac.ir

توزیع سایت‌های آلوده‌ساز (۱)

توزیع سایت‌های آلوده‌ساز در دنیا در ۳ ماهه چهارم ۲۰۱۰ (گزارش



sooraac.ir

جنگ سایبری (۱)

جنگ عراق و آمریکا در کویت – جنگ اول خلیج فارس (۱۹۹۱)

- ایجاد اختلال در سیستم ضدهوایی عراق
- توسط نیروی هوایی آمریکا با استفاده از ویروسی با نام AF/91
- انتقال از طریق چیپ پرینتر آلوده به ویروس از مسیر عمان و سوریه
- هر چند بعدها درستی موضوع تایید نشد! ولیکن ...

جنگ سایبری (۲)

حمله سایبری روسیه به استونی (۲۰۰۷)

- حمله به وزارتخانه‌ها، بانک‌ها، و رسانه‌ها
- حمله از طریق سِروِرهای اداری تحت کنترل روسیه

sooraac.ir

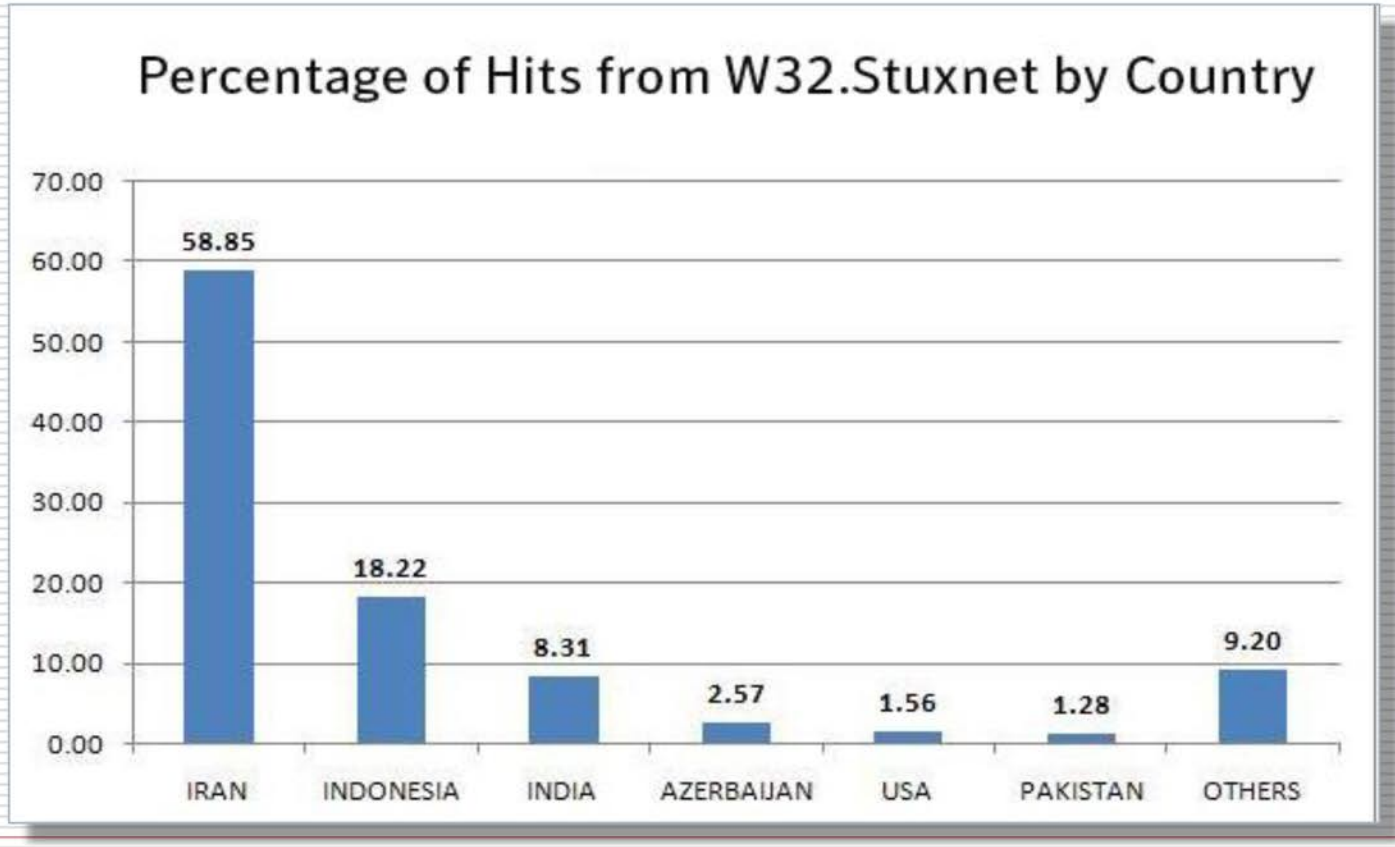
جنگ سایبری (۳)

- **حمله اسراییل به تاسیسات هسته‌ای ایران (۲۰۱۰)**
  - از طریق بدافزار Stuxnet
  - آلوده‌سازی سیستم‌های کنترل صنعتی و PLCها
  - هدف: آلوده‌سازی سانتریفیوژهای نطنز

sooraac.ir

جنگ سایبری (۴)

حمله اسراییل به تاسیسات هسته‌ای ایران: Stuxnet



sooraac.ir

جنگ سایبری (۵)

- **حمله به وزارت امورخارجه ایران (۲۰۱۱)**
  - توسط گروهی موسوم به گروه Anonymous
  - نفوذ به کارگزارهای پست الکترونیکی اداره گذرنامه و روادید وزارت امور خارجه
  - افشای محتوای بیش از **۱۰,۰۰۰ پست الکترونیکی**

sooraac.ir

فهرست مطالب

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

sooraac.ir

مبانی امنیت داده‌ها

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

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

sooraac.ir

محرمانگی

محرمانگی خود مشتمل بر دو نوع است:

- **محرمانگی داده (Data Confidentiality)**
  - اطمینان از اینکه داده‌های محرمانه و خصوصی به افراد غیرمجاز افشاء نمی‌شوند.
- **حفظ حریم خصوصی (Privacy)**
  - اطمینان از اینکه افراد می‌توانند بر روی امکان و نحوه جمع‌آوری، ذخیره‌سازی و انتشار یا افشای داده‌های خصوصی خود توسط دیگران کنترل و تاثیر داشته باشند.

محرمانگی

- مکانیزم‌های متداول:
  - رمزنگاری
  - کنترل دسترسی

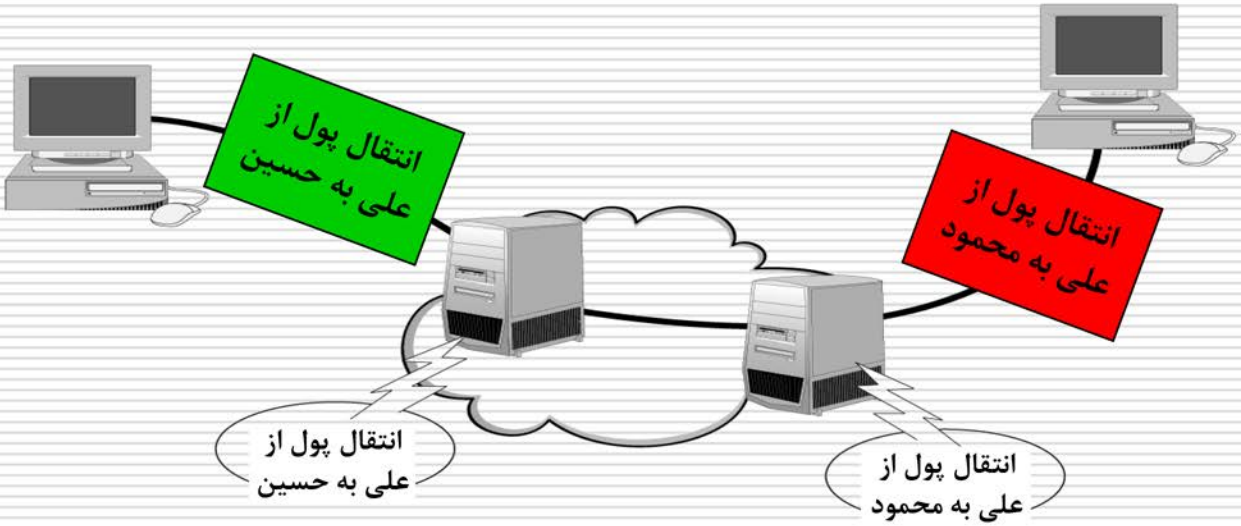
صحت

صحت خود مشتمل بر دو نوع است:

- **صحت داده (Data Integrity)**
  - اطمینان از اینکه داده‌ها و یا برنامه‌ها توسط افراد غیرمجاز دستکاری و یا تغییر نمی‌یابند.
- **صحت منبع (Origin Integrity)**
  - اطمینان از درستی و صحت منبع (فرستنده) اطلاعات.

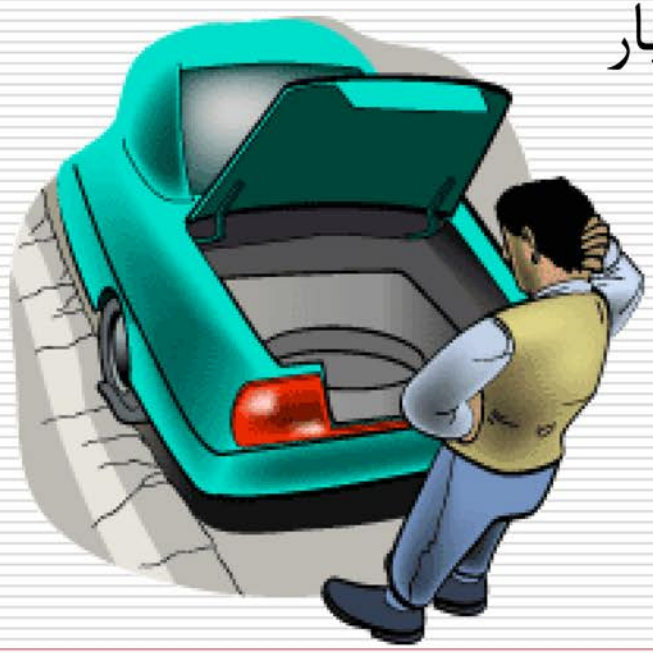
صحت

- مکانیزم‌های متداول:
  - امضای دیجیتال
  - کد احراز اصالت پیام
  - کنترل دسترسی



دسترس‌پذیری

- تعریف: دسترسی به داده‌ها و سرویس‌دهی به افراد مجاز در هر مکان و در هر زمان.
- مکانیزم متداول: وجود پشتیبان، تکرار داده و سرویس، به همراه سیستم‌های پایش و توزیع بار



sooraac.ir

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)

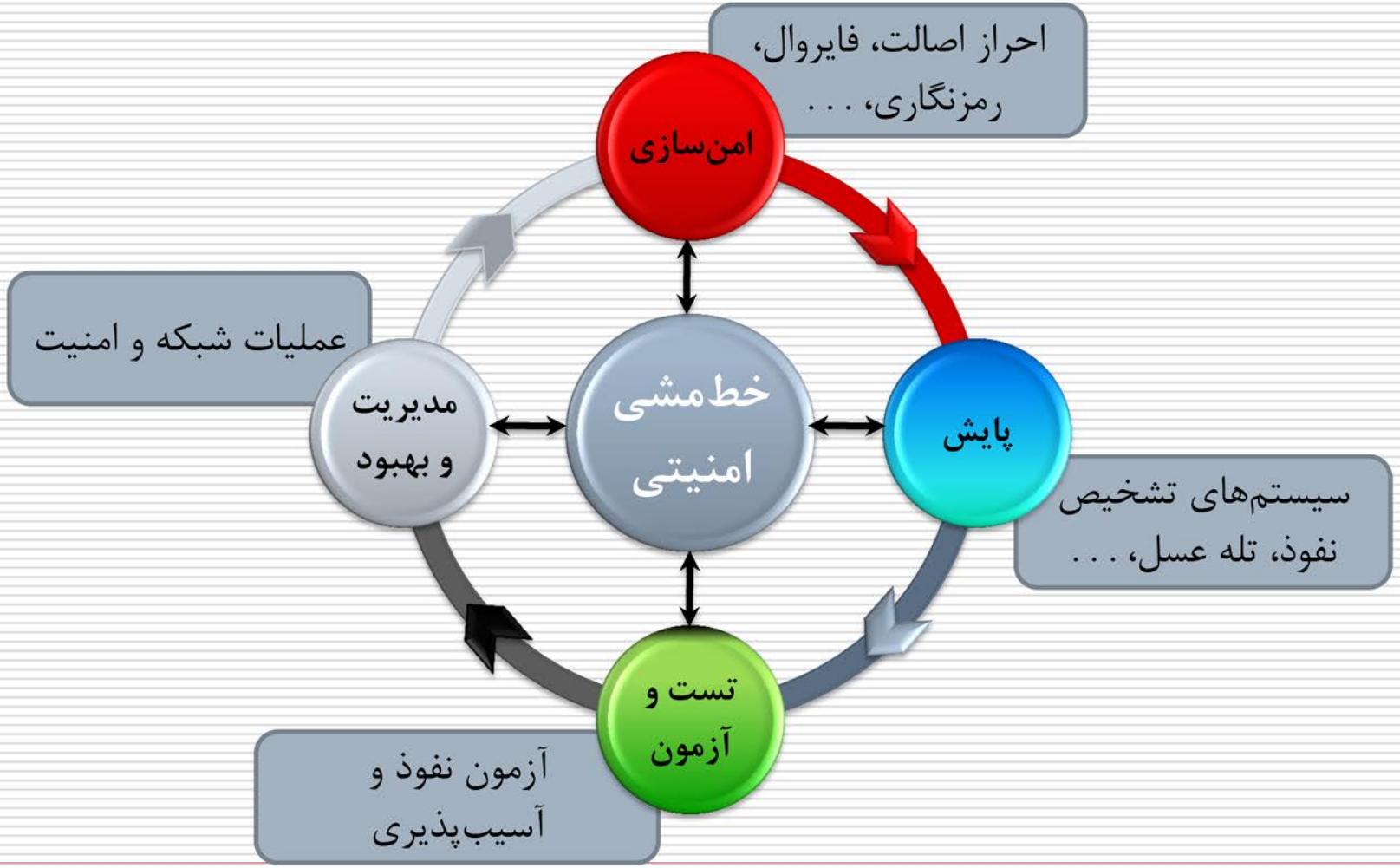
ضعف مدیریتی

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.

sooraac.ir

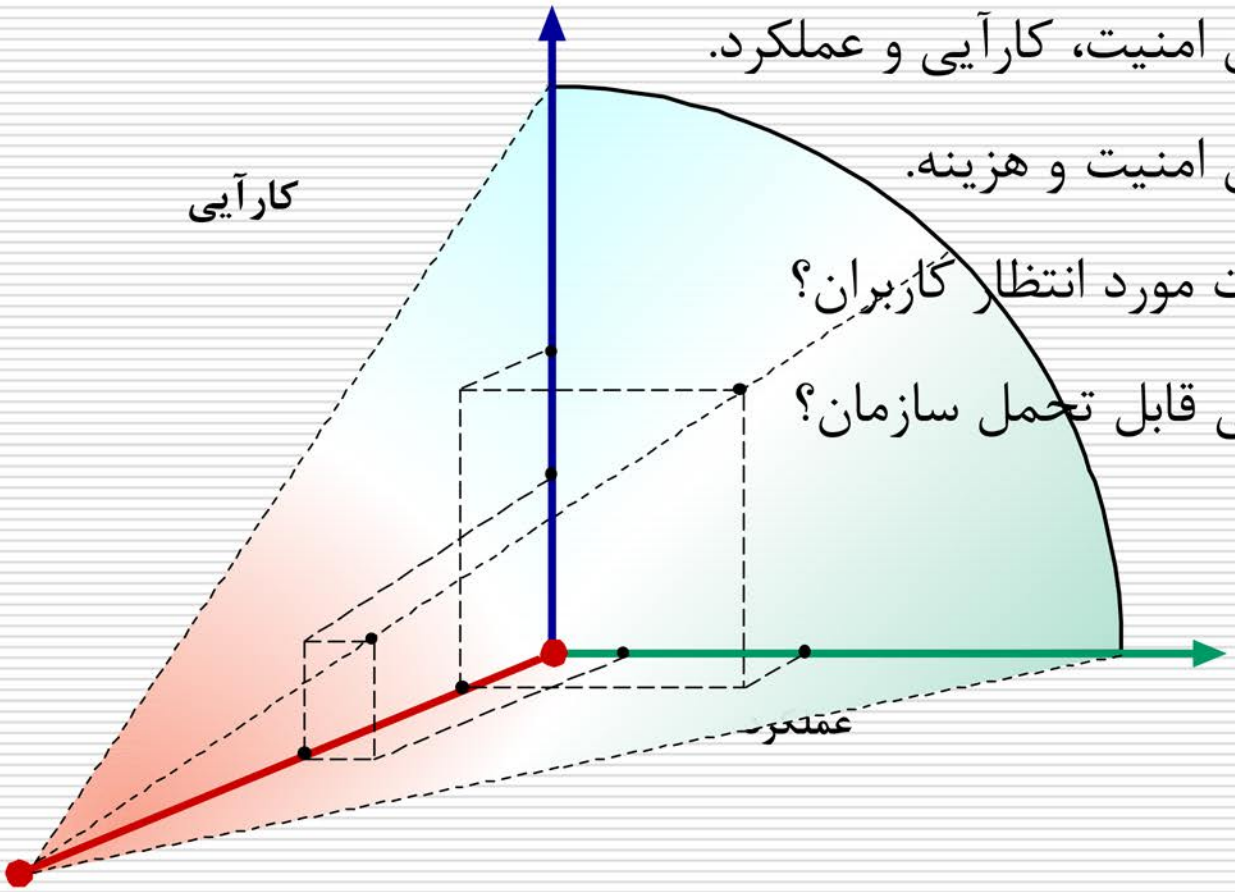
چرخه ایجاد امنیت



sooraac.ir

استراتژی امنیت سازمانی

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



sooraac.ir

خط‌مشی (سیاست‌های) امنیتی

- خط‌مشی (سیاستهای) 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 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.
- **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، پیاده‌سازی، پیکربندی، اجرا که بتوان از آن سوءاستفاده کرده و سیاست‌های امنیتی سیستم را نقض کرد.

sooraac.ir

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 یا بدخواهانه 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.

sooraac.ir

تعاریف و مفاهیم اولیه

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

- **نفوذ (Intrusion)**: هر مجموعه از اعمال که نتیجه 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).

sooraac.ir

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.

sooraac.ir

فهرست مطالب

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

sooraac.ir

دشواری برقراری امنیت

- 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.

sooraac.ir

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.

sooraac.ir

فهرست مطالب

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

sooraac.ir

سرویس‌های امنیتی

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

sooraac.ir

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

sooraac.ir

سرویس‌های امنیتی

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

- **کنترل دسترسی:** کاربر تنها به منابع مقرر شده حق دسترسی دارد.
  - مجازشماری هم نامیده می‌شود.

سرویس‌های امنیتی

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

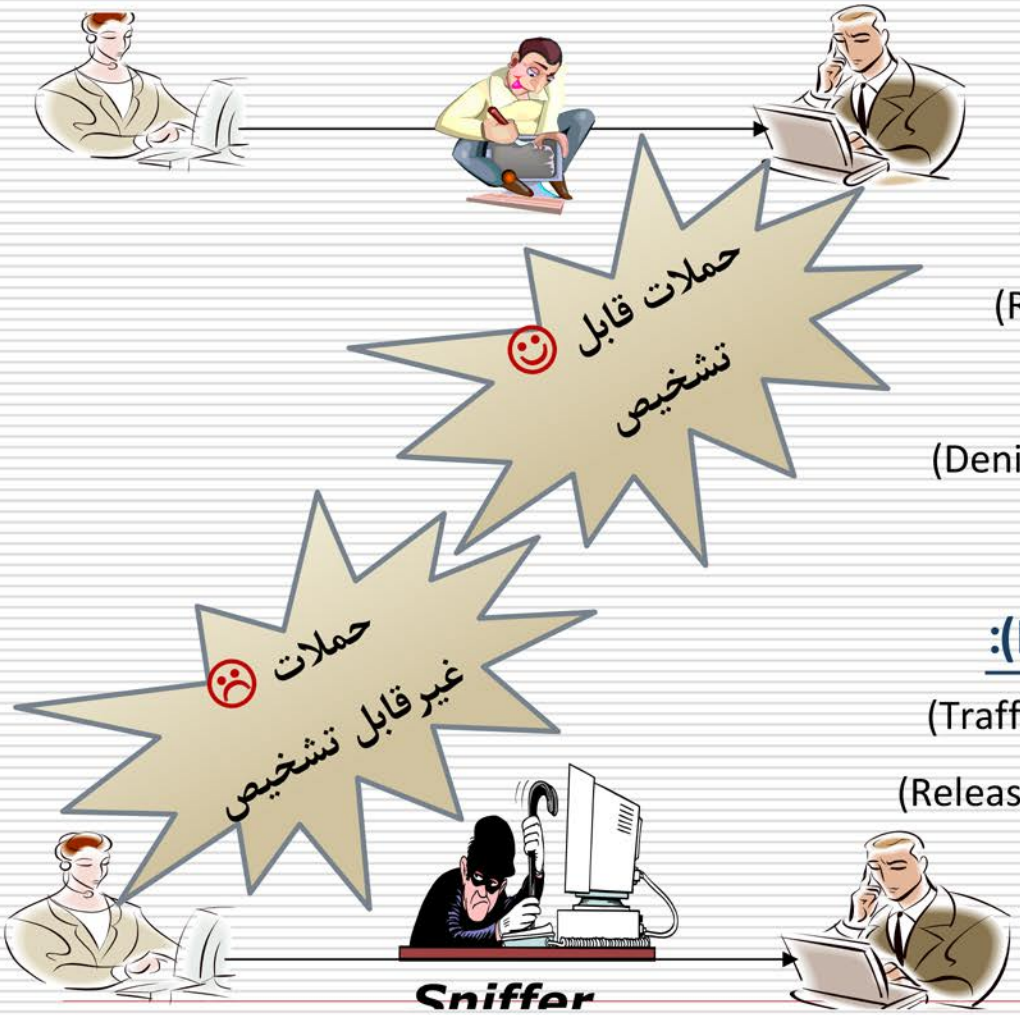
sooraac.ir

فهرست مطالب

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

sooraac.ir

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):**
  - تحلیل ترافیک (Traffic Analysis)
  - انتشار پیغام (Release of message)

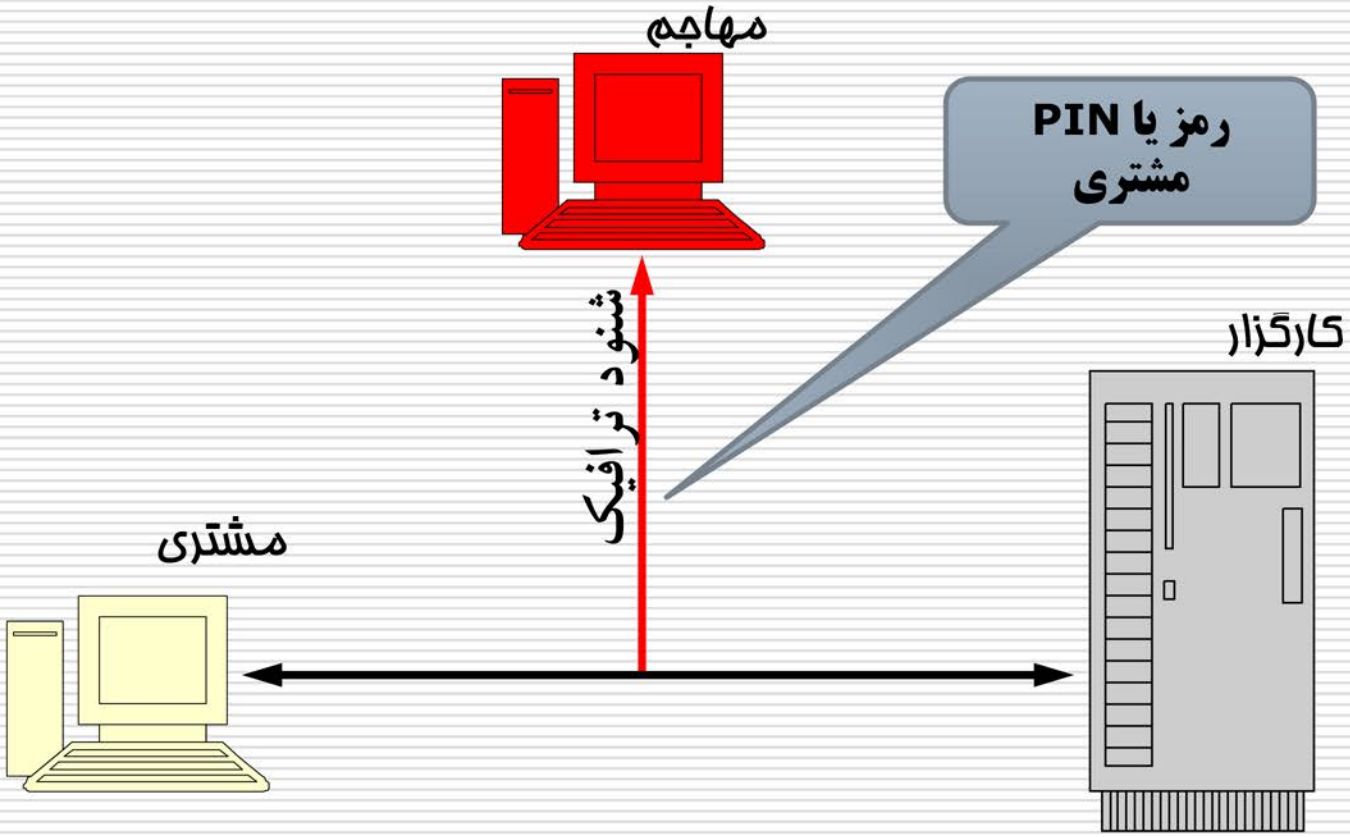
sooraac.ir

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

sooraac.ir

حمله شنود یا استراق سمع (ادامه)

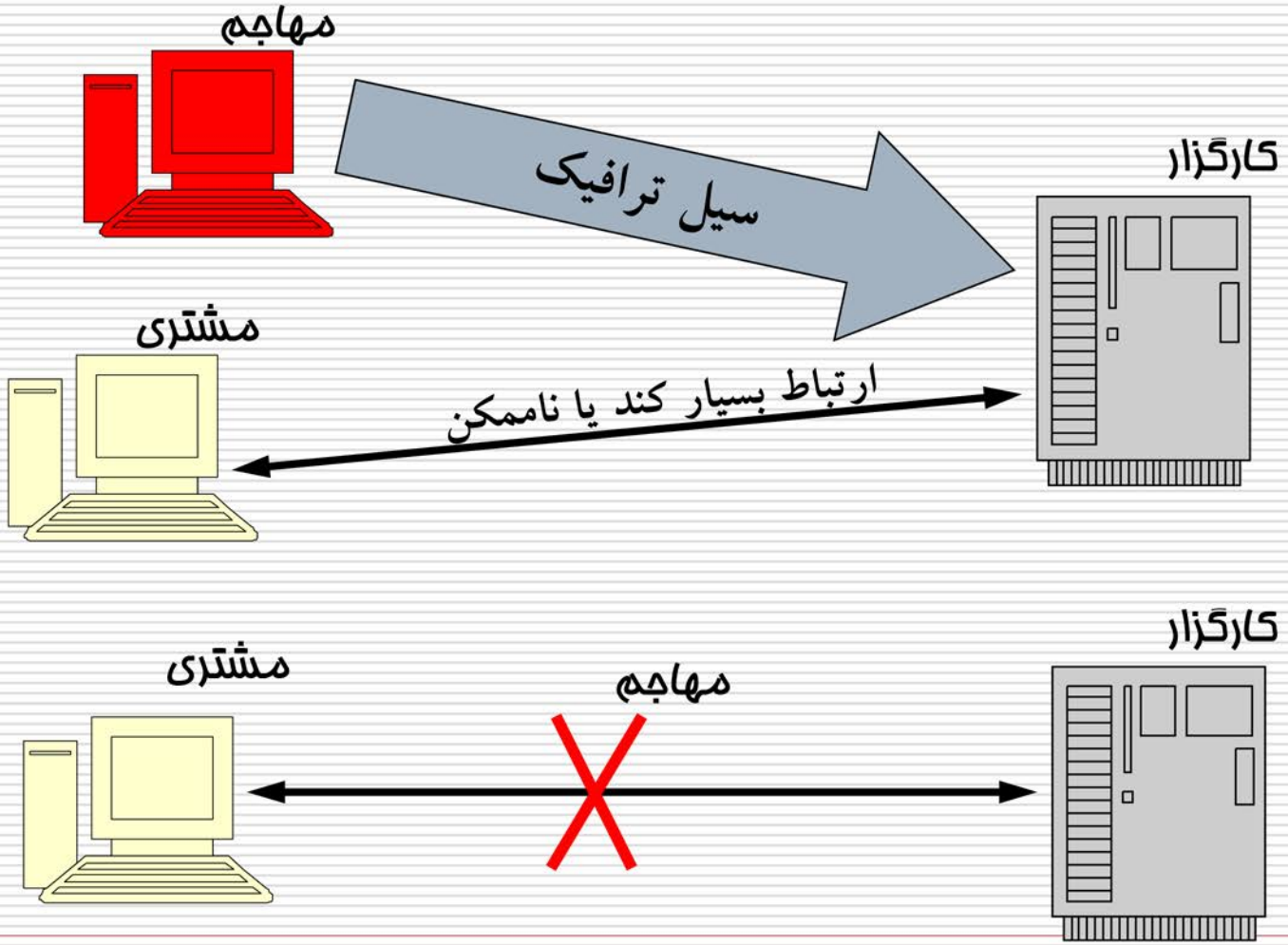


sooraac.ir

حمله منع سرویس یا 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 منع سرویس یا وقفه (ادامه)



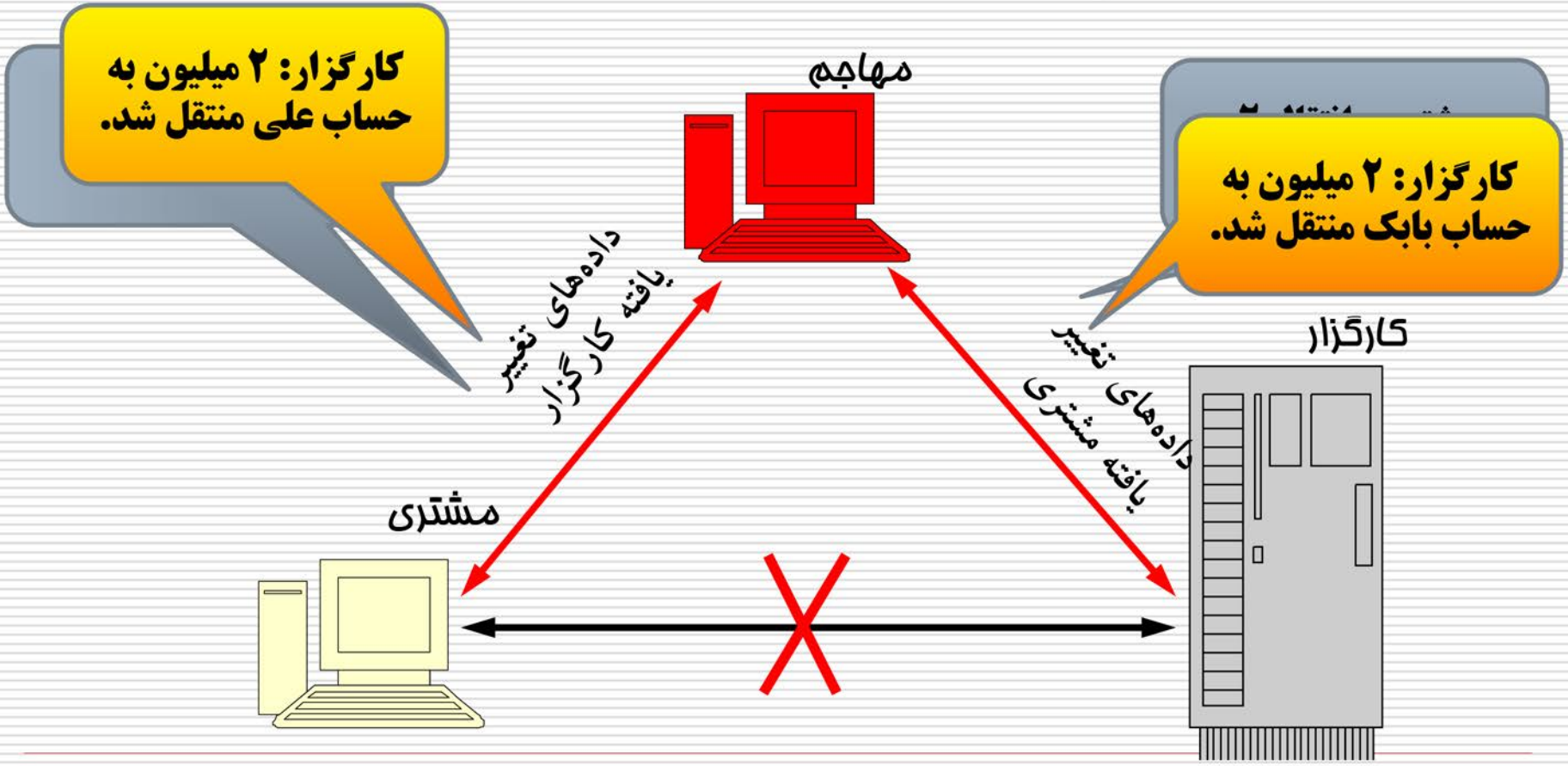
sooraac.ir

حمله تغییر یا 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 تغییر یا دستکاری داده‌ها (ادامه)

- حمله مرد میانی (Man in the Middle)



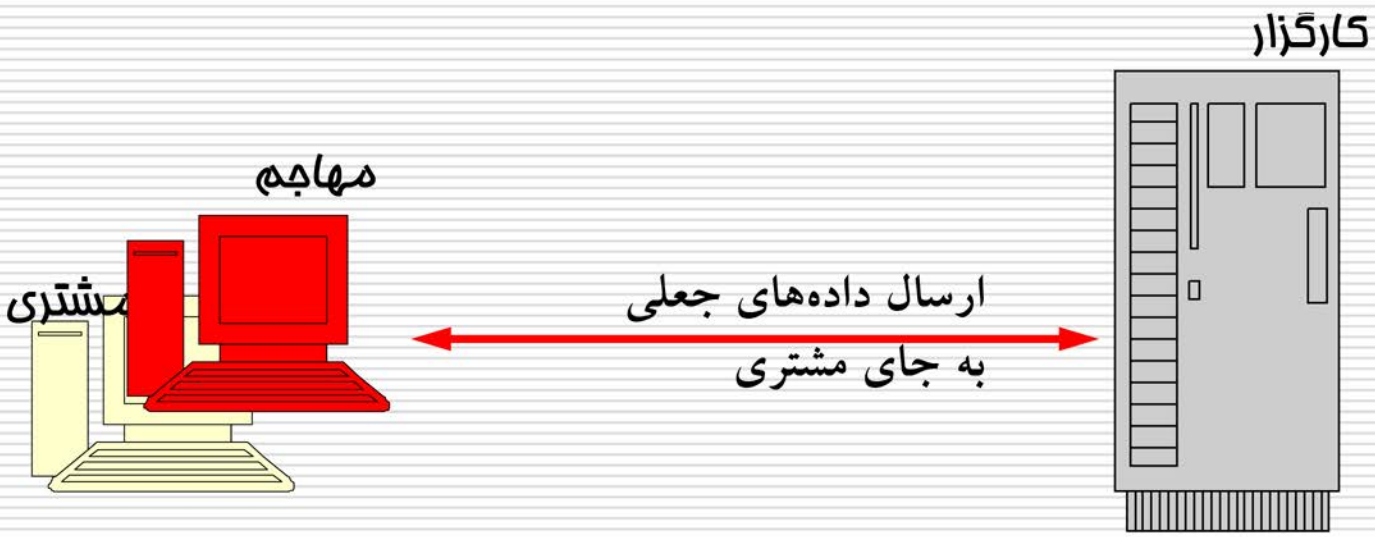
sooraac.ir

حمله جعل هویت

- 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 هویت (ادامه)

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



sooraac.ir

فهرست مطالب

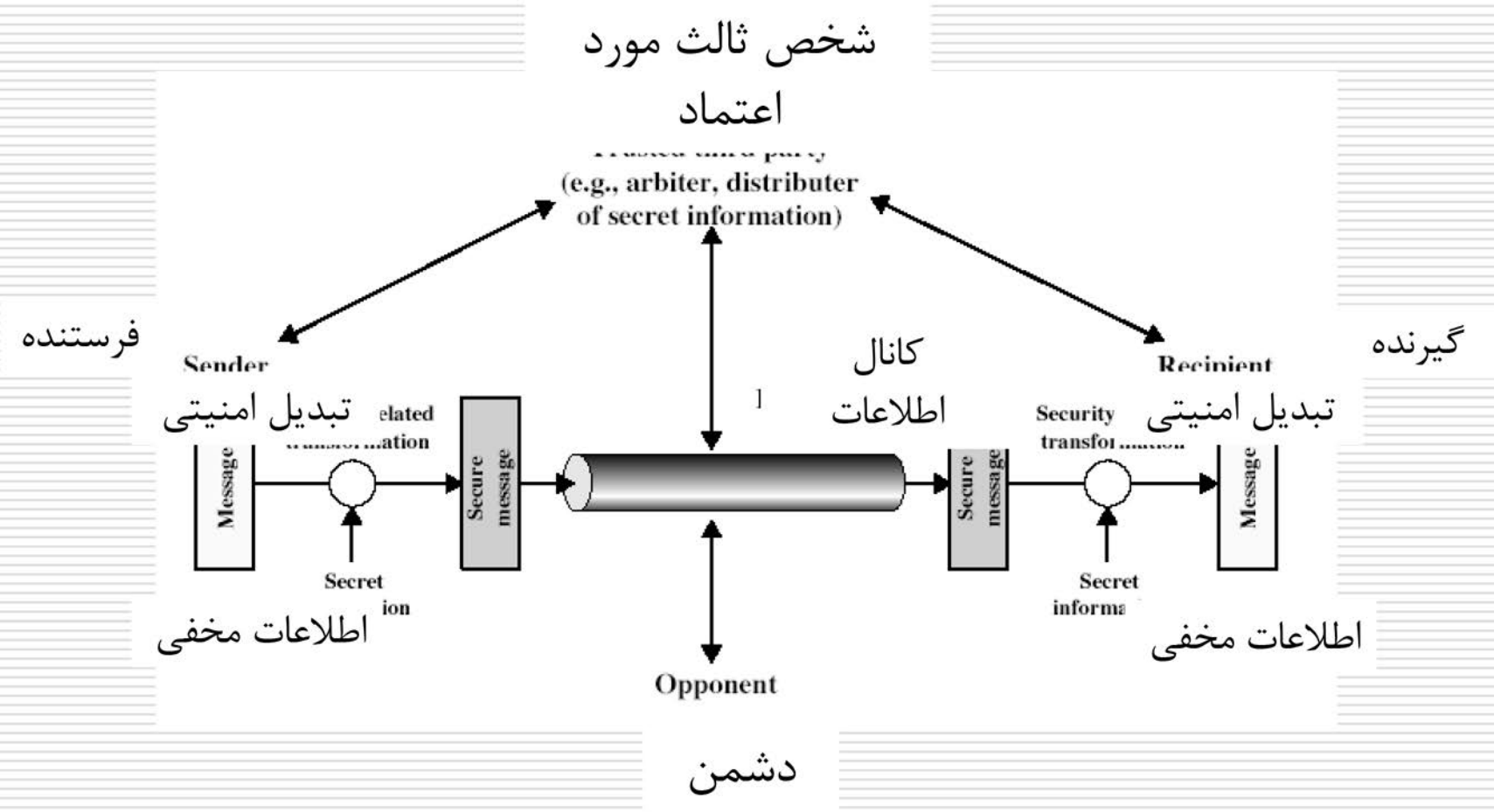
- محتوای درس
- ضرورت امنیت
- مفاهیم اولیه
- دشواری برقراری امنیت
- سرویس‌های امنیتی
- انواع و ماهیت حملات
- **مدل‌های امنیت شبکه**

sooraac.ir

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 سرویس‌های 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

sooraac.ir

پایان