یا ذاالامن والامان

مفاهیم و تعاریف اولیه

مبانی امنیت اطلاعات و شبکه‌های کامپیوتری

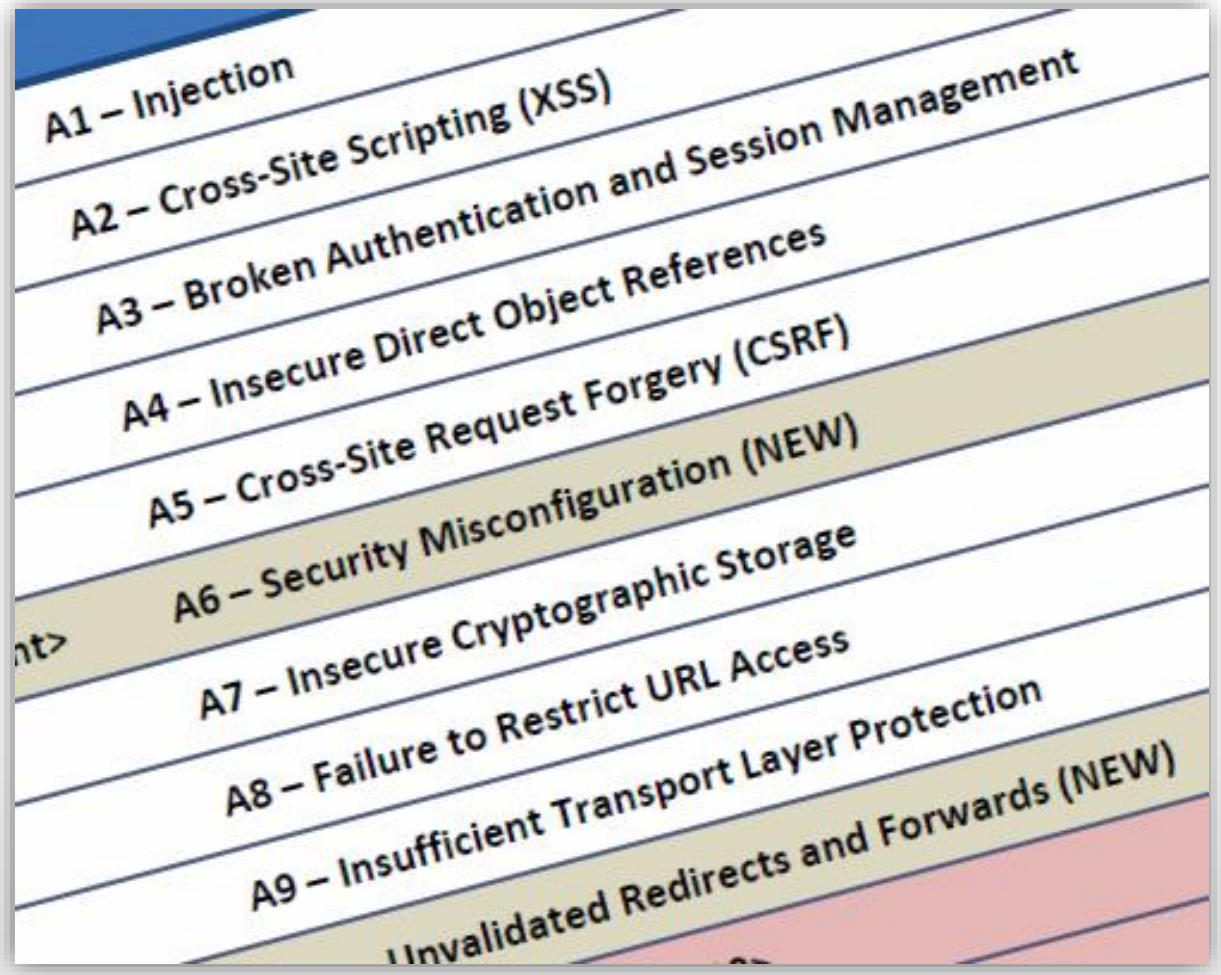
محمدرضا رازیان*
خزان ۱۳۹۵
مرکز تخصصی آپا
دانشگاه سمنان

مرکز تخصصی آپا دانشگاه سمنان
http://cert.semnan.ac.ir

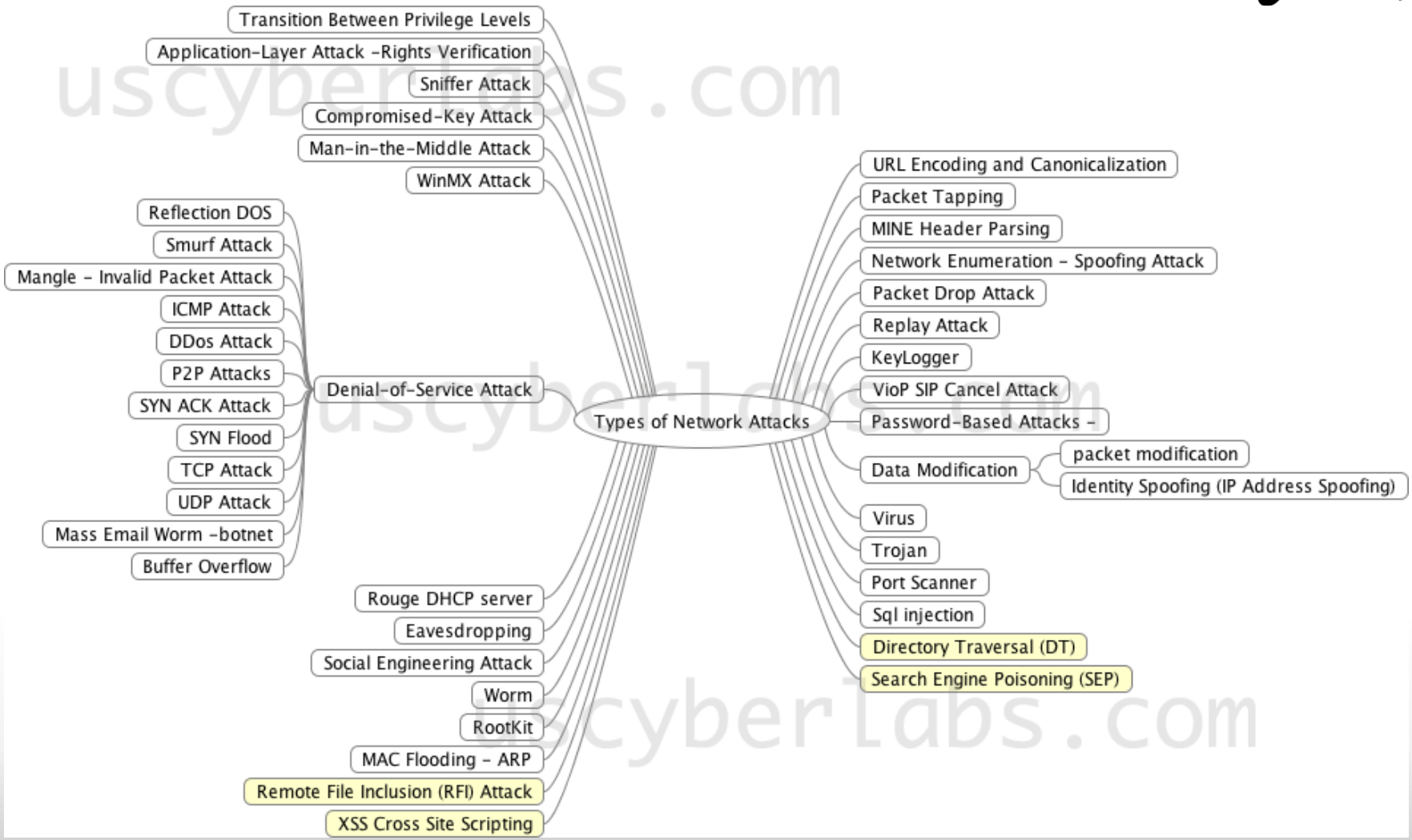
آزمایشگاه امنیت داده و شبکه شریف
http://dnsl.ce.sharif.ir

*Homepage: www.mrazian.com

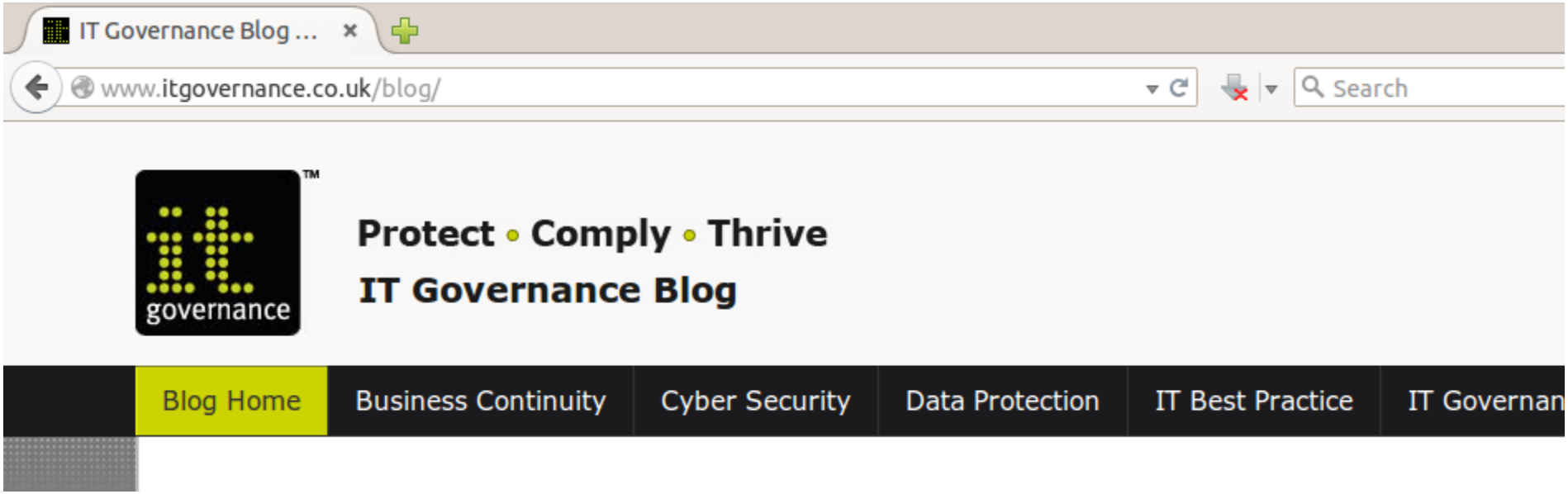
OWASP TOP 10


A1 – Injection
A2 – Cross-Site Scripting (XSS)
A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object References
A5 – Cross-Site Request Forgery (CSRF)
A6 – Security Misconfiguration (NEW)
A7 – Insecure Cryptographic Storage
A8 – Failure to Restrict URL Access
A9 – Insufficient Transport Layer Protection
Unvalidated Redirects and Forwards (NEW)

Types of Net. Attack



uscyberlabs.com


IT Governance Blog ...
www.itgovernance.co.uk/blog/
Search
governance
Protect • Comply • Thrive
IT Governance Blog
Blog Home
Business Continuity
Cyber Security
Data Protection
IT Best Practice
IT Governan

م

January

1 January, 2014 – 1.1 MILLION customers' credit card data was swiped in Neiman Marcus breach

20 January, 2014 – Credit Card Details of 20 Million South Koreans Stolen

21 January, 2014 – Microsoft blog hacked by Syrian Electronic Army

24 January, 2014 – CNN website, Twitter and Facebook hijacked by Syrian Electronic Army

25 January, 2014 – Michaels Stores confirms payment card information compromised in breach

ن

February

5 February, 2014 – Texas health system attacked, data on more than 400K compromised

14 February, 2014 – Forbes.com Hacked by Syrian Electronic Army Because of "Hate for Syria"

16 February, 2014 – Kickstarter hacked: Passwords, phone numbers, and phone numbers stolen

24 February, 2014 – YouTube ads spread banking malware

25 February, 2014 – Mt. Gox exchange goes dark as allegations of $350 million hack swirl

ی

March

10 March, 2014 – Hackers steal 12 million customer records from South Korean phone giant

14 March, 2014 – Credit Card Breach at California DMV

17 March, 2014 – Morrisons employee arrested following data breach involving details of 100k staff

20 March, 2014 – EA Games website hacked to phish Apple IDs from users

28 March, 2014 – Malware in 34 Spec's stores, payment data compromised for 550K

ت

April

7 April, 2014 – Germany suffers biggest ever data breach in its history

8 April, 2014 – The Heartbleed bug: serious vulnerability found in OpenSSL cryptographic software library

15 April, 2014 – German space centre endures cyber attack

15 April, 2014 – Welsh Councils break DPA 2.5 times a week

22 April, 2014 – Iowa State server breach exposes SSNs of nearly 30,000

29 April, 2014 – Security breach at AOL. Users told to change passwords

د

May

8 May, 2014 – Orange Suffers Data Breach Again, 1.3 Million Affected

9 May, 2014 – WooThemes users notified of payment card breach, 300 reports of fraud

21 May, 2014 – eBay Suffers Cyber Attack, Users Asked to Change Passwords

27 May, 2014 – Avast Suffers Cyber Attack; 400,000 users affected

۱

July

1 July, 2014 – Energy Firms Hacked by Cyber Espionage Group 'Dragonfly'

4 July, 2014 – $3.75 Billion Brazilian Boleto Malware Attack

8 July, 2014 – HotelHippo.com Closes after Data Leak

15 July, 2014 – CNET Hacked, One Million Users' Data Stolen

16 July, 2014 – Information Commissioner's Office Suffers Data Security Breach

23 July, 2014 – eBay has suffered a security breach for the second time this year

31 July, 2014 – Gizmodo Brazil hacked, fake Adobe Flash download opens backdoor

31 July, 2014 – Massive Paddy Power hack: nearly 650,000 customers' records stolen

د

August

5 August, 2014 – Goodwill and FBI Investigate Possible Security Breach

15 August, 2014 – Supervalu supermarket chain begin investigating possible data breach

19 August, 2014 – US Cyber Crime Goes Nuclear: NRC Computers Hacked THREE Times

21 August, 2014 – Over 50 UPS franchises hit by data breach

27 August, 2014 – Norwegian oil industry under attack by hackers

27 August, 2014 – Records of 25,000 Homeland Security Employees Stolen in Cyber Attack

28 August, 2014 – FBI Probes Possible Hacking Incident at J.P. Morgan

۵

September

4 September, 2014 – Home Depot suffers breach that may be larger than Target's

5 September, 2014 – 800k Payment Cards Compromised in Goodwill Industries Breach

5 September, 2014 – ObamaCare Website Hacked

18 September, 2014 – Home Depot: 56M Cards Impacted, Malware Contained

23 September, 2014 – 880,000 Affected by Viator Payment Card Breach

25 September, 2015 – Payment card data stolen in Jimmy John's data breach

29 September, 2014 – Hundreds of US Stores Affected as POS Provider is Hacked

30 September, 2014 – SuperValu compromised again – for the second time in three months

و

October

3 October, 2014 – JPMorgan suffers data breach affecting 76 million customers

10 October, 2014 – Dairy Queen data breach hits 395 stores

14 October, 2014 – 'Big K' raided by hackers: Kmart warns customers after malware discovered

21 October, 2014 – Staples stores investigated: suspected payment card breach

23 October, 2014 – POODLE attack digs up downgrade flaw in TLS

29 October, 2014 – White House unclassified network hacked

ش

November

7 November, 2014 – Home Depot admits 53 million email addresses stolen in data breach

13 November, 2014 – Data breach affects 2.7 million HSBC Turkey cardholders

17 November, 2014 – US State Department network shut amid reports of cyber breach

18 November, 2014 – Staples confirms POS malware attack

25 November, 2014 – Sony Pictures Entertainment hacked

27 November, 2014 – Syrian Electronic Army attack on Gigya affects Telegraph, Independent, Evening Standard…

ب

December

4 December, 2014 – Possible credit card breach at Bebe Stores

11 December, 2014 – Union Station parking lot suffers suspected data breach

11 December, 2014 – Electronic payment company CHARGE Anywhere suffers five-year breach

15 December, 2014 – Personal information leaked in University of California, Berkeley, data breach

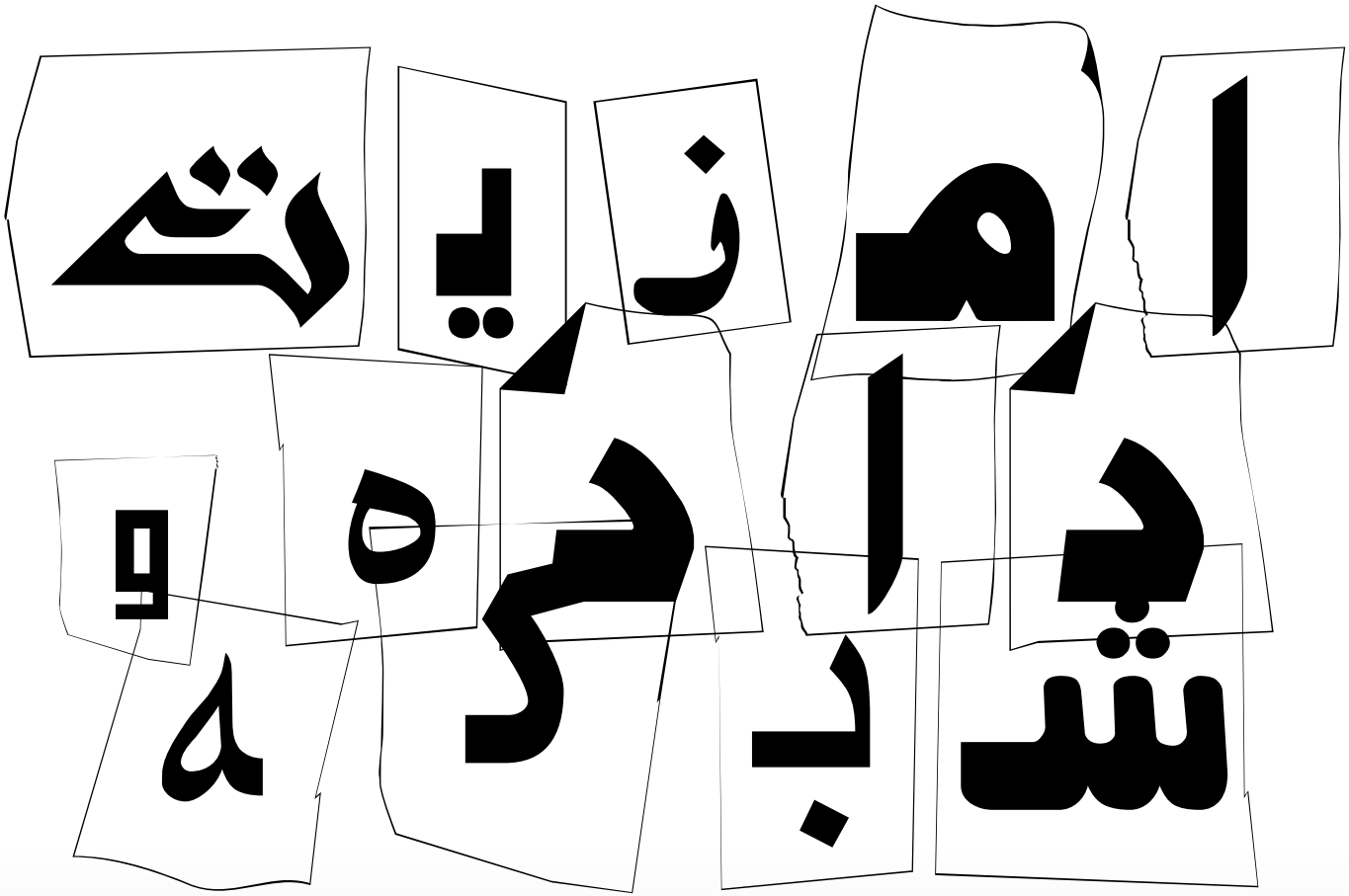
19 December, 2014 – KeyPoint cyber attack compromises 48,000 federal employees

22 December, 2014 – Staples confirm details of six-month breach, 1.16 million cards affected

جدای از صحت اخبار اما انگار ادبیاتی در راه است!

۵


CYBER CRIME
virus
worm
spyware
malware
phishing
pharming
adware
p2p
spamming
Nigerian 419 scheme
shareware
keystroke logging
keylogging
VoIP spambluebugging
cyber-stalking
piggybacking
zombie
trojan horse
software cracking
lurker
web crawler
bluejacking
sporgery
smishing
trojan
internet bots
joe job
dos attack
skiddie
web spider
e-mail spoofing
phreaking
address munging
stealware
script kitty
backdoor
crapflooding
internet troll
hacker
click fraud
money mule
script-running juvenile
pod slurping
advance fee fraud
spear phishing
sneakernet
vishing
warspying
script kiddie
black hat
white hat
backscatter
false flag operations
peer to peer
scam baiting
script bunny
web robot
denial-of-service attack
pigeon drop
Download from
Dreamstime.com
This watermarked comp image is for previewing purposes only.
ID 23925958
Jennifer Pitiquen | Dreamstime.com


امنیت
در شبکه

اوضاع هک و نفوذ در ایران

فهرست مطالب

۱ محتوای درس

۲ ضرورت امنیت داده و شبکه

۳ مفاهیم اولیه

۴ دشواری برقراری امنیت

۵ سرویس های امنیتی
مدلهای امنیت شبکه

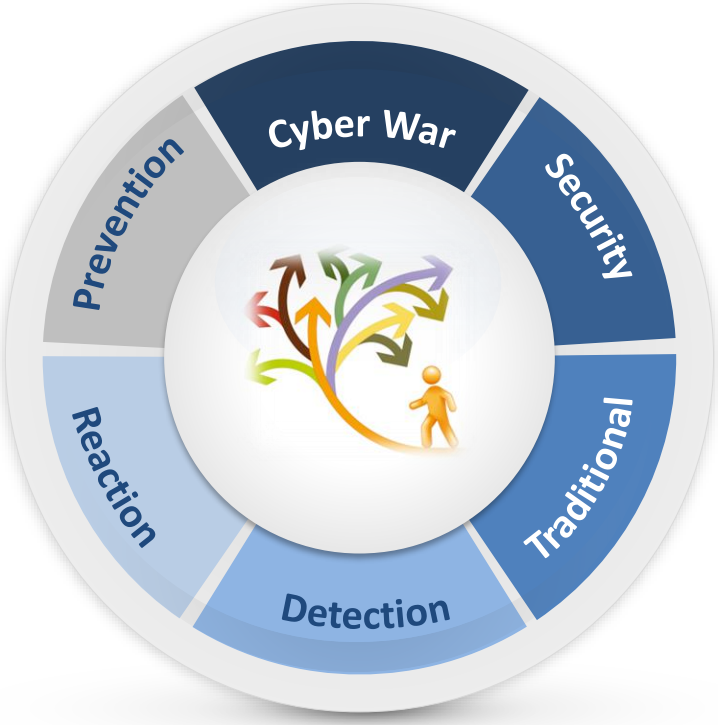
موضوعات تحت پوشش درس

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

موضوعات خارج از محدوده پوشش درس

- رمزنگاری پیشرفته
- اصول نظری در امنیت اطلاعات
- روشهای هک و نفوذ (ادر تمرین ها به این بخش می پردازیم)
- ...

فهرست مطالب



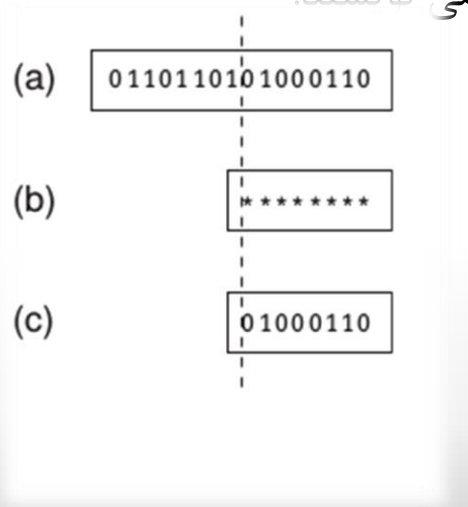
ضـــرورت امنیـــت داده و شبکه

امنیت چیست؟

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

نفوذ غیرعمدی

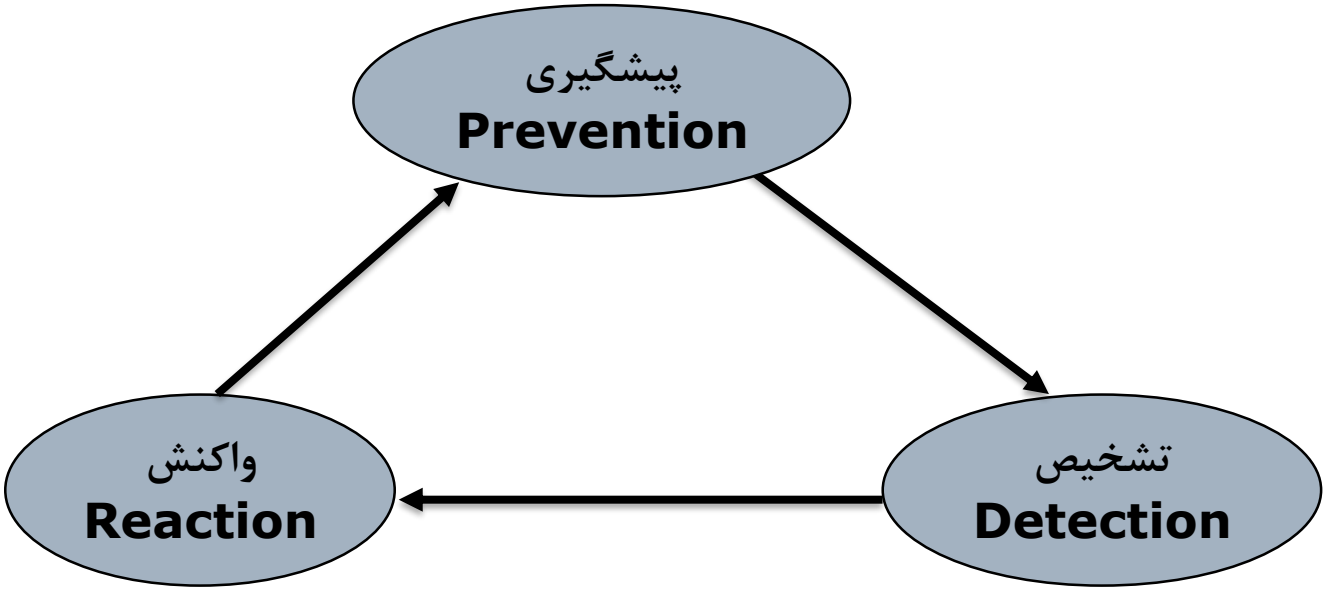
- خلا در امنیت سیستم می تواند بدخواهانه باشد یا نباشد
- یک نفوذرخنه غیرعمدی هر گونه نقص امنیتی یا تغییر داده است که نتیجه یک نفوذ برنامه ریزی شده نباشد.
  - بد کار کردن سخت افزار، خطاهای شناسایی نشده در سیستم عامل و یا برنامه های کاربردی، فجایع طبیعی، تغییر غیر کامل تصادفی داده‌ها (accidental incomplete modification of data)، بحث رقابت در پایگاه داده وقتی دو پردازه در حال کار کردن روی یک رکورد دانشجو هستند و نسخه های مختلف آن را در پایگاه داده می نویسند.
  - خطا زمانی که مقادیر داده به دلیل درنظر گرفتن ظرفیت نامناسب به طور نادرست ذخیره می شوند. برای مثال زمانی که یک فیلد فضای کمی برای داده عددی دارد فرترن (FORTRAN) عدد را به صورت ستاره ستاره پر می‌کند، COBOL ارقام با رتبه بالاتر را حذف می‌کند.



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



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

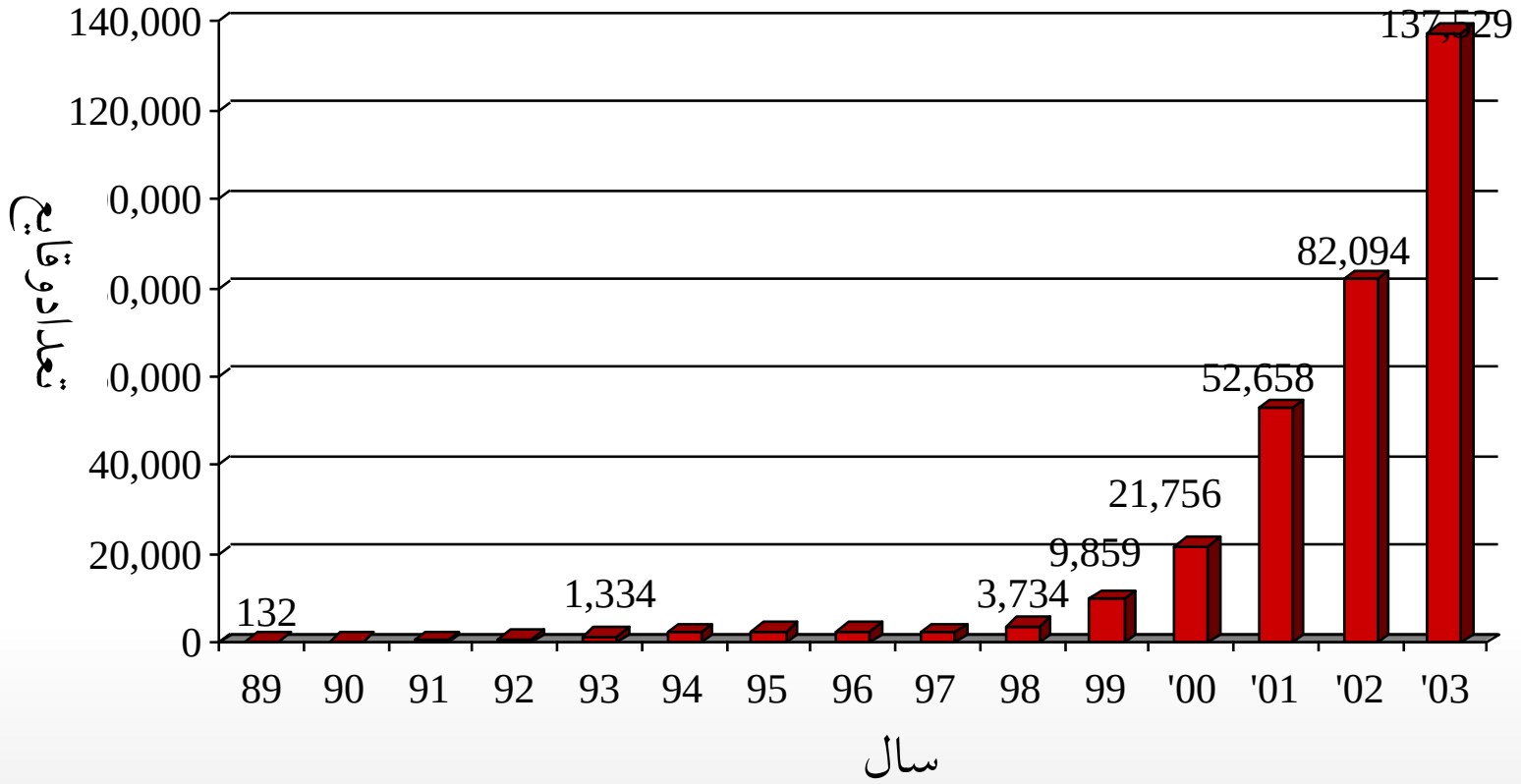
- بنابراین :
- در گذشته، امنیت با حضور فیزیکی و نظارتی تامین می‌شد،

ولی

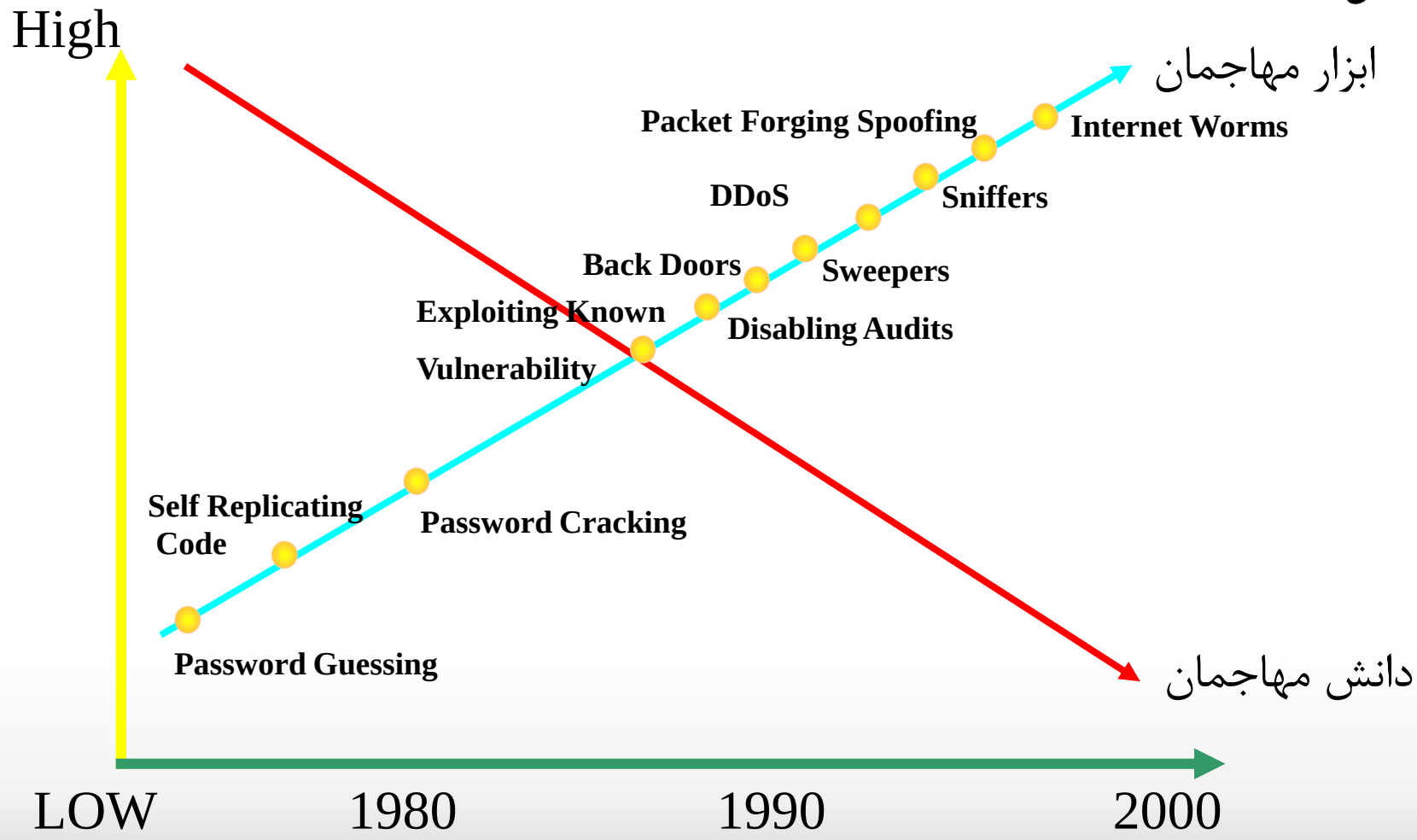
- امروزه از ابزارهای خودکار و مکانیزم‌های هوشمند برای حفاظت از داده‌ها استفاده می‌شود.

آمار منتشر شده توسط CERT

CERT (Computer Emergency Response Team)



ابزار مهاجمان



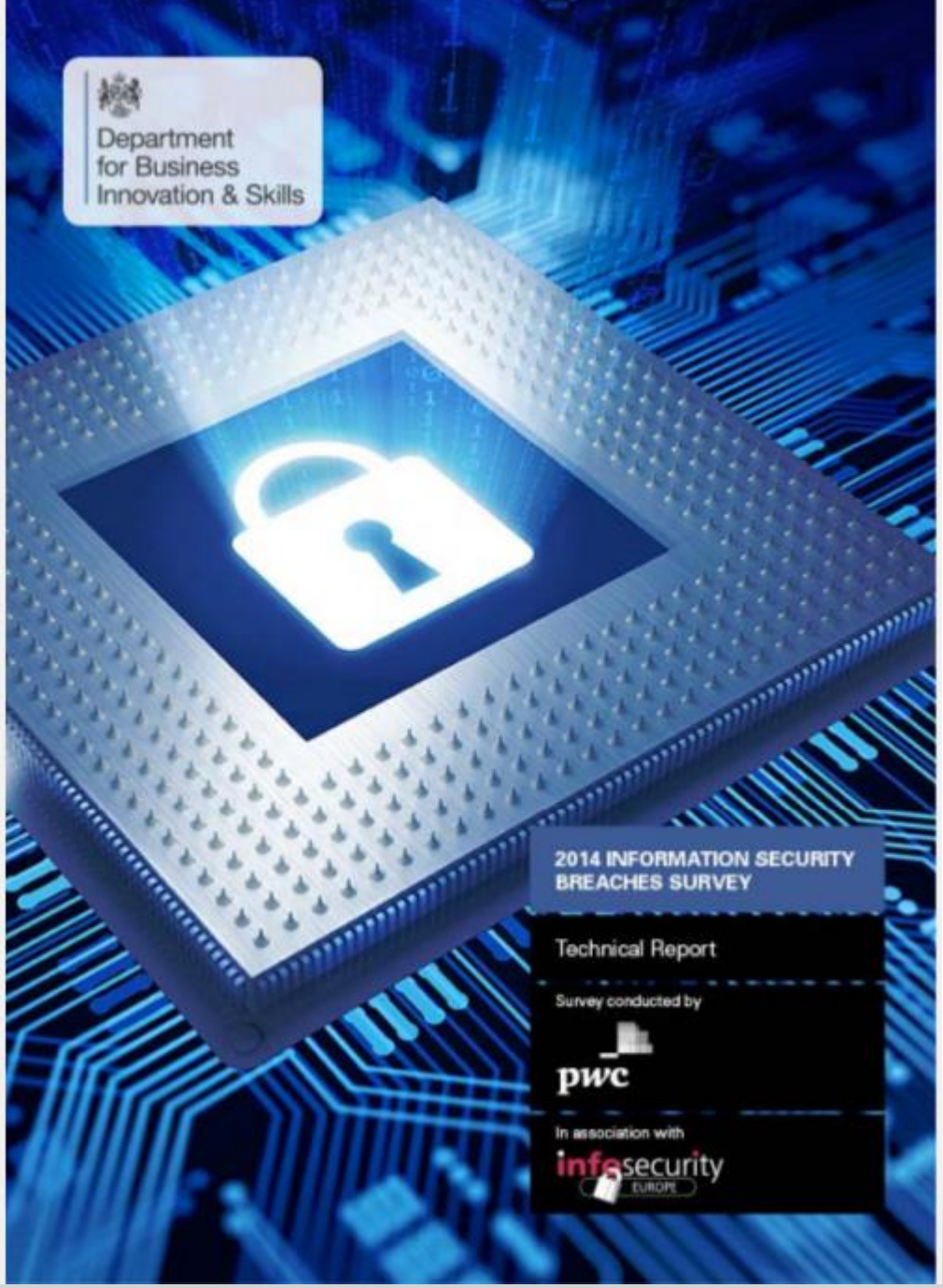
نیازهای امنیتی: گذشته و حال

- از دو نمودار قبلی بخوبی پیداست :

- تعداد حملات علیه امنیت اطلاعات به طور قابل ملاحظه‌ای افزایش یافته است.

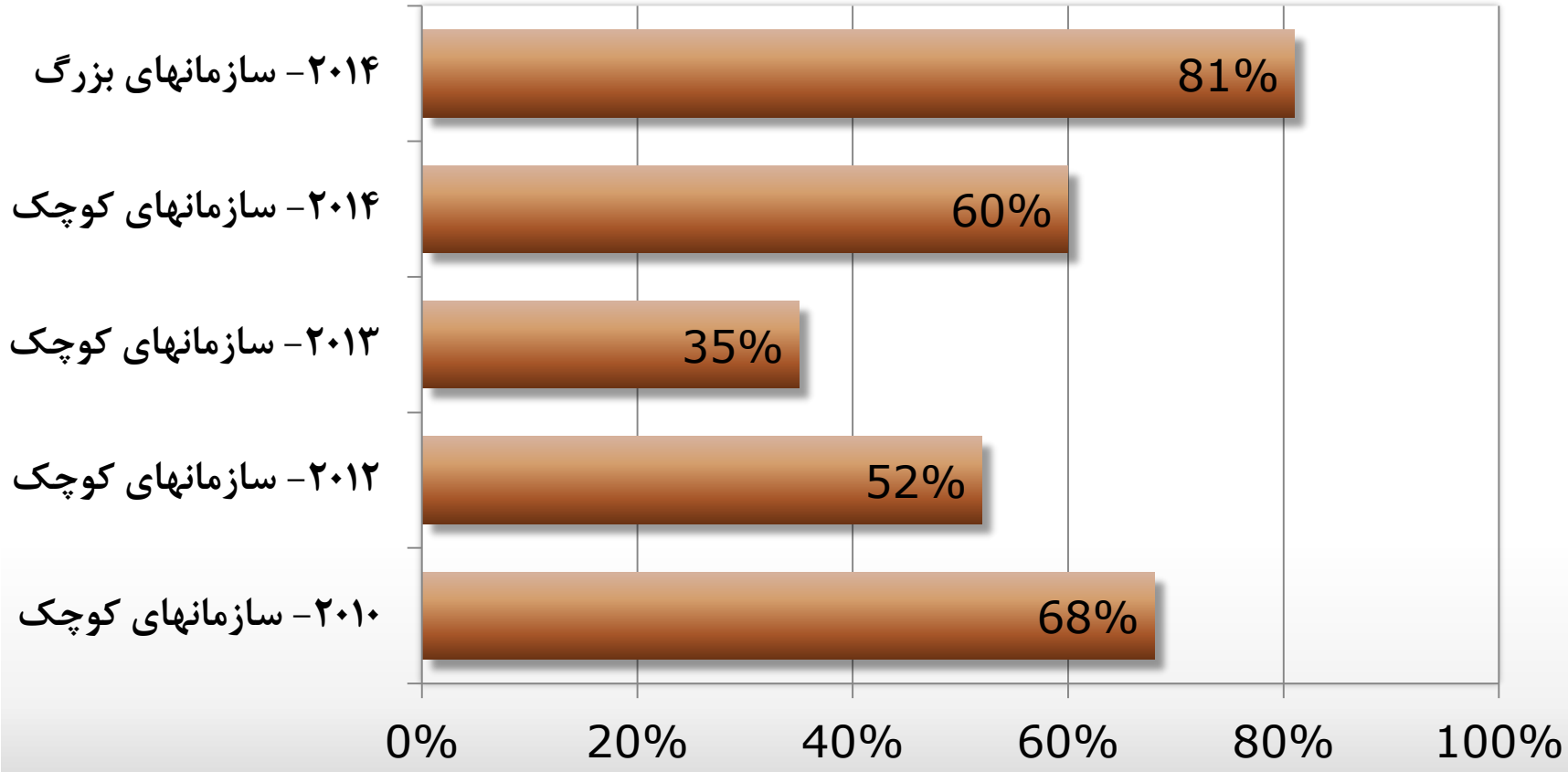
- امروزه تدارک حمله با در اختیار بودن ابزارهای فراوان در دسترس به دانش زیادی احتیاج ندارد (بر خلاف گذشته).

گزارش BIS انگلیس



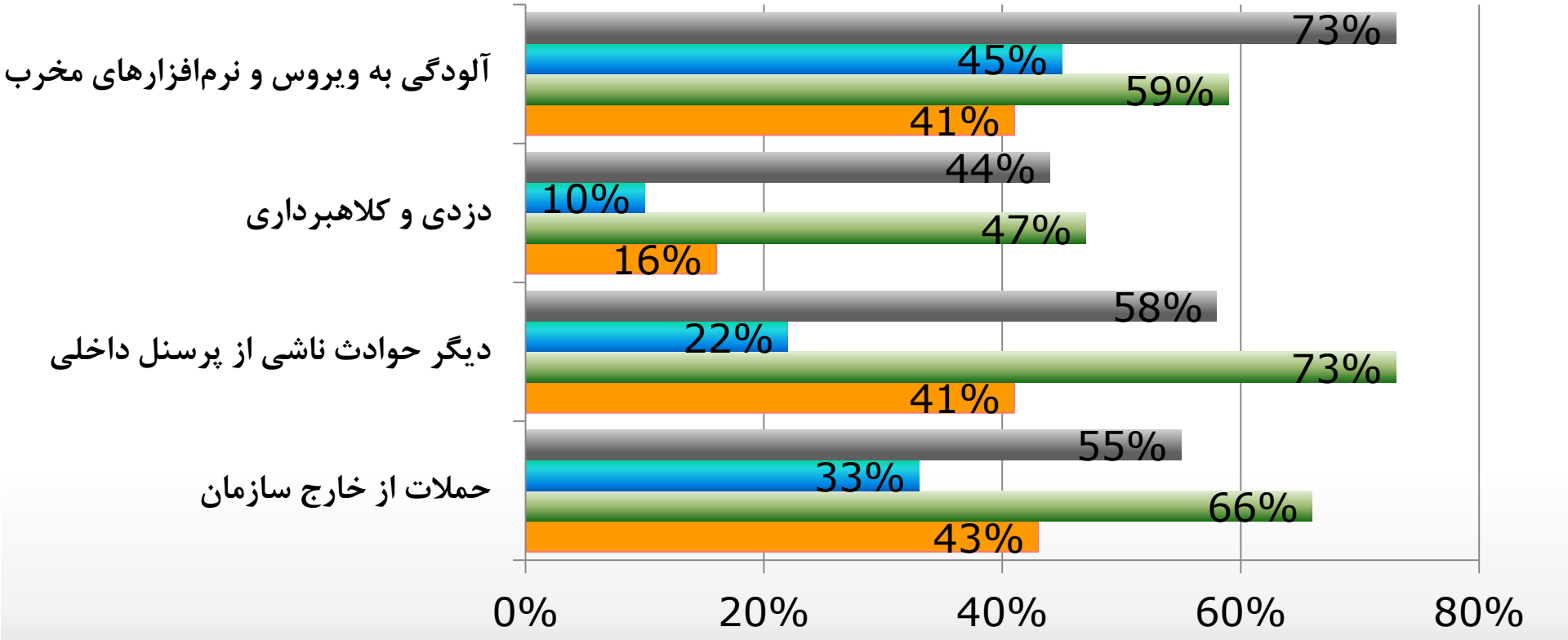
نگاهی به گزارش BIS انگلیس (۱)

حوادث امنیتی بدخواهانه در سازمانها



نگاهی به گزارش BIS انگلیس (۲)

انواع حوادث رخ داده در سازمانها



نگاهی به گزارش BIS انگلیس (۳)

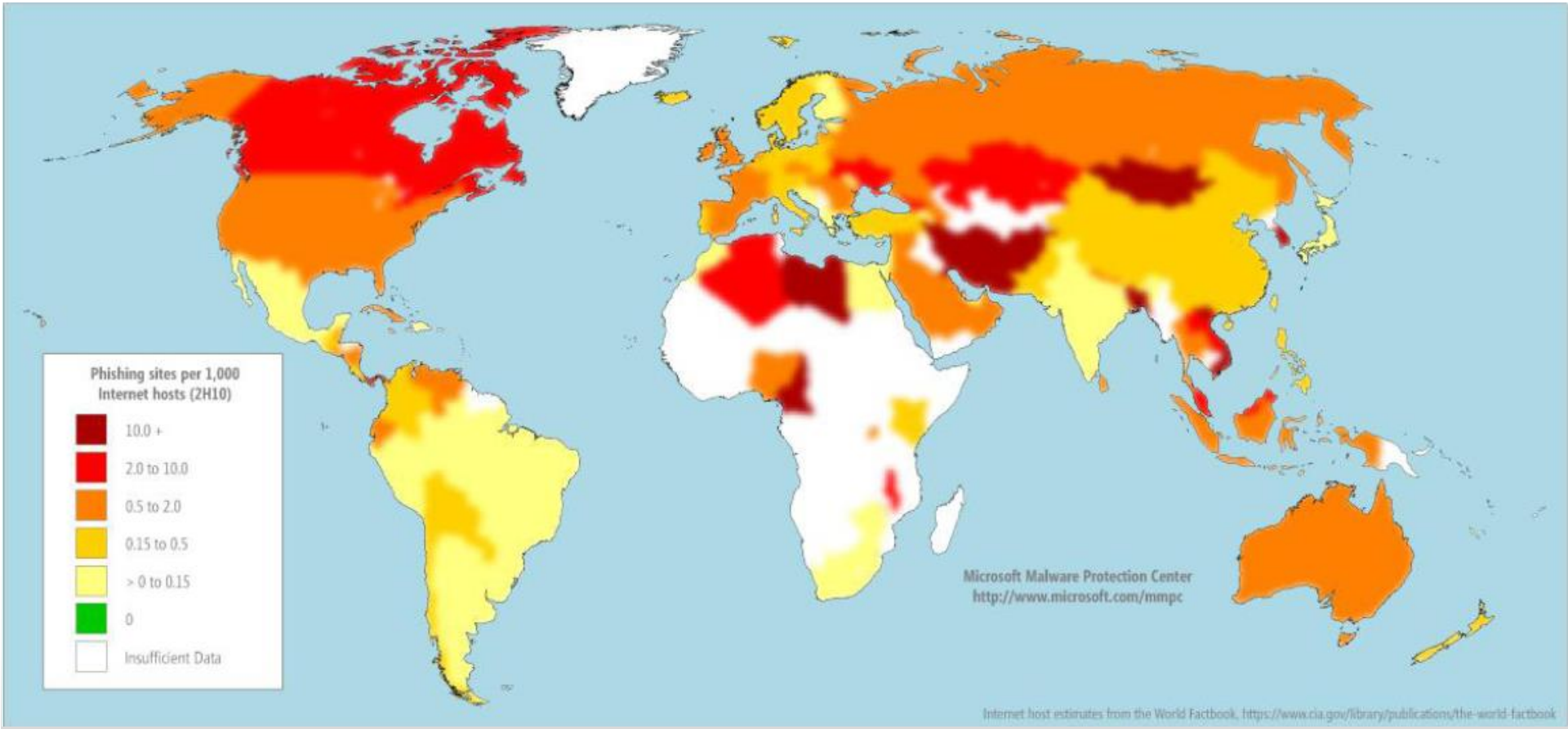
متوسط هزینه‌های مرتبط با یک حادثه سنگین امنیتی در سازمانها - ۲۰۱۴

	سازمانهای کوچک (معادل به میلیون تومان)	سازمانهای بزرگ (معادل به میلیون تومان)
تسلسل و وقفه در کسب و کار	۲۰۸ – ۳۱۲	۱۸۲۰ – ۳۳۸۰
زمان صرف شده برای مقابله با حادثه	۱۵/۶ – ۴۶/۸	۶۲/۴ – ۱۷۶/۸
هزینه‌های مستقیم مقابله با حادثه	۴۶/۸ – ۸۸/۴	۴۱۶ – ۷۰۲
جریمه و غرامت پرداختی به تنظیم مقررات	۱۰/۴ – ۲۰/۸	۱۲۴/۸ – ۲۰۸
خسارات مالی (شامل حق مالکیت معنوی) و کسب و کار	۴۴/۲ – ۸۸/۴	۴۵۲/۴ – ۶۴۴/۸
لطمه به شهرت و اعتبار	۸/۳۲– ۴۱/۶	۲۶۰ – ۹۳۶
متوسط کل هزینه یک حادثه سنگین امنیتی (۲۰۱۴)	۳۳۸ – ۵۹۸	۳۱۲۰ – ۵۹۸۰
متوسط کل هزینه یک حادثه سنگین امنیتی (۲۰۱۳)	۱۸۲ – ۳۳۸	۲۳۴۰ – ۴۴۲۰

نگاهی به گزارش SIR میکروسافت

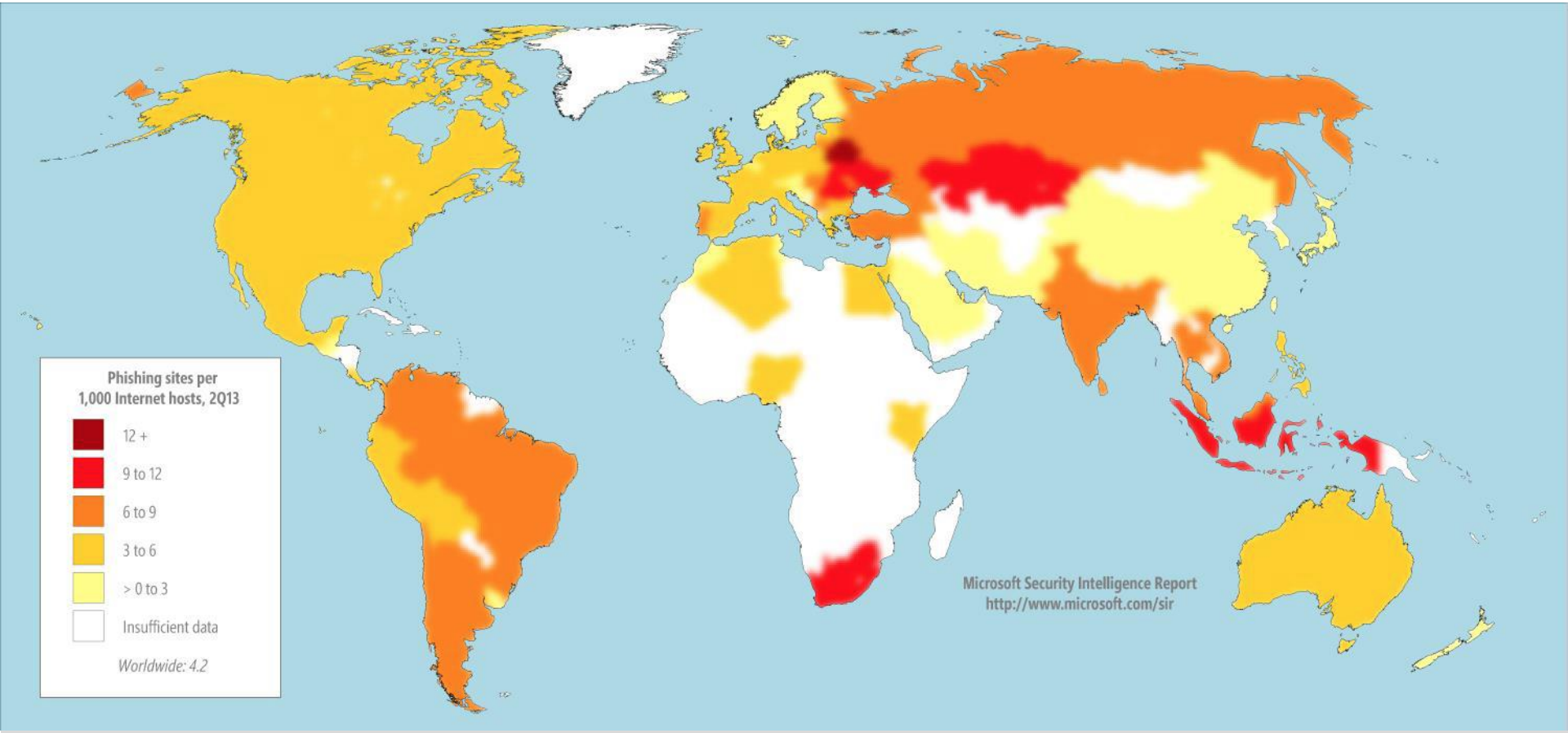
توزیع سایت‌های فیشینگ (۱)

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



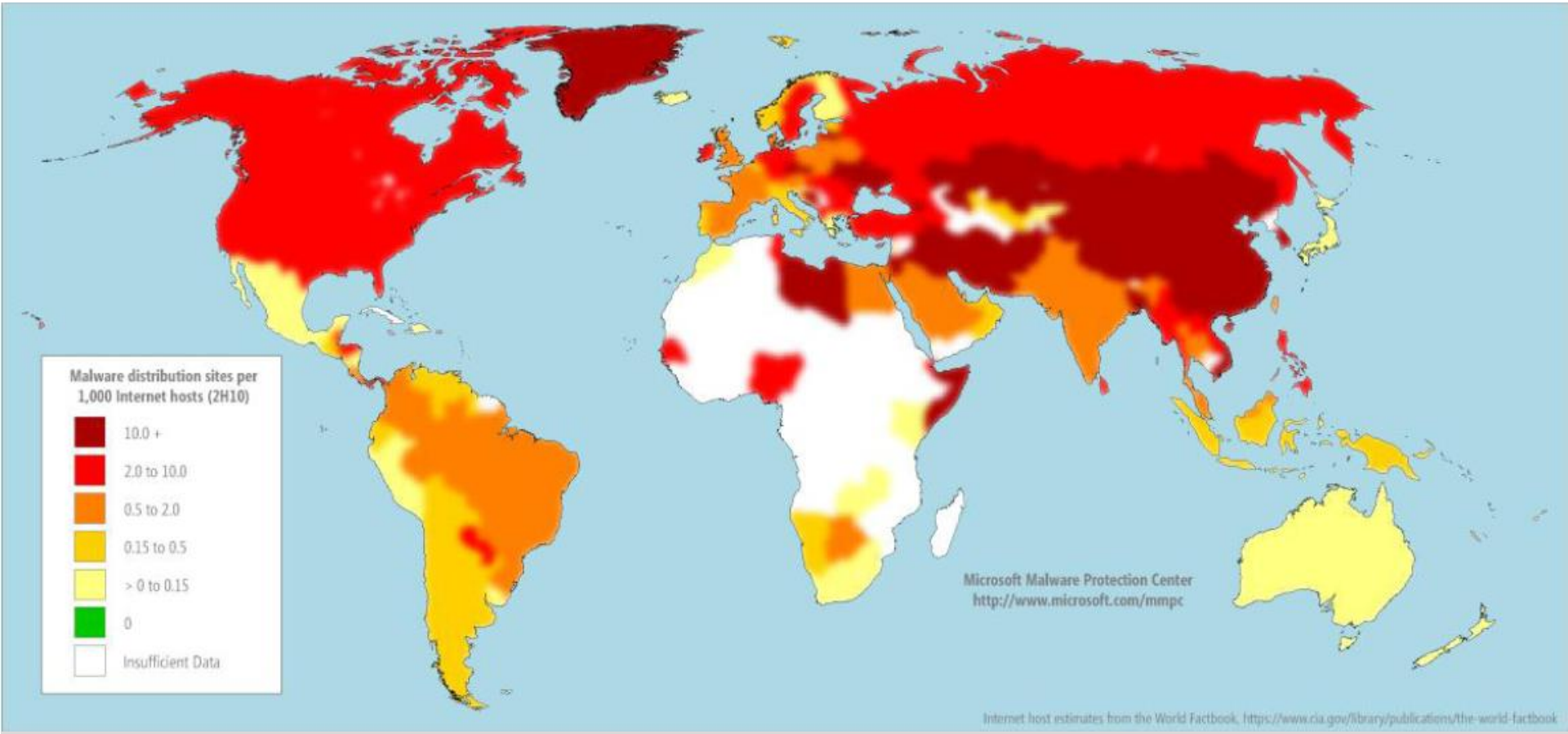
توزیع سایت‌های فیشینگ (۲)

توزیع سایت‌های فیشینگ در دنیا در ۶ ماه دوم ۲۰۱۳ (گزارش SIR)



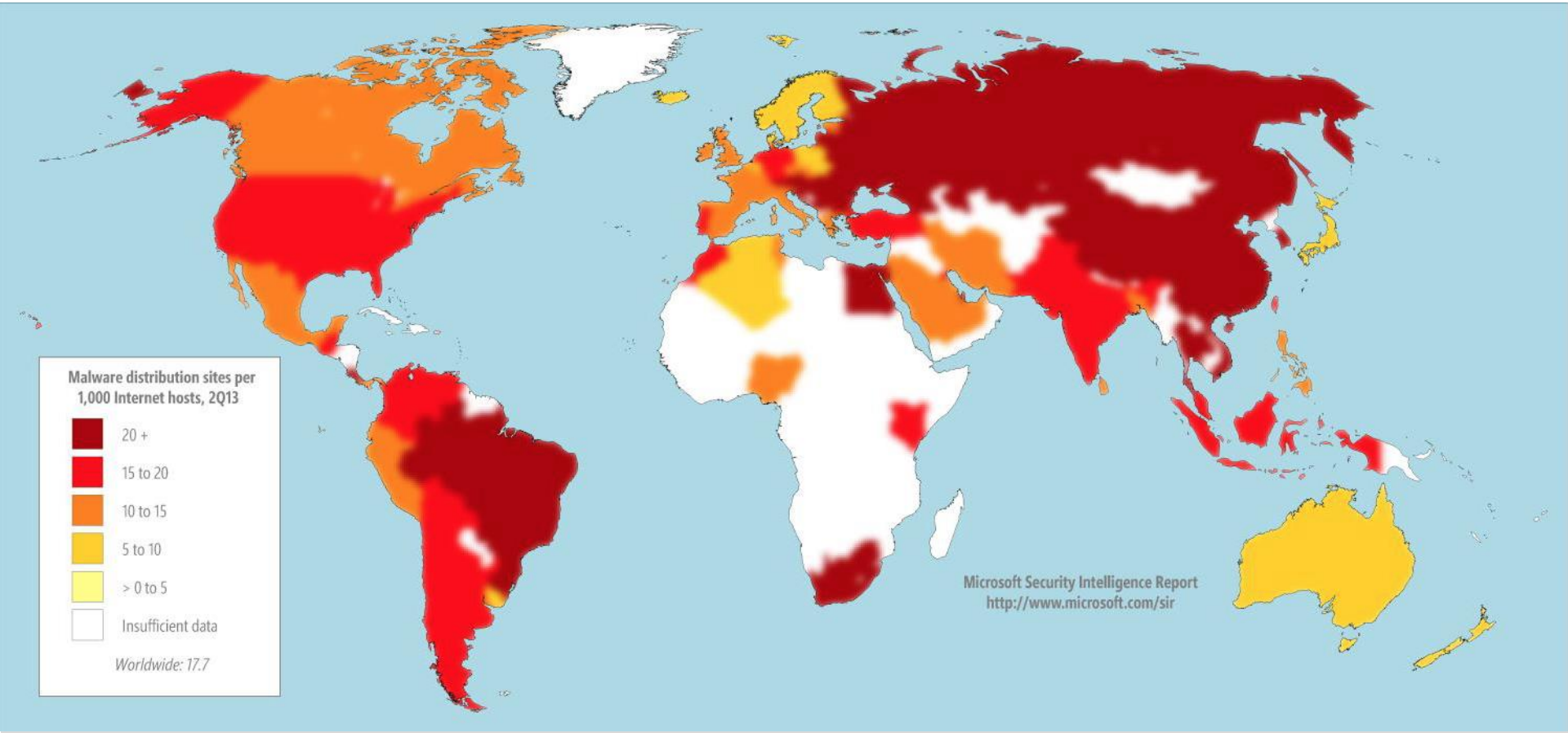
توزیع سیستم‌های آلوده (۱)

توزیع سیستم‌های آلوده به بدافزار در دنیا در ۳ ماهه دوم ۲۰۱۰ (گزارش SIR)



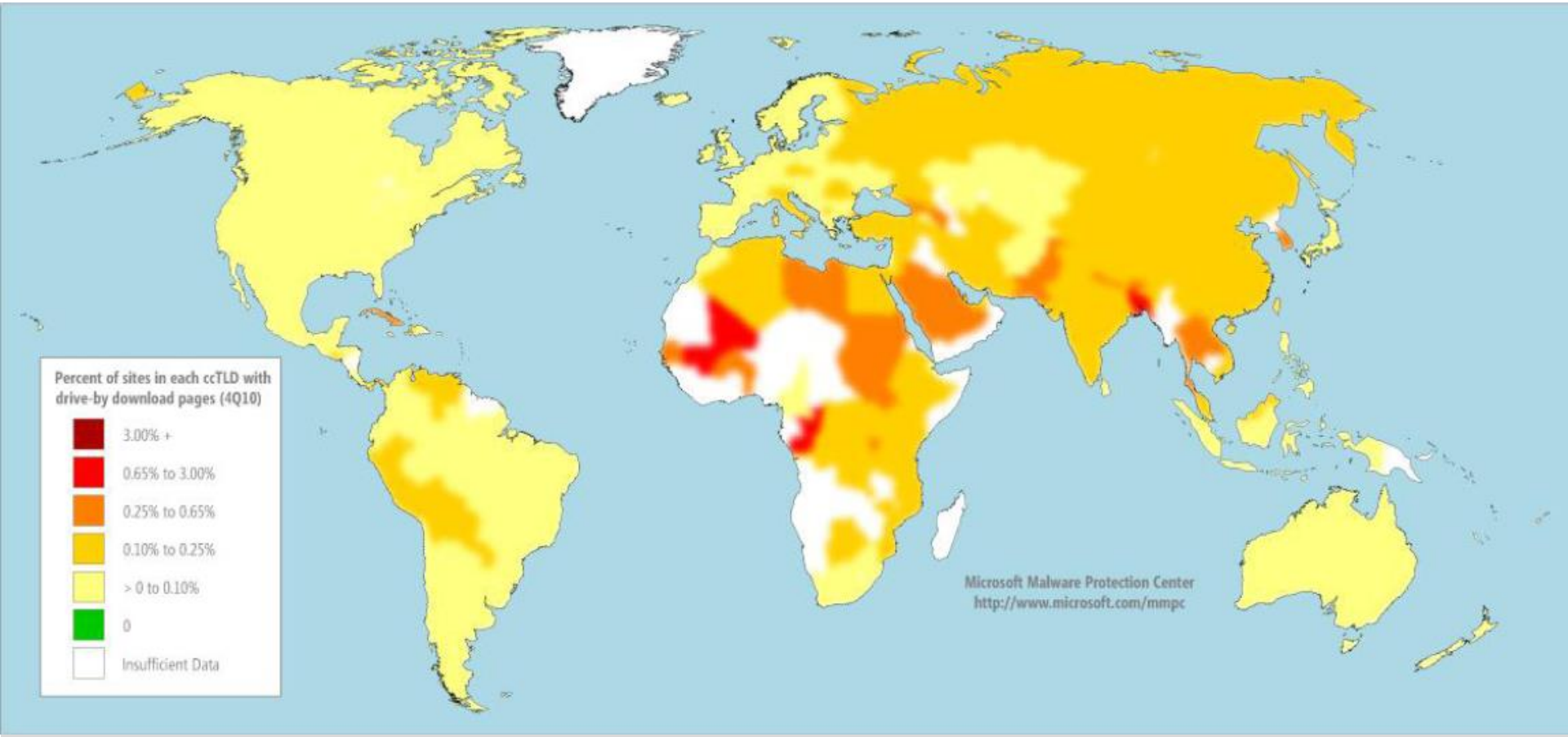
توزیع سیستم‌های آلوده (۲)

توزیع سیستم‌های آلوده به بدافزار در دنیا در ۳ ماهه دوم ۲۰۱۳ (گزارش SIR)



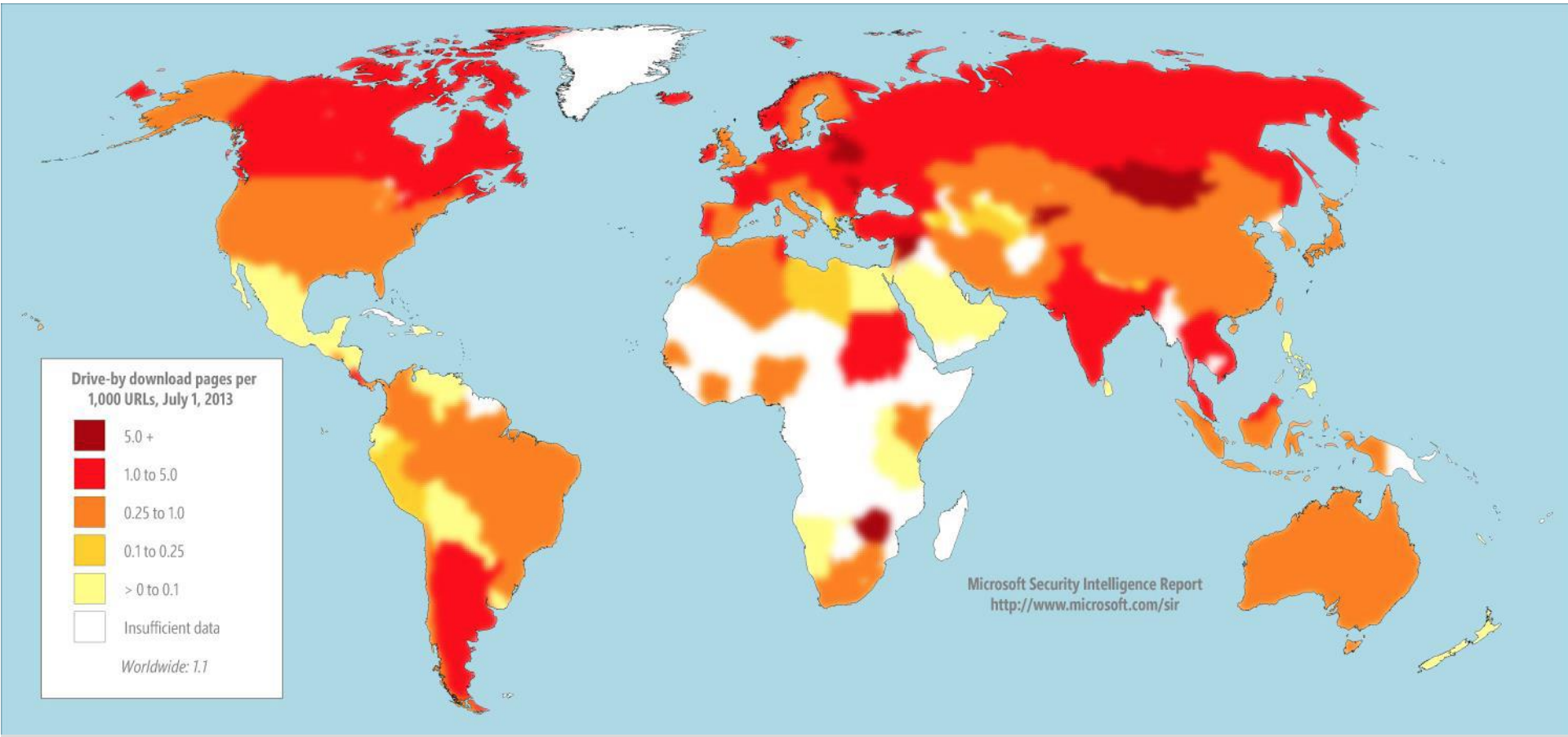
توزیع سایت‌های آلوده‌ساز (۱)

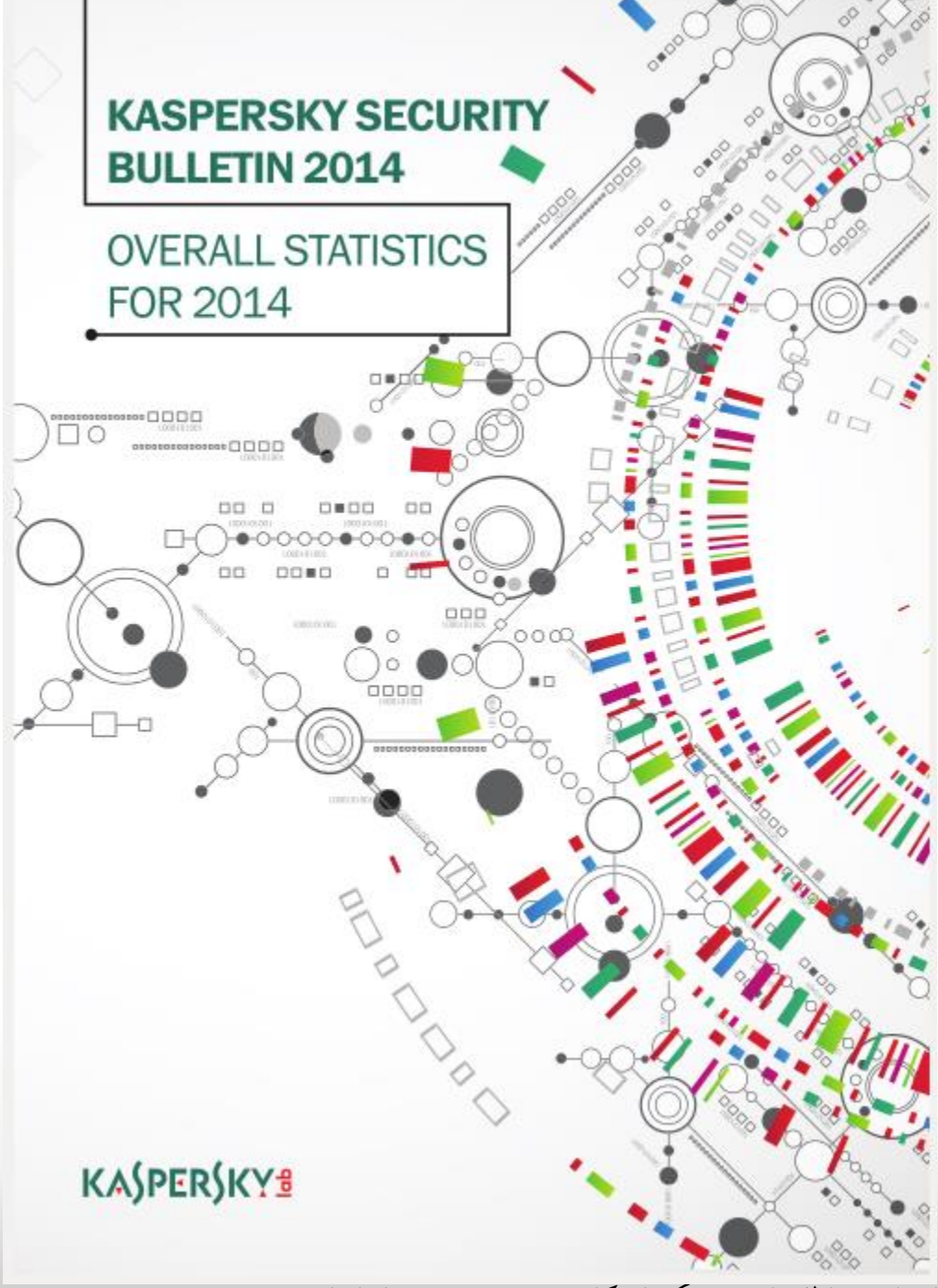
توزیع سایت‌های آلوده‌ساز در دنیا در ۳ ماهه چهارم ۲۰۱۰ (گزارش SIR)



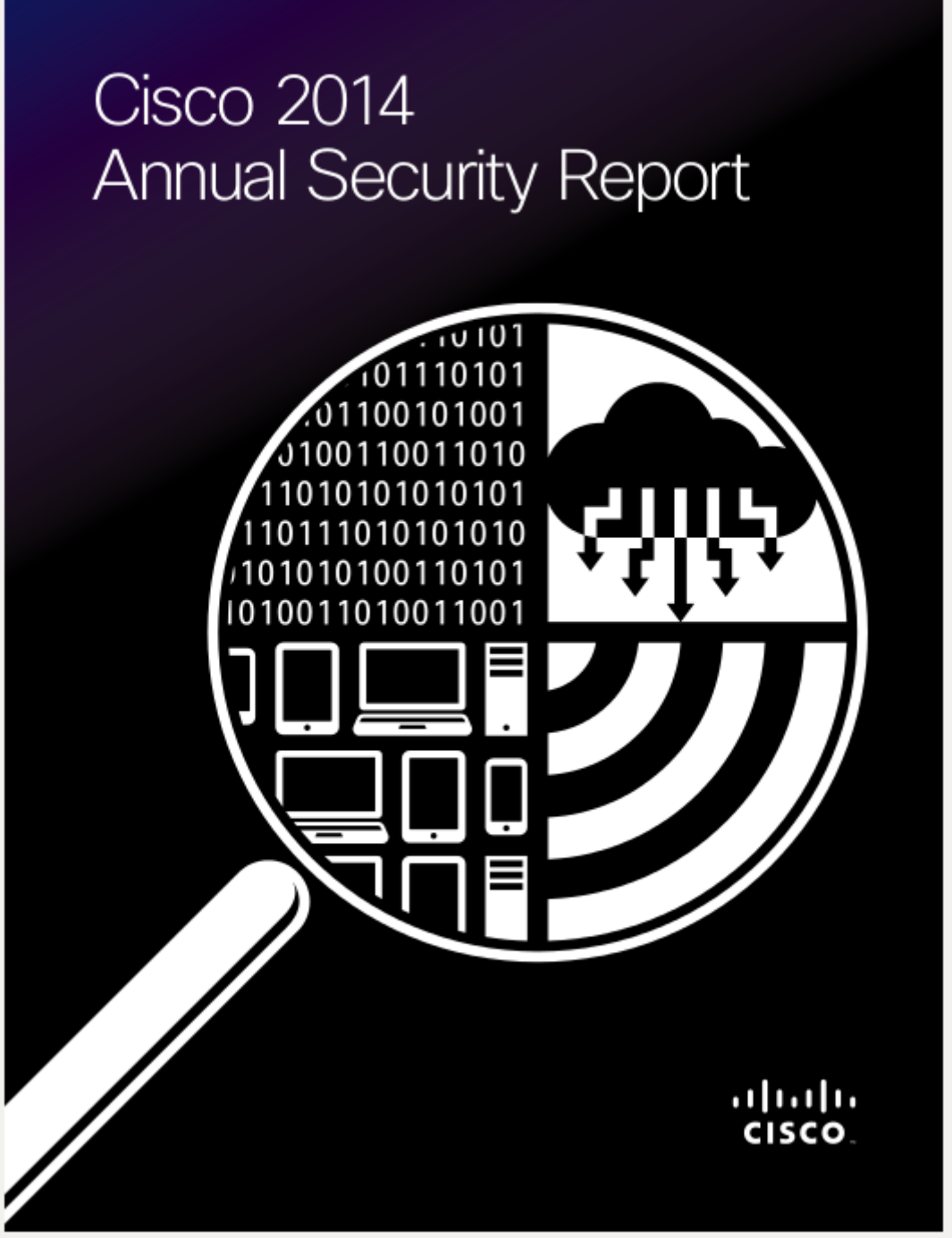
توزیع سایت‌های آلوده‌ساز (۲)

توزیع سایت‌های آلوده‌ساز در دنیا در ۳ ماهه چهارم ۲۰۱۳ (گزارش SIR)




KASPERSKY SECURITY
BULLETIN 2014
OVERALL STATISTICS
FOR 2014
KASPERSKY


Symantec.
2013 Trends, Volume 19, Published April 2014
ISTR
INTERNET SECURITY THREAT REPORT 2014


Cisco 2014
Annual Security Report
cisco

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 کارگزارهای (Server) اداری تحت کنترل روسیه

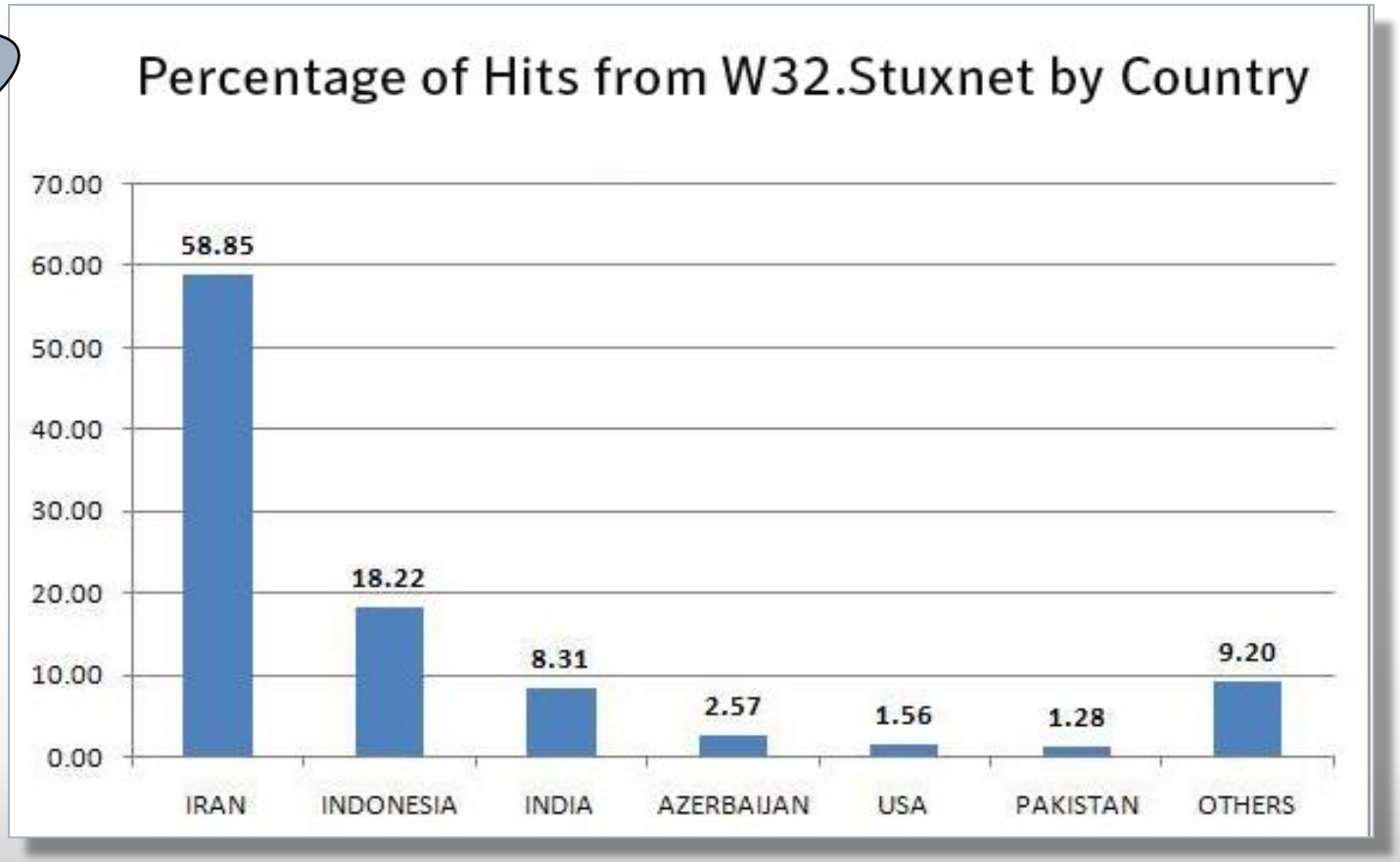
جنگ سایبری (۳)

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

جنگ سایبری (۴)

حمله اسراییل به تاسیسات هسته‌ای ایران: Stuxnet

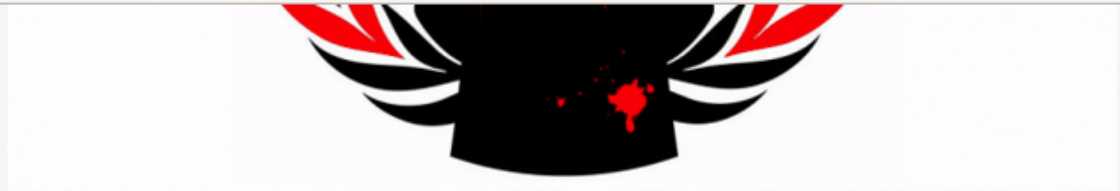
پخش مستند



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**

www.digitaltrends.com/computing/anonymous-leaks-10000-top-secret-iranian-govt-emails/



Hacker group Anonymous has leaked 10,365 “top secret” emails from Iran’s Ministry of Foreign Affairs. Anonymous says the files were accessed after the group infiltrated the Iranian Passport and Visa Office email center. All the files are currently available for download from MediaFire , as well as various BitTorrent sources.

Most of the emails concern visa applications for “an oil meeting,” according to an unnamed source who spoke with the *International Business Times*. And “many” of those are reportedly for people “from China.” A quick perusing of the files shows that, in most case, the emails are from Iranian government officials alerting visa applicants of their status.

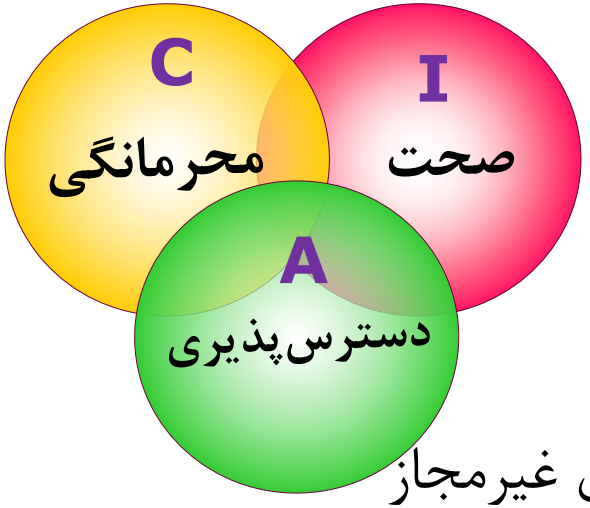
The initial attack apparently took place a number of days ago, and the Iranian government has been actively trying to keep news of the breach covered up. An Anonymous member said that the attacks were carried out in an attempt to damage Iran’s image in “both cyber space and the real world.” Tehran has yet to admit publicly that the breach and data theft even occurred.

فهرست مطالب

مفـــاهیم اولیـــه

مبانی امنیت داده‌ها

امنیت داده‌ها: مبتنی است بر تحقق سه اصل 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

محرمانگی

- محرمانگی پنهان کردن داده‌ها و یا منابع است.
- رعایت اصل محرمانگی اطلاعات تضمین می‌کند که
  - هر موجودیتی فقط به اندازه مجوزهایی که دارد می‌تواند به اطلاعات دسترسی پیدا کند. غالباً منظور از دسترسی، خواندن (مشاهده کردن) با فهم داده‌ها است.
- این اصل زمانی نقض خواهد شد که
  - یک کاربر غیرمجاز به منابع دسترسی پیدا کند. برای مثال شنود داده‌های طبقه‌بندی شده
- محرمانگی داده‌ها برای داده‌های ذخیره شده مثلاً محرمانه ماندن فایل‌های ثبت رخداد (Log Files)
- برای داده‌های در حال انتقال مثلاً مکالمات وُیْپ (Voice over Internet Protocol =VoIP)

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.

دسترس‌پذیری

- تعریف: دسترسی به داده‌ها و سرویس‌دهی به افراد مجاز در هر مکان و در هر زمان.
- به این مثال دقت کنید: اگر کامپیوتر خود را خاموش کنید و درون گاوصندوق قرار دهید محرمانگی اطلاعات و صحت اطلاعات حفظ می‌گردند اما اصل دسترس‌پذیری برقرار نخواهد بود پس امنیت وجود ندارد.

دلایل ناامنی شبکه‌ها

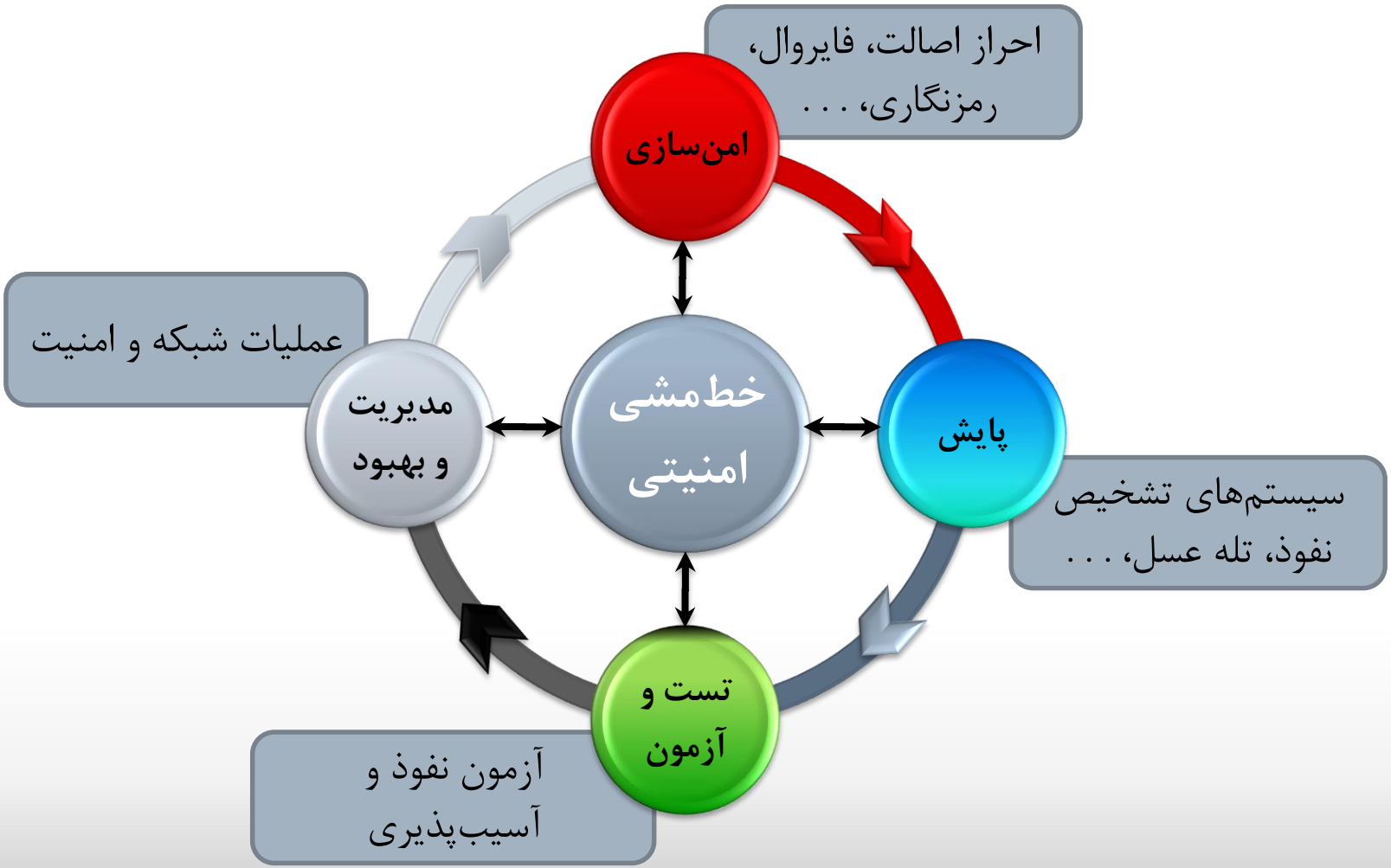
- ضعف فناوری
  - پروتکل، سیستم عامل، تجهیزات
- ضعف تنظیمات
  - رهاکردن تنظیمات پیش‌فرض، گذرواژه‌های نامناسب، عدم استفاده از رمزنگاری، راه‌اندازی سرویس‌های اینترنت بدون اعمال تنظیمات لازم، ...
- ضعف سیاست‌گذاری
  - عدم وجود سیاست امنیتی
  - عدم وجود طرحی برای مقابله و بازیابی مخاطرات
  - نداشتن نظارت امنیتی مناسب (مدیریتی و فنی)

ضعف مدیریتی

امن‌سازی

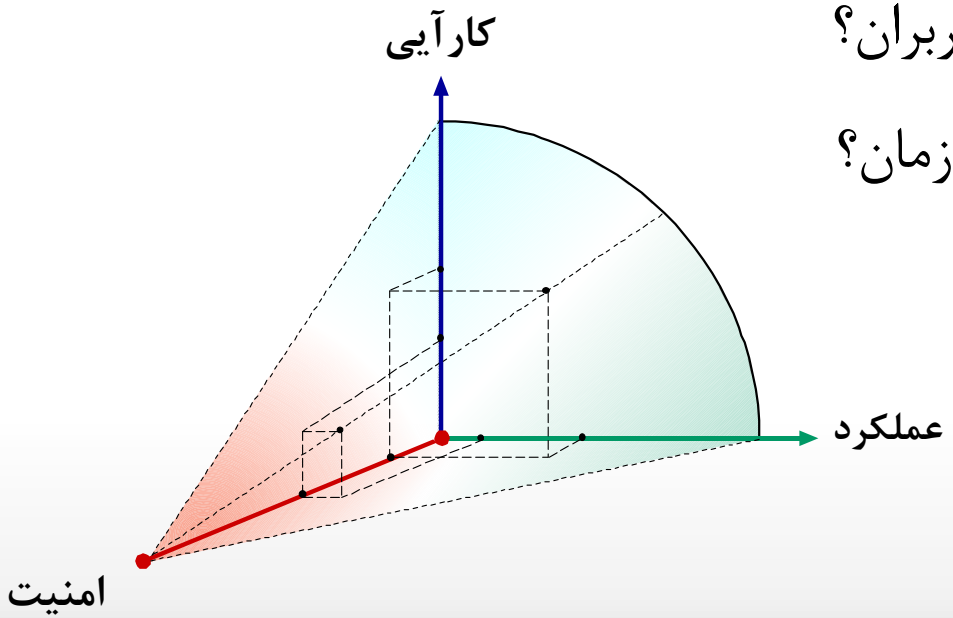
- گستره امنیت تمامی منابع سازمان است و نه تنها کارگزار اصلی.
- نگرش مدیریتی به مسئلهٔ امنیت لازم است و نه نگرش فنی.
- مهاجمین داخلی و مجاز خطر بالقوهٔ بیشتری دارند.
- مادام که انسان‌ها امن فکر نکنند نمی‌توان تراکنش امن داشت.
- امن‌سازی یک فرآیند است نه یک وظیفه خاص و مقطعی.

چرخه ایجاد امنیت



استراتژی امنیت سازمانی

- مصالحه بین امنیت، کارآیی و عملکرد.
- 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 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

- **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 (در این درس...)

- **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).

تعاریف 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 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

- 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

معماری امنیتی OSI

- مسئله: ارزیابی مؤثر نیازهای امنیتی سازمان (چه خط مشی امنیتی داشته باشد، چه محصول امنیتی داشته باشد)
- استاندارد ITU-T X.800، با نام معماری امنیتی OSI یک رویکرد سیستماتیک را برای فراهم کردن امنیت معرفی می‌کند.
- این استاندارد روی سه مفهوم زیر تمرکز می‌کند
  - حملات امنیتی
  - مکانیزم‌ها
  - سرویس‌ها

*The International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) is a United Nations-sponsored agency that develops standards, called Recommendations, relating to telecommunications and to open systems interconnection (OSI).

معماری امنیتی OSI (ادامه)

- **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.

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:** 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

سرویس های 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 + احراز اصالت

سرویس های امنیتی

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

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

مکانیزم‌های امنیتی

- مکانیزم‌ها به دو دسته تقسیم می‌شوند:
  - مکانیزم‌های خاص پروتکل یک لایه مثل TCP یا لایه کاربرد
  - مکانیزم‌هایی که مربوط به پروتکل لایه و سرویس امنیتی خاصی نیستند

Table 1.3 Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

رابطه بین سرویس امنیتی و مکانیزم

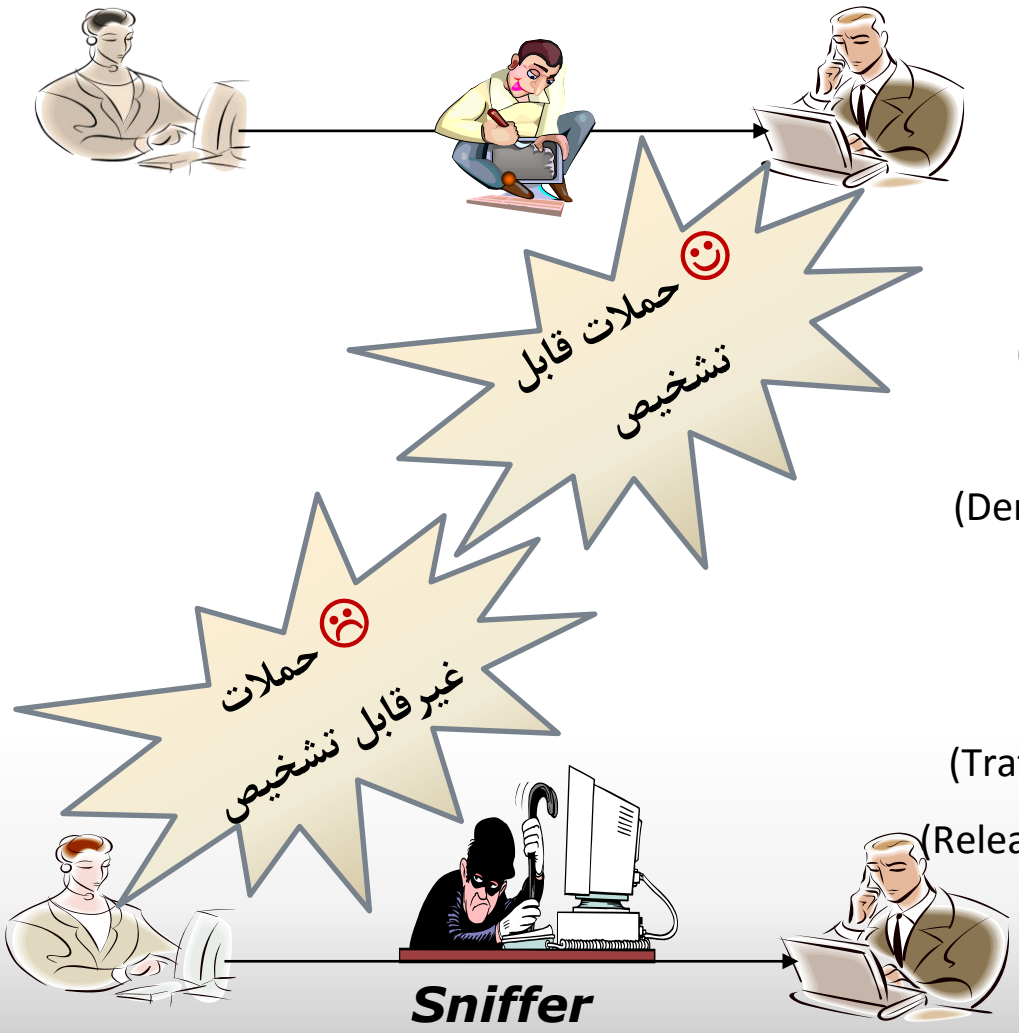
Table 1.4 Relationship Between Security Services and Mechanisms

	Mechanism							
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			

فهرست مطالب

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

انواع حملات (ادامه)



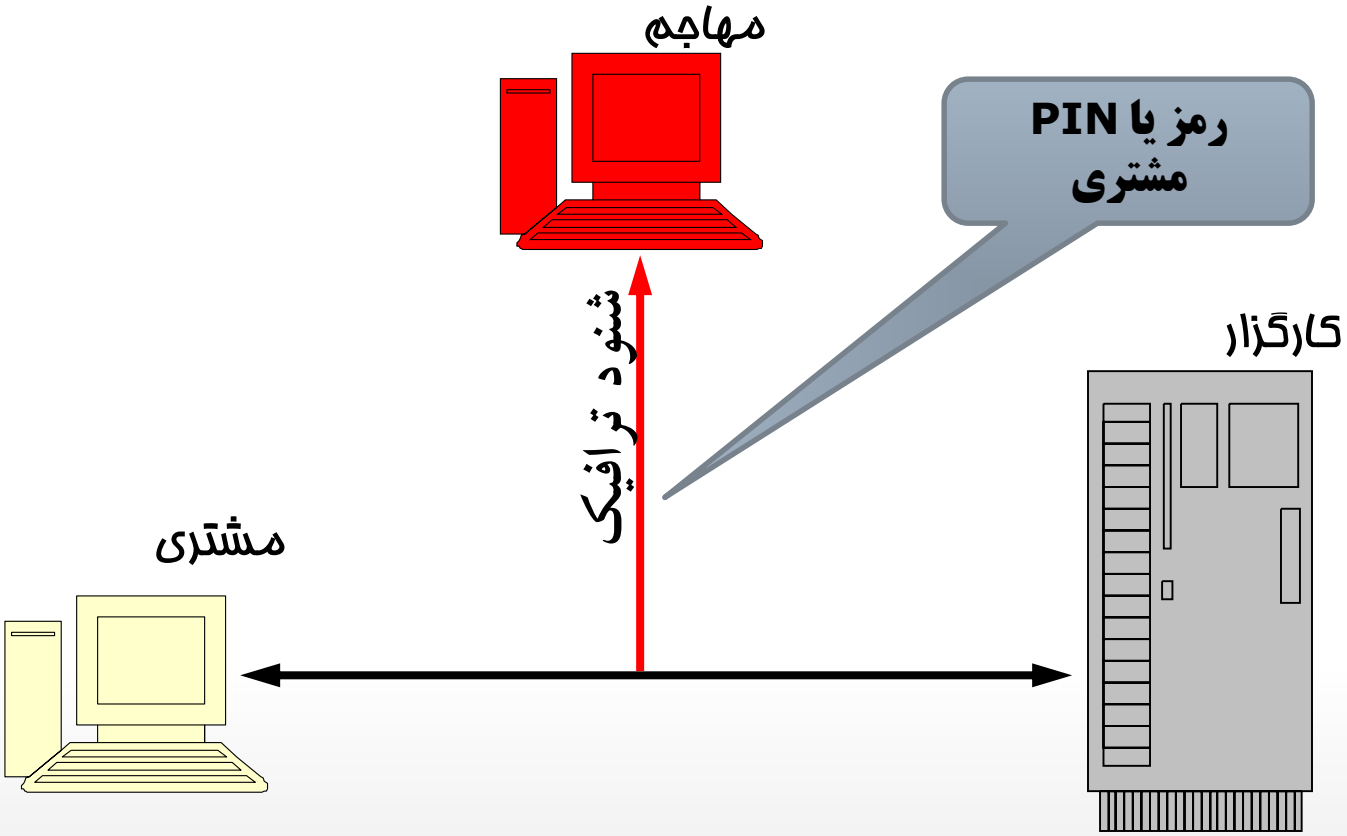
انواع حملات از نظر تاثیر:

- **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)

حمله شنود یا استراق سمع

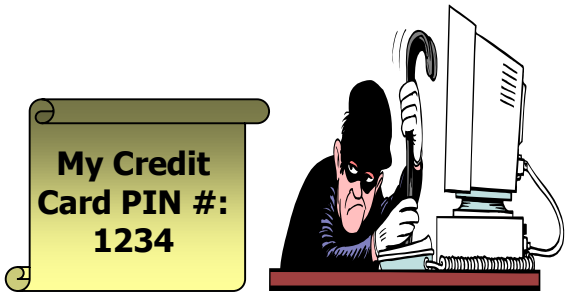
- هدف: نقض محرمانگی
- نتیجه: دسترسی غیرمجاز به داده‌های طبقه‌بندی شده
- راه‌های تحقق حمله:
  - اتصال فیزیکی به شبکه و دریافت بسته‌ها
  - دسترسی غیرمجاز به پایگاه‌داده‌ها
  - وجود ضعف و آسیب‌پذیری در سیستم کنترل دسترسی

حمله شنود یا استراق سمع (ادامه)



محرمانگی

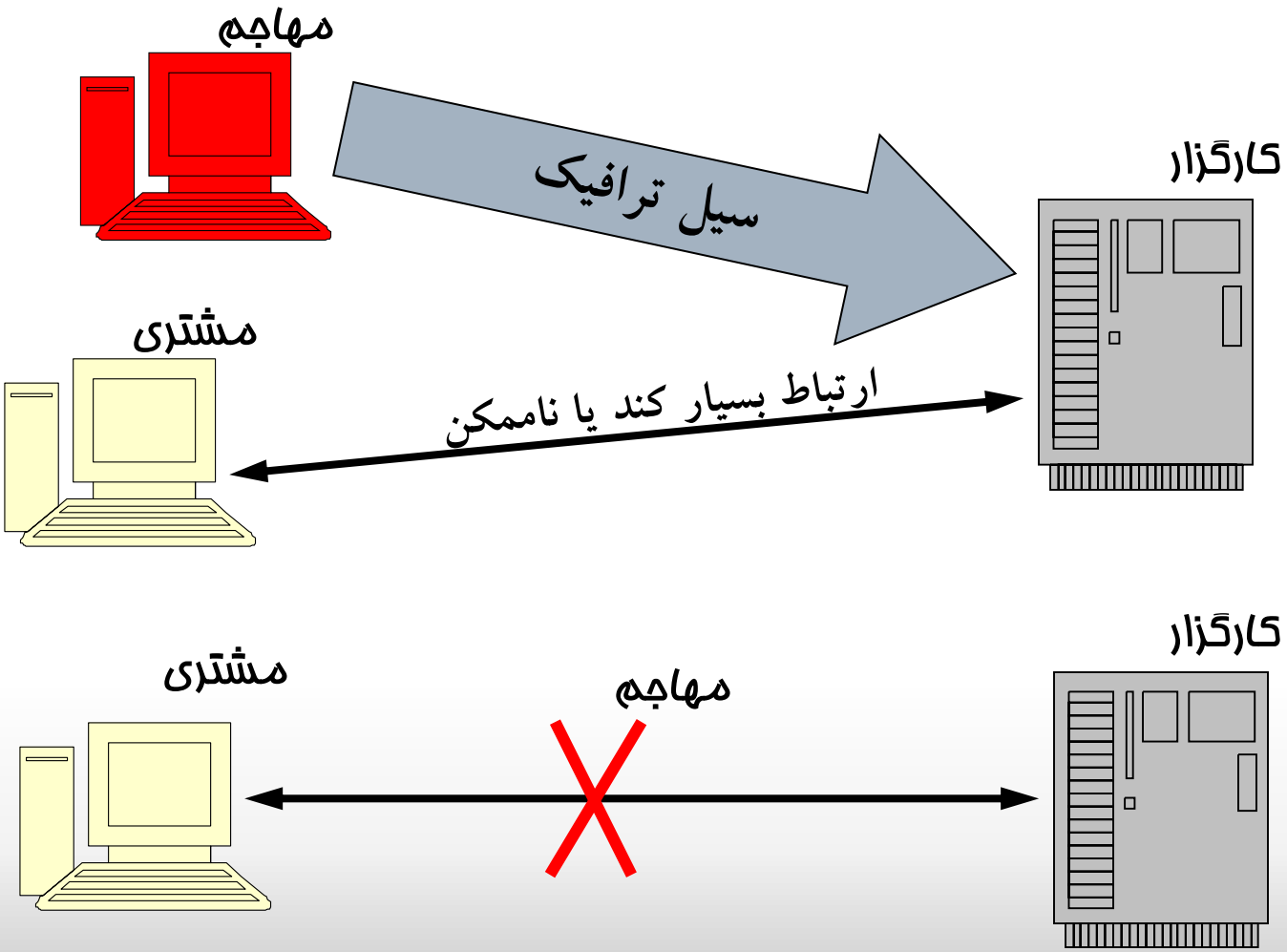
- روش‌های دستیابی به محرمانگی داده‌ها
  - رمزنگاری
  - کنترل دسترسی



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)

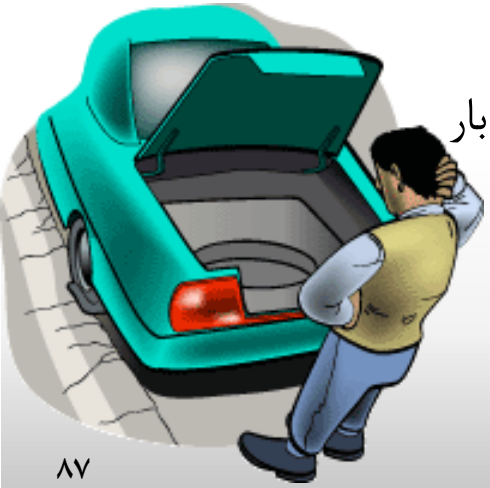


دسترس‌پذیری

- تعریف: دسترسی به داده‌ها و سرویس‌دهی به افراد مجاز در هر مکان و در هر زمان.
- به نقض اصل دسترس‌پذیری، حمله منع خدمت (منع سرویس) گفته می‌شود (Denial of Service = DoS).
- انجام این حمله با استفاده از چند منبع، منجر به ایجاد حمله منع سرویس توزیع شده می‌شود(Distributed DoS = DDoS).

دسترس‌پذیری

- حمله منع خدمت به روش‌های زیر انجام می‌گیرد:
  - اشغال منابعی مانند پردازنده، حافظه و پهنای باند (محدود بودن منابع)
  - ایجاد اختلال در اطلاعات پیکربندی مانند اطلاعات مسیریابی (توانایی تغییر اطلاعات پیکربندی)
  - اختلال در تجهیزات فیزیکی شبکه
- برای تأمین اصل دسترس‌پذیری راه‌حل استاندارد و معینی (مثل راه‌حل‌های ارائه شده برای دو اصل قبل) وجود ندارد اما راه‌حل‌های دفاعی به طور کلی دو خط مشی را در پیش می‌گیرند:
  - قرار دادن منابع جایگزین
  - وجود پشتیبان، تکرار داده و سرویس، به همراه سیستم‌های پایش و توزیع بار
  - مسدود سازی درخواست‌ها برای اخذ منابع و خدمات

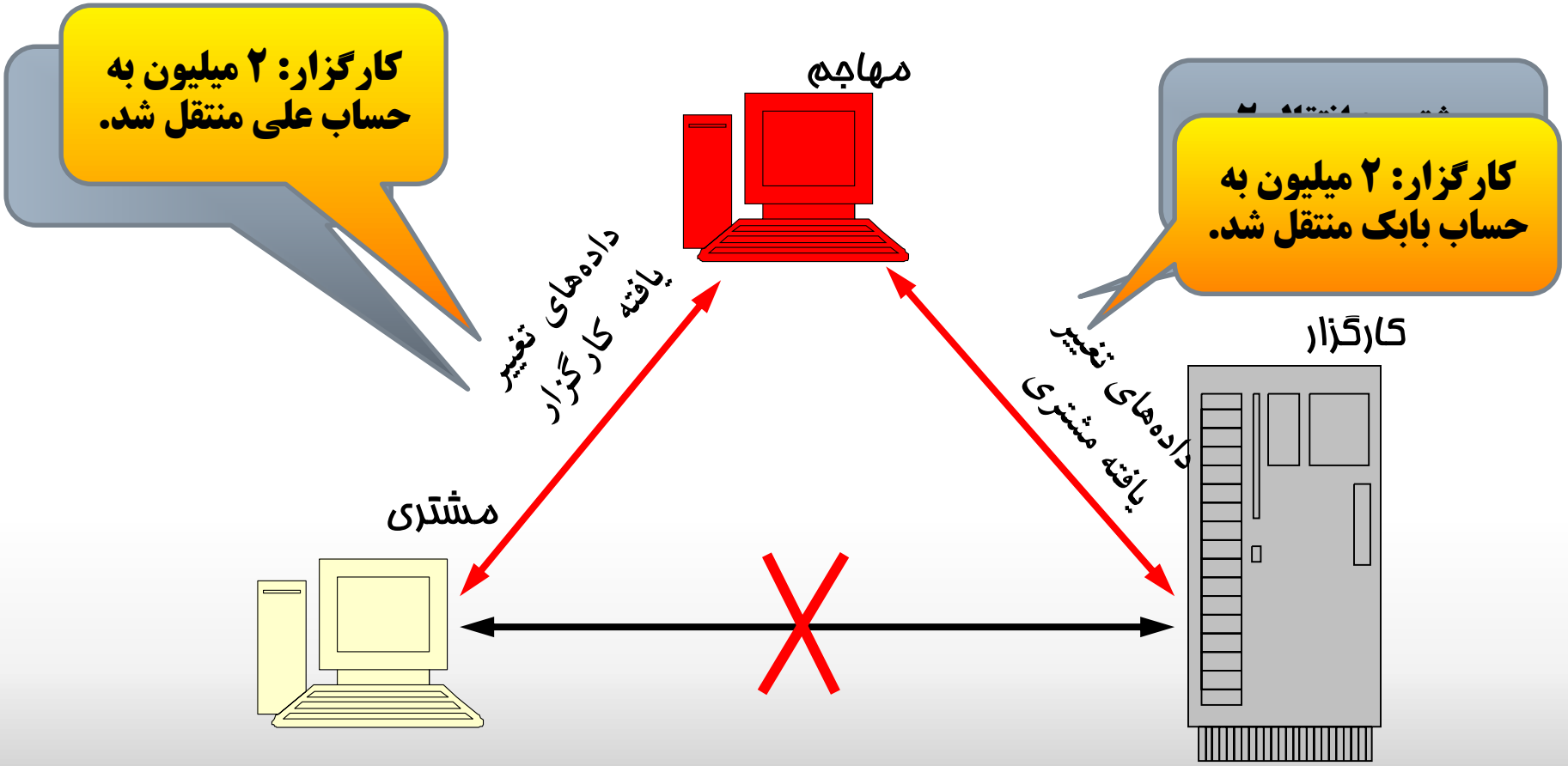


حمله تغییر یا دستکاری داده‌ها

- 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)

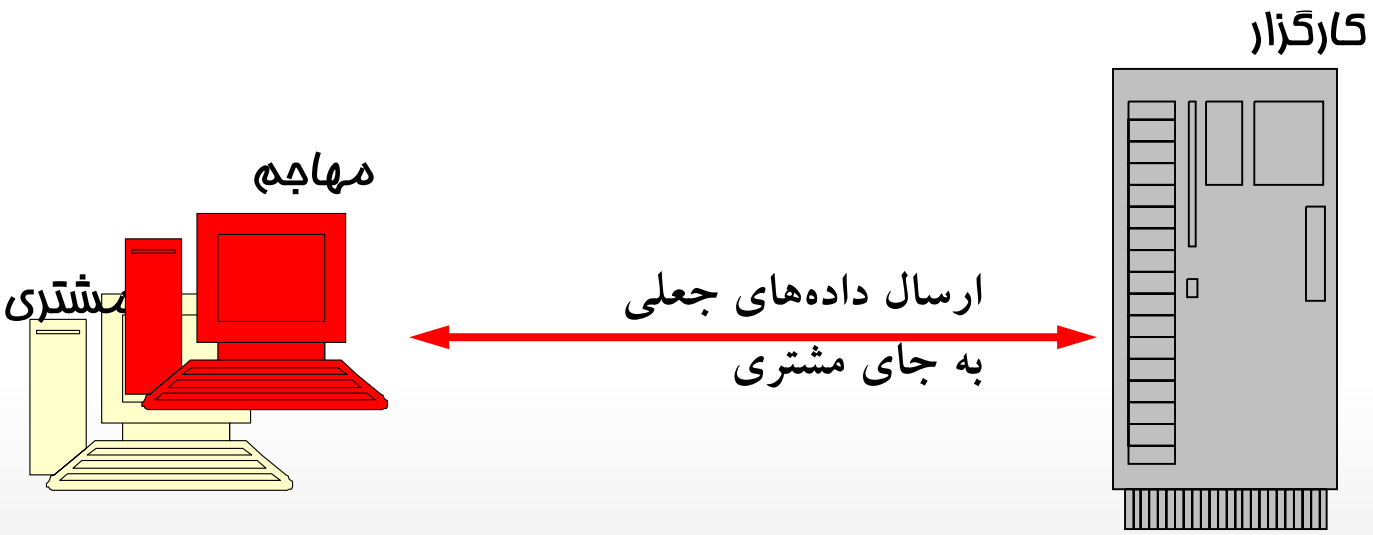


حمله جعل هویت

- هدف: نقض صحت
- نتیجه: جعل (یا 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

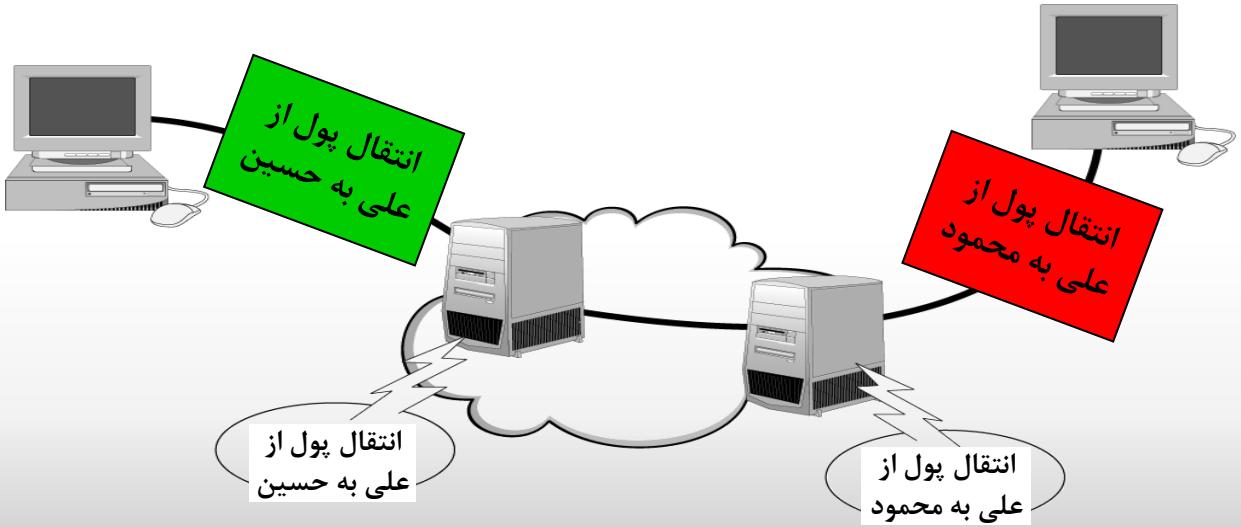
حمله جعل هویت (ادامه)

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



صحت

- مکانیزم‌های متداول:
  - امضای دیجیتال: مفهوم امضای دیجیتال شبیه به مفهوم امضا کردن یک سند در دنیای واقعی است
  - کد احراز اصالت پیام (Message Authentication Code =MAC)
  - کنترل دسترسی



تعریف کنترل دسترسی

کنترل دسترسی: دسترسی کاربران به منابع اطلاعاتی سیستم مطابق قوانین خاصی کنترل می‌شود.

- درجات مختلف دانه بندی برای دسترسی
  - برای پایگاه داده های رابطه ای: رابطه ها، تاپلها ، پایگاه داده ها
- حالات دسترسی مختلف
  - کنترل دسترسیهای مختلف با توجه به نوع عمل باید اِعمال گردند
  - مثلاً میان خواندن(read) و نوشتن(write) باید تمایز قائل شد.
- مجازشماری پویا
  - سمپاد (DBMS) باید تغییرات مجازشماریهای کاربران در حین اینکه پایگاه داده ها عملیاتی است را پشتیبانی نماید.

حـــــریم خصـــوصی

تعریف حریم خصوصی

- شامل هر نوع اطلاعات شخصی
- حفظ حریم خصوصی: حق افراد برای مشخص کردن اینکه اطلاعات شخصی خودشان *چه زمانی*، *چگونه* و *به چه میزانی* میتواند به دیگران منتقل گردد.
  - داده ها برای اهداف خاص جمع آوری می شوند.
  - هدف یا اهداف باید به همراه داده ذخیره شوند
  - هدف، نحوه استفاده از داده را محدود می کند.

حریم خصوصی – اصول پایه‌ای

- توصیف هدف(Purpose Specification)
  - هدف جمع آوری اطلاعات شخصی باید در کنار داده ها نگه داشته شوند
  - مثال: فروشنده کتاب، اطلاعات شخصی را برای آمار خریدها، توصیه کتاب به مشتری و ... نگه می دارد.
- توافق(Consent)
  - در مورد هدف بایستی توافق همه کسانی که مصادیق اطلاعات هستند وجود داشته باشد
  - مثال: خریدار می تواند برای خرید توافق خود را اعلام نماید ولی از سرویس توصیه کردن کتاب اجتناب نماید
- مجموعه محدود(Limited Collection)
  - مینیمم اطلاعات و در حد نیاز باید جمع آوری گردد
  - مثال: خریدار برای استفاده از سرویس توصیه کردن کتاب نیازی به ارائه شماره کارت اعتباری اش ندارد
- استفاده محدود(Limited Use)
  - تنها باید پرس و جوهایی توسط پایگاه داده اجرا گردد که سازگار با هدف باشد
  - مثال: یک پرس و جو برای توصیه کردن کتاب نمی تواند به آدرس تحویل کتاب دسترسی داشته باشد
- افشای محدود(Limited Disclosure)
  - افشای اطلاعات باید تنها در حدی باشد که توافق شده و سازگار با هدف است.
  - مثال: شرکت حامل کتاب نیازی به دانستن شماره کارت اعتباری خریدار ندارد.

حریم خصوصی – اصول پایه‌ای

- نگهداری محدود(Limited Retention)
  - اطلاعات باید در تنها تا زمانی نگه داشته شوند که مورد نیاز می باشند.
  - مثال: زمانی که خرید کتاب انجام شد، دیگر نیازی به نگه داشتن شماره کارت اعتباری نمی باشد.
- دقت(Accuracy)
  - اطلاعات شخصی نگه داشته شده در پایگاه داده ها باید دقیق و به روز باشد .
  - مثال: آدرس ارسال کتاب باید در پایگاه داده ها معتبر و دقیق باشد.

- ایمنی(Safety)
  - در مقابل هر نوع تخطی مانند دزدی اطلاعات باید ایمن باشد.
  - مثال: داده ها را باید رمز شده نگه دارد.
- باز بودن(Openness)
  - صاحب اطلاعات باید به تمام اطلاعات ذخیره شده در پایگاه داده ها مربوط به خودش دسترسی داشته باشد
  - مثال:کاربران می توانند به تمام سوابق خرید خود و اطلاعات شخصی خود دسترسی برای دیدن داشته باشند
- ایجاب(Compliance)
  - صاحب اطلاعات باید از اجابت شدن تمام توافقاتش، مطمئن باشد
  - مثال: ثبت تمام دسترسی ها به اطلاعات شخصی بطوریکه زمان و قلم داده مورد دسترسی را بتوان بدست آورد

رابطه رمزنگاری، حریم خصوصی و اصل محرمانگی؟

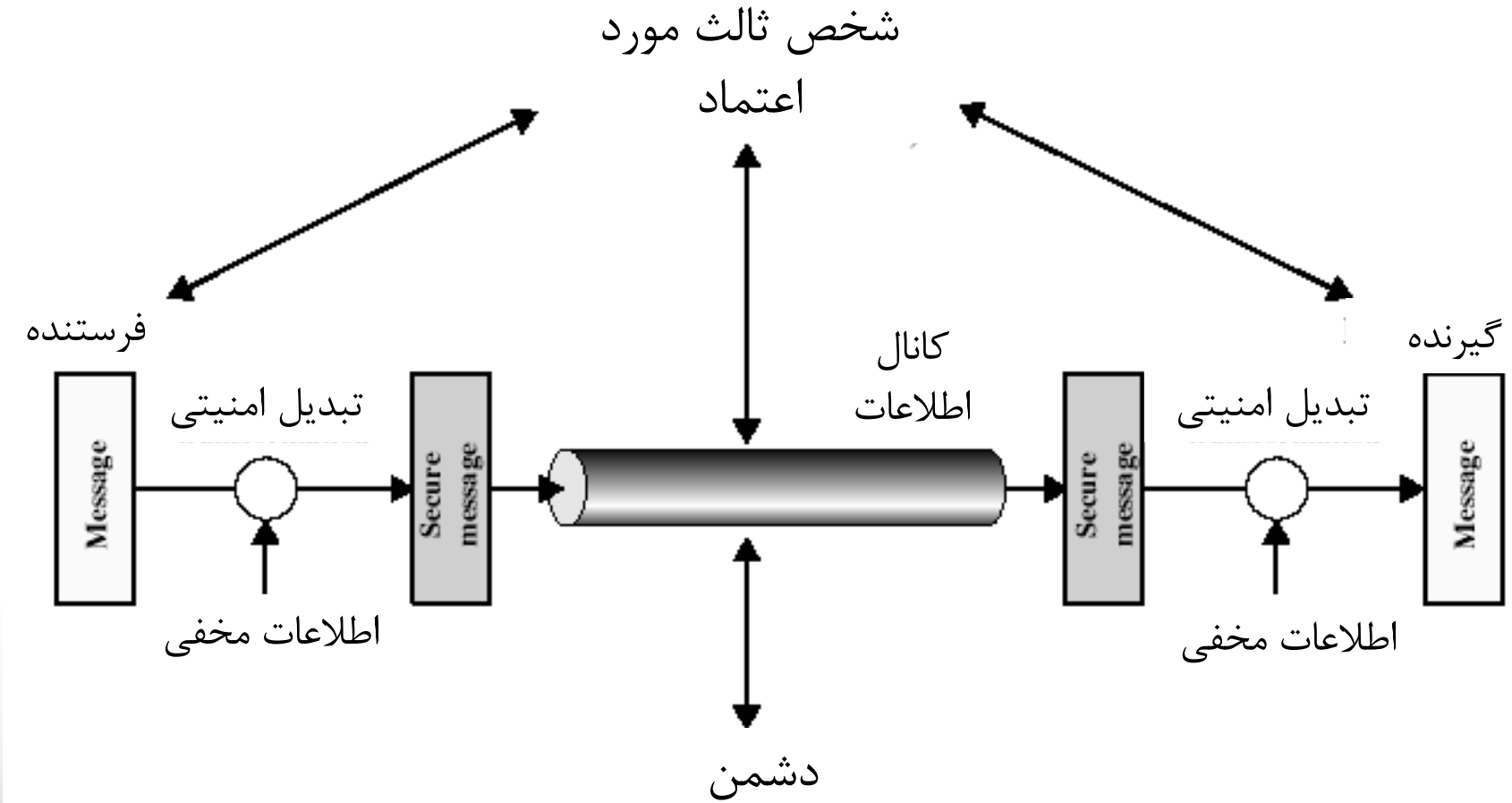
فهرست مطالب

- 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 سرویس‌های امنیتی موردنیاز
  - اطلاعات مخفی: که در تبدیل فوق مورداستفاده قرار می‌گیرند و به نحوی بین طرفین ارتباط به اشتراک گذاشته شده‌اند.

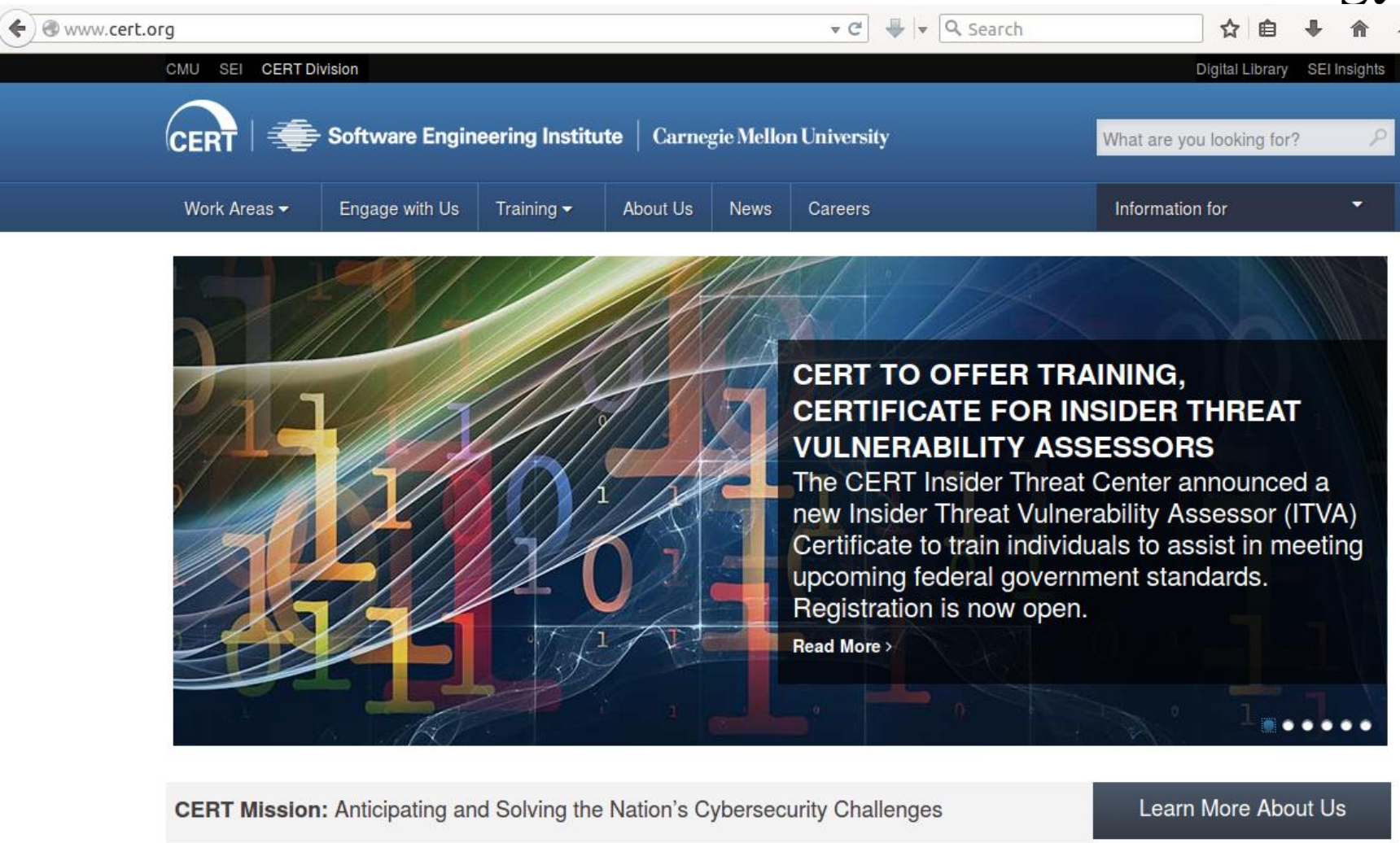
یک مدل نمونه برای ارتباط امن



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

تارنمای CERT



تارنمای مرکز ماهر

www.certcc.ir

مرکز ماهر

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معرفی مرکز ماهر | اطلاع رسانی | پایگاه دانش | رویدادها | تماس با ما

هزاران سرور ویندوز در معرض خطر هک

هزاران ویندوز سرور ۲۰۰۳ قدیمی، به روز رسانی نشده و از رده خارج شده هم چنان در حال کار می باشد که کاربران را در معرض خطر حملات هک قرار می دهد.

بیشتر

راهنمایی های امنیتی

- چندین آسیب پذیری در Pale Moon
- دو آسیب پذیری در Cyberfox
- به روز رسانی Oracle Linux برای ...
- به روز رسانی Ubuntu برای firefox
- به روز رسانی Ubuntu برای thunderbird

آرشیو

دریافت گزارش آسیب پذیری ها، نقص های امنیتی محصولات نرم افزاری و سخت افزاری داخلی و خارجی

تلفن : ۰۲۱-۲۲۱۱۵۹۵۰-۴۲۷۵۰۰۰۰

نمابر : ۰۲۱-۲۲۱۱۵۹۵۱

پست الکترونیکی :

cert@certcc.ir

هک برخی از دستگاه های سیسکو

انتشار اصلاحیه فوری و خارج از ...

اصلاح آسیب پذیری Ins•mnia در ...

انتشار اصلاحیه فوری ادوب برای ...

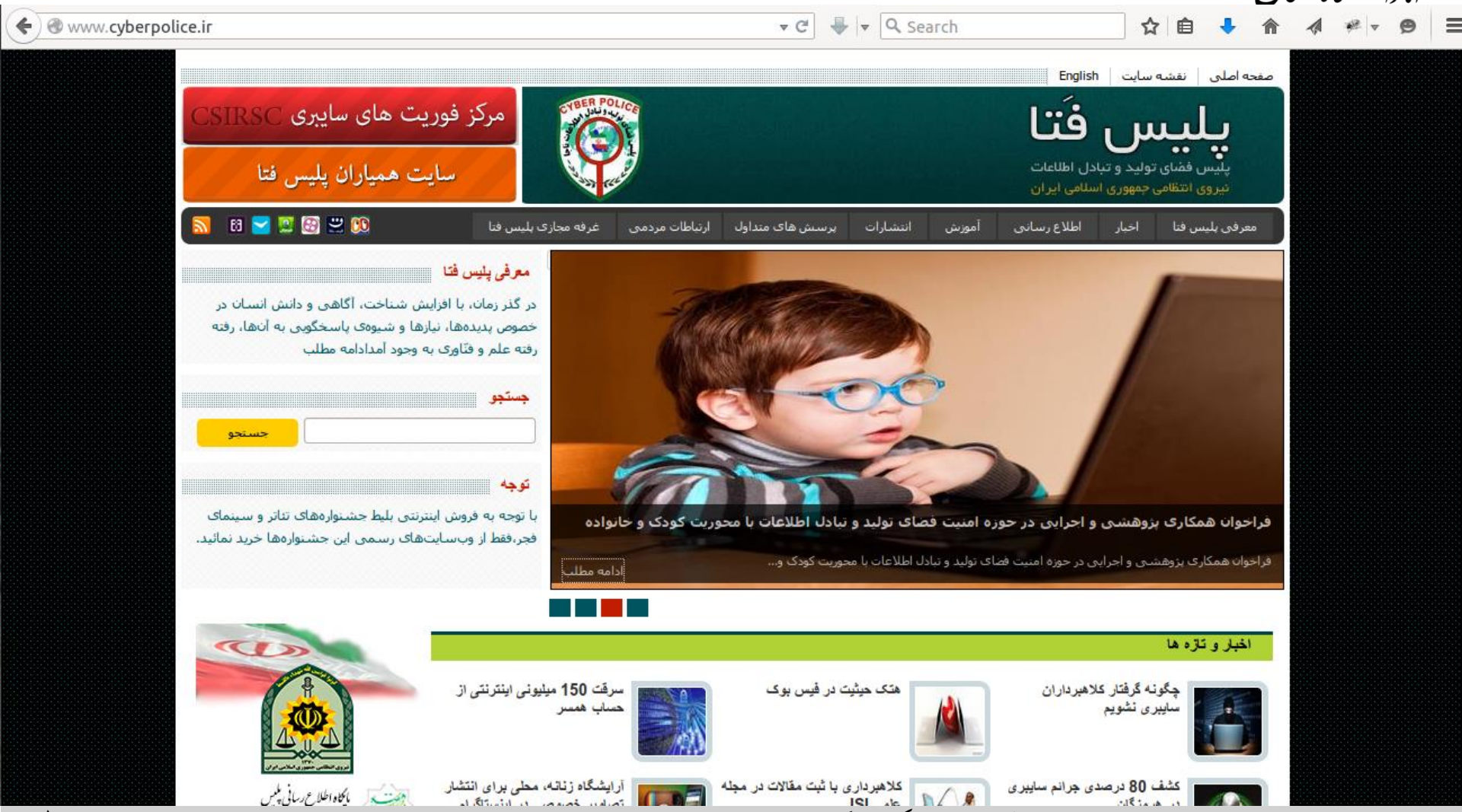
اصلاح ۲۹ آسیب پذیری در آخرین ...

گزارشات تحلیلی

مقالات

سایر اخبار

تارنمای پلیس فتا



منابع

- اسلایدهای دکتر مرتضی امینی (منبع اصلی) – درس امنیت داده و شبکه
- اسلایدهای دکتر رسول جلیلی- درس امنیت پایگاه داده‌ها
- Cryptography and Network Security Principles and Practices, By William Stallings 5th Edition
- Understanding Operating Systems, Ann McIver McHoes, Ida M. Flynn, 6th and 7th edition