یا ذاالامن والامان

امنیت داده و شبکه

مرور مکانیزم‌های تامین امنیت

مرتضی امینی - نیمسال اول ۹۰-۸۹

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

فهرست مطالب

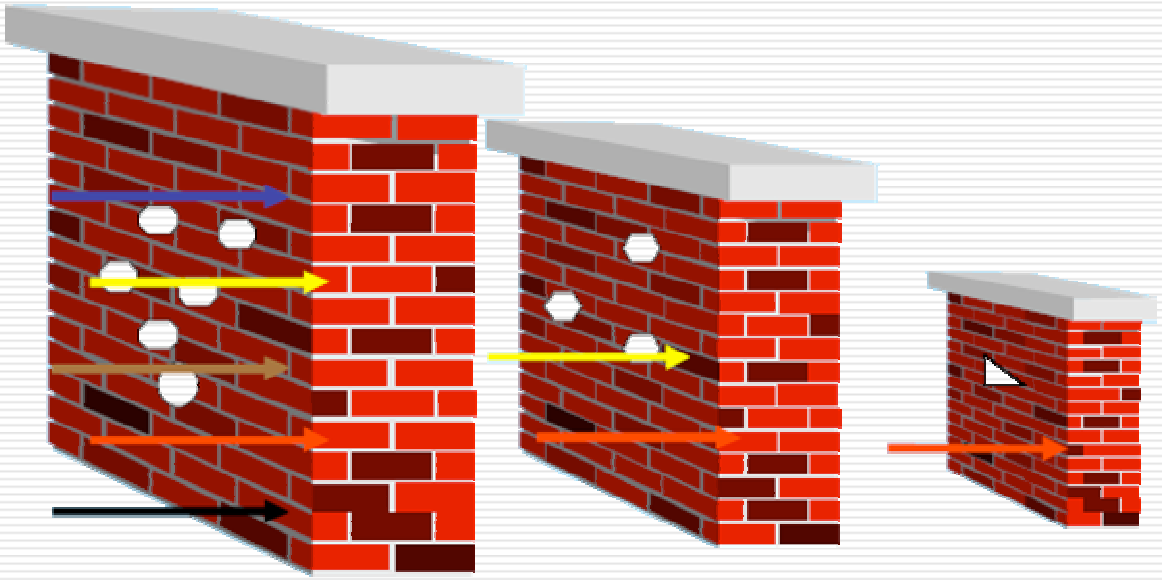
- روشهای تامین امنیت
- مکانیزم‌های پیشگیری
- مکانیزم‌های تشخیص
- مکانیزم‌های ترمیم

روش‌های تامین امنیت

- دفاع در عمق
- پیاده‌سازی راه‌حل‌های پیشگیرانه
- پیاده‌سازی راه‌حل‌های تشخیص
- پیاده‌سازی راه‌حل‌های 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 محرمانگی ارتباطات Wireless
- ارزیابی آسیب‌پذیری‌های سرویس‌های شبکه (email,Web,File Server,...)
- پیاده سازی راه‌حل‌های 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

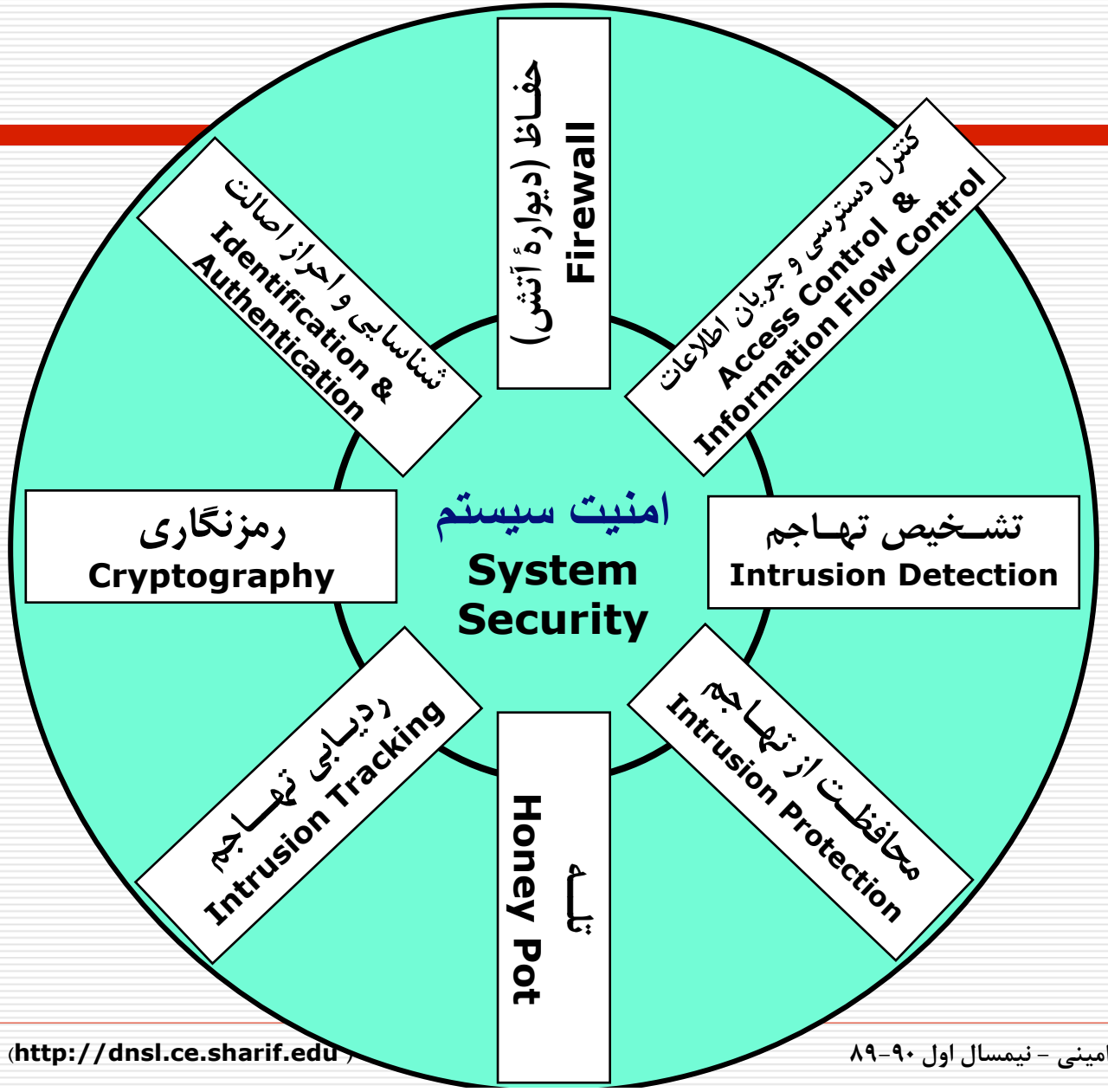
- استفاده از ضد ویروس (ترجیحاً به صورت Corporate)
- استفاده از دیواره آتش شخصی
- استفاده از وصله‌های امنیتی به روز سیستم‌عامل و نرم‌افزارهای نصب شده

دفاع در عمق در سیستم نرم‌افزاری

امن‌سازی همه لایه‌های نرم‌افزاری یک سیستم شامل:

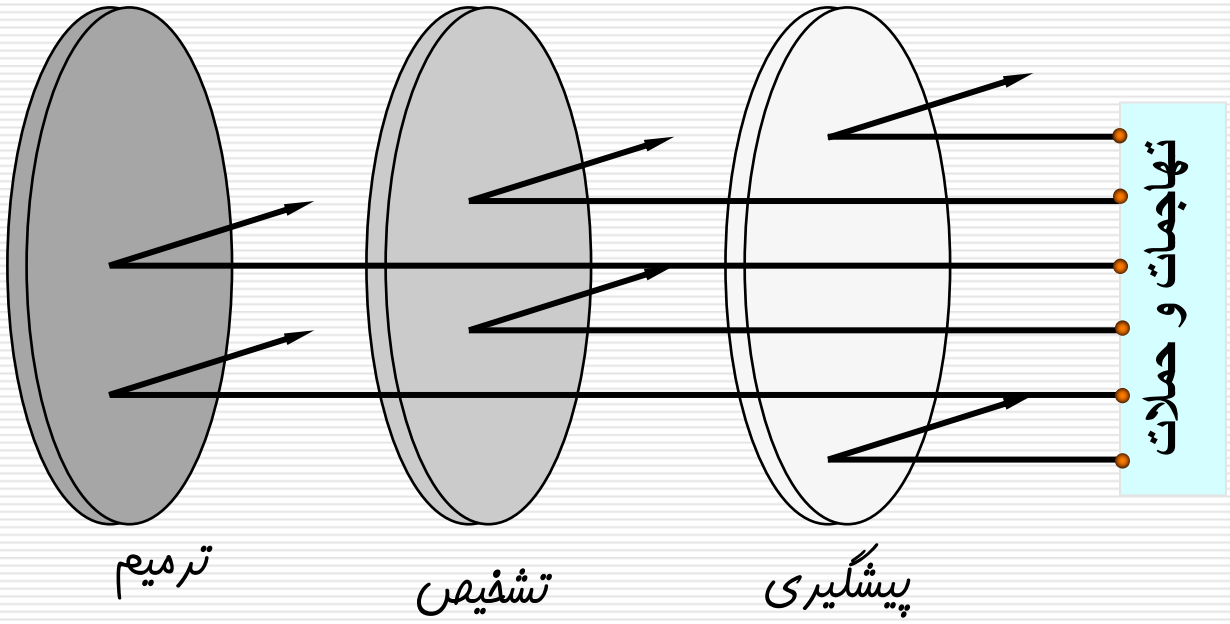
- شبکه (Network)
- سیستم‌عامل (Operating System)
- سیستم مدیریت پایگاه داده‌ها (DBMS)
- برنامه کاربردی (Application)

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 تله (Honeypot)

پیشگیری، تشخیص، ترمیم

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

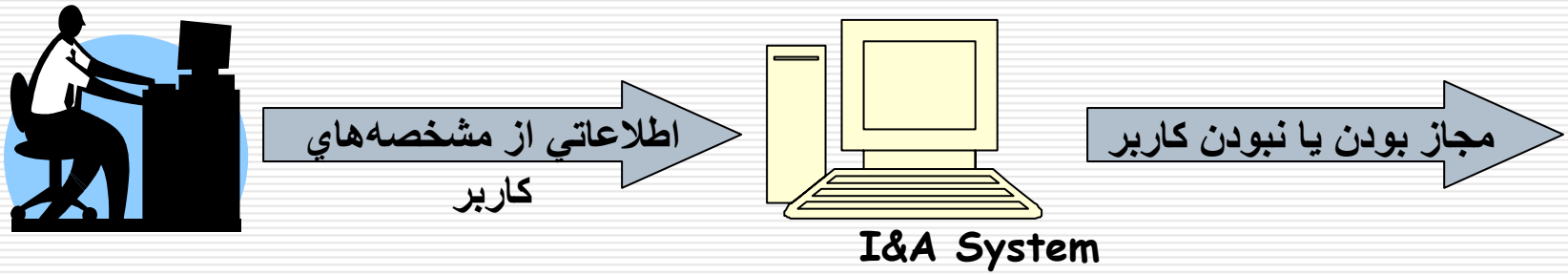
فهرست مطالب

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

پیشگیری – شناسایی و احراز هویت

Identification & Authentication

- پیش‌نیاز 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 افشای دانسته فردی

راه‌حل: 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)

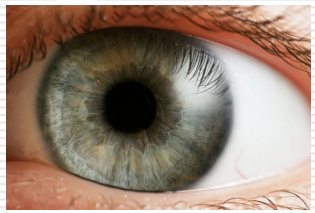
مساله اصلی: مفقود شدن داشته فرد

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



مساله اصلی: هزینه بالا و پیچیدگی سیستمی

پیشگیری – شناسایی و احراز هویت

حفاظت از داده های احراز هویت

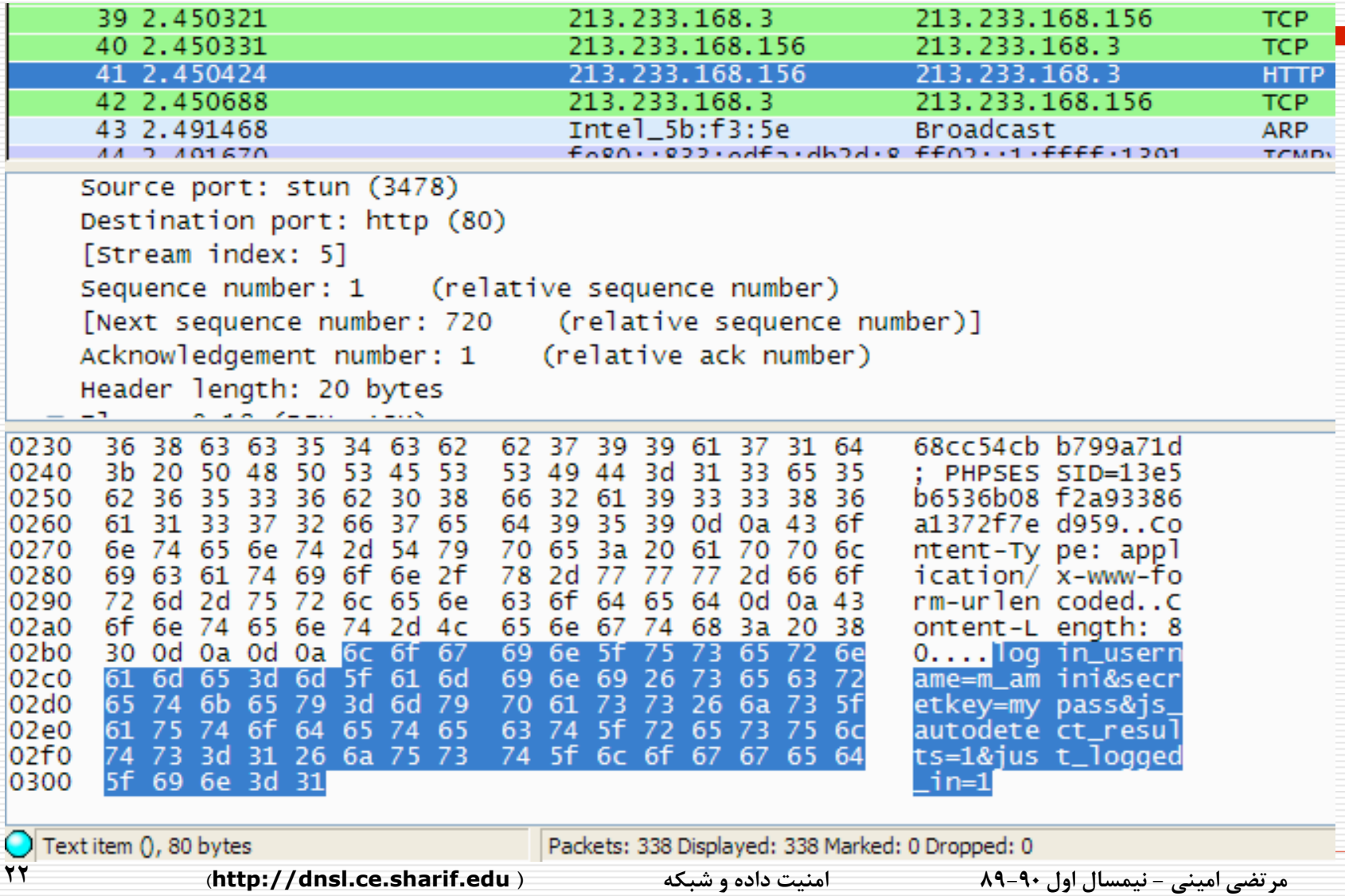
- نیاز به حفاظت از گذرواژه در حال گذر و یا ذخیره شده
  - نمایشی از گذرواژه‌های ذخیره شده در لینوکس (اسلاید بعد)
  - نمایشی از امکان دزدیده شدن گذرواژه در مسیر (دو اسلاید بعد)
- پیشگیری از امکان کپی‌برداری و یا افشای کلید ذخیره شده در توکن
- نیاز به حفاظت از داده‌های بیومتریک

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/aaporGgAmja8kBRBslLsrE28q95vO
m:14521:0:99999:7:::

پیشگیری – شناسایی و احراز هویت

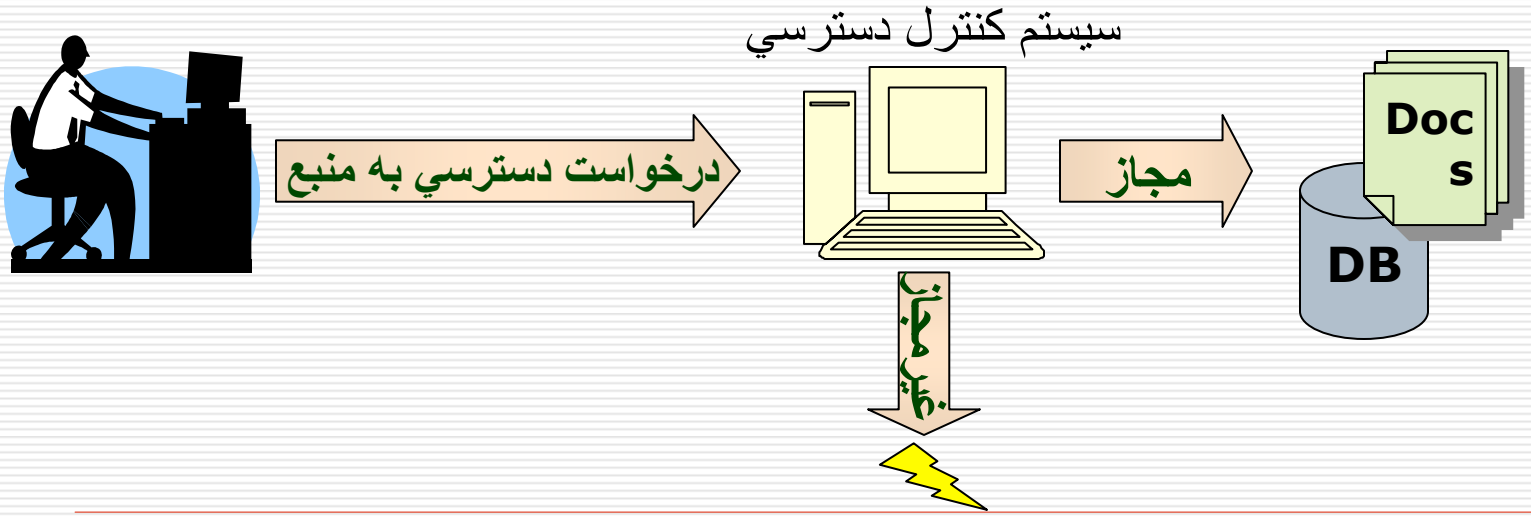


استخراج گذرواژه با شنود روی شبکه

پیشگیری – کنترل دسترسی

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.



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

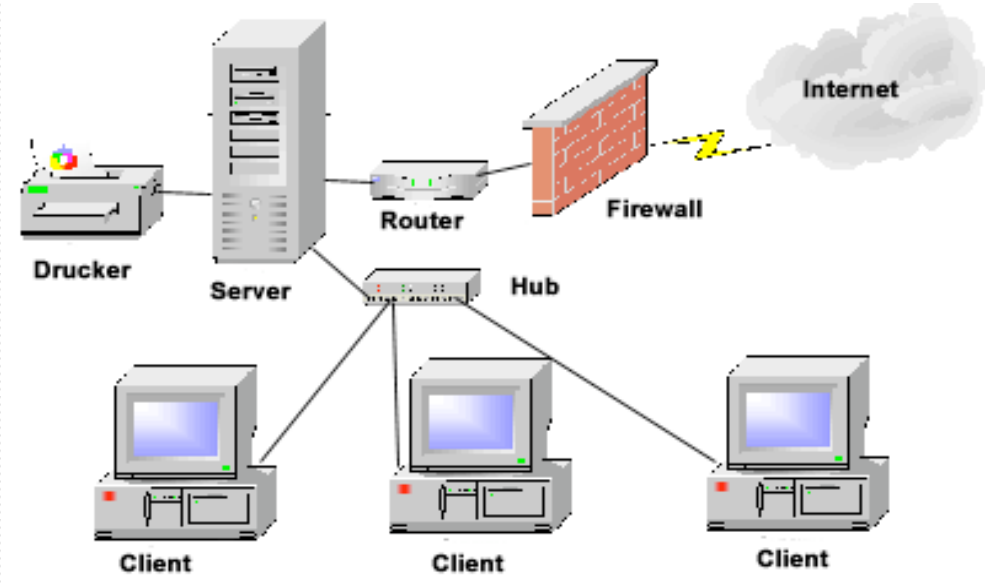
کنترل دسترسی – از خیال تا واقعیت

- وجود ارتباط منطقی و امن بین احراز هویت و کنترل دسترسی
- 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

پیشگیری – دیواره آتش

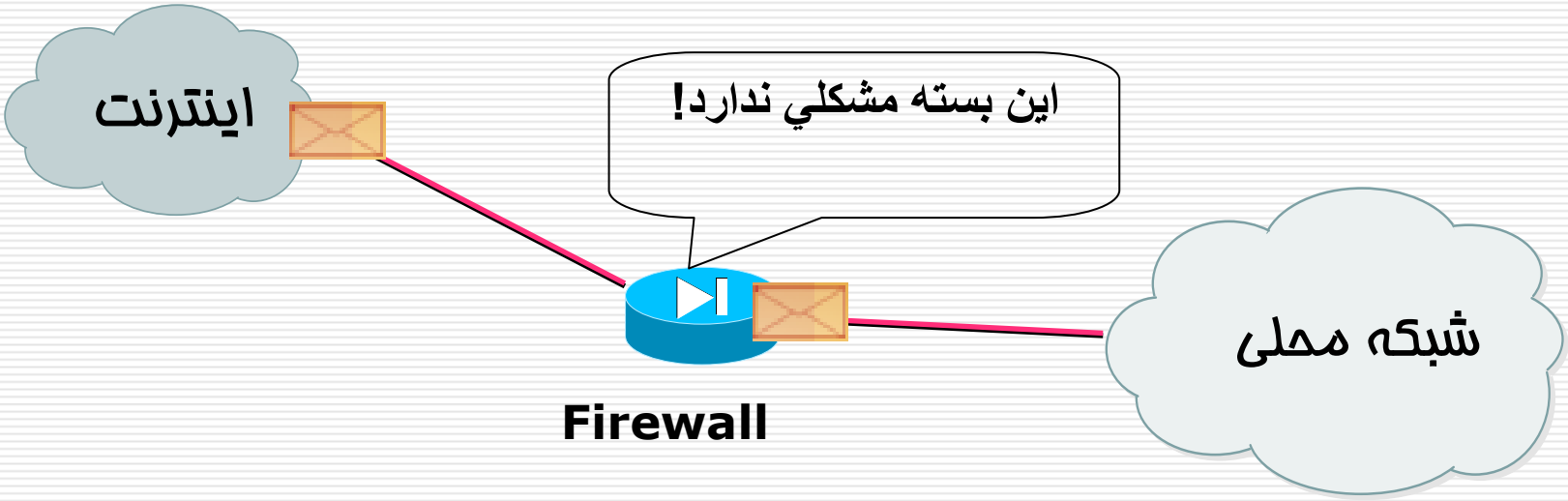
Firewall

- 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



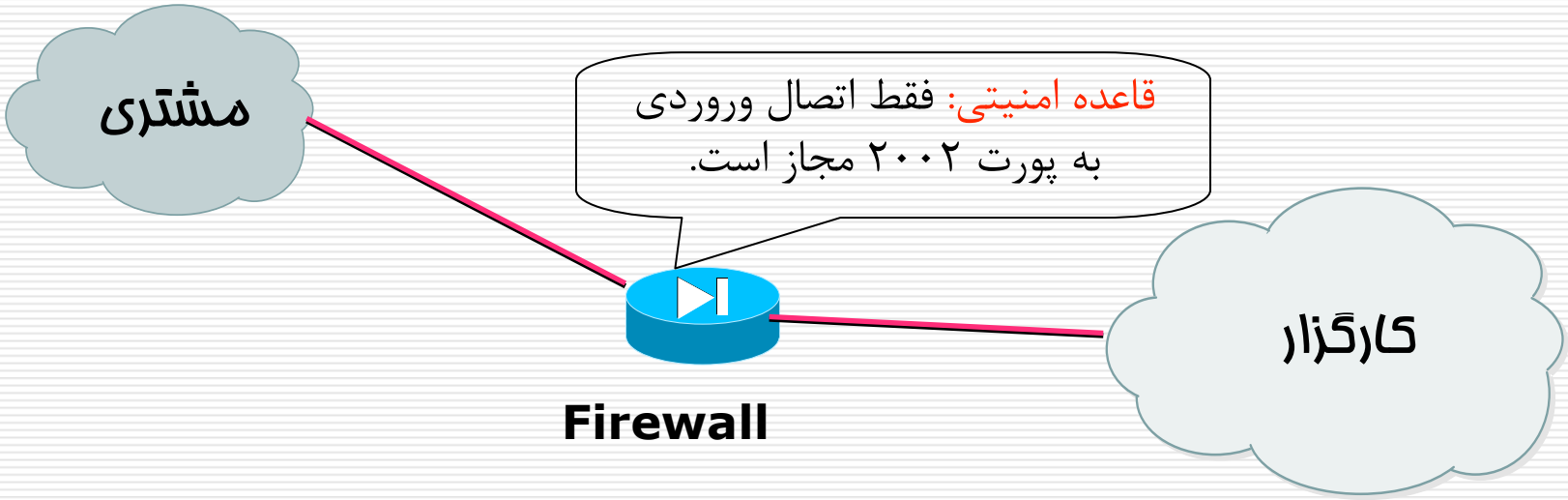
پیشگیری – دیواره آتش

- 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

- دیواره‌آتش 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 دادهٔ ذخیره شده و یا ارسالی بر روی شبکه تنها توسط گیرندهٔ 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.

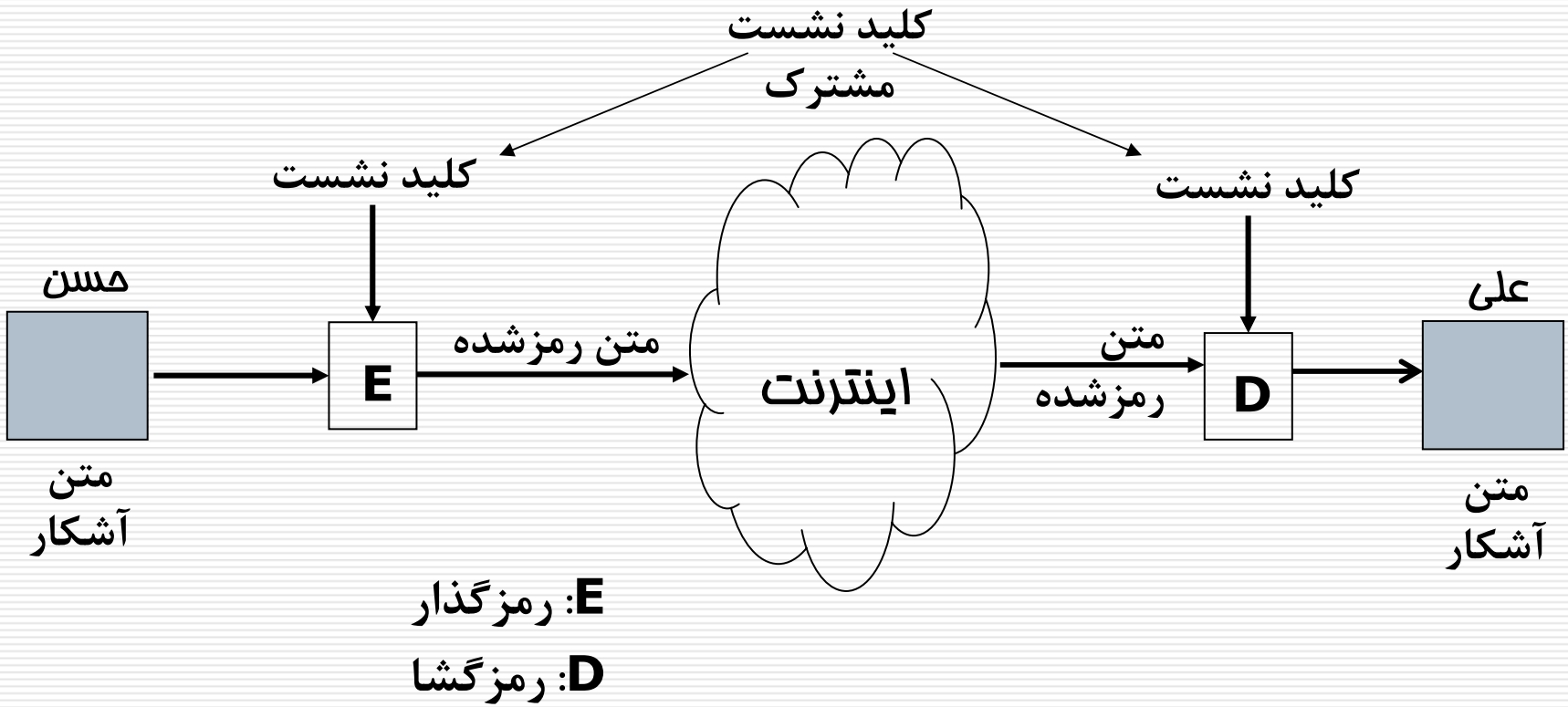
– **رمزنگاری: رمزگذاری (Encoding/Encryption) + رمزگشایی (Decoding/Decryption)**

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 اَمن
- **کابردها:** حفظ محرمانگی داده‌ها و کنترل صحت
- نیاز به زمان کمتری برای رمزگذاری و رمزگشایی (نسبت الگوریتم‌های نامتقارن) دارد.

رمزنگاری متقارن (ادامه)

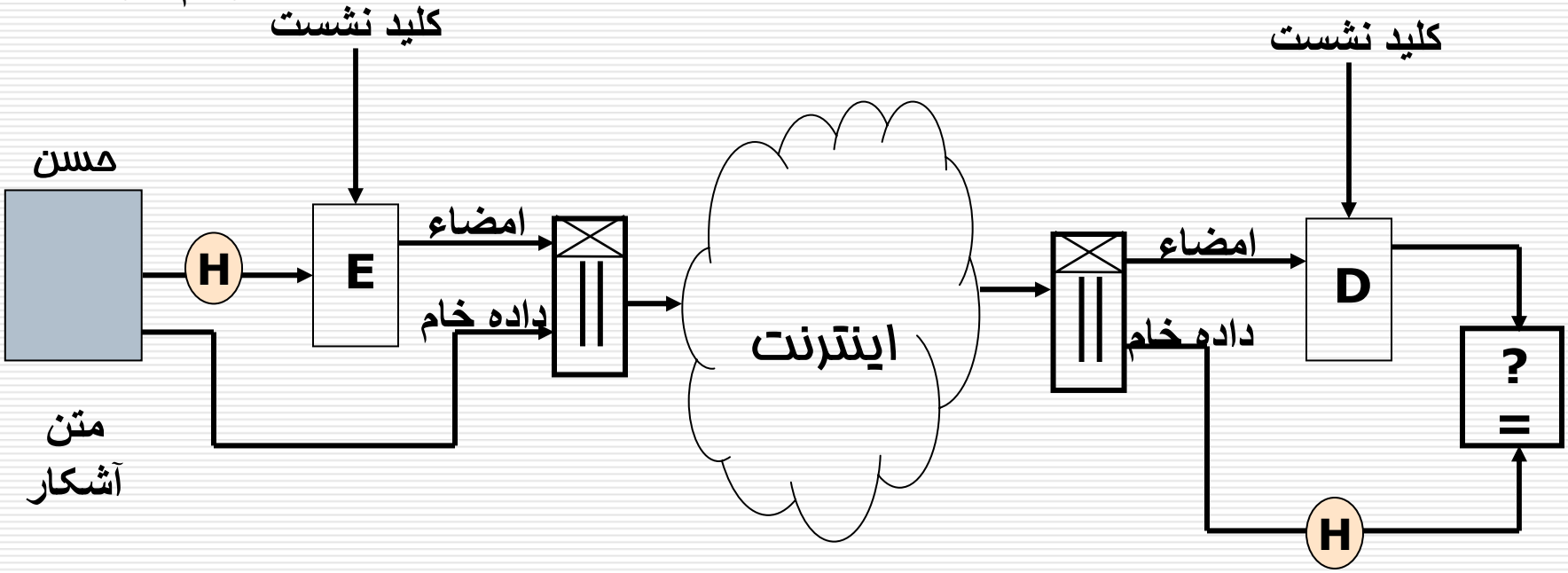
- رمزنگاری متقارن جهت حفظ محرمانگی



رمزنگاری متقارن (ادامه)

- فرآیند کنترل صحت با رمزنگاری متقارن

E: رمزگذار
D: رمزگشا
H: تابع درهم‌ساز

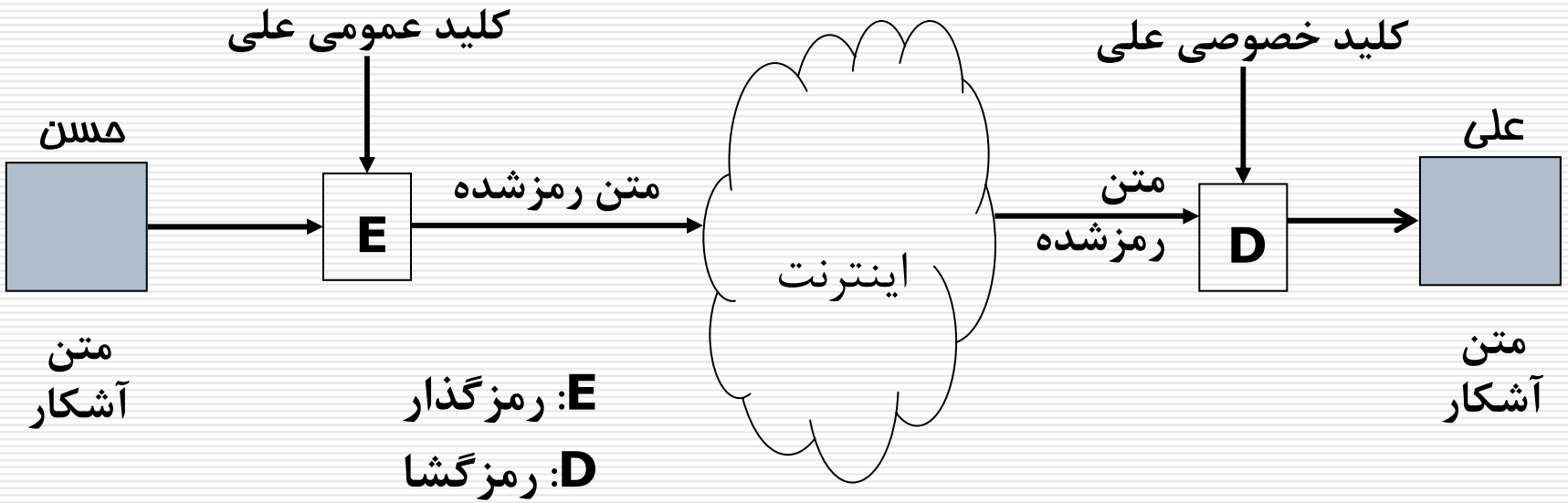


رمزنگاری نامتقارن

- 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:
  - 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 نامتقارن (ادامه)

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



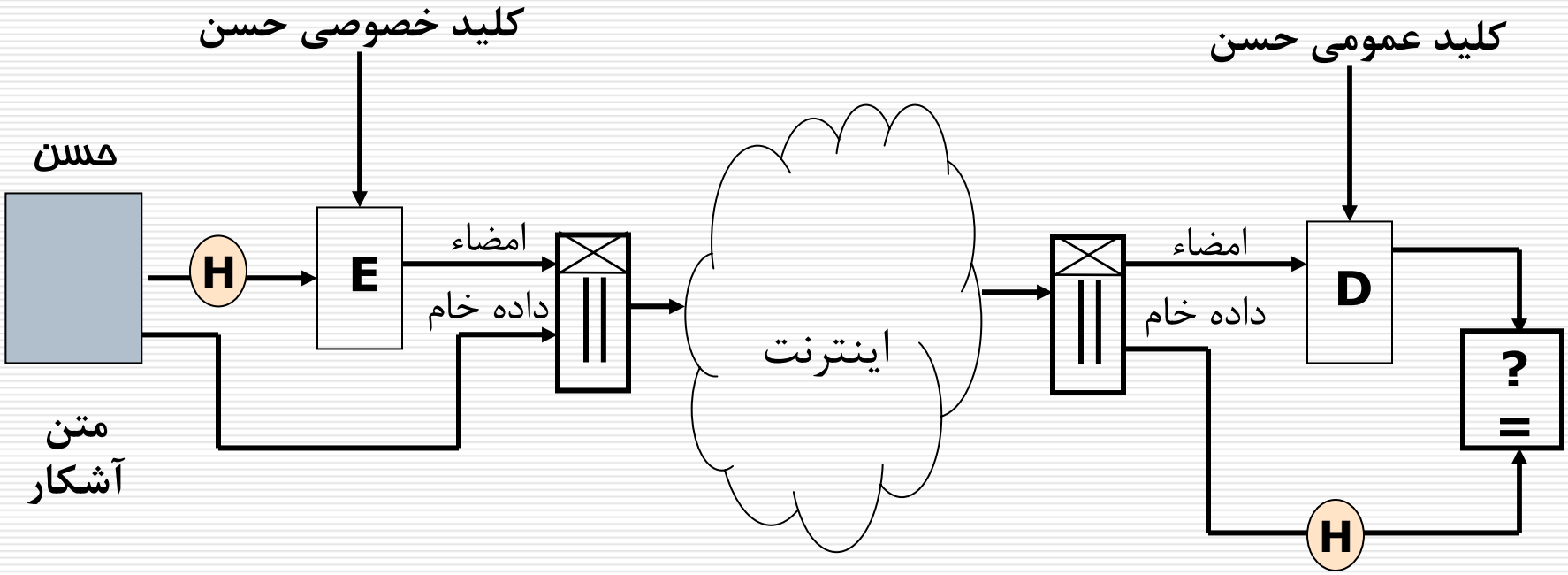
رمزنگاری نامتقارن (ادامه)

- 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 کلیدخصوصی فرد، لذا موارد زیر در مقصد با استفاده از کلیدعمومی قابل شناسایی است:
  - استفاده از کلید خصوصی ناصحیح در تولید امضاء
  - تغییر داده‌های امضاءشده در حین انتقال

رمزنگاری نامتقارن (ادامه)

- فرآیند تولید امضای دیجیتال و کنترل صحت

E: رمزگذار
D: رمزگشا
H: تابع درهم‌ساز



روشهای رمزنگاری ترکیبی

- تجمیع محاسن دو روش متقارن و نامتقارن
  - استفاده از رمزنگاری نامتقارن در تبادل کلید
  - استفاده از رمزنگاری متقارن در حفظ محرمانگی 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)

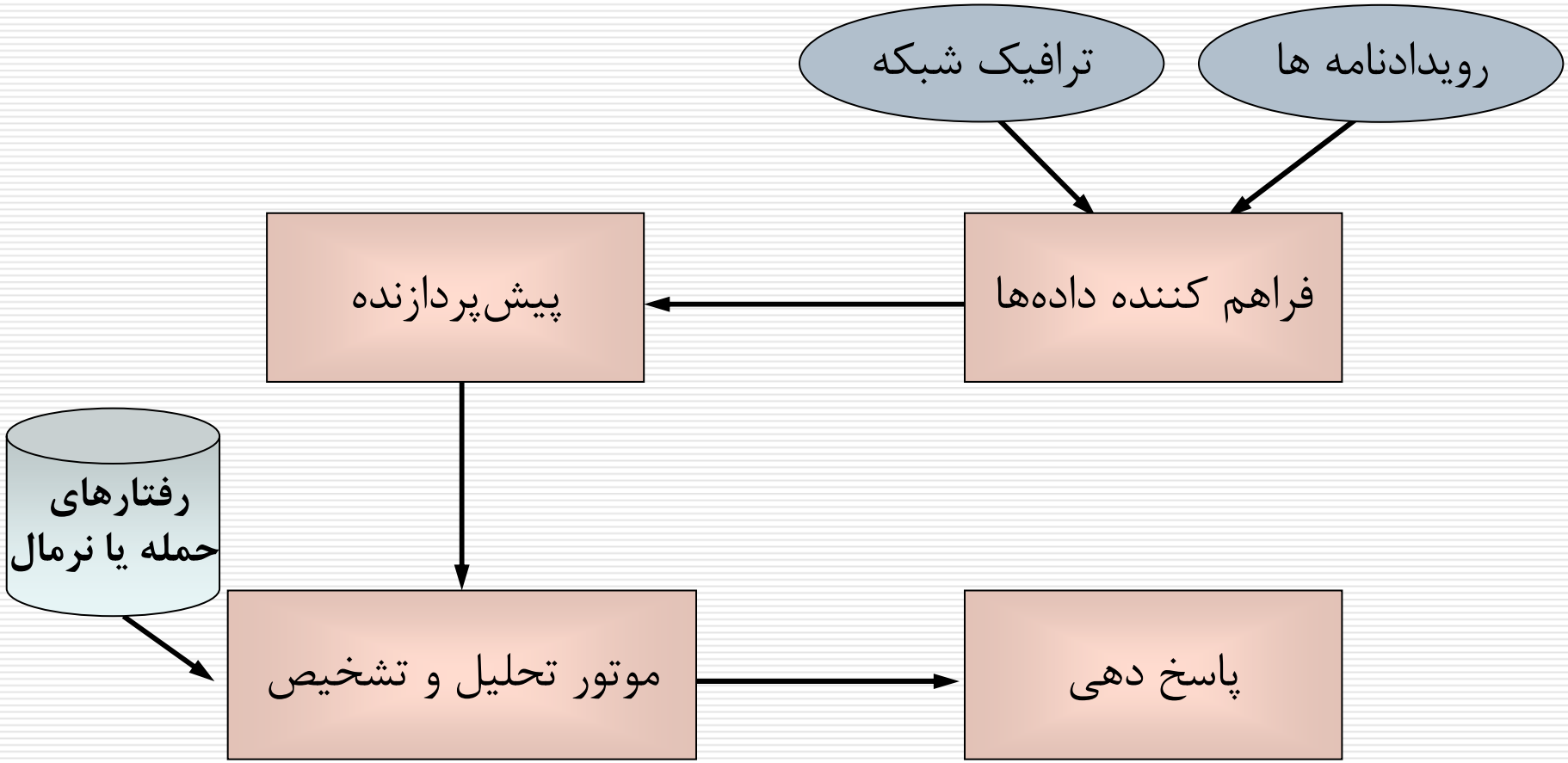
فرآیند نظارت بر وقایع رخ‌داده در یک شبکه و یا سیستم کامپیوتری در جهت کشف موارد انحراف از سیاستهای امنیتی

سیستم تشخیص نفوذ (IDS)

یک نرم‌افزار با قابلیت تشخیص، آشکارسازی و پاسخ به فعالیت‌های 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 وقایع که با یک الگوی از پیش تعریف شده مطابقت دارد.
- سیستم‌های تجاری اغلب مبتنی بر این روش عمل می‌نمایند.

تشخیص ناهنجاری

تشخیص ناهنجاری (Anomaly Detection)

- شناخت عملکرد نرمال سیستم
- تهیه 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 ناهنجار به سوی سیستم تله می‌تواند به کار برده شود.

تشخیص – سیستم ضدبدافزار

- **وظایف سیستم ضدبدافزار**
  - 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 ضدبدافزار

- **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 پهنای باند را بی‌جهت اشغال می کند.
- **بمب منطقی:** برنامه‌ای که به محض وقوع شرایطی خاص (مثلا 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 افشای اطلاعات حساس می‌پردازد.

تشخیص – سیستم ضدبدافزار

- ارائه نسخه های جدید در ترکیب با
  - سیستم تشخیص نفوذ مبتنی بر میزبان
  - دیواره آتش شخصی
  - سیستم ضد جاسوسی (Anti Spyware)
  - سیستم تشخیص سایتهای فیشینگ
- بروزرسانی دائم پایگاه تعریف بدافزارها

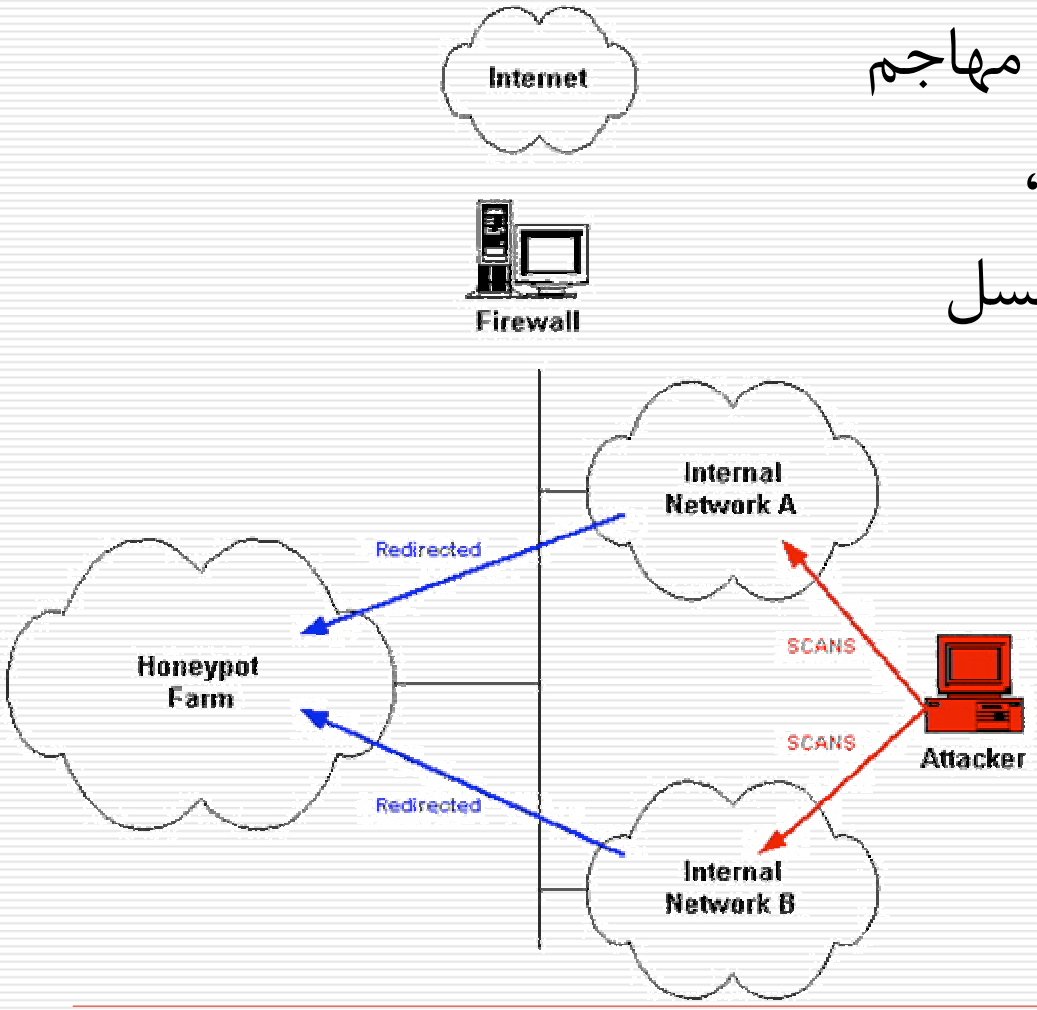
تشخیص – سیستم تله عسل

سیستم تله عسل (Honeypot)

- اغفال و فریب مهاجم جهت جمع‌آوری اطلاعات بیشتر از نحوهٔ 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 پشتیبان‌گیری‌شده

پایان

مرکز امنیت شبکه شریف

http://nsc.sharif.edu

پست الکترونیکی

m_amini@ce.sharif.edu