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

دانشگاه صنعتی شریف
دانشکده مهندسی کامپیوتر

درس ۲: ساز و کارهای تأمین امنیت

محمد صادق دوستی

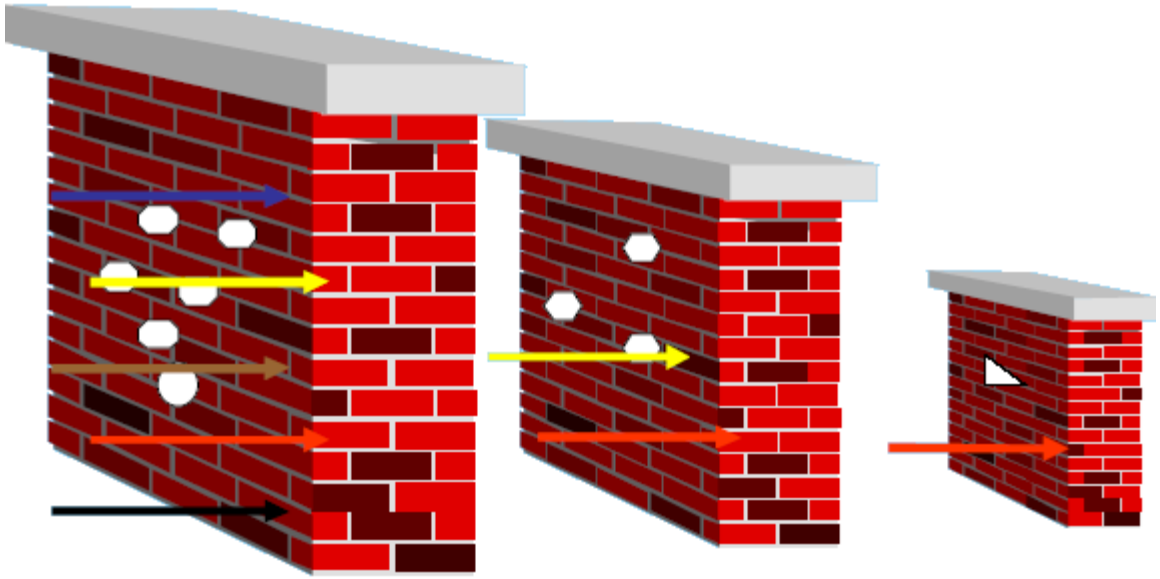
فهرست مطالب

روشهای تأمین امنیت

- دفاع چند لایه (Defense in Depth)
- پیاده‌سازی راه‌حل‌های پیشگیرانه
- پیاده‌سازی راه‌حل‌های تشخیص
- پیاده‌سازی راه‌حل‌های واکنش

دفاع چند لایه

- **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– 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 (ساز و کار VLAN)
- استفاده از ابزارهای مدیریت شبکه
- توجه به امنیت و محرمانگی ارتباطات Wireless
- ارزیابی آسیب‌پذیری‌های سرویس‌های شبکه (وب، رایانامه، ...)

دفاع چند لایه – امن‌سازی 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 ....

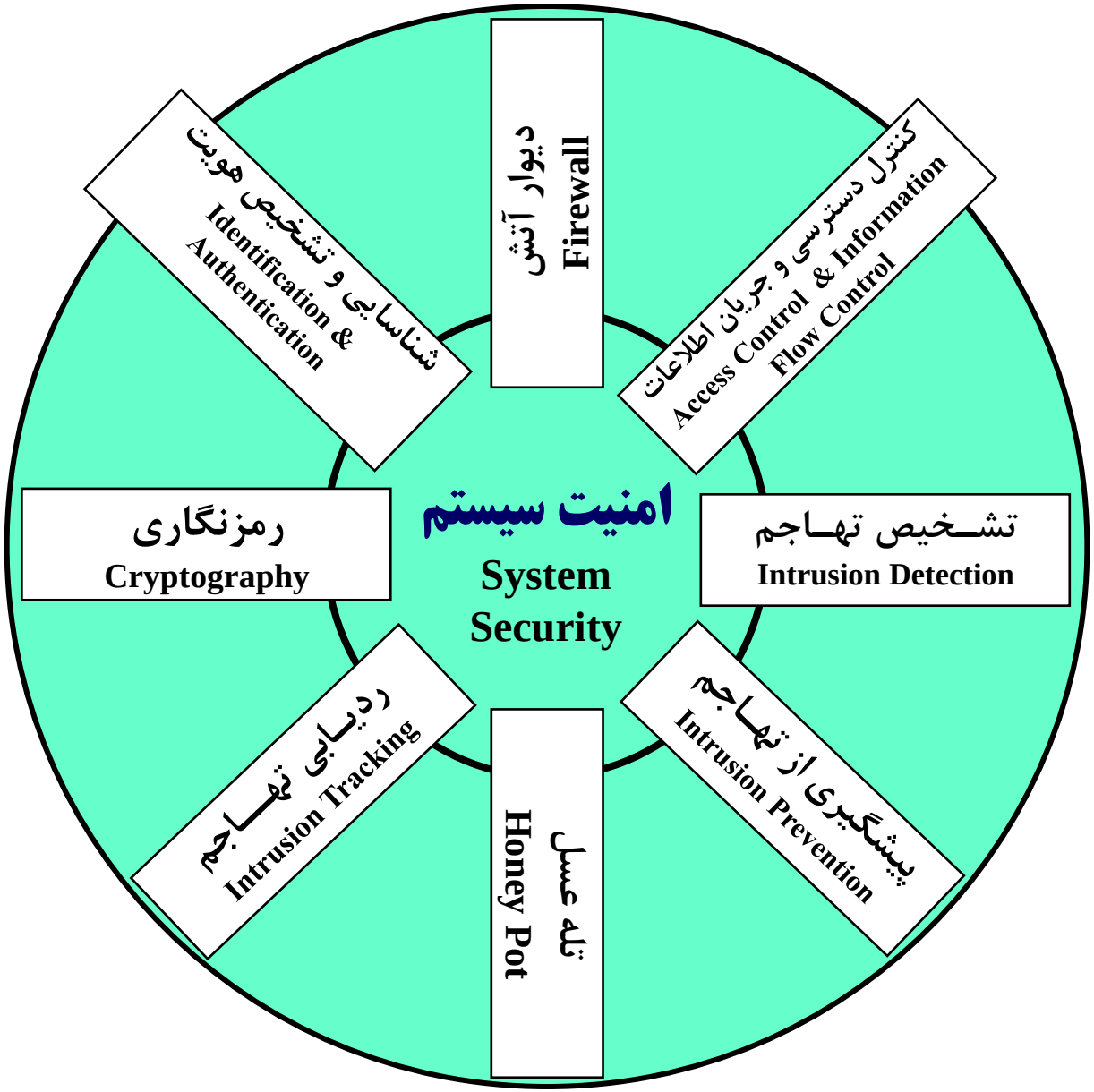
دفاع چند لایه – امن‌سازی کارخواه

- 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 پیش‌فرض
- مقاوم‌سازی (مرورگر و ...)

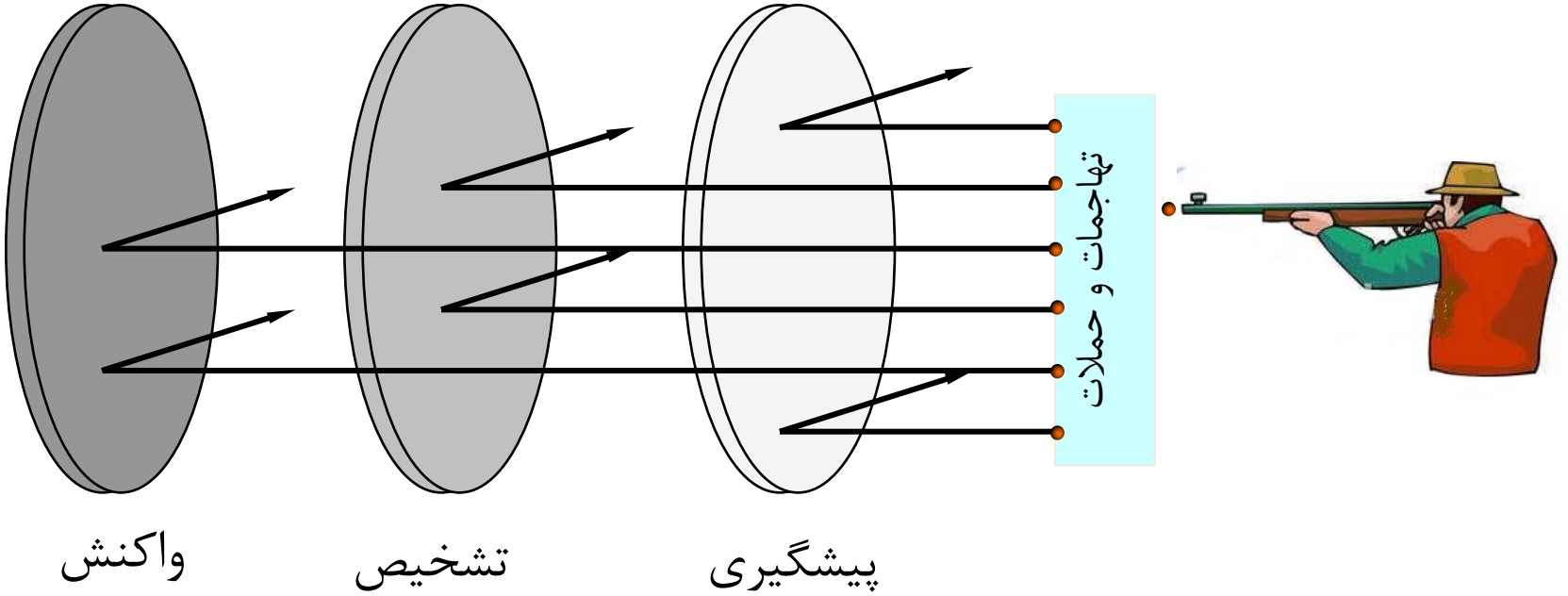
مثال: دفاع چند لایه در سیستم نرم‌افزاری

- امن‌سازی همه لایه‌های نرم‌افزاری یک سیستم شامل:
  - شبکه (Network)
  - سیستم‌عامل (Operating System)
  - سیستم مدیریت پایگاه داده‌ها (DBMS)
  - برنامه کاربردی (Application)

ساز و کارهای امنیتی



مراتب مقابله با نفوذ و تهاجم در سیستم



فهرست مطالب

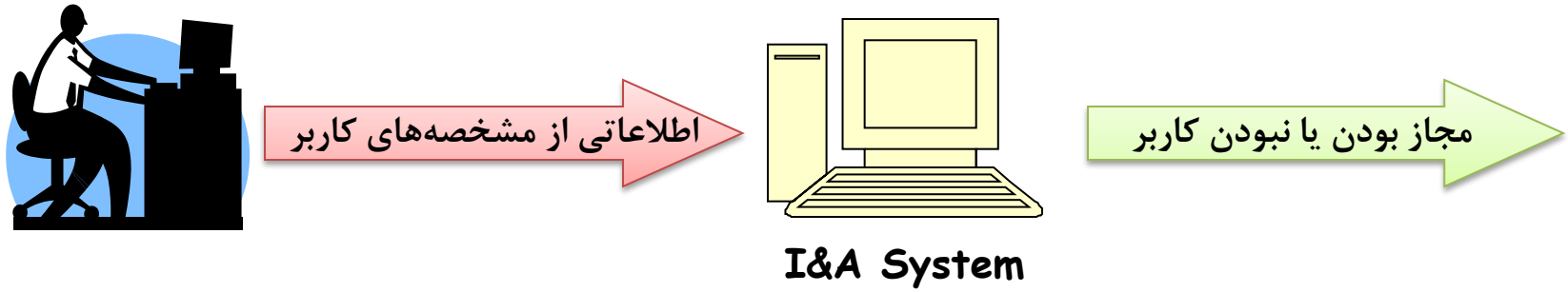
- روشهای تامین امنیت
- **ساز و کارهای پیشگیری**
- ساز و کارهای تشخیص
- ساز و کارهای واکنش

شناسایی و تشخیص هویت – ۱

❑ Identification & Authentication

☜ پیش‌نیاز کنترل دسترسی در هر سیستم، شناسایی کاربر (متقاضی) و تشخیص هویت مورد ادعای آن

☜ فرآیند شناسایی و تشخیص هویت



شناسایی و تشخیص هویت – ۲

- آنچه که کاربر در ذهن خود دارد:
  - ☜ گذرواژه
  - ☜ شماره شناسایی شخصی PIN
- **مسأله اصلی:** حدس یا افشای دانسته فردی
- **راه‌حل:** تغییر دوره‌ای دانسته
- **راه‌حل:** 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

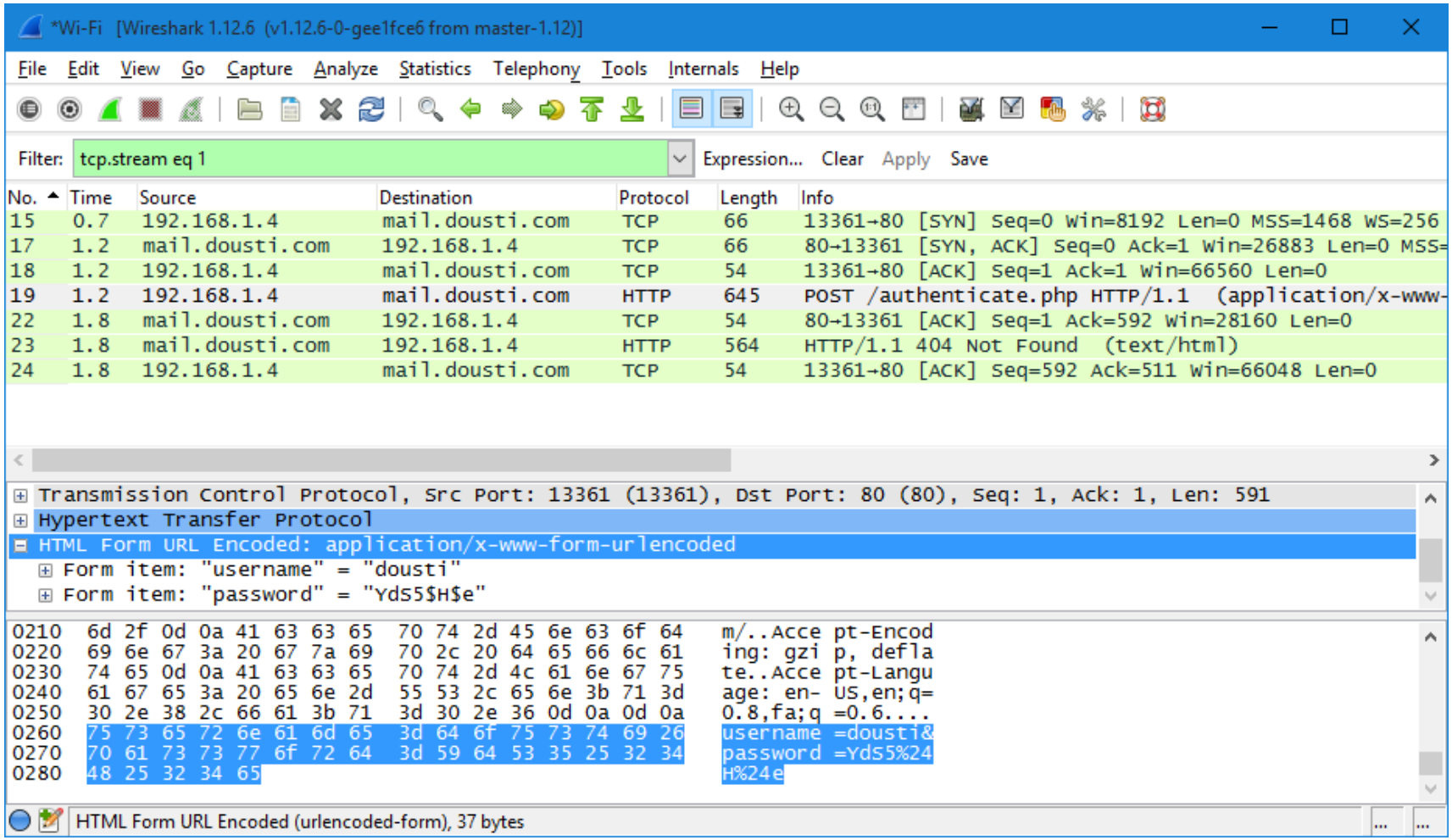
- نیاز به حفاظت از گذرواژه در حال گذر و یا ذخیره شده
  - ☜ نمایشی از گذرواژه‌های ذخیره شده در لینوکس (اسلاید بعد)
  - ☜ نمایشی از امکان دزدیده شدن گذرواژه در مسیر (دو اسلاید بعد)
- پیشگیری از امکان کپی‌برداری و یا افشای کلید ذخیره شده در توکن
- نیاز به حفاظت از داده‌های بیومتریک

- محتوای فایل /etc/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...dfIgN:16626:0:99999:7:::
```

شناسایی و تشخیص هویت – ۷

- استخراج گذرواژه با شنود روی شبکه (Wireshark)

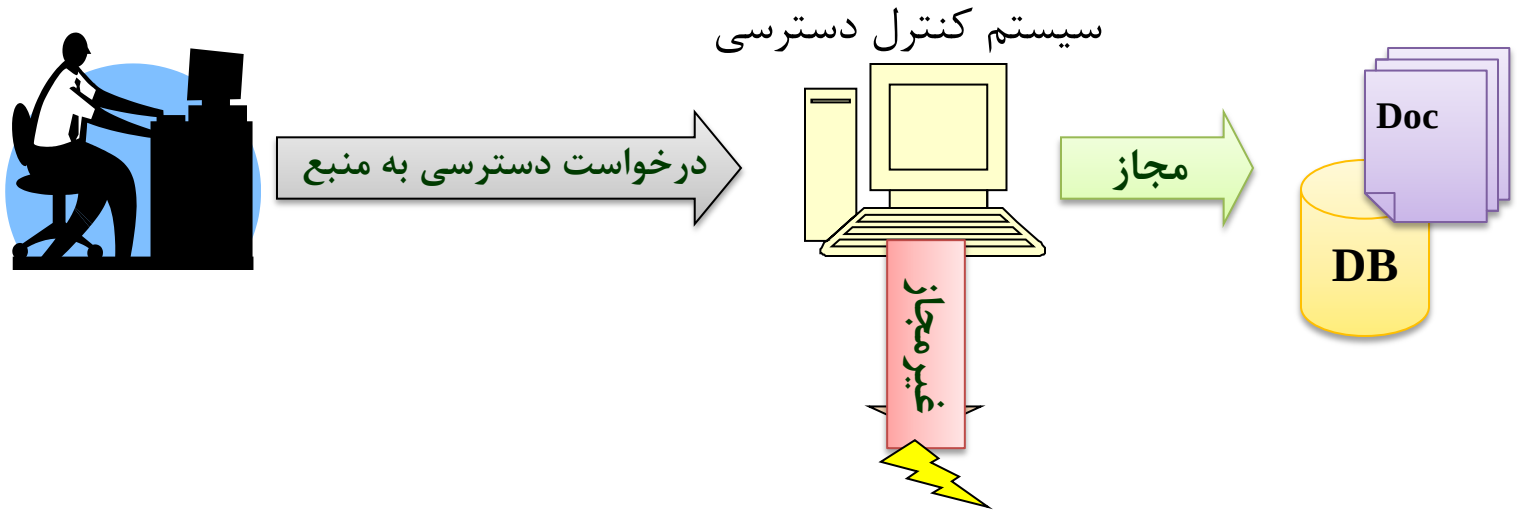


کنترل دسترسی – ۱

❑ Access Control

☜ ساز و کار بنیادی برای حفظ امنیت در هر سیستم

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



کنترل دسترسی – ۲

- 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

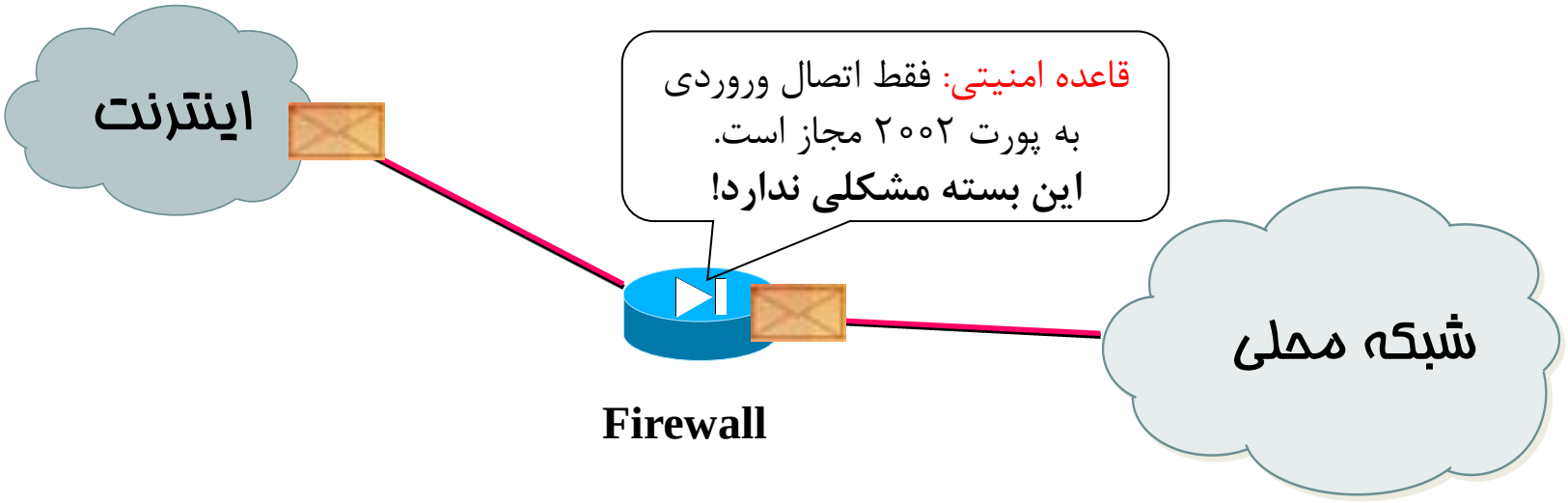
دیوار آتش – ۱

- 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 عبـور 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 (Cryptography)

- **رمزنگـــــاری** = رمزگـــذاری (Encryption) + رمزگشـــایی (Decryption). خدمات:

☜ **حفظ محرمانگی (پیشگیری)**: اطمینان از اینکه هر داده ذخیـره شده و یا ارسالی بر روی شبکه تنهـا توسـط فـرد مـورد نظـر قابـل رمزگشایی و استفاده است.

☜ **تشخیص هویت (تشخیص)**: رمز با کلیدی که صـرفاً در اختیـار مبدأ (و احتمالاً مقصد) است، و وارسی آن در مقصد.

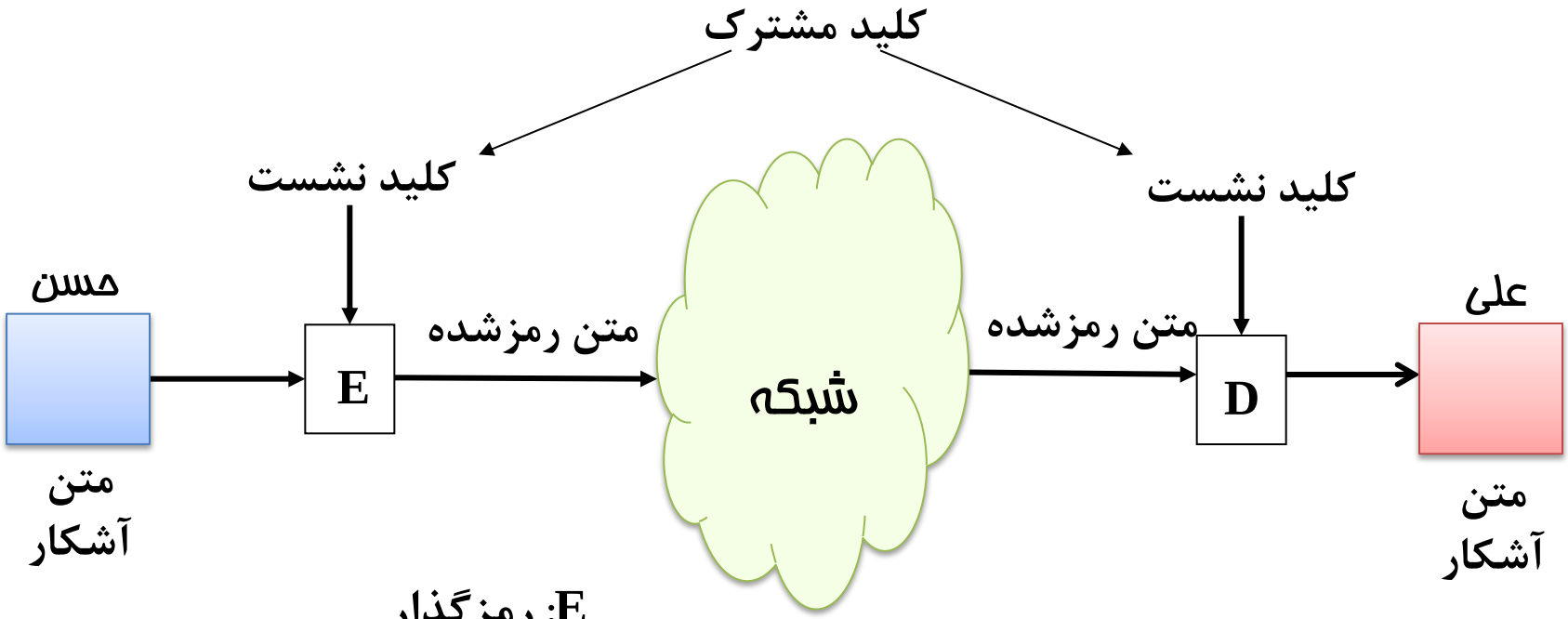
☜ **کنترل صحت (تشخیص)**: افزودن یک سرآیند محاسبه شـده بـا یک کلید به داده، و بازسازی و کنترل آن جهت وارسی صحت.

رمزنگاری متقارن – ۱

- استفاده از یک کلید **مشترک** برای رمز داده‌ها بین دو فرد
- **کاربردها:** 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 اَمن

رمزنگاری متقارن – ۲

- رمزنگاری متقارن جهت حفظ محرمانگی

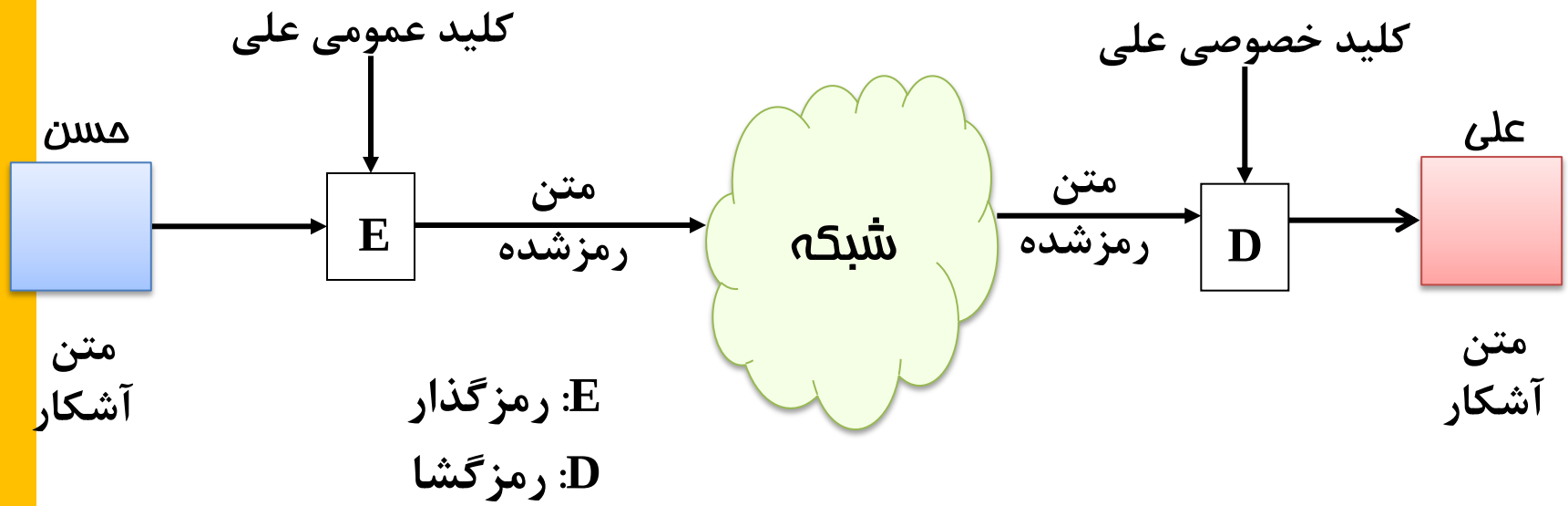


رمزنگاری نامتقارن – ۱

- 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 فردِ دارای کلید خصوصی (متناظر کلید عمومی به کاربرده شده) می‌تواند داده‌های رمز شده را رمزگشایی کند.



روشهای رمزنگاری ترکیبی (Hybrid)

- 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

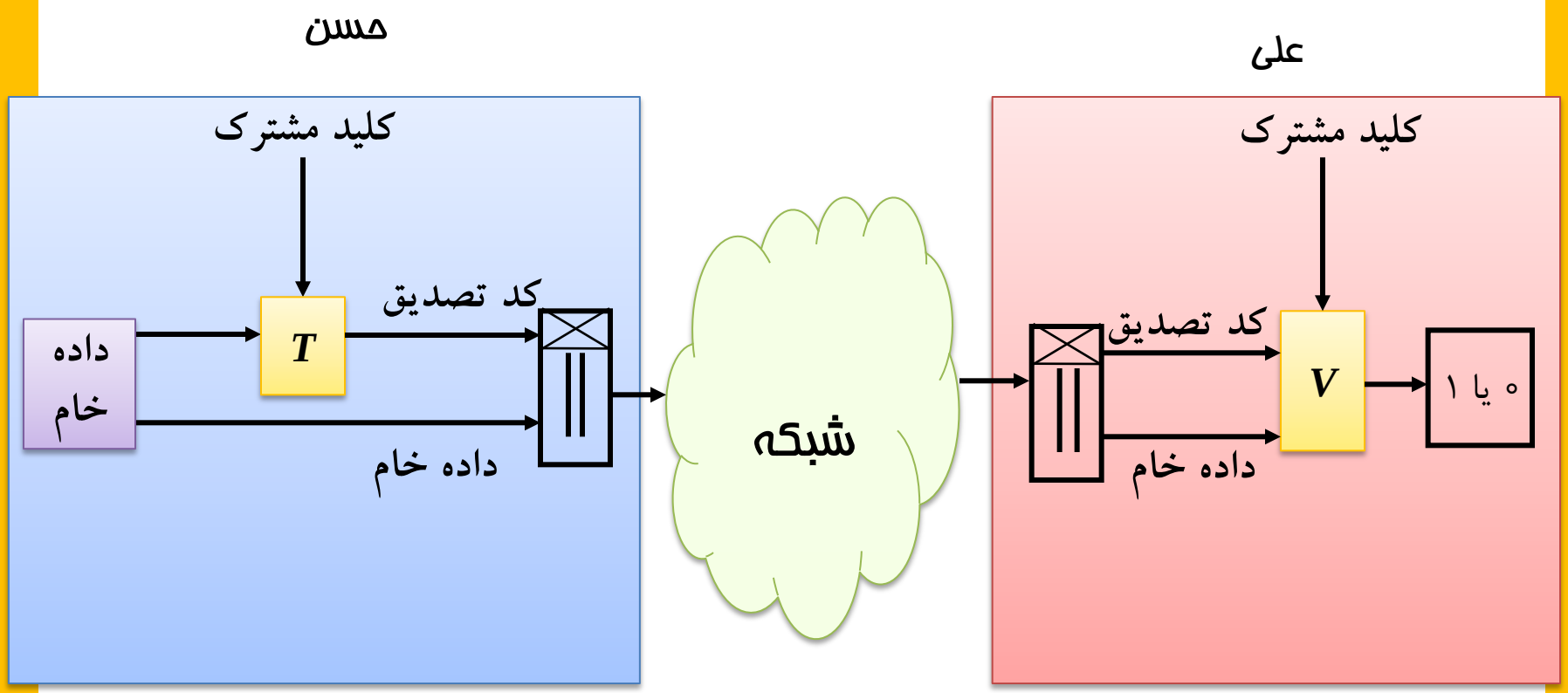
- روشهای تامین امنیت
- ساز و کارهای پیشگیری
- **ساز و کارهای تشخیص**
- ساز و کارهای واکنش

تشخیص: رمزنگاری متقارن

- رمزنگاری متقارن جهت حفظ صحت

***T*:** Tag

***V*:** Verification



تشخیص: رمزنگاری نامتقارن – ۱

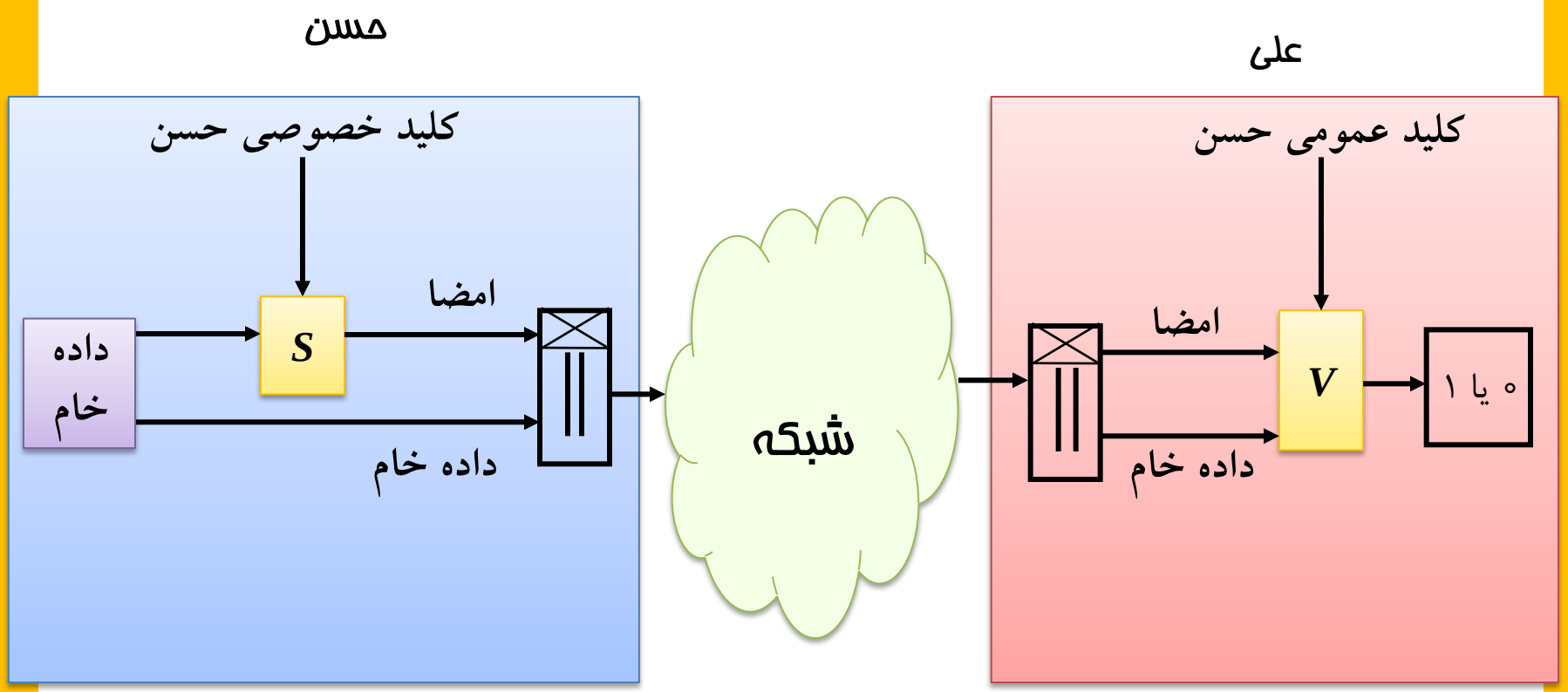
- رمزنگاری نامتقارن جهت تشخیص هویت و کنترل صحت (امضای دیجیتال)
  - استفاده از کلید خصوصی جهت تولید امضای دیجیتال از داده‌ها
  - استفاده از کلید عمومی جهت وارسی امضای دیجیتال
- امضا تابعی است از داده‌ها و کلیدخصوصی فرد، لذا موارد زیر در مقصد با استفاده از کلیدعمومی قابل شناسایی است:
  - استفاده از کلید خصوصی ناصحیح در تولید امضا
  - تغییر داده‌های امضا شده در حین انتقال

تشخیص: رمزنگاری نامتقارن – ۲

- فرآیند تولید امضای دیجیتال و کنترل صحت

***S*: Sign**

***V*: Verification**



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

سیستم تشخیص سوء استفاده (Misuse Detection)

- 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

انواع بدافزار – ۱

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

انواع بدافزار – ۲

- **ویروس:** برنامه کوچکی که به برنامه‌های دیگر می‌چسبد و با اجرای آنها، به انتشار خود و خرابکاری در سیستم می‌پردازد.
- **کرم:** برنامه مستقلی است که خود را به سرعت منتشر کرده و سایر سیستمها را آلوده می‌کند.
- **اسب تروا:** بدافزاری که در یک برنامه مفید ذخیره می‌شود یا به عنوان یک برنامه مفید خود را جا می‌زند.
- **بات:** پردازه‌ای که از نفوذگر فرمان گرفته و آنها را روی سیستم قربانی به طور خودکار اجرا می‌کند.
- **ابزار اختفا:** بدافزاری که خود را در در سیستم قربانی مخفی می‌کند.

انواع بدافزار – ۳

- **ابزار جاسوسی:** بدافزاری که اطلاعات سیستم قربانی را بدون رضایت صاحب آن دزدیده و برای مهاجم می‌فرستد.
- **جاسوس کیبورد:** بدافزاری که پس از نصب روی سیستم قربانی، آنچه را که صاحب سیستم تایپ می‌کند ذخیره کرده و برای مهاجم می‌فرستد.
- **تبلیغ افزار:** بدافزاری که برای صاحب سیستم تبلیغ نمایش می‌دهد.
- **بمب منطقی:** بدافزاری که به محض وقوع شرایطی خاص (مثلاً در یک تاریخ مشخص) فعال می‌شود و به خرابکاری می‌پردازد.
- **باج‌افزار:** بدافزاری که فایلهای سیستم قربانی را رمز نموده و برای رمزگشایی، باج می‌خواهد.

سیستم ضد بدافزار – ۱

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

سیستم ضد بدافزار – ۲

- 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
- به‌روزرسانی 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.

فهرست مطالب

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

ساز و کارهای واکنش

- وجود سایت فیزیکی مجزا
- وجود سیستم افزونه (Redundant/Replica)
- پشتیبان‌گیری از داده‌ها (Backup)
- استفاده از ضد بدافزار (ترمیم فایلهای آلوده)
- آموزش و استقرار گروه پاسخ‌گویی حوادث رایانه‌ای (CERT)

CERT: Computer Emergency Response Team