امنیت داده و شبکه

مرور مکانیزم‌های تامین امنیت

فهرست مطالب

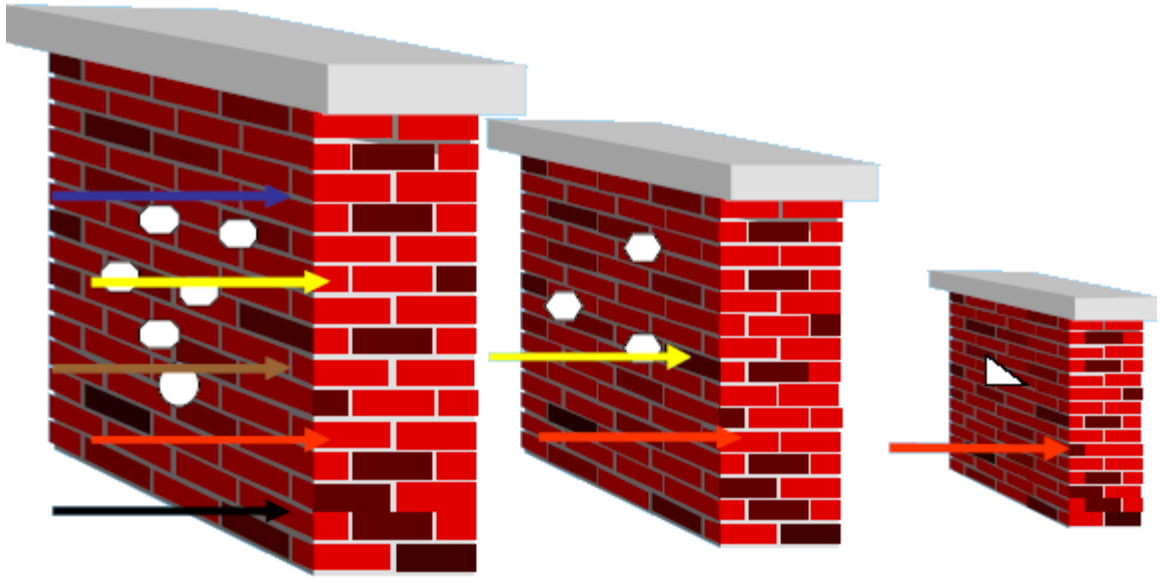
- روشهای تامین امنیت
- مکانیزم‌های پیشگیری
- مکانیزم‌های تشخیص
- مکانیزم‌های ترمیم

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 سیستم یا شبکه



مثال: دفاع در عمق در یک سیستم شبکه‌ای

- امن‌سازی شبکه و ارتباطات
- امن‌سازی کارگزار
- امن‌سازی کارخواه

دفاع در عمق- امن‌سازي شبكه 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,Web,File Server,...)

دفاع در عمق – امن‌سازي كارگزار

- استفاده از ضدبدافزار (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 در عمق – امن‌سازي كارخواه

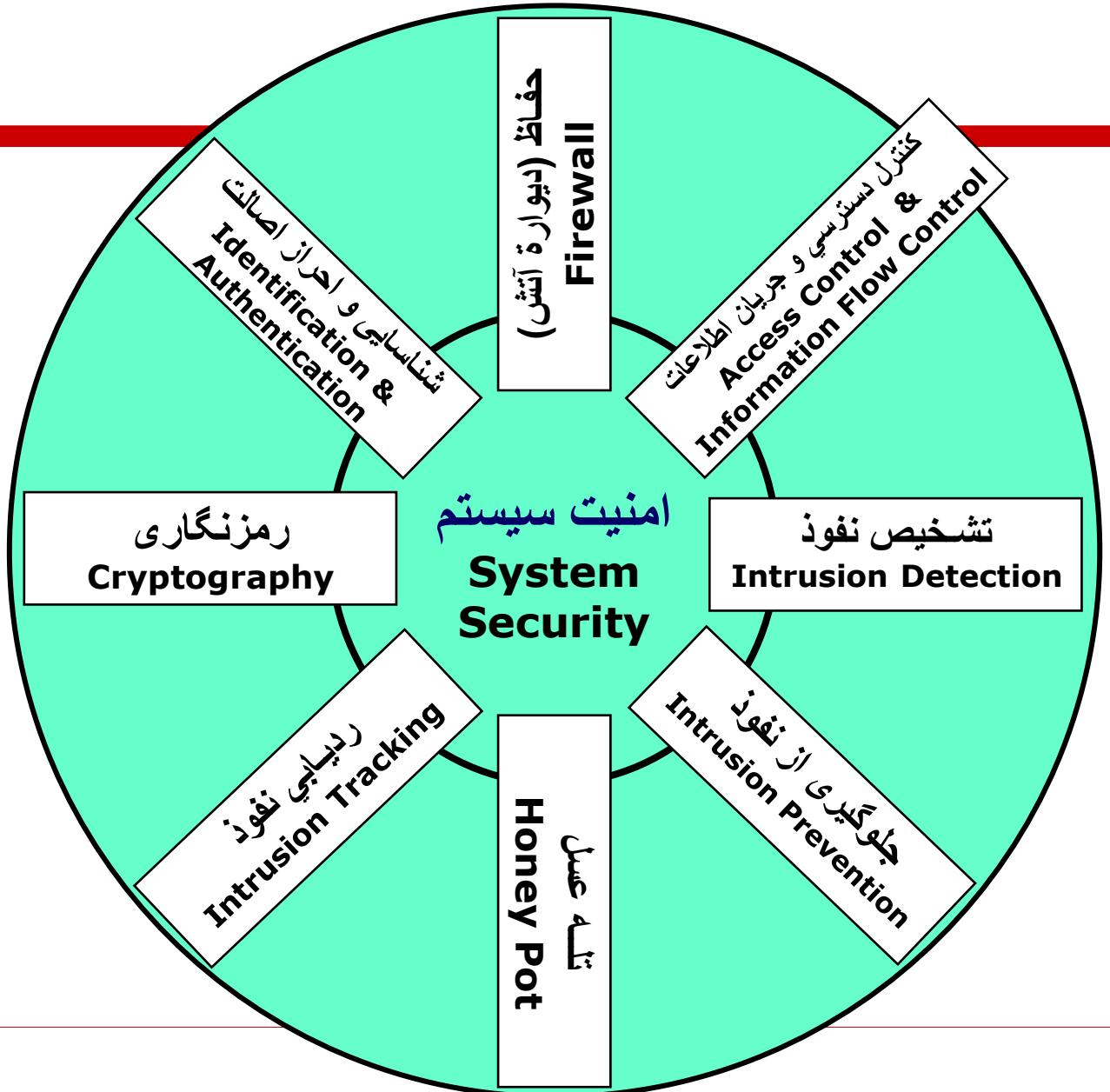
- استفاده از ضد بدافزار (ترجیحاً به صورت Corporate)
- استفاده از دیواره آتش شخصی
- استفاده از وصله‌های امنیتی به روز سیستم‌عامل و نرم‌افزارهای نصب شده

مثال: دفاع در عمق در سیستم نرم‌افزاري

امن‌سازی همه لایه‌های نرم‌افزاری یک سیستم شامل:

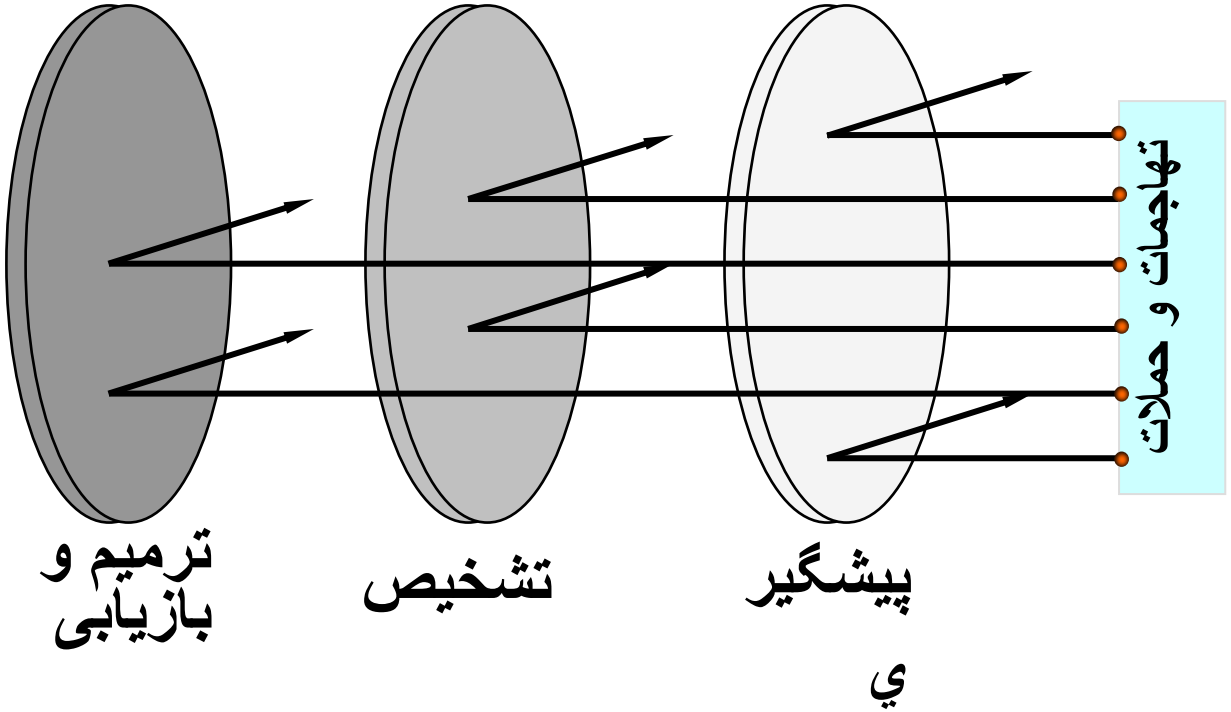
- شبکه (Network)
- سیستم‌عامل (Operating System)
- سیستم مدیریت پایگاه داده‌ها (DBMS)
- برنامه کاربردی (Application)

مکانیزمهای امنیتي



مراتب مقابله با نفوذ و تهاجم در سیستم

(پیشگیری، تشخیص، ترمیم)



پیشگیري، تشخیص، ترمیم

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

پیشگیري، **تشخیص**، ترمیم

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

پیشگیري، تشخیص، **ترمیم**

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

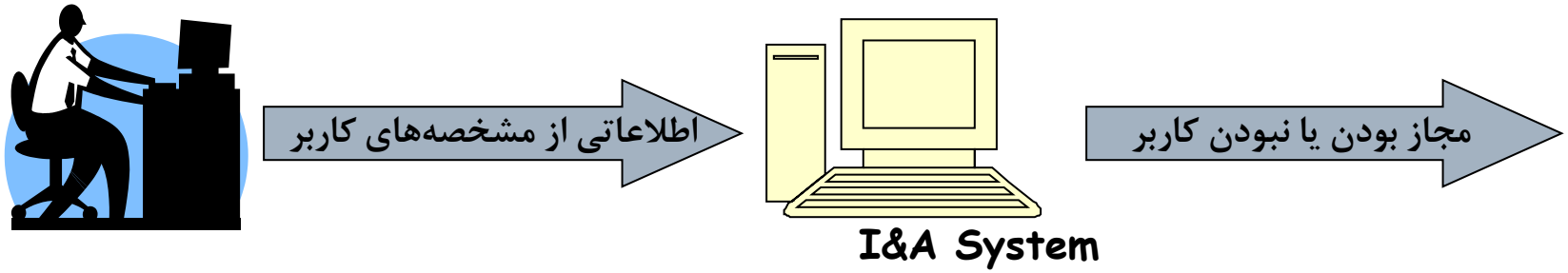
فهرست مطالب

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

پیشگیری – شناسایي و احراز اصالت

Identification & Authentication

- شناسایی کاربر و اطمینان از اینکه کاربر همان فردی است که ادعا می‌کند.
- پیش‌نیاز کنترل دسترسی در هر سیستم، شناسایی و احراز هویت کاربر است.
- فرآیند شناسایی و احراز هویت



پیشگیري – شناسايي و احراز اصالت

احراز هو يت بر اساس دانسته‌هاي کار بر

- 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 اصالت

احراز هو یت بر اساس داشته‌هاي کار بر

- 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

پیشگیري – شناسايي و احراز اصالت

احراز هو يت بر اساس مشخصه‌هاي بـ يولوژ يكي كار بر

- بر اساس مشخصه‌های طبیعی و منحصر به فرد کاربر:
  - اثر انگشت
  - عنبیه چشم
  - چهره
  - صوت

مساله اصلی: هزینه بالا و پیچیدگی سیستمی

پیشگیري – شناسايي و احراز اصالت

ح فاظت از داده های احراز هو یت

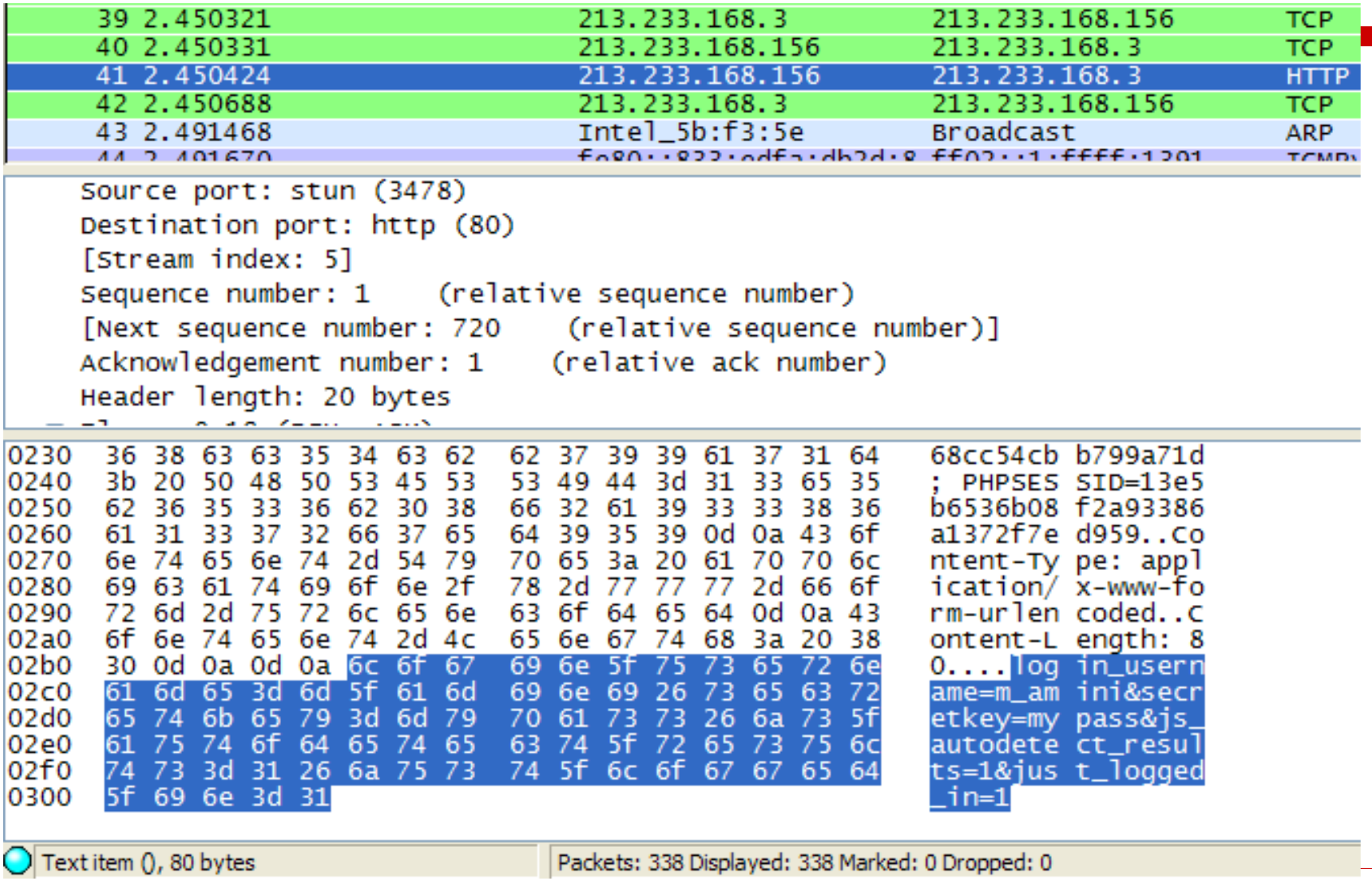
- نیاز به حفاظت از گذرواژه در حال گذر و یا ذخیره شده
  - نمایشی از گذرواژه‌های ذخیره شده در لینوکس (اسلاید بعد)
  - نمایشی از امکان دزدیده شدن گذرواژه در مسیر (دو اسلاید بعد)
- پیشگیری از امکان کپی‌برداری و یا افشای کلید ذخیره شده در توکن
- نیاز به حفاظت از داده‌های بیومتریک

پیشگیري – شناسايي و احراز اصالت

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/69XjeQn6GOT6.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/aaporGgAmja8kBRBslLsrE28q95vOm:14521:0:99999:7:::

پیشگیري – شناسايي و احراز اصالت

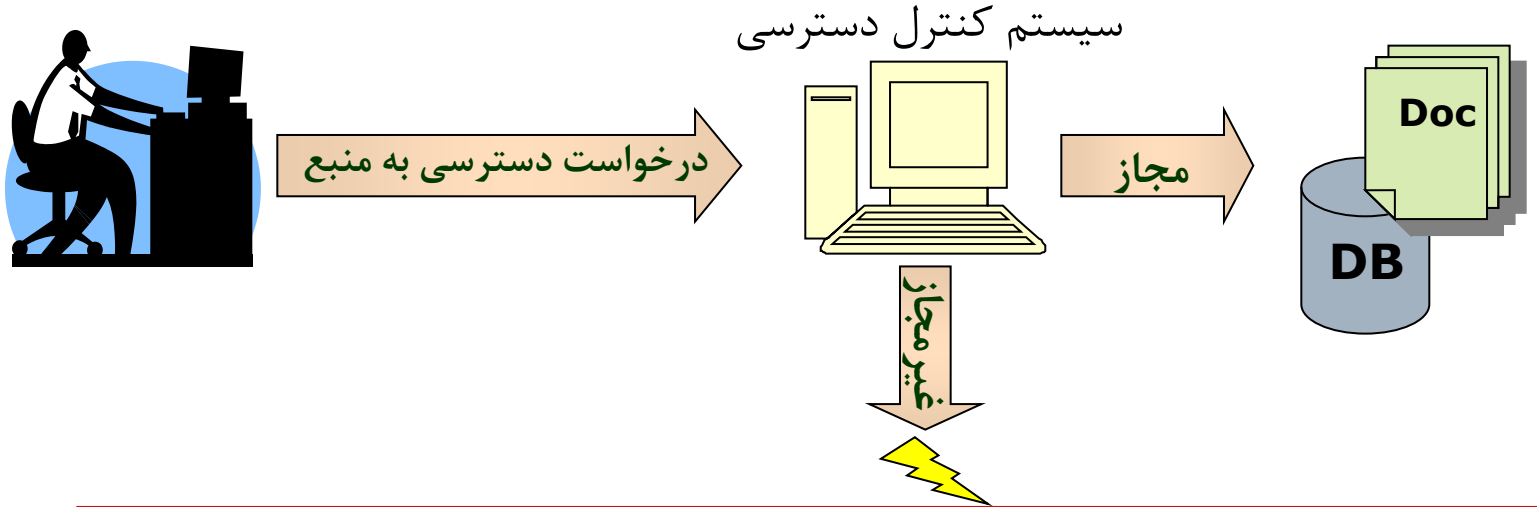


استخراج گذرواژه با شنود روی شبکه

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.



پیشگیري – کنترل دسترسي (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

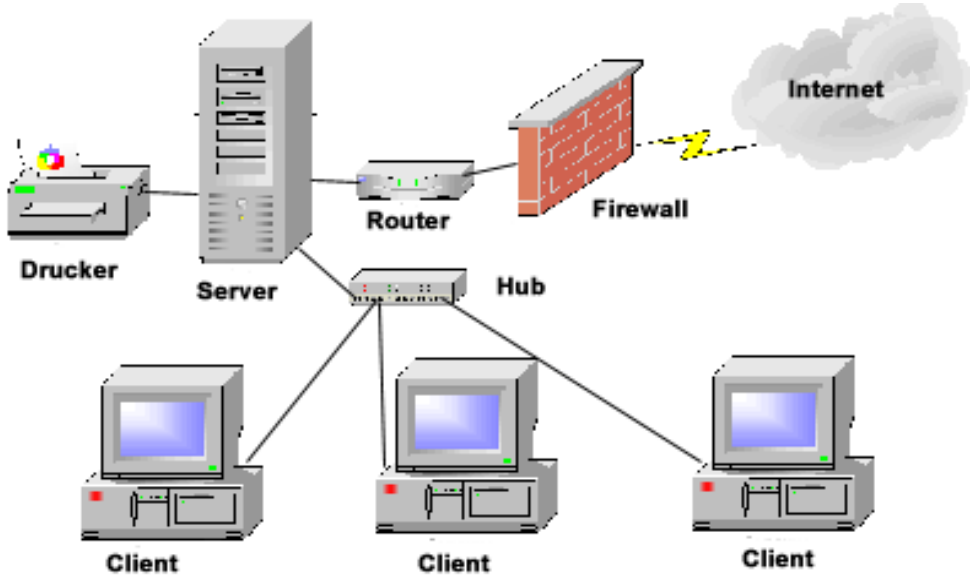
کنترل دسترسی – از خیال تا واقعیت

- وجود ارتباط منطقی و امن بین احراز هویت و 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

پیشگیري – دیواره آتش

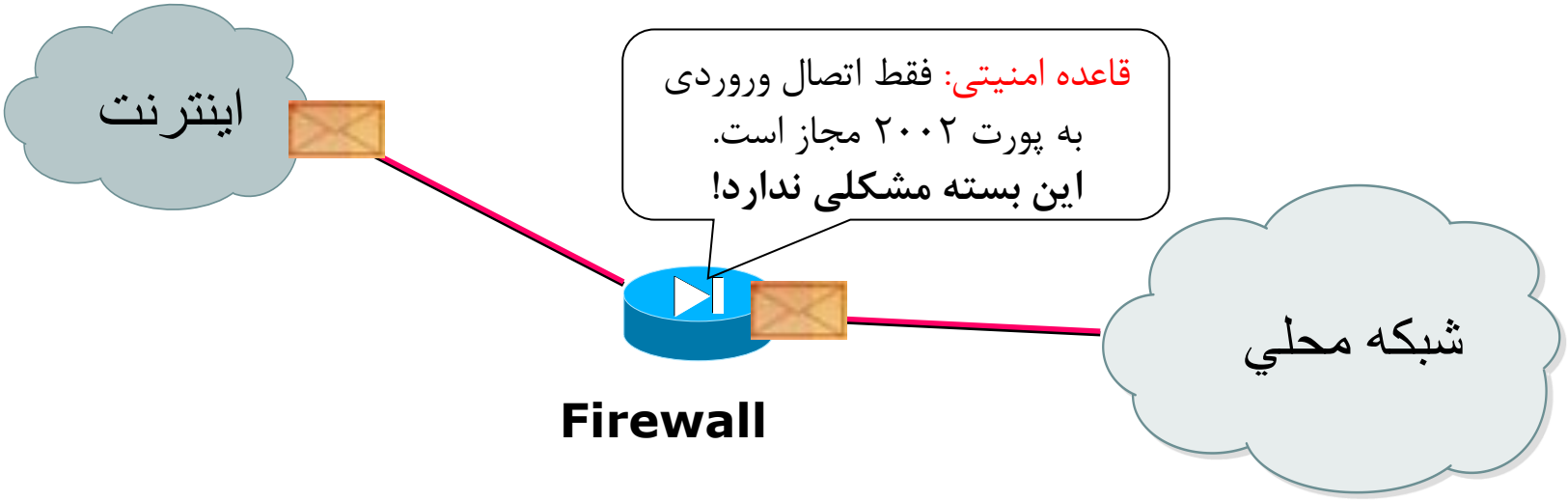
Firewall

- 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



پیشگیري – 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.



مشخصات عمومي يك ديواره آتش شبكه‌ای

- تعریف سیاست و قاعده امنیتی
- محافظت در برابر برخی حملات شناخته شده
- ثبت رویدادها
- پالایش (فیلترینگ) محتوا
- پشتیبانی از شبکه خصوصی مجازی (VPN)

پیشگیري - رمزنگاري

- **Cryptography**
  - **حفظ محرمانگی** (پیشگیری): اطمینان از اینکه هر دادهٔ ذخیره شده و یا ارسالی بر روی شبکه تنها توسط گیرندهٔ موردنظر می‌تواند رمزگشایی و استفاده گردد.
  - **کنترل صحت** (تشخیص): افزودن یک سرآیند رمزشده 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 وارسی آن در مقصد.

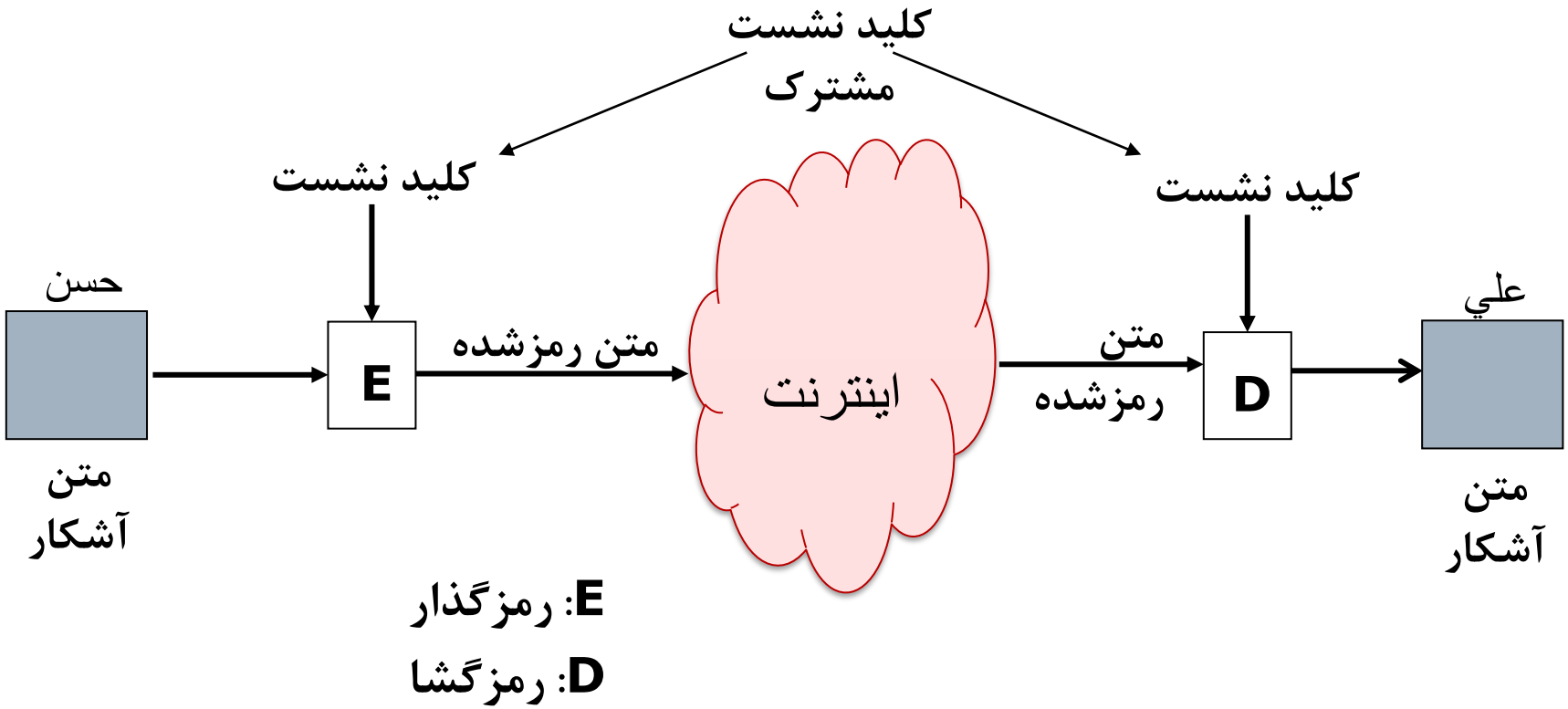
  - **رمزنگاری: رمزگذاری (Encoding) + رمزگشایی (Decoding)**

پیشگیری- رمزنگاري 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.

پیشگیری- رمزنگاري متقارن (ادامه)

- رمزنگاری متقارن جهت حفظ محرمانگی

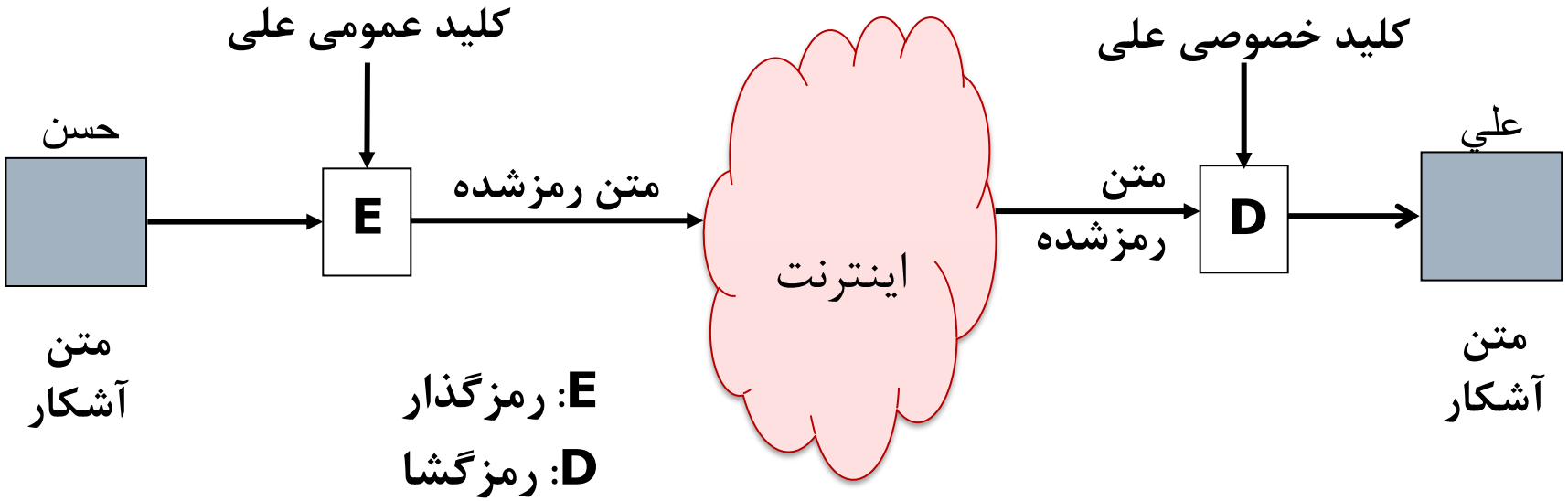


پیشگیری- رمزنگاري نامتقارن

- 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

رمزنگاري 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.



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 داده‌ها
- مثال‌های کاربردی:
  - شبکه های خصوصی مجازی VPN
  - پروتکل SSL
  - پروتکل SSH

فهرست مطالب

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

تشخیص - رمزنگاري

- **کنترل صحت** (تشخیص): افزودن یک سرآیند رمزشده 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 وارسی آن در مقصد.

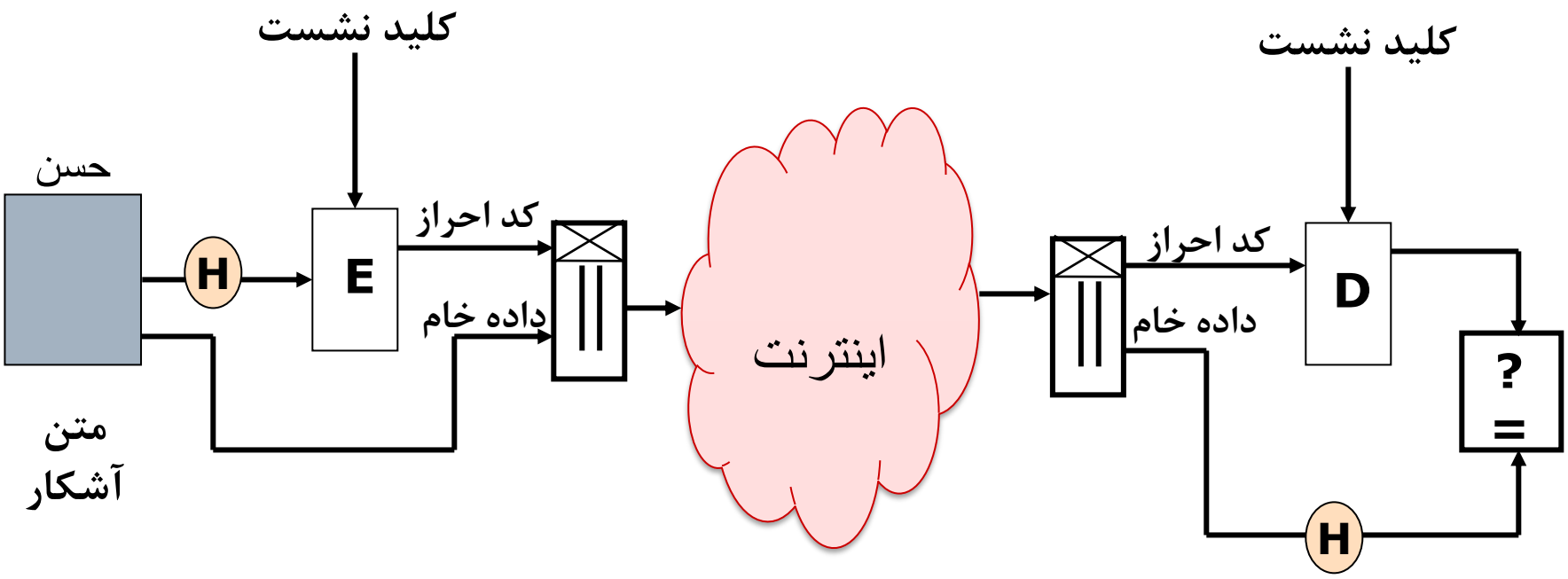
تشخیص - رمزنگاري متقارن

- فرآیند کنترل صحت با رمزنگاری متقارن

E: رمزگذار

D: رمزگشا

H: تابع درهم‌ساز



تشخیص - رمزنگاري نامتقارن

- رمزنگاری جهت احراز اصالت و کنترل صحت (امضای دیجیتال)
  - فرد می‌تواند با استفاده کلید خصوصی خود، یک امضای دیجیتال برای داده‌های ارسالی 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

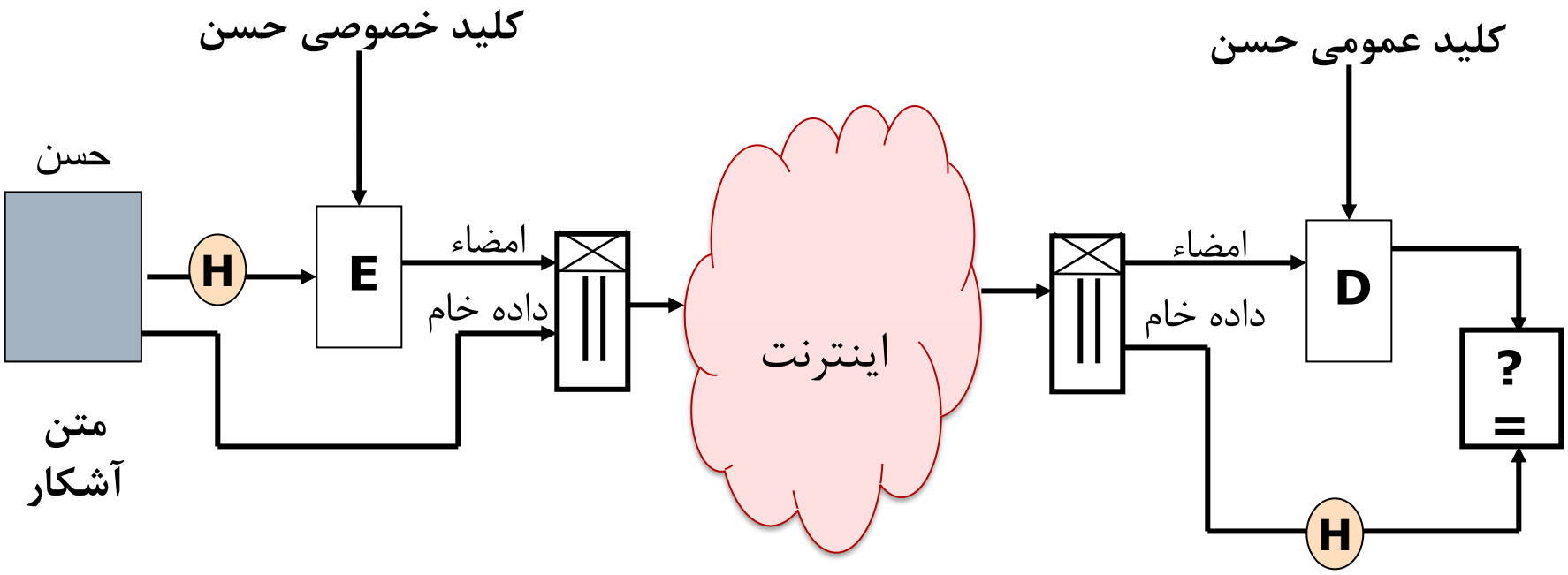
تشخیص - رمزنگاري نامتقارن

- فرآیند تولید امضای دیجیتال و کنترل صحت

E: رمزگذار

D: رمزگشا

H: تابع درهم‌ساز



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)

سیستم تشخیص سوء استفاده

سیستم تشخیص ناهنجاری

یک نرم‌افزار با قابلیت تشخیص، آشکارسازی و پاسخ به فعالیت‌های غیرمجاز یا غیرنرمال در رابطه با سیستم

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

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

انواع بدافزارها (۱)

- ویروس (Virus)
- کرم (Worm)
- اسب تروا (Trojan)
- بات (Bot)
- باج افزار (Ransomware)
- جاسوس‌افزار (Spyware)
- جاسوس کیبورد (Key logger)
- تبلیغ افزار (Adware)
- بمب منطقی (Logic Bomb)

انواع بدافزارها (۲)

- **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

انواع بدافزارها (۳)

- **جاسوس‌افزار (Spyware)**
  - به منظور جاسوسی از سیستم قربانی و ارسال اطلاعات محرمانه
- **تبلیغ‌افزار (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 می‌کند ذخیره کرده و برای مهاجم می‌فرستد.

انواع بدافزارها (۴)

بات (Bot) و شبکه بات (Botnet)

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

بمب منطقی (Logical Bomb)

- بدافزاری که به محض وقوع شرایطی خاص (مثلاً در یک تاریخ مشخص) فعال می‌شود و به خرابکاری می‌پردازد.

باج‌افزار (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.

تشخیص – سیستم ضدبدافزار

- ارائه نسخه های جدید در ترکیب با
  - سیستم تشخیص نفوذ مبتنی بر میزبان
  - دیواره آتش شخصی
  - سیستم تشخیص سایتهای فیشینگ
- ضرورت بروزرسانی مستمر پایگاه امضای 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.

فهرست مطالب

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

ترمیم و بازیابی

- 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
- پشتیبان‌گیری داده‌ها (Backup)
  - بازیابی داده‌ها و بازگرداندن سیستم به حالت قبل از بروز مشکل یا حمله با استفاده از داده‌های پشتیبان‌گیری‌شده

ترمیم و بازیابی

- 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