

یا ذالامن و الامان



آزمایشگاه امنیت داده و شبکه شریف

امنیت داده و شبکه

سازوکارهای تامین امنیت

مجید ذوالفقاری

نیم سال اول ۹۹-۰۰



❖ روش‌های تامین امنیت

❖ سازوکارهای پیشگیری

❖ سازوکارهای تشخیص

❖ سازوکارهای ترمیم و بازیابی

- دفاع در عمق

- پیاده‌سازی راه‌حل‌های پیشگیرانه

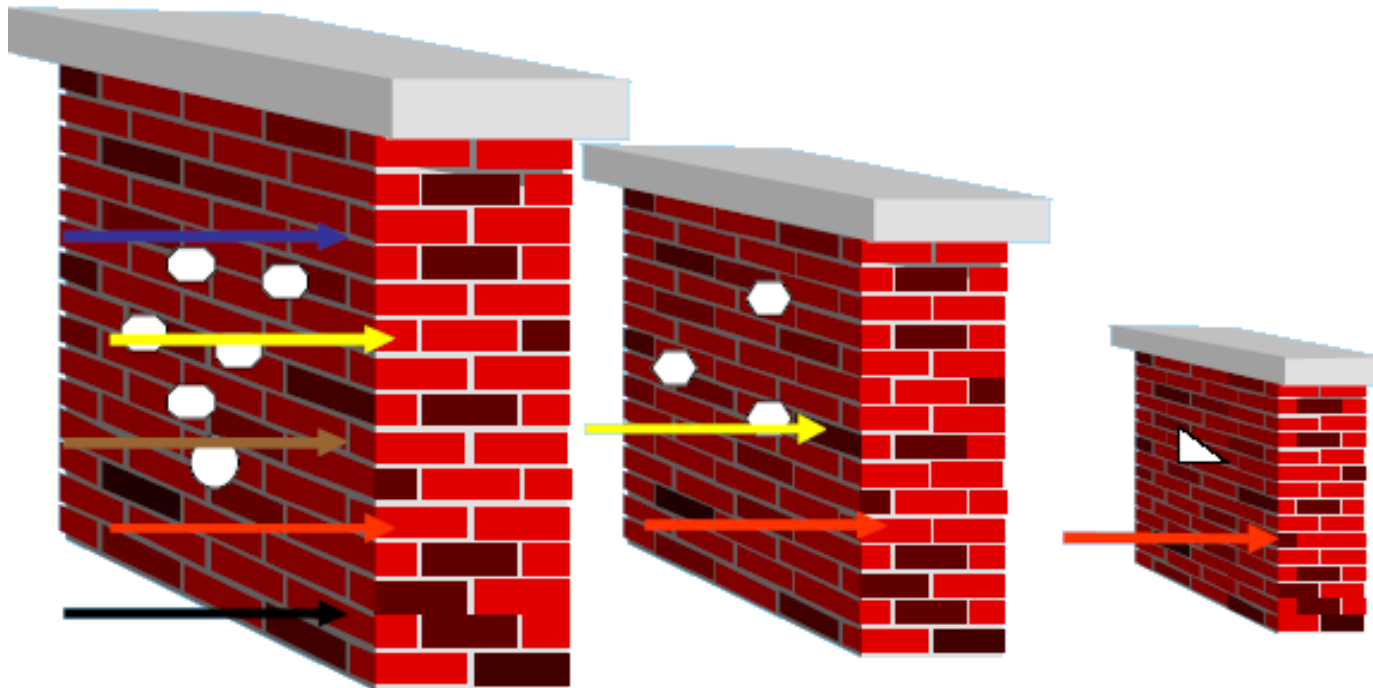
- پیاده‌سازی راه‌حل‌های تشخیص

- پیاده‌سازی راه‌حل‌های ترمیم و پشتیبانی



دفاع لایه به لایه یا دفاع در عمق

- تعریف: افزایش تعداد لایه‌های دفاعی و دشوار کردن مسیر دسترسی نفوذگران به مناطق حساس و کلیدی سیستم یا شبکه.



مثال ۱: دفاع در عمق در سیستم نرم‌افزاری

• امن‌سازی همه لایه‌های نرم‌افزاری یک سیستم شامل:

• شبکه (Network)

• سیستم‌عامل (Operating System)

• سیستم مدیریت پایگاه داده‌ها (DBMS)

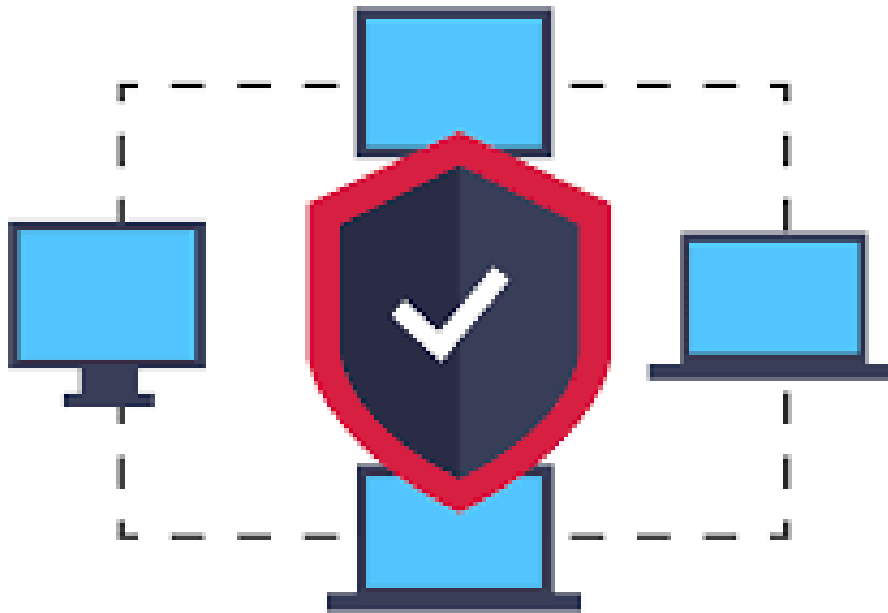
• برنامه کاربردی (Application)

مثال ۲: دفاع در عمق در یک سیستم شبکه‌ای

• امن‌سازی شبکه و ارتباطات

• امن‌سازی کارگزار

• امن‌سازی کارخواه



مثال ۲ - امن سازی شبکه و ارتباطات

- استفاده از شبکه مبتنی بر سوئیچ
- افزایش مصونیت نسبت به شنود بسته
- امکان تعریف نواحی مختلف با سطوح امنیتی مختلف (مکانیزم VLAN)
- امکان اعمال برخی سیاست‌های دسترسی با امکاناتی همچون Port Security
- استفاده از ابزارهای مدیریت شبکه
- توجه به امنیت و محرمانگی ارتباطات Wireless
- رفع آسیب‌پذیری‌های سرویس‌های شبکه (email, File Server, ...)

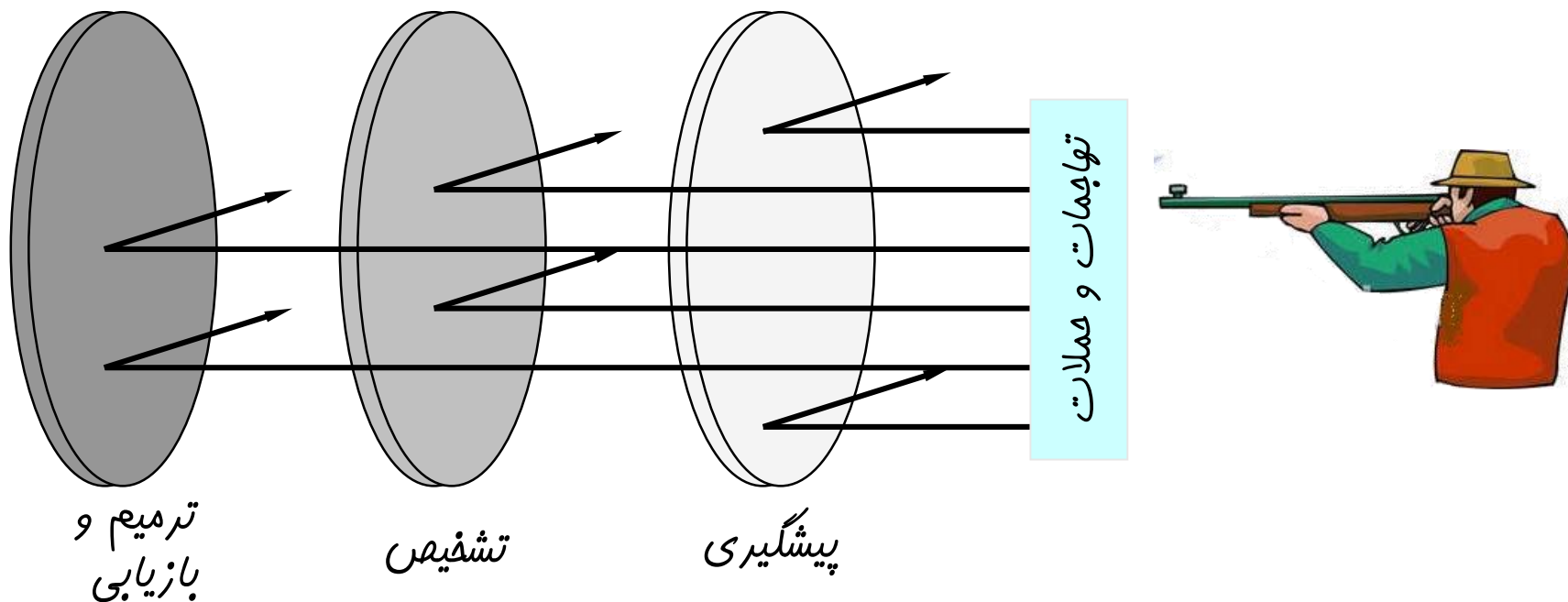
- استفاده از ضدبدافزار (ترجیحاً به صورت Corporate)
- استفاده از وصله‌های امنیتی (Patch) به روز سیستم‌عامل و نرم‌افزارهای نصب شده
- تغییر در تنظیمات پیش فرض
- غیرفعال کردن سرویس‌های غیرضروری
- مسدود کردن تمام پورت‌های TCP/IP به غیر از موارد لازم
- اجرای سیاست‌های امنیتی مختلف در خصوص گذرواژه، حسابرسی کاربران و

مثال ۲ - امن سازی کارخواه

- استفاده از ضد بدافزار ترجیحاً به صورت (Corporate)
- استفاده از دیواره آتش شخصی
- استفاده از وصله‌های امنیتی به روز سیستم‌عامل و نرم‌افزارهای نصب شده



مراتب مقابله با نفوذ و تهاجم در سیستم





- شناسایی و احراز اصالت
- کنترل دسترسی
- حفاظ (دیواره آتش)
- رمزنگاری و امضای دیجیتال

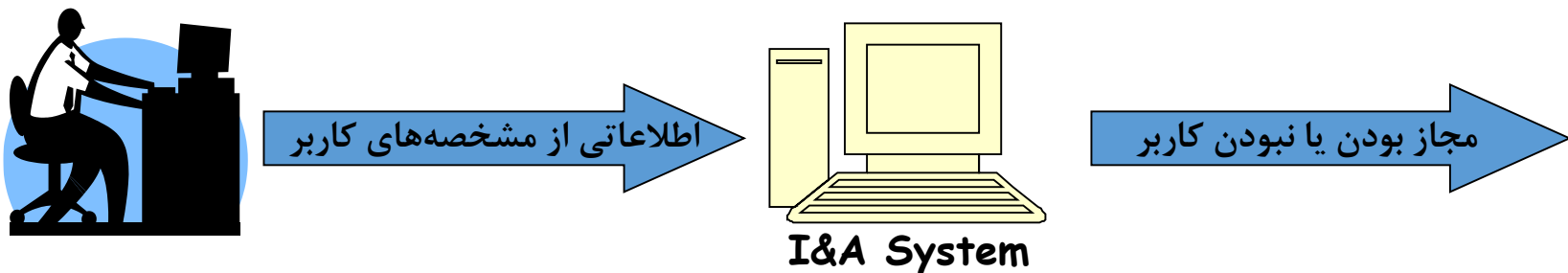
- سیستم تشخیص نفوذ (IDS)
- سیستم تله‌عسل (HoneyPot)
- سیستم مدیریت اطلاعات و رویدادهای امنیتی (SIEM)

- سیستم‌های پشتیبان و ترمیم خودکار
- مکانیزم‌های پشتیبان‌گیری و بازیابی اطلاعات
- راه‌اندازی سایت پشتیبان (به طور فیزیکی مجزا و مستقل)



Identification & Authentication •

- شناسایی کاربر و اطمینان از اینکه کاربر همان فردی است که ادعا می کند.
- پیش نیاز کنترل دسترسی در هر سیستم، شناسایی و احراز هویت کاربر است.
- فرآیند شناسایی و احراز هویت



احراز هویت بر اساس دانسته‌های کاربر

- آنچه که کاربر در ذهن خود دارد:
- گذرواژه

- شماره شناسایی شخصی PIN

مساله اصلی: حدس یا افشای دانسته فردی

راه حل: تغییر دوره‌ای دانسته

ترکیب با روش‌های دیگر



احراز هویت بر اساس داشته‌های کاربر

- آنچه که کاربر به طور فیزیکی در اختیار دارد:
 - کارت (پلاستیکی، مغناطیسی، هوشمند، ...)
 - توکن امنیتی (Security Token)
 - توکن تولید گذرواژه یکبار مصرف (OTP)

مساله اصلی: مفقود شدن داشته فرد

راه حل: ترکیب با روش‌های دیگر



احراز هویت بر اساس مشخصه‌های بیولوژیکی کاربر

• بر اساس مشخصه‌های طبیعی و منحصر به فرد کاربر:

• اثر انگشت

• عنبیه چشم

• چهره

• صوت



مساله اصلی: هزینه بالا و پیچیدگی سیستمی

حفاظت از داده های احراز هویت

- نیاز به حفاظت از گذرواژه در حال گذر و یا ذخیره شده
 - نمایشی از گذرواژه های ذخیره شده در لینوکس
 - نمایشی از امکان دزدیده شدن گذرواژه در مسیر
- پیشگیری از امکان کپی برداری و یا افشای کلید ذخیره شده در توکن
- نیاز به حفاظت از داده های بیومتریک

محتوای فایل shadow حاوی گذرواژه‌ها در لینوکس

```
at*:14521:0:99999:7:: avahi*:14222:0:99999:7:::
beagleindex*:14521:0:99999:7::: bin*:14222::: daemon*:14222:::
dnsmasq*:14222:0:99999:7::: ftp*:14222::: games*:14222:::
haldaemon*:14222:0:99999:7::: lp*:14222::: mail*:14222:::
man*:14222::: messagebus*:14222:0:99999:7::: news*:14222:::
nobody*:14222::: ntp*:14222:0:99999:7::: polkituser*:14222:0:99999:7:::
postfix*:14222:0:99999:7::: pulse*:14222:0:99999:7:::
root:$2a$05$w9Sm7gHWX509G6UVJ/UBZO7eIW0uvEZ072PvO/69XjeQn6GOT6.C
G:14521::: sshd*:14222:0:99999:7::: suse-ncc*:14222:0:99999:7:::
uucp*:14222::: uuidd*:14222:0:99999:7::: wwwrun*:14222:::
jamal:$2a$05$MAPpLUxiZy9QJOCr1Vw59O/aaporGgAmja8kBRBsILsrE28q95vOm:
14521:0:99999:7:::
```

39	2.450321	213.233.168.3	213.233.168.156	TCP
40	2.450331	213.233.168.156	213.233.168.3	TCP
41	2.450424	213.233.168.156	213.233.168.3	HTTP
42	2.450688	213.233.168.3	213.233.168.156	TCP
43	2.491468	Intel_5b:f3:5e	Broadcast	ARP
44	2.491670	fa80::822::edfa:db2d::8	ff02::1::ffff::1201	ICMPv6

```

Source port: stun (3478)
Destination port: http (80)
[Stream index: 5]
Sequence number: 1 (relative sequence number)
[Next sequence number: 720 (relative sequence number)]
Acknowledgement number: 1 (relative ack number)
Header length: 20 bytes
    
```

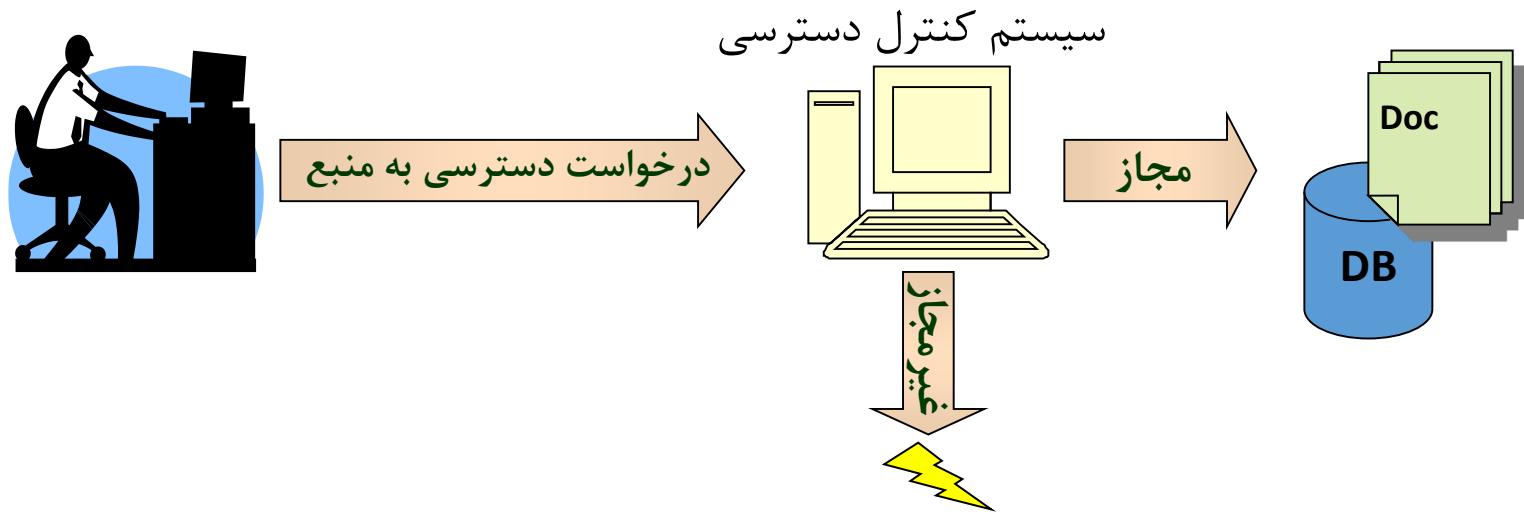
0230	36 38 63 63 35 34 63 62	62 37 39 39 61 37 31 64	68cc54cb b799a71d
0240	3b 20 50 48 50 53 45 53	53 49 44 3d 31 33 65 35	; PHPSES SID=13e5
0250	62 36 35 33 36 62 30 38	66 32 61 39 33 33 38 36	b6536b08 f2a93386
0260	61 31 33 37 32 66 37 65	64 39 35 39 0d 0a 43 6f	a1372f7e d959..co
0270	6e 74 65 6e 74 2d 54 79	70 65 3a 20 61 70 70 6c	ntent-Type: appl
0280	69 63 61 74 69 6f 6e 2f	78 2d 77 77 77 2d 66 6f	ication/ x-www-fo
0290	72 6d 2d 75 72 6c 65 6e	63 6f 64 65 64 0d 0a 43	rm-urllen coded..c
02a0	6f 6e 74 65 6e 74 2d 4c	65 6e 67 74 68 3a 20 38	ontent-L ength: 8
02b0	30 0d 0a 0d 0a 6c 6f 67	69 6e 5f 75 73 65 72 6e	0...log in_usern
02c0	61 6d 65 3d 6d 5f 61 6d	69 6e 69 26 73 65 63 72	ame=m_am ini&secr
02d0	65 74 6b 65 79 3d 6d 79	70 61 73 73 26 6a 73 5f	etkey=my pass&js
02e0	61 75 74 6f 64 65 74 65	63 74 5f 72 65 73 75 6c	autodete ct_resul
02f0	74 73 3d 31 26 6a 75 73	74 5f 6c 6f 67 67 65 64	ts=1&jus t_logged
0300	5f 69 6e 3d 31		_in=1

Text item (0), 80 bytes Packets: 338 Displayed: 338 Marked: 0 Dropped: 0

استخراج گذرواژه با شنود روی شبکه

Access Control •

- مکانیزم هسته‌ای برای حفظ امنیت در هر سیستم کنترل دسترسی است.
- وظیفه کنترل دسترسی کاربران و سیستم‌های دیگر را به منابع و اطلاعات سیستم و یا شبکه مورد حفاظت بر عهده دارد.



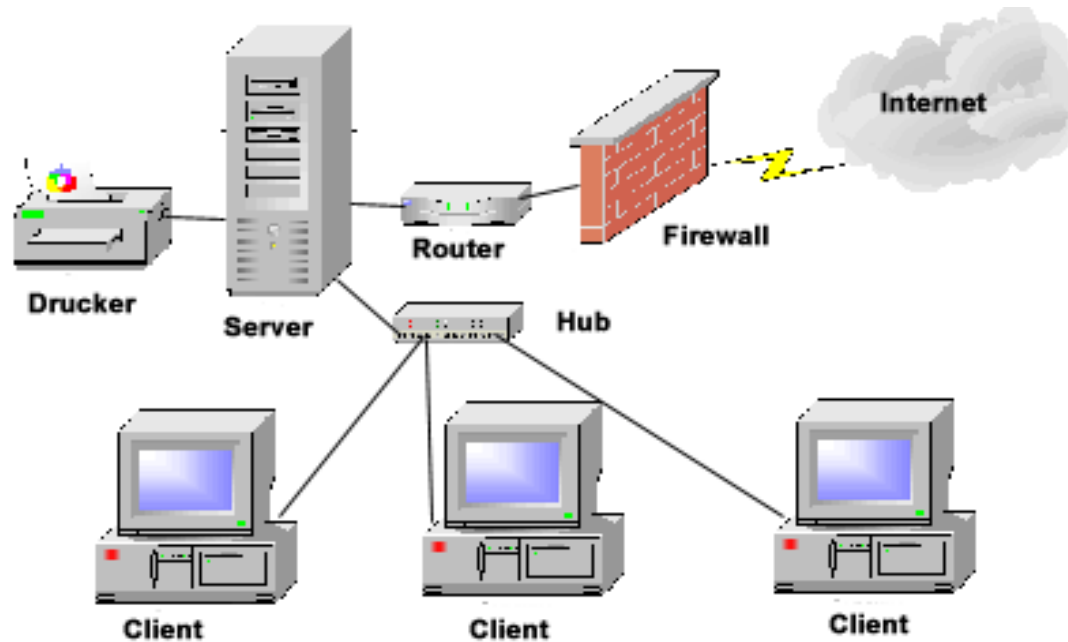
- پیش‌نیاز کنترل دسترسی، شناسایی کاربر و احراز اصالت هویت مورد ادعای آن است.
- پس از شناخت کاربر، دسترسی‌های وی به منابع بر اساس تدابیر امنیتی وضع شده توسط مدیر سیستم مشخص می‌شود.
- انواع روش‌های کنترل دسترسی
 - کنترل دسترسی اختیاری (DAC)
 - کنترل دسترسی اجباری (MAC)
 - کنترل دسترسی نقش-مبنا (RBAC)

کنترل دسترسی - از خیال تا واقعیت

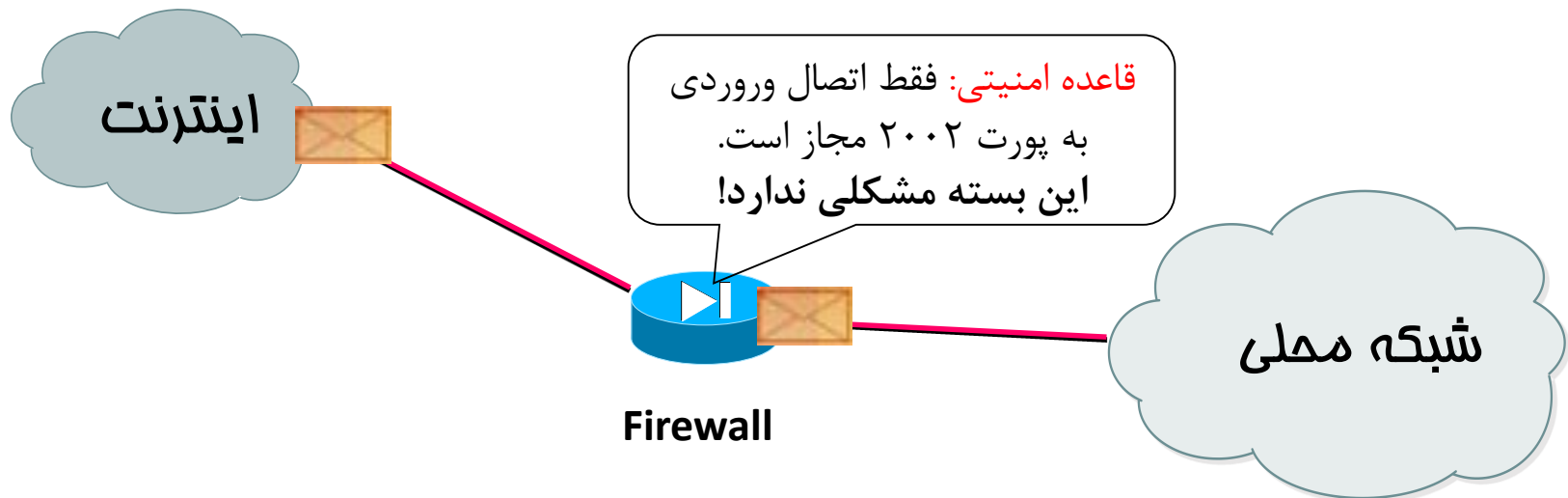
- وجود ارتباط منطقی و امن بین احراز هویت و مجازشماری
- نیاز به کنترل دسترسی در لایه‌های اصلی
- لایه واسط کاربری، لایه کاربرد، لایه دسترسی به داده‌ها (پایگاه داده‌ها)
- نیاز به حفظ صحت لیست‌های دسترسی

Firewall •

- یک سیستم امنیتی مبتنی بر مکانیزم کنترل دسترسی
- موظف به کنترل دسترسی کاربران خارجی به سیستم‌های داخلی
- تعیین مجوز دسترسی توسط مدیر امنیتی در قالب قواعد امنیتی



- ابزاری است برای کنترل و نظارت بر بسته‌های ارسالی و دریافتی
- بر اساس قواعدی که برایش تعریف می‌شود به بسته‌ها اجازه عبور یا عدم عبور می‌دهد.

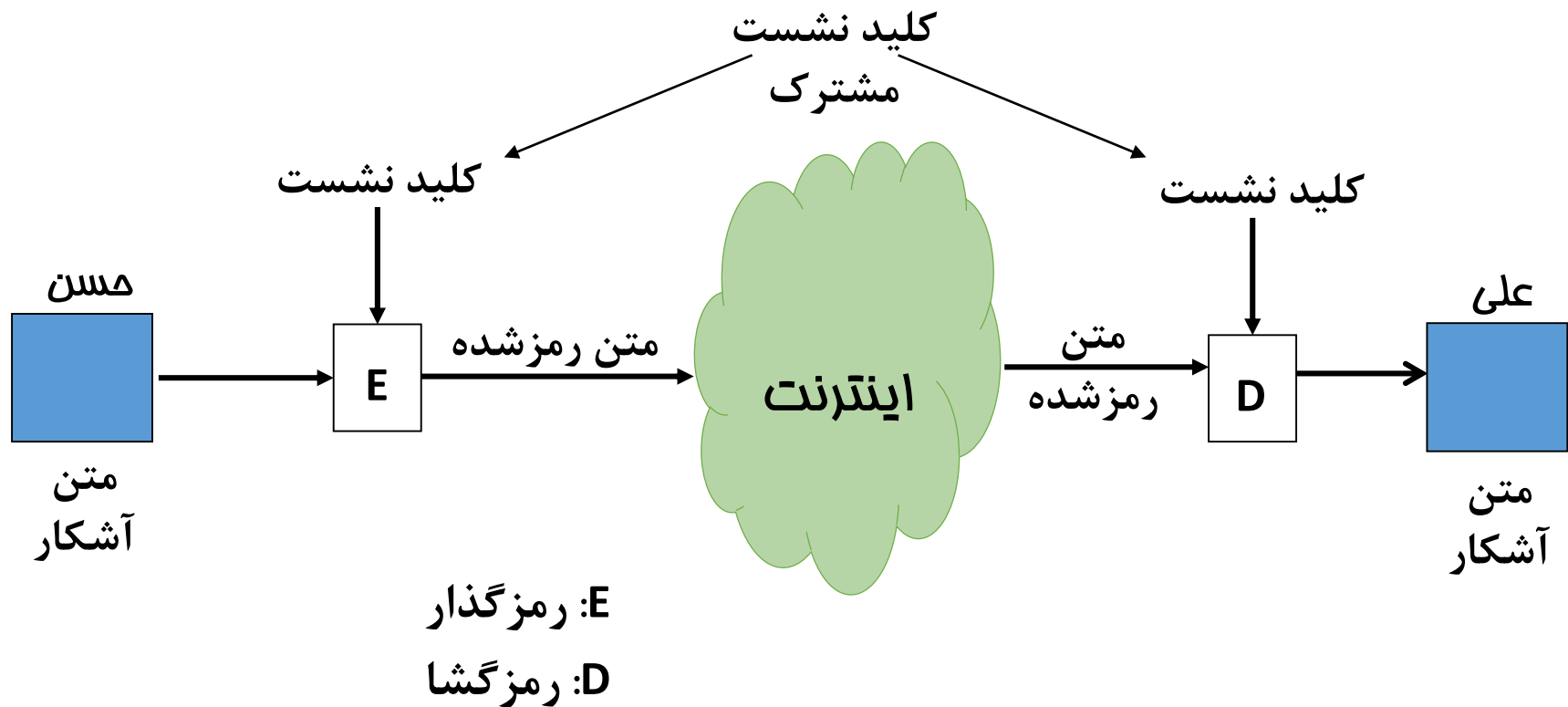


• Cryptography

- **حفظ محرمانگی (پیشگیری):** اطمینان از اینکه هر داده ذخیره شده و یا ارسالی بر روی شبکه تنها توسط گیرنده موردنظر می‌تواند رمزگشایی و استفاده گردد.
- **کنترل صحت (تشخیص):** افزودن یک سرآیند رمز شده با یک کلید به داده در حال انتقال و بازسازی و کنترل آن در مقصد.
- **احراز اصالت کاربر یا پیام (تشخیص):** رمز یک اطلاع با کلیدی که صرفاً در اختیار کاربر و یا مبدأ موردنظر است و واریسی آن در مقصد.
- **رمزنگاری: رمزگذاری (Encryption) + رمزگشایی (Decryption)**

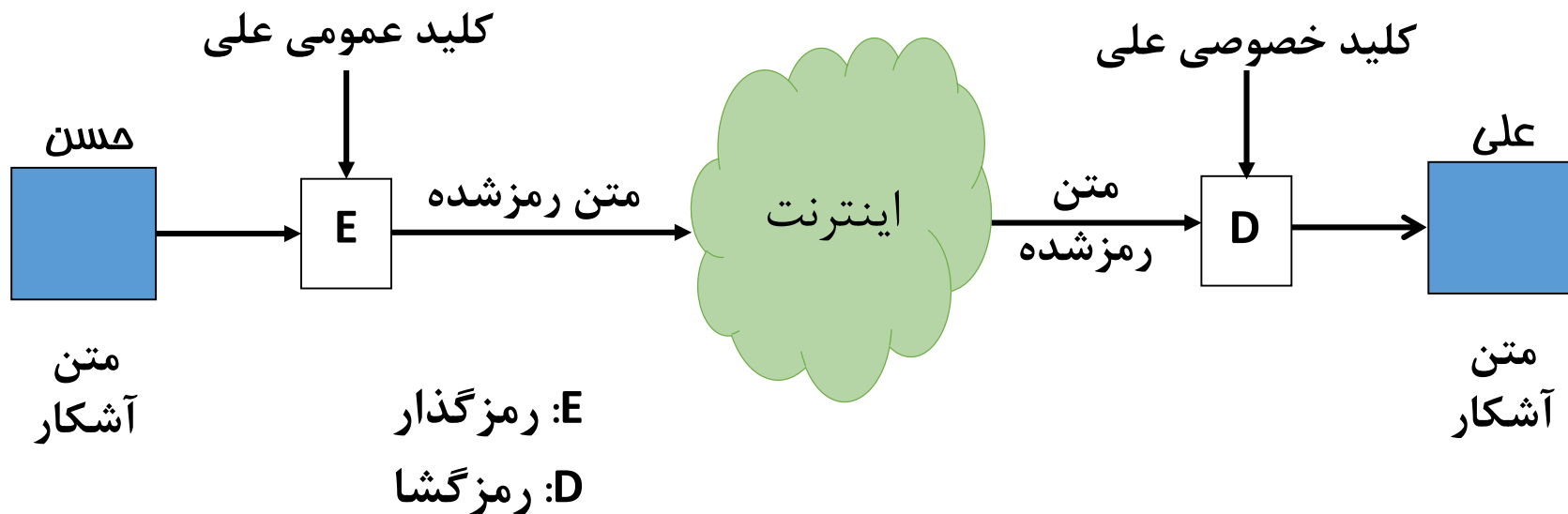
- استفاده از یک کلید نشست مشترک برای رمز داده‌ها بین دو فرد
- **مساله اصلی:** نیاز به تبادل کلید نشست مشترک از طریق یک کانال امن
- **کابردها:** حفظ محرمانگی داده‌ها و کنترل صحت
- نیاز به زمان کمتری برای رمزگذاری و رمزگشایی (نسبت به الگوریتم‌های نامتقارن) دارد.

• رمزنگاری متقارن جهت حفظ محرمانگی



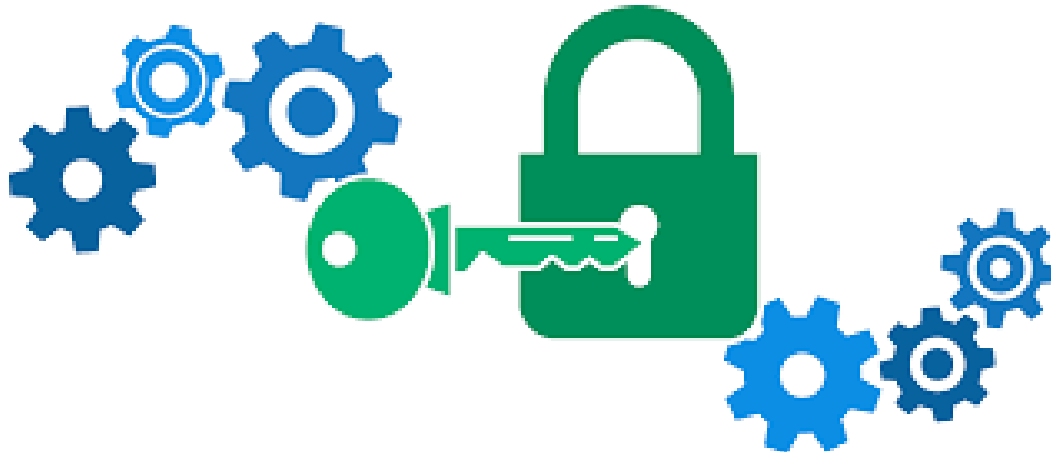
- هر فرد دارای یک کلید عمومی و یک کلید خصوصی است.
- کلید عمومی در اختیار همگان قرار دارد.
- کلید خصوصی صرفاً در اختیار فرد قرار دارد و باید به گونه‌ای امن نگهداری شود.
- کاربردها:
 - رمزنگاری جهت حفظ محرمانگی
 - امضای دیجیتال جهت احراز هویت، کنترل صحت و عدم انکار
 - نیاز به زیرساخت کلید عمومی (PKI) جهت صدور گواهی کلید عمومی

- رمزنگاری جهت **حفظ محرمانگی**
- هر کسی می تواند داده ها را با کلید عمومی فرد رمز گذاری نماید.
- فقط فرد دارای کلید خصوصی (متناظر کلید عمومی به کار برده شده) می تواند داده های رمز شده را رمز گشایی کند.



□ **کنترل صحت (تشخیص):** افزودن یک سرآیند رمز شده به داده در حال انتقال و بازسازی و کنترل آن در مقصد.

□ **احراز اصالت کاربر یا پیام (تشخیص):** رمز یک اطلاع با کلیدی که صرفاً در اختیار کاربر و یا مبدأ موردنظر است و واریسی آن در مقصد.

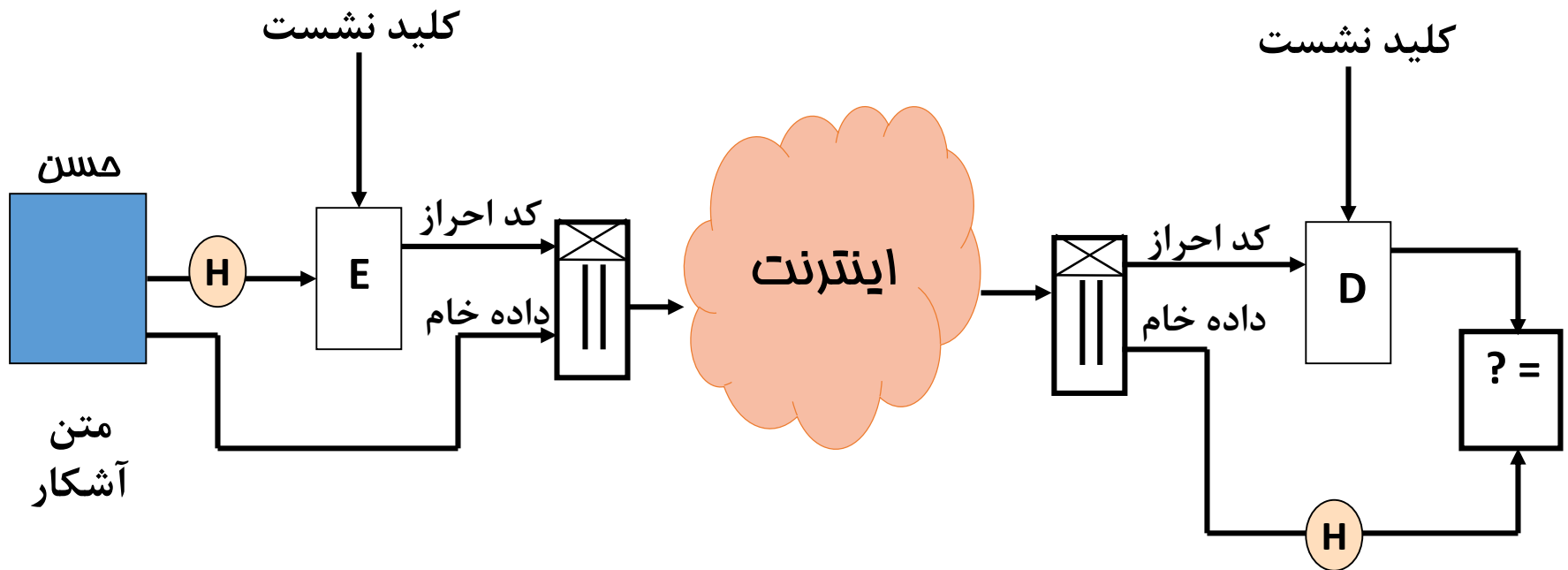


• فرآیند کنترل صحت با رمزنگاری متقارن

E: رمزگذار

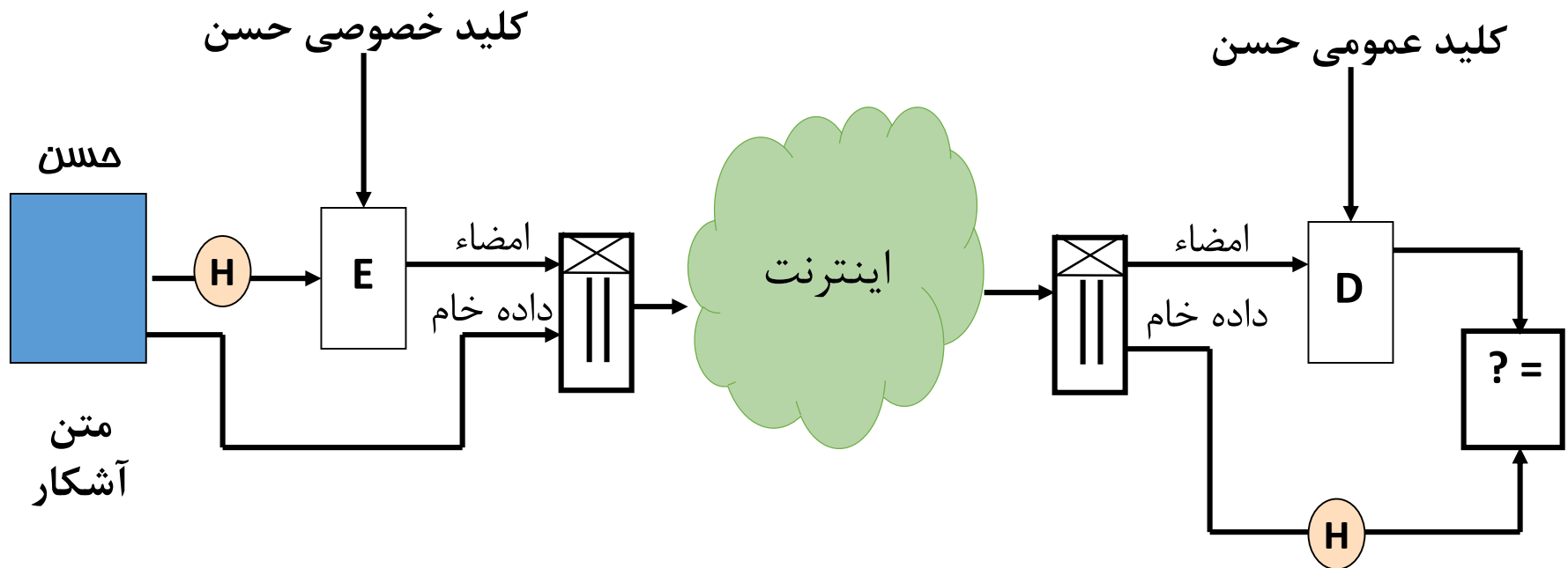
D: رمزگشا

H: تابع درهم‌ساز



- رمزنگاری جهت احراز اصالت و کنترل صحت (امضای دیجیتال)
- فرد می تواند با استفاده کلید خصوصی خود، یک امضای دیجیتال برای داده های ارسالی تولید نماید.
- دیگران می توانند با استفاده از کلید عمومی فرد، صحت امضای دیجیتال را بر مبنای داده های دریافتی کنترل نمایند.
- امضای تولید شده تابعی است از داده ها و کلید خصوصی فرد، لذا موارد زیر در مقصد با استفاده از کلید عمومی قابل شناسایی است:
 - استفاده از کلید خصوصی ناصحیح در تولید امضاء
 - تغییر داده های امضاء شده در حین انتقال

- فرآیند تولید امضای دیجیتال و کنترل صحت
- E: رمزگذار
D: رمزگشا
H: تابع درهم‌ساز



• تشخیص نفوذ (Intrusion Detection)

فرآیند نظارت بر وقایع رخ داده در یک شبکه و یا سیستم کامپیوتری در جهت کشف موارد انحراف از سیاستهای امنیتی

سیستم تشخیص سوء استفاده

سیستم تشخیص ناهنجاری

• سیستم تشخیص نفوذ (IDS)

یک نرم افزار با قابلیت تشخیص، آشکارسازی و پاسخ به فعالیت های غیرمجاز یا غیرنرمال در رابطه با سیستم

تشخیص - سیستم تله عسل (Honeypot)

- اغفال و فریب مهاجم جهت جمع‌آوری اطلاعات بیشتر از نحوه عملکرد آن
- شبیه‌سازی یک یا چند سرویس شبکه که بر روی کارگزار مورد حفاظت در حال اجرا می‌باشند.
- معمولاً حاوی اطلاعات و منابع با ارزشی هستند که مورد توجه مهاجمین قرار می‌گیرند و آنها را به سمت خود جذب می‌کنند.
- سیستم تله عسل ریسک امنیتی دارد. اگر مهاجم بر آن تسلط یابد، می‌تواند برای شبکه مشکل‌ساز باشد.



تشخیص - سیستم ضدبدافزار

• وظایف سیستم ضدبدافزار

- پیشگیری از آلودگی به بدافزار (پیش از آلودگی)
- تشخیص انواع بدافزارها و فایل‌های آلوده به بدافزار (پس از آلودگی)
- واکنشی: پاکسازی بدافزارها

• ارائه نسخه‌های جدید در ترکیب با:

- سیستم تشخیص نفوذ مبتنی بر میزبان
- دیواره آتش شخصی
- سیستم تشخیص سایت‌های فیشینگ

• ضرورت بروزرسانی مستمر پایگاه امضای بدافزارها

• **بدافزار (Malware):** یک قطعه کُد، اسکریپت، و یا برنامه که به قصد خرابکاری و اختلال در امنیت سیستم‌ها یا شبکه‌ها منتشر می‌شود.

• اهداف خرابکارانه بدافزارها:

- دزدی اطلاعات محرمانه و نقض حریم خصوصی (مثلا اطلاعات بانکی)
- کندی و ایجاد وقفه و اختلال در سیستم‌ها و سرویس‌دهی
- تخریب و تغییر اطلاعات
- سوءاستفاده از منابع و سرویس‌ها
- باج‌گیری

- | | |
|---|--|
| <input type="checkbox"/> ویروس (Virus) | <input type="checkbox"/> جاسوس افزار (Spyware) |
| <input type="checkbox"/> کرم (Worm) | <input type="checkbox"/> ترس افزار (Scareware) |
| <input type="checkbox"/> اسب تروا (Trojan) | <input type="checkbox"/> جاسوس کیبورد (Key logger) |
| <input type="checkbox"/> بات (Bot) | <input type="checkbox"/> تبلیغ افزار (Adware) |
| <input type="checkbox"/> باج افزار (Ransomware) | <input type="checkbox"/> بمب منطقی (Logic Bomb) |

• ویروس (Virus)

- یک قطعه برنامه کوچک با انتشار از طریق چسبیدن به دیگر فایل‌ها

• کرم (Worm)

- برنامه کوچک مستقل با توانایی کپی شدن و بیشتر انتشار از طریق شبکه

• اسب تروا (Trojan Horse)

- مخفی در یک برنامه مفید یا به صورت یک برنامه به ظاهر مفید

• بات (Bot) و شبکه بات (Botnet)

- فراهم نمودن امکان کنترل تعدادی سیستم قربانی برای مقاصد سوء و انجام حملات جمعی توزیع شده

• باج افزار (Ransomware)

- بدافزاری که دسترسی یا کنترل کاربر به سیستم یا داده‌هایش را محدود می‌نماید (با قفل کردن صفحه، یا رمزگذاری فایلها، یا دزدی فایلها و تهدید به انتشار) و باج‌خواهی می‌نماید.

• جاسوس افزار (Spyware)

- به منظور جاسوسی از سیستم قربانی و ارسال اطلاعات محرمانه.

• ترس افزار (Scareware)

- ترس افزار معمولا با یک سری ترفند به کاربر القا می‌کند که سیستم او دارای مشکلی است یا به یک ویروس آلوده شده و تنها راه پاکسازی آن، نصب همان ترس افزار است.

• تبلیغ افزار (Adware)

- با هدف تبلیغات به خصوص تبلیغات کالاها و خدمات غیرمجاز.

• جاسوس کیبورد (Key Logger)

- بدافزاری که پس از نصب روی سیستم قربانی، آنچه را که صاحب سیستم تایپ می کند ذخیره کرده و برای مهاجم می فرستد.

• بمب منطقی (Logical Bomb)

- بدافزاری که به محض وقوع شرایطی خاص (مثلاً در یک تاریخ مشخص) فعال می شود و به خرابکاری می پردازد.

- وجود سایت فیزیکی مجزا
- ترمیم سایت اصلی در صورت بروز بلایای طبیعی
- وجود سیستم پشتیبان یا افزونه (Replica/Redundant)
- جایگزینی خودکار سیستم (کارگزار) پشتیبان در صورت بروز مشکل در سیستم (کارگزار) اصلی
- پشتیبان گیری داده‌ها (Backup)
- بازیابی داده‌ها و بازگرداندن سیستم به حالت قبل از بروز مشکل یا حمله، با استفاده از داده‌های پشتیبان گیری شده
- استفاده از ضد بدافزار
- جهت ترمیم فایل‌های آلوده

- آموزش و استقرار گروه پاسخ‌گویی به حوادث رایانه‌ای (CERT)
- جهت رسیدگی به حوادث و رخدادهای امنیتی
- مدیریت آسیب‌پذیری‌ها

CERT: Computer Emergency Response Team

ماهر: مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای

CSIRT: Computer Security Incident Response Team

آپا: آگاهی‌رسانی، پشتیبانی، امداد رایانه‌ای

• منبع:

- اسلایدهای دکتر مرتضی امینی - درس امنیت داده و شبکه (منبع اصلی)
- Cryptography And Network Security, 7th Edition, by William Stallings.

آزمایشگاه امنیت داده و شبکه شریف

dnsl.ce.sharif.edu

رایانامه:

m.zolfaghari@sharif.edu