

madsage
IRan Education
Research
NETwork
(IRERNET)

شبکه آموزشی - پژوهشی مادسیج
با هدف بیبود پیشرفت علمی
و دسترسی راحت به اطلاعات
بزرگ علمی ایران
ابعاد شده است

مادسیج

شبکه آموزشی - پژوهشی ایران

madsg.com
مادسیج





پادا الامن والامان

امنیت داده و شبکه

مرور مکانیزم‌های تامین امنیت

مرتضی امینی - نیمسال اول ۹۰-۹۱



فهرست مطالب

- روش‌های تامین امنیت
- مکانیزم‌های پیشگیری
- مکانیزم‌های تشخیص
- مکانیزم‌های ترمیم

روش‌های تامین امنیت



□ دفاع در عمق

□ پیاده‌سازی راه حل‌های پیشگیرانه

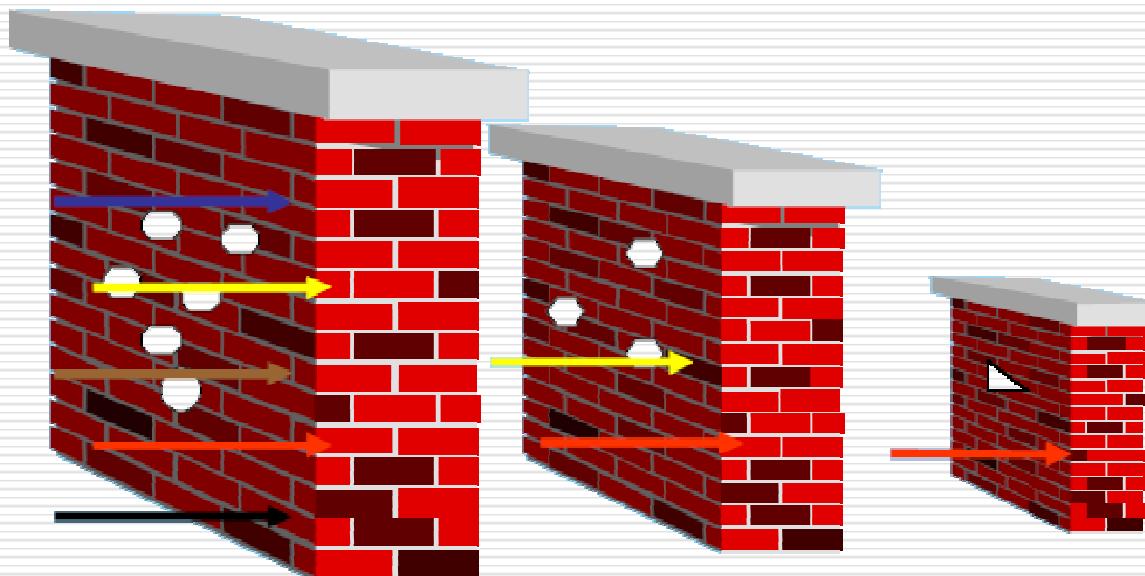
□ پیاده‌سازی راه حل‌های تشخیص

□ پیاده‌سازی راه حل‌های ترمیم و پشتیبانی



دفاع در عمق

□ دفاع لایه به لایه یا دفاع در عمق: افزایش تعداد لایه‌های دفاعی و دشوار کردن مسیر دسترسی نفوذگران به مناطق حساس و کلیدی شبکه



دفاع در عمق در یک سیستم شبکه‌ای



- امنسازی شبکه و ارتباطات
- امنسازی کارگزار
- امنسازی کارخواه

دفاع در عمق - امنسازی 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 (مکانیزم VLAN)

استفاده از ابزارهای مدیریت شبکه

توجه به امنیت و محرومگی ارتباطات Wireless

ارزیابی آسیب‌پذیری‌های سرویس‌های شبکه (email, Web, File Server, ...)

پیاده سازی راه حل‌های ضد ویروس در سطح شبکه (Corporate AV Solutions)

دفاع در عمق – امنسازی کارگزار



- استفاده از ضدویروس (ترجیحاً به صورت Corporate)
- استفاده از وصله‌های امنیتی (Patch) به روز سیستم‌عامل و نرم‌افزارهای نصب شده
- ایمن کردن 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

دفاع در عمق - امنسازی کارخواه



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

دفاع در عمق در سیستم نرم افزاری



امن‌سازی همه لایه‌های نرم افزاری یک سیستم شامل:

شبکه (Network)

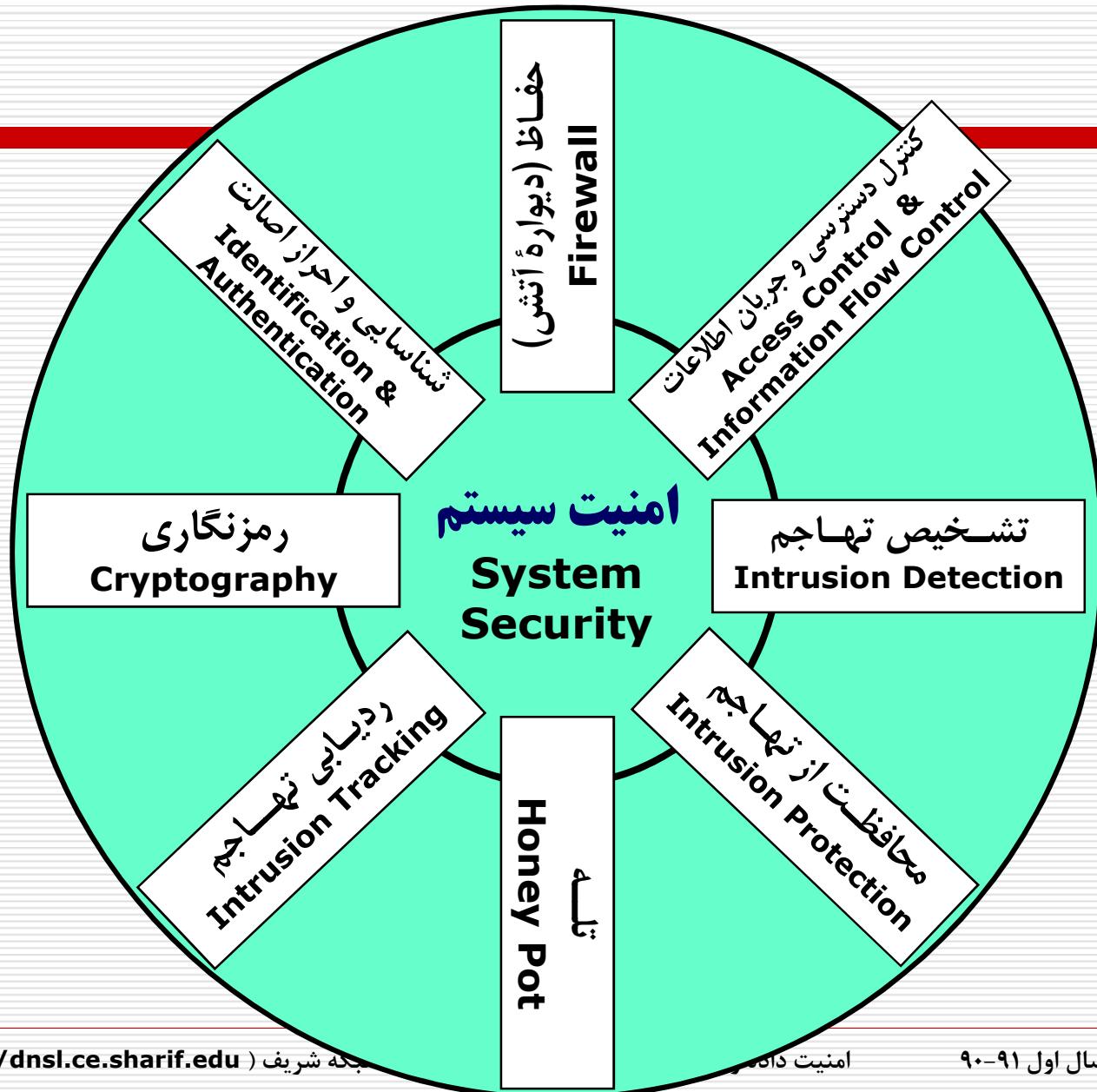
سیستم عامل (Operating System)

سیستم مدیریت پایگاه داده‌ها (DBMS)

برنامه کاربردی (Application)

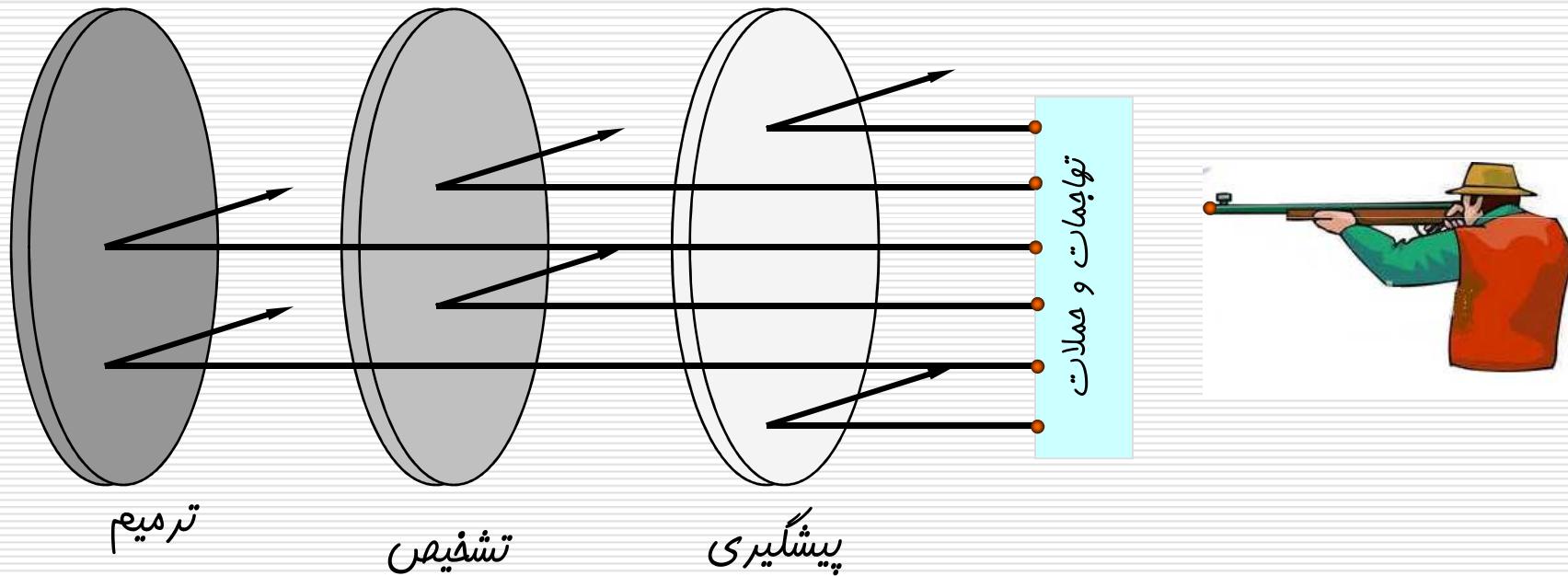


مکانیزمهای امنیتی



مراتب مقابله با نفوذ و تهاجم در سیستم

(پیشگیری، تشخیص، ترمیم)





پیشگیری، تشخیص، ترمیم

□ شناسایی و احراز اصالت

□ کنترل دسترسی

□ حفاظ (دیواره آتش)

□ رمزنگاری و امضای دیجیتال



پیشگیری، تشخیص، ترمیم

□ سیستم تشخیص نفوذ (IDS)

□ سیستم تله‌عسل (Honeypot)



پیشگیری، تشخیص، ترمیم

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



فهرست مطالب

□ روش‌های تامین امنیت

□ مکانیزم‌های پیشگیری

□ مکانیزم‌های تشخیص

□ مکانیزم‌های ترمیم

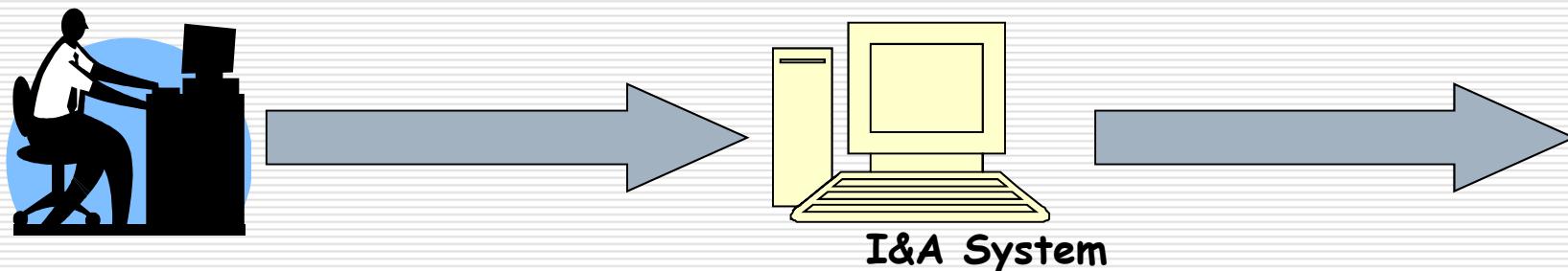
پیشگیری - شناسایی و احراز هویت



Identification & Authentication

پیش نیاز کنترل دسترسی در هر سیستم، شناسایی کاربر (متقاضی) و احراز هویت مورد ادعای آن

فرآیند شناسایی و احراز هویت



پیشگیری - 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 افشاری دانسته فردی

راه حل: تغییر دوره‌ای دانسته

ترکیب با روش‌های دیگر

پیشگیری - شناسایی و احراز هویت



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

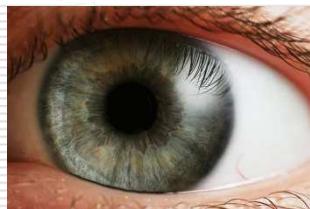


پیشگیری - شناسایی و احراز هویت



احراز هویت بر اساس مشخصه‌های بیولوژیکی کاربر

□ بر اساس مشخصه‌های طبیعی و غیرقابل جعل کاربر:



■ اثر انگشت

■ شبکیه چشم

■ مشخصات صورت

مسئله اصلی: هزینه بالا و پیچیدگی سیستمی

پیشگیری - شناسایی و احراز هویت



حفظ 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 (اسلاید بعد)
 - نمایشی از امکان دزدیده شدن گذرواژه در مسیر (دو اسلاید بعد)
- پیشگیری از امکان کپی برداری و یا افشاری کلید ذخیره شده در توکن
- نیاز به حفاظت از داده های بیومتریک

پیشگیری - شناسایی و احراز هویت



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/UBZO7elW0uvEZ072PvO/69XjeQn6GOT  
6.CG: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/aaporGgAmja8kBRBsILsrE28q95vO  
m:14521:0:99999:7:::
```



پیشگیری - شناسایی و احراز هویت

استخراج گذرواژه با سند روی شبکه

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	ff02::1::ffff:1201	ff02::1::ffff:1201	TCPMDP	
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-Ty pe: 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-urlen 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

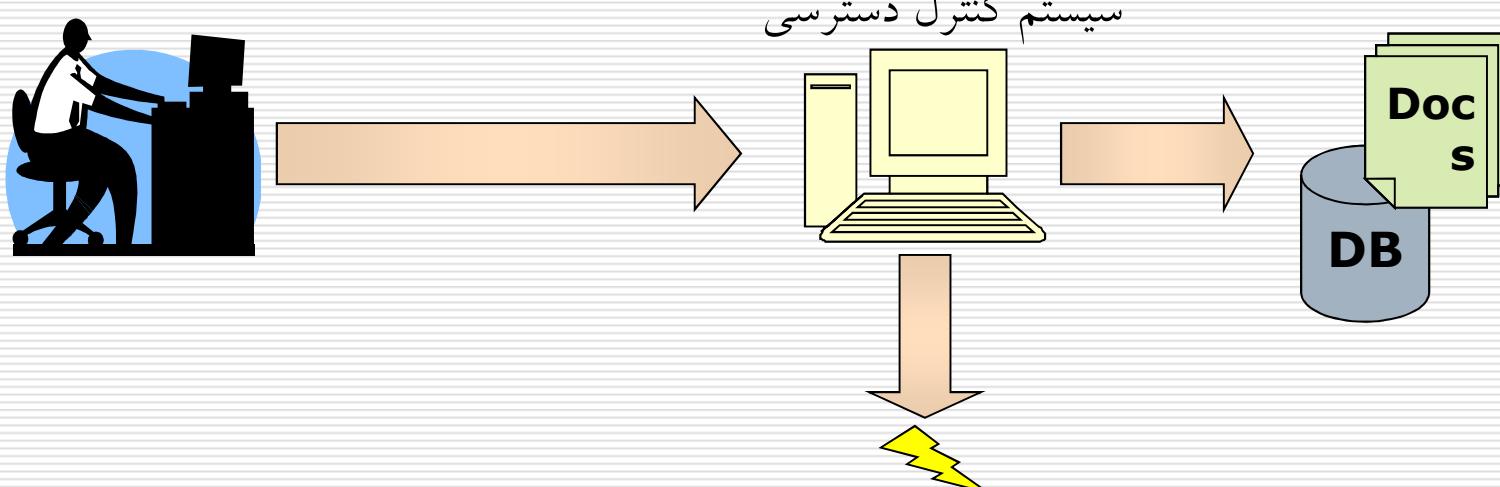
پیشگیری - کنترل دسترسی



Access Control

mekanizm hestehai bray hafte amniyat dar her sistem kntrol dstrsi ast

Wazifeh kntrol dstrsi karbaran o sistemhaye diger ra be manabu o atlauat sistem o ya shbke mord hafat ber uehde dard.



پیشگیری - کنترل دسترسی (ادامه)



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

پیشگیری - کنترل دسترسی



کنترل دسترسی - از خیال تا واقعیت

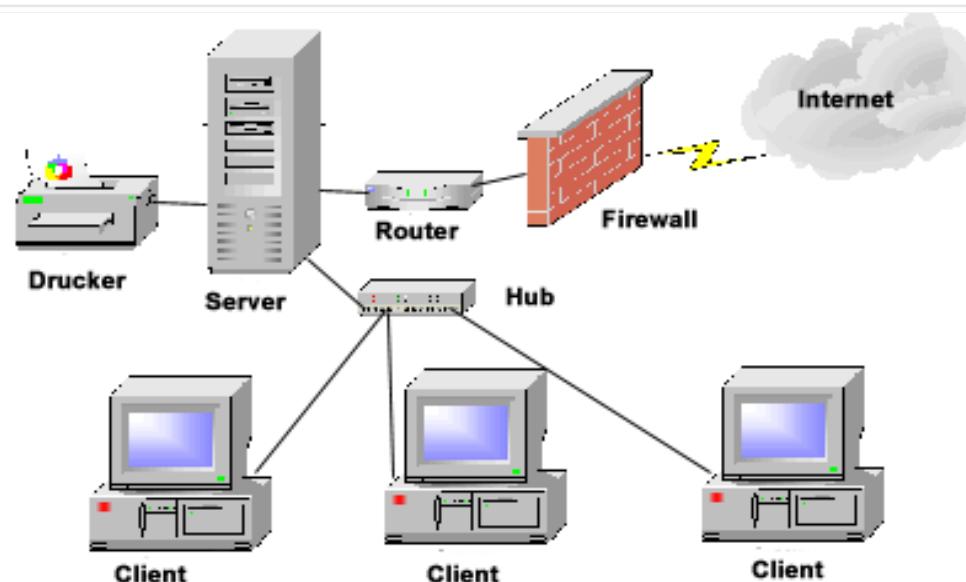
- وجود ارتباط منطقی و امن بین احراز هویت و مجاز شماری
- نیاز به کنترل دسترسی در لایه های اصلی
- لایه واسط کاربری، لایه کاربرد، لایه دسترسی به داده ها (پایگاه داده ها)
- نیاز به حفظ صحت داده ها یا لیست های دسترسی



پیشگیری - دیواره آتش

Firewall □

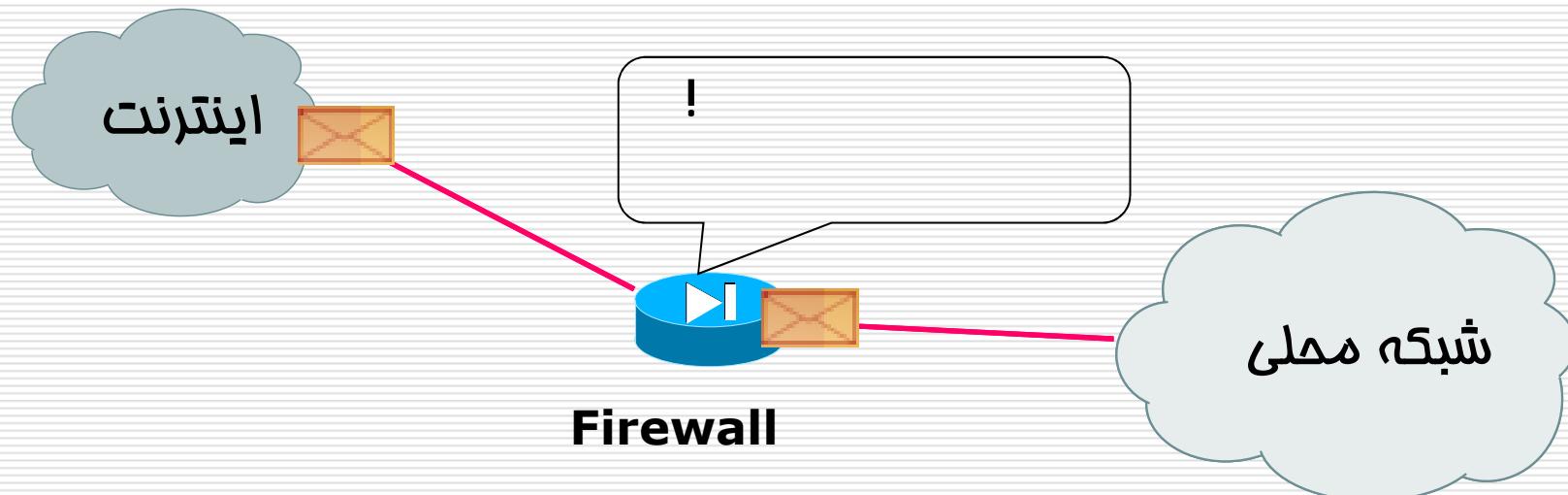
- یک سیستم امنیتی مبتنی بر مکانیزم کنترل دسترسی
- موظف به کنترل دسترسی کاربران خارجی به کارگزاران داخلی
- تعیین مجوز دسترسی توسط مدیر امنیتی در قالب قواعد امنیتی





پیشگیری - دیواره آتش

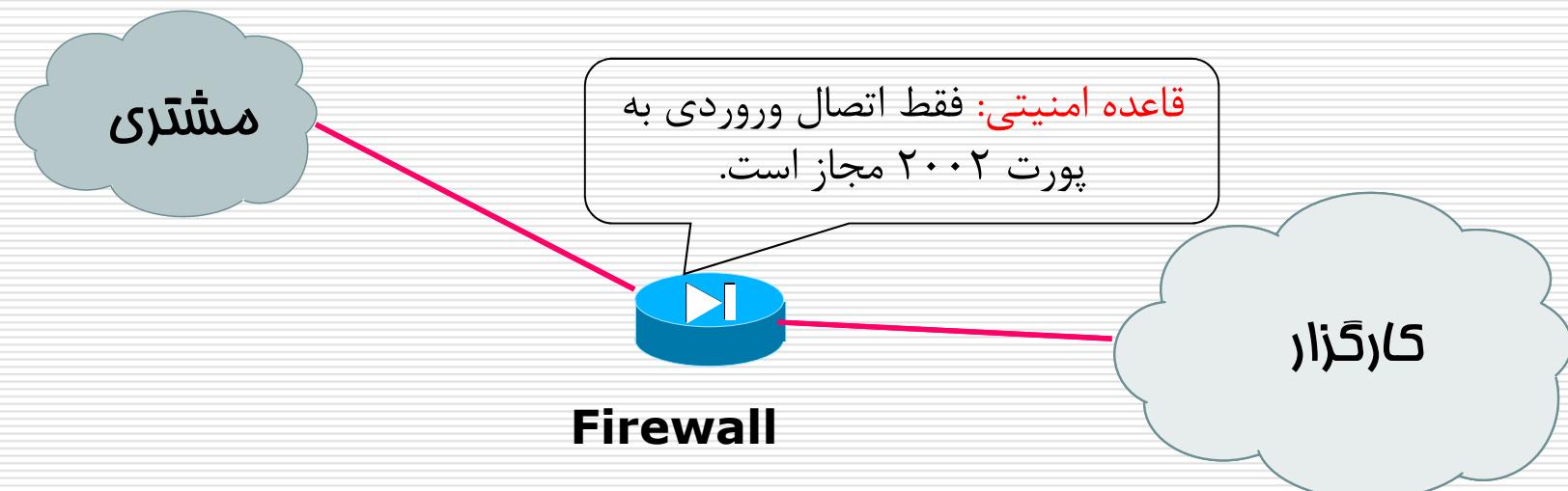
- ابزاری است برای کنترل و نظارت بر بسته‌های ارسالی و دریافتی
- بر اساس قواعدی که برایش تعریف می‌شود به بسته‌ها اجازه عبور یا عدم عبور می‌دهد.





پیشگیری - دیواره آتش

□ نمایش نمونه ای از عملکرد فایروال ویندوز





انواع دیواره آتش

□ دیواره آتش سطح شبکه

■ دیواره آتش سطح شبکه معمولاً تصمیم‌گیری در مورد رد یا قبول بسته‌ها را بر مبنای سرآیند لایه IP انجام می‌دهد.

■ این دیواره آتش علاوه بر اعمال سیاست امنیتی روی بسته‌ها، ترجمه آدرس (NAT) را نیز می‌تواند انجام دهد.

□ دیواره آتش سطح کاربرد

■ دیواره‌های آتش سطح کاربرد معمولاً برای هر قرارداد سطح کاربرد یک کارگزار نماینده (Proxy Server) دارند، که تمام ترافیک مربوط به یک قرارداد به کارگزار نماینده آن قرارداد ارسال می‌شود.

□ ترکیبی از هر دو

مشخصات عمومی یک دیواره آتش شبکه‌ای



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



پیشگیری - رمزنگاری

Cryptography •

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



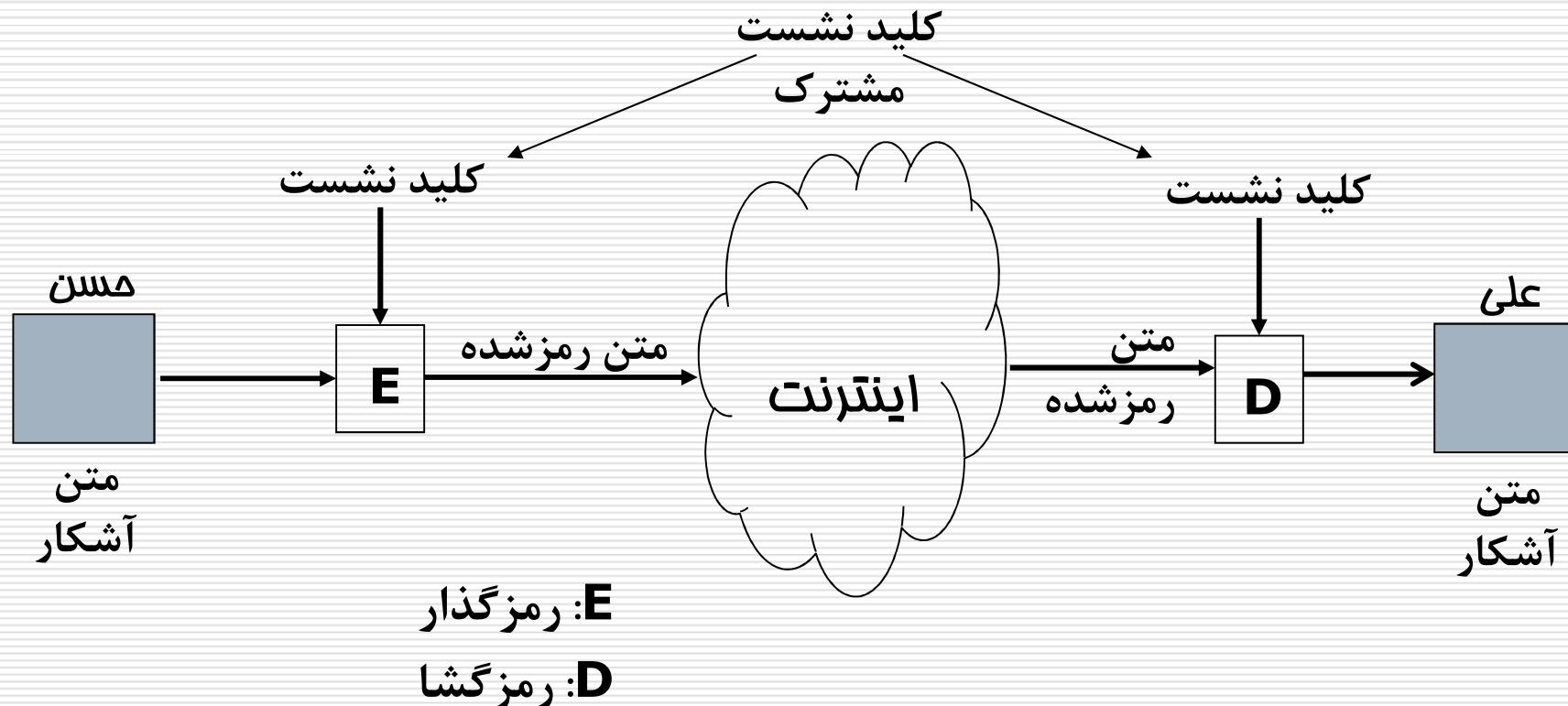
رمزنگاری متقارن

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



رمزگاری متقارن (ادامه)

□ رمزگاری متقارن جهت حفظ محرمانگی

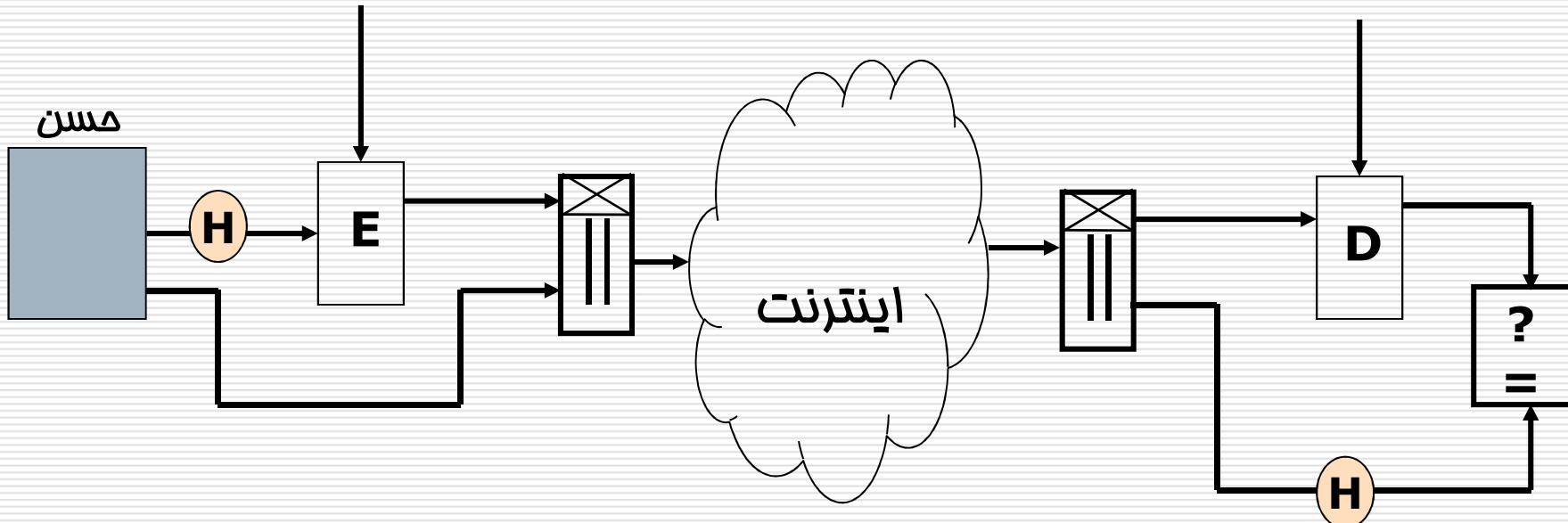




رمزگاری متقارن (ادامه)

:E
:D
:H

□ فرآیند کنترل صحت با رمزگاری متقارن





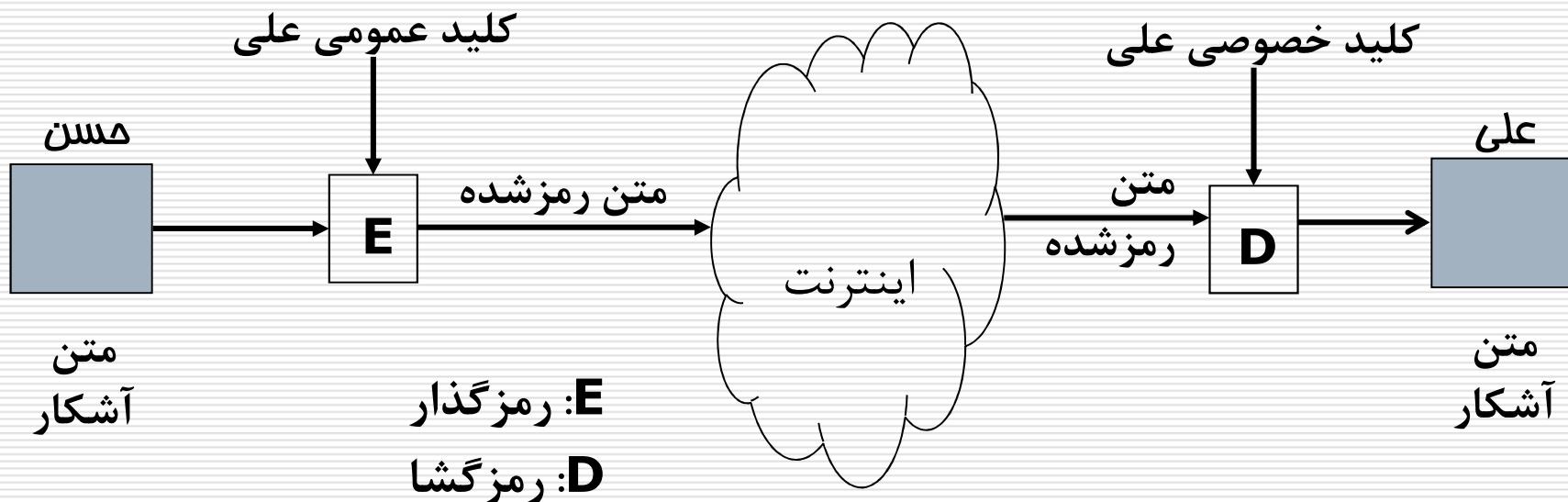
رمزگاری نامتقارن

- 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:
 - رمزگاری 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 نامتقارن (ادامه)

- رمزنگاری جهت حفظ محرمانگی
- هر کسی می‌تواند داده‌ها را با کلید عمومی فرد رمزگذاری نماید.
- فقط فرد دارای کلید خصوصی (منتظر کلید عمومی به کاربرده شده) می‌تواند داده‌های رمز شده را رمزگشایی کند.





رمزنگاری نامتقارن (ادامه)

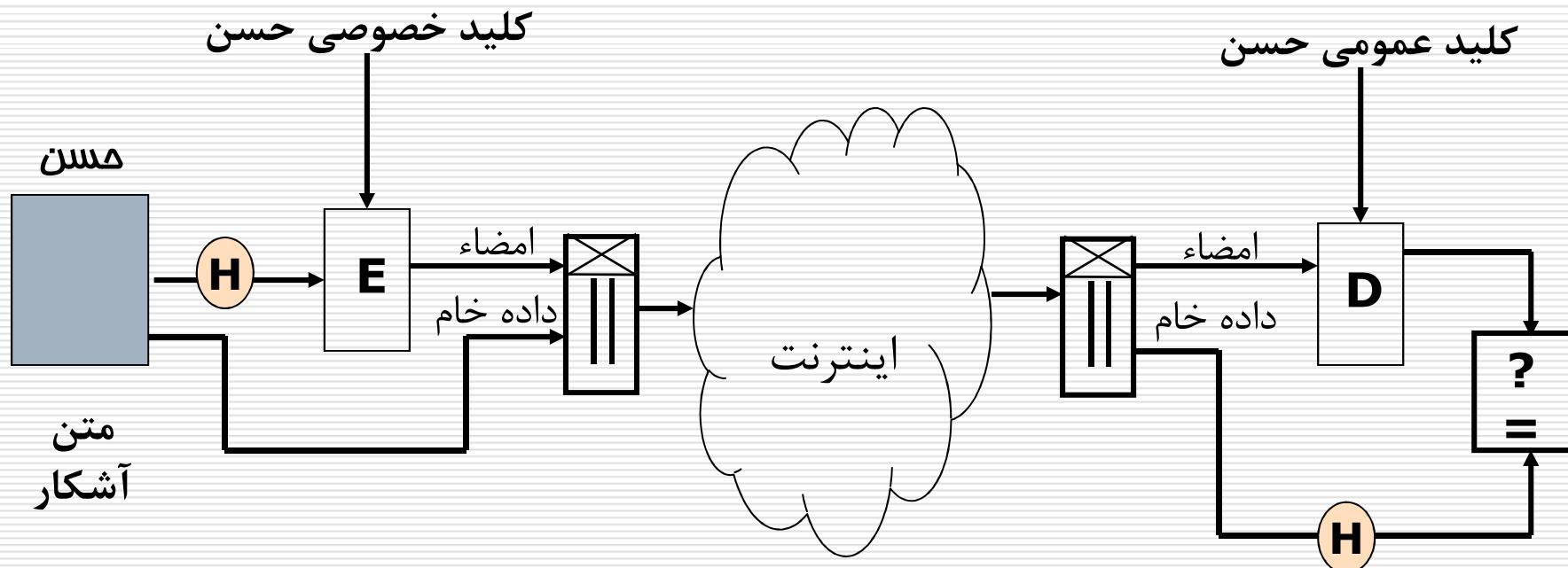
- رمزنگاری جهت احراز اصالت و کنترل صحت (امضای دیجیتال)
- فرد می‌تواند با استفاده کلید خصوصی خود از داده‌ها یک امضای دیجیتال تولید نماید.
- دیگران می‌توانند با استفاده از کلید عمومی فرد، صحت امضای دیجیتال را بر مبنای داده‌های دریافتی کنترل نمایند.
- امضای تولیدشده تابعی است از داده‌ها و کلید خصوصی فرد، لذا موارد زیر در مقصد با استفاده از کلید عمومی قابل شناسایی است:
 - استفاده از کلید خصوصی ناصحیح در تولید امضاء
 - تغییر داده‌های امضاء شده در حین انتقال



رمزنگاری نامتقارن (ادامه)

E: رمزگذار
D: رمزگشایی
H: تابع درهمساز

□ فرآیند تولید امضای دیجیتال و کنترل صحت





روش‌های رمزنگاری ترکیبی

- تجمعی محاسن دو روشن متقارن و نامتقارن
- استفاده از رمزنگاری نامتقارن در تبادل کلید
- استفاده از رمزنگاری متقارن در حفظ محترمانگی و صحت داده ها
- مثال‌های کاربردی:
- شبکه های خصوصی مجازی VPN
- پروتکل SSL
- پروتکل SSH



فهرست مطالب

□ روش‌های تامین امنیت

□ مکانیزم‌های پیشگیری

□ مکانیزم‌های تشخیص

□ مکانیزم‌های ترمیم



تشخیص - سیستم تشخیص نفوذ

□ تشخیص نفوذ (Intrusion Detection)

فرآیند نظارت بر واقع رخداده در یک شبکه و یا سیستم کامپیوتری در جهت کشف موارد انحراف از سیاستهای امنیتی

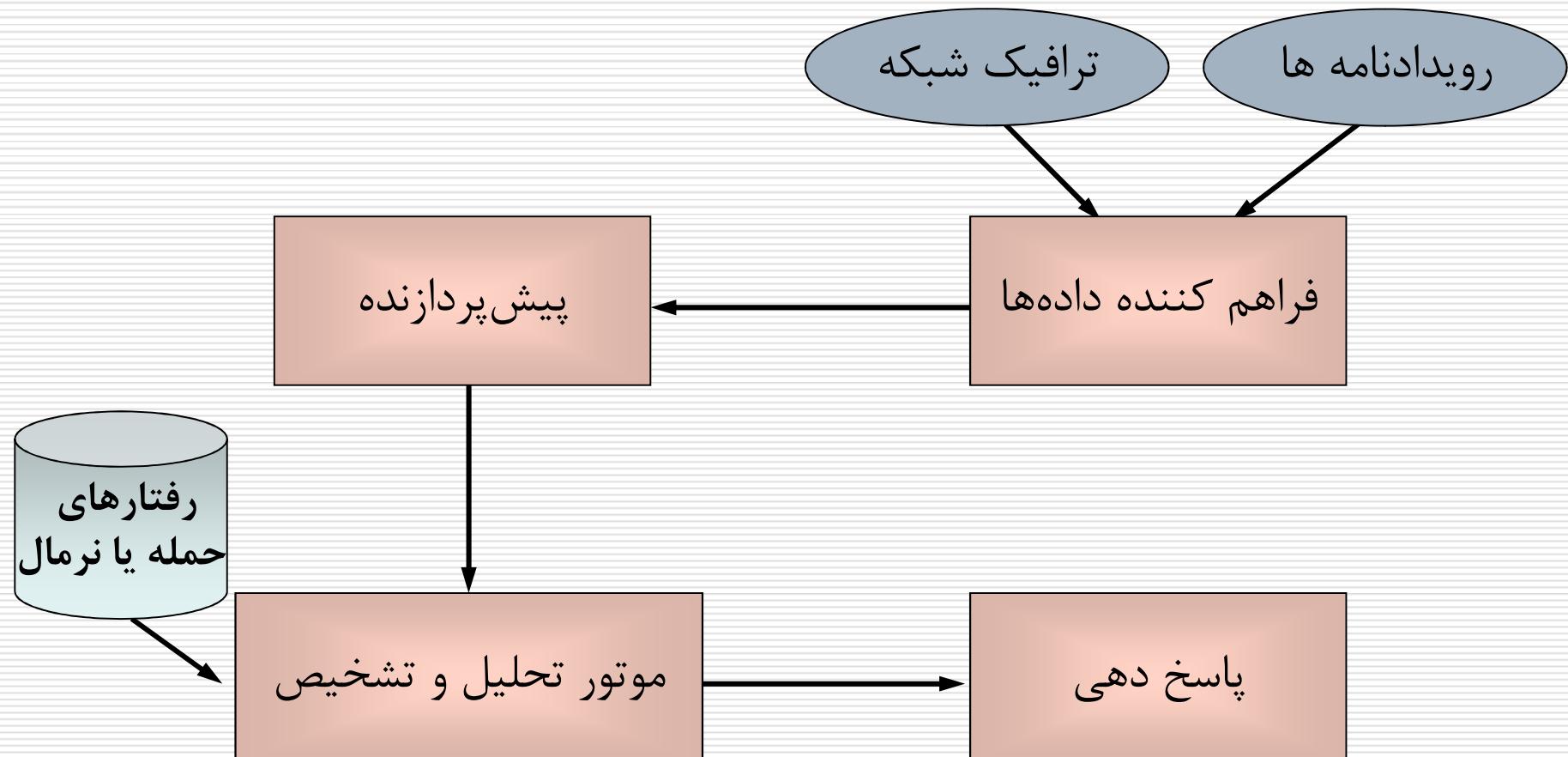
□ سیستم تشخیص نفوذ (IDS)

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



تشخیص نفوذ

□ فرآیند تشخیص نفوذ در IDS





تشخیص سوءاستفاده

□ تشخیص سوءاستفاده (Misuse Detection)

- شناخت حملات موجود
- تعریف الگوی حملات برای موتور تحلیل
- جستجوی مجموعه ای از واقعی که با یک الگوی از پیش تعریف شده مطابقت دارد.
- سیستم های تجاری اغلب مبتنی بر این روش عمل می نمایند.



تشخیص ناهمجارتی

□ تشخیص ناهمجارتی (Anomaly Detection)

- شناخت عملکرد نرمال سیستم
- تهییه نمایه هایی از رفتار نرمال سیستم برای موتور تحلیل
- جستجوی فعالیت غیر نرمال
- بیشتر جنبه تحقیقاتی دارد ولی اخیراً به صورت ترکیبی با تشخیص سوءاستفاده در محصولات تجاری ظاهر شده است.
- برای هدایت ترافیک ناهمجارتی به سوی سیستم تله می‌تواند به کار برد شود.



تشخیص - سیستم ضد بدافزار

□ وظایف سیستم ضد بدافزار

- تشخیص انواع بدافزارها و فایل‌های آلوده به بدافزار
- پاکسازی بدافزارها

□ بدافزار

- ویروس (Virus)
- کرم (Worm)
- تروجان (Trojan)
- بمب منطقی (Logical Bomb)
- ابزارهای جاسوسی (Spyware)
- ابزارهای حمله (Hack & Attack Tools)



تشخیص - سیستم ضد بدافزار

- **ویروس:** برنامه کوچکی که به برنامه‌های دیگر می‌چسبد و به انتشار خود و خرابکاری در سیستم می‌پردازد.
- **کرم:** برنامه مستقلی است که خود را به سرعت منتشر می‌کند و معمولاً منابع و پهنهای 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.
- **تروجان:** در یک برنامه مفید ذخیره می‌شود یا به عنوان یک برنامه مفید خود را جا می‌زند ولی در عمل به ارسال و افشاری اطلاعات حساس می‌پردازد.



تشخیص - سیستم ضد بدافزار

□ ارائه نسخه های جدید در ترکیب با

- سیستم تشخیص نفوذ مبتنی بر میزبان
- دیواره آتش شخصی
- سیستم ضد جاسوسی (Anti Spyware)
- سیستم تشخیص سایتها فیشینگ

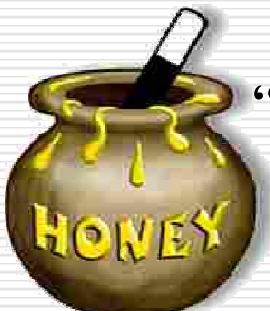
□ بروزرسانی دائم پایگاه تعریف بدافزارها



تشخیص - سیستم تله عسل

□ سیستم تله عسل (Honeypot)

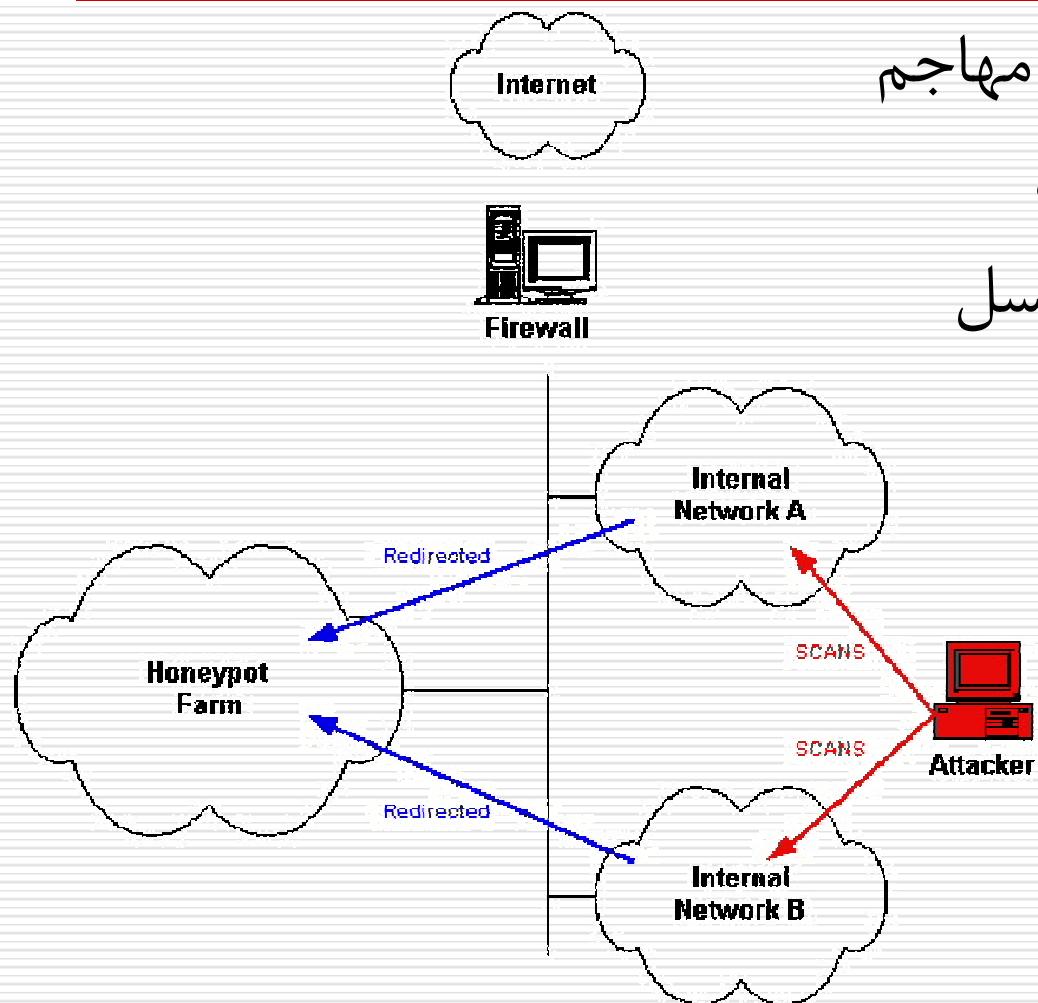
- اغفال و فریب مهاجم جهت جمع‌آوری اطلاعات بیشتر از نحوه عملکرد آن
- شبیه‌سازی یک یا چند سرویس شبکه که بر روی کارگزار مورد حفاظت در حال اجرا می‌باشند.
- معمولاً حاوی اطلاعات و منابع با ارزشی هستند که مورد توجه مهاجمین قرار می‌گیرند و آنها را به سمت خود جذب می‌کنند.
- سیستم تله عسل ریسک امنیتی دارد. اگر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





آرایش قرارگیری تله عسل

□ پس از شناسایی اولیه یک مهاجم (معمولاً با IDS یا دیواره آتش)، ترافیک آن به سمت یک تله عسل هدایت می‌شود.





فهرست مطالب

□ روش‌های تامین امنیت

□ مکانیزم‌های پیشگیری

□ مکانیزم‌های تشخیص

□ مکانیزم‌های ترمیم



ترمیم - پشتیبان‌گیری

- وجود سایت فیزیکی مجزا
- ترمیم سایت اصلی در صورت بروز بلایای طبیعی
- وجود سیستم پشتیبان
- جایگزینی خودکار سیستم (کارگزار) پشتیبان در صورت بروز مشکل در سیستم (کارگزار) اصلی
- پشتیبان‌گیری از پایگاهدادهها
- بازیابی دادهها و بازگرداندن سیستم به حالت قبل از بروز مشکل یا حمله با استفاده از دادههای پشتیبان‌گیری شده



پایان

مرکز امنیت داده و شبکه شریف
<http://dnsl.ce.sharif.edu>

پست الکترونیکی
m_amini@ce.sharif.edu

شبکه آموزشی - پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است



madsg.com
مادسیج

**IRan Education & Research NETwork
(IERNET)**

