امنیت داده و شبکه

مفاهیم و تعاریف اولیه

فهرست مطالب

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

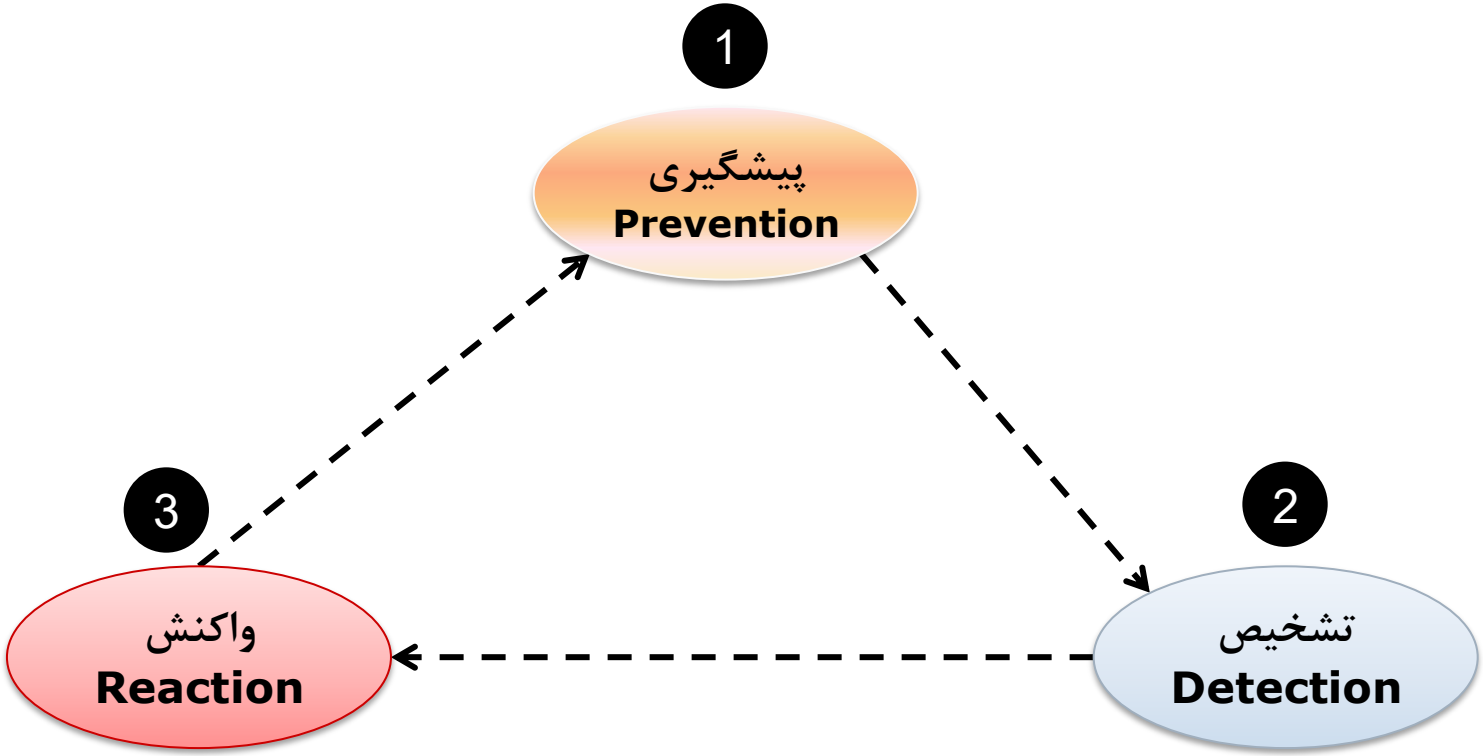
امنیت چیست؟

- 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

اقدامات امنیتی



دو واژه‌ای که امروزه مفهوم متفاوتی دارند (1)

- 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 (2)

- 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
- 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

نيازهاي امنيتي

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

ولی

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

آنچه این درس بررسي مي‌کند

- 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 - 1

- **درس ۱:** مفاهیم و تعاریف اولیه
- **درس ۲:** مکانیزم‌های تأمین امنیت
- **درس ۳:** مفاهیم رمزنگاری و رمزنگاری سنتی
- **درس ۴:** رمزنگاری متقارن (مدرن)
- **درس ۵:** رمزنگاری نامتقارن (کلید عمومی)
- **درس ۶:** کدهای تصدیق اصالت پیام و توابع چکیده‌ساز
- **درس ۷:** امضای رقمی و زیرساخت کلید عمومی
- **درس ۸:** طراحی پروتکلهای رمزنگاری

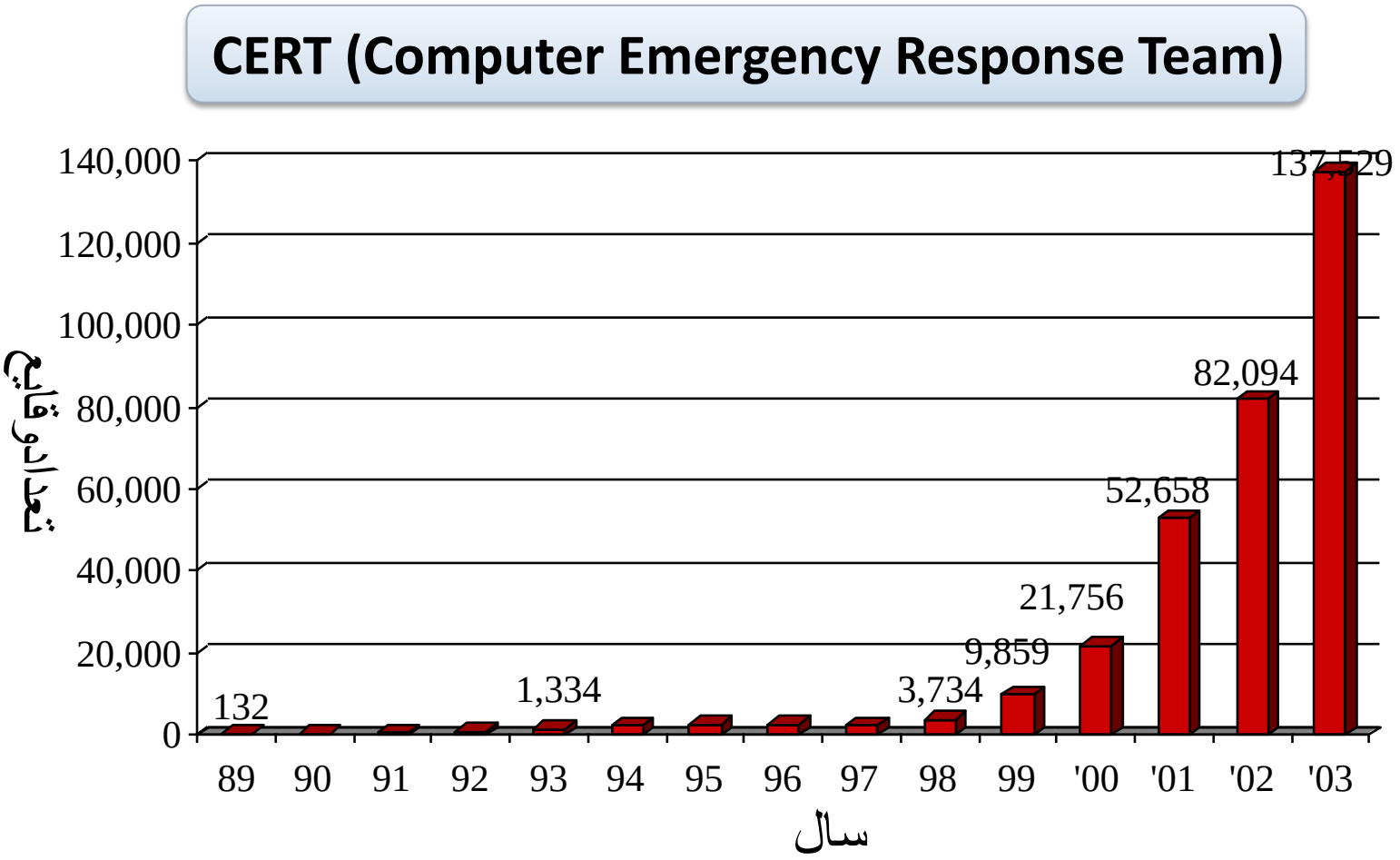
موضوعات تحت پوشش درس - 2

- **درس ۹:** پروتکل کربروس
- **درس ۱۰:** امنیت رایانامه (PGP)
- **درس ۱۱:** امنیت وب (SSL/TLS)
- **درس ۱۲:** امنیت لایه IP (IPSec)
- **درس ۱۳:** دیوار آتش
- **درس ۱۴:** سیستم تشخیص نفوذ
- **درس ۱۵:** کنترل دسترسی
- **درس ۱۶:** امنیت برنامه‌های کاربردی

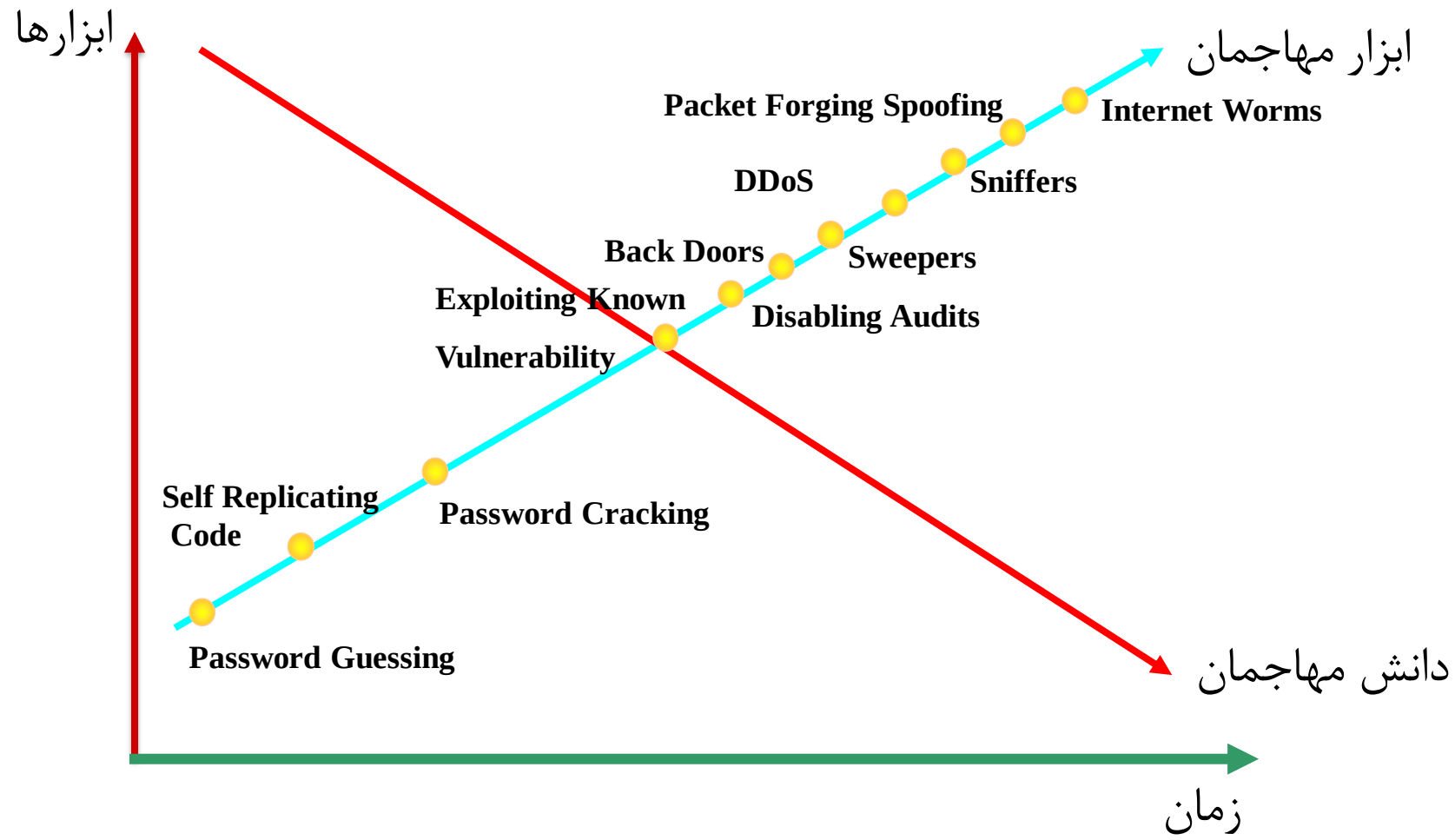
فهرست مطالب

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

آمار منتشر شده توسط CERT



ابزار مهاجمان



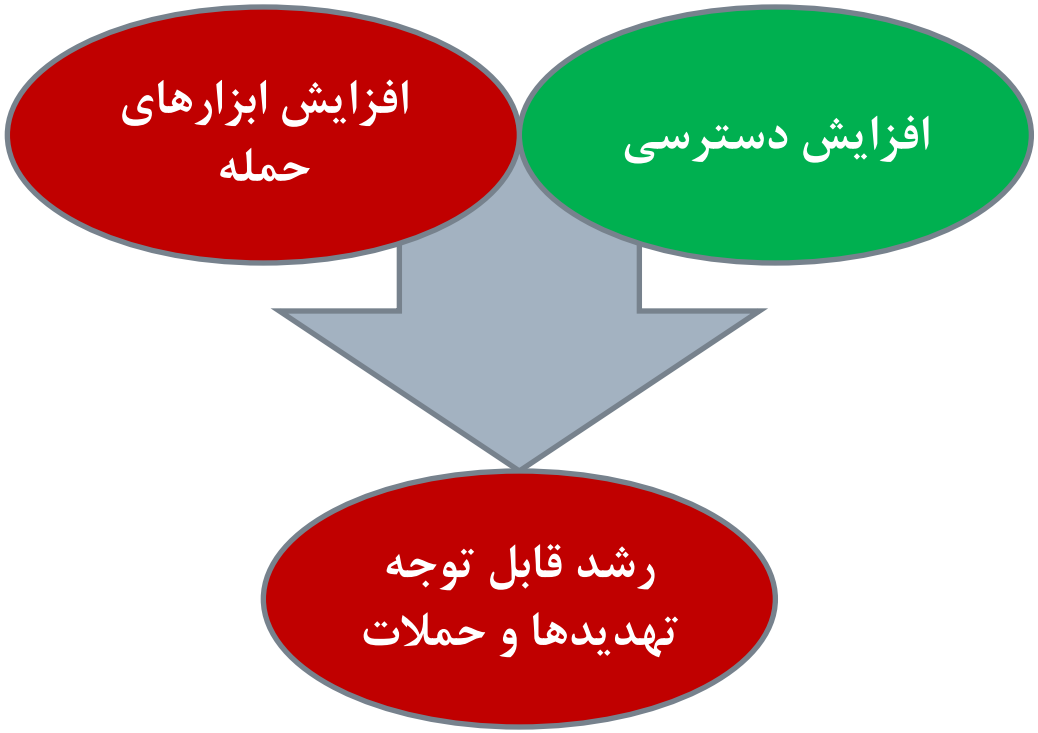
نیازهای امنیتی: گذشته و حال

- 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).

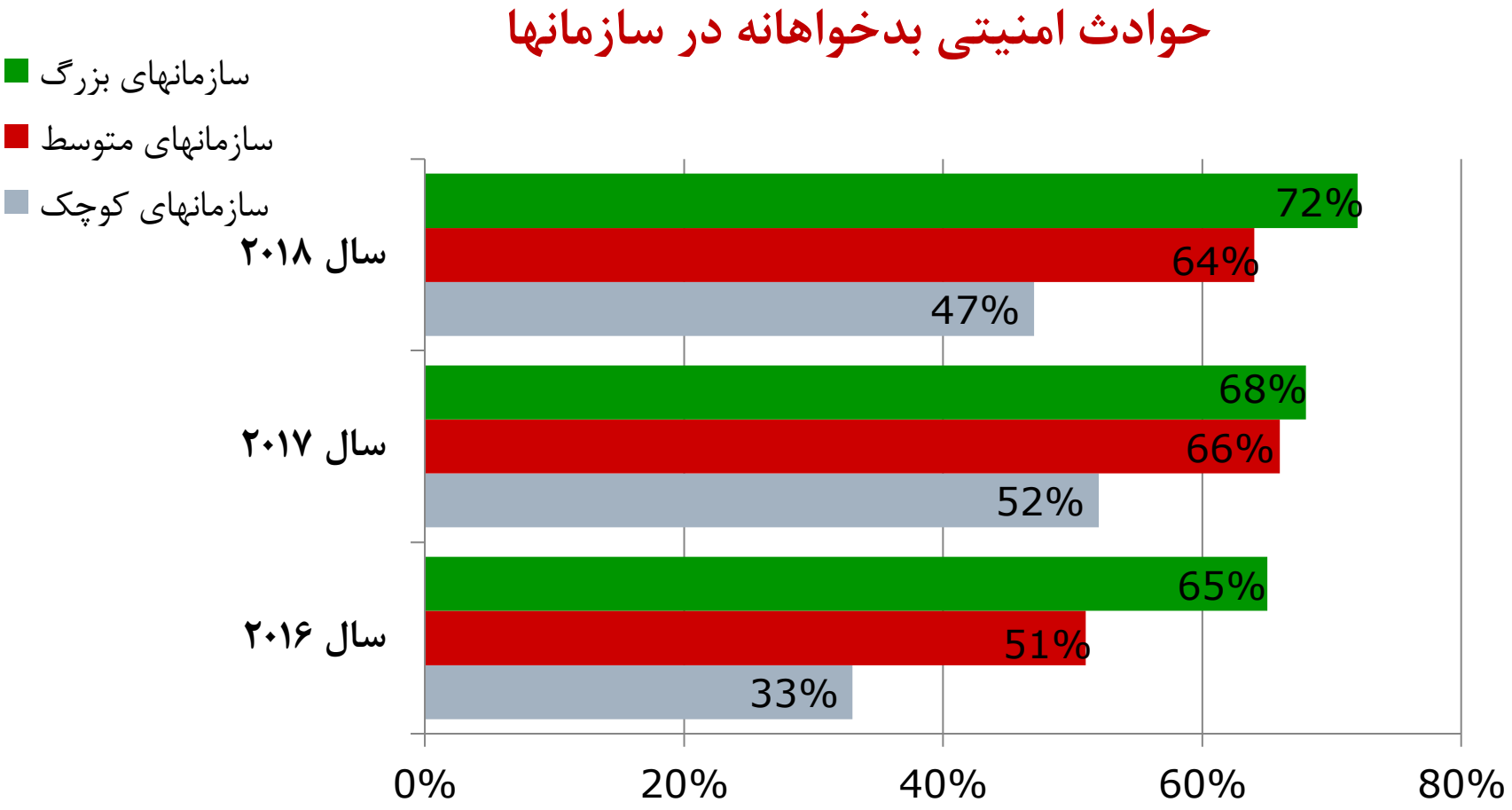
رشد تهدیدها و حملات



اهداف حملات

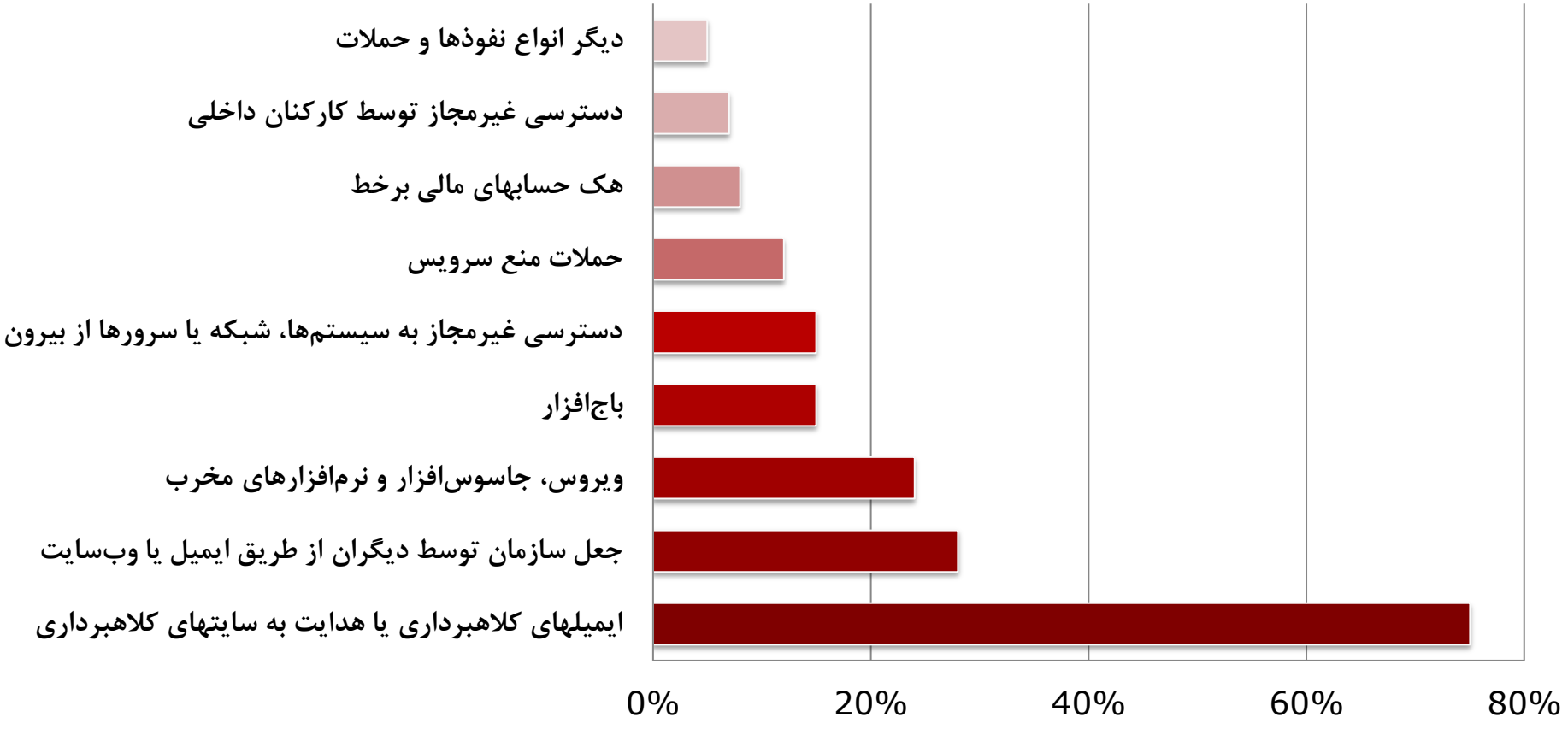
- **اهداف سیاسی**
  - تضعیف دولت‌ها (با حمله سایبری به زیرساخت‌های حساس و حیاتی)
- **اهداف اقتصادی**
  - ضربه زدن به رقبا
  - کسب اطلاعات رقبا
  - کسب درآمد از طرق نامشروع
- **اهداف شخصی**
  - انتقام‌جویی (خصومت‌های شخصی یا نارضایتی کاری)
  - اثبات و بروز توانمندی‌ها

نگاهي به گزارش رخنه‌های امنیتی انگلیس (1)



نگاهي به گزارش رخنه‌های امنیتی انگلیس (2)

انواع حوادث رخ داده در سازمانها (سال ۲۰۱۸)



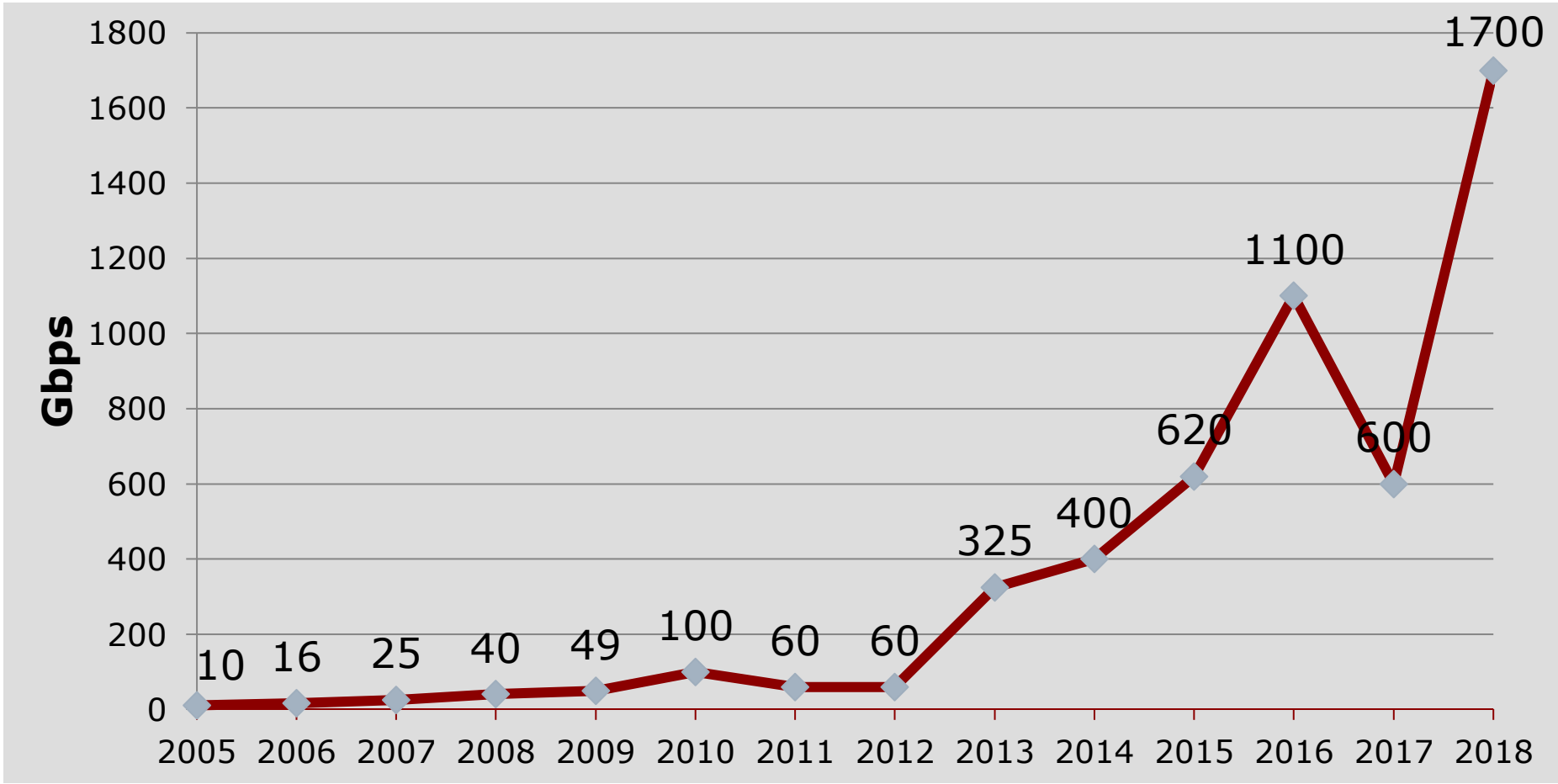
نگاهي به گزارش رخنه‌های امنیتی انگلیس (3)

متوسط هزینه‌های مرتبط با یک حادثه سنگین امنیتی – ۲۰۱۶ تا ۲۰۱۸

	سازمانهای کوچک (پوند)	سازمانهای متوسط (پوند)	سازمانهای بزرگ (پوند)
سال ۲۰۱۶	۳۱۰۰	۱۸۶۰	۳۶۵۰۰
سال ۲۰۱۷	۱۳۸۰	۳۰۷۰	۱۹۶۰۰
سال ۲۰۱۸	۸۹۴	۸۱۸۰	۹۲۶۰

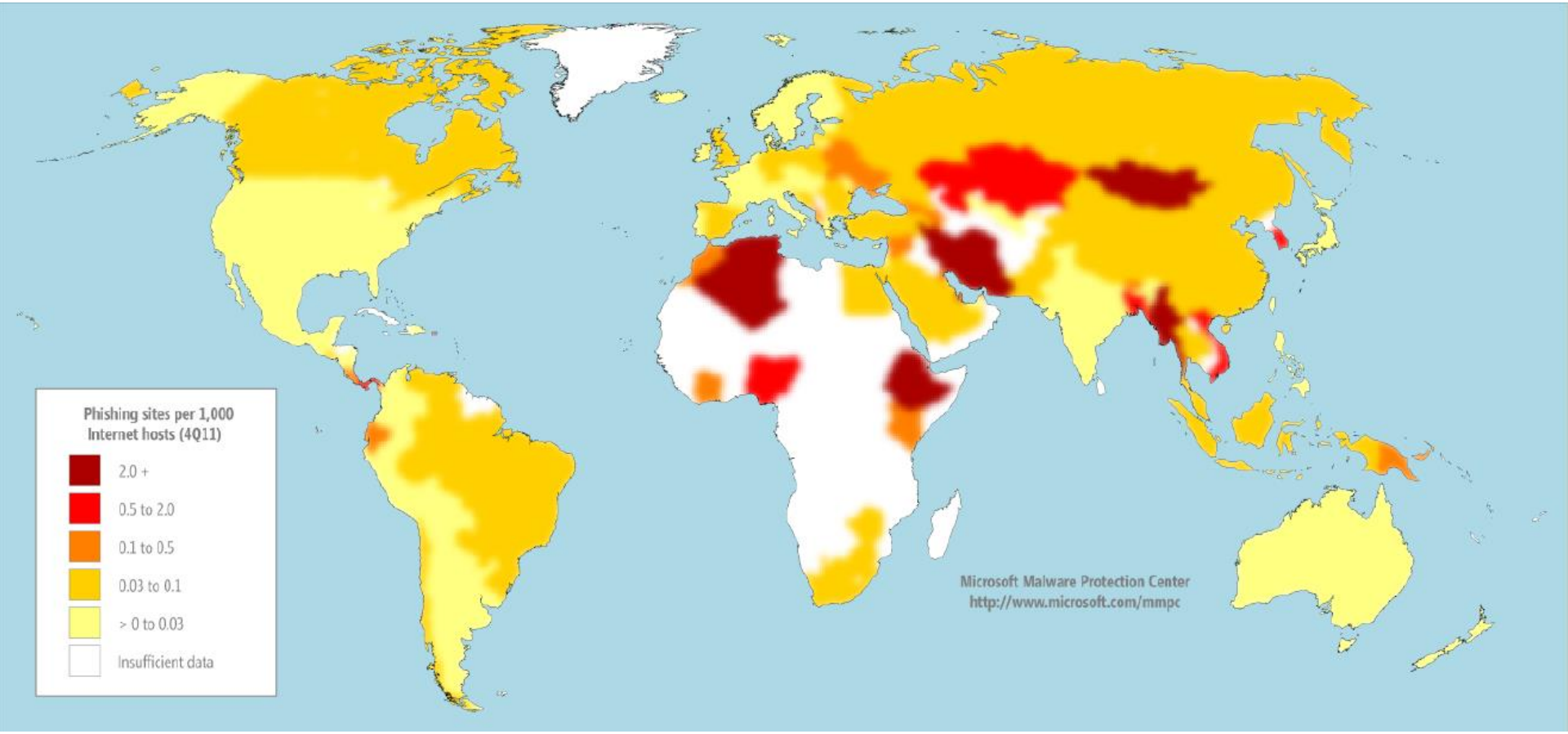
رشد حملات منعِ سرویس

رشد حملات منع سرویس بر اساس گزارش NETSCOUTیاArbor Networks سابق



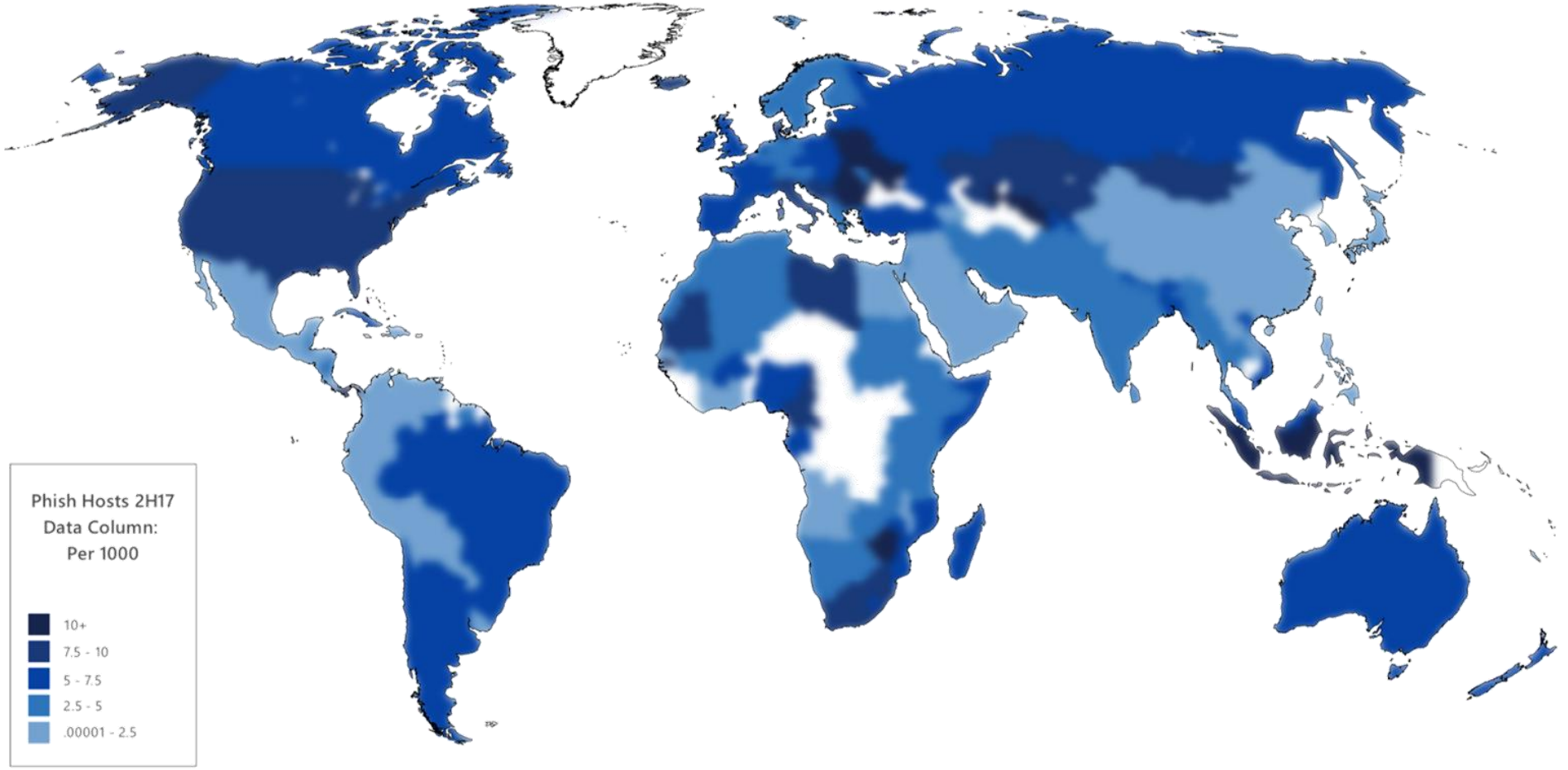
توزیع سایت‌های فیشینگ (1)

توزیع سایت‌های فیشینگ در دنیا در ۳ ماه چهارم ۲۰۱۱ (گزارش SIR)



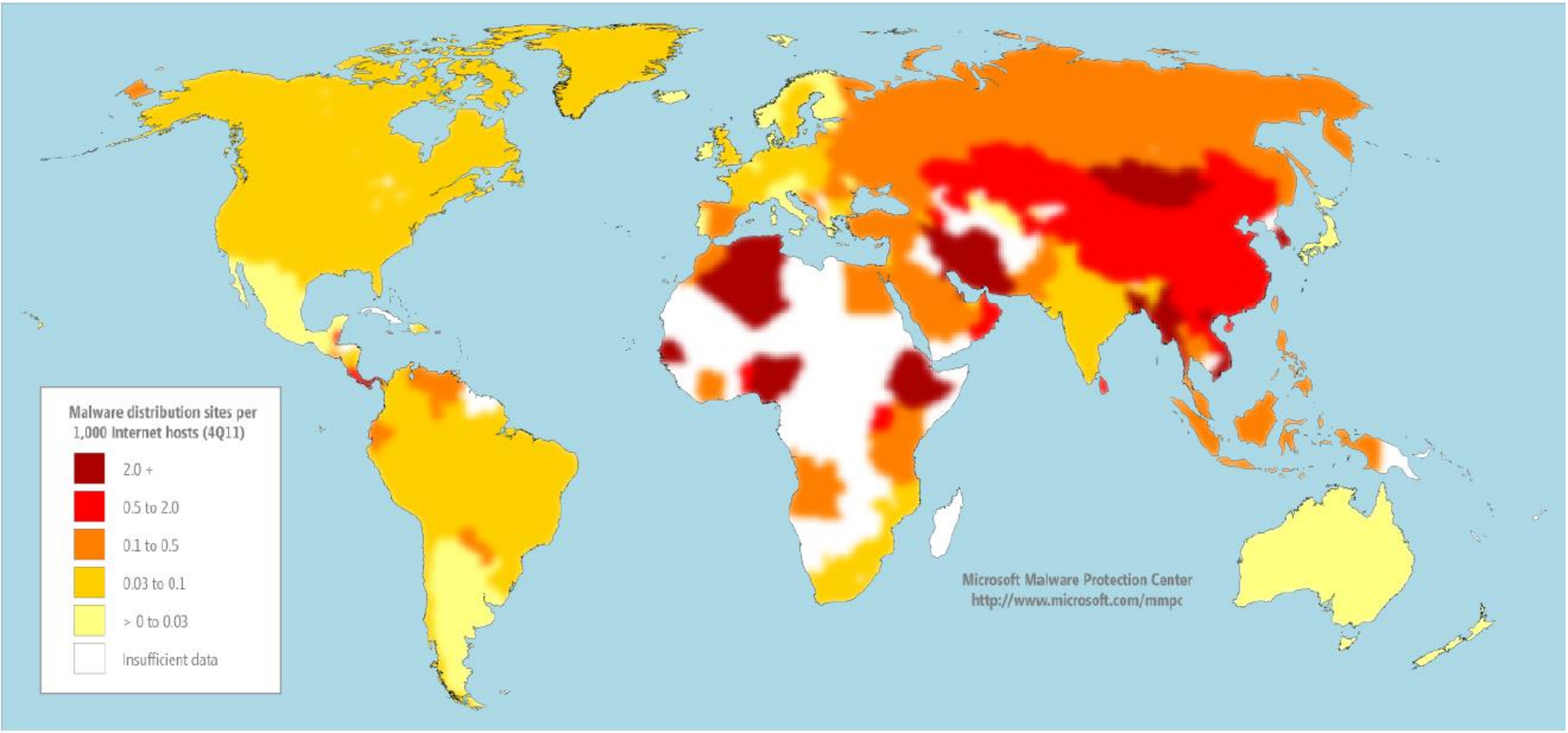
توزیع سایت‌های فیشینگ (2)

توزیع سایت‌های فیشینگ در دنیا در نیمه دوم ۲۰۱۷ (گزارش SIR)



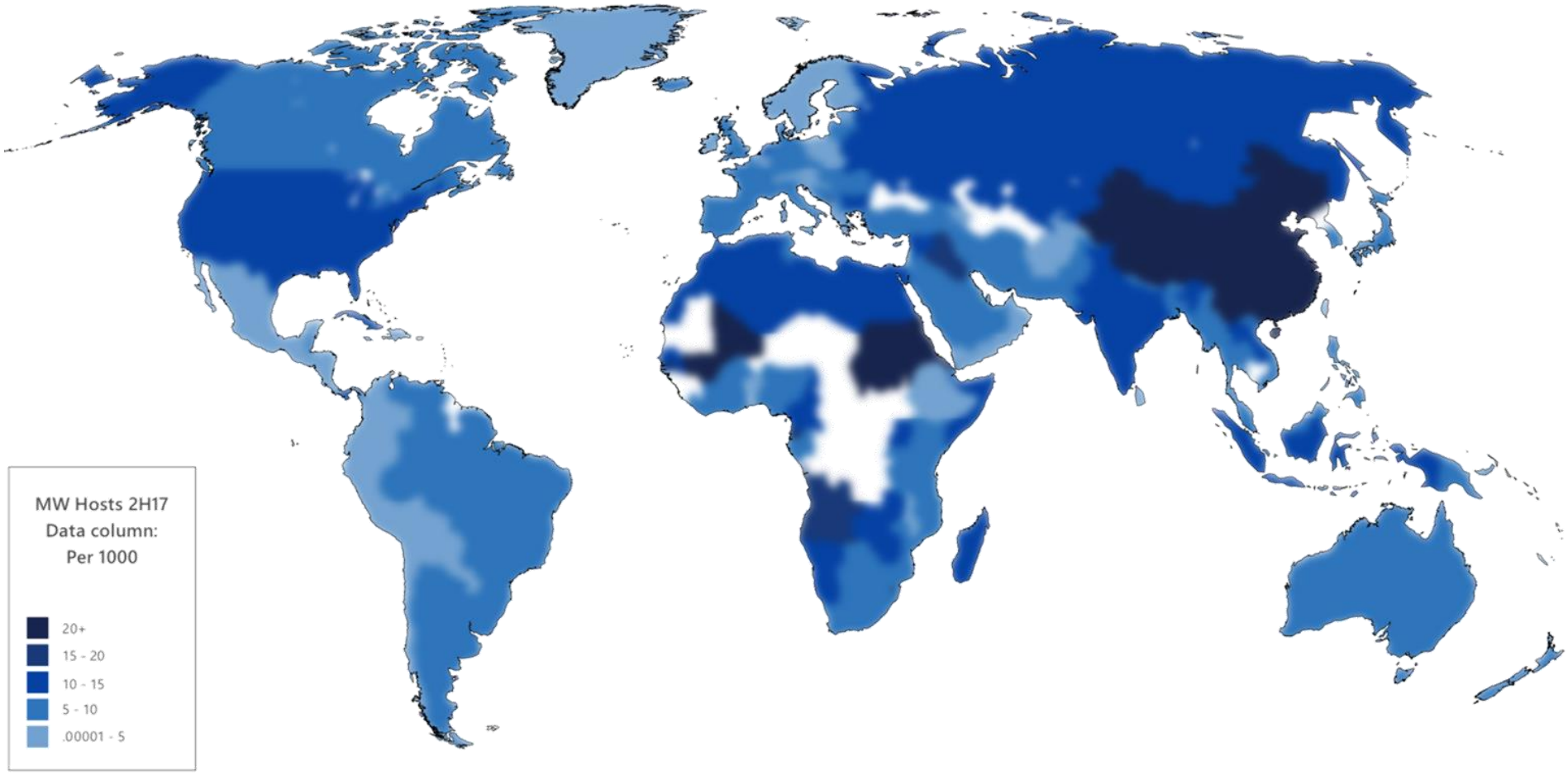
توزیع سیستم‌های آلوده (1)

توزیع سیستم‌های آلوده به بدافزار در دنیا در ۳ ماه چهارم ۲۰۱۱ (گزارش SIR)



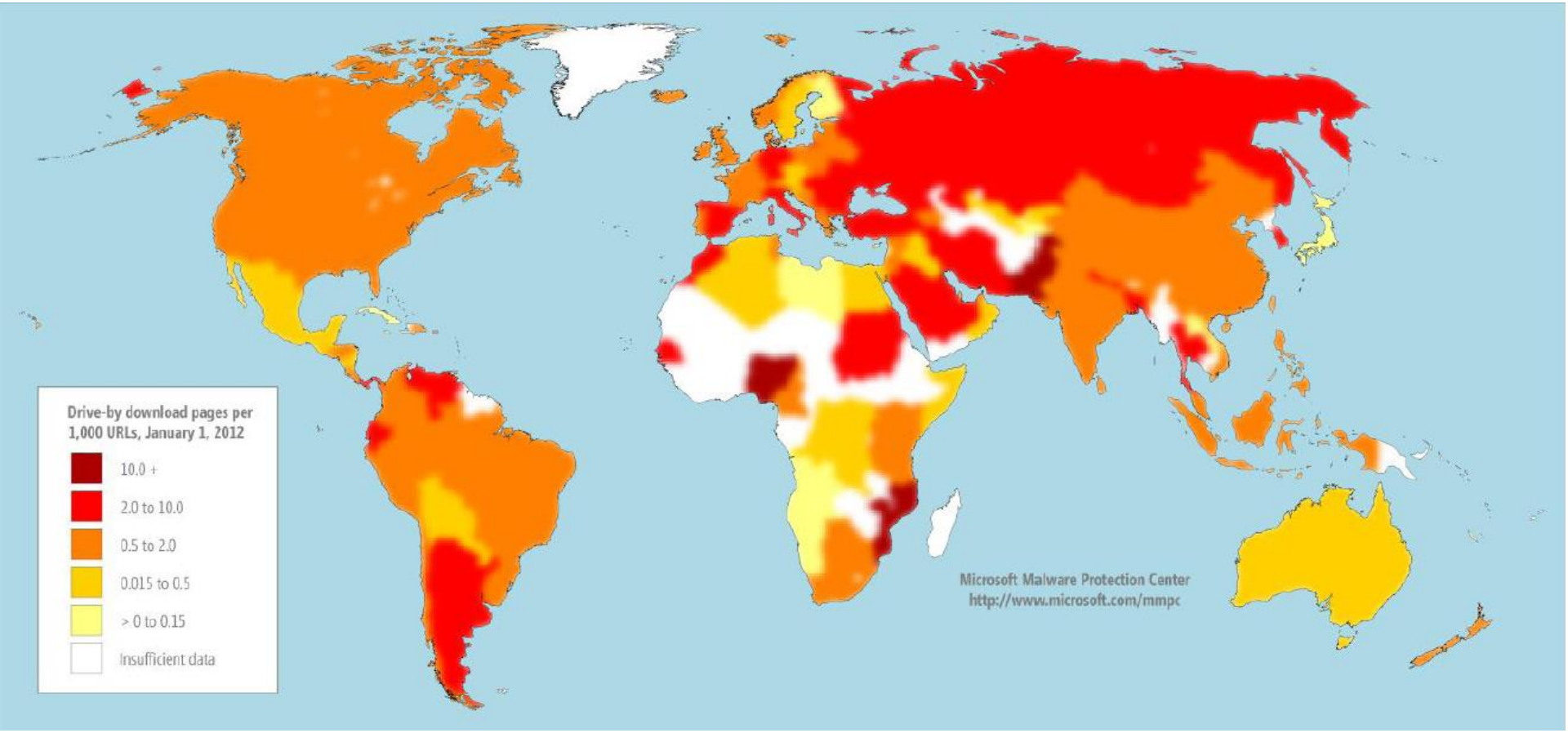
توزیع سیستم‌های آلوده (2)

توزیع سیستم‌های آلوده به بدافزار در دنیا در نیمه دوم ۲۰۱۷ (گزارش SIR)



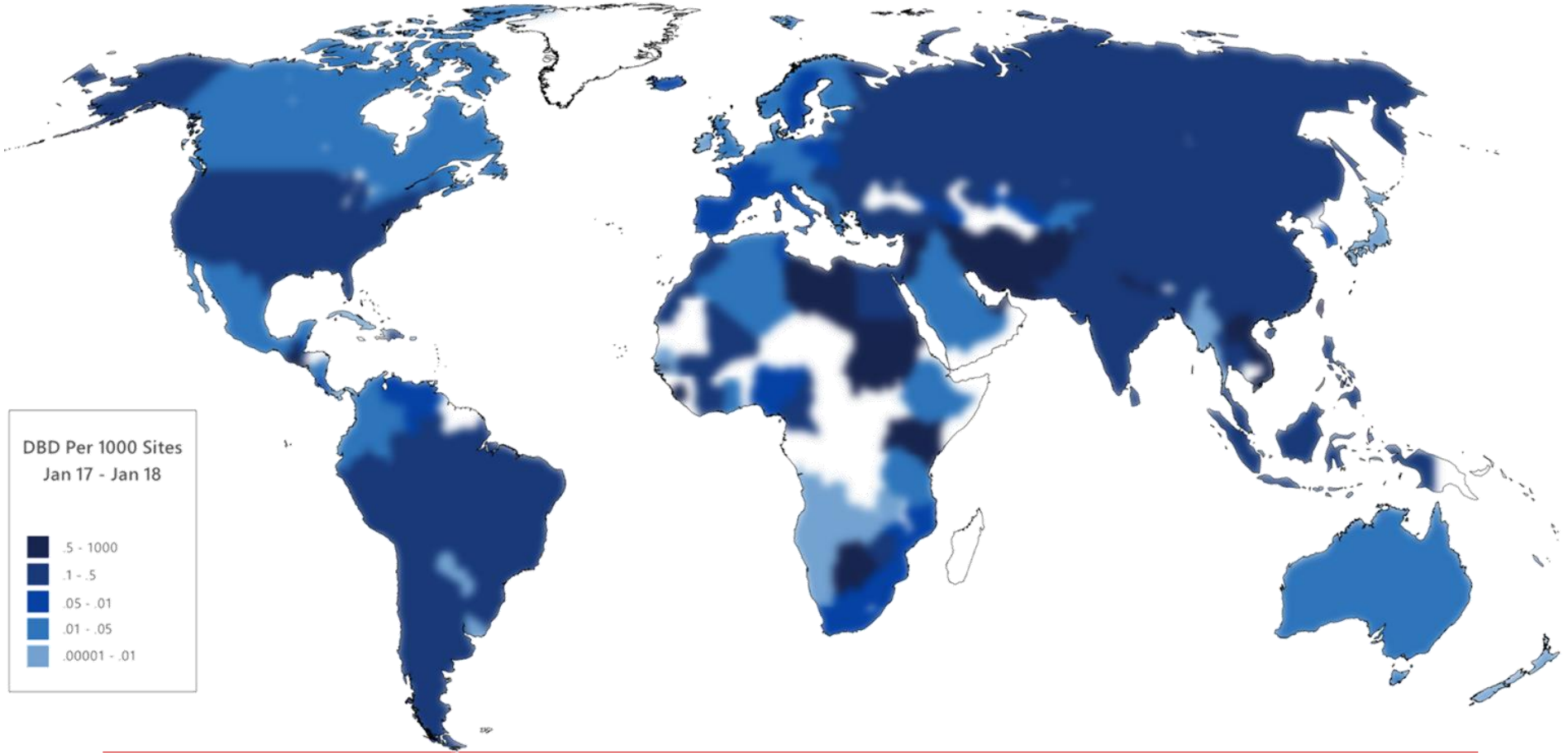
توزیع سایت‌های آلوده‌ساز (1)

توزیع سایت‌های آلوده‌ساز در دنیا در ۳ ماهه چهارم ۲۰۱۱ (گزارش SIR)



توزیع سایت‌های آلوده‌ساز (2)

توزیع سایت‌های آلوده‌ساز در دنیا در نیمه دوم ۲۰۱۷ (گزارش SIR)



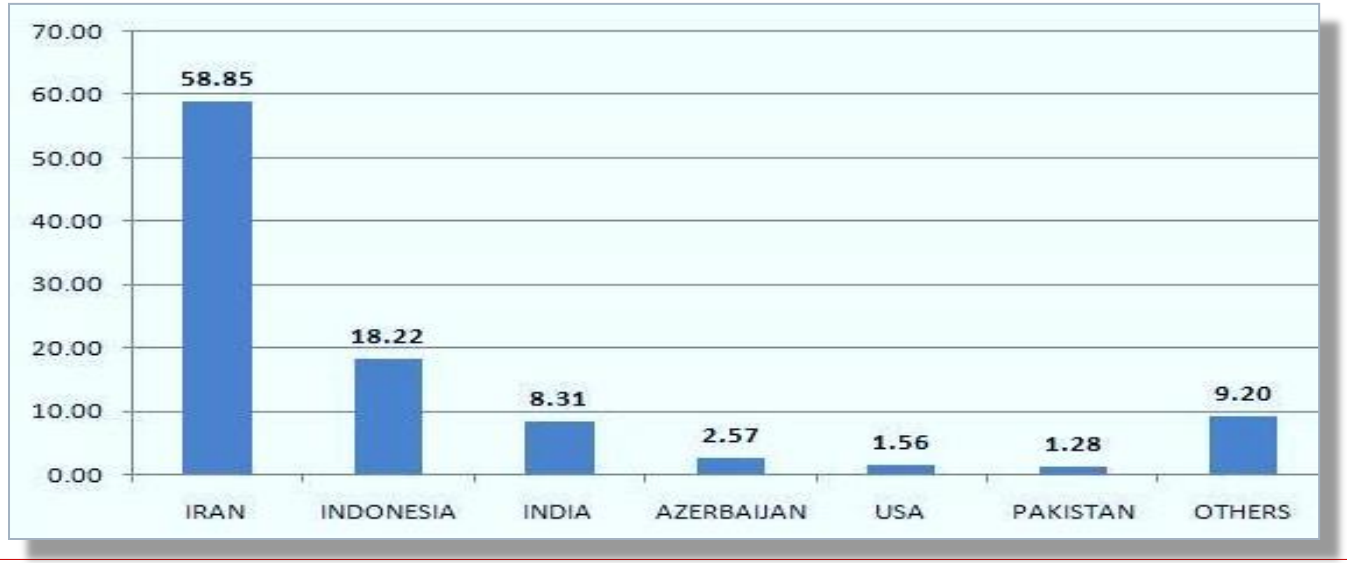
جنگ سایبری (1)

- **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 ...

- **حمله سایبری روسیه به استونی (۲۰۰۷)**
  - حمله به وزارتخانه‌ها، بانک‌ها، و رسانه‌ها
  - حمله از طریق سِروِرهای اداری تحت کنترل روسیه

جنگ سایبری (2)

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



جنگ سایبری (3)

- **حمله به وزارت خارجه ایران (۲۰۱۱)**
  - توسط گروهی موسوم به گروه Anonymous
  - نفوذ به کارگزارهای پست الکترونیکی یکی از ادارات مرتبط با وزارتخانه
  - افشای محتوای بیش از ۱۰,۰۰۰ پست الکترونیکی
- **جمع‌آوری اطلاعات محرمانه توسط تروجان Duqu (۲۰۱۱)**
  - Duqu به عنوان نسخه دوم Stuxnet
  - هدف اولیه: جمع‌آوری اطلاعات
  - هدف اصلی: نامعلوم؟!
  - بیشترین آلودگی‌ها: ایران و سودان

جنگ سایبری (4)

- **جاسوسی با بدافزار شعله – Flame (۲۰۱۲)**
  - جهت جاسوسی در مجموعه نفتی ایران
  - منبع حمله: نامعلوم! اسراییل یا آمریکا!
  - پویش و جمع‌آوری اطلاعات شبکه
  - ضبط صوت، تصویر صفحه نمایش و کلیدهای فشرده شده
  - جمع‌آوری اطلاعات فایلهای خاص و گذرواژه‌ها
  - ارسال اطلاعات جمع‌آوری شده به یک سیستم فرماندهی و کنترل

جنگ سایبری (۵)

- **نفوذ به برخی سیستمها در انتخابات ریاست جمهوری آمریکا (۲۰۱۶)**
  - هدف: تاثیرگذاری بر نتایج انتخابات ریاست جمهوری آمریکا
  - حمله کنندگان: دو تیم APT28 و APT29 روسی
  - سیستمهای مورد نفوذ:
    - سیستمهای کمیته ملی دموکراتها
    - سیستمهای ستاد انتخاباتی کنگره دموکراتها
    - پست الکترونیکی آقای پودستا رییس ستاد انتخاباتی خانم کلینتون

جنگ سایبری (۶)

- **حمله به سازمان‌ها و آژانس‌های دولتی آمریکایی- Sunburst (۲۰۲۰)**
  - هدف: جمع‌آوری اطلاعات و نه اقدامات خرابکارانه
  - شیوه حمله: تزریق dll مخرب به بسته بروزرسانی نرم‌افزار SolarWinds
  - حمله‌کننده: ظاهرا روسیه (به نقل از سرویس‌های اطلاعاتی و جاسوسی آمریکا)
  - سازمان‌های مورد حمله:
    - ۱۸هزار سازمان و آژانس آمریکایی
    - وزارتخانه‌های خزانه‌داری، دادگستری، بازرگانی، خارجه، دفاع، امنیت داخله آمریکا
    - رییس شرکت مایکروسافت (برد اسمیت) آن را بزرگترین و پیچیده‌ترین حمله سایبری عنوان کرده.

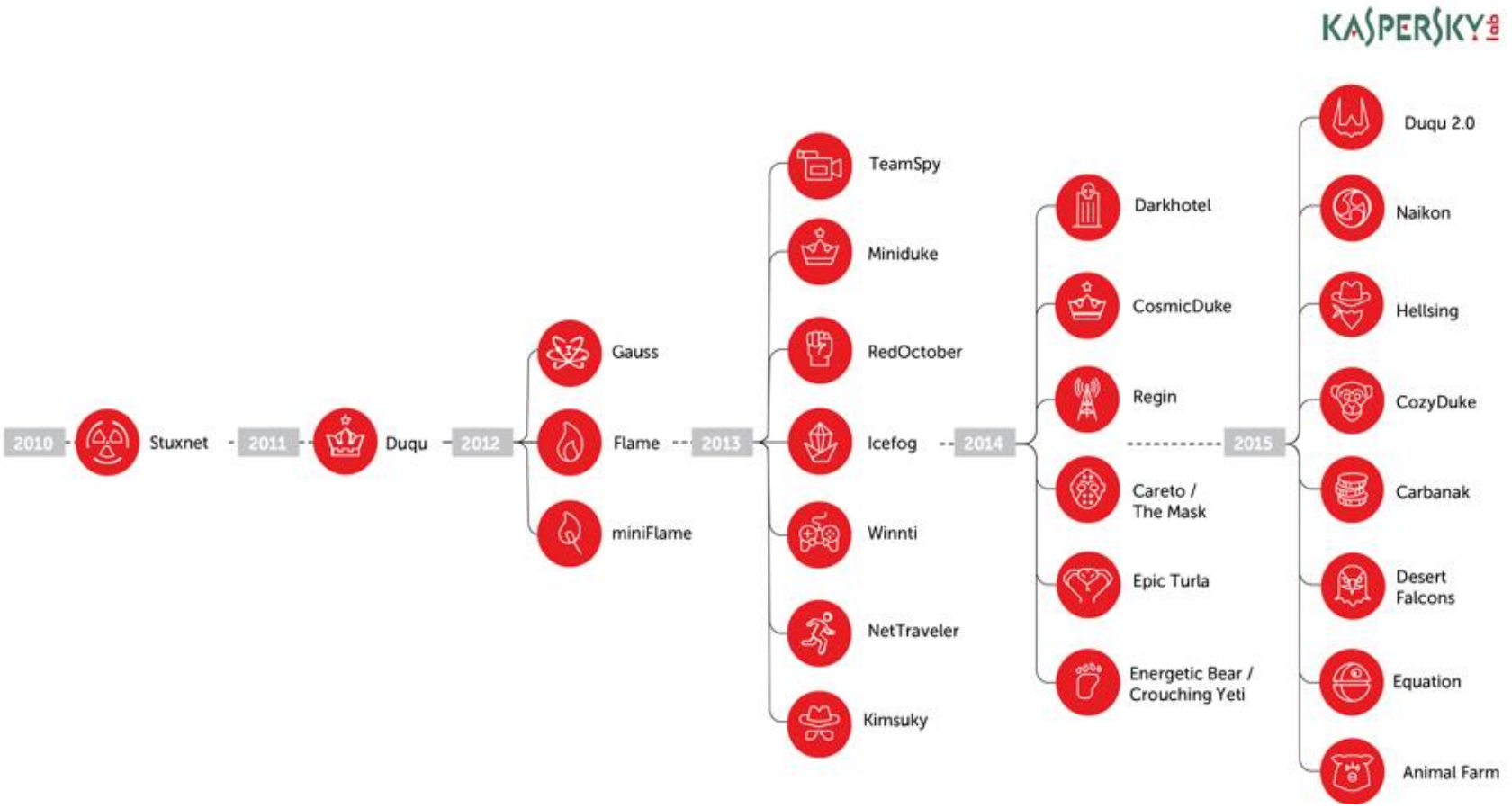
جنگ سایبری (۷)

تهدید یا حمله مانای پیشرفته (APT)

- **هدف:** حمله سازمان‌یافته و هدفمند توسط مهاجمین با سطح مهارت بالا علیه کشورها و سازمانها

جنگ سایبری (۷)

تهدید یا حمله مانای پیشرفته (APT)



فهرست مطالب

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

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

محرمانگي

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.

محرمانگي

- مکانیزم‌های متداول:
  - رمزنگاری
  - کنترل دسترسی

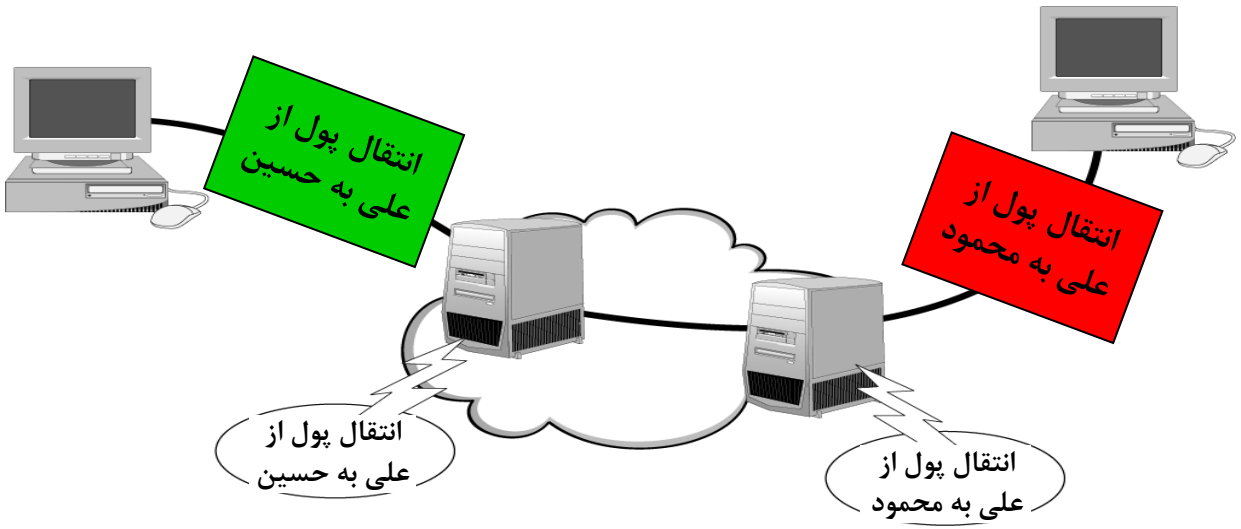
صحت

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



دسترس‌پذيري

- 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

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 تنظیمات

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

ضعف سیاست‌گذاری

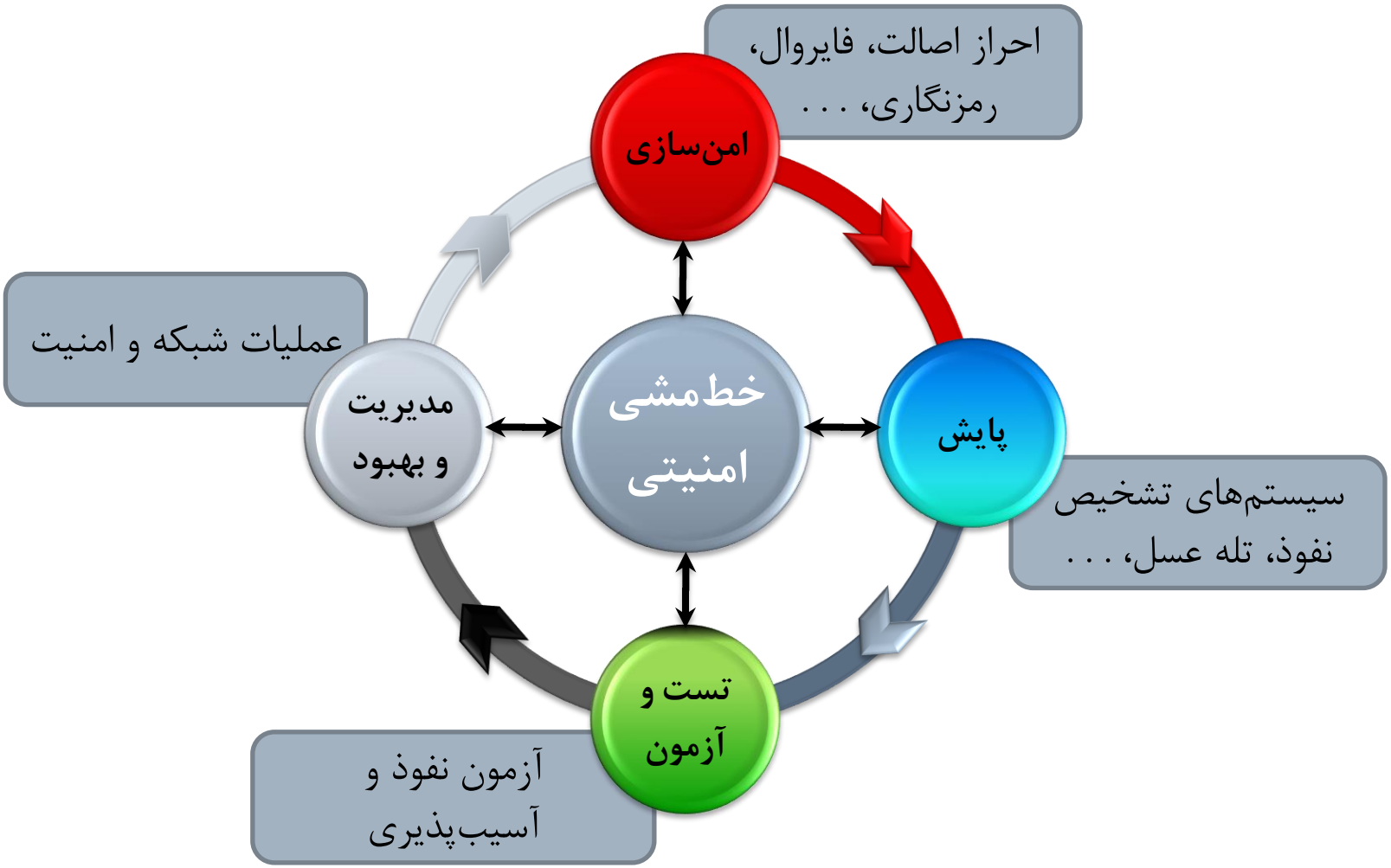
ضعف مدیریتی

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

امن‌سازي

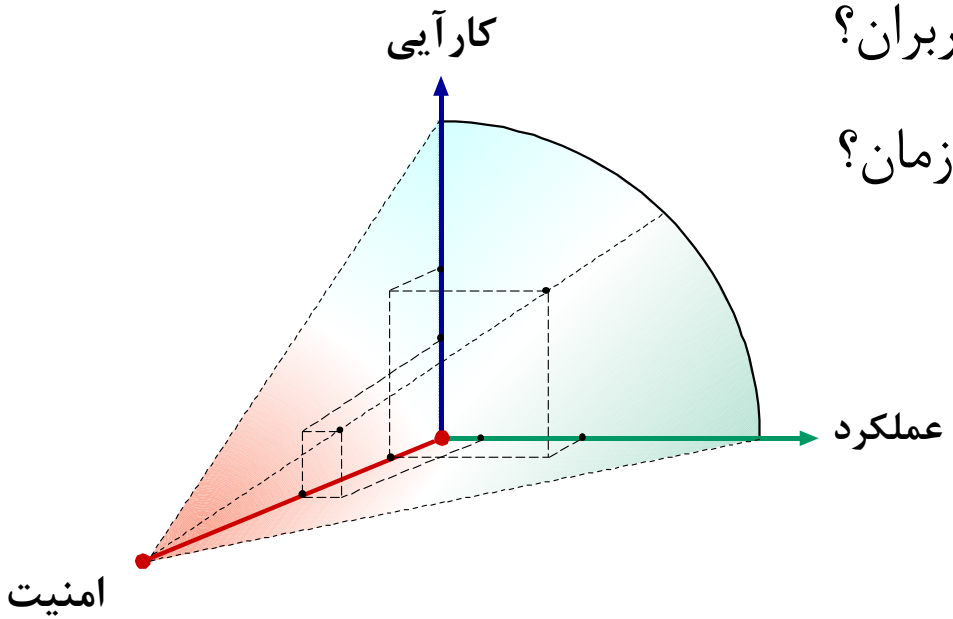
- نگرش مدیریتی به مسئلهٔ امنیت لازم است و نه صرفا نگرش فنی.
- امن‌سازی یک فرآیند است نه یک وظیفه خاص و مقطعی.
- مادام که انسان‌ها امن فکر نکنند نمی‌توان تراکنش امن داشت.

چرخه ایجاد امنیت



استراتژي امنيت سازماني

- مصالحه بين **امنیت**، **کارآیی (Performance)** و **عملکرد (Functionality)**.
- مصالحه بین **امنیت** و **هزینه**.
- میزان امنیت مورد انتظار کاربران؟
- میزان ناامنی قابل تحمل سازمان؟



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 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.
  - باید بدانید تا چه اندازه و در چه نقاطی نیاز به اقدامات محافظتی دارید.

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

(...)

- **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.

- **رخنه (Breach)**: نقض سیاست امنیتی یک سیستم

- **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).

- **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.

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

- 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.

- 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.

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

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

- **حفظ صحت داده‌ها:** اطمینان از اینکه آنچه رسیده همان است که فرستاده شده.
  - کد احراز هویت پیام (MAC)
  - امضاء
  - کنترل دسترسی
- **حفظ محرمانگی داده‌ها:** اطمینان از اینکه تنها کاربران مورد نظر قادر به درک پیامها است.
  - رمزنگاری
  - کنترل دسترسی

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

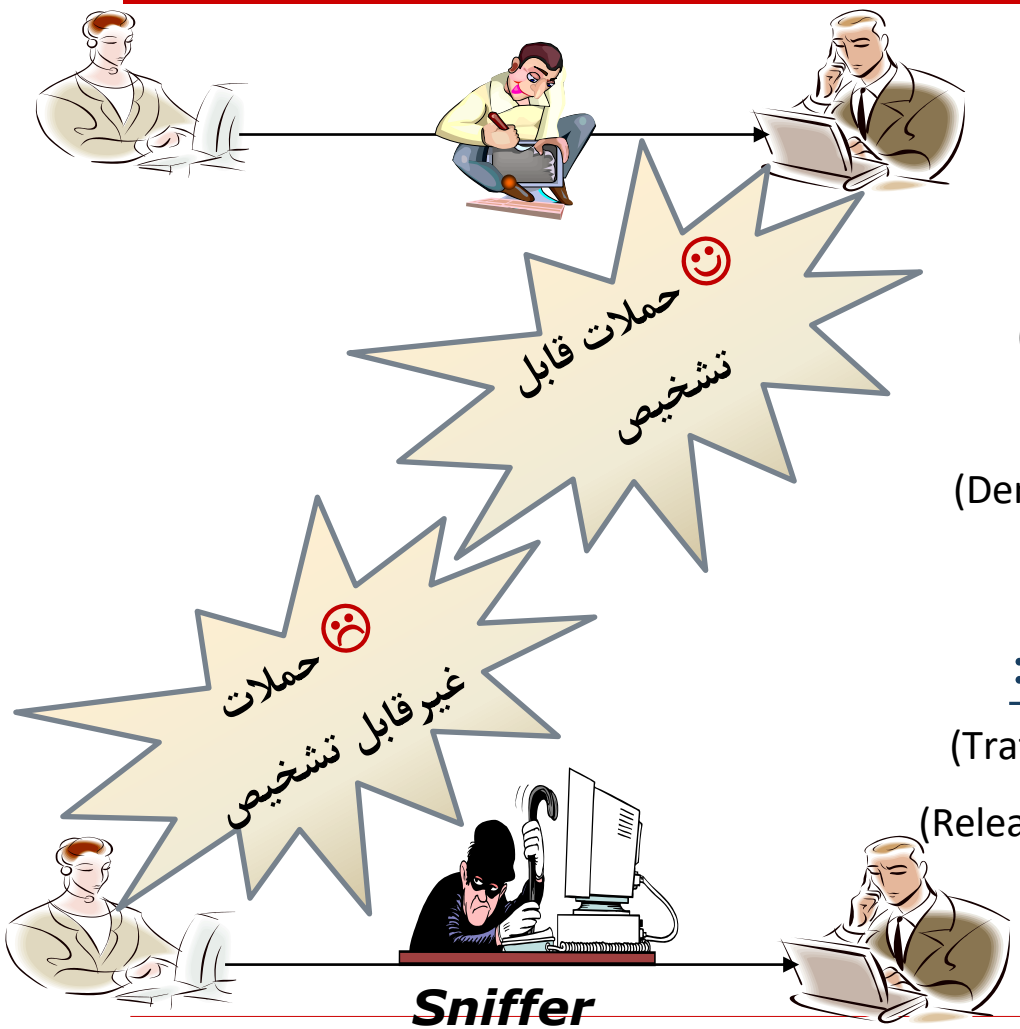
- **کنترل دسترسی:** کاربر تنها به منابع مقرر شده حق دسترسی دارد.
  - مجازشماری هم نامیده می‌شود.

- **عدم‌انکار:** عدم امکان انکار دریافت/ارسال توسط گیرنده/فرستنده
  - امضاء

- **دسترس‌پذیری:** در دسترس بودن به موقع خدمات برای کاربران مجاز

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

( )

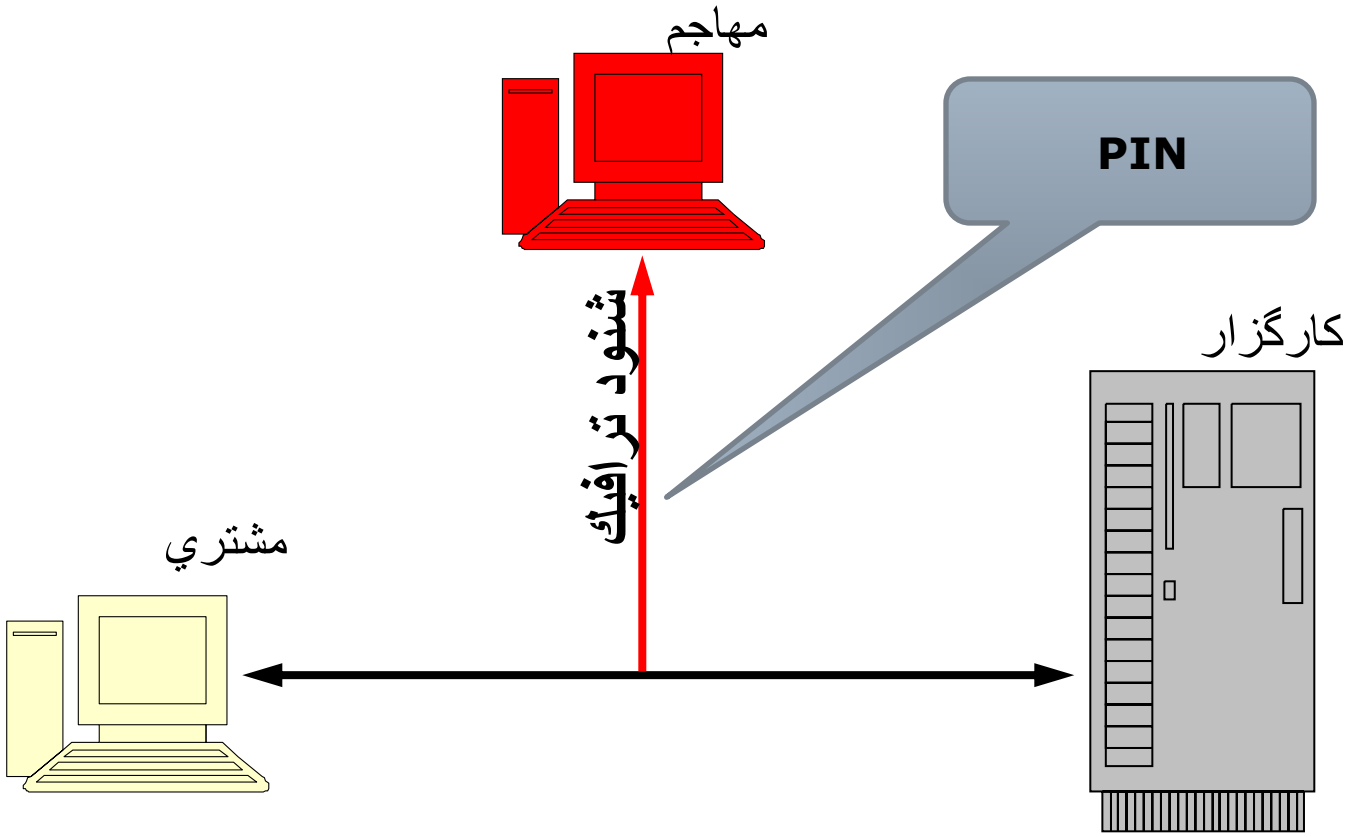


انواع حملات از نظر تاثیر:

- **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)

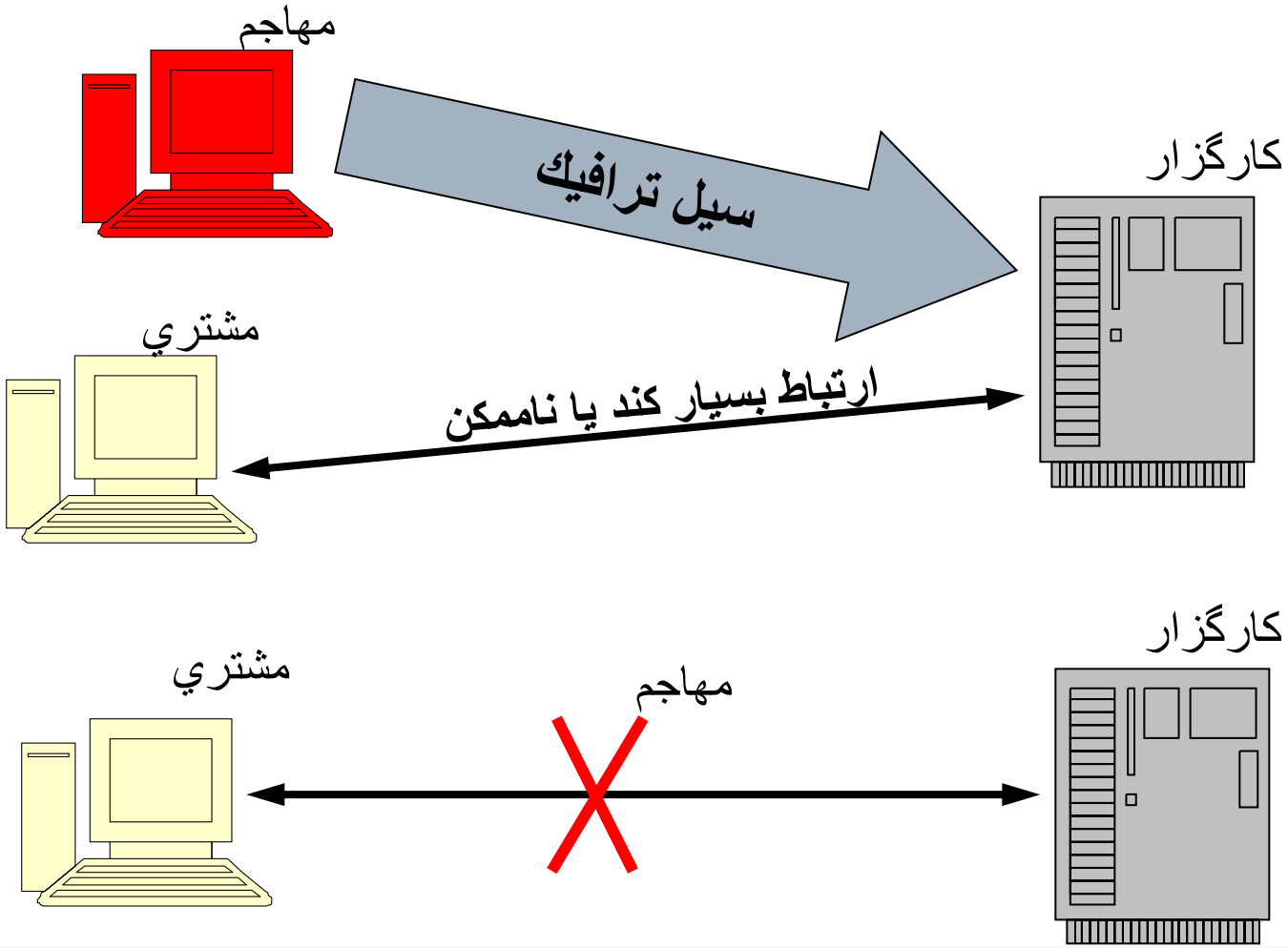
- هدف: نقض محرمانگی
- نتیجه: دسترسی غیرمجاز به داده‌های طبقه‌بندی شده
- راه‌های تحقق حمله:
  - اتصال فیزیکی به شبکه و دریافت بسته‌ها
  - دسترسی غیرمجاز به پایگاه‌داده‌ها
  - وجود ضعف و آسیب‌پذیری در سیستم کنترل دسترسی

( )


مهاجم
PIN
شنود ترافیک
کارگزار
مشتري

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

( )

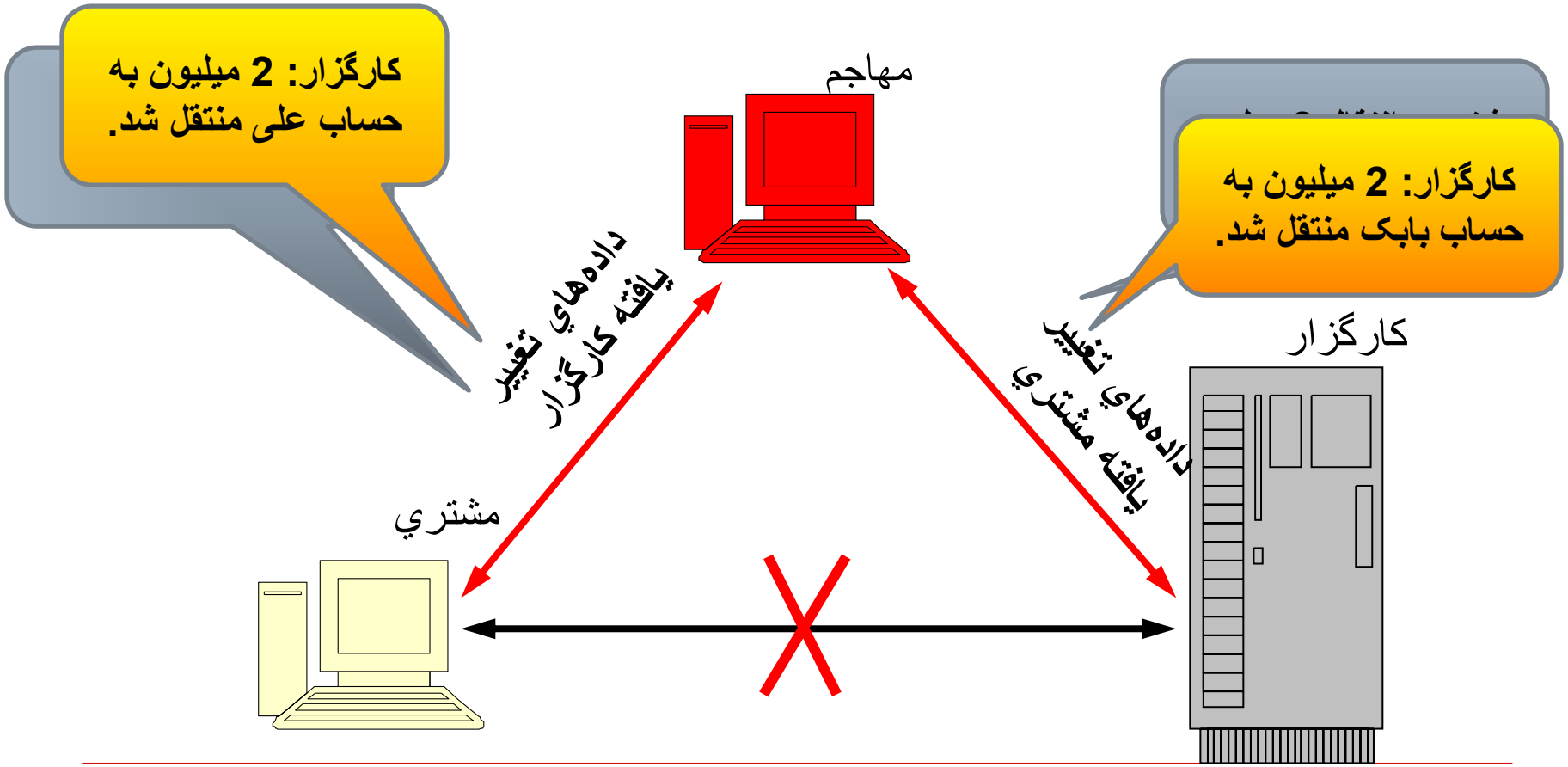

مهاجم
سيل ترافيك
كارگزار
مشتري
ارتباط بسيار كند يا ناممكن
كارگزار
مشتري
مهاجم

حمله تغییر یا دستکاري 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 تغيير يا دستكاري داده‌ها (ادامه)

- حمله مرد میانی (Man in the Middle)

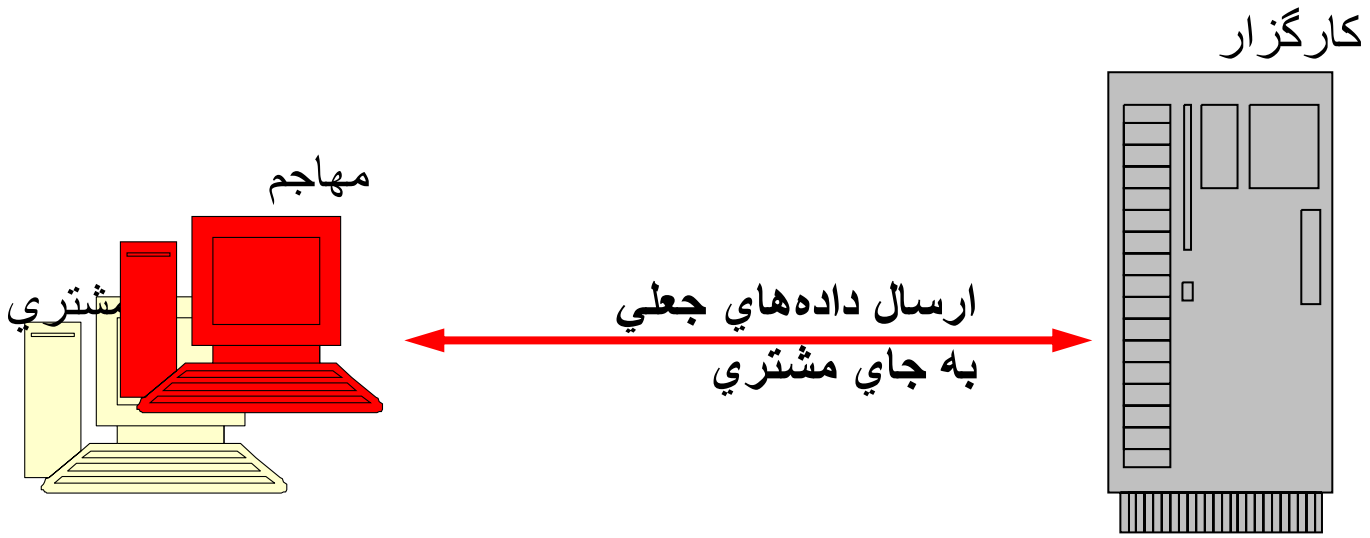


حمله جعل هویت

- 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)



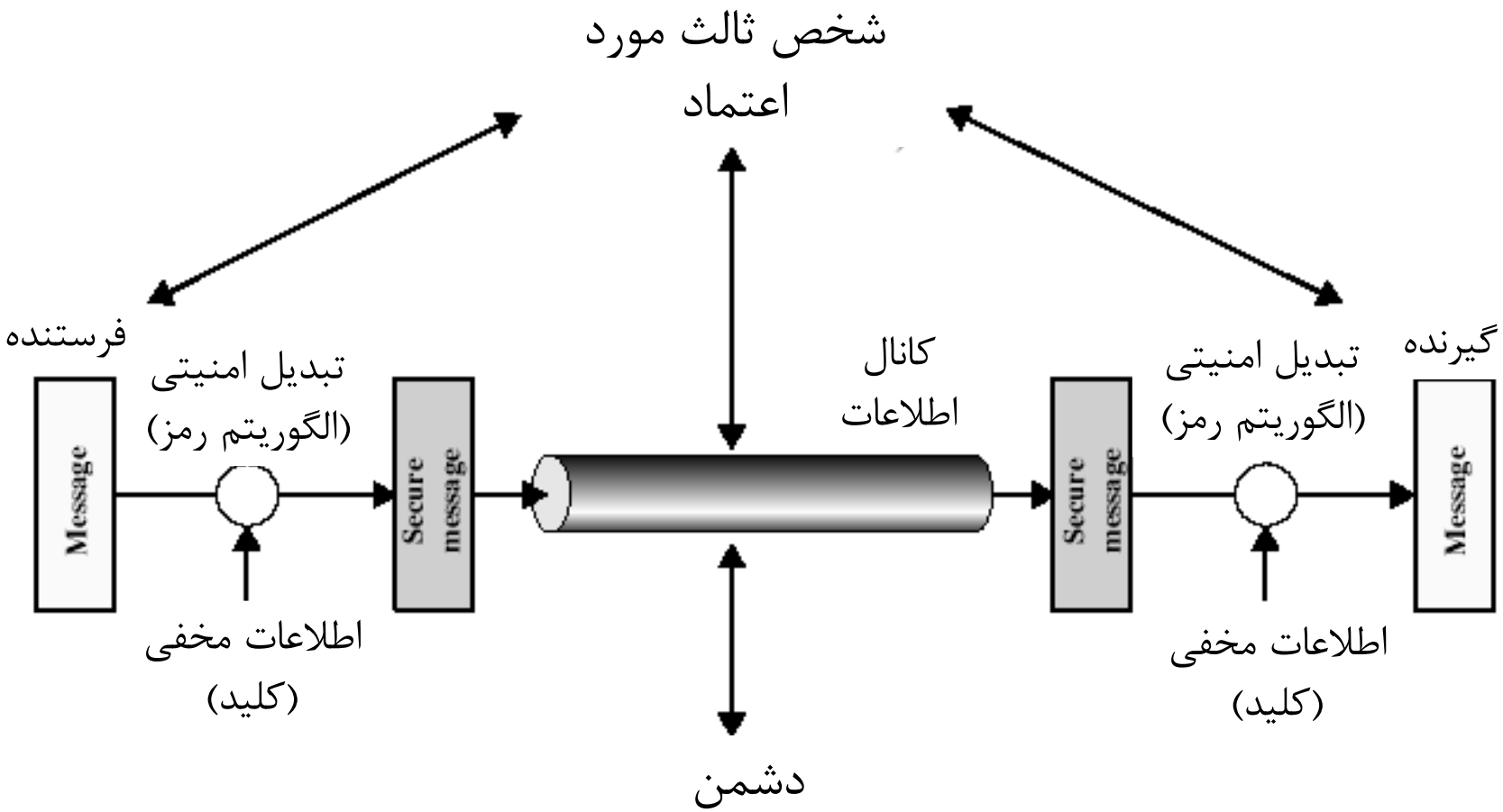
فهرست مطالب

- محتوا و جایگاه درس
- حوادث امنیتی و 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 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 (کلید) موردنیاز طرفین
  - استفاده از روش مناسب برای توزیع و توافق درباره اطلاعات مخفی (کلید)
  - طراحی یک پروتکل مناسب برای ارتباط طرفین و تضمین سرویس امنیتی