



یاد‌الامن والامان

امنیت داده و شبکه

مرور مکانیزم‌های تامین امنیت

مرتضی امینی - سیدمهدی خرازی

نیمسال اول ۱۴۰۳-۱۴۰۴



فهرست مطالب

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



فهرست مطالب

□ روش‌های تامین امنیت

□ مکانیزم‌های پیشگیری

□ مکانیزم‌های تشخیص

□ مکانیزم‌های ترمیم

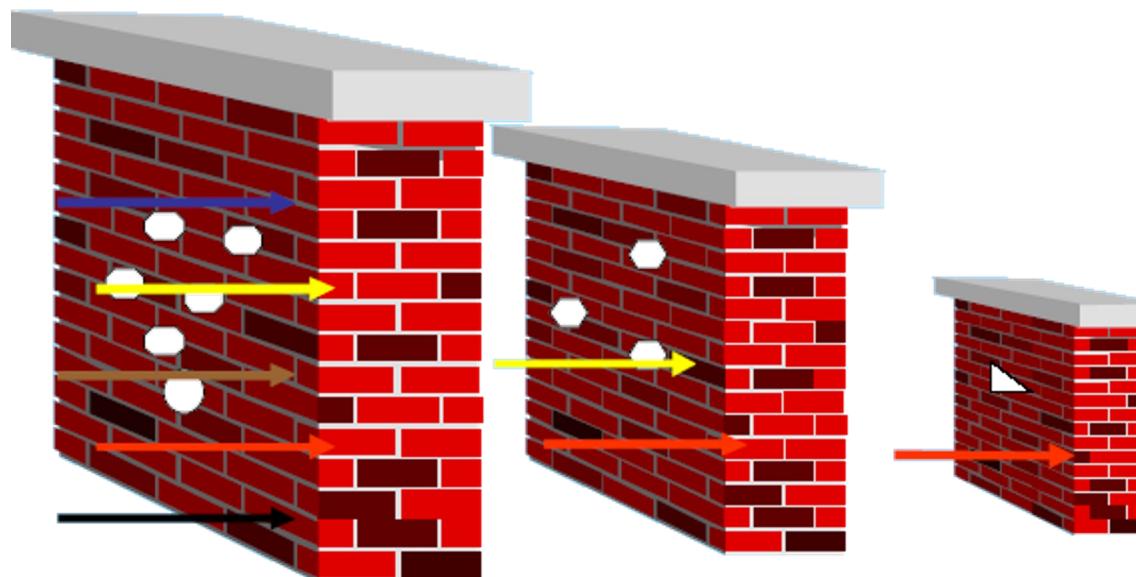


روش‌های تامین امنیت

- 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 سیستم یا شبکه





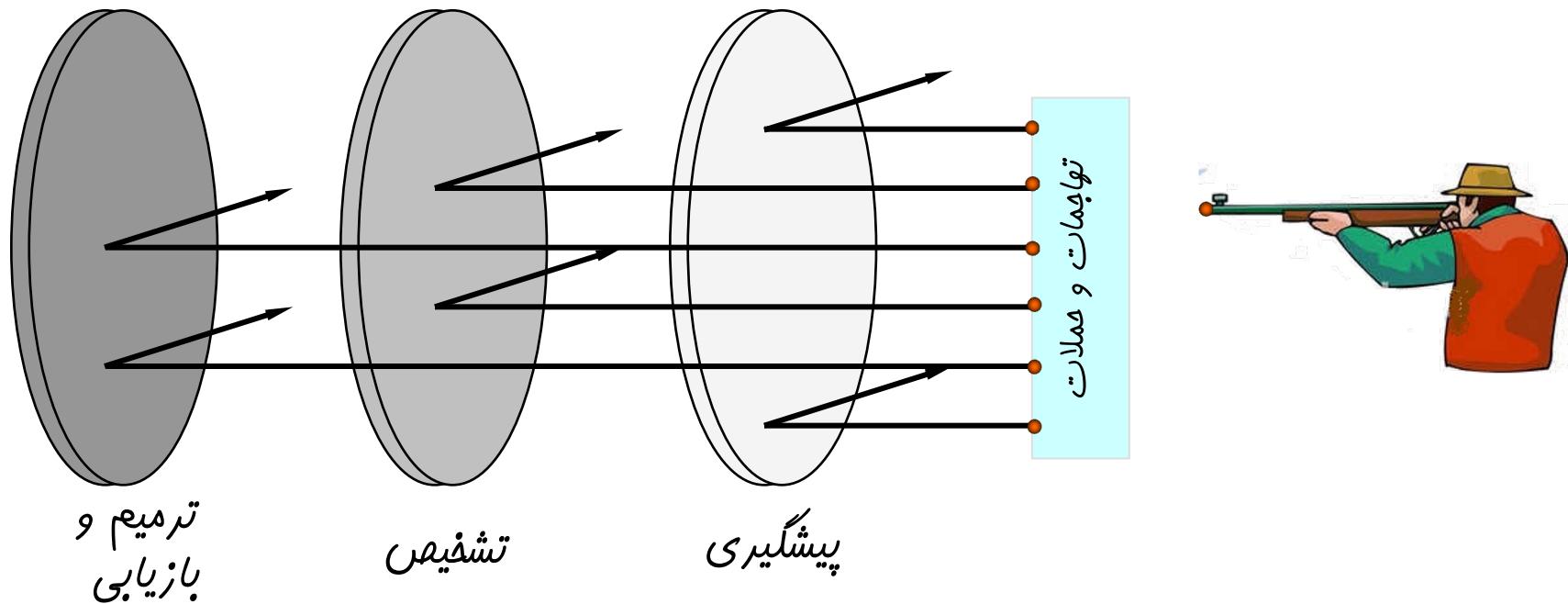
مثال: دفاع در عمق در یک سیستم شبکه‌ای

- سیستم عامل
 - وب‌سرور
 - پایگاه داده
 - برنامه کاربردی
- امنسازی در لایه شبکه و ارتباطات
- امنسازی در لایه کارگزار (Server)
- امنسازی در لایه کارخواه (Client)



مراقبه با نفوذ و تهاجم در سیستم

(پیشگیری، تشخیص، ترمیم)





پیشگیری، تشخیص، ترمیم و بازیابی

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



پیشگیری، تشخیص، ترمیم و بازیابی

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



پیشگیری، تشخیص، ترمیم و بازیابی

- 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 اصالت

Identification & Authentication □

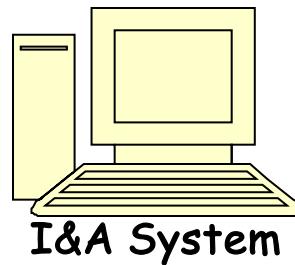
شناسایی کاربر و اطمینان از اینکه کاربر همان فردی است که ادعا می‌کند.

پیش‌نیاز کنترل دسترسی در هر سیستم، شناسایی و احراز هویت کاربر است.

فرآیند شناسایی و احراز هویت



اطلاعاتی از مشخصه‌های کاربر



مجاز بودن یا نبودن کاربر



پیشگیری – شناسایی و احراز اصالت

خطر افشا، حدس زدن، فراموشی



خطر سرقت، مفقود شدن، کپی کردن



□ بر اساس دانسته‌های کاربر

- مانند گذرواژه یا PIN

□ بر اساس داشته‌های کاربر

- کارت (پلاستیکی، مغناطیسی، هوشمند، ...)
- توکن امنیتی (Security Token)
- توکن تولید گذرواژه یکبار مصرف (OTP)



پیشگیری – شناسایی و احراز اصالت

خطر خطا در تشخیص، هزینه بالا

□ بر اساس مشخصات بیولوژیکی کاربر

- آنچه که هست: مانند اثر انگشت، چهره، شبکیه چشم
- آنچه که انجام می‌دهد: مانند ریتم تایپ کردن، نحوه صحبت کردن، یا نحوه



نوشتن با دست

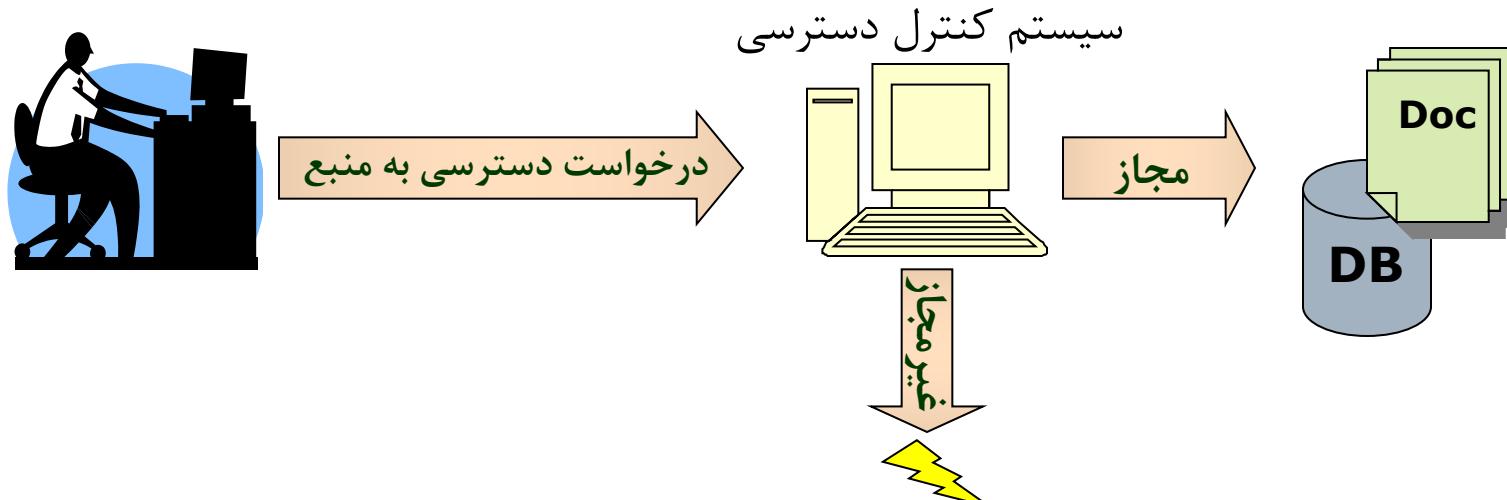


پیشگیری – کنترل دسترسی

Access Control □

mekanizm hestehai bari hafte amniyat dar hir siyestem kntrol dstrsi ast.

Wzifeh kntrol dstrsi karbaran o siyestemhahi diger ra be manabu o atlalat siyestem o ya shbke mord hafat br uehde dard.





پیشگیری – کنترل دسترسی (ادامه)

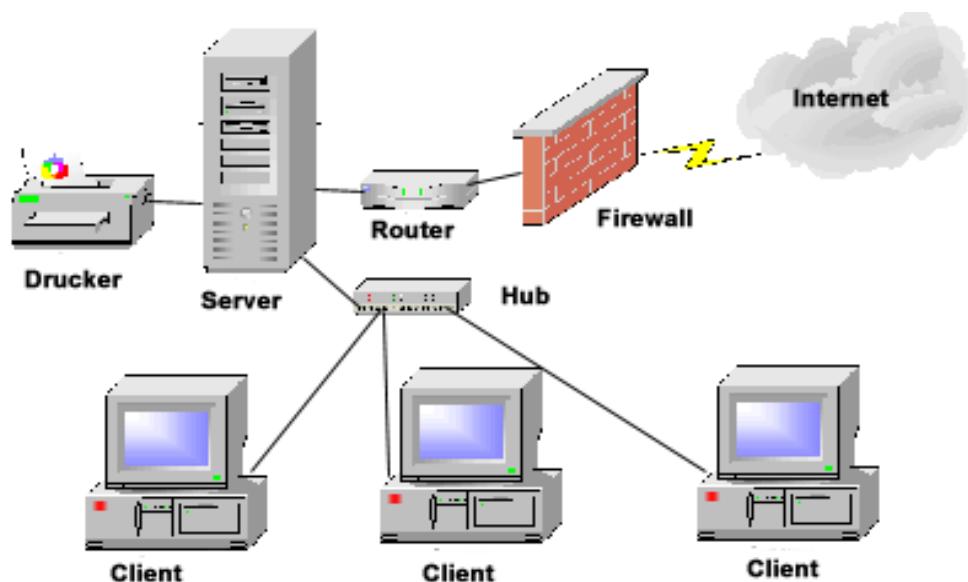
- پیش‌نیاز کنترل دسترسی، شناسایی کاربر و احراز اصالت هویت مورد ادعای آن است.
- پس از شناخت کاربر، دسترسی‌های وی را منابع بر اساس تدابیر امنیتی وضع شده توسط مدیر سیستم مشخص می‌نماییم.
- انواع روش‌های کنترل دسترسی
 - کنترل دسترسی اختیاری (DAC)
 - کنترل دسترسی اجباری (MAC)
 - کنترل دسترسی نقش-مبنای (RBAC)



پیشگیری - دیواره آتش

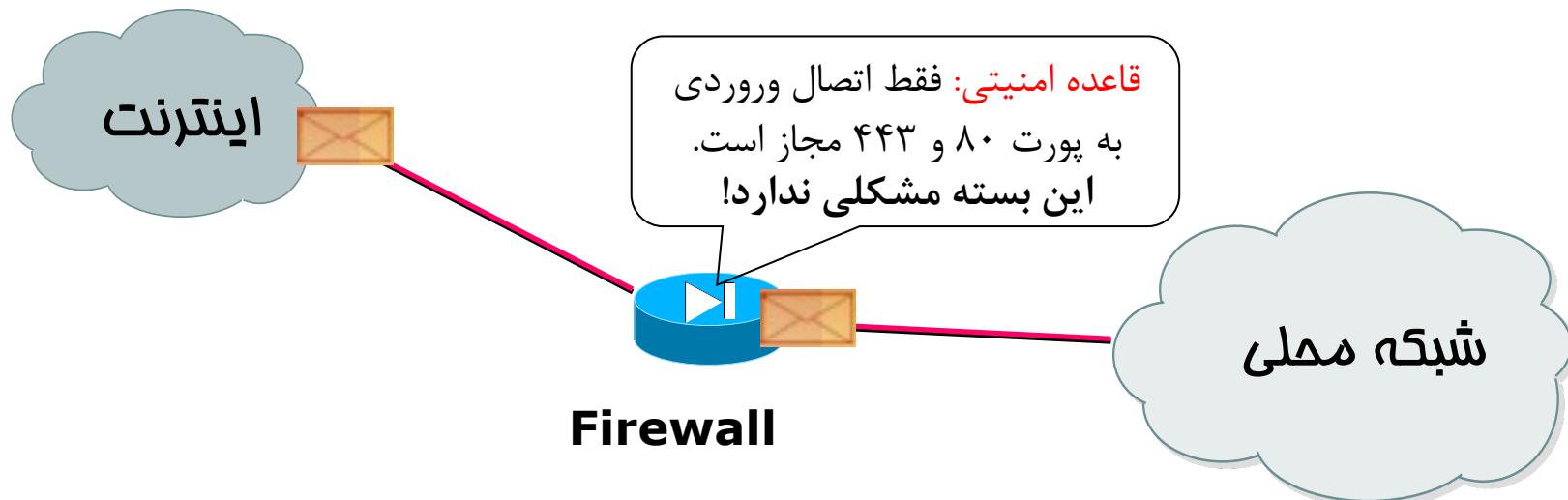
Firewall □

- یک سیستم امنیتی مبتنی بر مکانیزم کنترل دسترسی
- موظف به کنترل دسترسی کاربران خارجی به سیستم‌های شبکه 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.





امکانات یک دیواره آتش تجاری

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



پیشگیری - رمزنگاری

Cryptography •

- حفظ محربمانگی (پیشگیری): اطمینان از اینکه هر داده ذخیره شده و یا ارسالی بر روی شبکه تنها توسط گیرنده 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 (Decoding) + رمزگشایی (Encoding)



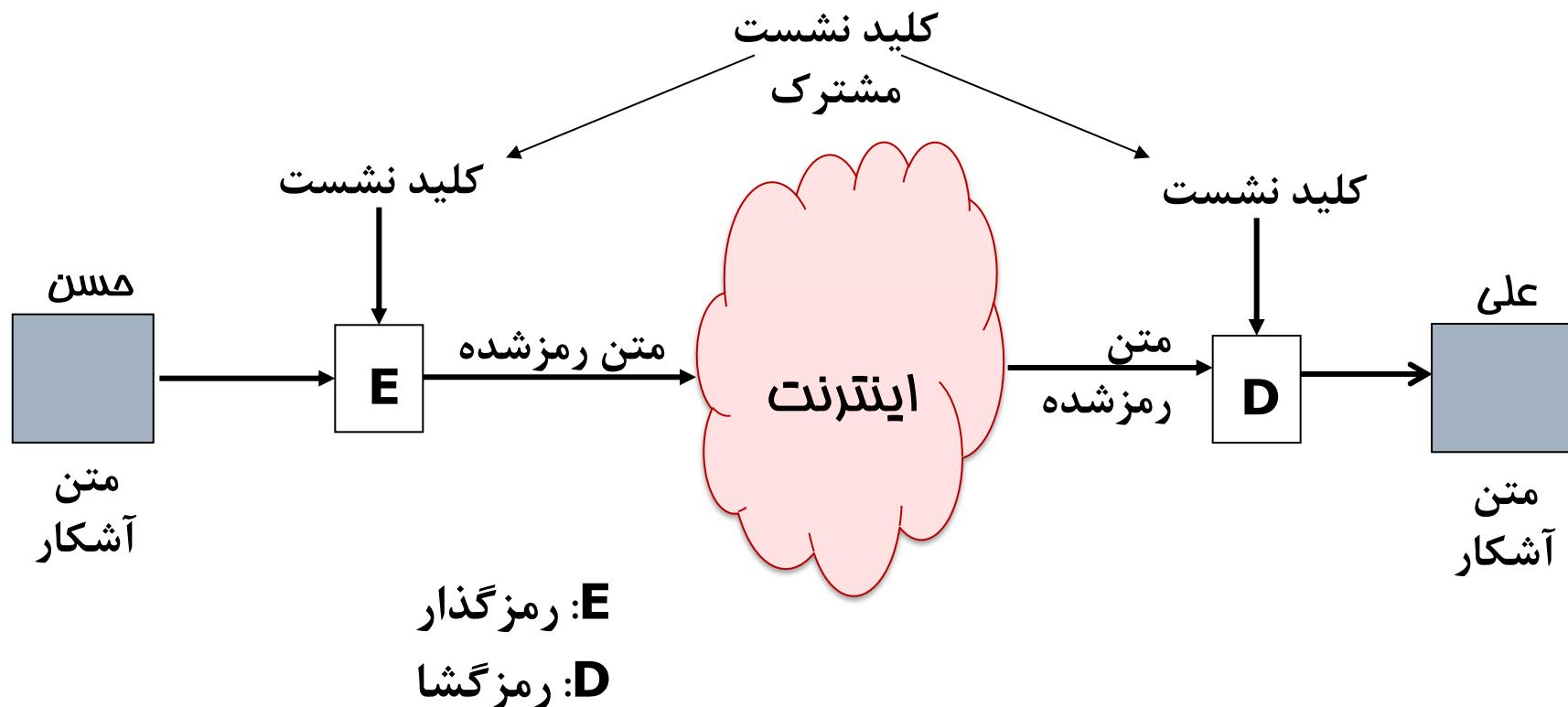
پیشگیری - رمزگاری متقارن

- 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 محربانگی داده‌ها و کنترل صحت
- نیاز به زمان کمتری برای رمزگذاری و رمزگشایی (نسبت الگوریتم‌های نامتقارن) دارد.



پیشگیری - رمزگاری متقارن (ادامه)

□ رمزگاری متقارن جهت حفظ محرمانگی





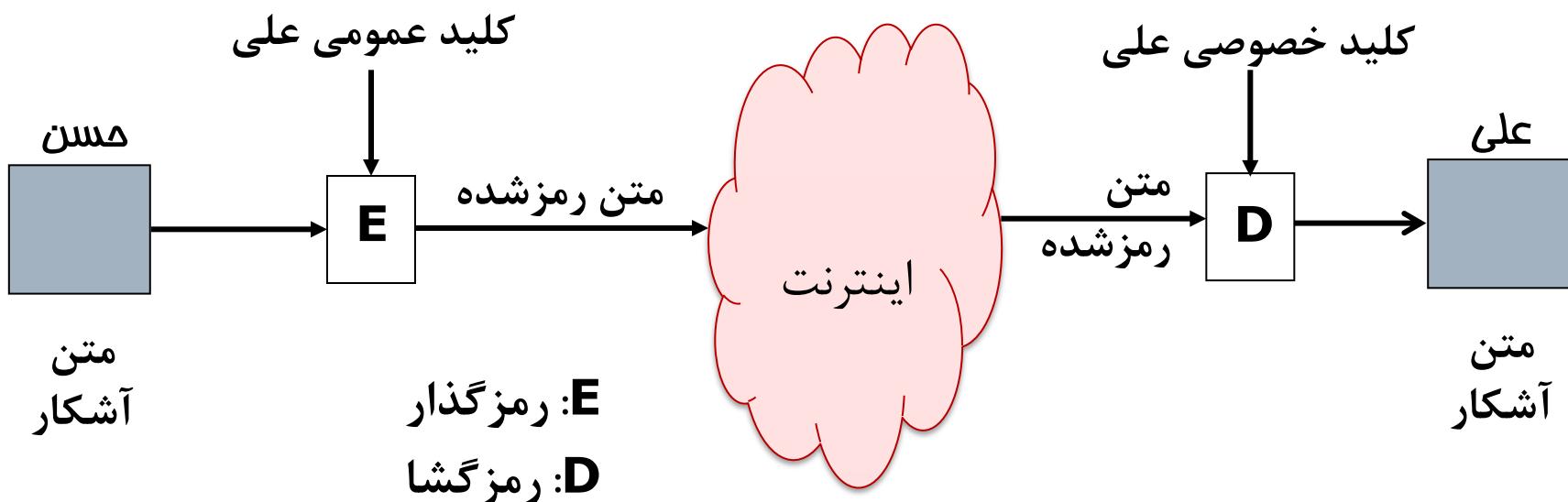
پیشگیری - رمزنگاری نامتقاضان

- 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



رمزگاری نامتقارن (ادامه)

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





روش‌های رمزنگاری ترکیبی

- تجمعیع محسن دو روش متقارن و نامتقارن
 - استفاده از رمزنگاری نامتقارن در تبادل کلید
 - استفاده از رمزنگاری متقارن در حفظ محترمانگی و صحت داده‌ها
- مثال‌های کاربردی:
 - شبکه‌های خصوصی مجازی VPN
 - پروتکل SSL
 - پروتکل SSH



فهرست مطالب

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



تشخیص - رمزگاری

- **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 پیام یا یک اطلاع با **کلیدی** که صرفاً در اختیار کاربر و یا مبدأ موردنظر است و وارسی آن در مقصد.

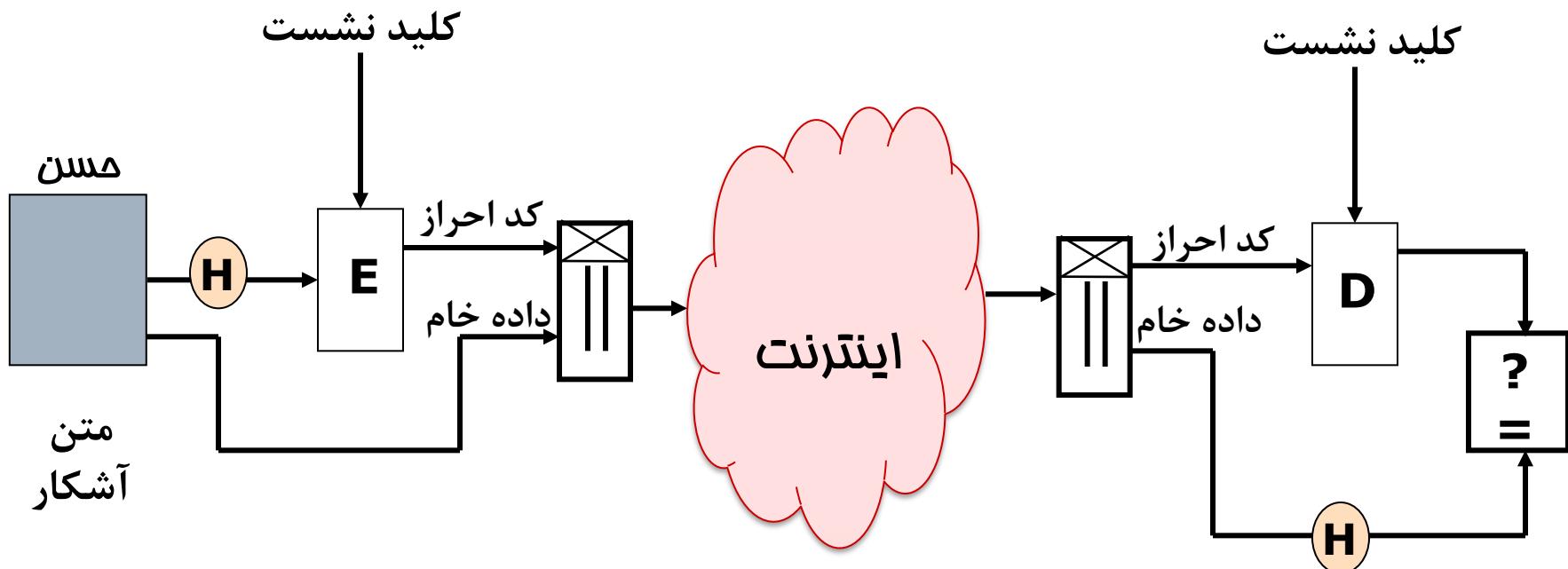


تشخیص - رمزگاری متقارن

E: رمزگذار
D: رمزگشایش

H: تابع درهمساز

□ فرآیند کنترل صحت با رمزگاری متقارن





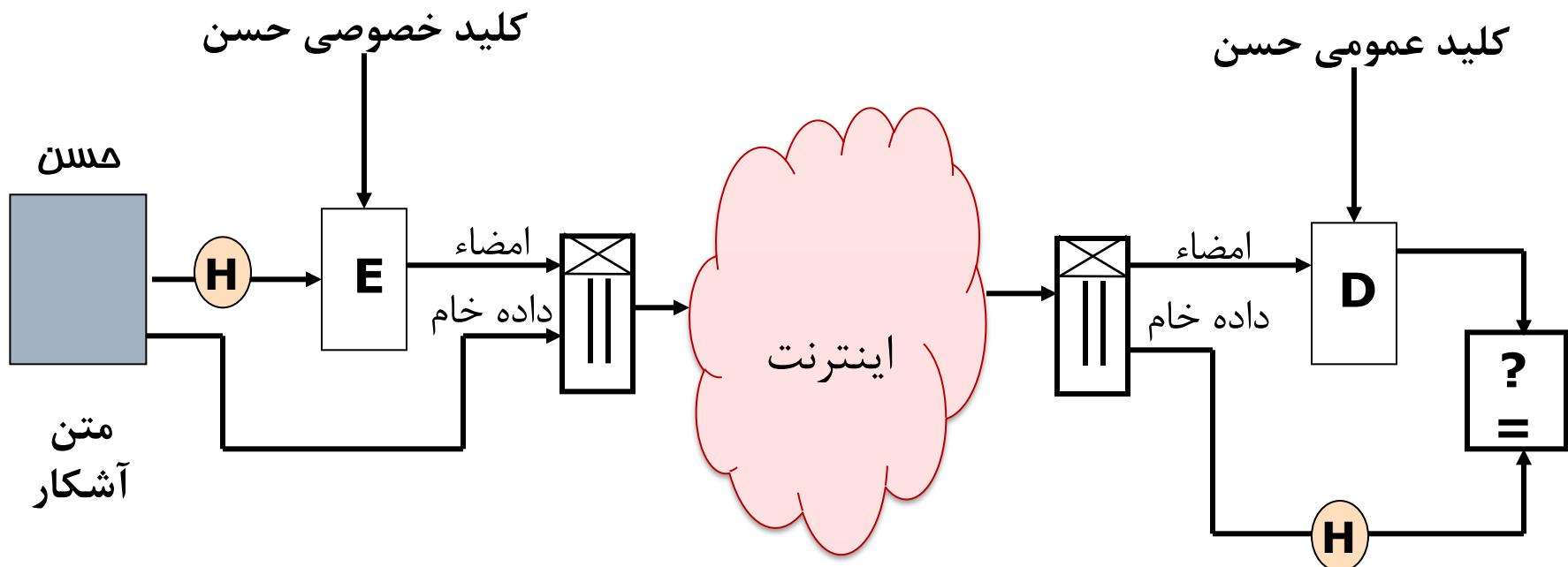
تشخیص - رمزنگاری نامتقارن

- رمزنگاری جهت احراز اصالت و کنترل صحت (امضای دیجیتال)
 - فرد می‌تواند با استفاده کلید خصوصی خود، یک امضا دیجیتال برای داده‌های ارسالی تولید نماید.
 - دیگران می‌توانند با استفاده از کلید عمومی فرد، صحت امضا دیجیتال را بر مبنای داده‌های دریافتی کنترل نمایند.
- امضا 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

تشخیص - رمزگاری نامتقارن

E: رمزگذار
D: رمزگشایی
H: تابع درهم‌ساز

□ فرآیند تولید امضا دیجیتال و کنترل صحت





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 سوء استفاده

□ سیستم تشخیص نفوذ (IDS)

سیستم تشخیص ناهنجاری

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



تشخیص - سیستم ضد بدافزار

□ وظایف سیستم ضد بدافزار

- پیشگیری از آلودگی به بدافزار (پیش از آلودگی)
- تشخیص انواع بدافزارها و فایل‌های آلوده به بدافزار (پس از آلودگی)
- واکنشی: قرنطینه/ پاکسازی بدافزارها

KASPERSKY

McAfee

Norton
from symantec

AVIRA

avast!
be free

AVG
Anti-Virus

TREND
MICRO

bitdefender
secure your every bit

NOD32
antivirus

G DATA

eset

F-Secure.



بدافزارها

□ **بدافزار (Malware):** یک قطعه گُد، اسکریپت، و یا برنامه که به قصد خرابکاری و اختلال در امنیت سیستم‌ها یا شبکه‌ها منتشر می‌شود.

□ اهداف خرابکارانه بدافزارها:

- دزدی اطلاعات محترمانه و نقض حریم خصوصی (مثلًا 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)

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



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

□ اسپ تروا (Trojan Horse)

■ مخفی در یک برنامه مفید یا به صورت یک برنامه به ظاهر مفید



انواع بدافزارها (۳)

□ جاسوس افزار (Spyware)

■ به منظور جاسوسی از سیستم قربانی و ارسال اطلاعات محترمانه

□ تبلیغ افزار (Adware)

■ با هدف تبلیغات به خصوص تبلیغات کالاها و خدمات غیرمجاز

□ کلیدنگار (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 توزیع شده

□ بمب منطقی (Logical Bomb)

- بدافزاری که به محض وقوع شرایطی خاص (مثلًاً 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.



انواع بدافزارها (۵)

WannaCry ransomware

The screenshot shows a Windows-style dialog box from the WannaCry ransomware. At the top right is a language selection dropdown set to English. The main message reads "Oops, your files have been encrypted!" Below it, a section titled "What Happened to My Computer?" states: "Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service." A second section, "Can I Recover My Files?", assures users they can recover files safely if they pay. It includes a note about the price doubling after three days and a warning about permanent file loss after seven days. A third section, "How Do I Pay?", explains payment via Bitcoin, providing a link to learn about Bitcoin and a specific Bitcoin address: 115p7UMMnqoj1pMvkpHijcRdfJNXj6LrLn. Buttons at the bottom include "Check Payment" and "Decrypt". Two sections of the interface are circled in red: the "Your files will be lost on" timer and the Bitcoin payment address.

Payment will be raised on
5/15/2017 16:50:06

Time Left
02:23:34:22

Your files will be lost on
5/19/2017 16:50:06

Time Left
06:23:34:22

Send \$300 worth of bitcoin to this address:
115p7UMMnqoj1pMvkpHijcRdfJNXj6LrLn

Contact Us Check Payment Decrypt



تشخیص - سیستم ضد بد افزار

- 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 بد افزارها



تشخیص – سیستم تله عسل

□ سیستم تله عسل (Honeypot)

- اغفال و فریب مهاجم جهت جمع‌آوری اطلاعات بیشتر از نحوه عملکرد آن
- شبیه‌سازی یا ارایه یک یا چند سرویس شبکه که بر روی کارگزار مورد حفاظت در حال اجرا می‌باشند.
- سیستم تله عسل ریسک امنیتی دارد. اگر مهاجم بر آن تسلط یابد، می‌تواند برای شبکه مشکل‌ساز باشد.





تشخیص – سیستم تله عسل

□ سیستم‌های تله عسل کم تعامل (Low Interaction)

- به شبیه‌سازی سرویس‌ها و سیستم‌ها می‌پردازند.
- هر ترافیک به سمت این سرویس‌ها مشکوک است.
- فایل‌های ارسالی به این سرویس‌ها احتمالاً **بدافزار (کرم)** هستند.

□ سیستم‌های تله عسل پر تعامل (High Interaction)

- سرویس‌های واقعی در محیطی ایزوله و کاملاً کنترل شده ارایه می‌شوند.
- تمام فعالیت‌های مهاجم در این سرویس‌ها ثبت و مورد تحلیل قرار می‌گیرند.
- با توجه به واقعی بودن سیستم، خطر تسلط مهاجم به سیستم و نفوذ به شبکه وجود دارد.



تشخیص - سیستم تله عسل

میزبان‌های شبیه‌سازی شده

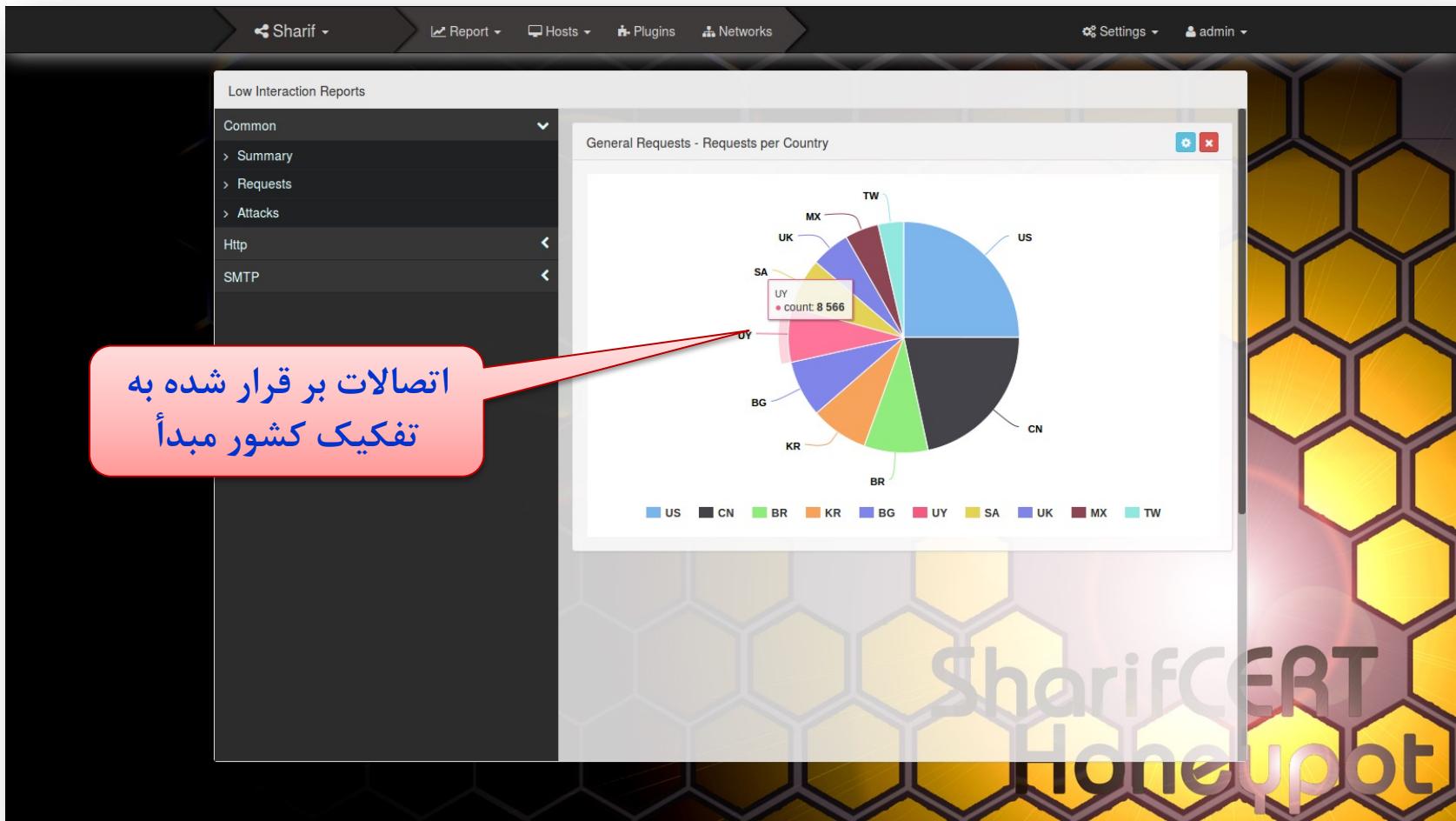
The screenshot displays the HoneyPot web-based management interface. The top navigation bar includes links for 'Sharif', 'Report', 'Hosts' (selected), 'Plugins', 'Networks', 'Settings', and 'admin'. The main content area is divided into several sections:

- Low Interaction Hosts:** A grid of 16 hosts, each represented by a small monitor icon and labeled host1 through host16. Host 1 is highlighted in blue.
- Create Host:** A green button for adding new hosts.
- Host Configuration:** A detailed view for host 1, showing its ID (1), name (host1), and status (On). It also lists its IP configuration: IP (192.168.253.101), IP mask (255.255.255.0), and gateway (192.168.253.254).
- Delete Host:** A red button to remove the host.
- Plugin Host:** A list of 25 configured ports:
 - 1. ftp [21]
 - 2. ssh [22]
 - 3. telnet [23]
 - 4. smtp [25]
 - 5. dns-tcp [53]
 - 6. http [80]
 - 7. kerberos [88]
 - 8. pop3 [110]
 - 9. netbios [137]
 - 10. imap [143]



تشخیص - سیستم تله عسل

نمونه گزارش‌ها





تشخیص - سیستم تله عسل

نمونه گزارش‌ها

جزییات در خواست مهاجم

Client	Server	Request time	Country	City	Expert info
115.230.124.164:3178	192.168.253.106:80	2016-02-01 16:56:11+03:30	China (CN)	Beijing	<button>view</button>
115.230.124.164:3491	192.168.253.108:80	2016-02-01 16:56:11+03:30	China (CN)	Beijing	<button>view</button>
115.230.124.164:3134	192.168.253.116:80	2016-02-01 16:56:11+03:30	China (CN)	Beijing	<button>view</button>
115.230.124.164:2581	192.168.253.111:80	2016-02-01 16:56:12+03:30	China (CN)	Beijing	<button>view</button>
<pre>connection: application-id: 7d596674-3eb2-405e-b94a-cd6e14cf0359 start-time: '2016-02-01 16:56:11+03:30' end-time: '2016-02-01 16:56:13+03:30' duration: 2 info: ATTACK: - name: Bad Request raw: 'GET http://zc.qq.com/cgi-bin/common/attr?id=260714&r=0.7927286104172206 HTTP/1.1' - name: INCLUSION description: "http\\:\\\\\\\"</pre>					
115.230.124.164:3378	192.168.253.110:80	2016-02-01 16:56:12+03:30	China (CN)	Beijing	<button>view</button>
115.230.124.164:3596	192.168.253.109:80	2016-02-01 16:56:12+03:30	China (CN)	Beijing	<button>view</button>
115.230.124.164:1366	192.168.253.103:80	2016-02-01 16:56:13+03:30	China (CN)	Beijing	<button>view</button>
115.230.124.164:3854	192.168.253.101:80	2016-02-01 16:56:13+03:30	China (CN)	Beijing	<button>view</button>
115.230.124.164:1362	192.168.253.102:80	2016-02-01 16:56:13+03:30	China (CN)	Beijing	<button>view</button>
183.3.202.108:58530	192.168.253.115:22	2016-02-01 16:56:13+03:30	China (CN)	Beijing	<button>view</button>

« 4 of 2402 »



تشخیص - سیستم مدیریت اطلاعات و رویدادهای امنیتی

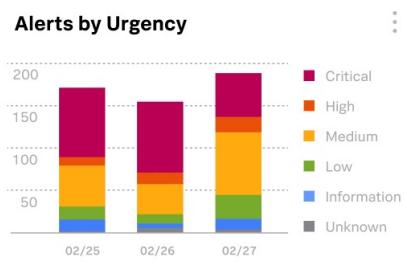
Security Information & Event Management (SIEM) □

- **وظایف:** جمع‌آوری اطلاعات و رویدادهای امنیتی/سیستمی/شبکه‌ای، همبسته‌سازی و تحلیل، تشخیص و پاسخ
- جمع‌آوری اطلاعات و رویدادها از

ArcSight

دستگاه‌های مختلف امنیتی (دیواره آتش، سیستم تشخیص نفوذ، ...)

splunk



سیستم‌ها و سرورها (لاگ سیستم عامل، لاگ کارگزار وب، ...)

تجهیزات شبکه (سوییچ‌های اصلی، مسیریاب، ...)

- **مزایا:** حذف هشدارهای مثبت-غلط

کاهش و تجمعیه هشدارها

Qradar



تشخیص - سیستم مدیریت اطلاعات و رویدادهای امنیتی

splunk

splunk>cloud Apps ▾ 4 Messages ▾ Settings ▾ Activity ▾ Find SOS Admin ▾ Support & Services ▾ Enterprise Security

Security Posture Incident Review Investigations Security Intelligence ▾ Security Domains ▾ Cloud Security ▾ Audit ▾ Search ▾ Configure ▾ Edit Export ...

Security Posture

Key Indicators

Access Notables Total Count 72 +72 **Endpoint Notables** Total Count 0 **Network Notables** Total Count 163 +163 **Identity Notables** Total Count 0 **Audit Notables** Total Count 0 **Threat Notables** Total Count 110 +110 **UBA Notables** Total Count 3 +3

Notable Events By Urgency

urgency	count
critical	72
high	100
low	55
medium	115

Notable Events Over Time

time	access	network	threat
8:00 PM Wed May 25 2022	10	8	5
12:00 AM Thu May 26 2022	15	12	8
4:00 AM	10	8	5
8:00 AM	8	5	3
12:00 PM	10	8	5
4:00 PM	12	10	8

Top Notable Events

rule_name	sparkline	count
Unusual Volume of Outbound Traffic By Src 2020		158
Geographically Improbable Access Detected		72
Risk Threshold Exceeded For Object Over 24 Hour Period		30
ESCU - Malicious PowerShell Process - Encoded Command - Rule		22
ESCU - Monitor Email For Brand Abuse - Rule		22
RIR - 7 Day ATT&CK Tactic Threshold Exceeded		17

Top Notable Event Sources

src	sparkline	correlation_search_count	security_domain_count	count
104.207.83.63		1	1	24
199.66.91.253		1	1	24
172.16.0.127		2	2	16
172.16.0.13		2	2	16
172.16.0.149		2	2	16
10.0.1.4		2	2	15



تشخیص - سیستم مدیریت اطلاعات و رویدادهای امنیتی

splunk

splunk>cloud Apps 4 Messages Settings Activity Find SOS Admin Support & Services

Security Posture Incident Review Investigations Security Intelligence Security Domains Cloud Security Audit Search Configure Enterprise Security

Incident Review

Search... Hide Charts Hide Filters

Urgency

Informational
Low
Medium
High
Critical

Status

Unassigned
New
In Progress
Pending
Resolved
Closed

Owner

SOS Admin
SOAR Admin
Splunk Cloud Admin
unassigned

Domain

Access
Endpoint
Network
Threat
Identity
Audit

Saved filters Tag Urgency Status Owner Security Domain Type Search Type Time or Associations Time Last 24 ...

Select... Add tags... Select... Select... Select... Select... Correlatio... Select... Time Last 24 ...

Save new filters Update Clear all Submit Time Range: Last 24 hours

338 Notables

Unselect all | Edit Selected | Edit All Matching Events (338) | Add Selected to Investigation

1 2 3 4 5 ... Next > 20 per page Refresh

Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
--	--	Notable	Today, 4:24 PM	Undetermined	Threat	⚠ Medium	New	unassigned	
332	7	Risk Notable	Today, 4:21 PM	Undetermined	Threat	⚠ Medium	New	unassigned	
378	--	Risk Notable	Today, 4:09 PM	Undetermined	Threat	⚠ Medium	In Progress	unassigned	
624	--	Risk Notable	Today, 4:09 PM	Undetermined	Threat	⚠ Medium	In Progress	unassigned	

Notable Details:

- Malicious PowerShell Process - Encoded Command On FYODOR-L.splunktshirtcompany.com
- 24 hour risk threshold exceeded for system=mvalitus-L.splunktshirtcompany.com
- RBA: ATT&CK Tactic threshold exceeded (≥ 3) over previous 7 days for user=mvalitus@splunktshirtcompany.com spanning 3 Risk Rules, 3 ATT&CK tactics, and 7 ATT&CK techniques
- RBA: ATT&CK Tactic threshold exceeded (≥ 3) over previous 7 days for system=mvalitus-L.splunktshirtcompany.com spanning



تشخیص - سیستم مدیریت اطلاعات و رویدادهای امنیتی

splunk

The screenshot shows the Splunk Cloud Enterprise Security interface. At the top, there's a navigation bar with links like 'splunk>cloud', 'Messages', 'Settings', 'Activity', 'Find', 'SOS Admin', 'Support & Services', and 'Enterprise Security'. Below the navigation is a 'Security Posture' section with tabs for 'Incident Review', 'Investigations', 'Security Intelligence', 'Security Domains' (which is selected), 'Cloud Security', 'Audit', 'Search', and 'Configure'. A pink box highlights the 'Access' sub-menu under 'Security Domains'.

The main area features an 'Access Center' with sections for 'Action' (All) and 'App' (All). It displays 'Key Indicators' such as 'AUTH. APPS' (13, +13), 'AUTH. SOURCES' (6, +6), 'AUTH. DEST'S' (2, +2), 'AUTH. USERS' (7, +7), and 'AUTH. ATTEMPTS' (0). Below these are two charts: 'Access Over Time By Action' (green area chart with 'success' and 'failure' segments) and 'Access Over Time By App' (blue area chart with various app names listed on the legend).

At the bottom, there are two tables: 'Top Access By Source' and 'Top Access By Unique Users'. The 'Top Access By Source' table lists sources like 'unspecified', '199.66.91.253', and '107.77.211.7' with their respective counts. The 'Top Access By Unique Users' table lists unique users with their counts, such as 'unspecified' (18553), '104.207.83.63' (1238), and '107.77.211.7' (775).



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 پشتیبان‌گیری شده



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



پایان

پست الکترونیکی

amini@sharif.edu

kharrazi@sharif.edu