یا ذاالامن والامان

مرور مکانیزم‌های تامین امنیت

مبانی امنیت اطلاعات و شبکه‌های کامپیوتری

محمدرضا رازیان*

بهار و تابستان 1395

مرکز تخصصی آپا

دانشگاه سمنان

مرکز تخصصی آپا دانشگاه سمنان

http://cert.semnan.ac.ir

آزمایشگاه امنیت داده و شبکه شریف

http://dnsl.ce.sharif.ir

*Homepage: www.mrazian.com

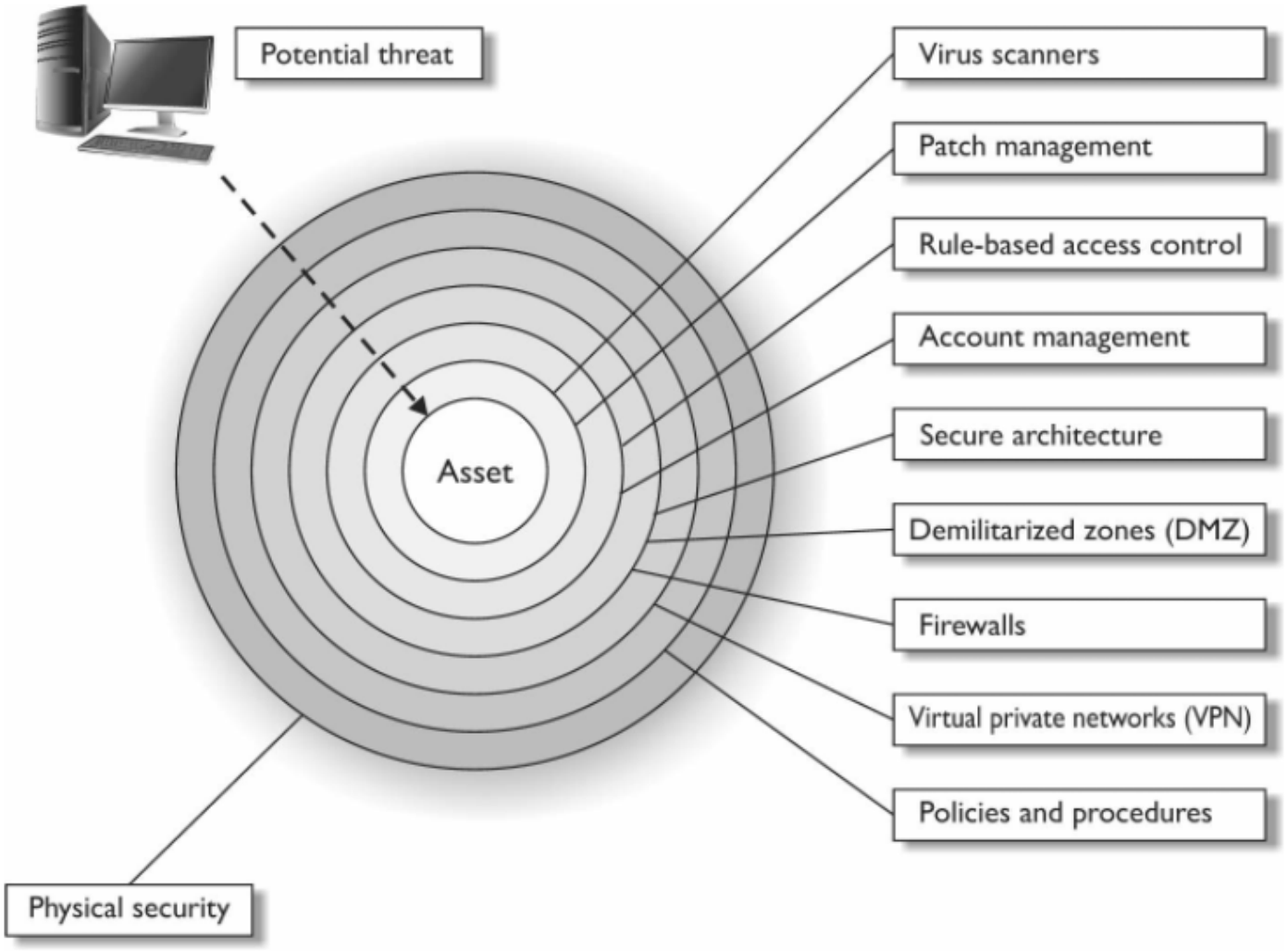
فهرست مطالب

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

روش‌های تامین امنیت

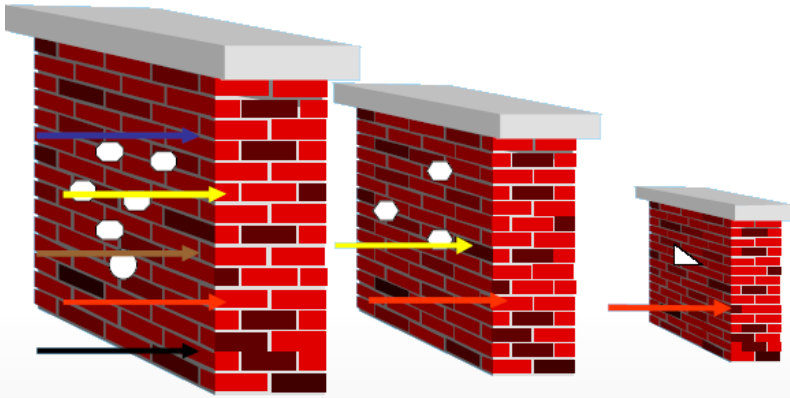
- دفاع در عمق
- پیاده‌سازی راه‌حل‌های پیشگیرانه
- پیاده‌سازی راه‌حل‌های تشخیص
- پیاده‌سازی راه‌حل‌های ترمیم و پشتیبانی

دفاع در عمق


Potential threat
Asset
Physical security
Virus scanners
Patch management
Rule-based access control
Account management
Secure architecture
Demilitarized zones (DMZ)
Firewalls
Virtual private networks (VPN)
Policies and procedures

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

- 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,...)

دفاع در عمق – امن‌سازی کارگزار

- 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 – امن‌سازی کارخواه

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

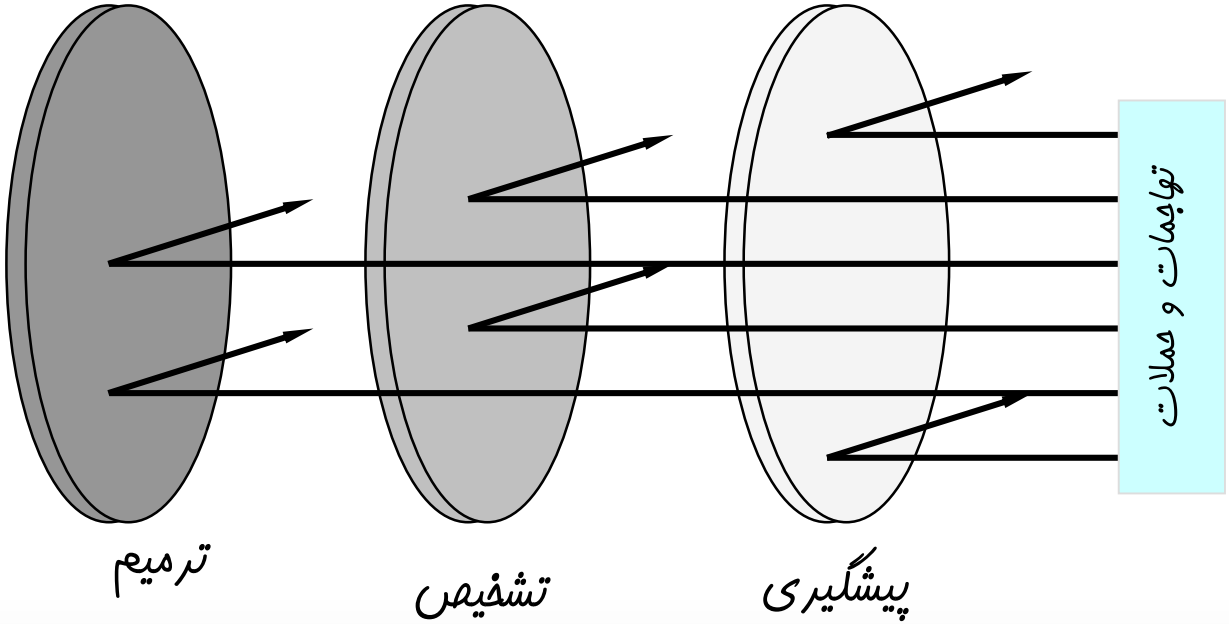
مثال: دفاع در عمق در سیستم نرم‌افزاری

امن‌سازی همه لایه‌های نرم‌افزاری یک سیستم شامل:

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

مراتب مقابله با نفوذ و تهاجم در سیستم

(پیشگیری، تشخیص، ترمیم)



فهرست مطالب

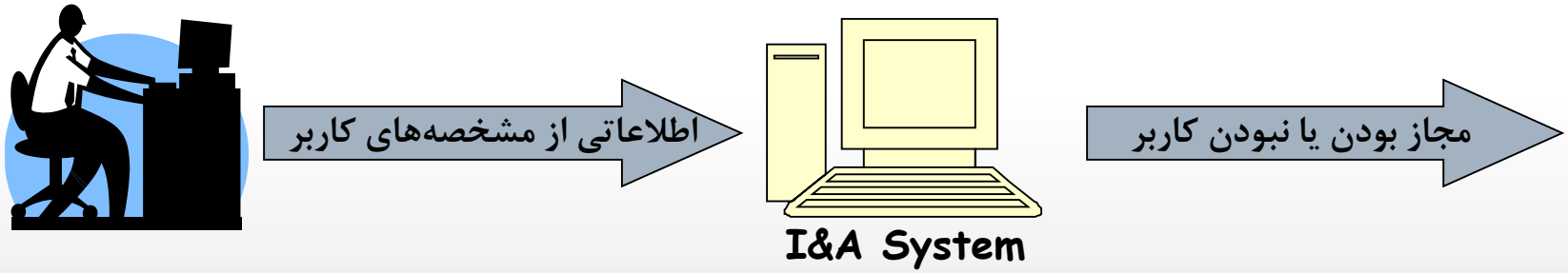
- روشهای تامین امنیت
- **مکانیزم‌های پیشگیری**
- مکانیزم‌های تشخیص
- مکانیزم‌های ترمیم

مکانیزم‌های پیشگیری

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

پیشگیری – شناسایی و احراز اصالت

- Identification & Authentication
  - پیش‌نیاز کنترل دسترسی در هر سیستم، شناسایی کاربر (متقاضی) و احراز اصالت مورد ادعای آن
  - فرآیند شناسایی و احراز اصالت



پیشگیری – شناسایی و احراز اصالت

احراز اصالت 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 اصالت

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

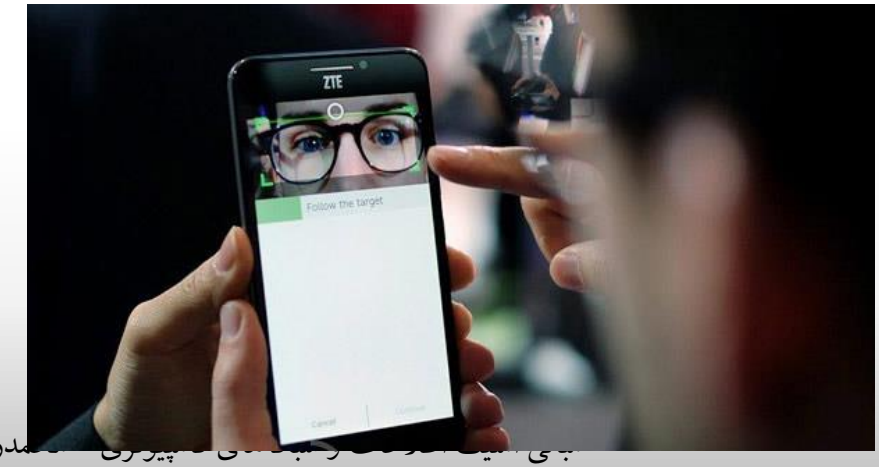
راه حل: ترکیب با روش‌های دیگر

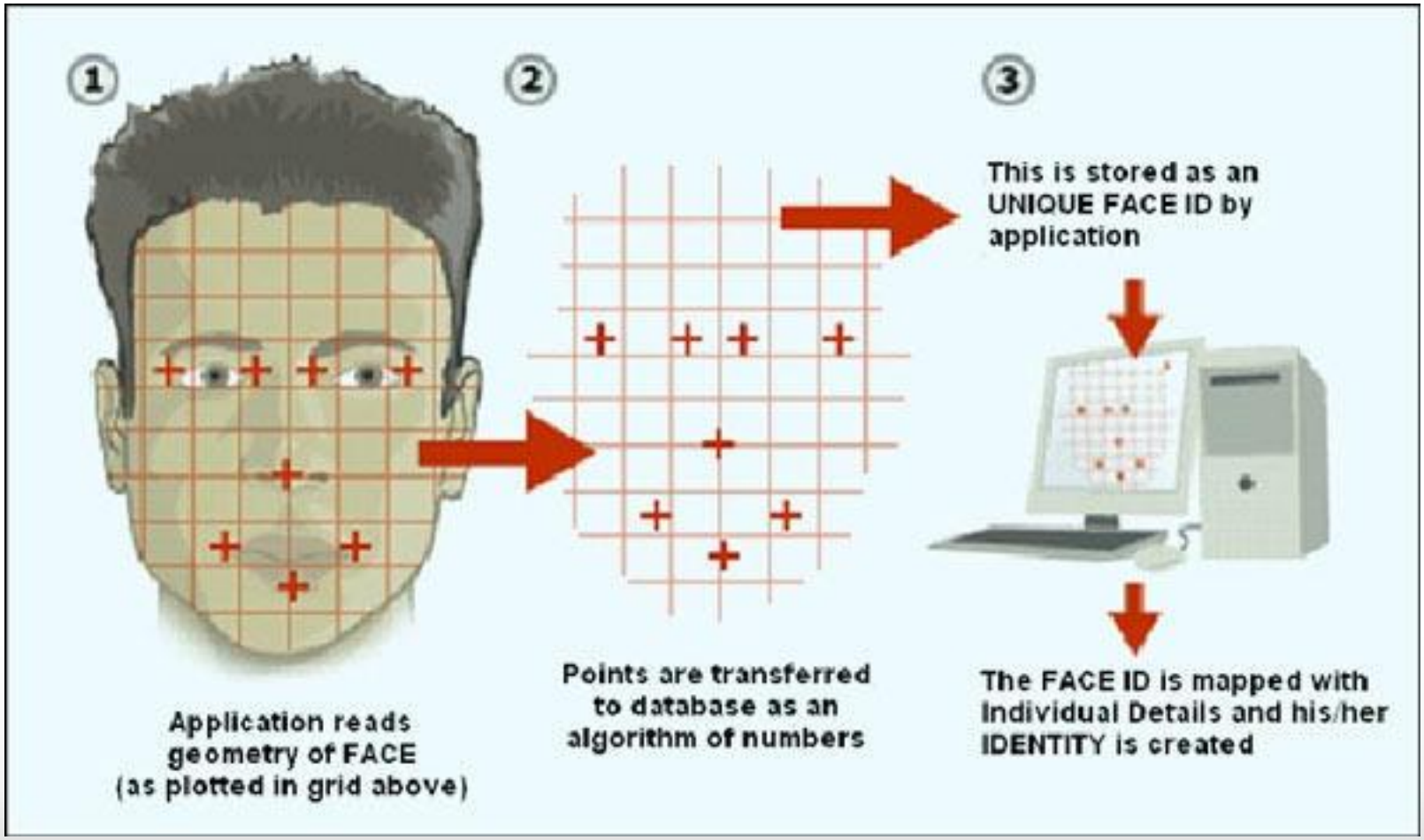
پیشگیری – شناسایی و احراز اصالت

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




1
2
3
This is stored as an UNIQUE FACE ID by application
Application reads geometry of FACE (as plotted in grid above)
Points are transferred to database as an algorithm of numbers
The FACE ID is mapped with Individual Details and his/her IDENTITY is created

پیشگیری – شناسایی و احراز اصالت

حفاظت از داده های احراز اصالت

- 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 اصالت

- محتوای فایل shadow حاوی گذرواژه‌ها در لینوکس

```
libuuid:!:16177:0:99999:7:::
syslog:*:16177:0:99999:7:::
messagebus:*:16177:0:99999:7:::
usbmux:*:16177:0:99999:7:::
dnsmasq:*:16177:0:99999:7:::
avahi-autoipd:*:16177:0:99999:7:::
kernoops:*:16177:0:99999:7:::
rtkit:*:16177:0:99999:7:::
saned:*:16177:0:99999:7:::
whoopsie:*:16177:0:99999:7:::
speech-dispatcher:!:16177:0:99999:7:::
avahi:*:16177:0:99999:7:::
lightdm:*:16177:0:99999:7:::
colord:*:16177:0:99999:7:::
hplip:*:16177:0:99999:7:::
pulse:*:16177:0:99999:7:::
mohammad:$6$0gTjGBrI$gLt9t/5l1Y4iQ0sARo3tMp7w2Tx28g0sCKcXZWfLZNuHPMJg8YUVSQozuql9WOX8xQ/OPxU.D3DdNlgEdVqK/.:16582:0:99999:7:::
privoxy:*:16215:0:99999:7:::
debian-tor:*:16215:0:99999:7:::
mysql:!:16223:0:99999:7:::
ali:$6$zeH.69eQ$8nBw5uJh6FFGYpoYXR0K3JZGCGcu3pfMwRu/tXFQRH3J8q3XNiDv3P7dozf88BoLp/.1wPbxGOeVqEAtnCp8q1:16582:0:99999:7:::
94121314:$6$Yv/AslRj$17KvjFzUW7hRnkaVpX2l94wHYVfqm/Cljavi86xr.djNWcRFYvNOCzxLVQgrg4kAzKOOoOut8H2OKqkgUx5UI/:16703:0:99999:7:::
```

پیشگیری – شناسایی و احراز اصالت

مکانیزم‌های تشخیص

- سیستم تشخیص نفوذ (IDS)
- سیستم تله‌عسل (Honeypot)

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

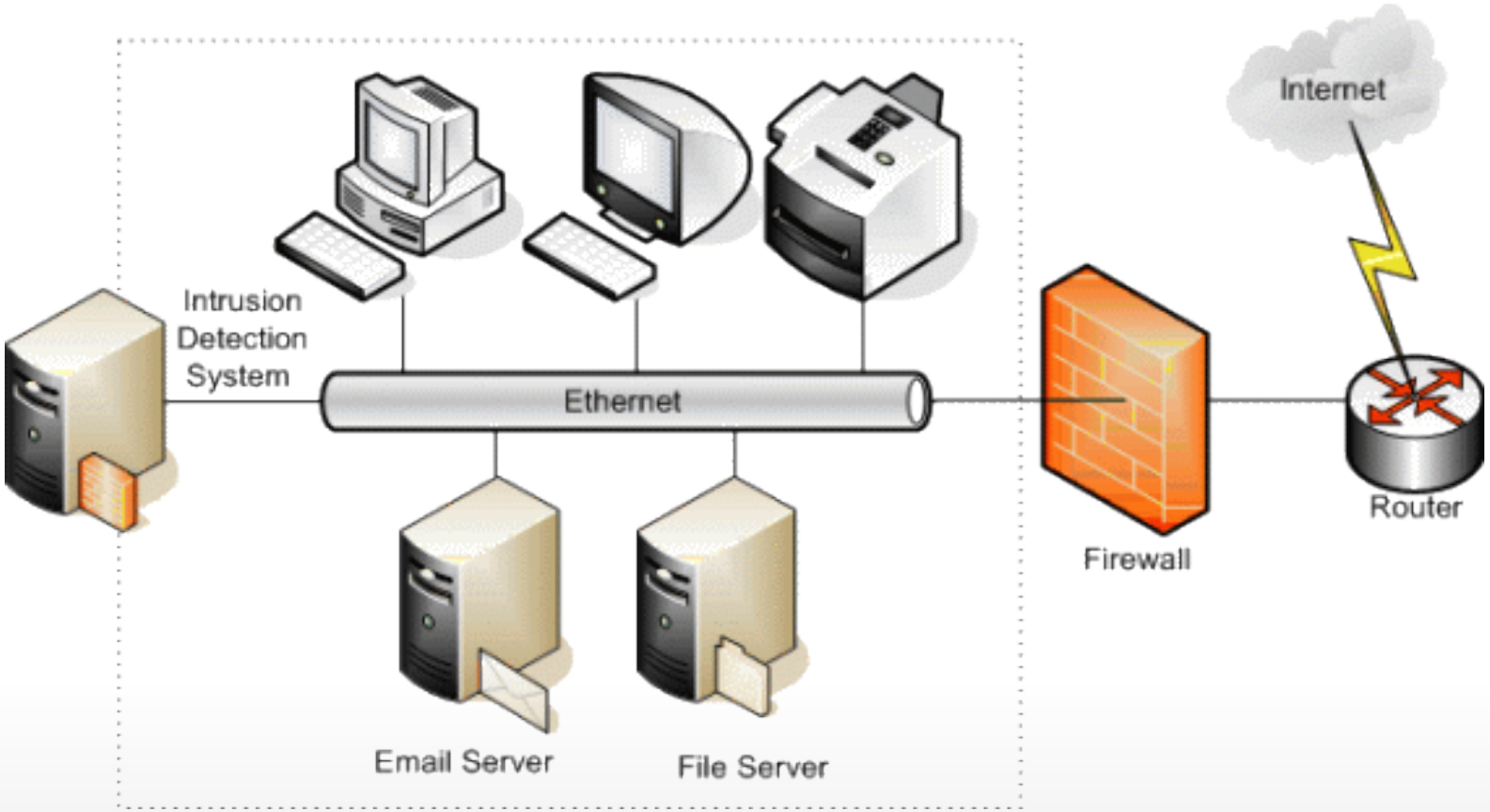
- **سیستم تشخیص نفوذ (IDS)**

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

سیستم تشخیص سوء استفاده

سیستم تشخیص ناهنجاری

تشخیص – سیستم تشخیص نفوذ



سیستم تشخیص سوءاستفاده

- **تشخیص سوءاستفاده (Misuse Detection)**
  - شناخت حملات موجود
  - تعریف الگوی 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

- **تشخیص ناهنجاری (Anomaly Detection)**
  - شناخت عملکرد نرمال سیستم
  - تهیه نمایه‌هایی از رفتار نرمال سیستم برای موتور تحلیل
  - تشخیص فعالیت غیرنرمال به عنوان حمله

تشخیص – سیستم ضدبدافزار

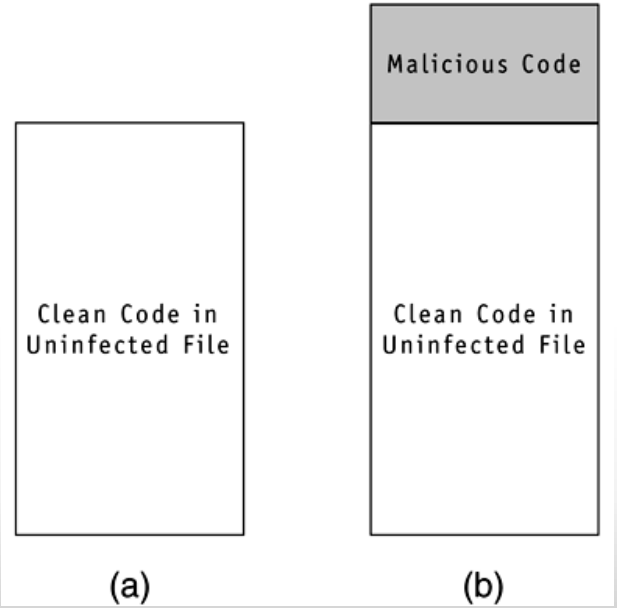
- **وظایف سیستم ضدبدافزار**
  - تشخیص انواع بدافزارها و فایلهای آلوده به بدافزار
  - پاکسازی بدافزارها
- **بدافزار**
  - ویروس (Virus)
  - کرم (Worm)
  - تروجان (Trojan)
  - بمب منطقی (Logical Bomb)
  - ابزارهای جاسوسی (Spyware)
  - ابزارهای حمله (Hack & Attack Tools)

بدافزارها

- بد افزار، نرم افزاری است که به قصد انجام اعمالی هدفمند وارد یک سیستم می‌شود در صورتی که اجازه انجام آن اعمال را ندارد.
- واژه بدافزار (Malware) از دو واژه Malicious و Software گرفته شده است. در ادامه با برخی از انواع بدافزارها آشنا می‌شویم.

ویروس

- برنامه کوچکی که به برنامه‌های دیگر می‌چسبد و به انتشار خود و خرابکاری در سیستم می‌پردازد.
- برای مثال ویروس می‌تواند به یک نرم افزار ویرایشگر متن اضافه شود حال زمانی که این نرم افزار شروع به کار کند، ویروس فعال شده و به فعالیت‌های خود مثل انتشار خود، از کار انداختن نرم افزارهای تشخیص بدافزار و... بر روی یک سیستم کامپیوتری می‌پردازد.
- ویروس با استفاده از USB، Floppy و ... می‌تواند
- از یک کامپیوتر به کامپیوتر دیگر منتقل شود.



کرم

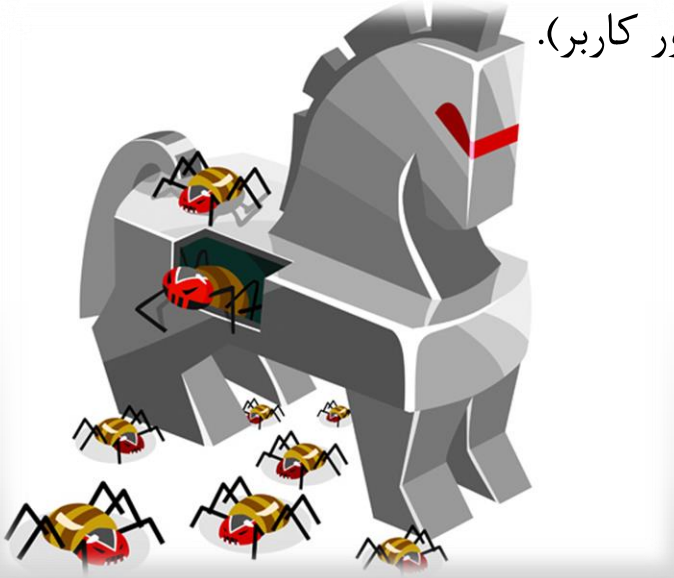
- **کرم:** برنامه مستقلی است که خود را به سرعت منتشر می‌کند و معمولاً منابع و پهنای باند را بی‌جهت اشغال می‌کند.
- کرم‌ها (Worm) برای انتشار خود نیاز به اضافه شدن (مقیم شدن) به نرم‌افزار خاصی ندارند و خودشان می‌توانند اجرا شوند.
- تفاوت اصلی کرم با ویروس این است که کرم نیازی به مقیم شدن در برنامه دیگر را ندارد.
- تفاوت دیگر در مدل انتشار آن‌ها است ویروس‌ها تلاش می‌کنند تا در برنامه‌ها و فایل‌های یک کامپیوتر منتشر شوند در صورتی که کرم‌ها از طریق شبکه به انتشار خود می‌پردازند تا بتوانند شبکه‌ای از کامپیوترها را آلوده کنند.

بمب منطقی – تروجان

- **بمب منطقی:** برنامه‌ای که به محض وقوع شرایطی خاص (مثلا در یک تاریخ مشخص) فعال می‌شود و به خرابکاری می‌پردازد.
- بمب‌های منطقی می‌توانند به عنوان یک برنامه مستقل و یا به عنوان بخشی از یک ویروس یا کرم باشند
- مثالی از یک بمب منطقی می‌تواند ویروسی باشد که صبر می‌کند تا تعداد خاصی از میزبان‌ها آلوده شوند سپس اجرا می‌شود
- بمب زمانی زیرمجموعه‌ای از بمب منطقی است که در تاریخ یا زمانی خاص فعال می‌شود
- بمب‌های منطقی تا قبل از اینکه اجرا شوند غیرقابل شناسایی خواهند بود
- مثالی از بمب زمانی: ویروس Friday the 13th

بمب منطقی – تروجان

- **تروجان** (Trojan Horse): 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.
- طراح تروجان، آن را در یک برنامه جاسازی می‌کند. این برنامه به عنوان یک برنامه مفید به کاربر نشان داده می‌شود (مثلاً برنامه نمایش وضع آب و هوا) اما فعالیت‌های مخرب خود را انجام می‌دهد (مثل ثبت کلیدهایی که کاربر بر روی صفحه کلید فشار می‌دهد و ارسال این اطلاعات و یا شبیه سازی صفحه Login و دزدیدن نام کاربری و کلمه عبور کاربر).



جاسوسی

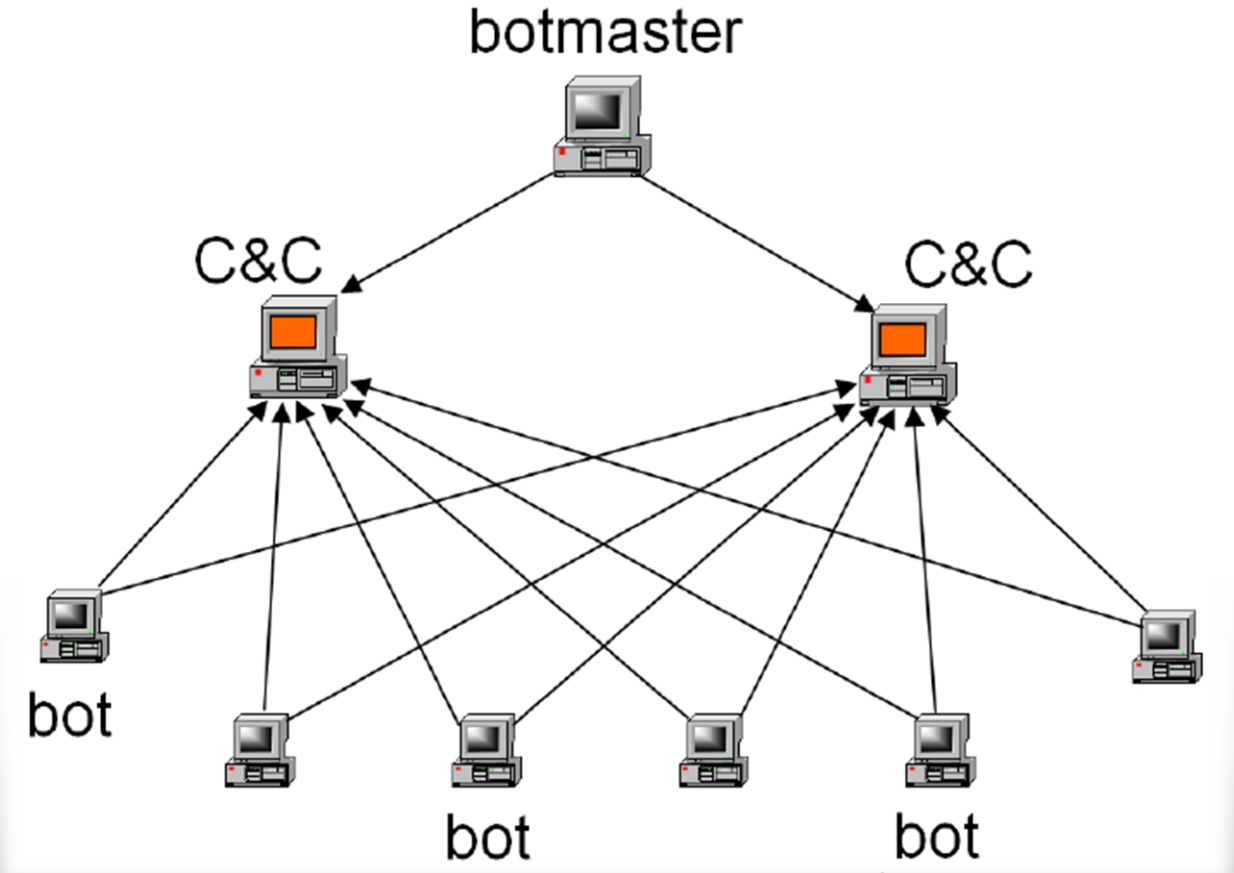
- جاسوسی (Spyware): به طور کلی به نرم افزارهایی که قصد زیر نظر قرار دادن کاربر را دارند و به جمع آوری اطلاعات شخصی وی می‌پردازند گفته می‌شود.
- این اطلاعات شامل صفحاتی است که کاربر آن‌ها را مشاهده کرده است، ایمیل‌هایی که ارسال کرده است، شماره کارت اعتباری، جمع آوری اطلاعات صفحه کلید و غیره.
- عموماً Spyware از طریق دانلود نرم افزارهای رایگان یا آزمایشی (Trial) وارد می‌شود.

Adware

- Adware (Advertising-supported Software): این بدافزار به دانلود، پخش و نمایش تبلیغات به طور خودکار می‌پردازد.
- این بدافزار نیز می‌تواند درون نرم افزارهای رایگان قرار گیرد و وارد کامپیوتر شود.

بات‌نت

- بات‌نت (Botnet): شبکه ای از کامپیوترهای آلوده که تحت کنترل یک مرکز فرماندهی (Bot Master) هستند.



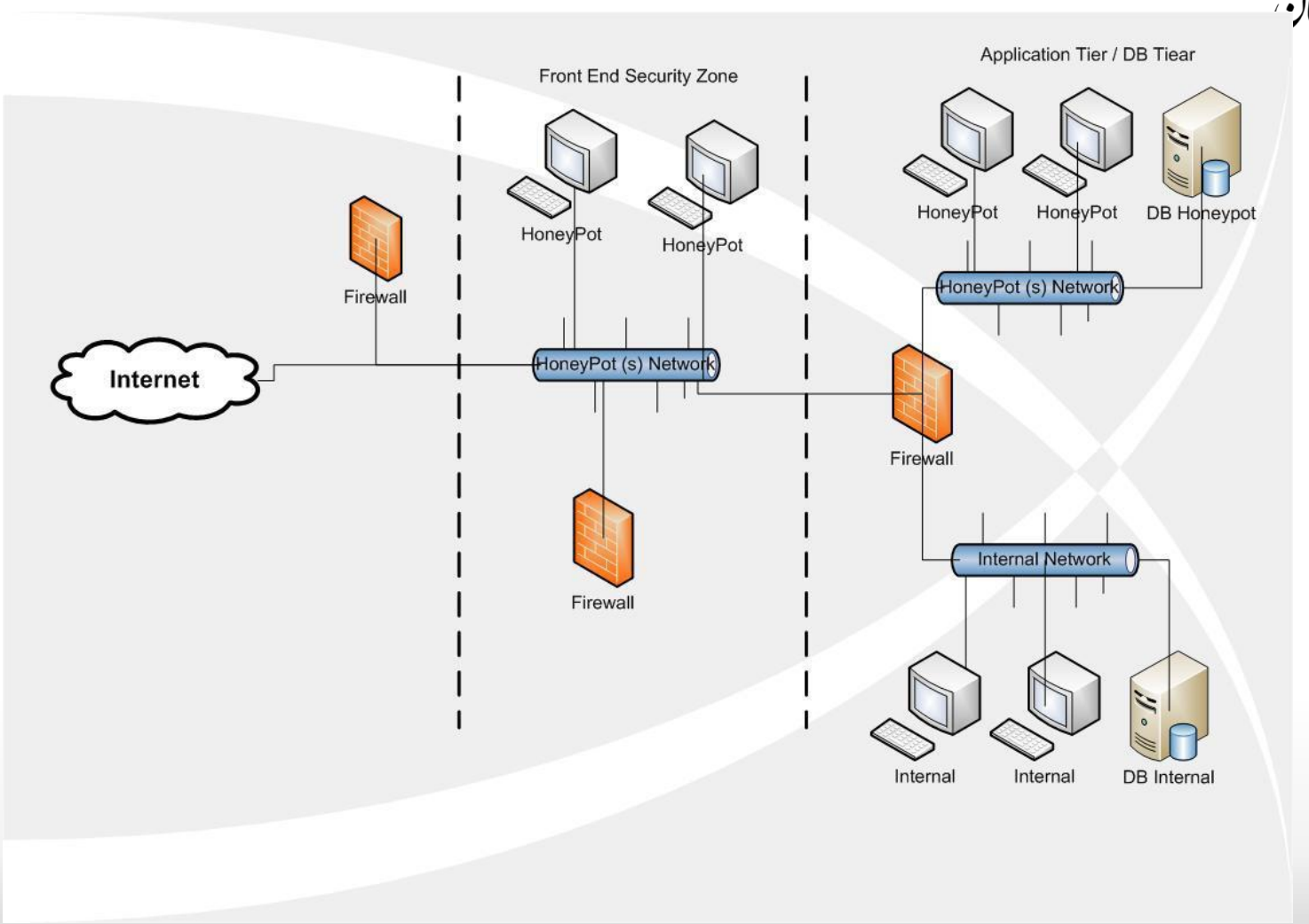
تشخیص – سیستم ضدبدافزار

- **ارائه نسخه‌های 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.

تشخیص – سیستم تله عسل



مکانیزم‌های ترمیم

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

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

منابع

- اسلایدهای دکتر مرتضی امینی (منبع اصلی) – درس امنیت داده و شبکه
- Ann McIver McHoes, Ida M. Flynn, Understanding Operating Systems, 6th and 7th edition
- Idika, Nwokedi, and Aditya P. Mathur. "A survey of malware detection techniques." Purdue University 48 (2007).