دانشگاه شهید بهشتی
دانشکده‌ی مهندسی و علوم کامپیوتر

# مقدمه

## امنیت شبکه‌های کامپیوتری

دکتر مقصود عباسپور

# محتویات درس

- **مقدمه‌ای بر امنیت کامپیوتر و شبکه**

- **بررسی امنیت در لایه‌های مختلف**
  - امنیت کاربرد
  - امنیت سیستم عامل
  - امنیت وب
  - امنیت شبکه

# اطلاعات کلی

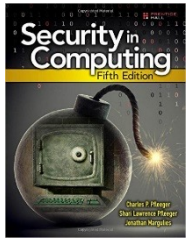
- **پیشنیازها :**
  - شبکه های کامپیوتری
  - سیستم عامل
  - زبان برنامه نویسی
- **ارزیابی :**
  - امتحان ۱۴ نمره
  - تکالیف ۲ نمره
  - پروژه ۴ نمره
- **کمک استاد :**

# فهرست مطالب

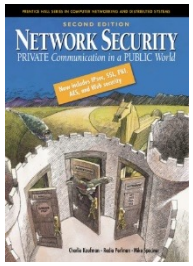
- ✓ تعاریف و اصطلاحات
- ✓ مقدمه‌ای بر رمزنگاری
- ✓ امنیت نرم افزار( Buffer Overflow) و راه های جلوگیری
- ✓ آسیب پذیری‌های پروتکل های اصلی شبکه ( IP-TCP-DNS-ARP )
- ✓ امنیت لایه ترانسپورت Secure Sockets Layer (SSL)
- ✓ امنیت شبکه (IPsec)
- ✓ Firewall
- ✓ Intrusion Detection Systems (IDS)
- ✓ مرکز عملیات امنیت و همبستگی هشدارها (Alert Correlation)
- ✓ حملات منع سرویس و راههای جلوگیری(Denial of Service)
- ✓ شبکه های بات

# منابع درس امنیت شبکه های کامپیوتری

- Charles P. Pfleeger, "**Security in Computing**", Fourth Edition.




- Kaufman, Perlman and Speciner, "**Network Security: Private Communication in a Public World**", Second Edition.

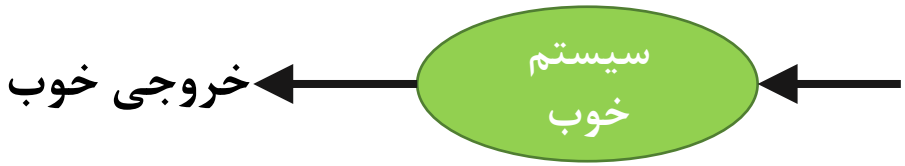



- Avinash Kak, - **Introduction to Computer Security**, Purdue University

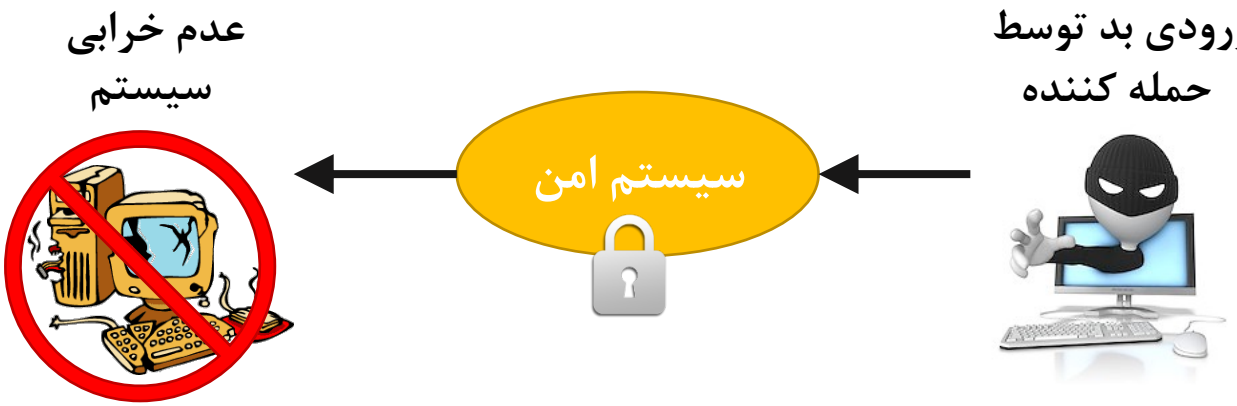
- Papers -- will be announced during the course

# امنیت چیست؟

## سیستم درست :




## امنیت :




- **سیستم خوب**
  امکانات بیشتر خوب است!
- **امنیت**
  امکانات بیشتر دردسر است!

# تعاریف

- تعریف امنیت
  - به معنی نبودن خطر و تهدید
  - محافظت از فرد/سازمان/کشور از خطرات و جنایات و تهدیدات
  - دفاغ از اطلاعات در مقابل دسترسی های غیر مجاز برای دیدن/تغییر/ داده سازی/تحلیل...
- امنیت داده های سایبری
  - محافظت از داده ها در فضای کامپیوتری و دیجیتال

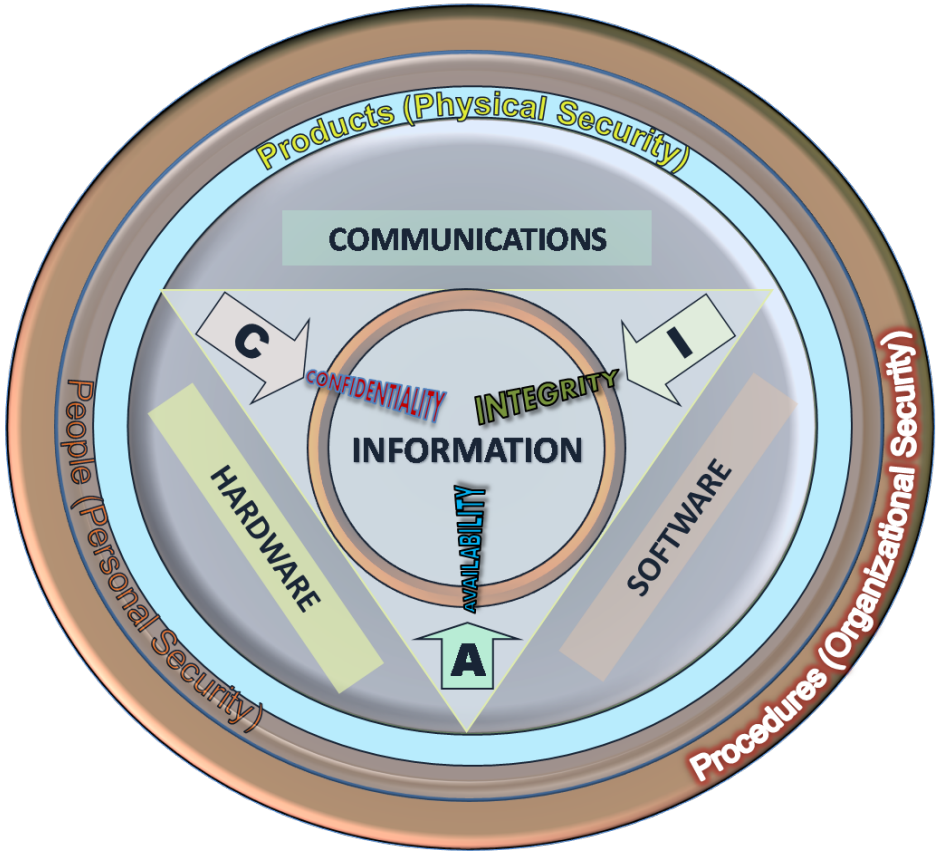
# امنیت فضای سایبری

امنیت فضای سایبری

- یک دیسیپلین است که شامل اجزاء مختلف
- مردم -تکنولوژی - اطلاعات - فرآیند ها برای اطمینان از عملکرد امن است
- شامل:
  - ایجاد فرایند های امنیتی
  - عملیات امنیت
  - تحلیل
  - آزمون
  - تحلیل/مدیریت ریسک
  - سیاست های امنیتی
  - قوانین امنیتی

An Introduction to Information Security and ISO27001:2013,
by Steve G Watkins, by IT Governance Publishing (2013)

# خصوصیات امنیت

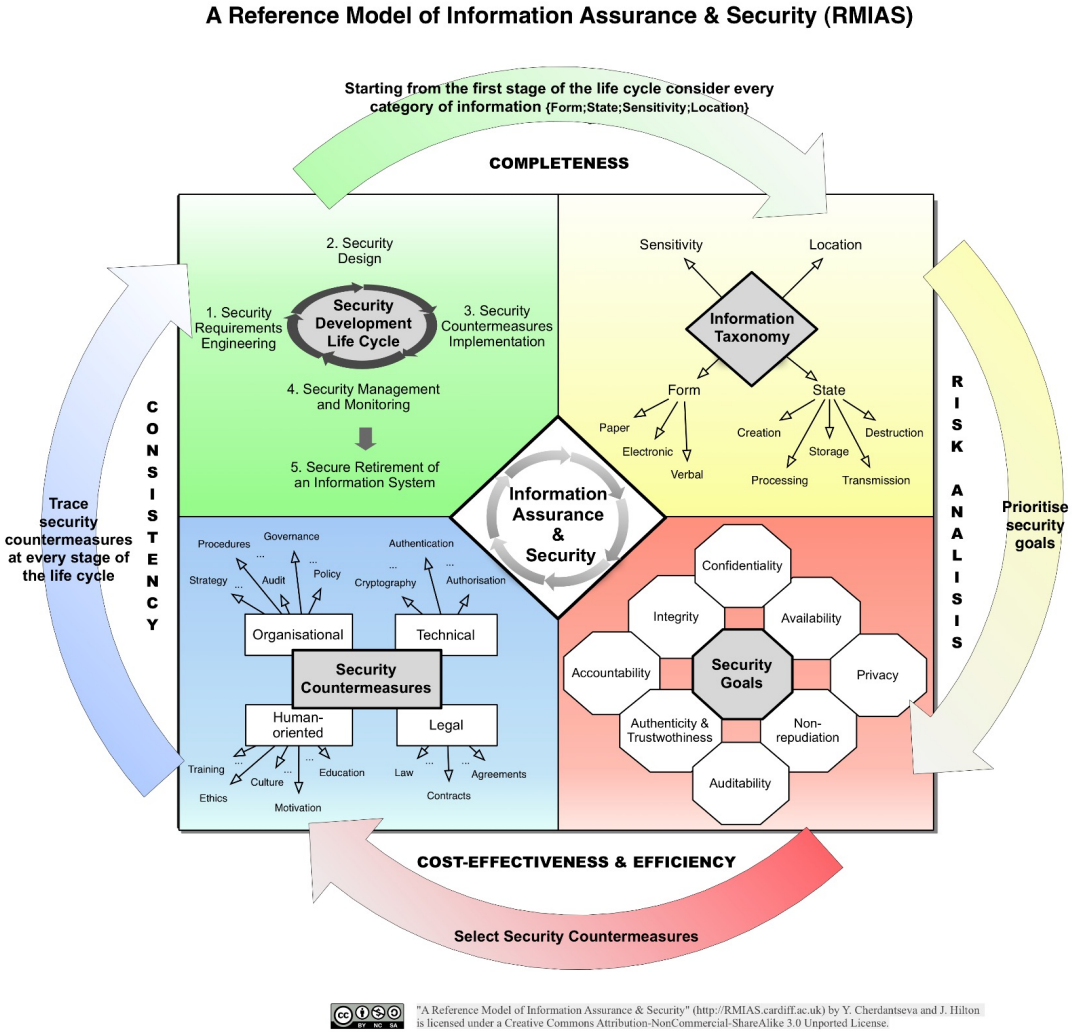



محرمانگی: عدم دسترسی عیر مجاز به اطلاعات
اصلی ترین مکانیزم: رمزنگاری

یکپارچگی: صحت اطلاعات عدم امکان تغییر، حذف و ایجاد اطلاعات
اصلی ترین مکانیزم: امضا دیجیتال

دسترسی پذیری: در زمان مورد نیاز اطلاعات/خدمات در دسترس باشد.
- تکنولوژی های مختلفی لازم دارد.

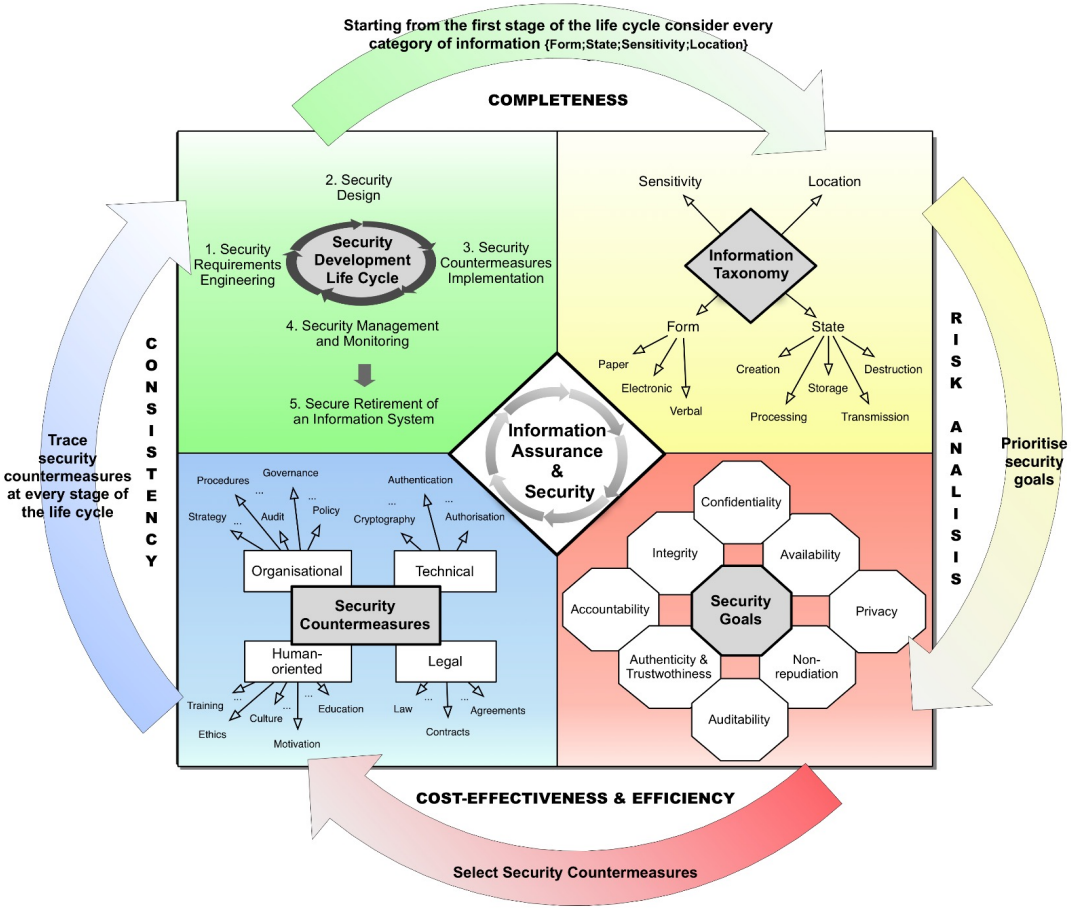
# خصوصیات امنیت مدل RMIAS



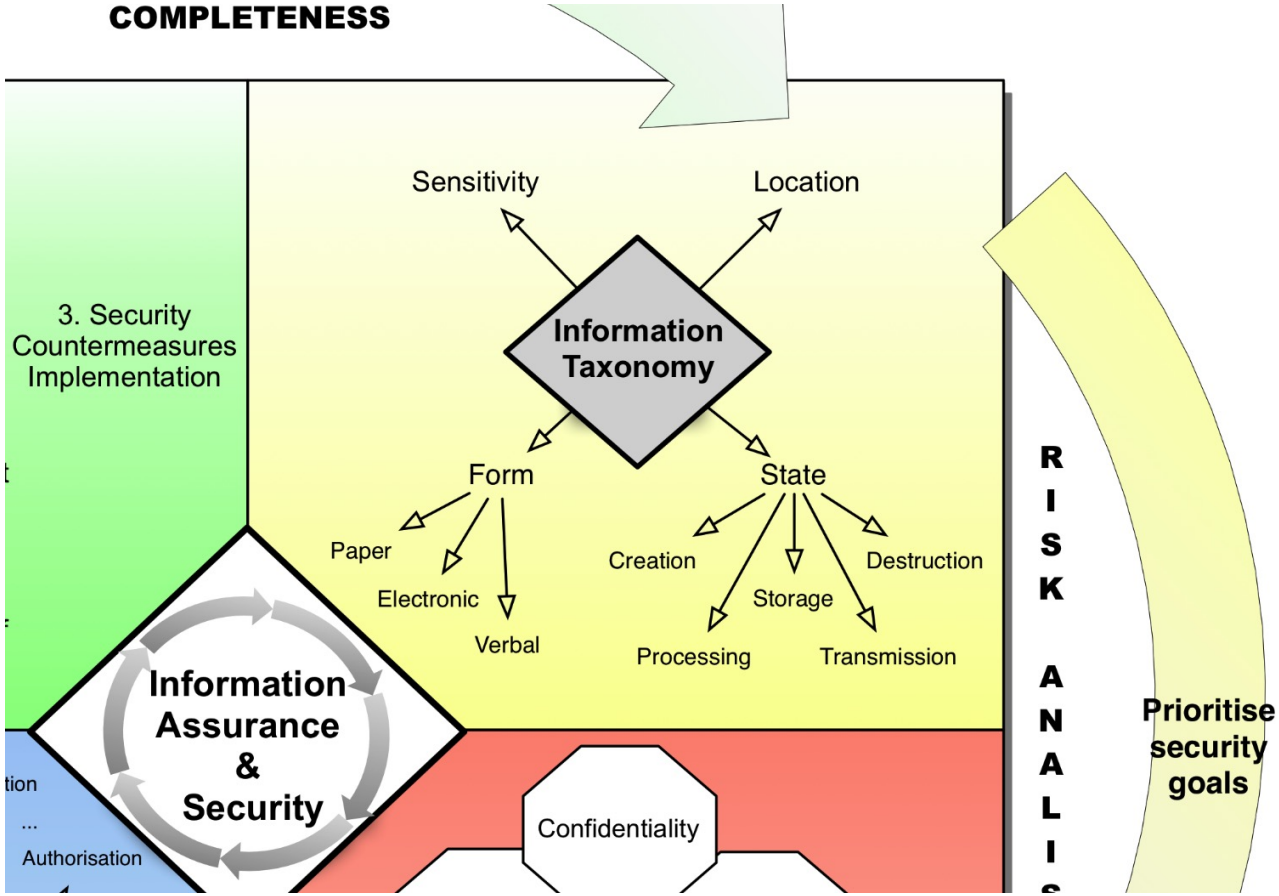



Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance & Security," Availability, Reliability and Security (ARES), 2013 Eighth International Conference on , vol., no., pp.546-555,

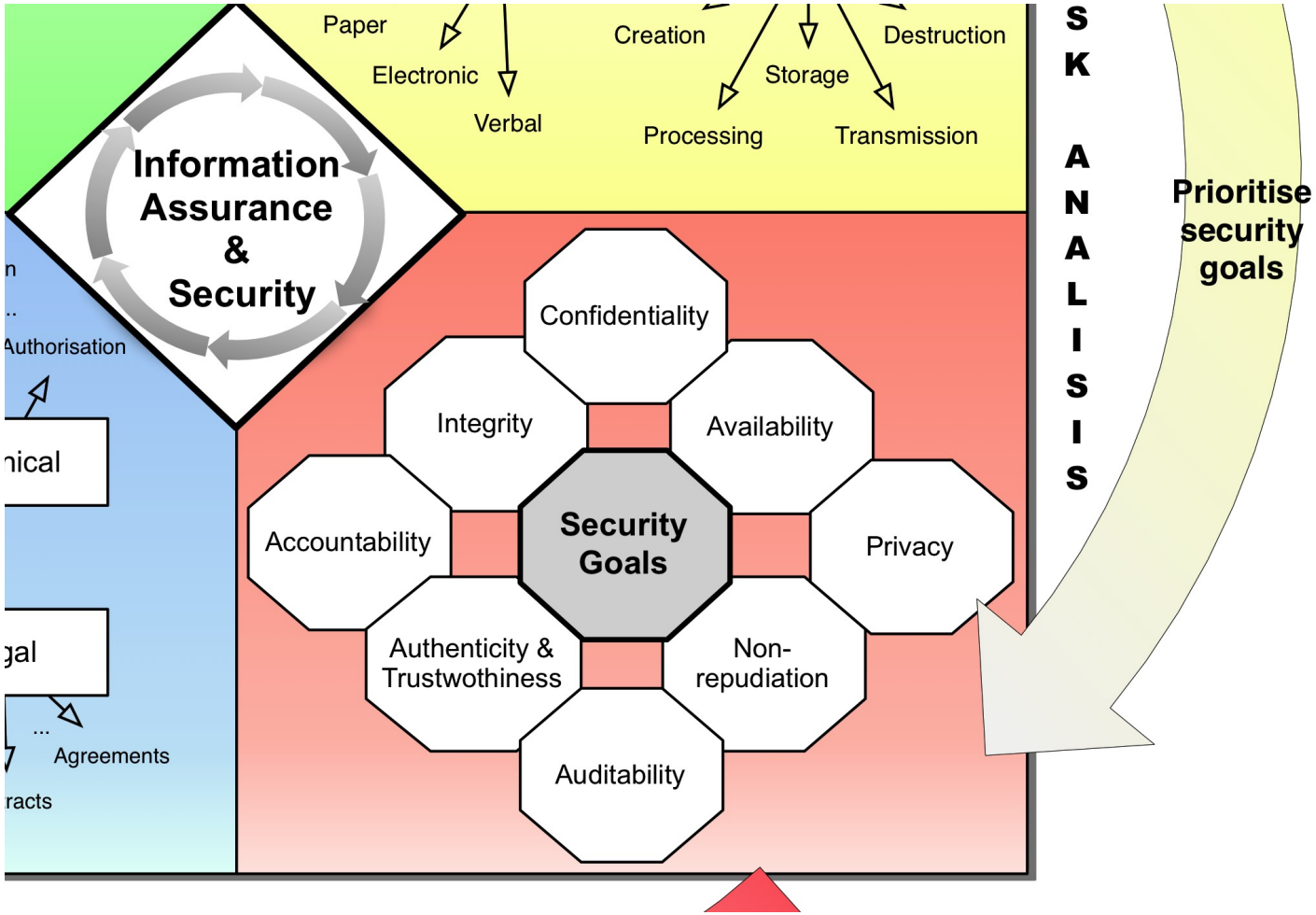
# خصوصیات امنیت مدل RMIAS



# خصوصیات امنیت مدل RMIAS



# خصوصیات امنیت مدل RMIAS



# خصوصیات امنیت مدل RMIAS

Table I
THE FINALISED LIST OF SECURITY GOALS

| Security Goal | Definition | Analysed Literature | Components of an Information System | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | Information | People | Processes | Hardware | Software | Networks |
| Accountability | An ability of a system to hold users responsible for their actions (e.g. misuse of information) | [22], [31], [32] | | X | | | | |
| Auditability | An ability of a system to conduct persistent, non-bypassable monitoring of all actions performed by humans or machines within the system | [33], [34], [35] | | | X | | | |
| Authenticity/Trustworthiness | An ability of a system to verify identity and establish trust in a third party and in information it provides | [13], [22], [23], [31], [35], [36] | X | X | X | X | X | X |
| Availability | A system should ensure that all system's components are available and operational when they are required by authorised users | [7], [13], [16], [22], [31], [35] | X | X | X | X | X | X |
| Confidentiality | A system should ensure that only authorised users access information | [7], [13], [16], [31], [36] | X | | | | | |
| Integrity | A system should ensure completeness, accuracy and absence of unauthorised modifications in all its components | [7], [13], [16], [22], [31], [35] | X | X | X | X | X | X |
| Non-repudiation | An ability of a system to prove (with legal validity) occurrence/non-occurrence of an event or participation/non-participation of a party in an event | [22], [31], [35], [36] | X | | X | | | |
| Privacy | A system should obey privacy legislation and it should enable individuals to control, where feasible, their personal information (user-involvement) | [32], [37], [38], [40], [39], [41] | X | X | | | | |

# خصوصیات امنیت مدل RMIAS

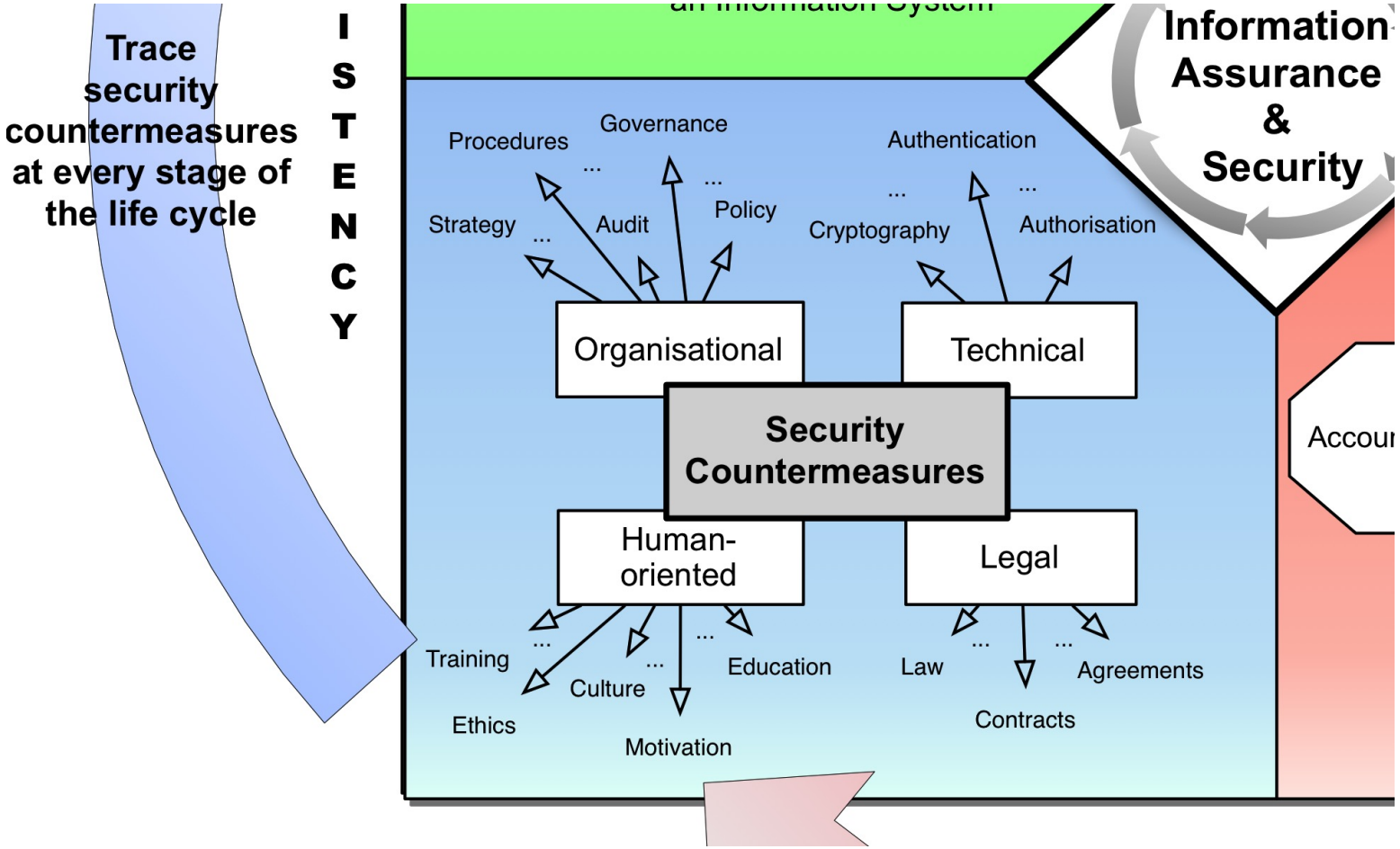
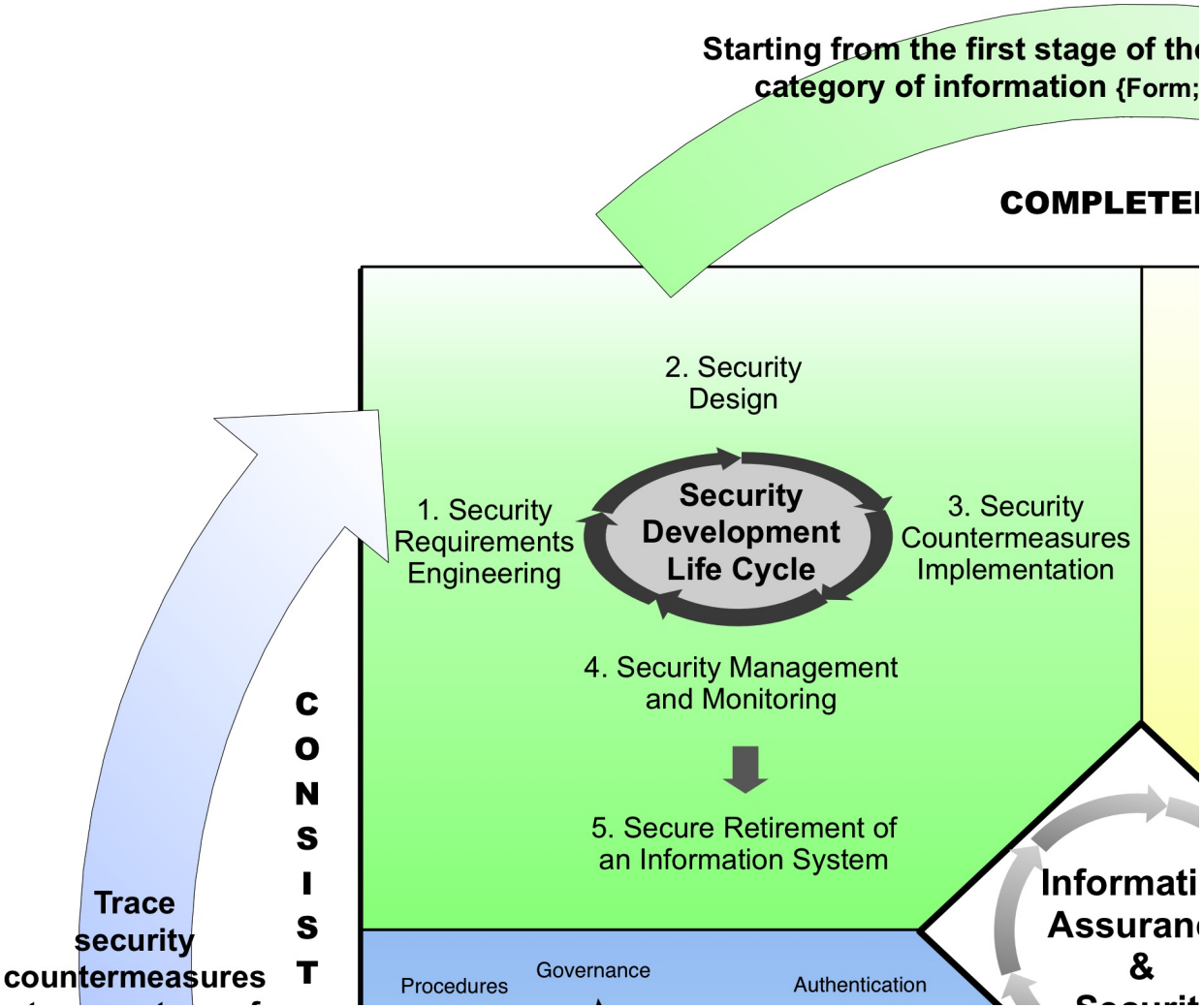


Table II
THE STRUCTURING OF AN INFORMATION SECURITY POLICY DOCUMENT USING THE RMIAS METHOD (EXCERPT)

| | **1. Form** | **2. Sensitivity** | **3. Location** | **4. State** | **5. Security Goal** | **6. Security Countermeasure Type: Description** |
|---|---|---|---|---|---|---|
| 1 | Paper | Secret | Controlled | Creation | Confidentiality | Organisational: *Apply Protective Marking (Avoid over or under marking*). |
| 2 | Any | Any | Controlled | Destruction | Availability | Organisational: *No information, held on any media, can be destroyed unless it has been reviewed.* |
| 3 | Paper | Confidential | Partially Controlled | Transmission | Accountability, Confidentiality | Organisational: *Documents marked CONFIDENTIAL may be taken home only with a written approval of a designated person. All actions with documents marked CONFIDENTIAL to be logged.* |
| 4 | Electronic | Protect | Uncontrolled | Storage, Processing | Confidentiality, Integrity | Technical: *Any data marked PROTECT must be encrypted when taken outside the office*. |

# خصوصیات امنیت مدل RMIAS



# اصطلاحات امنیتی

- ✓ **آسیب پذیری (Vulnerability) :**

یک خطا یا نقص در *طراحی*، *پیاده سازی* یا *عملیات* سیستم.

Attach password to monitor.

TLS heartbleed attack.

IP protocol doesn't have encryption.

- ✓ **حمله (Attack) :**

بهره برداری از آسیب پذیری‌های یک سیستم.

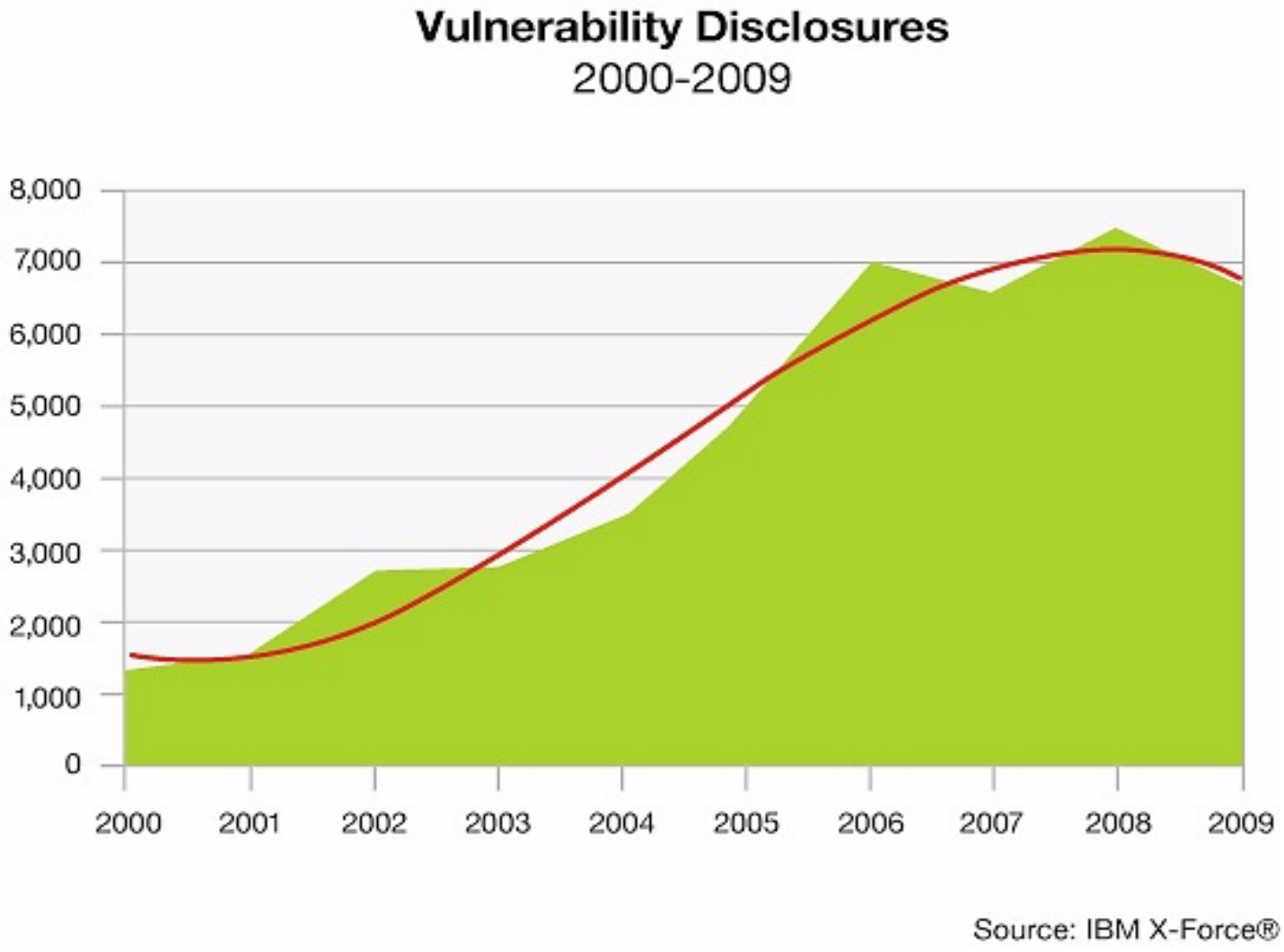
- ✓ **تهدید (Threat) :**

فردی بدخواه که انگیزه و توانایی حمله داشته باشد.

- ✓ **تایید هویت (Authentication)**

- ✓ **اجازه (Authorization)**

# روند پیدایش آسیب پذیری ها

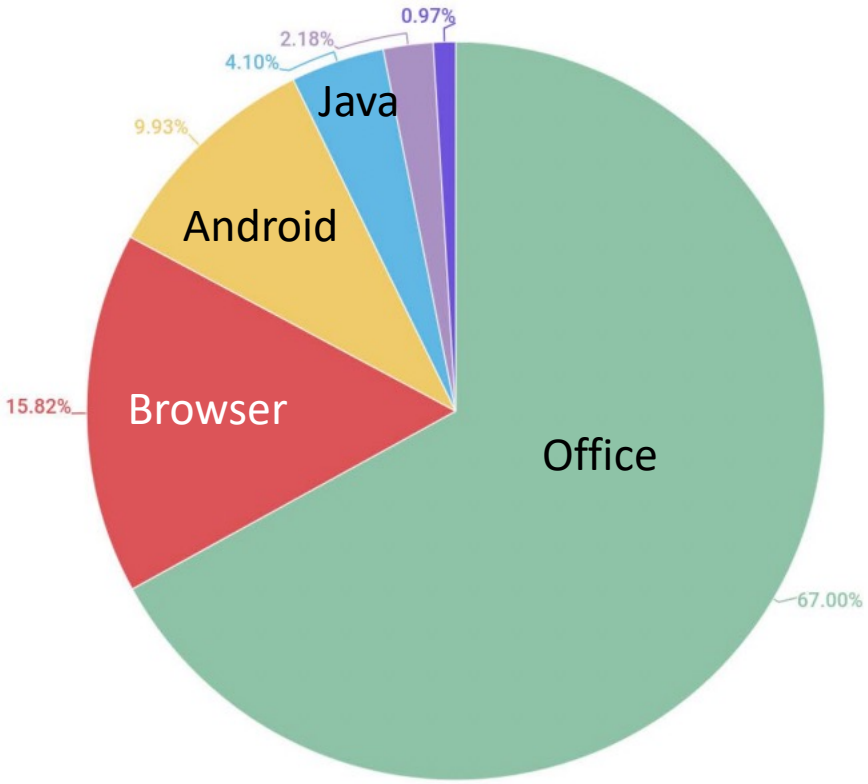


# Top 10 products by total number of “distinct” vulnerabilities in 2019

| | Product Name | Vendor Name | Product Type | Number of Vulnerabilities |
|---|---|---|---|---|
| 1 | Android | Google | OS | 414 |
| 2 | Debian Linux | Debian | OS | 360 |
| 3 | Windows Server 2016 | Microsoft | OS | 357 |
| 4 | Windows 10 | Microsoft | OS | 357 |
| 5 | Windows Server 2019 | Microsoft | OS | 351 |
| 6 | Acrobat Reader Dc | Adobe | Application | 342 |
| 7 | Acrobat Dc | Adobe | Application | 342 |
| 8 | Cpanel | Cpanel | Application | 321 |
| 9 | Windows 7 | Microsoft | OS | 250 |
| 10 | Windows Server 2008 | Microsoft | OS | 248 |

https://www.cvedetails.com/top-50-product-cvssscore-distribution.php

# Vulnerable applications being exploited



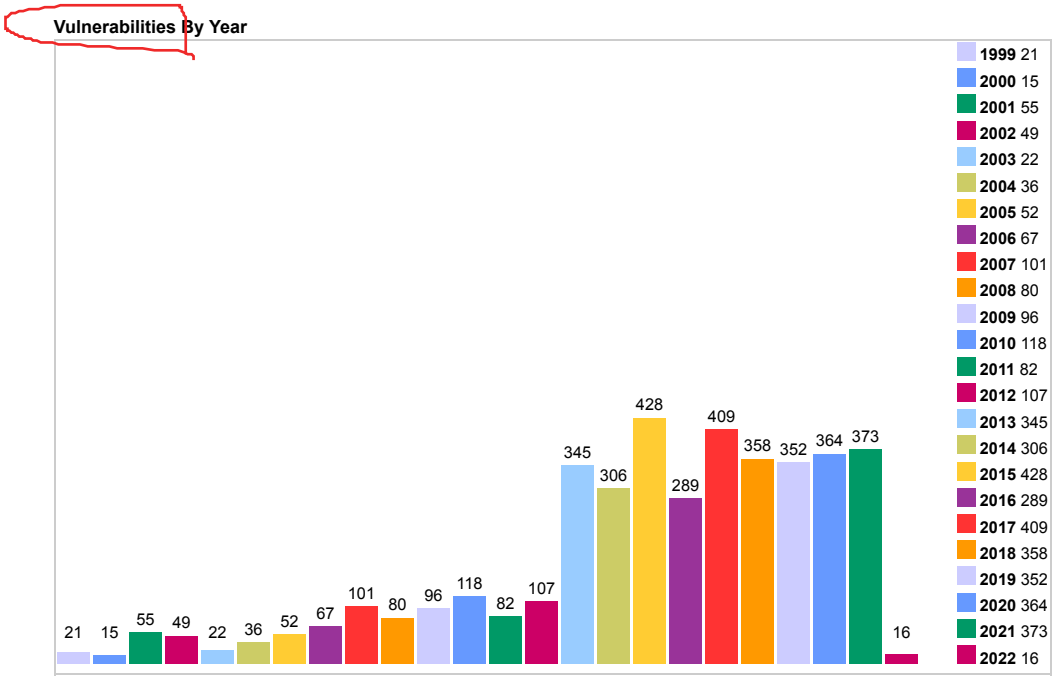

Source: Kaspersky Security Bulletin 2020

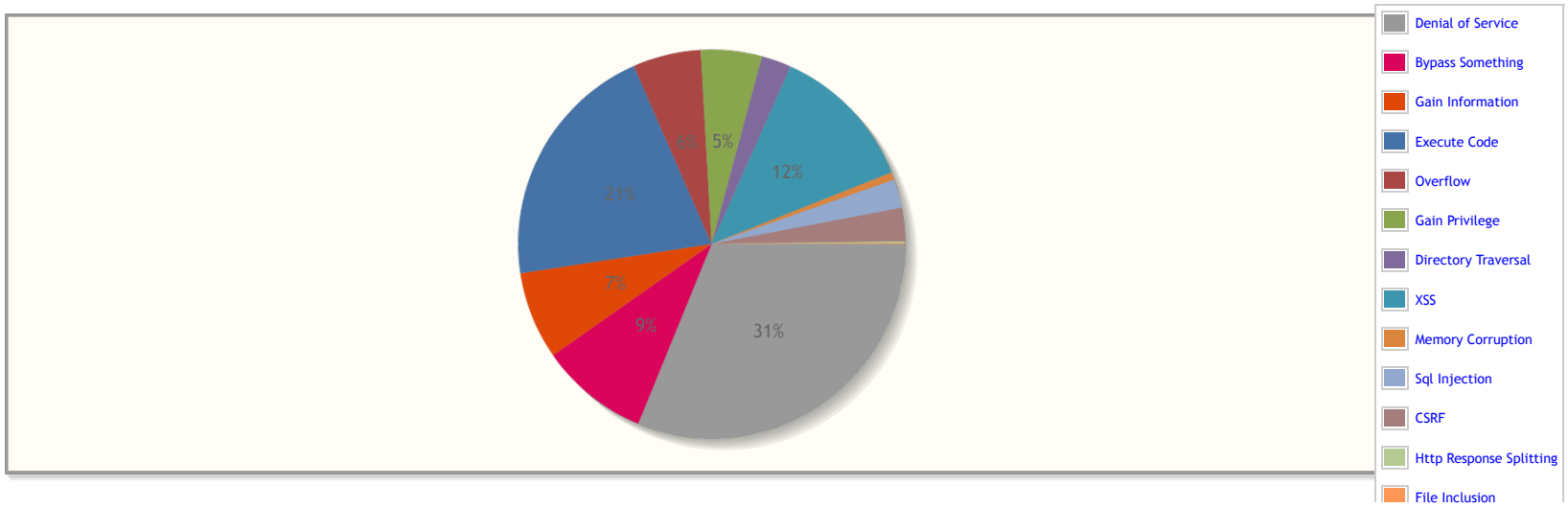
# A global problem

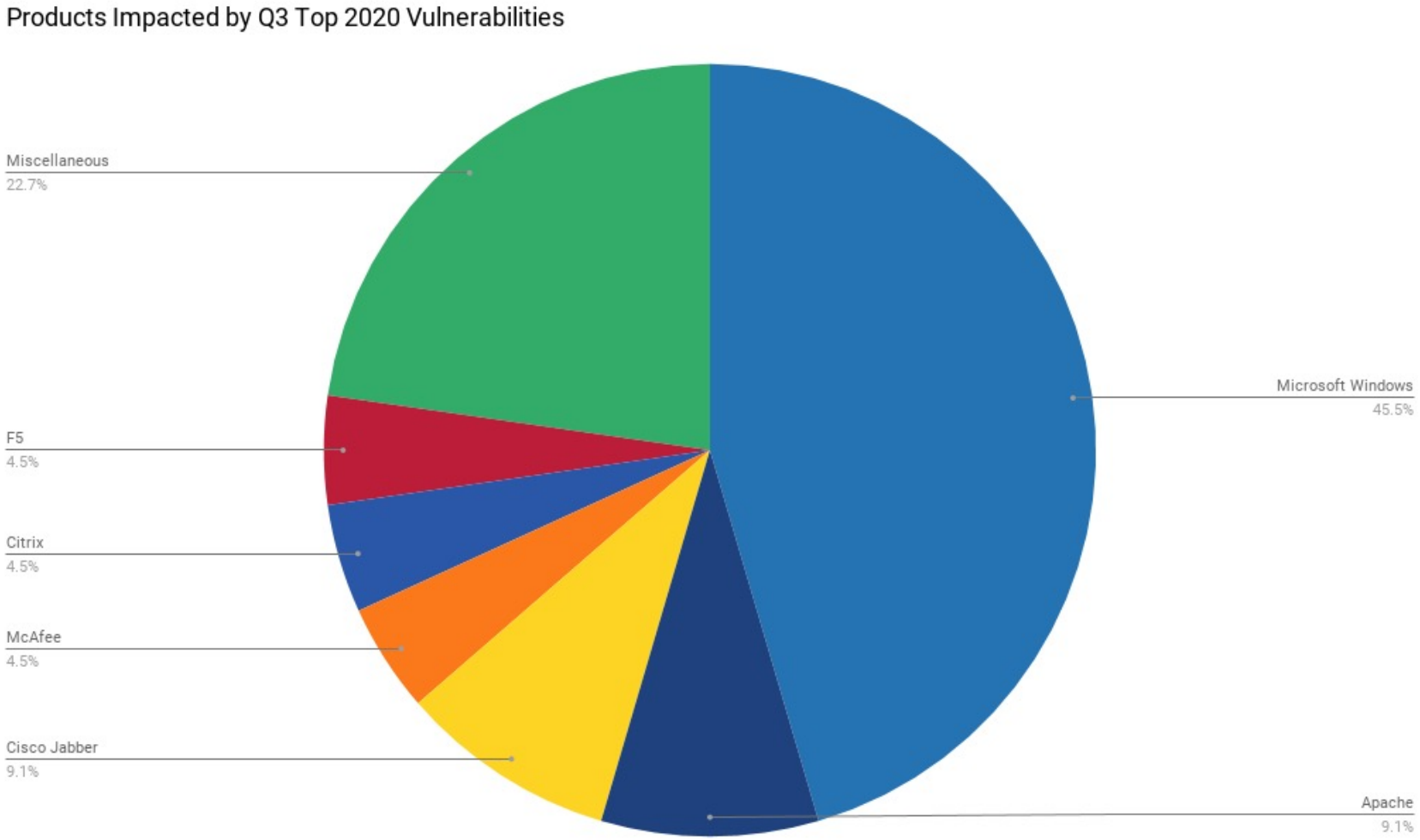
Top 10 countries by share of attacked users:

| | Country* | %** |
|---|---|---|
| 1 | Spain | 14.03 |
| 2 | France | 13.54 |
| 3 | Canada | 11.35 |
| 4 | USA | 10.76 |
| 5 | India | 10.53 |
| 6 | Brazil | 10.22 |
| 7 | Mexico | 9.86 |
| 8 | Italy | 9.80 |
| 9 | Australia | 9.09 |
| 10 | Great Britain | 8.99 |

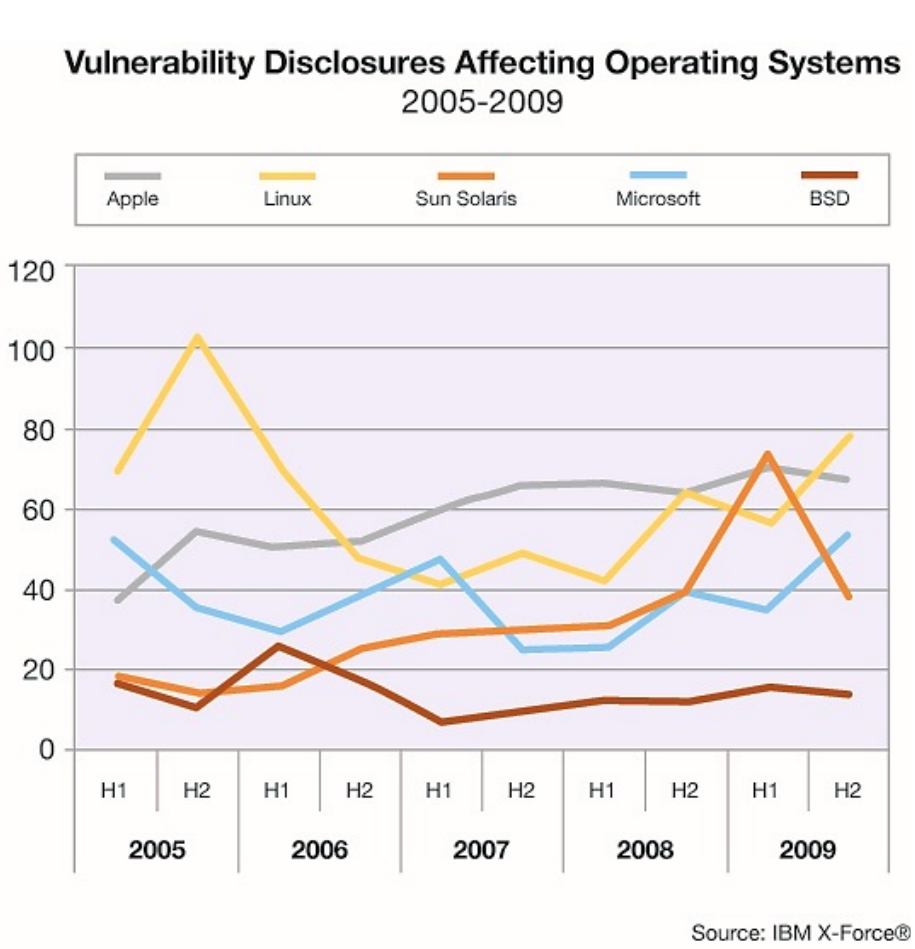
Source: Kaspersky Security Bulletin 2020


Vulnerabilities By Year
1999 21
2000 15
2001 55
2002 49
2003 22
2004 36
2005 52
2006 67
2007 101
2008 80
2009 96
2010 118
2011 82
2012 107
2013 345
2014 306
2015 428
2016 289
2017 409
2018 358
2019 352
2020 364
2021 373
2022 16
21 15 55 49 22 36 52 67 101 80 96 118 82 107 345 306 428 289 409 358 352 364 373 16

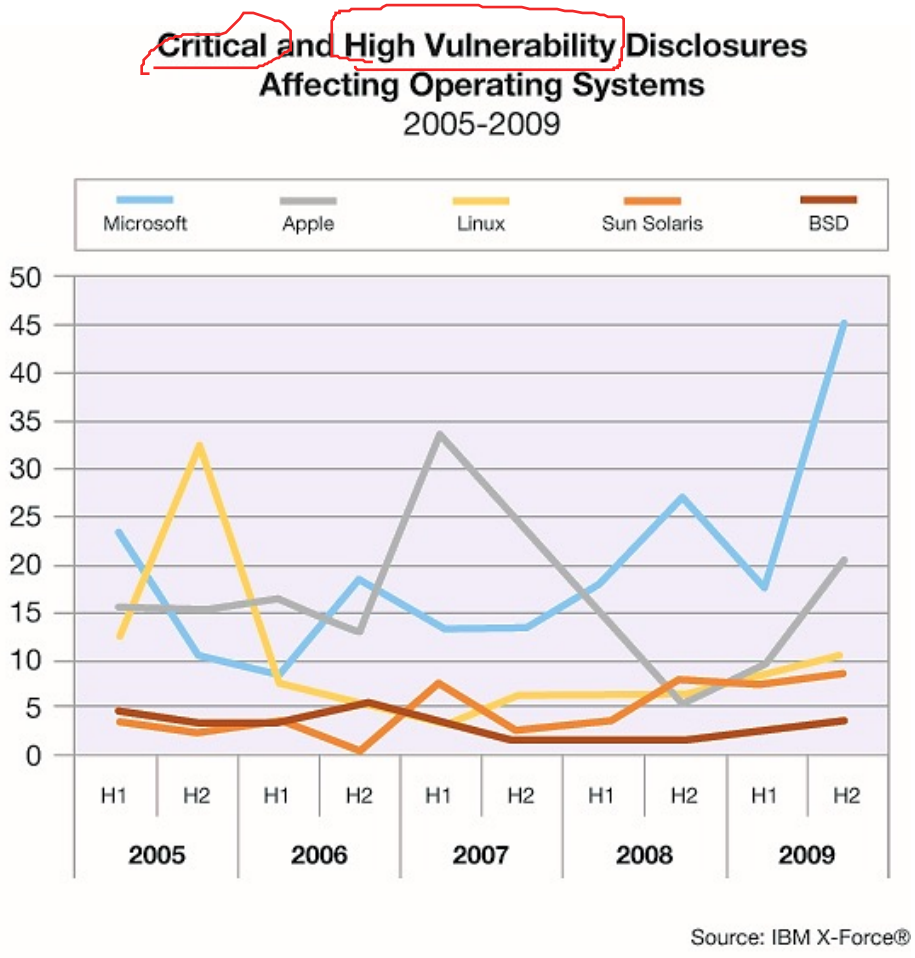

Denial of Service
Bypass Something
Gain Information
Execute Code
Overflow
Gain Privilege
Directory Traversal
XSS
Memory Corruption
Sql Injection
CSRF
Http Response Splitting
File Inclusion
21%
7%
9%
31%
5%
12%


Products Impacted by Q3 Top 2020 Vulnerabilities
Miscellaneous
22.7%
F5
4.5%
Citrix
4.5%
McAfee
4.5%
Cisco Jabber
9.1%
Microsoft Windows
45.5%
Apache
9.1%

# آسیب پذیری های سیستم عامل

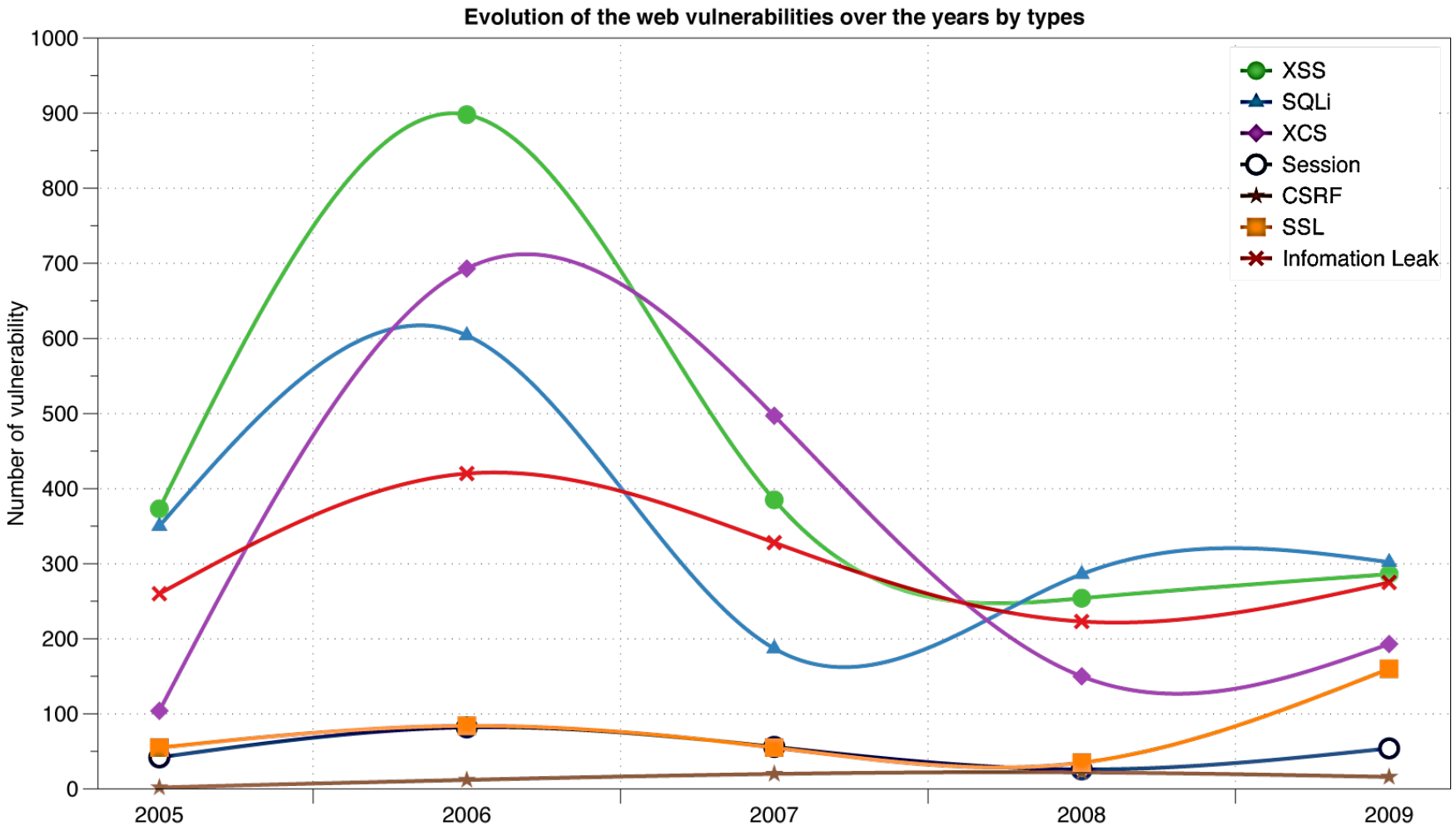



Source: IBM X-Force®

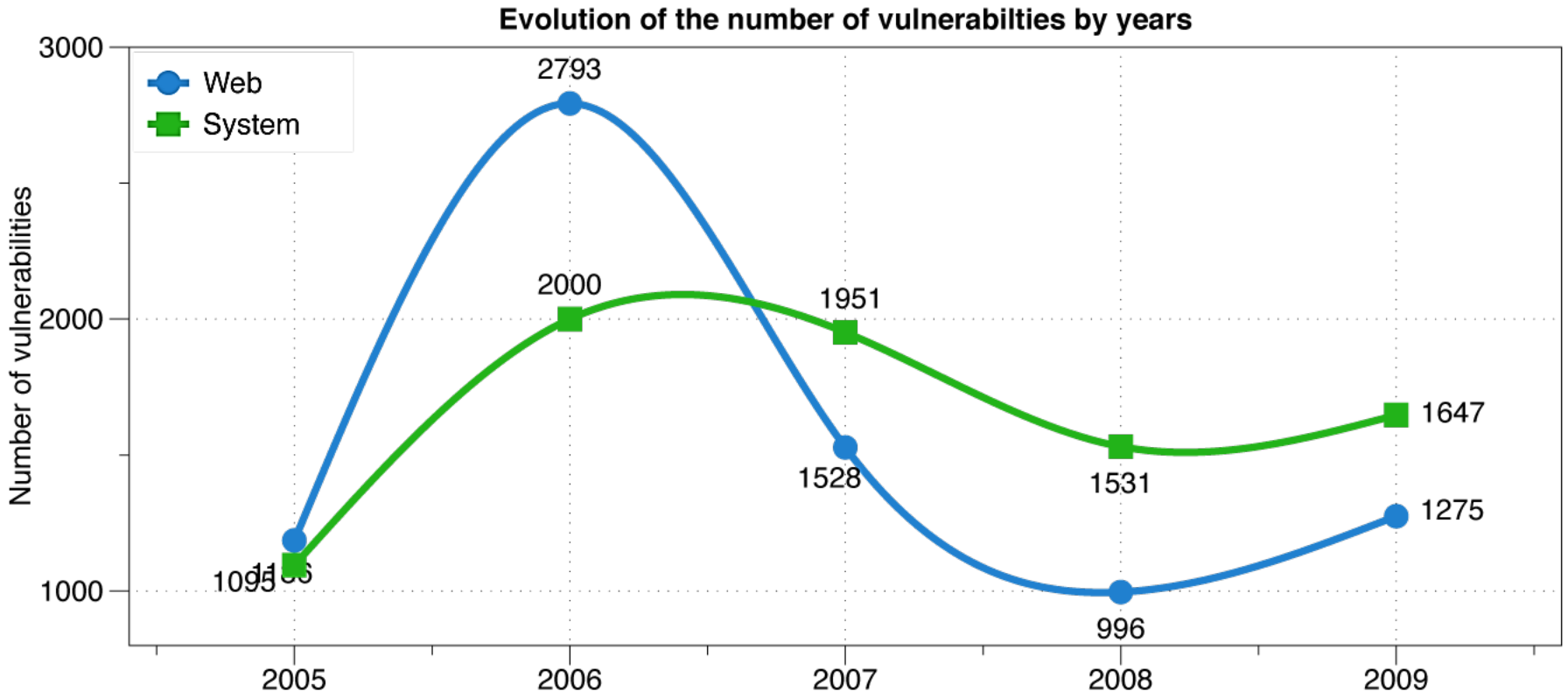



Source: IBM X-Force®

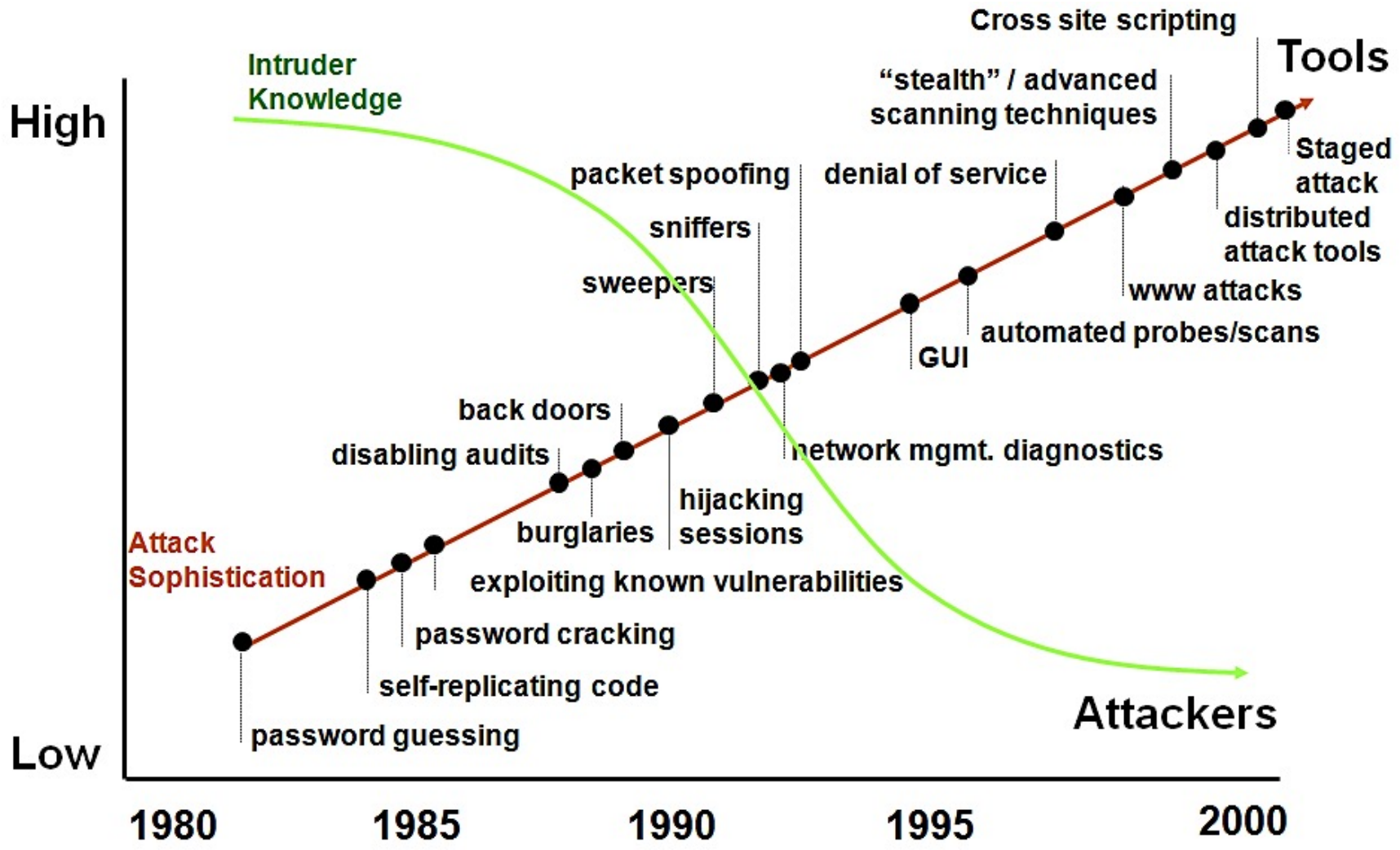
# آسیب پذیری های وب



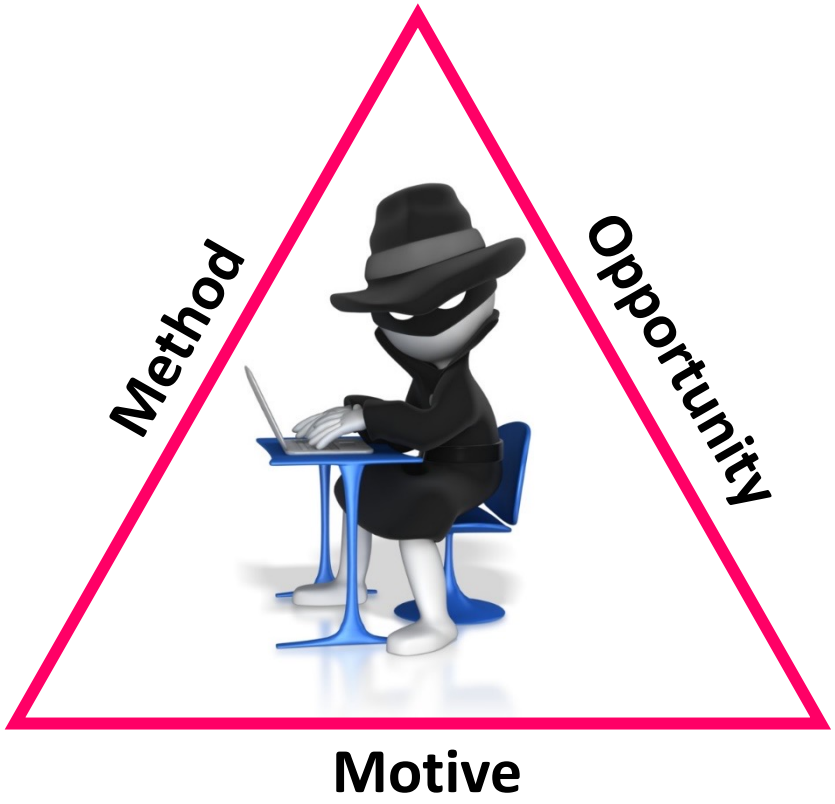
# آسیب پذیری های وب و سیستم



# دانش حمله کننده ها در مقایسه با ابزارها



# مفهوم MOM در حملات



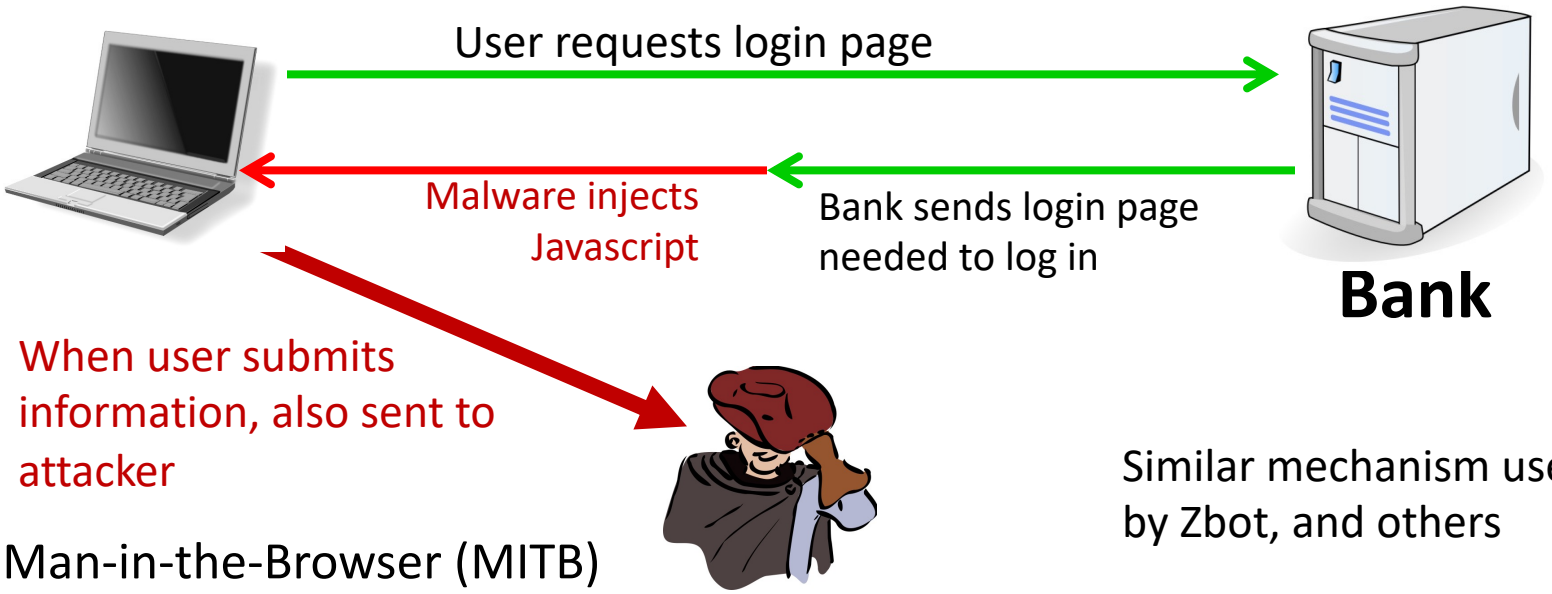

- روش (Method)
  - مهارت
  - دانش
  - ابزار
- فرصت (Opportunity)
  - زمان
  - دسترسی
- انگیزه (Motive)
  - **سرگرمی** : خرابکاری
  - **منفعت** : سازماندهی شده
  - **جاسوسی**

# دلایل نفوذ به کامپیوتر کاربران – دزدی پسورد

keylogger

keylog for banking passwords, corporate passwords, gaming pwds

Example: SilentBanker (and many like it)




Similar mechanism used by Zbot, and others

# بدافزارهای مالی

| | |
|---|---|
| 1 | Trojan-Spy.Win32.Zbot |
| 2 | Trojan.Win32.Nymaim |
| 3 | Trojan.Win32.Neurevt |
| 4 | SpyEye |
| 5 | Trojan-Banker.Win32.Gozi |
| 6 | Emotet |
| 7 | Caphaw |
| 8 | Trickster |
| 9 | Cridex/Dridex |
| 10 | Backdoor.Win32.Shiz |

- records banking passwords via keylogger
- spread via spam email and hacked web sites
- maintains access to PC for future installs

Source: Kaspersky Security Bulletin 2017

# حمله های مشابه روی دستگاههای موبایل

**Example**: FinSpy.

- Works on **iOS and Android** (and Windows)
- once installed: collects contacts, call history, geolocation, texts, messages in encrypted chat apps, …
- How installed?
  - Android pre-2017: links in SMS / links in E-mail
  - iOS and Android post 2017: physical access

# Ransomware

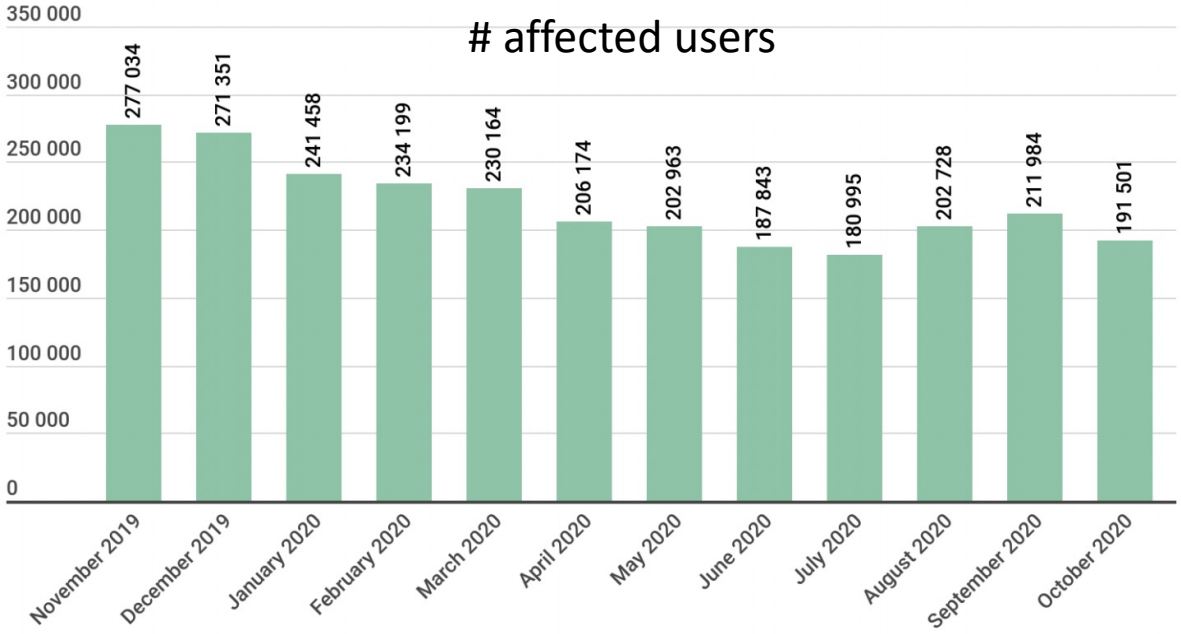
| | Name | % of attacked users** |
|---|---|---|
| 1 | WannaCry | 7.71 |
| 2 | Locky | 6.70 |
| 3 | Cerber | 5.89 |
| 4 | Jaff | 2.58 |
| 5 | Cryrar/ACCDFISA | 2.20 |
| 6 | Spora | 2.19 |
| 7 | Purgen/GlobeImposter | 2.11 |
| 8 | Shade | 2.06 |
| 9 | Crysis | 1.25 |
| 10 | CryptoWall | 1.13 |

a worldwide problem

- Worm spreads via a vuln. in SMB (port 445)
- Apr. 14, 2017: Eternalblue vuln. released by ShadowBrokers
- May 12, 2017: Worm detected (3 weeks to weaponize)

WannaCry ransomware

# Bitcoin mining




Examples:

1. Trojan.Win32.Miner.bbb
2. Trojan.Win32.Miner.ays
3. Trojan.JS.Miner.m
4. Trojan.Win32.Miner.gen

Source: Kaspersky Security Bulletin 2020

# دزدی عرض باند و آدرس IP

Attacker's goal: look like a random Internet user

Use the IP address of infected machine or phone for:

- **Spam** (e.g. the storm botnet)

  Spamalytics: 1:12M pharma spams leads to purchase

  1:260K greeting card spams leads to infection

- **Denial of Service:** Services: 1 hour (20$), 24 hours (100$)
- **Click fraud** (e.g. Clickbot.a)

# حمله به سرور ها

**(1) Data theft**: credit card numbers, intellectual property

- Example: Equifax (July 2017), ≈ 143M "customer" data impacted
  - Exploited known vulnerability in Apache Struts (RCE)
- Many many similar attacks since 2000

**(2) Political motivation**:

- DNC (2015), Ukraine power grid (2015-)

**(3) Infect visiting users**

# دزدی اطلاعات

**Typical attack steps**:

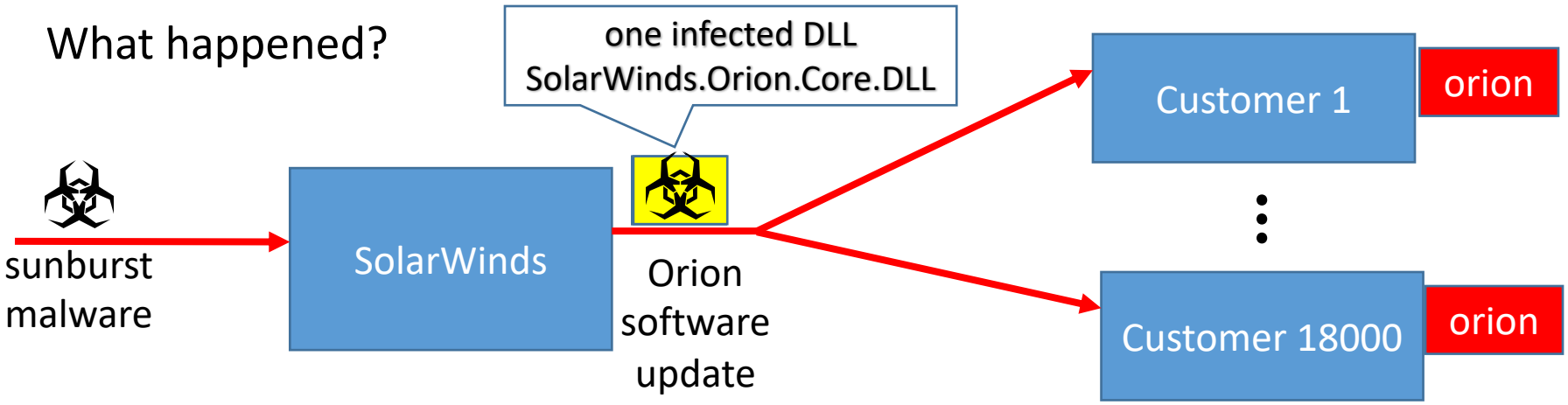
- Reconnaissance
- Foothold: initial breach
- Internal reconnaissance
- Lateral movement
- Data extraction
- Exfiltration

Security tools available to try and stop each step (kill chain)

# Case study: SolarWinds Orion (2020)

SolarWinds Orion: set of monitoring tools used by many orgs.

What happened?




Attack (Feb. 20, 2020): attacker corrupts **SolarWinds software update process**

Large number of infected orgs … not detected until Dec. 2020 .

# Sunspot: malware injection

How did attacker corrupt the SolarWinds build process?

- **taskhostsvc.exe** runs on SolarWinds build system:
  - monitors for processes running **MsBuild.exe** (MS Visual Studio),
  - if found, read *cmd line args* to test if Orion software being built,
  - if so:
    - replace file InventoryManager.cs with malware version
      (store original version in InventoryManager.bk)
    - when MsBuild.exe exits, restore original file … no trace left

How can an org like SolarWinds detect/prevent this ???

# Fallout …

Large number of orgs and govt systems exposed for many months

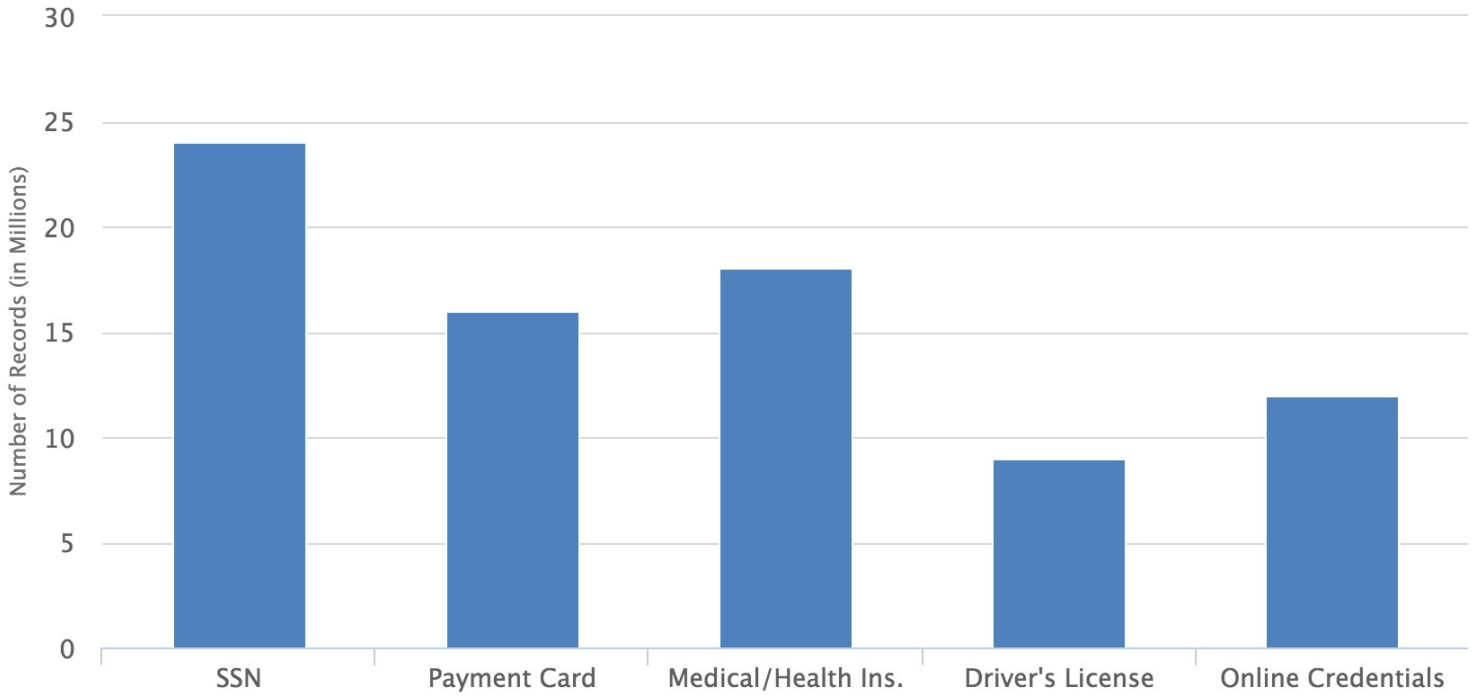
More generally: a **supply chain attack**

- Software, hardware, or service supplier is compromised

  $\Longrightarrow$ many compromised customers

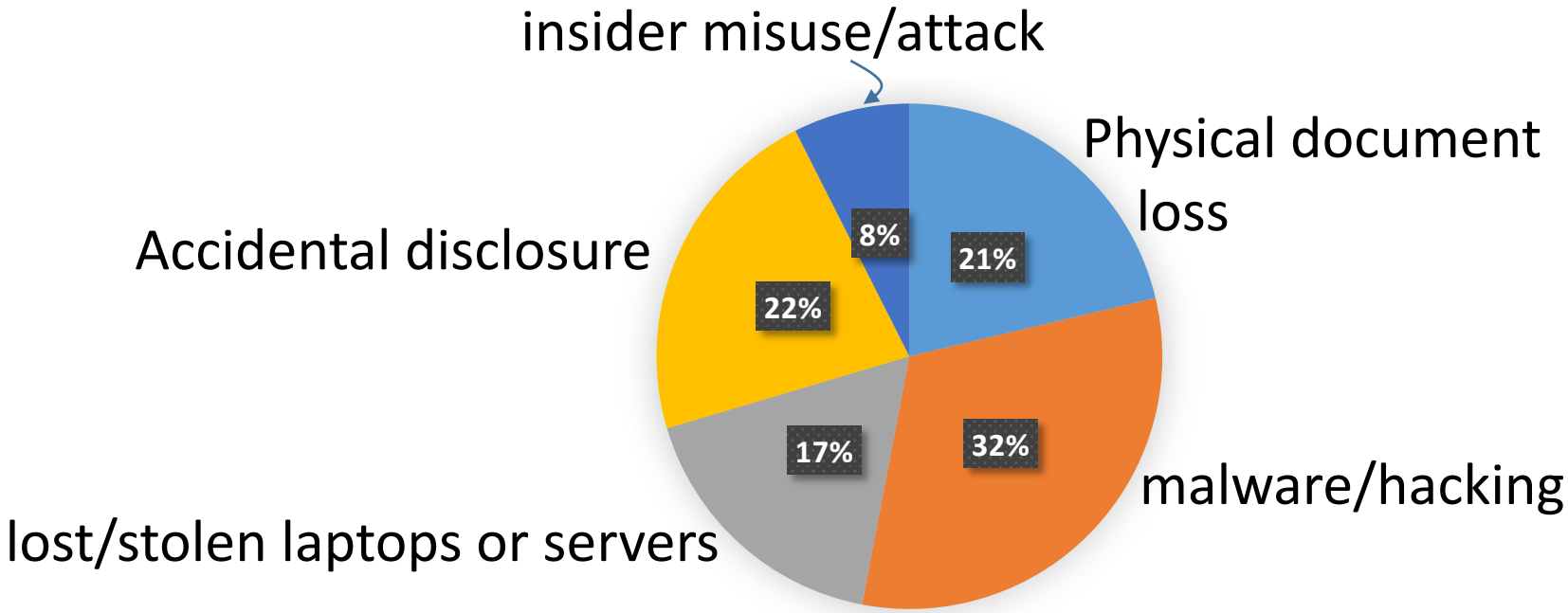
- Many examples of this in the past (e.g., Target 2013, … )
- Defenses?

# Data theft: what is stolen (2012-2015)




Source: California breach notification report, 2015

# How companies lose customer data




How do we have this data?

Source: PrivacyRights.org, 2020

# Why compromise web sites: (3) infect users

- **Mpack**: PHP-based tools installed on compromised web sites
  - Embedded as an iframe on infected page
  - Infects browsers that visit site
- Features
  - management console provides stats on infection rates
  - Sold for several 100$
  - Customer care can be purchased, one-year support contract
- Impact: 500,000 infected sites (compromised via SQL injection)
  - Several defenses: e.g. Google safe browsing

# Marketplace for Vulnerabilities

**Option 1**: bug bounty programs (many)

- Google Vulnerability Reward Program: up to $31,337
- Microsoft Bounty Program: up to $100K
- Apple Bug Bounty program: up to $200K
- Stanford bug bounty program: up to $1K
- Pwn2Own competition: $15K

**Option 2**:

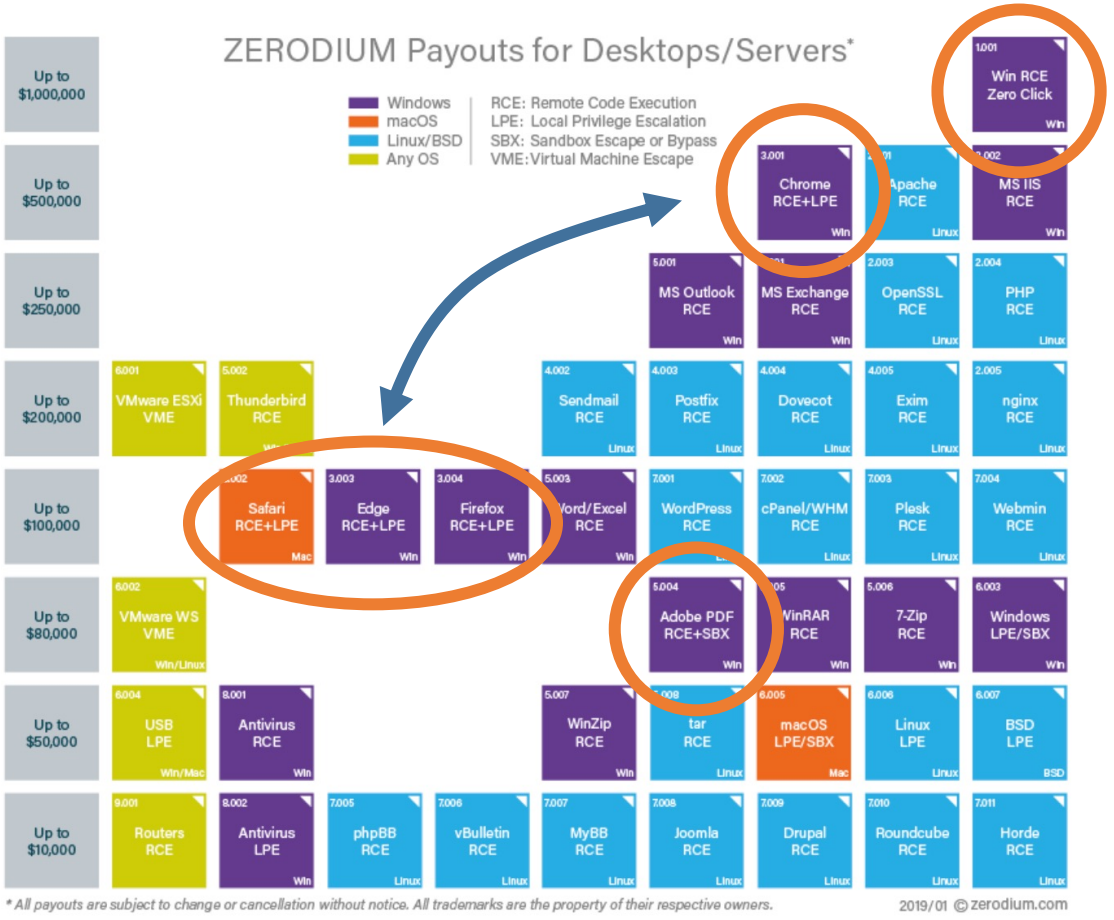
- Zerodium: up to $2M for iOS, $2.5M for Android (since 2019)
- … many others

# Marketplace for Vulnerabilities

RCE: remote code execution

LPE: local privilege escalation

SBX: sandbox escape



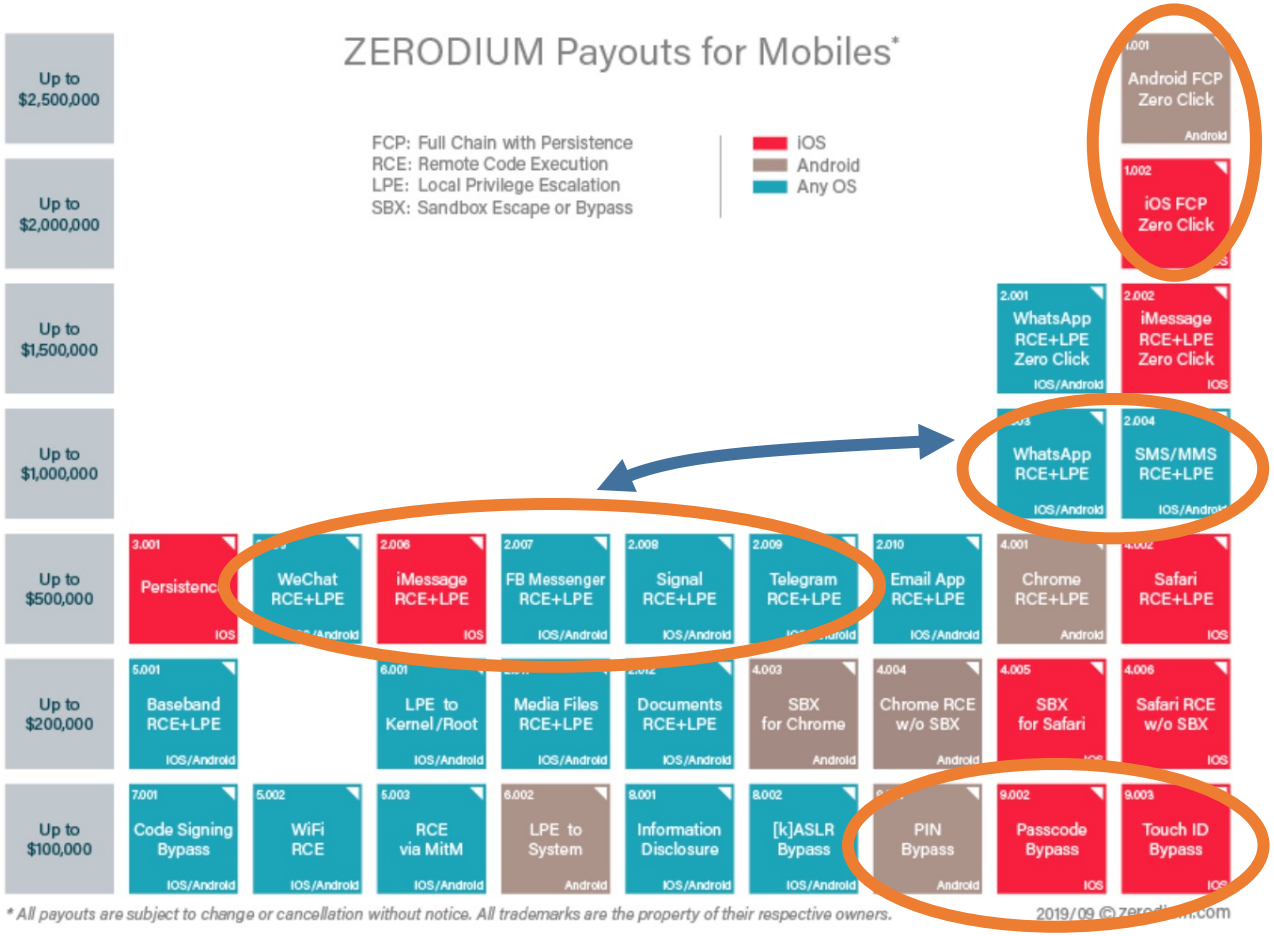

Source: Zerodium payouts

# Marketplace for Vulnerabilities

RCE: remote code execution

LPE: local privilege escalation

SBX: sandbox escape




Source: Zerodium payouts

# Why buy 0days?

**How the acquired security research is used by ZERODIUM?**

ZERODIUM extensively tests, analyzes, validates, and documents all acquired vulnerability research and reports it, along with protective measures and security recommendations, solely to its clients subscribing to the ZERODIUM Zero-Day Research Feed.

**Who are ZERODIUM's customers?**

ZERODIUM customers are government organizations (mostly from Europe and North America) in need of advanced zero-day exploits and cybersecurity capabilities.

https://zerodium.com/faq.html

# گروه های تهدید کننده

| Group | Labels | Motives |
|---|---|---|
| Novices | Novices, newbies and script kiddies | Notoriety, curiosity, thrill seeking and reputation |
| Browsers and cyber-punks | Browsers, students, cyber-punks and pranksters | Intellectual challenge, but also financial gain |
| Ethical hackers | Grey hats, old guard and ethical hackers, quiet, paranoid and skilled hackers | Intellectual challenge, passion |
| Hacktivists | Hacktivists, political activists | Cause and ideology, but also status, ego |
| Insiders | Insiders, internals | Revenge, financial gain |
| Crackers | Crackers, crashers, sport intruders, malicious hackers, virus writers, coders, elite and black hats | Revenge, ego, entertainment |
| Professional Criminals | Thieves, career criminals, darksiders, professional criminals, organised crime groups and petty thieves | Financial gain |
| Government agents | National states, foreign intelligence, government agents, military hackers | Ideology, cause |

# انواع آسیب پذیری ها

- **آسیب پذیری های Host :**
  - نرم‌افزار
  - سیستم عامل
- **آسیب پذیری های Network :**
  - **لایه لینک** : ARP Spoofing
  - **لایه شبکه** : IP Forgery
  - **لایه انتقال** : حدس زدن TCP Sequence-Number
  - **لایه کاربرد** : کرم‌های اینترنتی

# دسته بندی کلی حملات

- **قطع ارتباط (Interruption)**
  - عدم دسترس پذیری
- **سرقت اطلاعات (Interception)**
  - عدم محرمانگی
- **تغییر اطلاعات (Modification)**
  - عدم صحت
- **جعل اطلاعات (Fabrication)**
  - عدم اعتبار
- **رد درخواست (Denial of Service)**
  - عدم دسترس پذیری

# نمونه ای از حملات

- **اسکن کردن شبکه**
  - شناسایی ساختار شبکه سازمان

- **مصرف پهنای باند**
  - Denial of Service (DoS)
  - استفاده از پهنای باند سازمان برای حمله به یک شبکه‌ی دیگر
  - Reflector Attack

- **سوء استفاده**
  - استفاده از کامپیوترهای یک سازمان برای کارهای بدخواهانه

# نمونه ای از حملات

- **استراق سمع (Eavesdropping)**
  - برنامه های استنشاق اطلاعات (Sniffer)
  - استنشاق کارت‌های اعتباری

- **مهندسی اجتماعی**
  - تحریک مدیران فنی سیستم و اخذ اطلاعات

# روش های دفاعی

- **ممانعت کردن (Prevent)**
- **باز داشتن (Deter)**

تا جای ممکن سخت کردن وقوع حمله.

- **منحرف کردن (Deflect)**

ایجاد اهداف ساختگی برای منحرف کردن حمله به سمت آن‌ها.

- **شناسایی کردن (Detect)**
- **مدارا کردن (Tolerate)**

تا جای ممکن اثر حمله را کم کردن.

- **باز یافتن (Recover)**

# تأمین امنیت

- **امنیت Host**
  - راحت‌تر قابل کنترل است.
  - مدل‌های خوبی برای تأیید هویت و اجازه طراحی و پیاده‌سازی شده است.

- **امنیت Network**
  - همه می‌توانند به شبکه متصل باشند.
  - نحوه اتصال ماشین‌ها به شبکه قابل کنترل نیست.

# تأمین امنیت شبکه

- **جایگزینی ساختارهای آسیب پذیر**
  - استفاده از رمزنگاری به جای تأیید هویت مبتنی بر آدرس
- **استفاده از Firewall برای ایجاد محدودیت در دسترسی به سرویس‌های مهم**
- **بررسی شیوه‌مند و پی در پی برای جلوگیری از حملات**
  - مانیتورینگ شبکه برای شناسایی ARP Spoofing
- **پایش شبکه**

# پایان مقدمه