دانشگاه آزاد اسلامی واحد تبریز

نام درس: سیستم مدیریت امنیت اطلاعات

بخش: تشخیص نفوذ

نام استاد: دکتر مسعود کارگر

فهرست مطالب

- انواع نفوذگرها
- تکنیکهای نفوذ
- تشخیص نفوذ
- مدیریت گذرواژه

انواع نفوذگرها

- تهدید : نفوذ ناخواسته یا خصمانه به یک سیستم بصورت غیرمجاز(از طریق شبکه یا بصورت مستقیم)

- انواع نفوذگرها(Intruders)
  - Masquerader : یک کاربر غیر مجاز از یک حساب کاربری مجاز سرقت شده استفاده می کند.
  - Misfeasor:یک کاربر مجاز که از داده ها ،برنامه ها یا منابع غیرمجاز استفاده می کند.
  - Clandestine : یک کاربر مخفی که از ثبت اتفاقات در داخل سیستم(Auditing) طفره می رود.

تکنیک های نفوذ

- دسترسی غیرمجاز یا افزایش اختیارات در داخل یک سیستم.
- در بیشتر موارد به یافتن گذرواژه(password) ختم می شود.
- روشهای نگهداری فایل password کاربران توسط سیستم:
  - رمزگذاری یکطرفه(oneway encryption)
    - کاربر گذرواژه را ارایه می دهد.
    - گذرواژه توسط سیستم رمز می شود(غیر قابل برگشت)
    - با گذرواژه ذخیره شده مقایسه می شود.
  - محدودیت دسترسی(Access Control) : تنها یک یا تعداد محدودی از کاربران به فایل password ها دسترسی دارند.

تکنیک های نفوذ

حدس زدن گذرواژه

- از رایج ترین روشهای نفوذ می باشد.
- نفوذگر شناسه کاربری را می داند.
- تلاش می کند تا گذرواژه را به یکی از روشهای زیر کشف کند:

  - گذرواژه های پیش فرض اختصاص داده شده توسط سیستم
  - آزمایش همه گذرواژه های کوتاه
  - آزمایش لغات دیکشنری
  - آزمایش اطلاعات شخصی کاربران(نام،شماره تلفن،تاریخ تولد،شخصیت ها یا موزیکهای مورد علاقه و یا ترکیبی از آنها)

تکنیک های نفوذ

حدس زدن گذرواژه

- آزمایش های فوق در بیشتر موارد بدون دسترسی به فایل گذرواژه ها ممکن نیست.
- میزان موفقیت نفوذگر به گذرواژه انتخاب شده توسط کاربران بستگی دارد.
- تحقیقات نشان می دهد بسیاری از کاربران گذرواژه های ضعیفی انتخاب می کنند.

تکنیک های نفوذ

دزدیدن گذرواژه (password capture)

- استفاده از اسب تراوا
- کنترل کردن یک login ناامن از طریق شبکه(Email،FTP،telnet)
- دستیابی به اطلاعات ذخیره شده در سیستم پس از یک Login موفق(web history/cache,…)
- نگاه کردن به صفحه کلید هنگام وارد کردن گذرواژه توسط کاربر

تشخیص نفوذ
Intrusion Detection

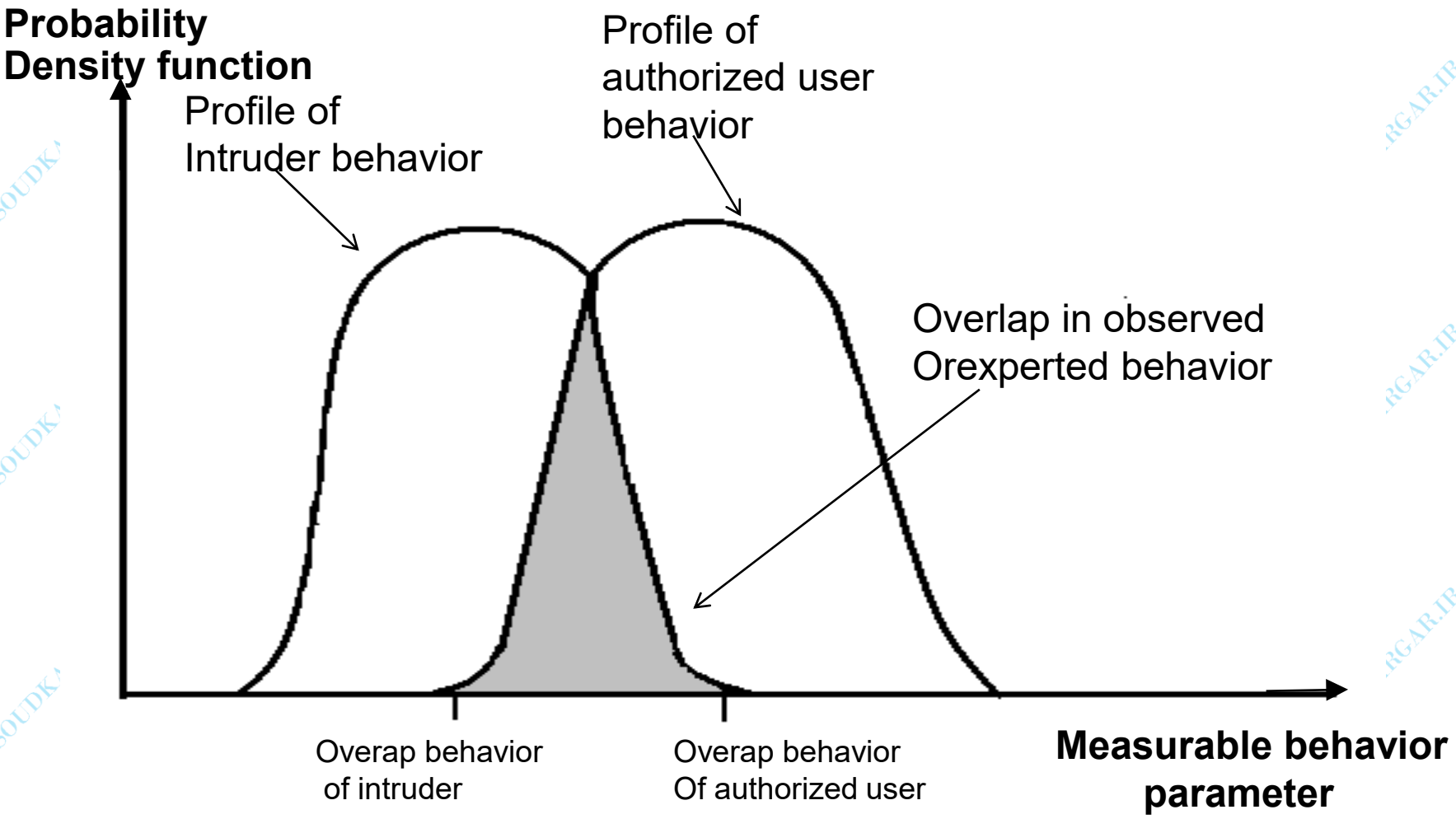
- روشهای جلوگیری از نفوذ(Prevention) صددرصد قابل اطمینان نیستند.
- در کنار آن همیشه به تشخیص نفوذ نیازمندیم :
  - امکان جلوگیری از نفوذ در صورت کشف سریع
  - جمع آوری اطلاعات درباره روشهای نفوذ برای بهبود prevention
  - تشخیص نفوذ در بسیاری وارد می تواند نقش بازدارنده داشته باشد.

تشخیص نفوذ
Intrusion Detection

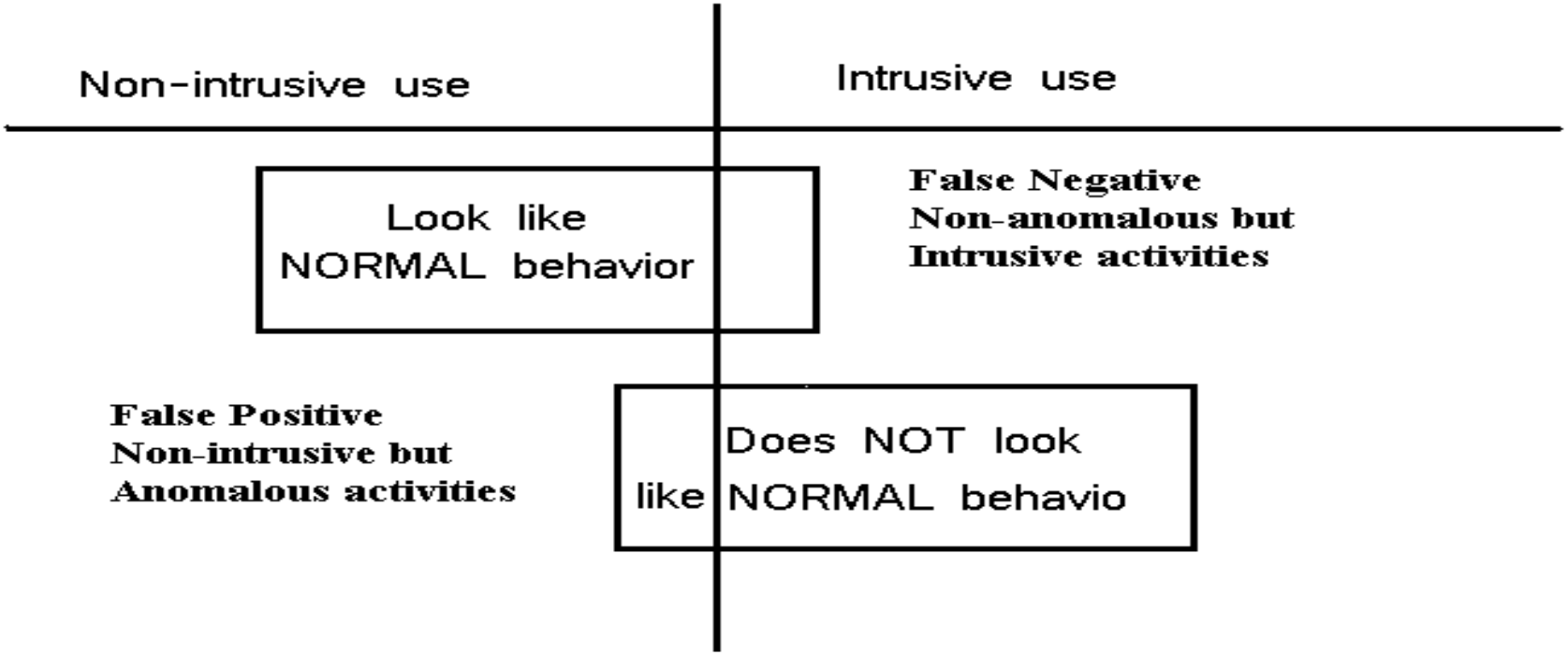
مبتنی بر این فرض می باشند که الگوی رفتاری نفوذکننده با کاربر مجاز متفاوت است.

- اگرچه نمی توان مرز مشخصی بین آنها قایل شد(شکل صفحه بعد...)
- این امر منجر به بروز دو خطای اصلی در این نوع سیستم ها می شود.
- مثبت خطا(False Positive): یک کاربر مجاز،غیر مجاز شناخته می شود.
- منفی خطا(False Negative):یک نفوذگر،مجاز شناخته می شود!

Behavior Profiles



False Positive vs . False Negative



تشخیص نفوذ

روشهای تشخیص نفوذ

- تشخیص آماری آنومالی(statistical anomaly):جمع آوری اطلاعات مربوط به رفتار کاربران مجاز در طول زمان،رفتار کاربران جاری و مقایسه آنها.مبتنی بر:
  - Threshold: تعریف حد آستانه(مستقل از کاربران) برای میزان رخداد اتفاقات(events) متفاوت
  - Profile: ثبت فعالیتهای کاربران در داخل profile آنها و تشخیص تغییرات
- تشخیص مبتنی بر قواعد(rule-based): تعریف قوانین مشخص کننده رفتار نفوذگران

تشخیص نفوذ

روشهای تشخیص نفوذ – مقایسه

- روشهای آماری تشخیص آنرمالی توانایی تشخیص کاربران
- غیر مجاز(Masqueraderها) را دارند،ولی برای تشخیص کاربران مجاز خاطی(Misfeasorها) مناسب نیستند.
- روشهای تشخیص مبتنی بر قانون ممکن است بتوانند حمله های فوق را تشخیص دهند.
- در مجموع،یک سیستم تشخیص نفوذ کامل ممکن است از ترکیب هر دو مکانیسم فوق استفاده کند.

تشخیص نفوذ

رکوردهای بازرسی(Audit Records)

- یک ابزار پایه برای تشخیص نفوذ
- گزارش ثبت شده از فعالیتهای در حال انجام در سیستم را در بر میگیرند.
- در واقع ورودر سیستم های تشخیص نفوذ محسوب می شوند.

تشخیص نفوذ

دو مکانیسم برای تولید آنها وجود دارد:

- رکوردهای بازرسی بومی(native): بخشی از کلیه OSهای چند کاربره عمومی محسوب می شود.
  - مزیت: عدم نیاز به نرم افزار ثبت رکورد جداگانه
  - ضعف: ممکن است همه اطلاعات مورد نیاز امنیتی را شامل نشوند.

- رکوردهای بازرسی ویژه تشخیص نفوذ(detection-specific) : برای جمع آوری اطلاعات خاص امنیتی ایجاد شده اند.
  - مزیت: امکان ایجاد بسته های نرم افزاری مستقل از سیستم عامل خاص
  - ضعف: ایجاد سربار ناشی از اجرای دو بسته بازرسی روی یک ماشین

تشخیص نفوذ

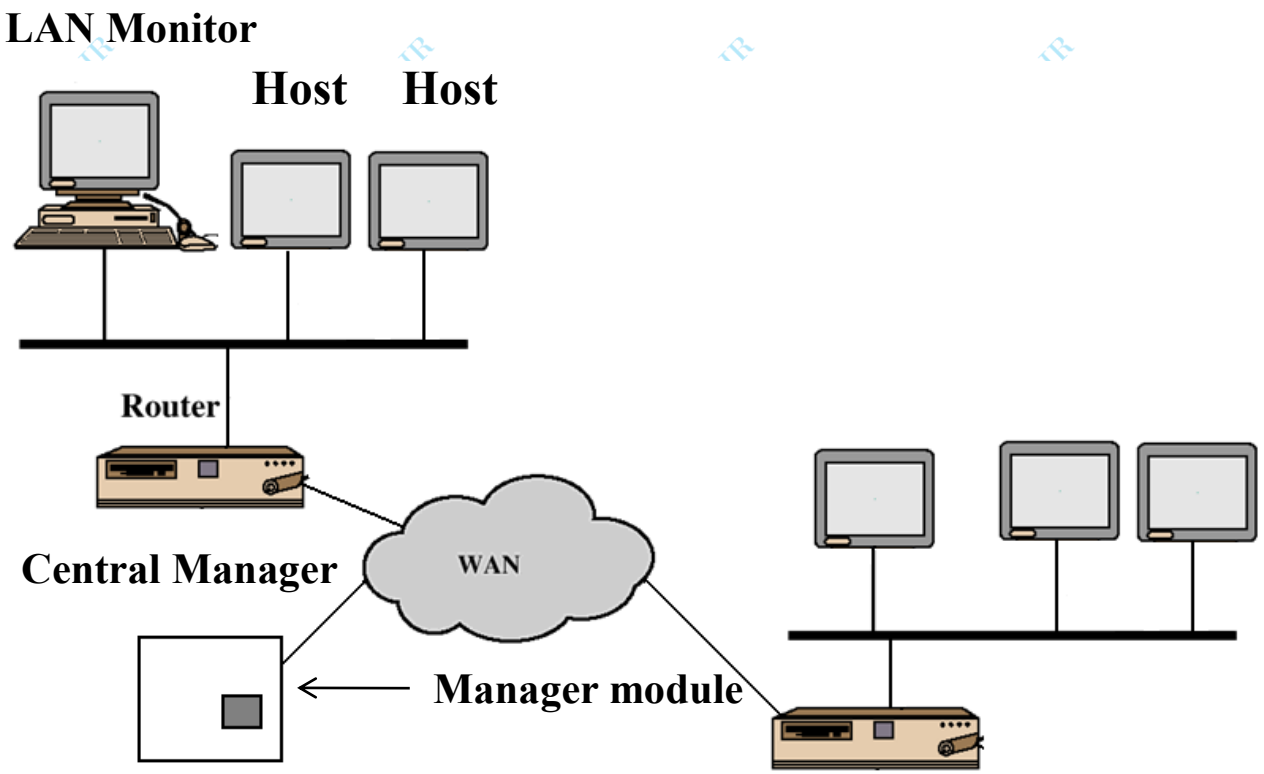
- تشخیص نفوذ توزیع شده
  - بصورت سنتی تاکید روی سیستمهای stand-alone بوده است
  - تشخیص نفوذ از طریق شبکه ها باید در نظر گرفته شود.
  - یک سیستم تشخیص نفوذ توزیع شده با مسایل زیر مواجه است
    - سروکار داشتن با فرمت های متفاوت رکوردها روی hostهای مختلف
    - انتقال رکوردها در شبکه و حفظ تمامیت و محرمانگی داده های ردوبدل شده
    - استفاده از معماری متمرکز یا غیر متمرکز

تشخیص نفوذ

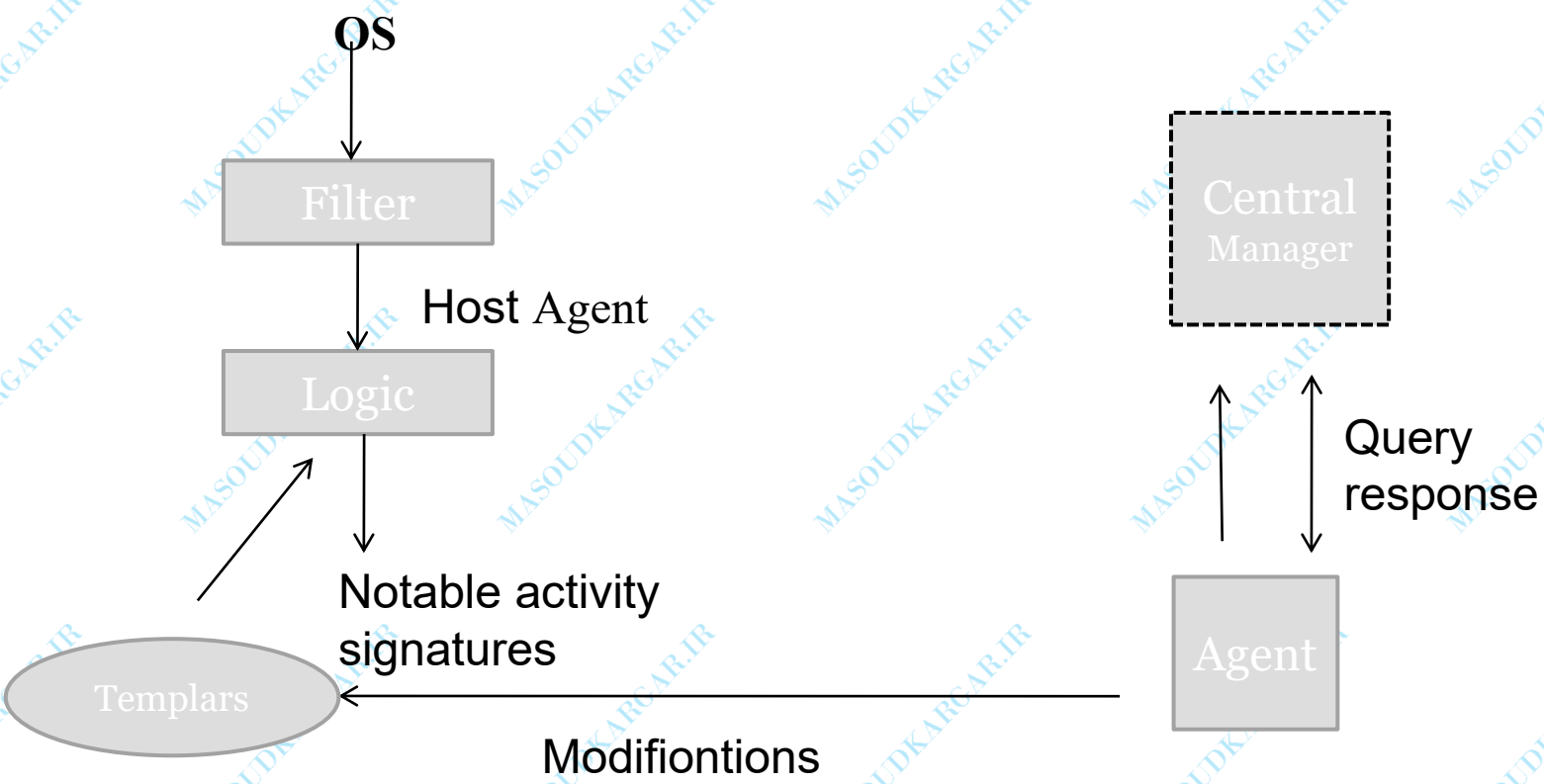
یک سیستم نمونه توزیع شده از اجزای زیر تشکیل شده است

- عامل میزبان(Host Agent): وظیفه جمع آوری و ارسال رکوردهای بازرسی برای مدیر مرکزی را بر عهده دارد.
- عامل کنترل LAN: وظیفه کنترل ترافیک بین میزبان ها در LAN و ارسال آنها به مدیر مرکزی
- مدیر مرکزی: اطلاعات فوق را دریافت می کند و نفوذ را تشخیص می‌دهد.

Distributed Intrusion Detection-Architecture



Distributed Intrusion Detection -Agent Implementation



مدیریت گذر واژه

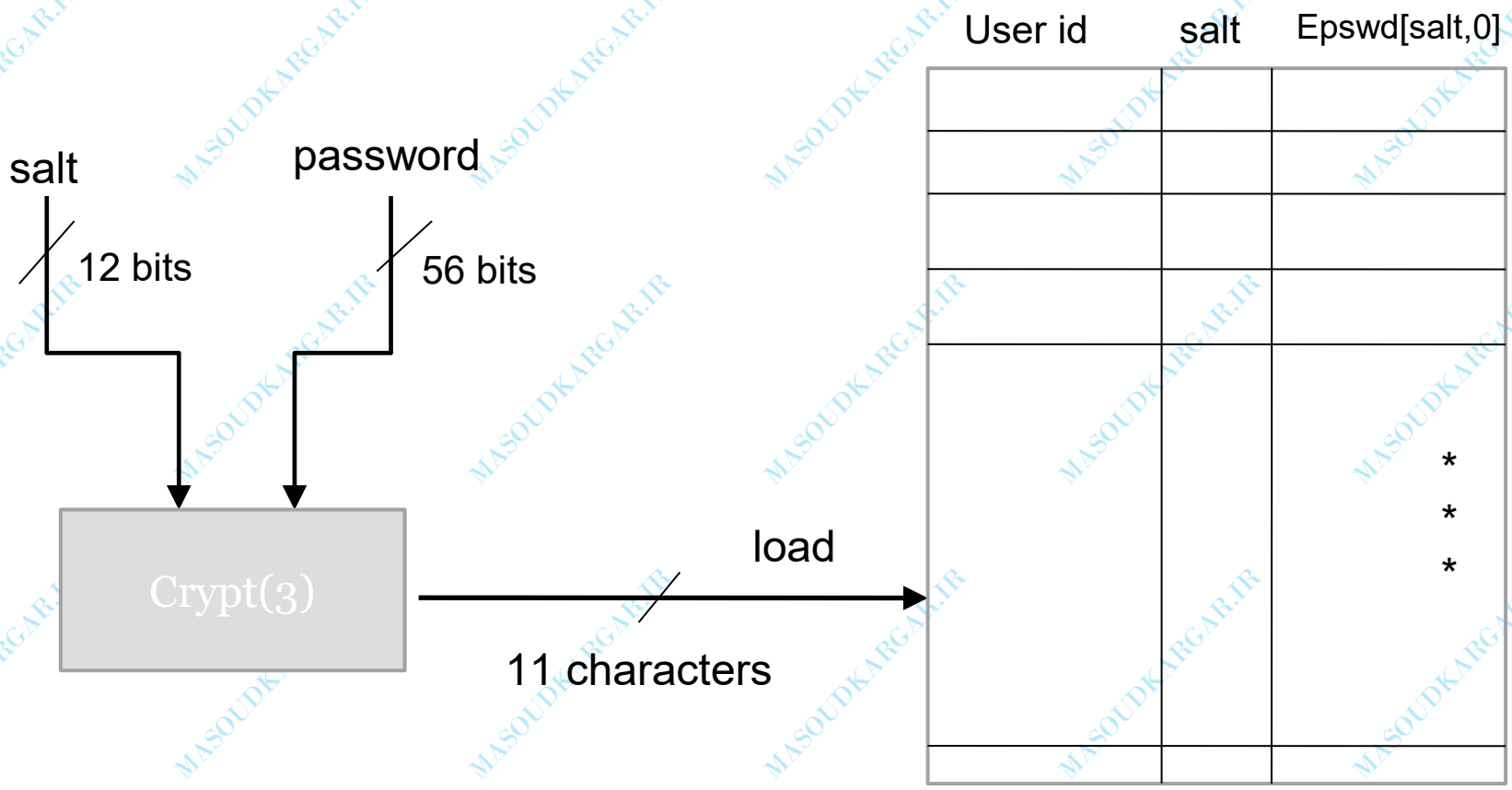
- تهدیدات متداول گذرواژه

  - کاربران گذرواژه های پیش فرض را عوض نمی کنند.
  - گذرواژه های کوتاه
  - لغات دیکشنری
  - نوشتن گذرواژه ها روی کاغذ یا روی یک فایل(بدون رمزنگاری)
  - استفاده از مشخصات فردی و علایق شخصی
  - استفاده از یک اسب تروا برای سرقت گذرواژه
  - ....

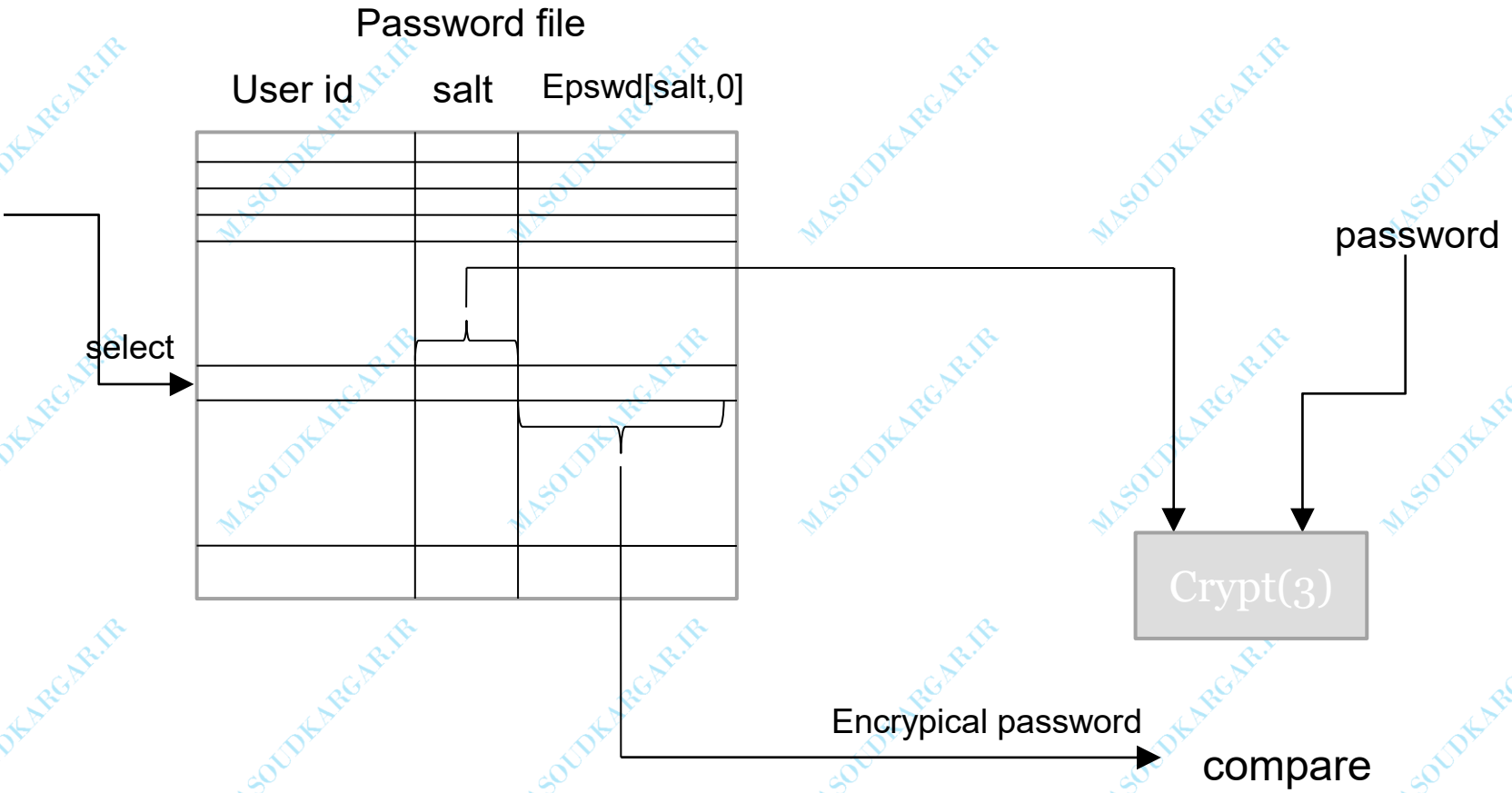
مدیریت گذر واژه

- Password اولین خط دفاعی در مقابل نفوذ کننده می باشد.
- شناسه کاربر بیانگر حقوق دسترسی کاربر و گذرواژه نشان دهنده هویت کاربر می باشد.
- گذر واژه معمولا بصورت رمزشده نگهداری می شوند.
- Unix از الگوریتم DES تغییر داده شده استفاده می کند(مطابق شکل صفحه بعد)
- بعضی از سیستم های جدید از توابع درهم استفاده می کنند.

Loading a new Password



Verifying a Password



مدیریت گذر واژه

- کارکرد Salt

  - با اضافه شدن Salt گذرواژه های تکراری به مقادیر رمز شده متفاوتی در فایل گذر واژه تبدیل می شوند.
  - فضای جستجو گذرواژه را افزایش می دهد.
  - استفاده از نسخه های پیاده سازی شده سخت افزاری DES برای تشخیص گذرواژه را غیرممکن می کند.

مدیریت گذر واژه

- نیاز به اتخاذ سیاست مناسب و آموزش کاربران دارد.
- اطمینان از اینکه هر شناسه یک گذرواژه پیش فرض دارد.
- اطمینان از اینکه کاربران گذرواژه های پیش فرض را تغییر می دهند.
- فایل گذرواژه ها از دسترس عموم دور نگه داشته شود
- ملزم نمودن کاربران به انتخاب گذرواژه های مناسب

  - رعایت حداقل طول گذرواژه(<۶)
  - انتخاب ترکیبی از اعداد،حروف کوچک و بزرگ و نیز علایم نشانه گذاری.
  - عدم استفاده از لغات شناخته شده دیکشنری

مدیریت گذر واژه

استراتژی های انتخاب گذرواژه

1. آموزش کاربران
   - در محیطهای با حجم کاربران زیاد کارساز نیست
2. انتخاب گذرواژه توسط سیستم
   - از نظر مقبولیت کاربری مشکل دارد.
3. چک کردن گذرواژه ها بصورت واکنشی(reactive):اجرای ابزارهای تشخیص گذرواژه های نامناسب بصورت دوره ای
   - یک ابزار کامل و مطمئن وقت زیادی ازCPU را اشغال می کند.

مدیریت گذر واژه

استراتژی های انتخاب گذرواژه(ادامه...)

۴. چک کردن گذرواژه ها در زمان انتخاب (proactive):به کاربر اجازه انتخاب گذرواژه را می دهد،ولی باید توسط سیستم تایید شود:

- اعمال قوانین ساده انتخاب گذرواژه
- نگهداری یک دیکشنری از گذرواژه های نامناسب و چک کردن گذرواژه به هنگام انتخاب
- استفاده از روشهای الگوریتمی (مانند مدل مارکوف) برای تشخیص انتخاب های نامناسب