



# یادداشتن و الامان

امنیت داده و شبکه

## مفاهیم و تعاریف اولیه

مرتضی امینی - سیدمهدی خرازی

نیمسال اول ۱۴۰۳-۱۴۰۴



# فهرست مطالب

- ضرورت تامین امنیت
- معرفی درس
- مفاهیم اولیه
- انواع و ماهیت حملات متداول



# فهرست مطالب

ضرورت تامین امنیت

معرفی درس

مفاهیم اولیه

انواع و ماهیت حملات متداول



# امنیت چیست؟

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

- در برابر حملات عمدی ■
- در برابر نفوذ غیرعمدی ■





# نیازهای امنیتی: گذشته و حال

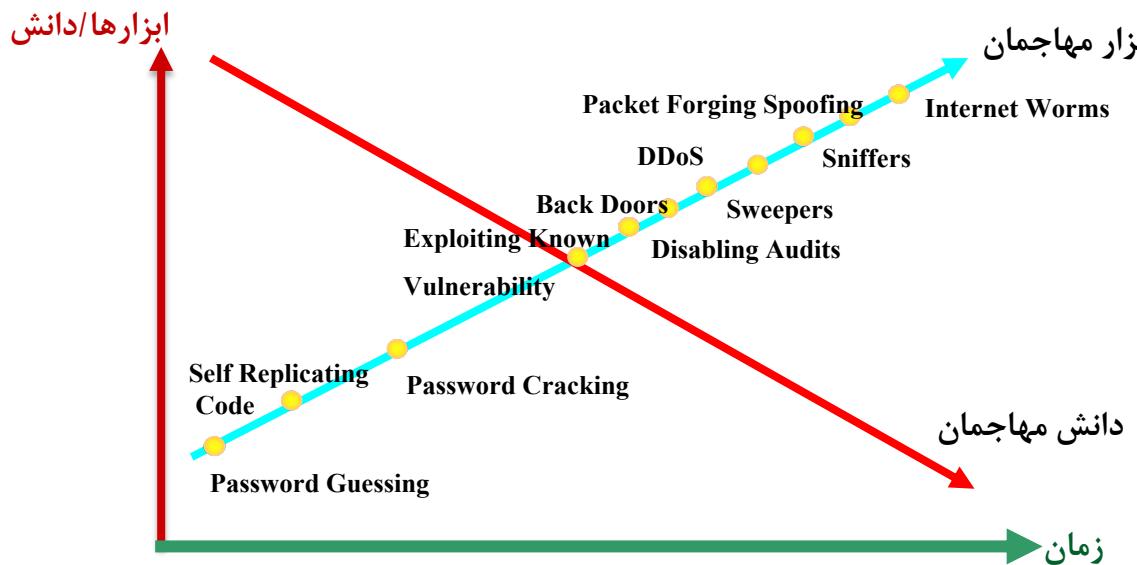
□ در گذشته، امنیت با حضور فیزیکی و نظارتی تامین می‌شد،

## ولی

□ امروزه از ابزارهای خودکار و مکانیزم‌های کامپیوتري و بعضا هوشمند برای حفاظت از داده‌ها استفاده می‌شود.

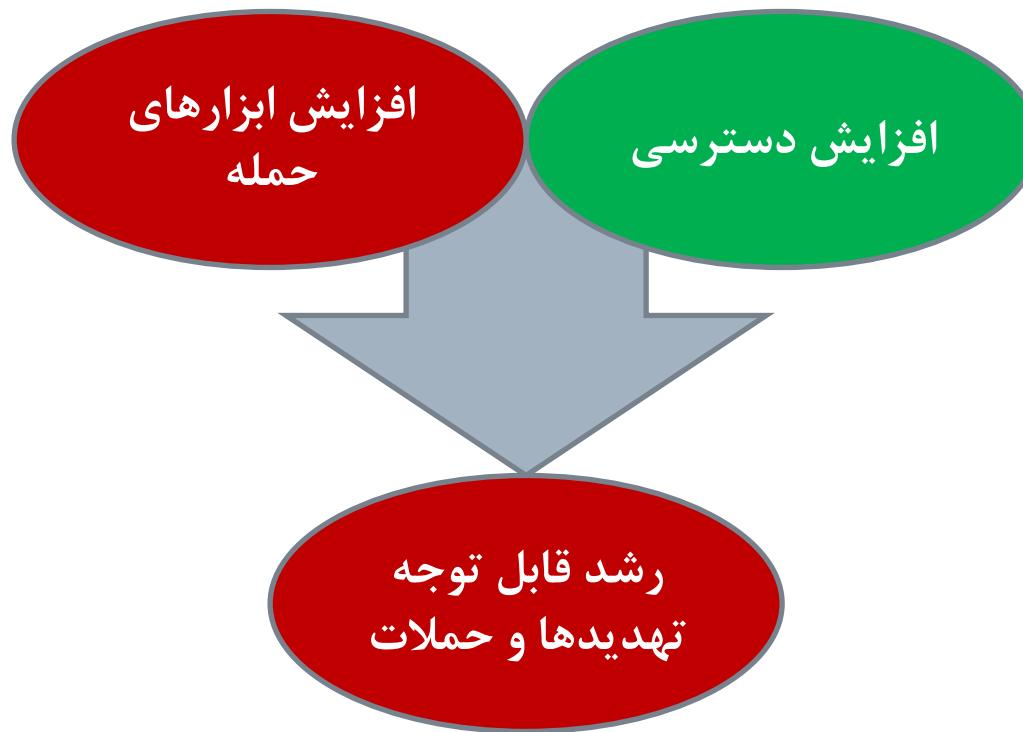
# نیازهای امنیتی: گذشته و حال

- 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



نیازمند اقدامات امنیتی در سطح سیستم، شبکه، برنامه‌های کاربردی و ...



# اهداف حملات

## □ اهداف اقتصادی

- ضربه زدن به رقبا
- کسب اطلاعات رقبا
- کسب درآمد از طرق نامشروع

## □ اهداف شخصی

- انتقام‌جویی (خصوصیت‌های شخصی یا نارضایتی کاری)
- اثبات و بروز توانمندی‌ها

## □ اهداف سیاسی

- تضعیف دولتها (با حمله سایبری به زیرساخت‌های حساس و حیاتی)



# آسیب‌پذیری‌ها عامل اصلی حملات

## Top 50 Products By Total Number Of "Distinct" Vulnerabilities

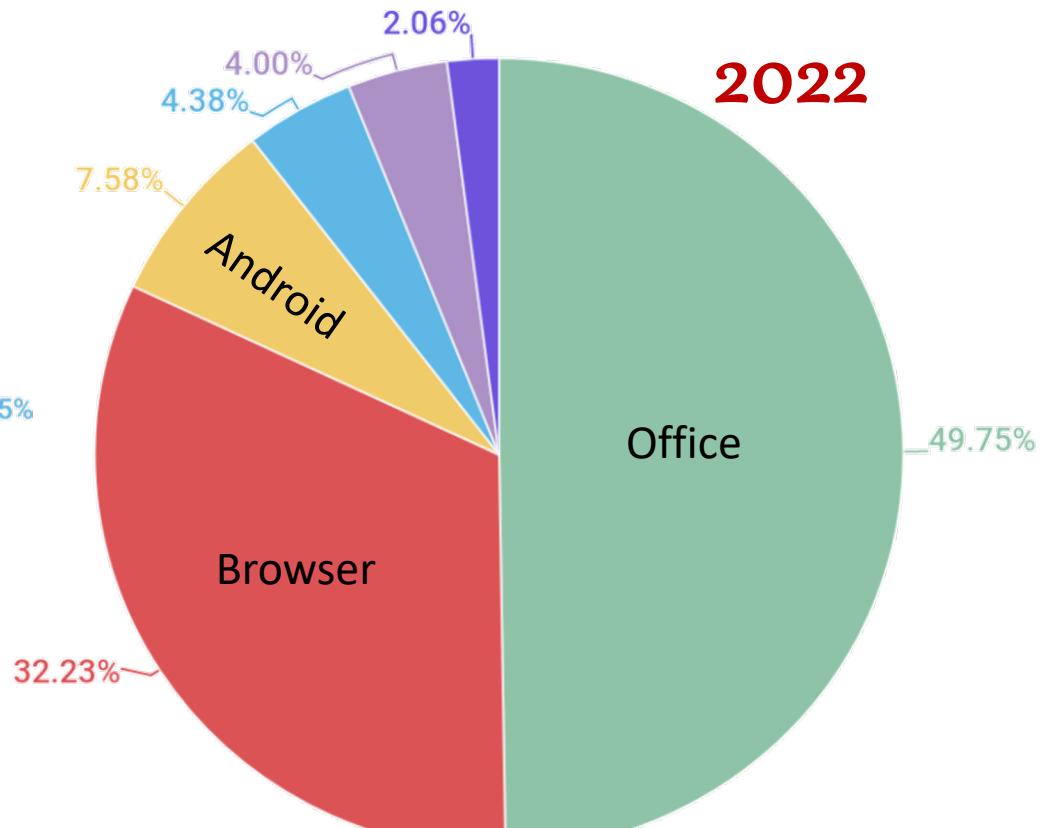
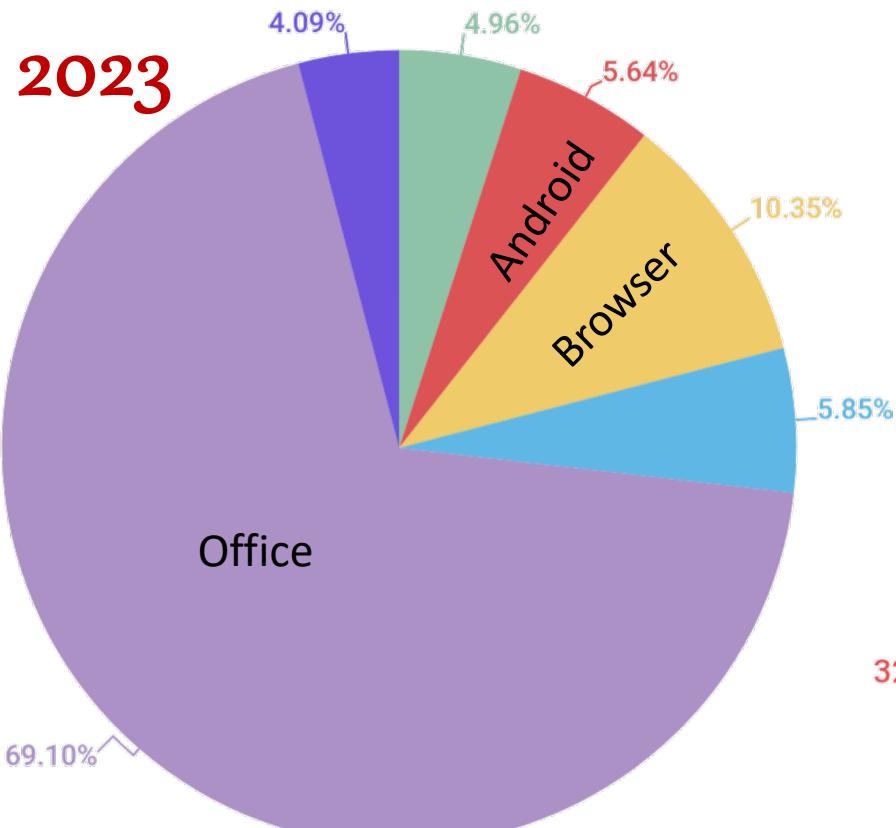
Go to year: 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 All Time Leaders

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	8796
2	Android	Google	OS	7163
3	Linux Kernel	Linux	OS	5329
4	Fedora	Fedoraproject	OS	5116
5	Ubuntu Linux	Canonical	OS	4093
6	Windows Server 2016	Microsoft	OS	3661
7	Chrome	Google	Application	3497
8	Iphone Os	Apple	OS	3402
9	Windows Server 2019	Microsoft	OS	3217
10	Mac Os X	Apple	OS	3206
11	Windows Server 2012	Microsoft	OS	3057
12	Windows 10	Microsoft	OS	3032
13	Windows Server 2008	Microsoft	OS	2966
14	Firefox	Mozilla	Application	2665
15	Windows 7	Microsoft	OS	2370
16	Windows 8.1	Microsoft	OS	2217
17	Windows Rt 8.1	Microsoft	OS	2017

منبع: <https://www.cvedetails.com/top-50-products.php>



# بهره کشی از آسیب‌پذیری‌ها در نرم‌افزارها



منبع: Kaspersky Security Bulletin. Statistics



# ZERODIUM Payouts for Desktops/Servers\*

<https://zerodium.com/program.html>

Windows	RCE: Remote Code Execution
macOS	LPE: Local Privilege Escalation
Linux/BSD	SBX: Sandbox Escape or Bypass
Any OS	VME: Virtual Machine Escape

ZERODIUM Payouts for Desktops/Servers*									
https://zerodium.com/program.html									
Up to \$1,000,000									
Up to \$500,000									
Up to \$250,000									
Up to \$200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE  Win/Linux			4.002 Sendmail RCE  Linux	4.003 Postfix RCE  Linux	4.004 Dovecot RCE  Linux	4.005 Exim RCE  Linux	2.005 nginx RCE  Linux
Up to \$100,000		3.002 Safari RCE+LPE  Mac	3.003 Edge RCE+LPE  Win	3.004 Firefox RCE+LPE  Win	5.003 Word/Excel RCE  Win	7.001 WordPress RCE  Linux	7.002 cPanel/WHM RCE  Linux	7.003 Plesk RCE  Linux	7.004 Webmin RCE  Linux
Up to \$80,000	6.002 VMware WS VME  Win/Linux					5.004 Adobe PDF RCE+SBX  Win	5.005 WinRAR RCE  Win	5.006 7-Zip RCE  Win	6.003 Windows LPE/SBX  Win
Up to \$50,000	6.004 USB LPE  Win/Mac	8.001 Antivirus RCE  Win			5.007 WinZip RCE  Win	5.008 tar RCE  Linux	6.005 macOS LPE/SBX  Mac	6.006 Linux LPE  Unix	6.007 BSD LPE  BSD
Up to \$10,000	9.001 Routers RCE	8.002 Antivirus LPE  Win	7.005 phpBB RCE	7.006 vBulletin RCE	7.007 MyBB RCE	7.008 Joomla RCE	7.009 Drupal RCE	7.010 Roundcube RCE	7.011 Horde RCE  Linux

*\* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

2019/01 ©zerodium.com



## ZERODIUM Payouts for Mobiles\*

<https://zerodium.com/program.html>

FCP: Full Chain with Persistence  
RCE: Remote Code Execution  
LPE: Local Privilege Escalation  
SBX: Sandbox Escape or Bypass

IOS  
Android  
Any OS

Up to \$2,500,000									
Up to \$2,000,000									
Up to \$1,500,000									
Up to \$1,000,000									
Up to \$500,000	3.001 Persistence IOS	2.005 WeChat RCE+LPE IOS/Android	2.006 iMessage RCE+LPE IOS	2.007 FB Messenger RCE+LPE IOS/Android	2.008 Signal RCE+LPE IOS/Android	2.009 Telegram RCE+LPE IOS/Android	2.010 Email App RCE+LPE IOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE IOS
Up to \$200,000	5.001 Baseband RCE+LPE IOS/Android	6.001 LPE to Kernel/Root IOS/Android	2.011 Media Files RCE+LPE IOS/Android	2.012 Documents RCE+LPE IOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari IOS	4.006 Safari RCE w/o SBX IOS	
Up to \$100,000	7.001 Code Signing Bypass IOS/Android	5.002 WiFi RCE IOS/Android	5.003 RCE via MitM IOS/Android	6.002 LPE to System Android	8.001 Information Disclosure IOS/Android	8.002 [k]ASLR Bypass IOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass IOS	9.003 Touch ID Bypass IOS

\* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

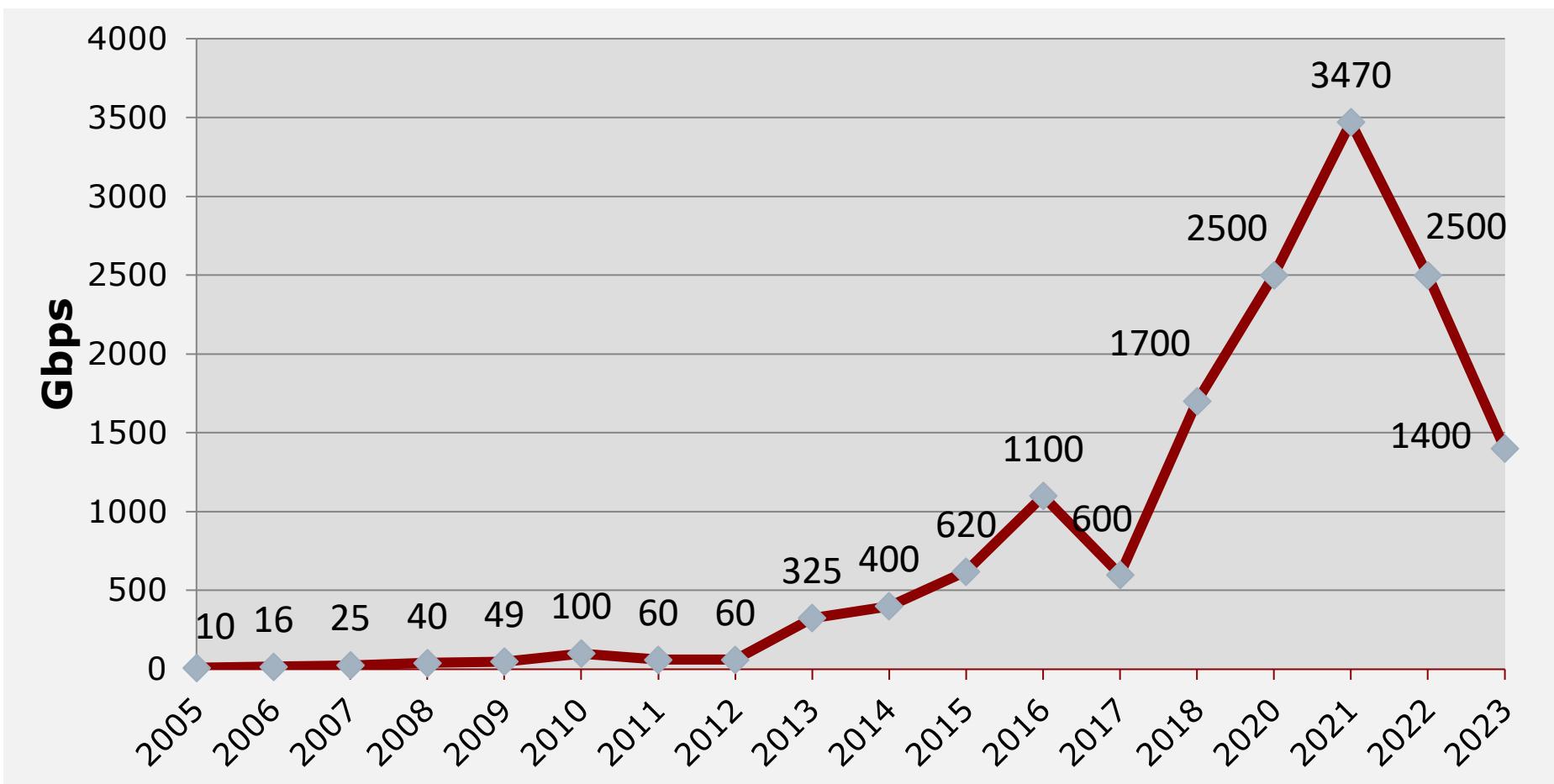
2019/09 © zerodium.com

دانشگاه صنعتی اسلامی  
دانشگاه صنعتی اسلامی



# رشد حملات منع سرویس

بر اساس گزارش Clouflare , Microsoft Stormwall .NETSCOUT





# فروش سرویس اجرای حملات منع سرویس

**\$23.99**

1 month

1 Month Gold

Time per boot 2400 sec

Concurrents 1

Total network 220Gbps

Tools Included

Support 24/7

Buy with Paypal



**bitcoin**

**\$34.99**

1 month

1 Month Diamond

Time per boot 3600 sec

Concurrents 2

Total network 220Gbps

Tools Included

Support 24/7

Buy with Paypal



**bitcoin**

**\$44.99**

10 years

Lifetime Bronze

Time per boot 600 sec

Concurrents 2

Total network 220Gbps

Tools Included

Support 24/7

Buy with Paypal



**bitcoin**

<https://www.imperva.com/learn/ddos/booters-stressers-ddosers>



# حملات سایبری (۱)

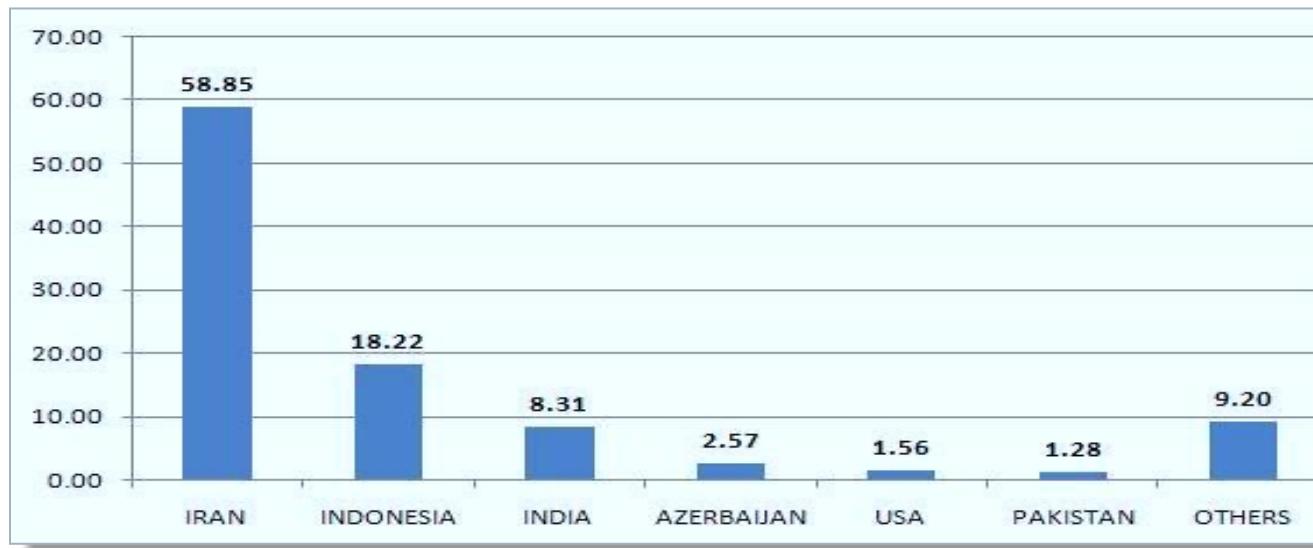
## □ جنگ عراق و آمریکا در کویت - جنگ اول خلیج فارس (۱۹۹۱)

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



# حملات سایبری (۲)

- حمله اسرائیل به تاسیسات هسته‌ای ایران (۲۰۱۰)
  - از طریق بدافزار Stuxnet (از طریق پمپ آب آلوده به بدافزار)
  - آلوده‌سازی سیستم‌های کنترل صنعتی و PLC‌ها
  - **هدف:** از کار انداختن سانتریفیوژهای نطنز و اختلال در برنامه هسته‌ای





# حملات 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
  - سیستمها مورد نفوذ:
    - سیستمها کمیته ملی دموکراتها
    - سیستمها ستاب انتخاباتی کنگره دموکراتها
    - پست الکترونیکی آقای پودستا رئیس ستاب انتخاباتی خانم کلینتون



# حملات 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:

□ ۱۸ هزار سازمان و آژانس آمریکایی

□ وزارت‌خانه‌های خزانه‌داری، دادگستری، بازرگانی، خارجه، دفاع، امنیت داخله آمریکا

□ رئیس شرکت مایکروسافت (برد اسمیت) آن را بزرگ‌ترین و پیچیده‌ترین حمله سایبری عنوان کرد.



# حملات سایبری (۷)

## □ حمله به شرکت خط لوله Colonial (۲۰۲۱)

- **هدف:** جمع‌آوری اطلاعات و باجگیری
- این بدافزار منجر به اختلال در انتقال محصولات نفتی از جمله بنزین و سوخت هواپیما شد.

■ **شیوه حمله:** انتشار باجافزار در سطح سیستم‌های کنترل خط لوله شرکت

■ **حمله‌کننده:** گروه DarkSide

■ درخواست ۷۵ بیت‌کوین (معادل ۴/۴ میلیون دلار) باج بابت بازیابی اطلاعات



# حملات سایبری (۸)

## □ حمله به وزارت دفاع و بانک‌های اوکراین (۲۰۲۲)

- حمله به وبسایت وزارت دفاع و یکی از بزرگترین بانک‌های اوکراین
- حمله در اوج بحران روسیه در مواجهه با غرب در خصوص اوکراین
- شیوه حمله: ایجاد ترافیک سنگین برای حمله منع خدمت توزیع شده
- حمله کننده: به احتمال زیاد گروههای روسی

# حملات سایبری (۹)

- حمله به سامانه هوشمند سوخت ایران (۲۰۲۱ و ۲۰۲۳)
- حمله به سامانه سوخت و از کاراندازی جایگاه‌های سوخت
- شیوه حمله: آلودگی به بدافزار از طریق آسیب‌پذیری شبکه پرداخت
- حمله کننده: گروه هکری گنجشک درندہ



# حملات سایبری (۱۰)

## □ تهدید یا حمله مانای پیشرفته (APT)

- هدف: حمله سازمان یافته و هدفمند توسط مهاجمین با سطح مهارت بالا علیه کشورها و سازمانها

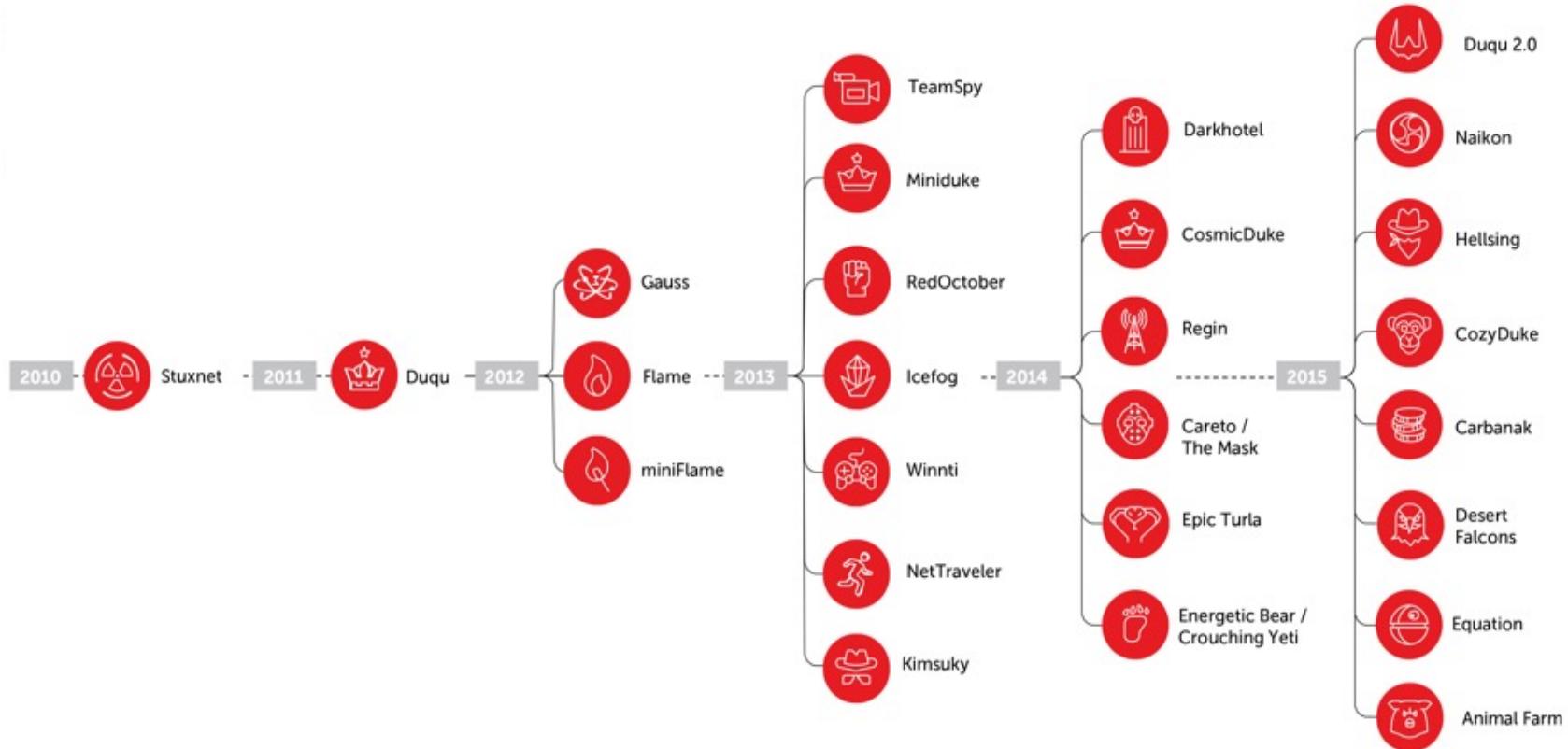




# حملات سایبری (۱۱)

## □ تهدید یا حمله مانای پیشرفته (APT)

KASPERSKY





# اقتصاد امنیت

□ امنیت اساساً یک مسئله اقتصادی است: هزینه در مقابل سود

## مدافعان:

□ ارزش دارایی چقدر است؟ / چه مقدار برای امنیت می‌توانید هزینه نمایید؟

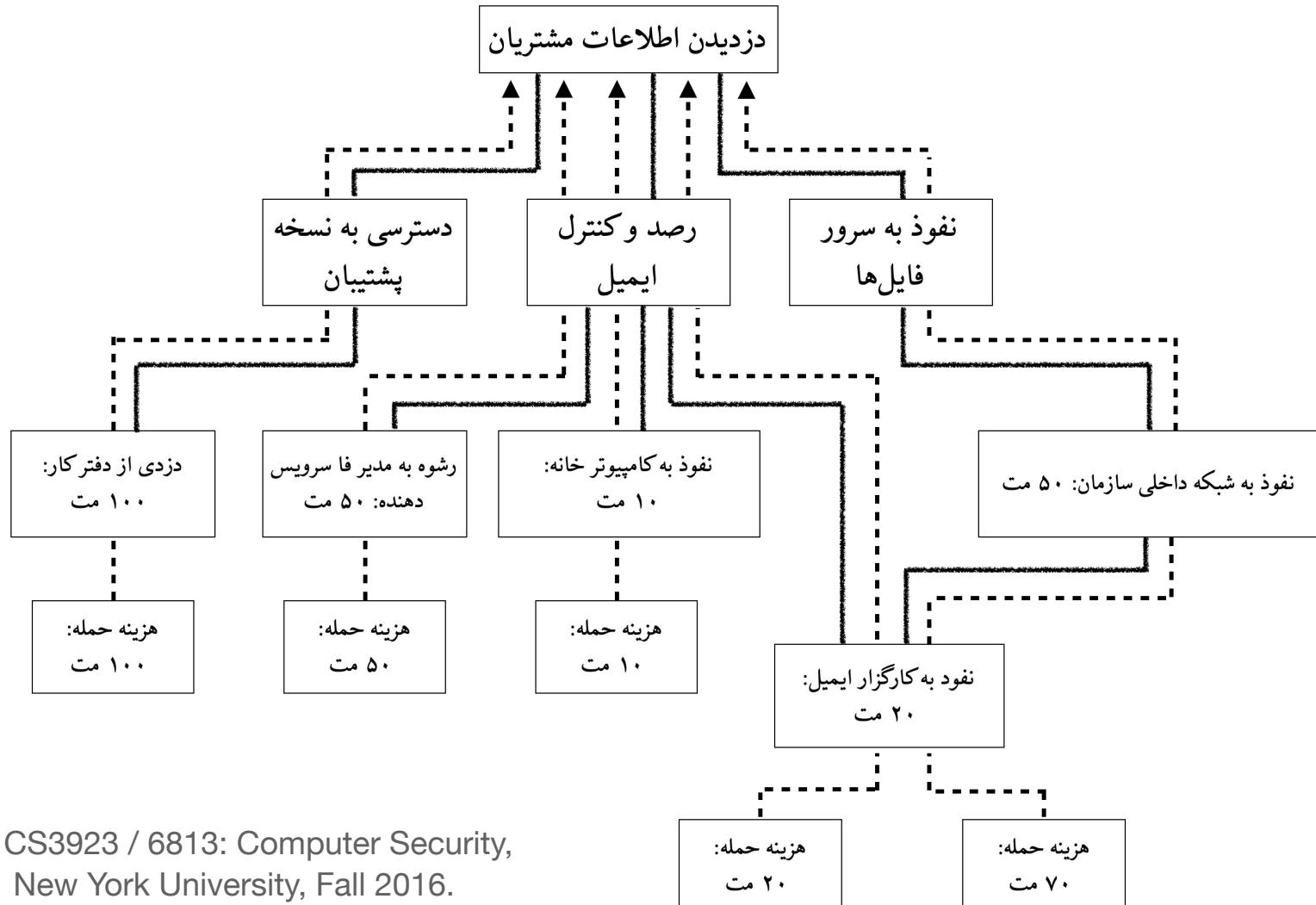
## حمله‌کنندگان:

□ چقدر بهره می‌برید؟ / چقدر می‌توانید هزینه کنید؟

□ خود پرداز بانکی که فقط اسکناس‌های ۱۰۰,۰۰۰ تومانی دارد خیلی جذاب‌تر از خودپردازی است که فقط اسکناس‌های ۵۰,۰۰۰ تومانی دارد.



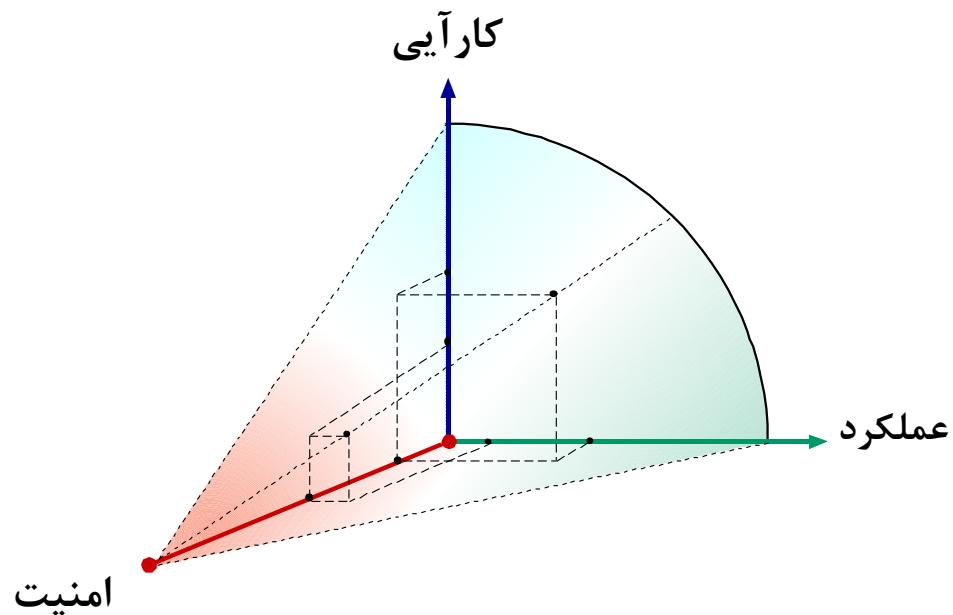
# تحلیل اقتصادی بر اساس درخت حمله



منبع: CS3923 / 6813: Computer Security,  
New York University, Fall 2016.

# استراتژی امنیت

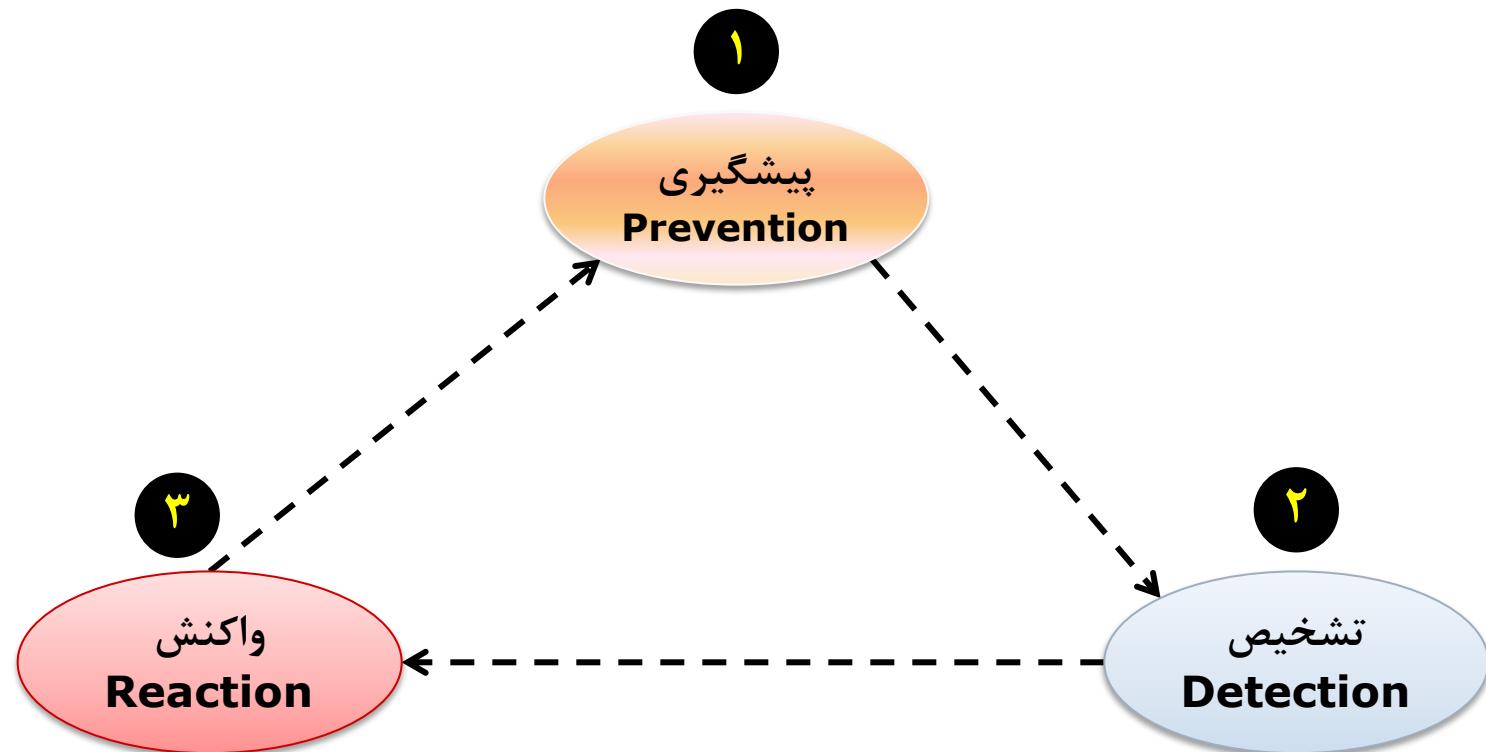
- مصالحه بین امنیت و هزینه.
- مصالحه بین امنیت، کارآیی (Functionality) و عملکرد (Performance).



- میزان امنیت مورد انتظار؟
- میزان ناامنی قابل تحمل؟



# اقدامات امنیتی





# 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



# فهرست مطالب

ضرورت تامین امنیت

معرفی درس

مفاهیم اولیه

انواع و ماهیت حملات متداول



# آنچه این درس بررسی می‌کند

□ این درس مفاهیم زیر را در بر می‌گیرد:

- تهدیدها و آسیب‌پذیری‌های امنیتی
- نیازهای امنیتی
- مکانیزم‌ها و پروتکل‌های امنیتی

□ برای داده‌های

- |                   |   |                         |
|-------------------|---|-------------------------|
| امنیت پایگاه داده | ← | ذخیره شده               |
| امنیت شبکه        | ← | در حال انتقال (در شبکه) |
| امنیت سیستم       | ← | در حال پردازش           |



# موضوعات تحت پژوهش درس

- مفاهیم و تعاریف اولیه
- مکانیزم‌های تأمین امنیت
- خط‌نمودهای امنیتی و مدل‌های کنترل دسترسی
- امنیت سیستم و برنامه‌های کاربردی
- امنیت برنامه‌های تحت وب
- مفاهیم رمز و رمزگاری متقارن و نامتقارن
- کدهای تصدیق اصالت پیام و توابع چکیده‌ساز
- امضای رقمی و زیرساخت کلید عمومی
- امنیت شبکه مبتنی بر پروتکلهای رمزگاری
- فایروال (دیواره آتش)
- امنیت موبایل



# منابع درس

- Cryptography and Network Security Principles and Practices, 8th Edition, *By William Stallings*
- Computer Security Course Slides (CS155) *By Dan Boneh*
- Computer Security, *By Matt Bishop*
- برخی مطالب نیز مبتنی بر مقالات شناخته شده و مرجع در این حوزه تدوین شده است.



# شیوه ارزیابی

- میان ترم (۷.۵ نمره)
- پایان ترم (۷.۵ نمره)
- تمرین‌ها (۶ نمره)

**مجموع = ۲۱ نمره !**

نحوه توزیع نمرات ممکن است در انتهای ترم (بسته به کیفیت محتوای هریک از موارد فوق) تغییراتی داشته باشد.



# فهرست مطالب

- ضرورت تامین امنیت
- معرفی درس
- مفاهیم اولیه
- انواع و ماهیت حملات متداول



# اهداف پایه امنیتی (۱)

**امنیت داده‌ها:** مبتنی است بر تحقق سه ویژگی یا هدف محترمانگی، صحت و دسترسی‌پذیری.



## ✓ **محترمانگی (Confidentiality)**

- عدم افشای غیرمجاز داده‌ها

## ✓ **صحت (Integrity)**

- عدم دستکاری داده‌ها توسط افراد یا نرم‌افزارهای غیرمجاز

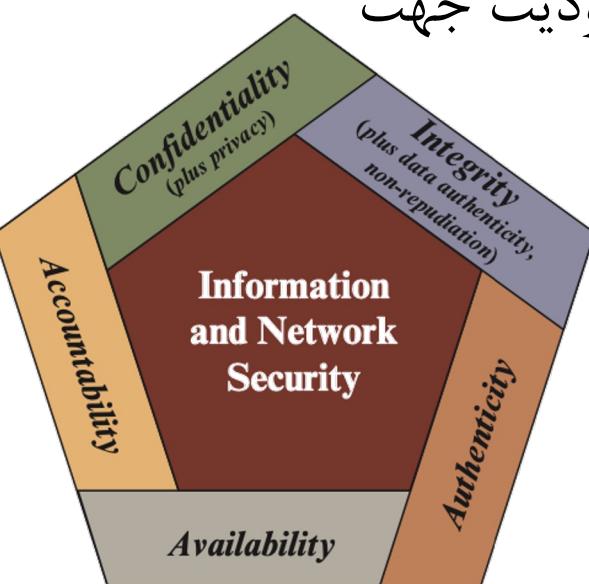
## ✓ **دسترسی‌پذیری (Availability)**

- دسترسی به داده‌ها توسط افراد مجاز بدون وقفه



# اهداف پایه امنیتی (۲)

برخی متخصصین، دو ویژگی یا هدف زیر را نیز به سه ویژگی یا هدف CIA اضافه می‌نمایند.



## ✓ اصالت (Authenticity)

- قابلیت اثبات اصالت هویت مورد ادعای یک موجودیت جهت اعتماد به آن برای انجام اعمال یا مرجعیت داده

## ✓ پاسخگویی (Accountability)

- قابلیت ردگیری اعمال مربوط به یک موجودیت و انتساب آن منحصراً به موجودیت موردنظر



# اهداف پایه امنیتی - 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 افشاری داده‌های خصوصی خود توسط دیگران کنترل و تاثیر داشته باشند.



# اهداف پایه امنیتی - محرمانگی

## □ مکانیزم‌های متداول:

- تغییر داده یا رمزنگاری
- کنترل دسترسی





# اهداف پایه امنیتی - صحت

صحت خود مشتمل بر چند 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 سیستم (System Integrity) یا صحت اجرا

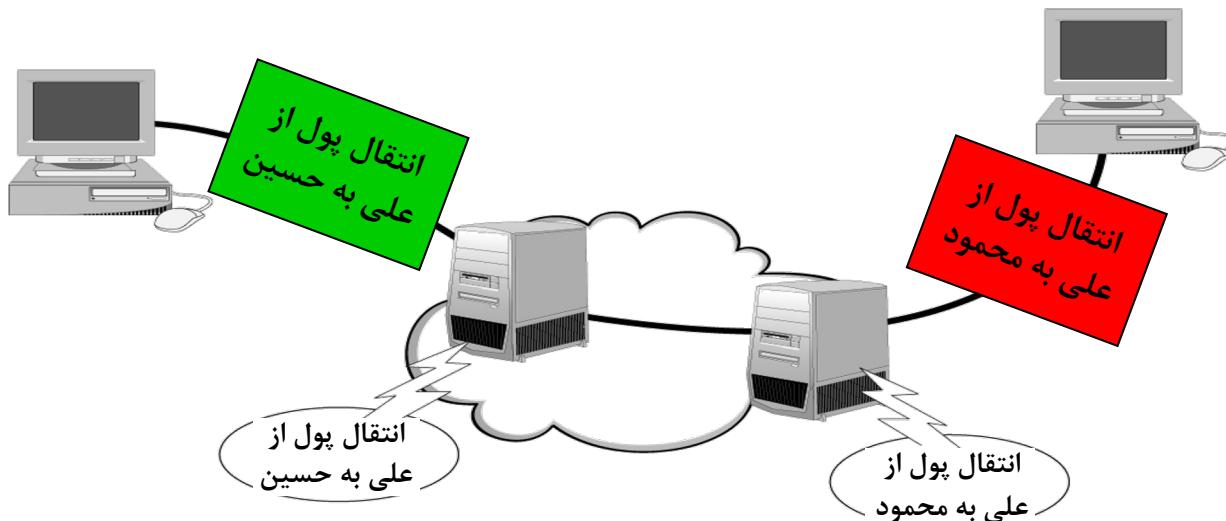
- اطمینان از صحت عملکرد سیستم (اجرای برنامه) مطابق با اهداف تعریف شده



# اهداف پایه امنیتی - صحت

## □ مکانیزم‌های متداول:

- امضا دیجیتال
- کد احراز اصالت پیام
- کنترل دسترسی
- کد وارسی صحت اجرا





# اهداف پایه امنیتی - دسترسی‌پذیری

□ **تعريف:** دسترسی به داده‌ها و سرویس‌دهی به افراد مجاز بدون وقفه و منع دسترسی.

□ **mekanizm متداول:** وجود پشتیبان، تکرار داده و سرویس، به همراه سیستم‌های پایش و توزیع بار





# اهداف پایه امنیتی - اصالت

- **تعريف:** قابلیت اثبات اصالت هویت مورد ادعای یک موجودیت جهت اعتماد به آن برای انجام اعمال یا مرجعیت داده.
- به عبارت دیگر اطمینان از اینکه هویت یک موجودیت، همانی است که ادعا می‌کند و یا منبع یک داده دریافتی همانی است که ادعا می‌شود.
- **مکانیزم‌های متداول:**
  - احراز هویت با روش‌های مختلف
  - کد احراز اصالت و صحت پیام (MAC)
  - امضای دیجیتال



# اهداف پایه امنیتی - پاسخگویی

- **تعريف:** یک ویژگی که بر اساس آن ردگیری فعالیت‌های صورت گرفته در یک سیستم تا تعیین افراد مسئول آن امکان‌پذیر می‌شود.
- به این ترتیب افرادی که تخلف کرده‌اند و یا به امنیت سامانه آسیب وارد کرده‌اند قابل شناسایی و پیگیری خواهند بود.
- **مکانیزم‌های متداول:**
  - رویدادنگاری (Auditing) و ممیزی (Logging)
  - امضای دیجیتال



# تعریف و مفاهیم اولیه (در این درس...)

- **خط مشی (سیاست‌های امنیتی) امنیتی (Security Policy):** نیازمندی‌های امنیتی یک سازمان و یا یک سیستم اطلاعاتی / ارتباطی را بیان می‌نماید.
- در تعریف سیاست‌های امنیتی به طور نمونه:
  - 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 دارد.



# تعریف و مفاهیم اولیه (در این درس...)

## □ 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 یا بدخواهانه است.

**Malicious Hacker = Attacker**



# تعاریف و مفاهیم اولیه (در این درس...)

- آسیب‌پذیری (**Vulnerability**): درز یا مشکل شناخته شده 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 محترمانگی، صحت و یا دسترس‌پذیری یک منبع باشد.



# تعاریف و مفاهیم اولیه (در این درس...)

- **تهدید (Threat):** شرایط یا رخدادی که پتانسیل تاثیر مخرب بر سیستم یا سازمان (شامل ماموریت‌ها، کارکردها، خدمات، وجهه و شهرت، دارایی‌ها، و افراد مرتبط) را با استفاده از اقداماتی همچون دسترسی غیرمجاز، تخریب، افشا، دستکاری داده‌ها، یا منع سرویس داشته باشد.
- **حمله (Attack):** به یک نفوذ **عمدی** در یک سیستم اطلاعاتی / ارتباطی، حمله گفته می‌شود (معمولًاً با بهره‌کشی از آسیب‌پذیری‌های موجود).
- در واقع حمله نتیجه تهدیدی است که از حالت بالقوه به بالفعل تبدیل شده است.



# تعریف و مفاهیم اولیه (در این درس...)

- **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 تامین یا تضمین‌کننده امنیت در یک سیستم و یا شبکه گفته می‌شود. هر سرویس با مجموعه‌ای از مکانیزم‌های امنیتی می‌تواند ارایه شود (مانند سرویس محربانگی)



# فهرست مطالب

- ضرورت تامین امنیت
- معرفی درس
- مفاهیم اولیه
- انواع و ماهیت حملات متداول

# مهم ترین انواع حملات متداول



## انواع حملات از نظر تاثیر:

### حملات فعال (Active)

- جعل هويت (Masquerade)
- ارسال دوباره پيغام (Replay)
- تغيير (Modification)
- منع سرويس (Denial of Service)

### حملات غيرفعال (Passive)

- تحليل ترافيك (Traffic Analysis)
- حمله شنود محتوا (Sniffing / Release of Message Content)

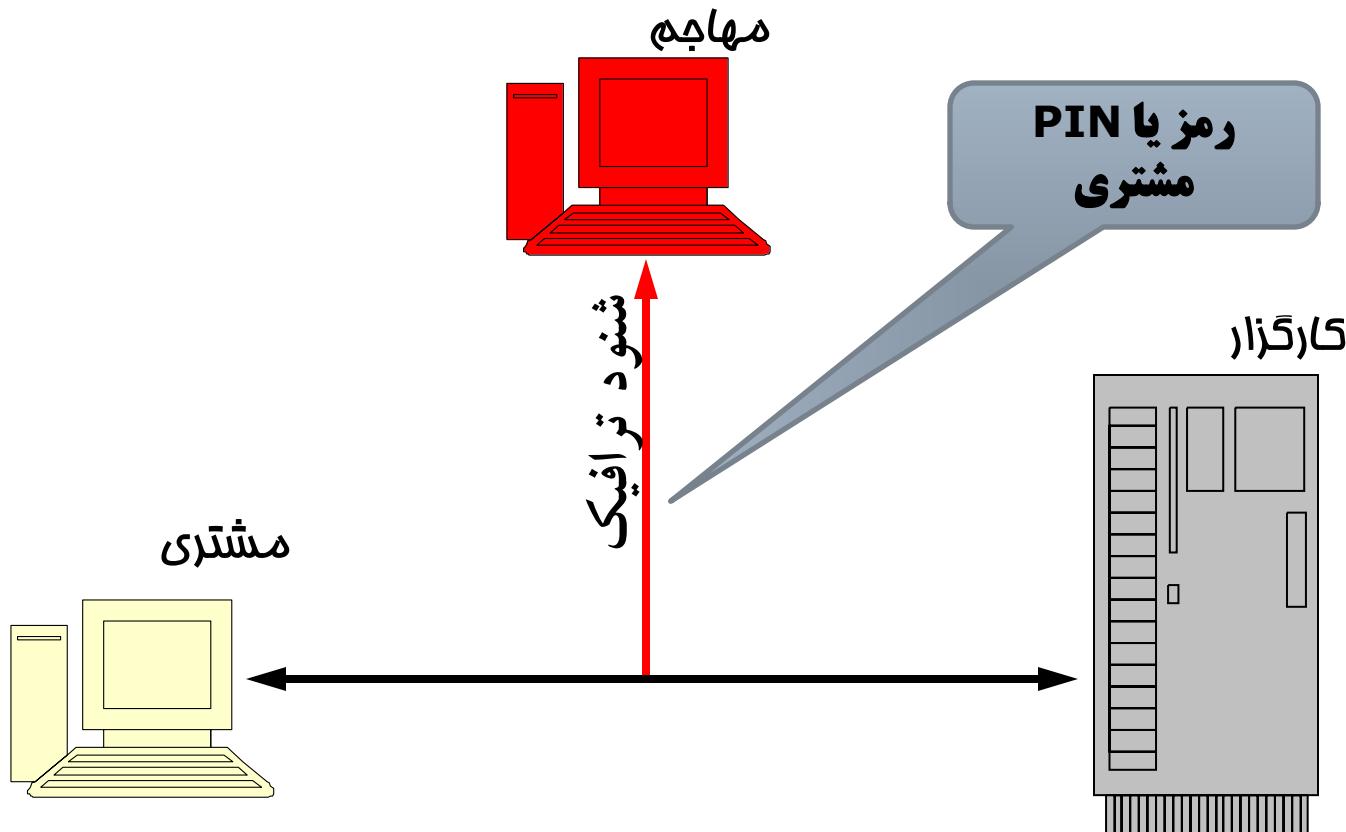


# حمله شنود یا استراحت سمع

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



# حمله شنود یا استراق سمع (ادامه)



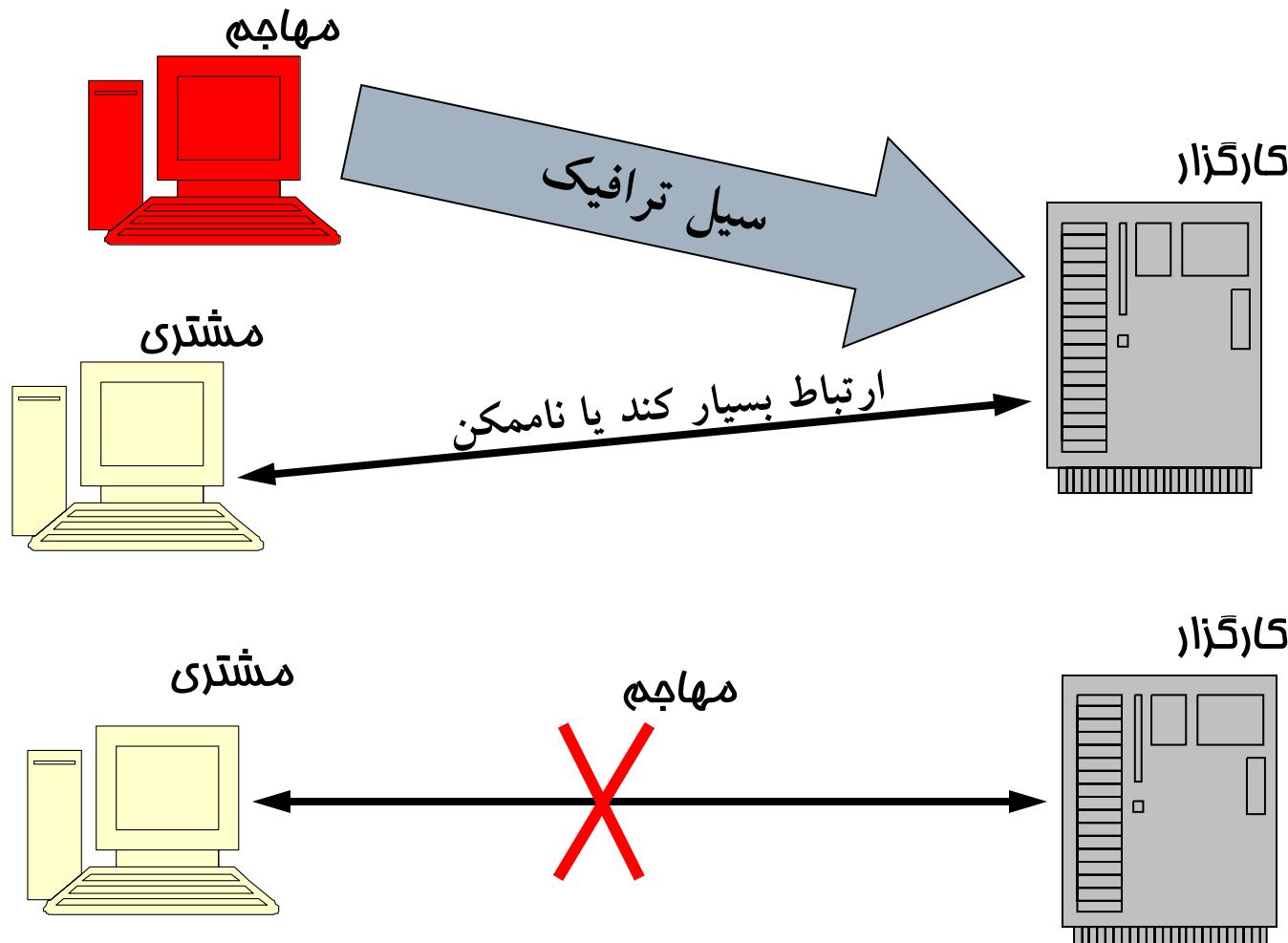


# حمله منع سرویس یا وقفه

- هدف: نقض دسترس پذیری
- 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 و یا سرویس‌ها



# حمله منع سرویس یا وقفه (ادامه)



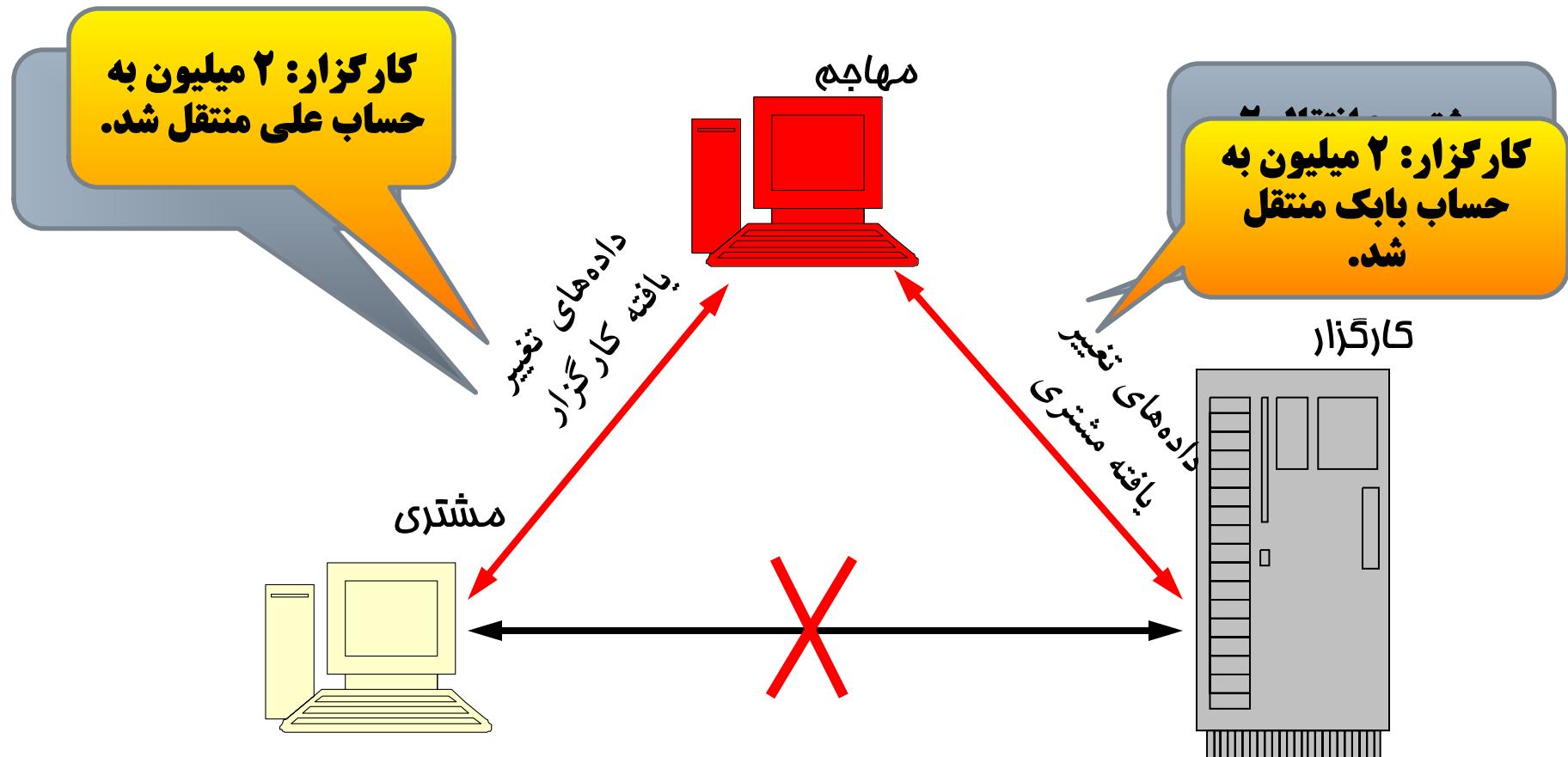


# حمله تغییر یا دستکاری داده‌ها

- 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)



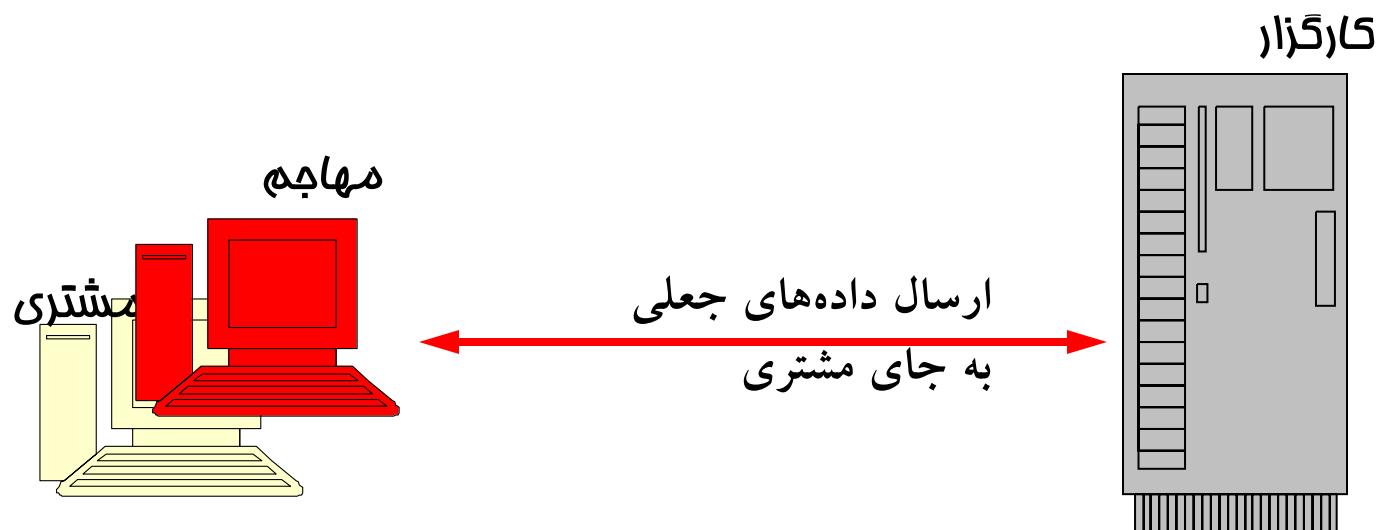


# حمله جعل هویت

- هدف: نقض صحت
- نتیجه: جعل (یا ایجاد) پیامها و داده‌هایی که می‌توانند مخرب یا منشأ سوءاستفاده باشند.
- راههای تحقق حمله:
  - بازارسال بسته‌های شنود شده پس از اعمال 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)





# پایان

پست الکترونیکی

[amini@sharif.edu](mailto:amini@sharif.edu)

[kharrazi@sharif.edu](mailto:kharrazi@sharif.edu)