
بسم الله الرحمن الرحیم

امنیت شبکه

Ali Fanian

Fanian.iut.ac.ir

a.fanian@iut.ac.ir

فهرست مطالب

- کتاب مرجع
  - استفاده از مراجع مختلف از قبیل
    - INFORMATION SECURITY Principles and Practice, Second Edition by Mark Stamp
    - CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE 7th Edition by William Stallings.
    - Some papers and technical reports
- ارزیابی
  - میان ترم: ۴۰ درصد
  - پایان ترم : ۴۰ درصد
  - پروژه (ها)، تکالیف و پروژه ها : ۲۵
  - حضور فعال در کلاس : بیش از ۳ جلسه غیبت کسر نمره ۰.۲ در هر جلسه در صورت کسب نمره کمتر از ۱۸

سرفصل درس

- Introduction
- Attack Model
  - Reconnaissance
    - *Social engineering*
    - *Physical Security*
    - *Google Hacking*
    - *Organization's Website*
    - *Whois Databases*
    - *Domain Name System*
  - Scanning
    - *OS Fingerprint*
    - *Port Scan*
  - Gaining access
    - *Sniffing*
    - *Spoofing*
    - *Web Spoofing*
    - *Buffer Overflow*
    - *SQL Injection*
    - *Network attacks/DoS attacks*
    - *Malicious Logic attacks*
  - Maintaining access
    - Spywares & Trojan horses
    - Rootkits
    - Covert channels
  - Covering tracks and hiding

سرفصل درس

- WEB Security
  - A1: Injection (Injection flaws, such as SQL, OS, and LDAP injection)
  - A2: Broken Authentication and Session Management
  - A3: Cross-Site Scripting (XSS)
  - A4: Insecure Direct Object References
  - A5: Security Misconfiguration
  - A6: Sensitive Data Exposure
  - A7: Missing Function Level Access Control
  - A8: Cross-Site Request Forgery (CSRF)
  - A9: Using Components with Known Vulnerabilities
  - A10: Unvalidated Redirects and Forwards
- Firewall
  - Packet Filtering Router
  - Application Level Gateway
  - Circuit Level Gateway
  - Introducing iptables

سرفصل درس

- Intrusion detection Systems
  - Types of IDS
  - Attacks to the IDS
  - Snort Intrusion Detection System
  - Host-based Intrusion Detection
  - Introducing Snort
- PKI
  - Public Key Infrastructure (X509 PKI)
  - Digital Signature
  - Digital Certificate
  - Basic Component
- SSL
  - Introducing SSL Protocol
  - Some Attack against SSL
- VPN
  - Tunneling Concept
  - VPN Architecture
  - Remote access VPN
  - Site-to-Site VPN
  - Protocols (PPTP, L2TP, IPSec)

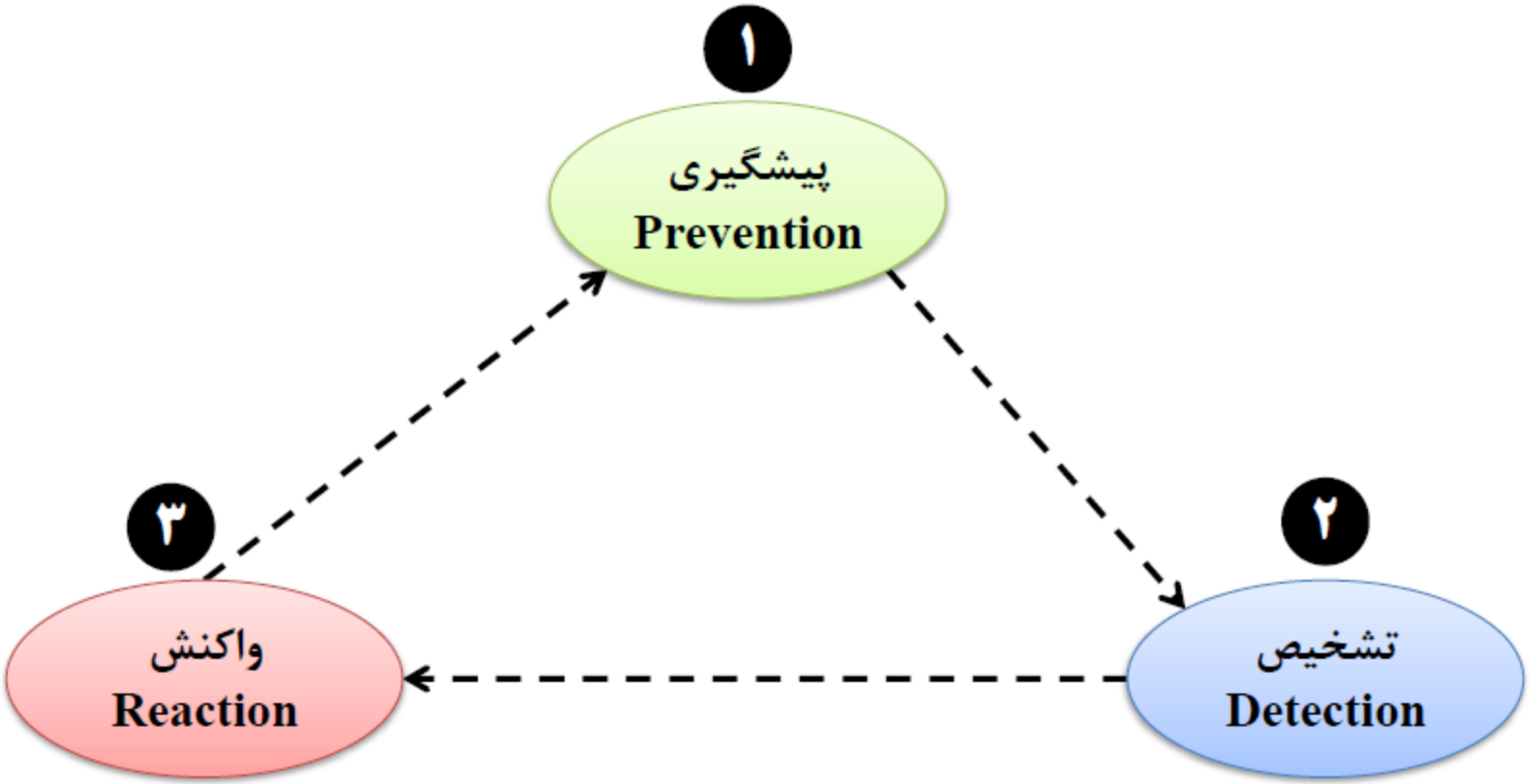
مقدمه: تعریف امنیت

- به طور غیر رسمی: امنیت عبارتست از حفاظت از آنچه برا ی ما مهم است
  - در برابر حملات عمدی
  - در برابر نفوذ غیر عمدی

اقدامات امنیتی

- پیشگیری (Prevention)
  - جلوگیری از خسارت
- تشخیص و ردیابی (Detection & Tracing)
  - میزان خسارت
  - هویت دشمن
  - چگونگی حمله (زمان، مکان، دلایل حمله، نقاط ضعف و ...)
- واکنش (Reaction)
  - ترمیم، بازیابی و جبران خسارات
  - جلوگیری از حملات مجدد

اقدامات امنیتی



امنیت اطلاعات گذشته و حال

امنیت اطلاعات سنتی

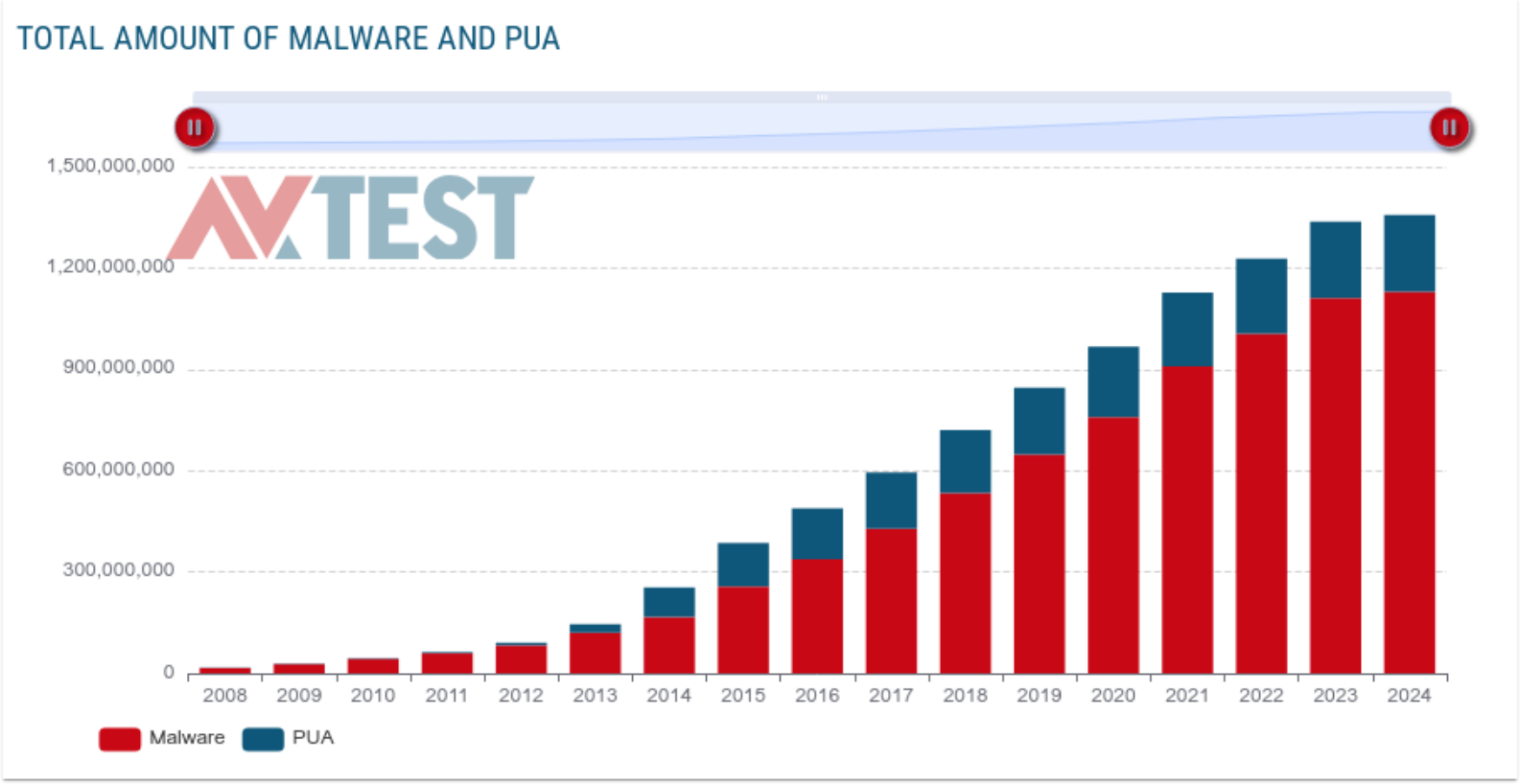
- نگهداری اطلاعات در قفسه‌های قفل‌دار
- نگهداری قفسه‌ها در مکان‌های امن
- استفاده از نگهبان
- استفاده از سیستم‌های الکترونیکی نظارت
- روشهای فیزیکی و مدیریتی

امنیت اطلاعات دنیای نوین

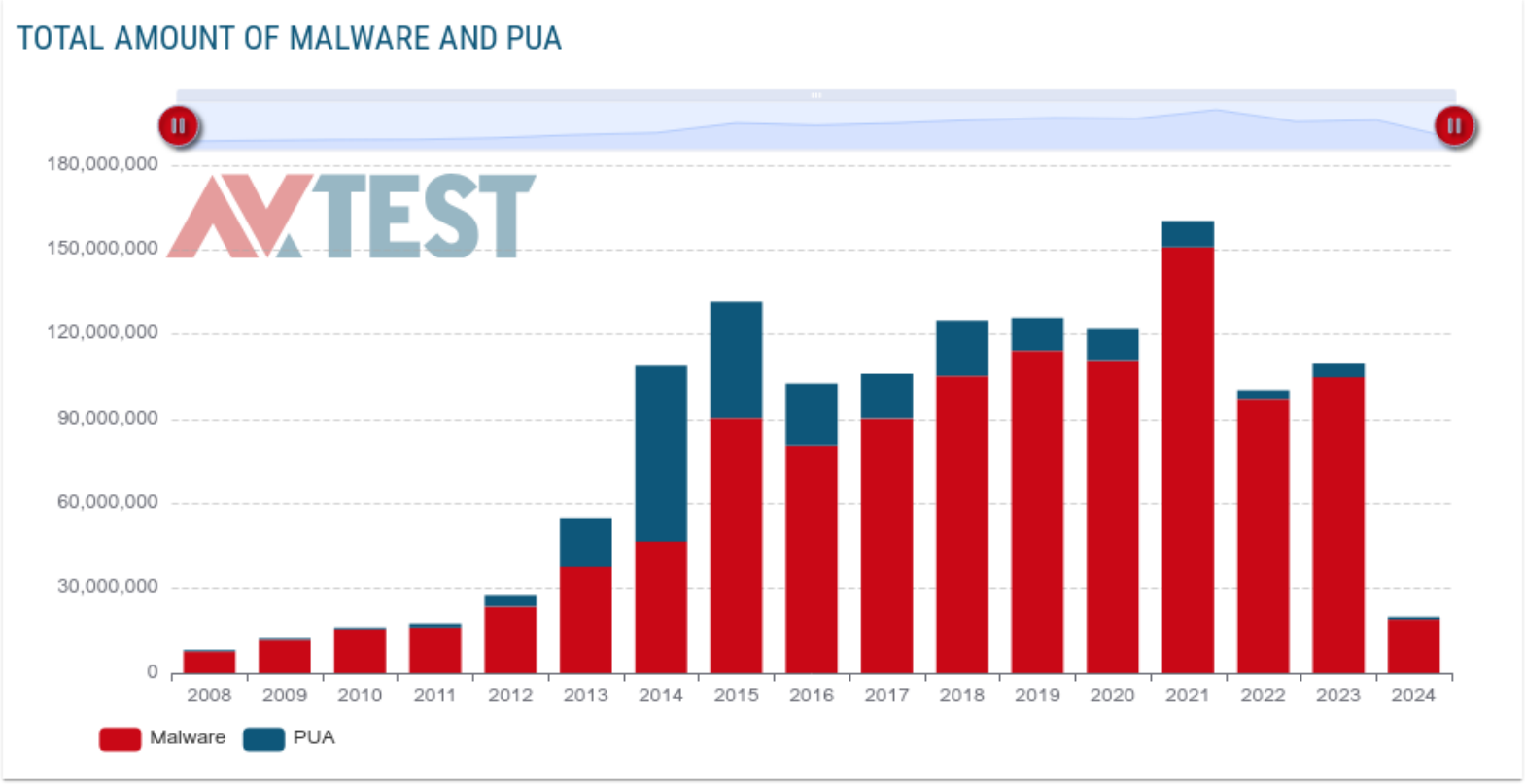
- نگهداری اطلاعات در کامپیوترها
- برقراری ارتباط شبکه‌ای بین کامپیوترها
- برقراری امنیت در کامپیوترها و شبکه‌ها

آمارگان کل بدافزار در سالهای مختلف

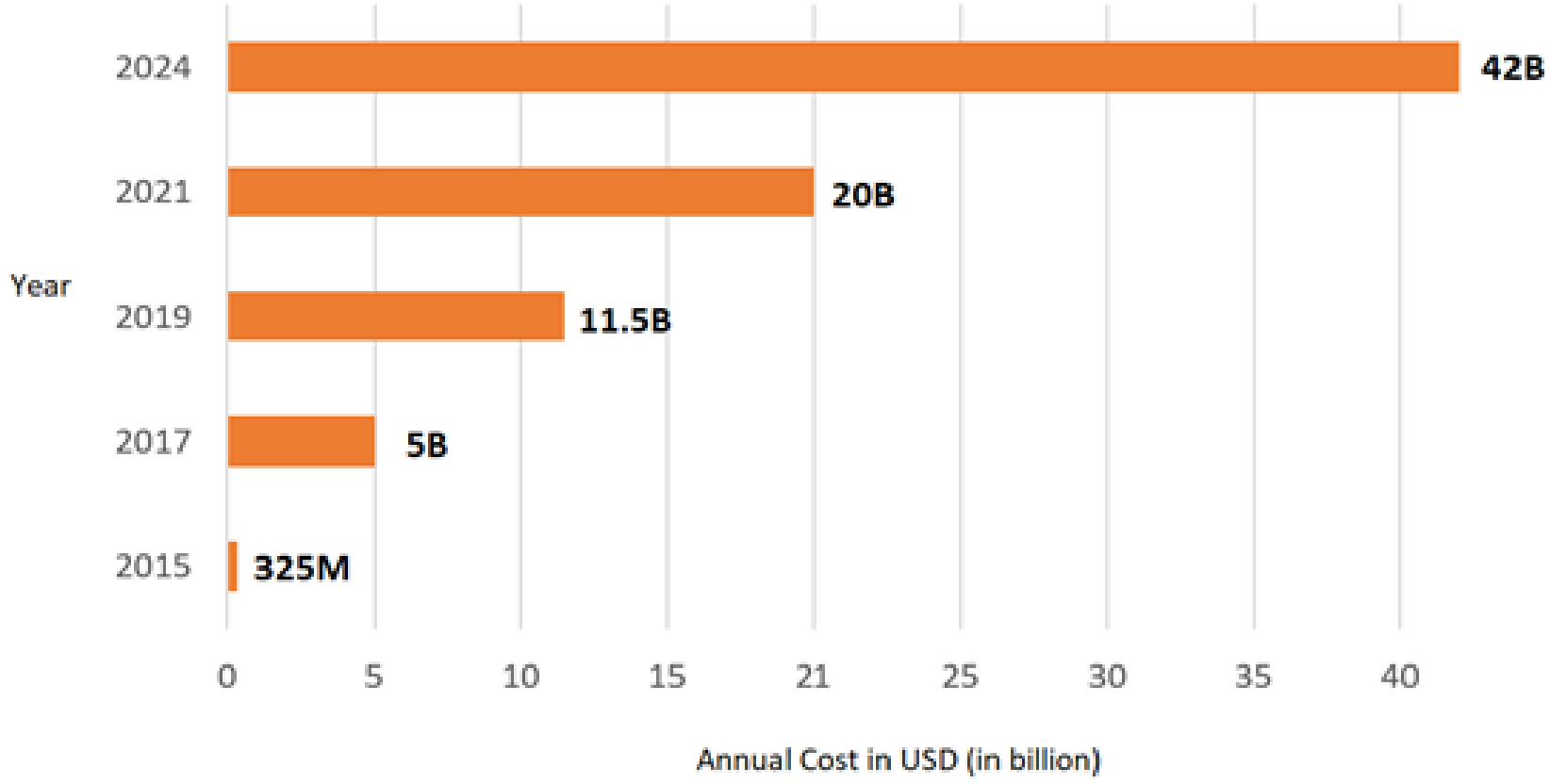
- تعداد کل بدافزار



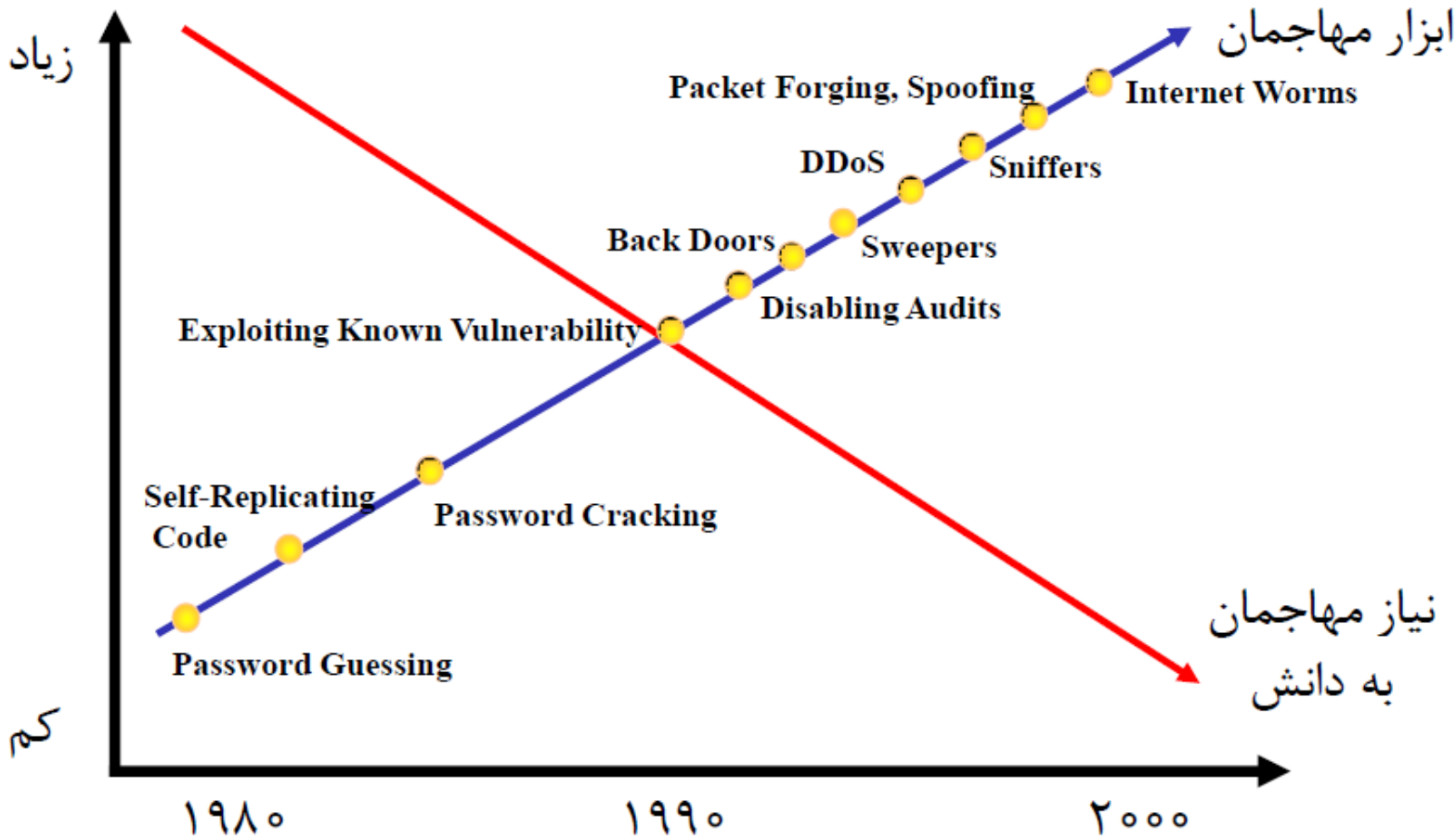
تعداد بدافزارهای جدید



ضررهای ناشی از یک نمونه بدافزار



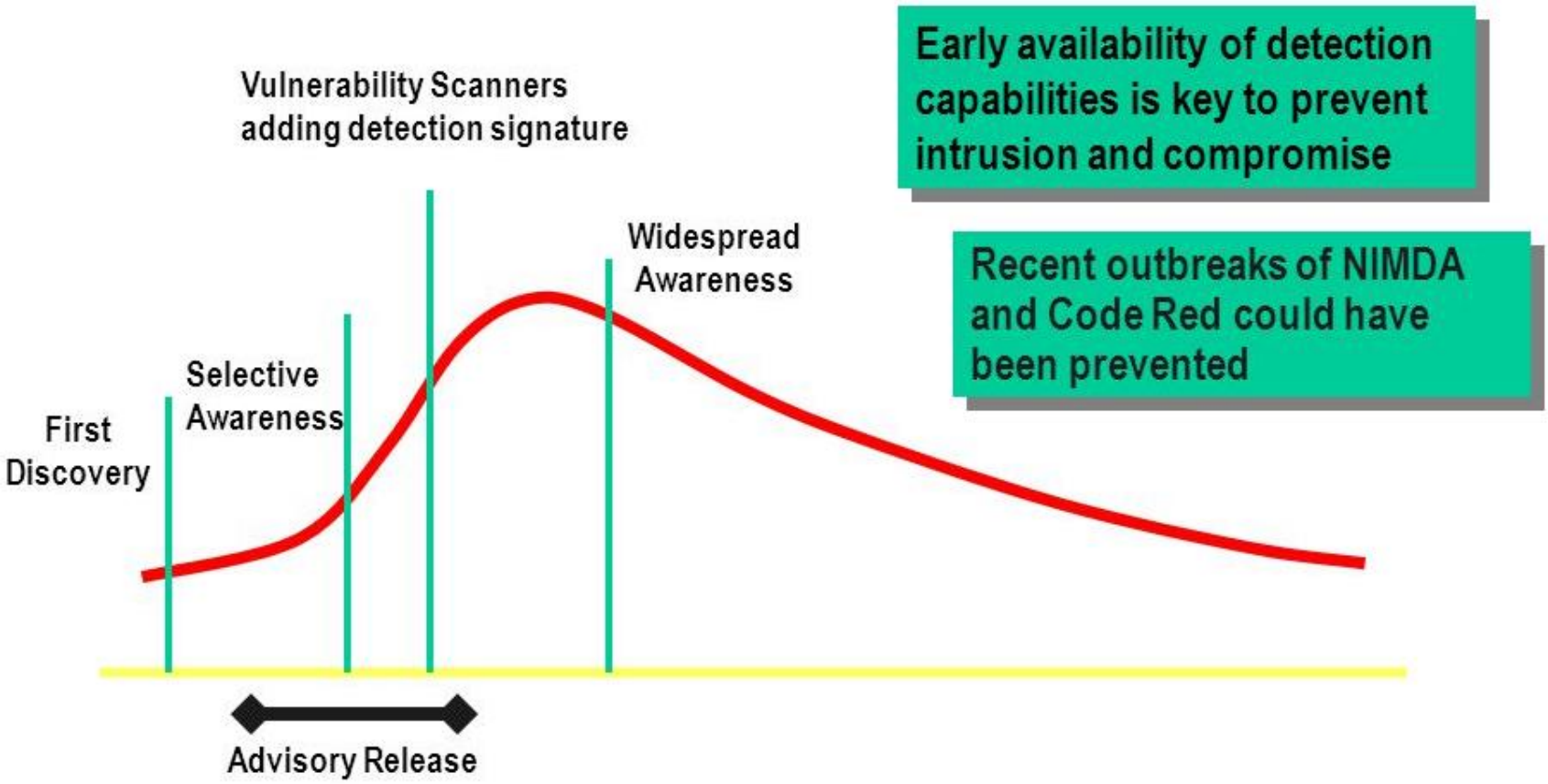
ابزار مهاجمان



نیازهای امنیتی: گذشته و حال

- از دو نمودار قبلی بخوبی پیداست:
  - تعداد حملات علیه امنیت اطلاعات به طور قابل ملاحظه ای افزایش یافته است.
- امروزه تدارک حمله با در اختیار بودن ابزارهای فراوان در دسترس به دانش زیادی احتیاج ندارد (بر خلاف گذشته).

چرخه آسیب پذیری



Early availability of detection capabilities is key to prevent intrusion and compromise

Recent outbreaks of NIMDA and Code Red could have been prevented

هزینه تجهیزات تهاجمی

- هزینه یک فروند بمب افکن stealth

1.5 $ to 2$ billion

- هزینه یک فروند جنگنده stealth

80 $ to 120$ million

- هزینه یک فروند موشک Cruise

1 $ to 2$ million

- هزینه یک سلاح سایبری

300 $ to 50.000 $

جنگ های سایبری

- جنگ عراق و آمریکا در کویت – جنگ اول خلیج فارس ۱۹۹۱
- ایجاد اختلال در سیستم ضد هوایی عراق
- توسط نیروی هوایی آمریکا با استفاده از ویروسی با نام AF/91

جنگ های سایبری (ادامه)

- حمله رژیم صهیونیستی به تاسیسات هسته ای ایران ۲۰۱۰ از طریق بدافزار Stuxnet
  - آلوده سازی سیستم های کنترل صنعتی و PLC ها
  - هدف: آلوده سازی سانتریفیوژهای نطنز

PLC زیمنس مدل S7-300

جنگ های سایبری (ادامه)

July 9,2021
سرویس‌های راه‌آهن

July 10, 2021
وزارت راه و شهرسازی

August 22, 2021
دوربین‌های امنیتی زندان اوین

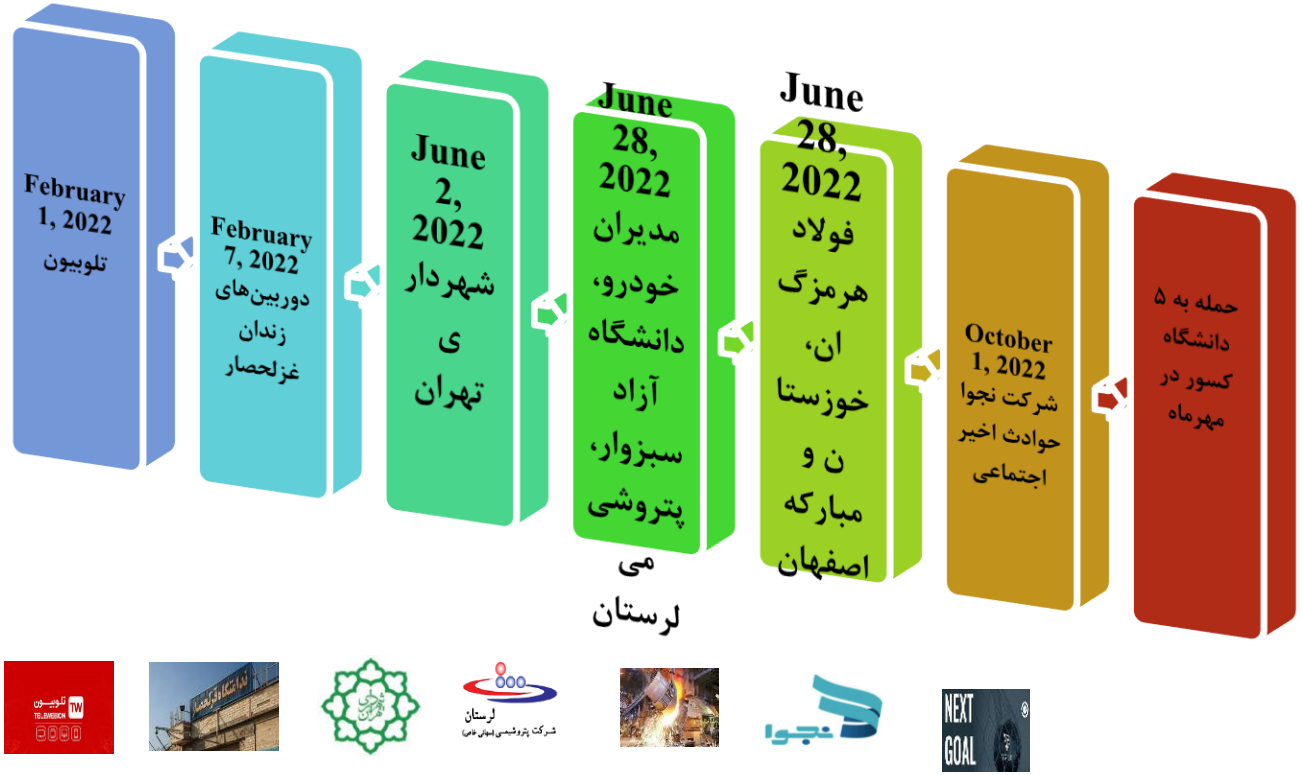
October 26, 2021
اختلال در جایگاه‌های سوخت

November 21, 2021
هواپیمایی ماهان

January 27, 2021
صدا و سیما

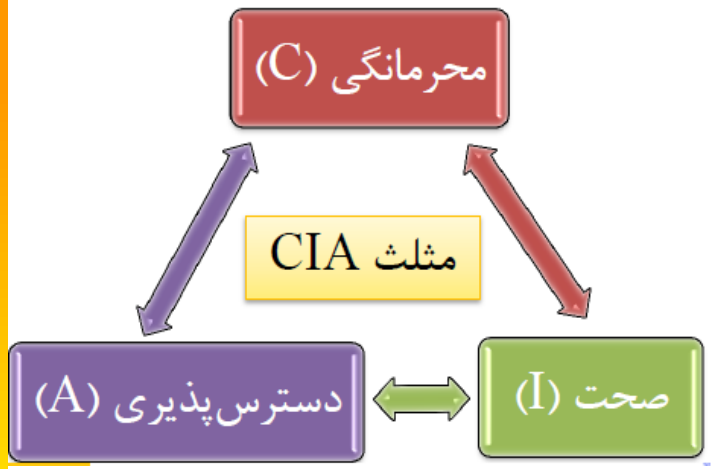



جنگ های سایبری (ادامه)



مبانی امنیت اطلاعات

- سه ویژگی اساسی: محرمانگی، صحت و دسترس پذیری



- محرمانگی Confidentiality
  - عدم افشای غیرمجاز داده ها
- صحت Integrity
  - عدم امکان دستکاری و/یا امکان کشف دستکاری داده ها توسط افراد یا نرم افزارهای غیرمجاز
- دسترس پذیری Availability
  - دسترسی به داده ها توسط افراد مجاز در مکان و زمان مجاز

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 سری ۲۷۰۰۰ (مشهور به ISMS)
- NIST IR 7298 (واژه‌نامه اصطلاحات اساسی امنیت اطلاعات)
- واژگان ENISA
- واژگان ISACA
- ...

محرمانگی

- محرمانگی داده (Data Confidentiality)
  - اطمینان از اینکه داده های محرمانه و خصوصی برای افراد غیرمجاز فاش نمی شوند.
  - اهداف
    - عدم افشا محتوا
    - عدم امکان تحلیل ترافیک
    - عدم نشت اطلاعات
    - عدم افشای نامها (Anonymity)
    - حفظ حریم خصوصی (Privacy)

محرمانگی

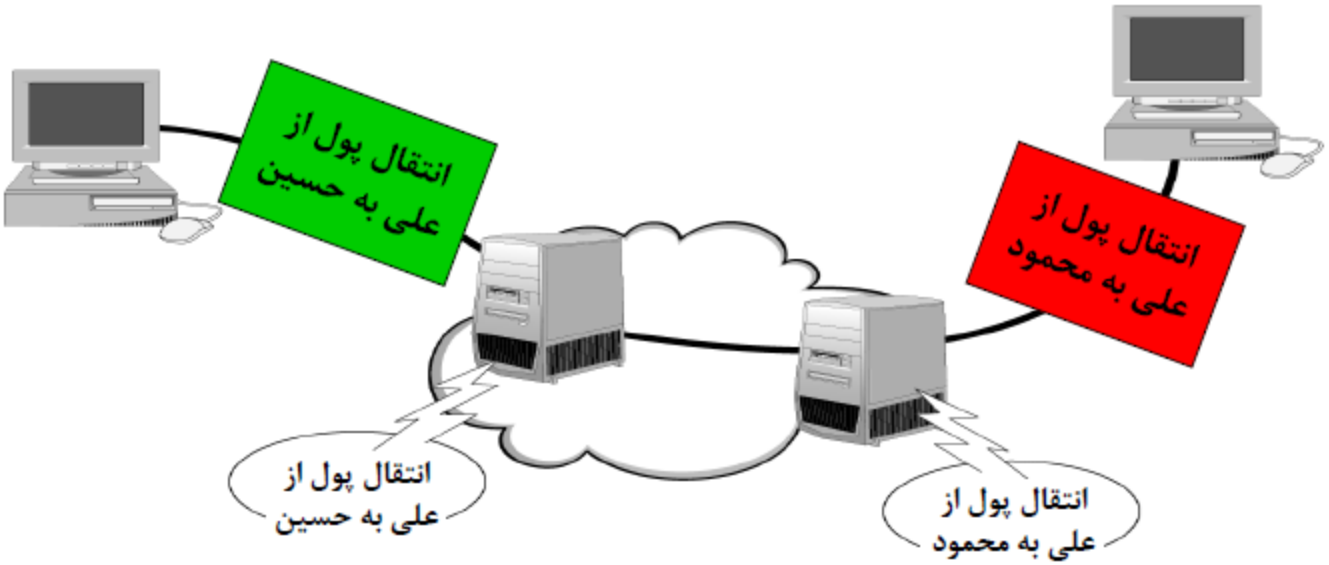
- ساز و کارهای متداول:
  - رمزنگاری
  - کنترل دسترسی

صحت

- صحت داده (Data Integrity)
  - اطمینان از اینکه داده ها و یا برنامه ها توسط افراد غیرمجاز تغییر نمی یابند و در صورت تغییر ما متوجه خواهیم شد.
- صحت منبع (Origin Integrity)
  - اطمینان از درستی و صحت منبع (فرستنده) اطلاعات.
  - اهداف
    - اصالت داده‌ها (عدم حذف, اضافه و تکرار)
    - اصالت مبدأ داده‌ها (Data Origin Authentication)
    - اصالت و حضور موجودیتها (On-line Entity Authentication)
    - انکارناپذیری (Non-Repudiation)

صحت

- ساز و کارهای متداول:
  - امضای دیجیتال
  - کد تصدیق هویت پیام
  - کنترل دسترسی

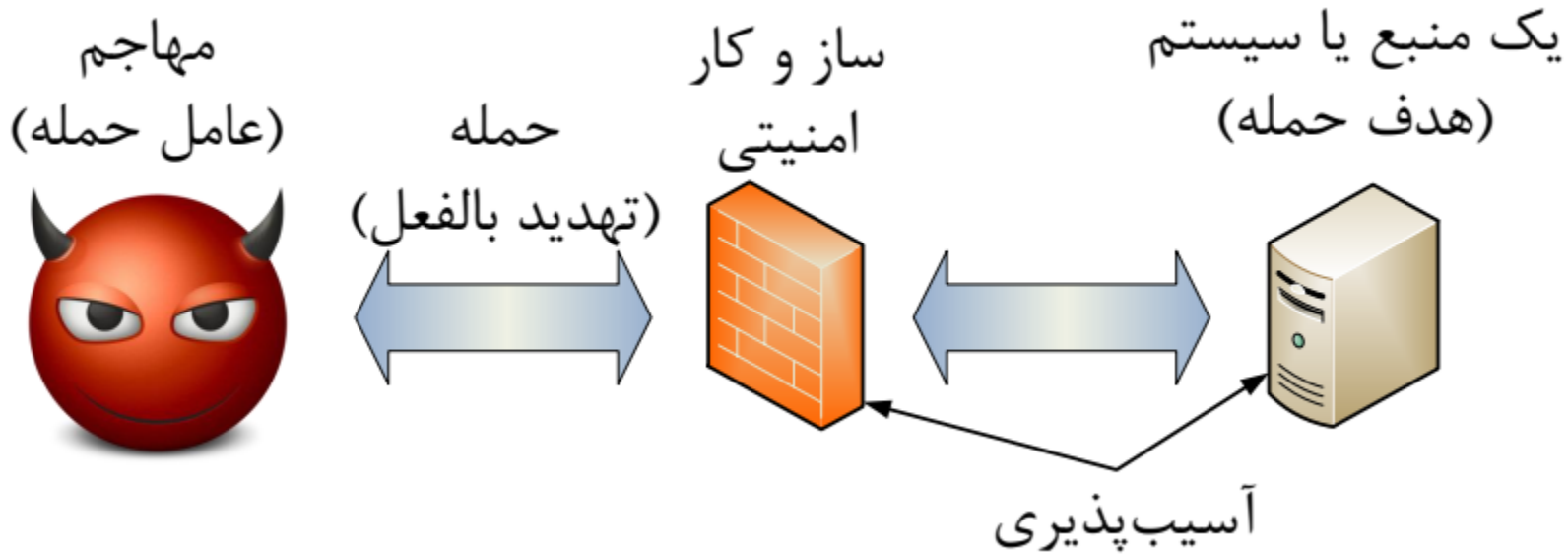


دسترس پذیری

- **تعریف:** دسترسی به داده ها و خدمت دهی به افراد مجاز در زمان و مکان مجاز

- **ساز و کارهای متداول:**
  - وجود پشتیبان
  - تکرار داده و خدمت
  - سیستم های پایش و توزیع بار
- اهداف
  - سهولت دسترسیهای مجاز : حل تقابل ذاتی امنیت و تسهیل ارتباطات
  - مقابله با حملات جلوگیری از ارائه سرویس (Denial of Service)

آسیب پذیری، تهدید، حمله و مهاجم



آسیب پذیری(Vulnerability)

- نقصان یا ضعف؛
- در طراحی، پیاده‌سازی، یا عملیات و مدیریت سیستم؛
- که با سوء استفاده از آن می‌توان سیاست امنیتی سیستم را نقض کرد.
- **مثال:** **CVE:** Common Vulnerabilities and Exposures
  - آسیب‌پذیری خونریزی قلبی (HeartBleed) در OpenSSL
  - آسیب‌پذیری سر ریز بافر (Buffer Overflow)

تهدید Threat

- امکان بالقوه برای نقض امنیت.
- متناظر با هر آسیب‌پذیری، (حداقل) یک تهدید وجود دارد.
- می‌تواند عمدی یا غیر عمدی باشد.

☜ **عمدی:** امکان نقض امنیت توسط یک موجودیت هوشمند (فرد یا سازمان)

☜ **غیر عمدی:** امکان خطای انسانی، عملکرد ناصحیح ابزار، وقایع طبیعی (زلزله، سیل، آتش سوزی، و ...)

حمله و مهاجم

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

مهاجم و رخنه گر

- 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

دشواری برقراری امنیت

- امنیت معمولاً قربانی افزایش کارایی و مقیاس‌پذیری 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.

دلایل ناامنی شبکه ها

- ضعف فناوری (تحلیل، طراحی، پیاده‌سازی)
  - پروتکل، سیستم عامل، تجهیزات
- ضعف تنظیمات
  - رهاکردن تنظیمات پیش‌فرض، گذرواژه‌های نامناسب، عدم استفاده از رمزنگاری، راه‌اندازی خدمات 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)

امن سازی

- گستره امنیت تمامی منابع سازمان است و نه تنها کارگزار اصلی.
- مسئله امنیت نیازمند نگرش مدیریتی است، نه صرفاً نگرش فنی.
- مهاجمین داخلی 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.

استاندارد X.800

- فراهم کننده یک چارچوب ستماتیک برای توصیف
  - حملات امنیتی
  - مکانیزم های امنیتی
  - سرویس های امنیتی

تعاریف در X.800

- حمله امنیتی : (Security Attack)
  - تلاش برای رخنه در یک سیستم
- مکانیزم امنیتی: (Security Mechanism)
  - روشهای پایه برای تشخیص, جلوگیری و بازیابی از حملات
    - رمز نگاری، امضای دیجیتال ، پروتکل های احراز اصالت و...
- سرویس امنیتی(Security Service)
  - سرویس های تضمین کننده امنیت با استفاده از مکانیزمهای بالا
    - محرمانگی، انکار ناپذیری، صحت و..

انواع حملات از نظر تاثیر

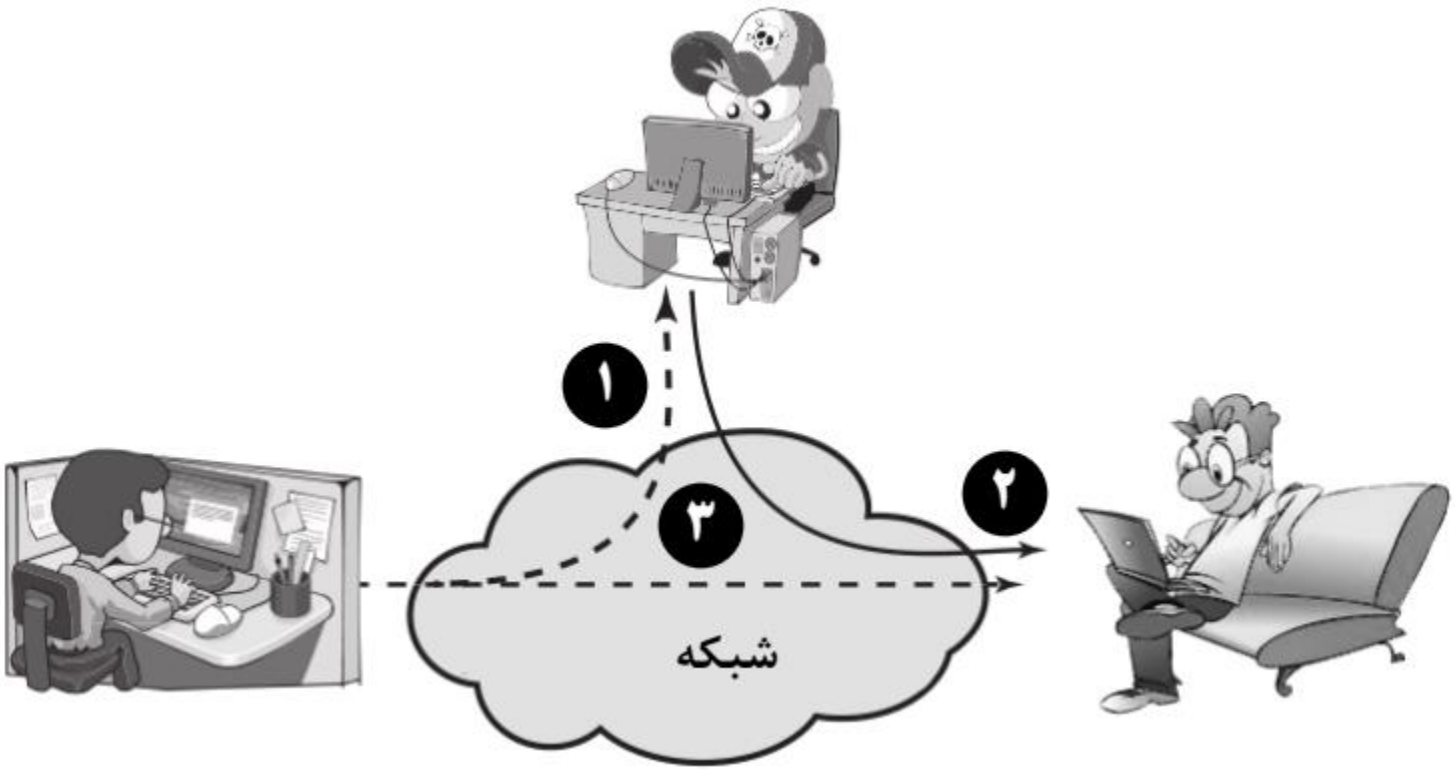
حملات فعال (Active)

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

حملات منفعل (Passive)

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

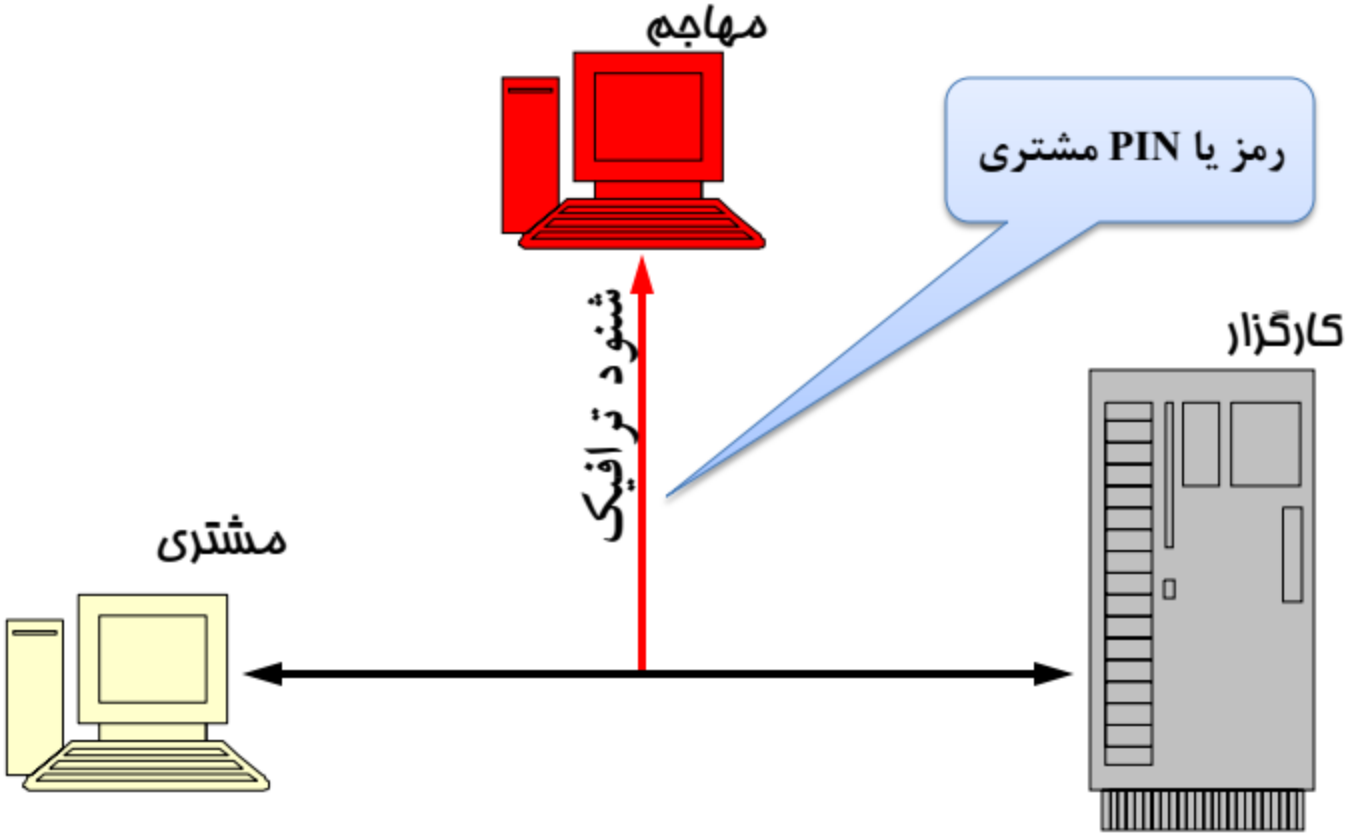
حملات فعال



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

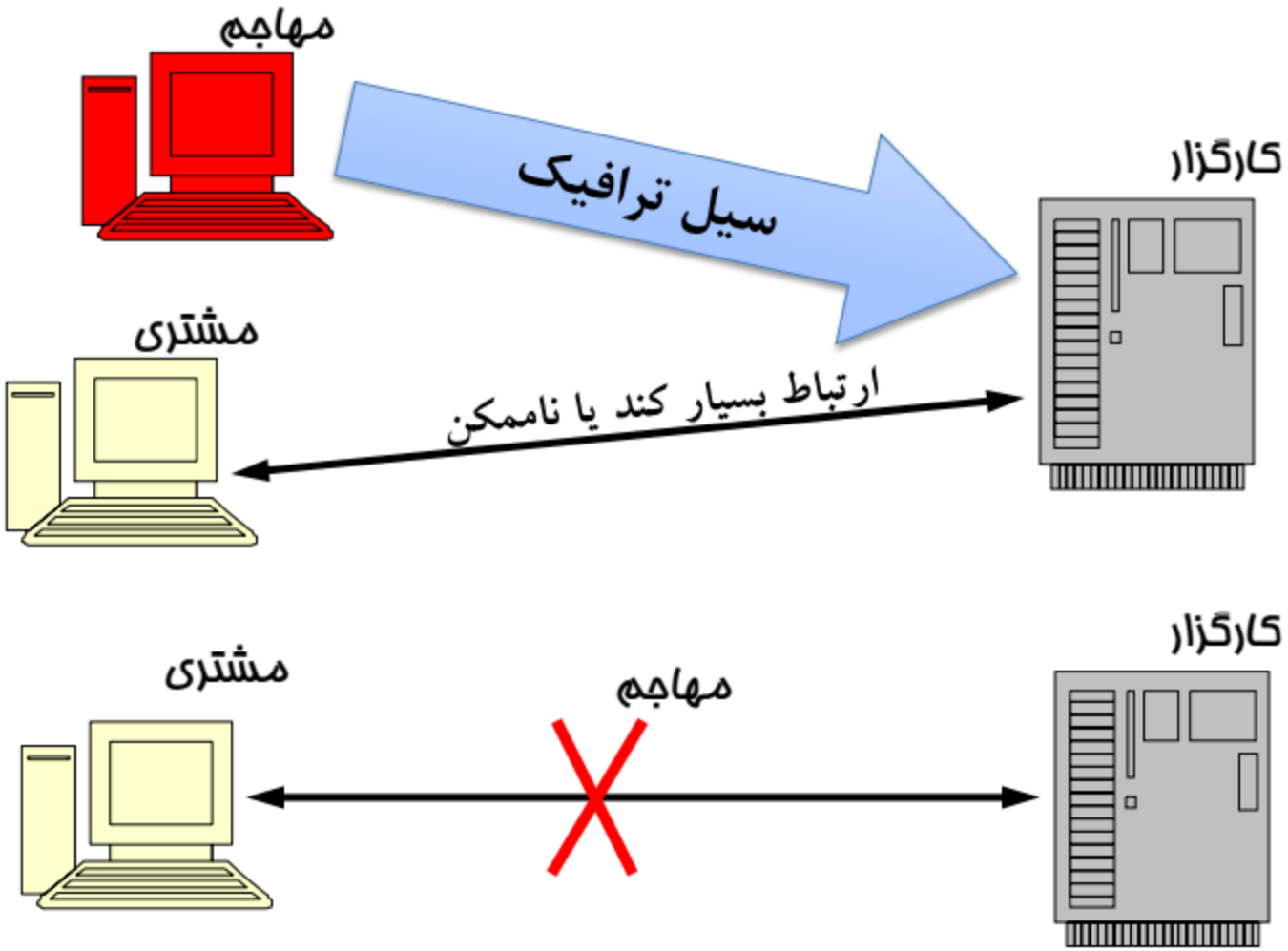
حمله شنود یا استراق سمع



حمله منع خدمت یا وقفه

- **هدف:** نقض دسترس‌پذیری
- **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 ویا خدمات

حمله منع خدمت یا وقفه

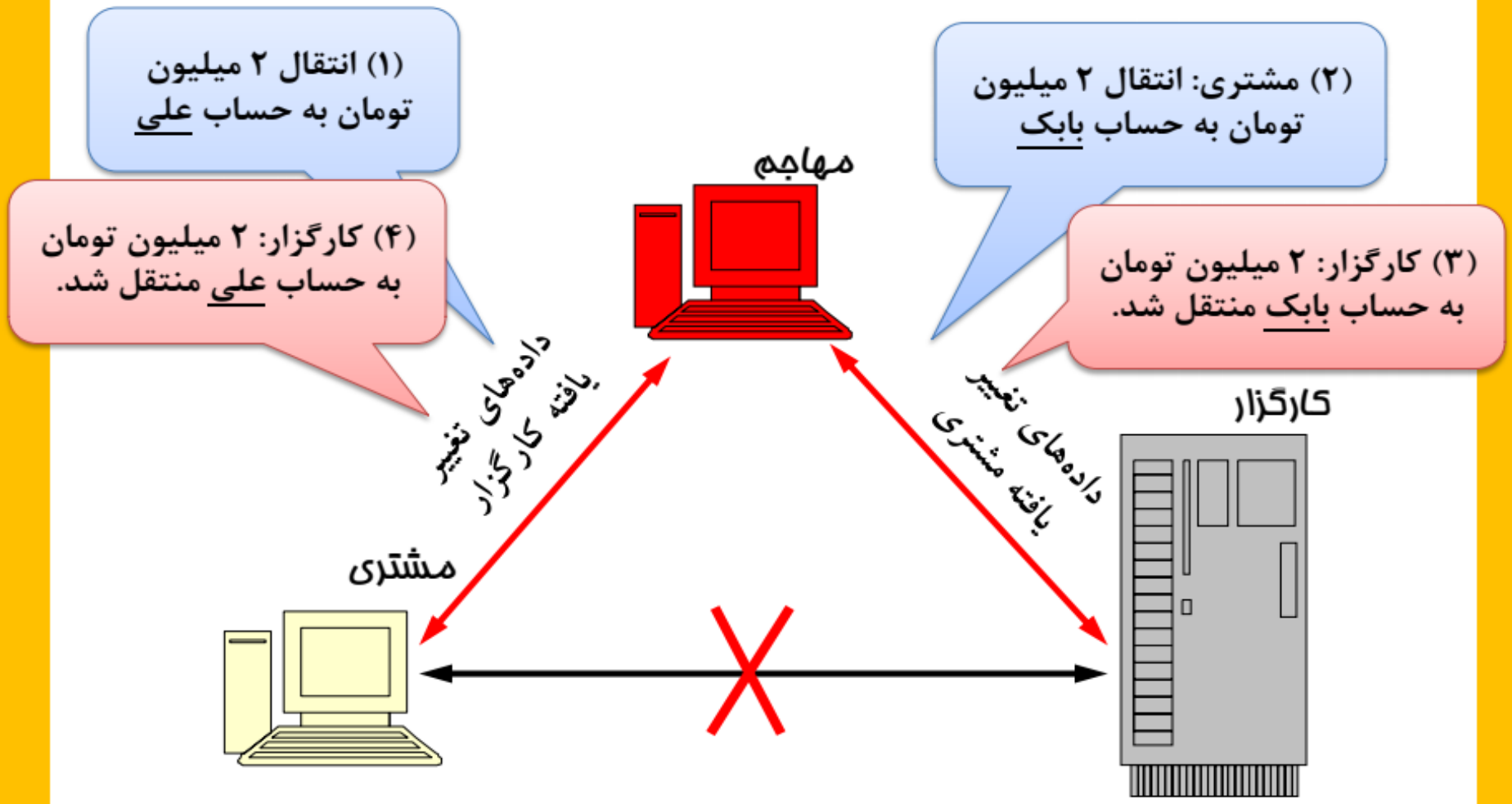


حمله تغییر یا دستکاری داده ها

- **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 داده ها

- حمله مرد میانی (Man in the Middle)

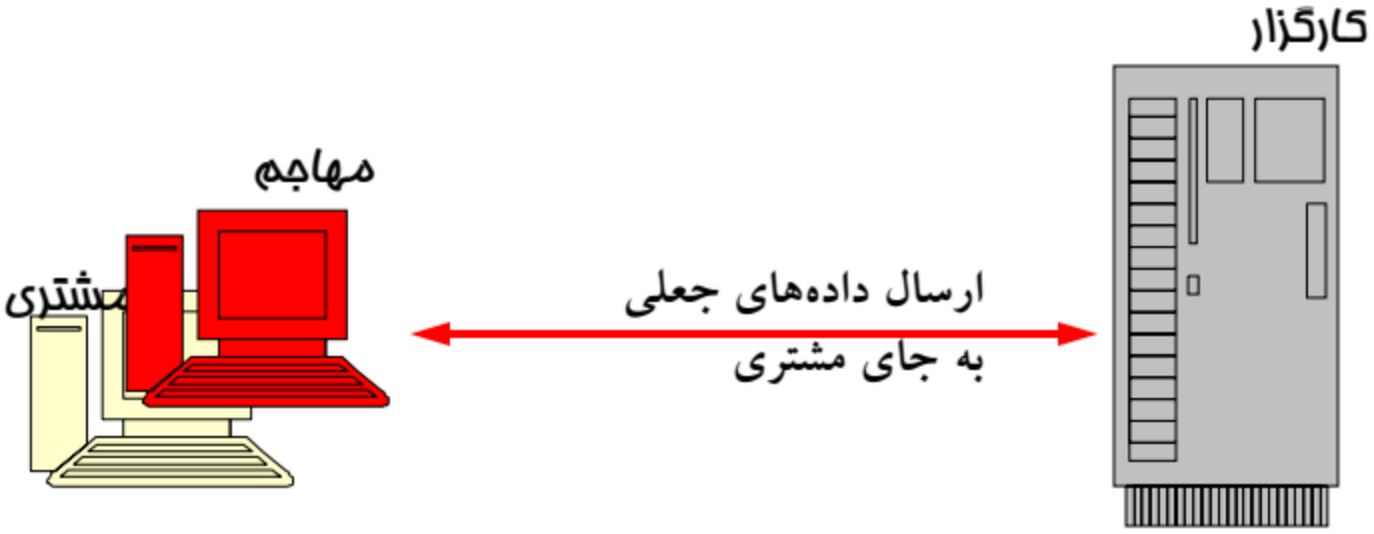


حمله جعل هویت

- **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 ساز و کار تصدیق هویت و کنترل صحت

حمله جعل هویت

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



مکانیزمهای امنیتی

- Encipherment
- Digital Signature
- Access Control
- Data Integrity
- Authentication Exchange
- Traffic Padding
- Routing Control
- Notarization

سرویسهای امنیتی

- سرویس امنیتی : فرایندی ارائه شده توسط یک سیستم برای محافظت از منابع
- X.800 سرویس های امنیتی را به ۵ دسته و ۱٤ سرویس تقسیم بندی می کند
  - احراز اصالت
  - کنترل دسترسی
  - محرمانگی
  - صحت داده
  - انکار ناپذیری

- احراز اصالت : اطمینان از ماهیت طرفین ارتباط
- Peer Entity Authentication
  - منظور از Peer دو سیستم متفاوت که یک پروتکل مشابه را پیاده سازی کرده اند
  - هویت طرفین را در شروع ارتباط و در طول آن تضمین می کند
- Data-Origin Authentication
  - تایید هویت منبع ارسال داده
  - در مقابل حمله تکرار آسیب پذیر است

- کنترل دسترسی (Access Control): اعمال محدودیت در دسترسی به سیستم ها و منابع از طریق شبکه
- محرمانگی : اطمینان از افشای غیر مجاز
  - Connection Confidentiality : محافظت از تمامی اطلاعات کاربر در ارتباط
  - Connectionless Confidentiality : محافظت از تمامی اطلاعات کاربر در یک بلوک داده
  - Selective-Field Confidentiality : محافظت از برخی فیلدهای اطلاعاتی در طول یک ارتباط یا یک بلوک داده
  - Traffic-Flow Confidentiality : محافظت از اطلاعاتی که با مشاهده جریان اطلاعات بدست می آید

- صحت داده : اطمینان از عدم تغییر غیر مجاز داده
  - Connection Integrity with Recovery : سرویس صحت بر روی تمامی اطلاعات کاربر و تشخیص تمامی عوامل برهم زننده صحت با تلاش برای بازیابی
  - Connection Integrity without Recovery : مشابه قبلی بدون عملیات بازیابی
  - Selective-Field Connection Integrity
  - Connectionless Integrity
  - Selective-Field Connectionless Integrity
- انکار ناپذیری
  - Nonrepudiation, Origin
  - Nonrepudiation, Destination

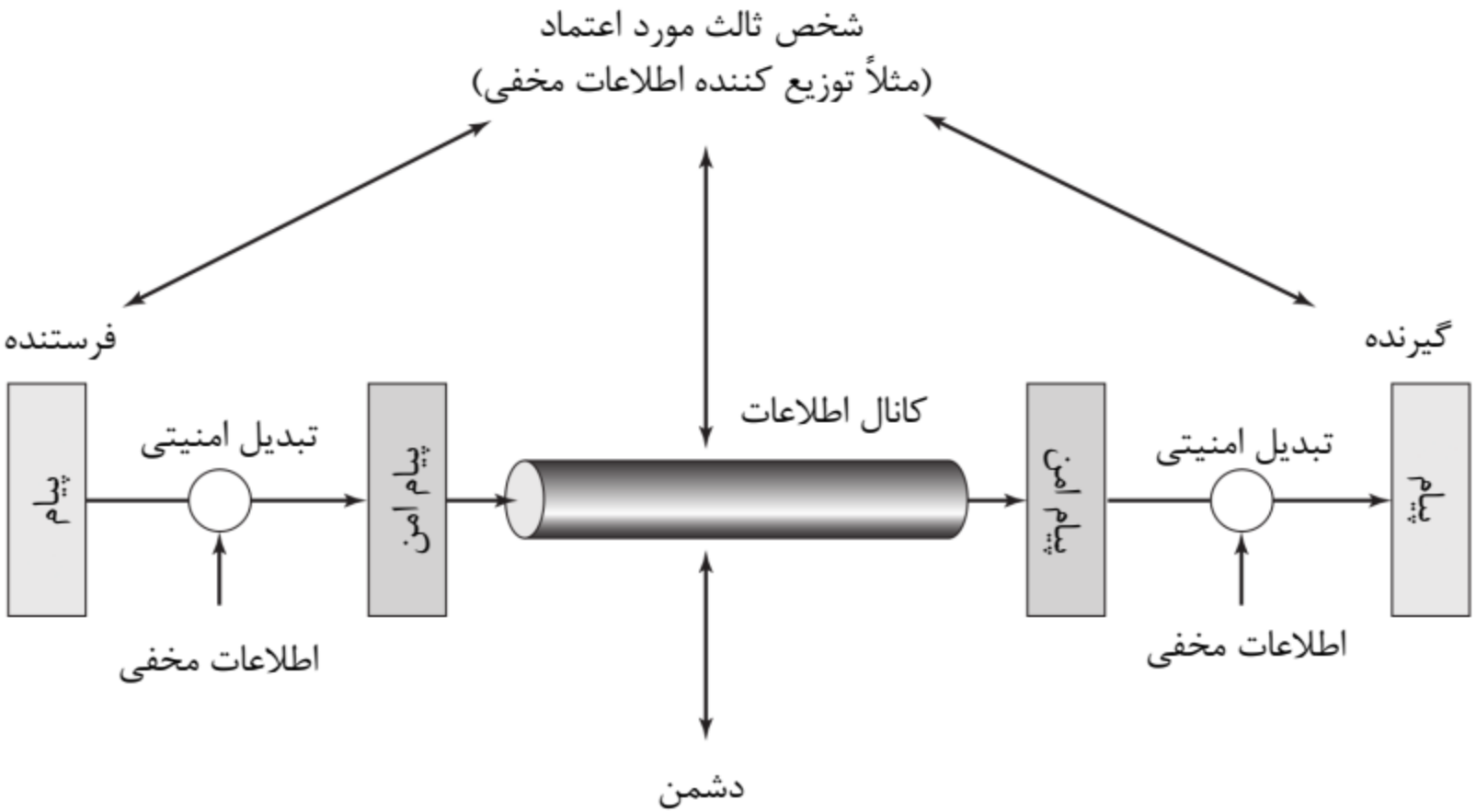
ارتباط بین خدمات و سرویس های امنیتی

Service	Encipherment	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			

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 تأمین خدمات محرمانگی، صحت، تصدیق هویت، و ...
- روشهای مورد استفاده عموما 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.

مدل کلی در یک ارتباط امن



تضمین خدمت امنیتی

- مدل فوق نشان می‌دهد که برای فراهم آمدن یک خدمت امنیتی 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 تضمین خدمت امنیتی