



# درس ۲: ساز و کارهای تأمین امنیت

## • روشهای تامین امنیت

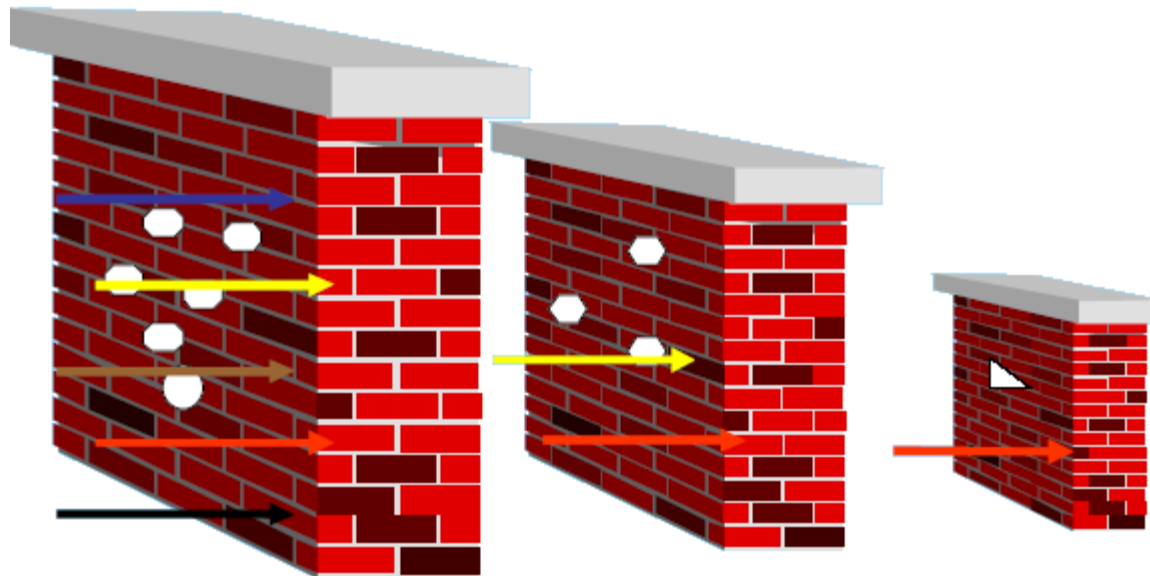
• ساز و کارهای پیشگیری

• ساز و کارهای تشخیص

• ساز و کارهای ترمیم

- دفاع چند لایه (Defense in Depth)
- پیاده‌سازی راه‌حل‌های پیشگیرانه
- پیاده‌سازی راه‌حل‌های تشخیص
- پیاده‌سازی راه‌حل‌های ترمیم و پشتیبانی

□ دفاع چند لایه (دفاع چند لایه): افزایش تعداد لایه‌های دفاعی و دشوار کردن مسیر دسترسی مهاجمین به مناطق حساس و کلیدی سیستم یا شبکه



# مثال: دفاع چند لایه در یک سیستم شبکه‌ای

- امن‌سازی شبکه و ارتباطات
- مقاوم‌سازی کارگزار (Server Hardening)
- مقاوم‌سازی کارخواه (Client Hardening)

# دفاع چند لایه – امن سازی شبکه و ارتباطات

□ استفاده از شبکه مبتنی بر سوئیچ

☞ افزایش کارایی و سرعت

☞ افزایش مصونیت نسبت به شنود بسته

☞ امکان تعریف نواحی مختلف با سطوح امنیتی مختلف (ساز و کار  
(VLAN)

□ استفاده از ابزارهای مدیریت شبکه

□ توجه به امنیت و محرمانگی ارتباطات Wireless

□ ارزیابی آسیب پذیری های سرویس های شبکه (وب، رایانامه، ...)

# دفاع چند لایه – امن سازی کارگزار

- استفاده از ضد بدافزار (ترجیحاً به صورت Corporate)
- استفاده از وصله‌های امنیتی (Patch) به روز سیستم‌عامل و نرم‌افزارهای نصب شده
- تغییر در تنظیمات پیش‌فرض
- 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 ....

# دفاع چند لایه – امن سازی کارخواه

- استفاده از ضد بدافزار (ترجیحاً به صورت Corporate)
- استفاده از دیوار آتش شخصی
- استفاده از وصله‌های امنیتی به روز سیستم‌عامل و نرم‌افزارهای نصب شده
- تغییر در تنظیمات پیش فرض
- مقاوم سازی (مرورگر و ...)




# مثال: دفاع چند لایه در سیستم نرم‌افزاری

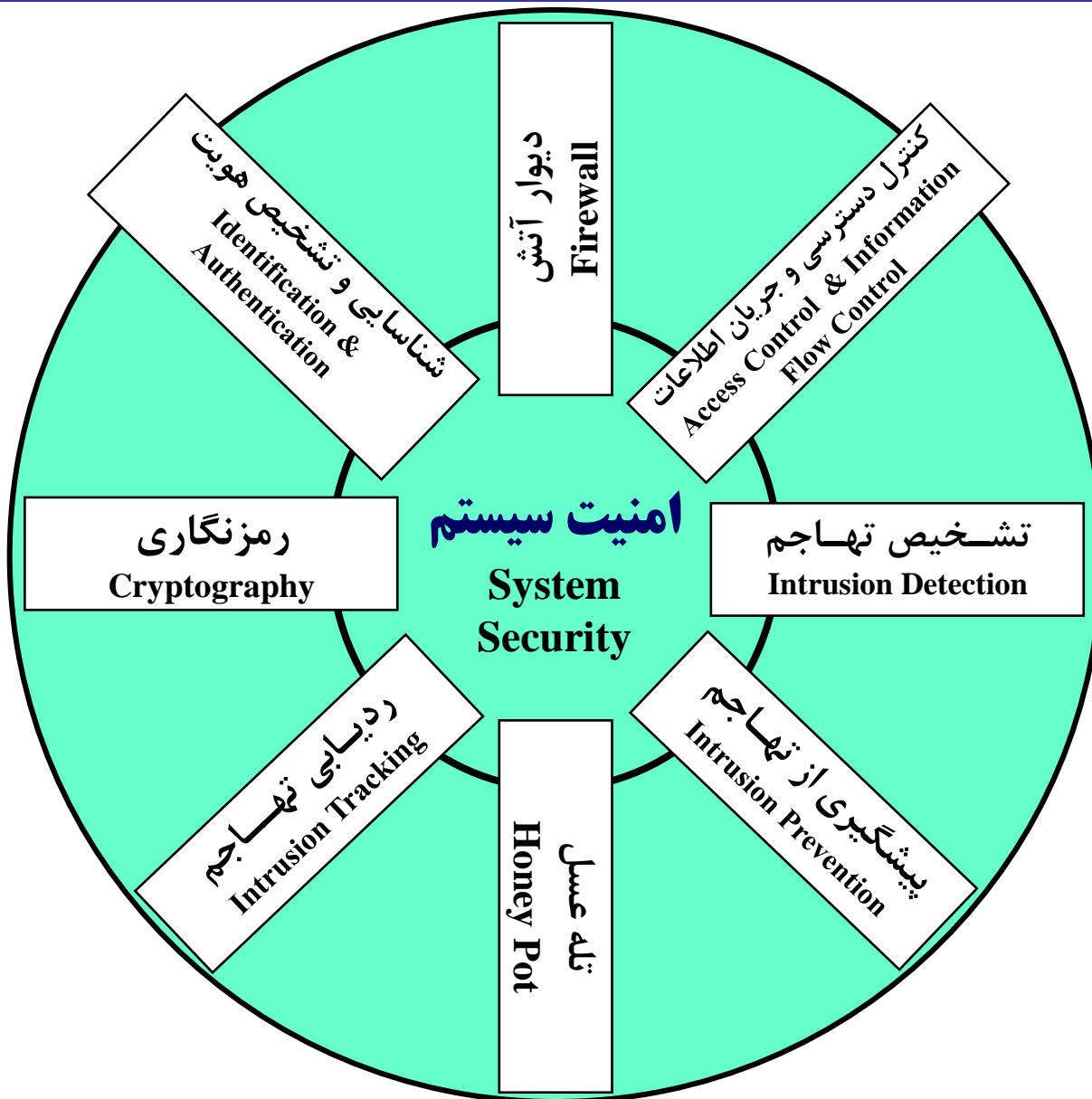
□ امن‌سازی همه لایه‌های نرم‌افزاری یک سیستم شامل:

شبکه (Network) 

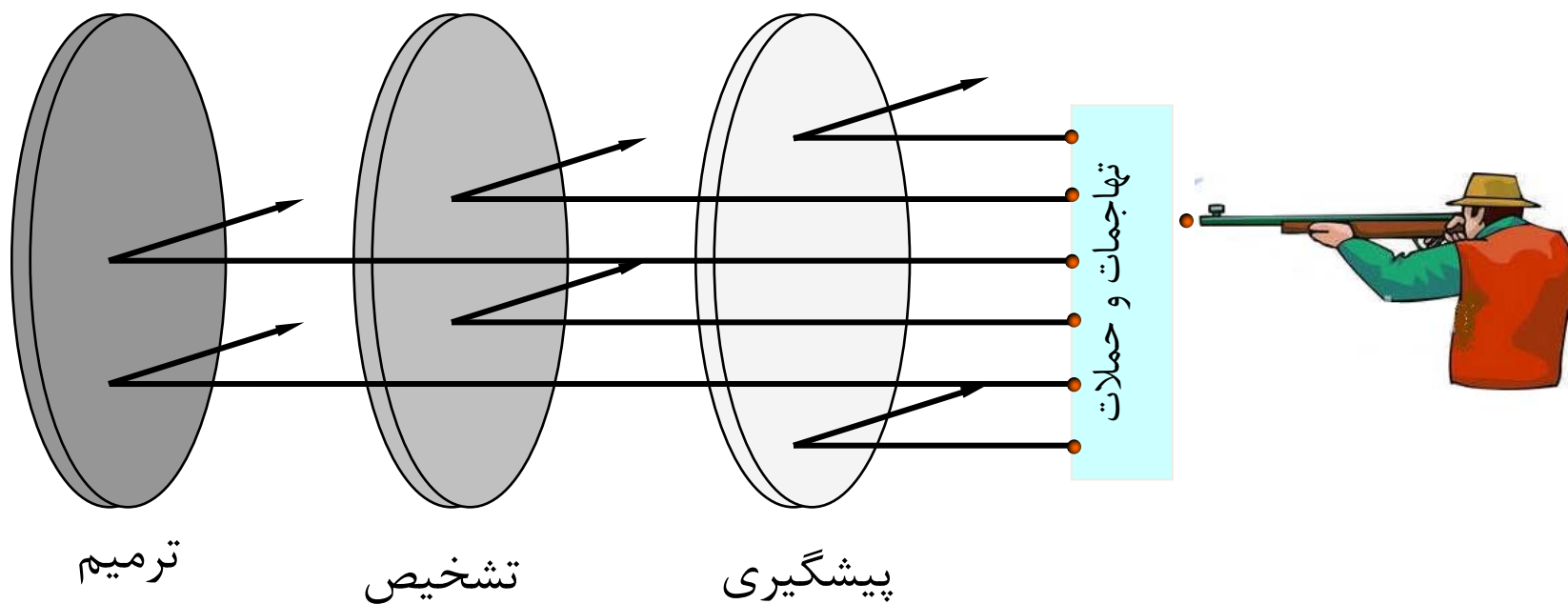
سیستم‌عامل (Operating System) 

سیستم مدیریت پایگاه داده‌ها (DBMS) 

برنامه کاربردی (Application) 



# مراتب مقابله با نفوذ و تهاجم در سیستم



□ شناسایی و تشخیص هویت

□ کنترل دسترسی

□ دیوار آتش 


□ رمزنگاری (پیشگیری از افشای اطلاعات)

- رمزنگاری و امضای دیجیتال (تشخیص تغییر پیام)
- سیستم تشخیص نفوذ (IDS)
- سیستم تله‌عسل (HoneyPot)

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

- روشهای تامین امنیت
- **ساز و کارهای پیشگیری**
- ساز و کارهای تشخیص
- ساز و کارهای ترمیم

## Identification & Authentication □

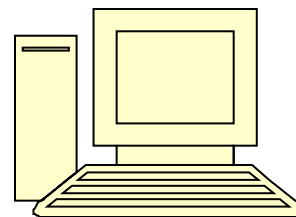
پیش‌نیاز کنترل دسترسی در هر سیستم، شناسایی کاربر 

(متقاضی) و تشخیص هویت مورد ادعای آن

فرآیند شناسایی و تشخیص هویت 



اطلاعاتی از مشخصه‌های کاربر



I&A System

مجاز بودن یا نبودن کاربر



## شناسایی و تشخیص هویت – ۲

□ آنچه که کاربر در ذهن خود دارد:

☞ گذرواژه

☞ شماره شناسایی شخصی PIN

□ مسأله اصلی: حدس یا افشای دانسته فردی

□ راه حل: تغییر دوره‌ای دانسته

□ راه حل: ترکیب با روش‌های دیگر



# شناسایی و تشخیص هویت – ۳

□ آنچه که کاربر به طور فیزیکی در اختیار دارد:

☞ کارت (پلاستیکی، مغناطیسی، هوشمند، ...)

☞ توکن امنیتی (Security Token)

☞ توکن تولید «یکبار رمز» (OTP)

□ مسأله اصلی: مفقود شدن داشته فرد

□ راه حل: ترکیب با روش‌های دیگر



# شناسایی و تشخیص هویت – ۴

□ بر اساس مشخصه‌های طبیعی (زیستی) و غیرقابل جعل کاربر:

☞ اثر انگشت

☞ شبکیه (Retina) چشم

☞ مشخصات صورت

□ مسأله اصلی: هزینه بالا و پیچیدگی سیستمی



# شناسایی و تشخیص هویت – ۵

□ نیاز به حفاظت از گذرواژه در حال گذر و یا ذخیره شده

☞ نمایشی از گذرواژه‌های ذخیره شده در لینوکس (اسلاید بعد)

☞ نمایشی از امکان دزدیده شدن گذرواژه در مسیر (دو اسلاید بعد)

□ پیشگیری از امکان کپی‌برداری و یا افشای کلید ذخیره شده در

توکن

□ نیاز به حفاظت از داده‌های بیومتریک

□ محتوای فایل shadow حاوی گذرواژه‌ها در لینوکس

```
at:*:14521:0:99999:7:::avahi:*:14222:0:99999:7:::  
daemon:*:14222:~:~:~:dnsmasq:*:14222:0:99999:7:::  
.  
.  
.  
root:$6$nDbF5cBs$qRZHp3A...dfIqN:16626:0:99999:7:::
```

# شناسایی و تشخیص هویت – ۷

□ استخراج گذرواژه با شنود روی شبکه (Wireshark)

The screenshot shows the Wireshark interface with a filter set to 'tcp.stream eq 1'. The packet list pane shows several packets, with packet 19 selected. The packet details pane shows the following structure:

- Transmission Control Protocol, Src Port: 13361 (13361), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 591
- Hypertext Transfer Protocol
- HTML Form URL Encoded: application/x-www-form-urlencoded
  - Form item: "username" = "dousti"
  - Form item: "password" = "Yd55\$H\$e"

The packet bytes pane shows the raw data of the selected packet, with the password field highlighted in blue:

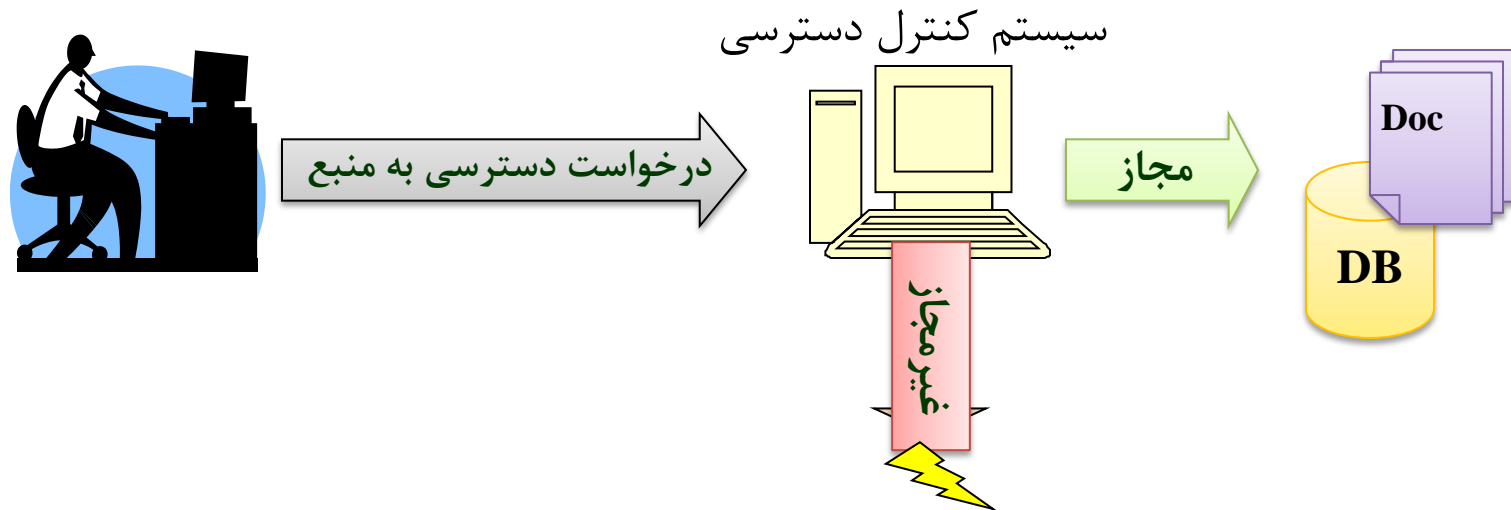
```
0210 6d 2f 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 m/..Acce pt-Encod
0220 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 ing: gzi p, defla
0230 74 65 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 te..Acce pt-Langu
0240 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d age: en- US,en;q=
0250 30 2e 38 2c 66 61 3b 71 3d 30 2e 36 0d 0a 0d 0a 0.8,fa;q =0.6...
0260 75 73 65 72 6e 61 6d 65 3d 64 6f 75 73 74 69 26 username =dousti&
0270 70 61 73 73 77 6f 72 64 3d 59 64 53 35 25 32 34 password =Yd55%24
0280 48 25 32 34 65 H%24e
```

The status bar at the bottom indicates: HTML Form URL Encoded (urlencoded-form), 37 bytes

## Access Control □

ساز و کار بنیادی برای حفظ امنیت در هر سیستم

وظیفه کنترل دسترسی کاربران و سیستم‌های دیگر را به منابع و اطلاعاتی سیستم و یا شبکه مورد حفاظت بر عهده دارد.



□ وجود ارتباط منطقی و امن بین تشخیص 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 داده‌ها یا لیست‌های دسترسی



## Firewall □

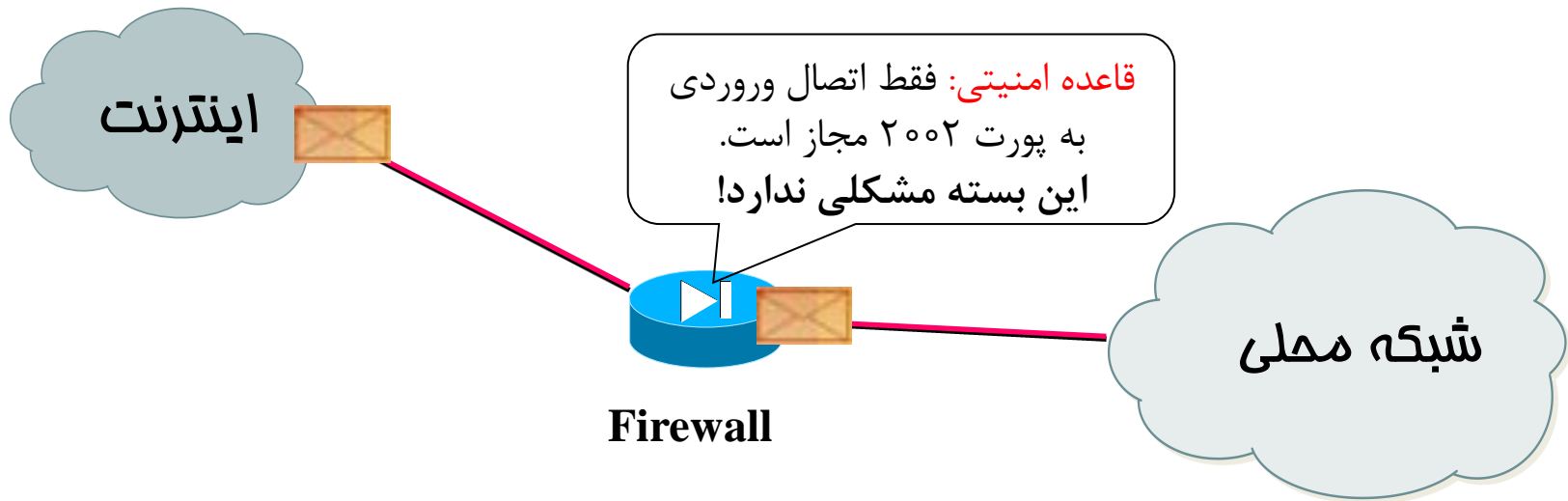
👉 یک سیستم امنیتی مبتنی بر ساز و کار کنترل دسترسی

👉 موظف به کنترل دسترسی کاربران به منابع شبکه

👉 تعیین مجوز دسترسی توسط مدیر امنیتی در قالب قواعد امنیتی

## دیوار آتش - ۲

- 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.



# مشخصات عمومی یک دیوار آتش شبکه‌ای

- تعریف سیاست و قاعده امنیتی
- محافظت در برابر مهاجمان
- ثبت رویدادها
- دارا بودن فیلترهای محتوای برنامه
- پشتیبانی از شبکه خصوصی مجازی (VPN)

□ رمزنگاری = رمزگذاری (Encryption) + رمزگشایی (Decryption). خدمات:

👉 **حفظ محرمانگی (پیشگیری):** اطمینان از اینکه هر داده ذخیره شده و یا ارسالی بر روی شبکه **تنها توسط فرد مورد نظر** قابل رمزگشایی و استفاده است.

👉 **تشخیص هویت (تشخیص):** رمز با کلیدی که صرفاً در اختیار مبدأ (و احتمالاً مقصد) است، و واریسی آن در مقصد.

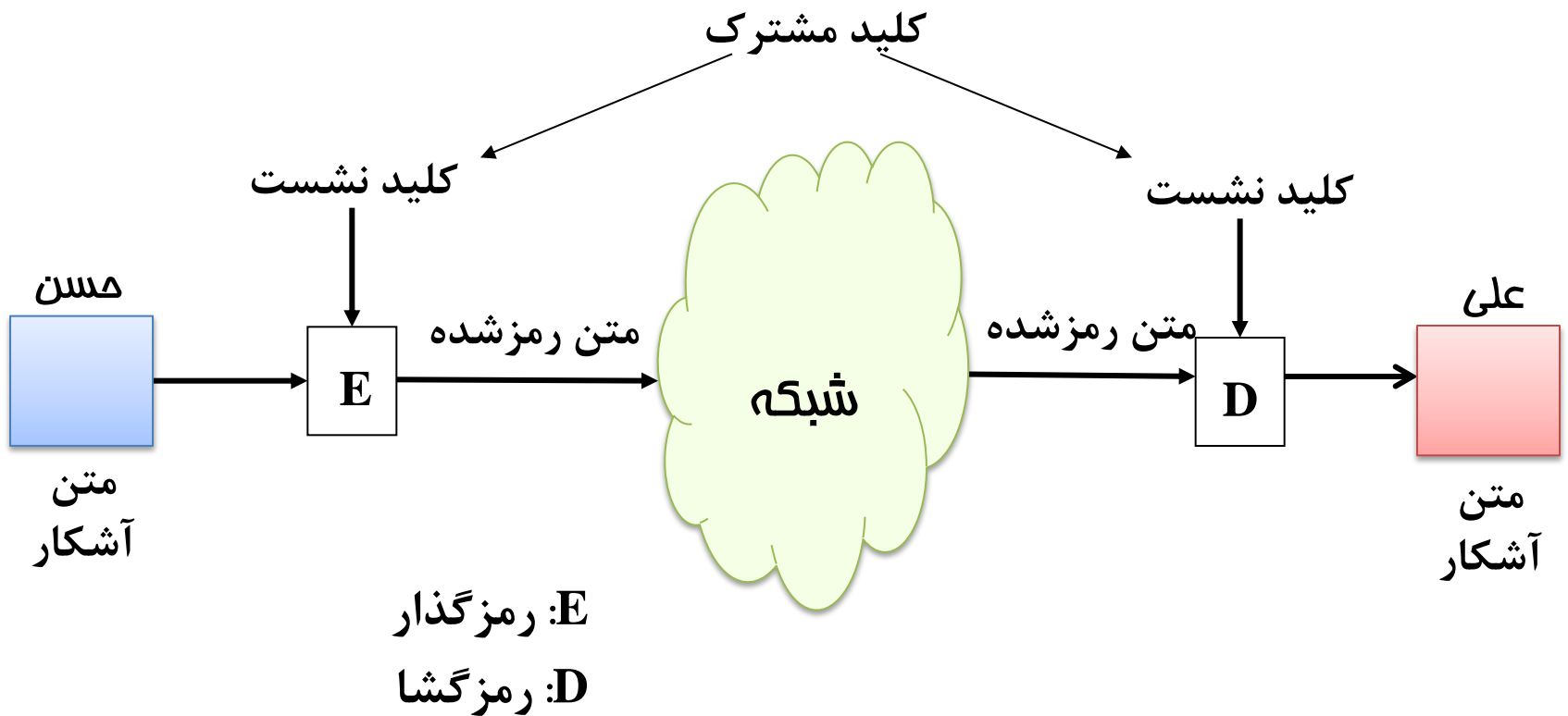
👉 **کنترل صحت (تشخیص):** افزودن یک سرآیند محاسبه شده با یک کلید به داده، و بازسازی و کنترل آن جهت واریسی صحت.

# رمزنگاری متقارن – ۱

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

# رمزنگاری متقارن – ۲

□ رمزنگاری متقارن جهت حفظ محرمانگی



# رمزنگاری نامتقارن – ۱

□ هر فرد دارای یک کلید عمومی و یک کلید خصوصی است.

☞ کلید عمومی در اختیار همگان قرار دارد.

☞ کلید خصوصی صرفاً در اختیار فرد. باید امن نگهداری شود.

□ کاربردها:

☞ رمزنگاری جهت حفظ محرمانگی

☞ امضای دیجیتال جهت تشخیص هویت، کنترل صحت و عدم انکار

□ نیاز به زیرساخت کلید عمومی (PKI) جهت صدور گواهی کلید

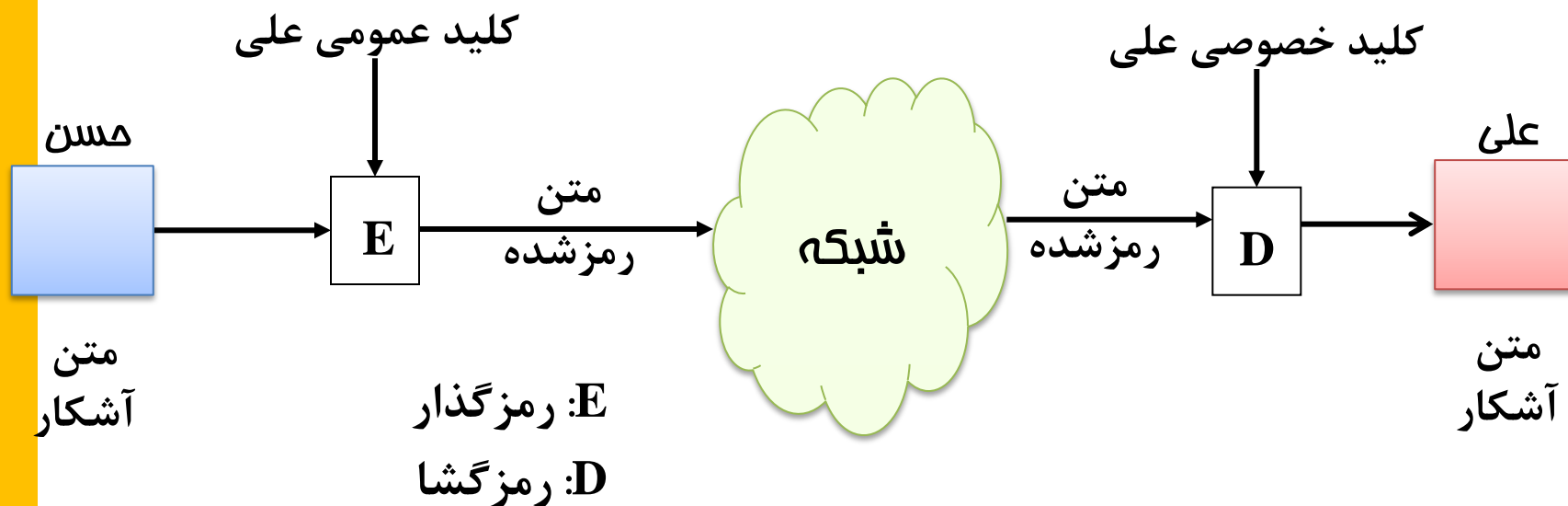
عمومی

## رمزنگاری نامتقارن – ۲

□ رمزنگاری نامتقارن جهت حفظ محرمانگی

☞ هر کسی می‌تواند داده‌ها را با کلید عمومی فرد رمزگذاری نماید.

☞ فقط فرد دارای کلید خصوصی (متناظر کلید عمومی به کاربرده شده) می‌تواند داده‌های رمز شده را رمزگشایی کند.





# روشهای رمزنگاری ترکیبی (Hybrid)

□ جمع محاسن دو روش متقارن و نامتقارن

☞ استفاده از رمزنگاری نامتقارن در تبادل کلید

☞ استفاده از رمزنگاری متقارن در حفظ محرمانگی و صحت دادهها

□ مثالهای کاربردی:

☞ شبکه های خصوصی مجازی VPN

☞ پروتکل SSL

☞ پروتکل SSH

- روشهای تامین امنیت
- ساز و کارهای پیشگیری
- **ساز و کارهای تشخیص**
- ساز و کارهای ترمیم

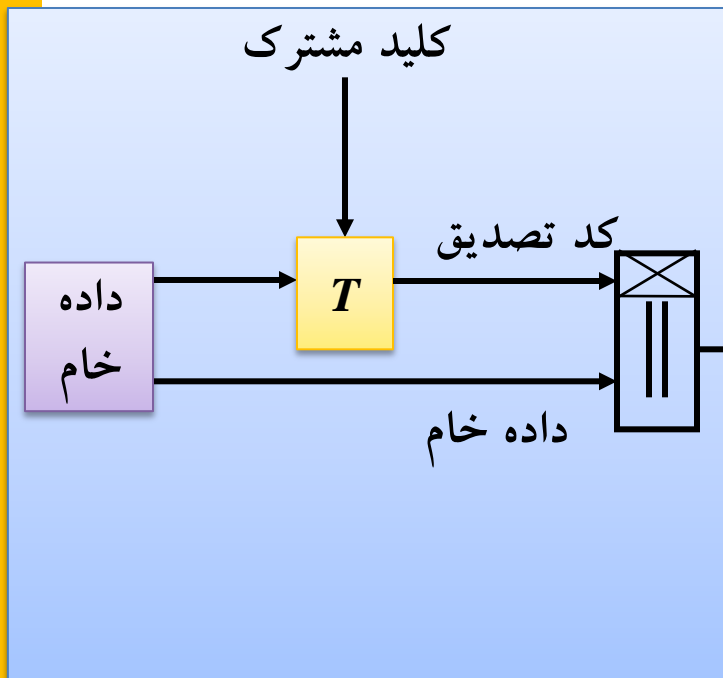
# تشخیص: رمزنگاری متقارن

□ رمزنگاری متقارن جهت حفظ صحت

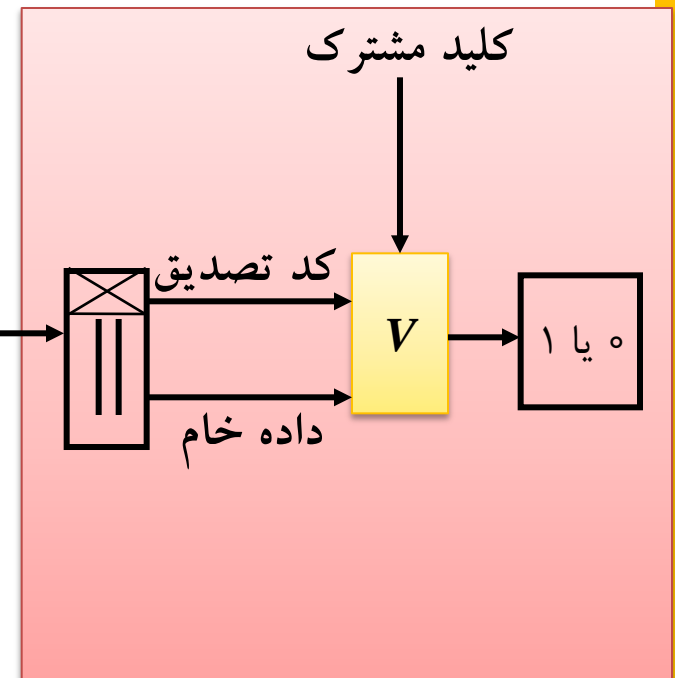
$T$ : Tag

$V$ : Verification

مسلن



علی



# تشخیص: رمزنگاری نامتقارن – ۱

□ رمزنگاری نامتقارن جهت تشخیص هویت و کنترل صحت (امضای دیجیتال)

☞ استفاده از کلید خصوصی جهت تولید امضای دیجیتال از داده‌ها

☞ استفاده از کلید عمومی جهت واری امضای دیجیتال

□ امضا تابعی است از **داده‌ها** و **کلید خصوصی فرد**، لذا موارد زیر در مقصد با استفاده از کلید عمومی قابل شناسایی است:

☞ استفاده از کلید خصوصی ناصحیح در تولید امضا

☞ تغییر داده‌های امضا شده در حین انتقال

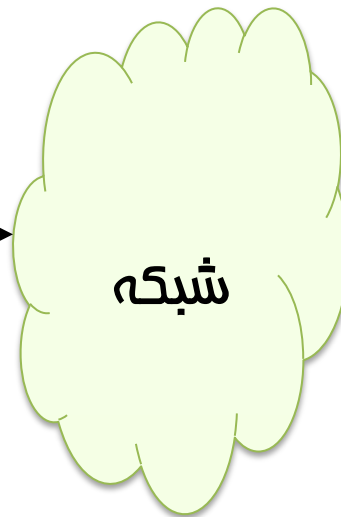
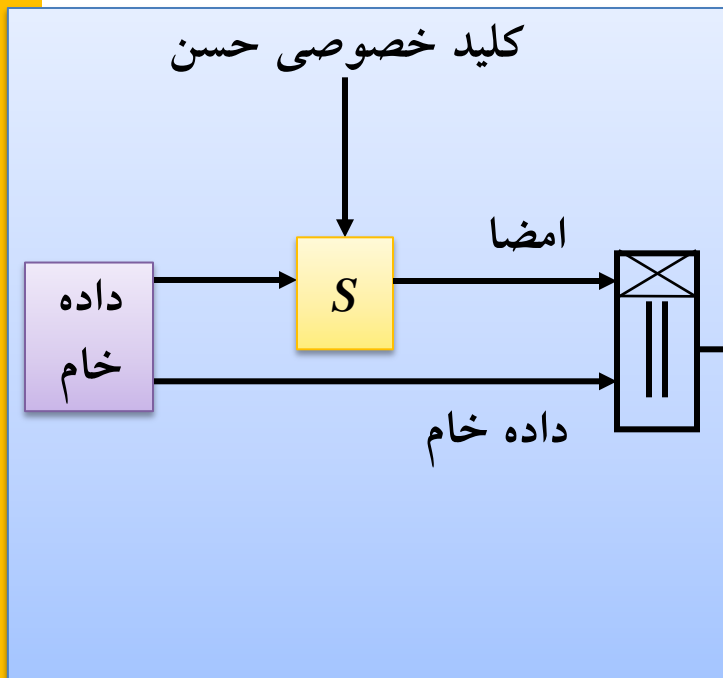
# تشخیص: رمزنگاری نامتقارن – ۲

□ فرآیند تولید امضای دیجیتال و کنترل صحت

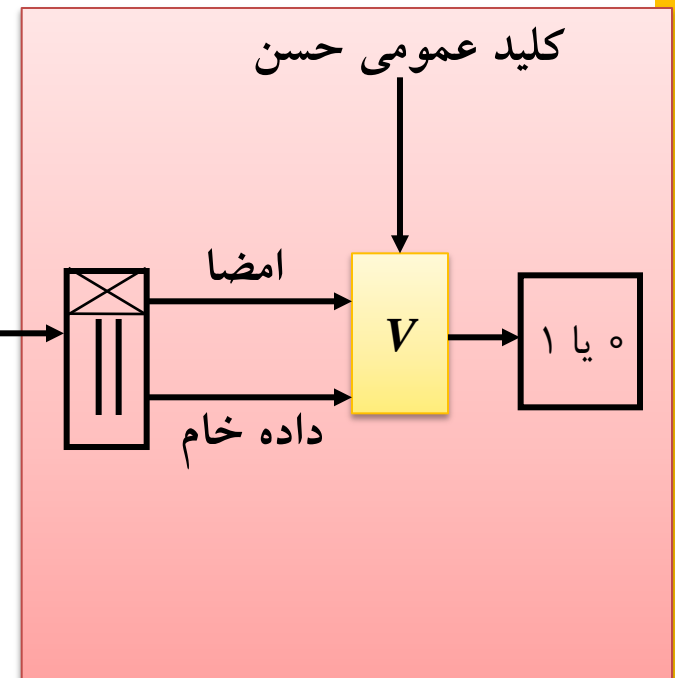
$S$ : Sign

$V$ : Verification

مسلن



علی



# سیستم تشخیص نفوذ (Intrusion Detection)

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

□ سیستم تشخیص نفوذ (IDS)

☞ سیستمی با قابلیت تشخیص فعالیت‌های غیرمجاز یا غیر عادی در سیستم

□ انواع:

☞ سیستم تشخیص سوء استفاده

☞ سیستم تشخیص ناهنجاری

- شناخت حملات موجود
- تعریف الگو (امضای) حملات برای موتور تحلیل
- جستجوی مجموعه‌ای از وقایع که با یک الگوی از پیش تعریف شده مطابقت دارد.
- سیستم‌های تجاری اغلب مبتنی بر این روش عمل می‌نمایند.

# سیستم تشخیص ناهنجاری (Anomaly Detection)

- شناخت عملکرد عادی (هنجار) سیستم
- تهیه پروفایلی از رفتار هنجار سیستم برای موتور تحلیل
- تشخیص فعالیت ناهنجار به عنوان حمله



# سیستم ضد بدافزار – ۱

□ وظایف سیستم ضد بدافزار

☞ پیشگیری از آلودگی به بدافزار

☞ تشخیص انواع بدافزارها و فایل‌های آلوده به بدافزار

☞ پاکسازی بدافزارها

□ انواع بدافزار:

☞ بمب منطقی (Logical Bomb)

☞ ویروس (Virus)

☞ ابزارهای جاسوسی (Spyware)

☞ کرم (Worm)

☞ ابزارهای حمله (Hack & Attack Tools)

☞ اسب تروا (Trojan)

- **ویروس:** برنامه کوچکی که به برنامه‌های دیگر می‌چسبد و با اجرای آنها، به انتشار خود و خرابکاری در سیستم می‌پردازد.
- **گرم:** برنامه **مستقلی** است که خود را به سرعت منتشر کرده و معمولاً منابع و پهنای باند را بی‌جهت اشغال می‌کند.
- **بمب منطقی:** برنامه‌ای که به محض وقوع شرایطی خاص (مثلاً در یک تاریخ مشخص) فعال می‌شود و به خرابکاری می‌پردازد.
- **اسب تروا:** در یک برنامه مفید ذخیره می‌شود یا به عنوان یک برنامه مفید خود را جا می‌زند ولی در عمل به ارسال و افشای اطلاعات حساس می‌پردازد.

□ ارائه نسخه های جدید ضد بدافزار در ترکیب با:

☞ سیستم تشخیص نفوذ مبتنی بر میزبان

☞ دیوار آتش شخصی

☞ سیستم ضد جاسوسی (Anti Spyware)

☞ سیستم تشخیص سایتهای فیشینگ

□ به روزرسانی دائم پایگاه امضای بدافزارها

# 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.
- ظاهراً 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.



- روشهای تامین امنیت
- ساز و کارهای پیشگیری
- ساز و کارهای تشخیص
- ساز و کارهای ترمیم

- وجود سایت فیزیکی مجزا
- وجود سیستم تکراری (Replica)
- پشتیبان‌گیری از داده‌ها (Backup)
- استفاده از ضد ویروس (ترمیم فایل‌های ویروسی شده)

