یا ذالامن والامان

نفوذگرها و نرم‌افزارهای مخرب

Intruders and Malicious Softwares

توسط: حمید رضا شهریاری

http://ceit.aut.ac.ir/~shahriari

فهرست مطالب

- انواع نفوذگرها
- تکنیکهای نفوذ
- تشخیص نفوذ
- مدیریت گذرواژه
- نرم افزارهای مخرب
- روشهای مقابله با ویروس

تهدیدها

- دو تهدید عمده سیستم های کامپیوتری

  - **نفوذگران (Intruders/Hackers/Crackers)**
  - **ویروسها**

نفوذگرها

- انواع نفوذگرها مطابق تقسیم بندی **Anderson** ۱۹۸۰
  - Masquerader : یک کاربر غیرمجاز که 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 یا از اختیارات خود سوءاستفاده می کند.
  - Clandestine user : یک کاربر که گذرواژه مدیر سیستم را دزدیده و از ثبت رویدادها در داخل سیستم(Auditing) جلوگیری می کند.

تکنیکهای نفوذ

- **تکنیکهای نفوذ**
  - دسترسی غیرمجاز یا افزایش اختیارات در داخل یک سیستم.
  - در بیشتر موارد به یافتن گذرواژه(password)ختم می شود
- **روشهای حفاظت از فایل password کاربران توسط سیستم:**
  - رمزگذاری یکطرفه(one-way encryption)
    - کاربر گذرواژه را ارائه می دهد
    - گذرواژه توسط سیستم رمز می شود(غیرقابل 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

تکنیکهای 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 موردعلاقه و یا ترکیبی از آنها)

تکنیکهای 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

تکنیکهای نفوذ

دزدیدن گذرواژه(password capture)

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

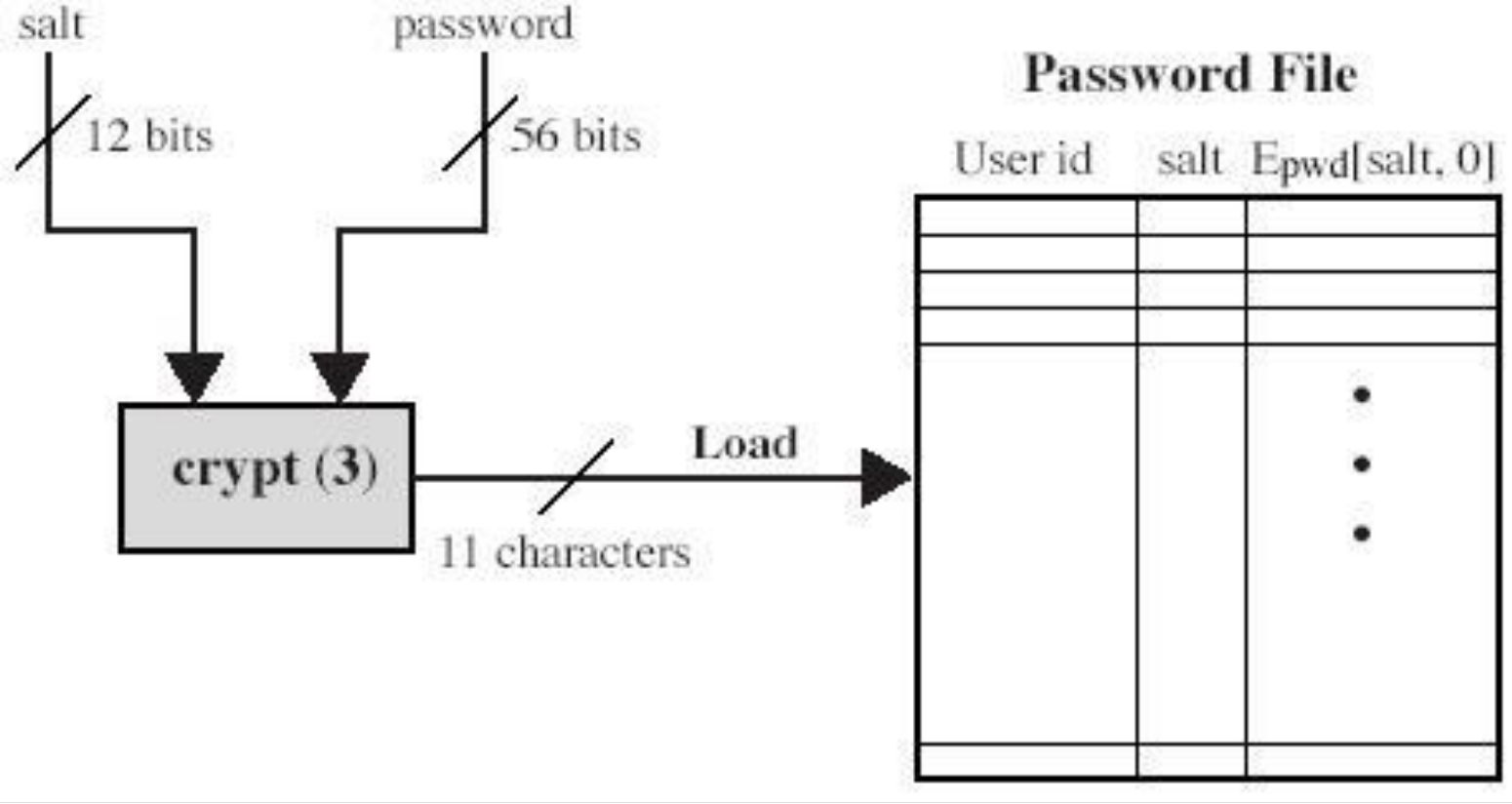
مدیریت گذرواژه

- تهدیدهای 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 علائق شخصی
  - استفاده از یک اسب تروا برای سرقت گذرواژه
  - ...

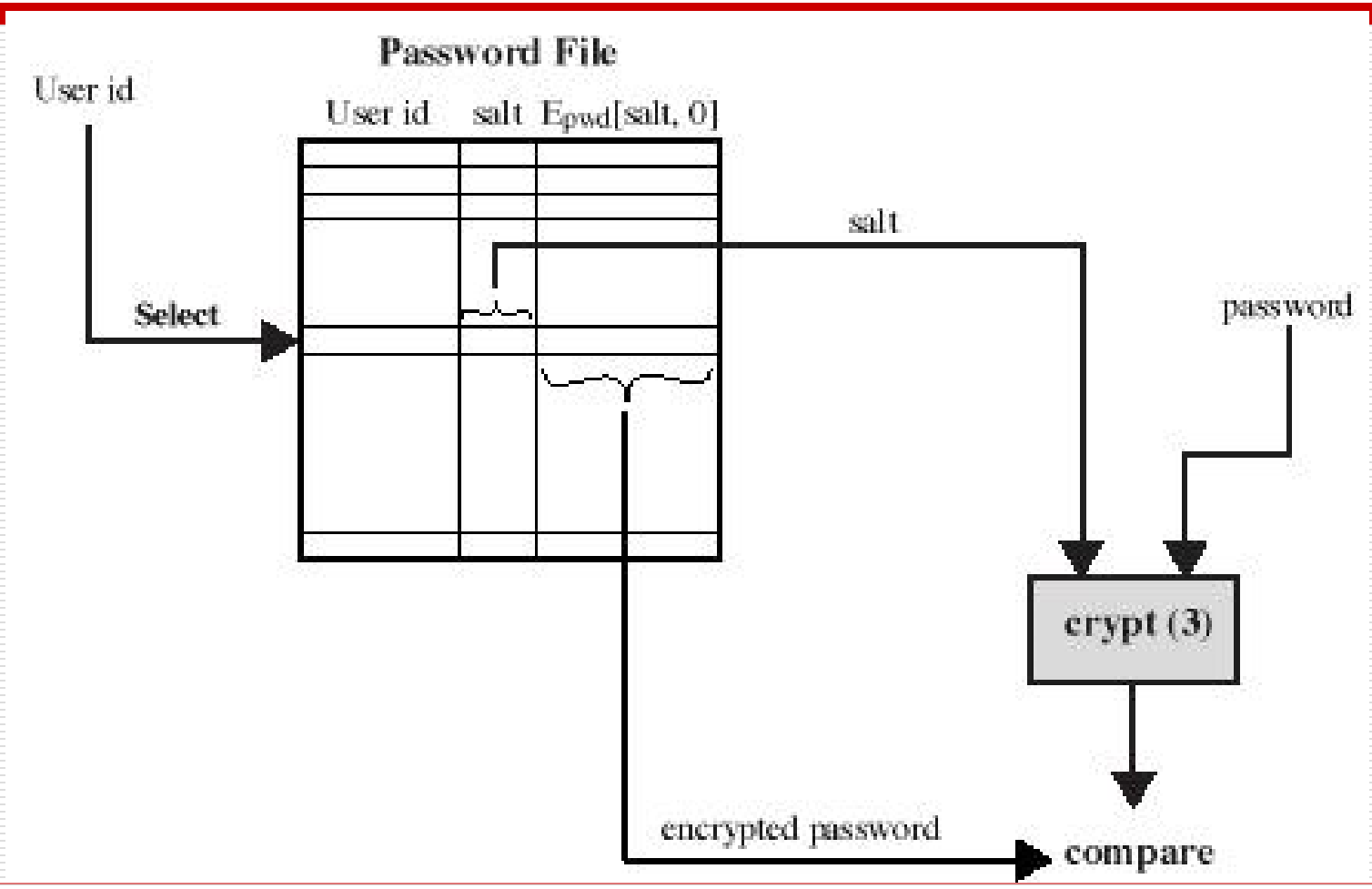
مدیریت گذرواژه

- Password اولین خط دفاعی در مقابل نفوذکننده می باشد
- شناسه کاربر بیانگر حقوق دسترسی کاربر و گذرواژه نشان دهنده هویت صحیح کاربر می باشد.
- گذرواژه ها معمولا بصورت رمزشده نگهداری می شوند
- Unix از الگوریتم DES تغییر داده شده استفاده می کند(مطابق شکل صفحه بعد)
- بعضی از سیستمهای جدید از توابع درهم مانند MD5 استفاده می کنند.

Loading a new Password



Verifying a Password



مدیریت گذرواژه

- کارکرد Salt
  - با اضافه شدن Salt گذرواژه های تکراری به مقادیر رمزشده متفاوتی در فایل گذرواژه ها تبدیل می شوند.
  - فضای جستجوی گذارواژه ها را افزاریش می دهد.
  - استفاده از نسخه های پیاده سازی شده سخت افزاری DES برای تشخیص گذرواژه را غیرممکن می کند.

مدیریت گذرواژه

- 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 نگهداشته شود
- ملزم نمودن کاربران به انتخاب گذرواژه های مناسب
  - رعایت حداقل طول گذارواژه(> ٦)
  - انتخاب ترکیبی از اعداد، حروف کوچک و بزرگ و نیز علائم نشانه گذاری.
  - عدم استفاده از لغات شناخته شده دیکشنری

مدیریت گذرواژه

استراتژیهای انتخاب گذرواژه

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

مدیریت گذرواژه

استراتژیهای انتخاب گذرواژه(ادامه...)

٤. چک کردن گذارواژه 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

Spafford (Bloom Filter)

- فیلتر از مرتبه **k** دارای **k** تابع درهم سازی $H_1(x),\ldots,H_k(x)$ است. که هر تابع گذرواژه را به یک عدد نگاشت می دهد.

$$H_i(X_i) = y \quad 1 \le i \le k; \quad 1 \le j \le D; \quad 0 \le y \le N-1$$

$$X_i = jth\,word\ in\ password\ dictionary$$

$$D = number\ of\ word\ in\ password\ dictionary$$

Spafford (Bloom Filter)

- سپس رویه زیر به دیکشنری اعمال می شود:
  - جدولی **N** بیتی در نظر گرفته می شود (مقدار اولیه همه صفر)
  - برای یک گذرواژه مقادیر درهم سازی آن محاسبه شده و بیتهای متناظر آن در جدول **1** می شوند
  - هنگامی که کاربر گذرواژه ای انتخاب می کند، مقادیر درهم سازی آن محاسبه شده و بیتهای متناظر آنها در جدول بررسی می شوند. اگر همه مقادیر **1** بودند، گذرواژه پذیرفته نمی شود.

تشخیص نفوذ(Intrusion Detection)

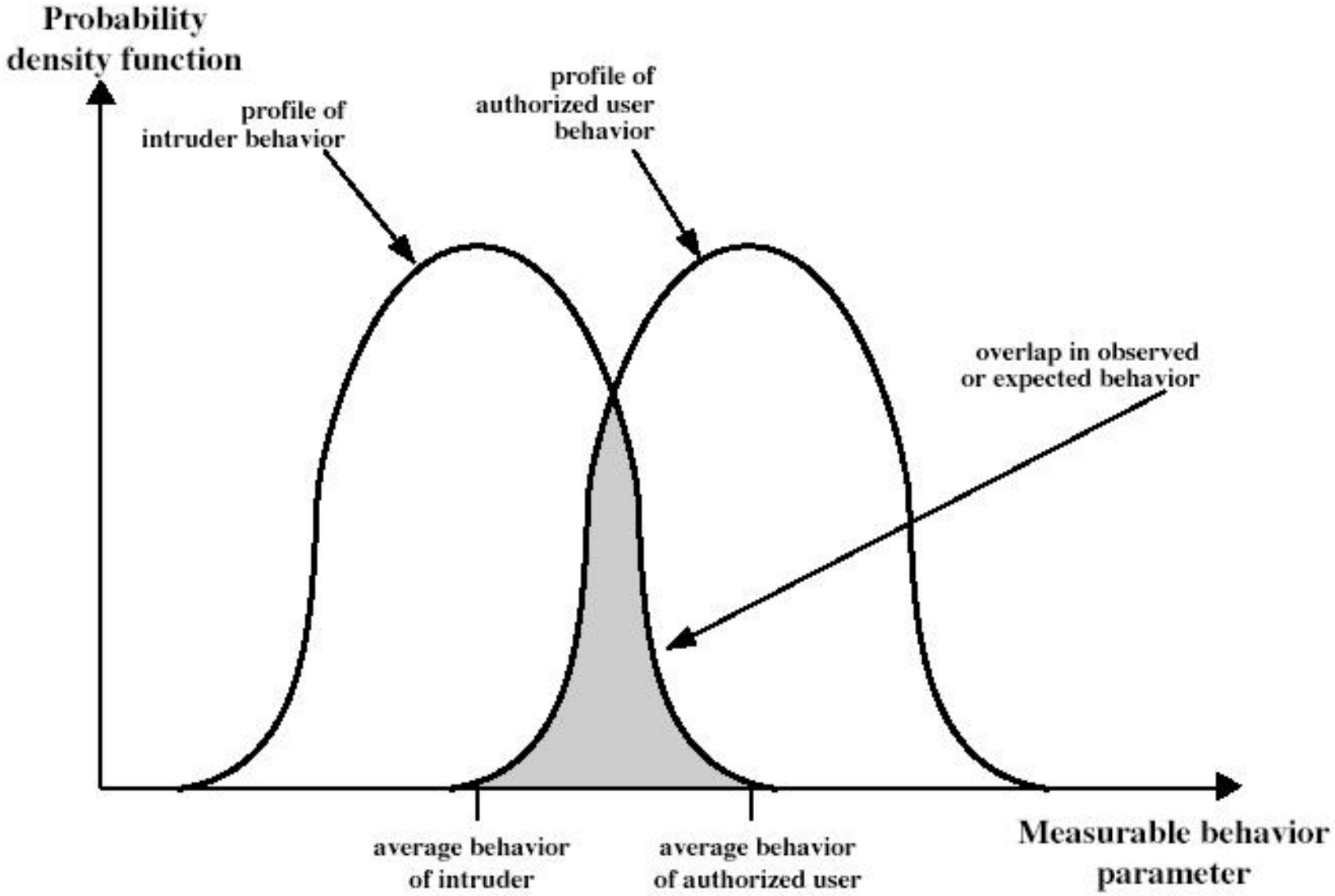
- روشهای بازدارنده (prevention) صددرصد قابل اطمینان نیستند
- در کنار آن همیشه به تشخیص نفوذ نیازمندیم:
  - امکان جلوگیری از نفوذ در صورت کشف سریع
  - جمع آوری اطلاعات درباره روشهای نفوذ برای بهبود prevention
  - تشخیص نفوذ در بسیاری موارد می تواند نقش بازدارنده داشته باشد

تشخیص نفوذ
(Intrusion Detection)

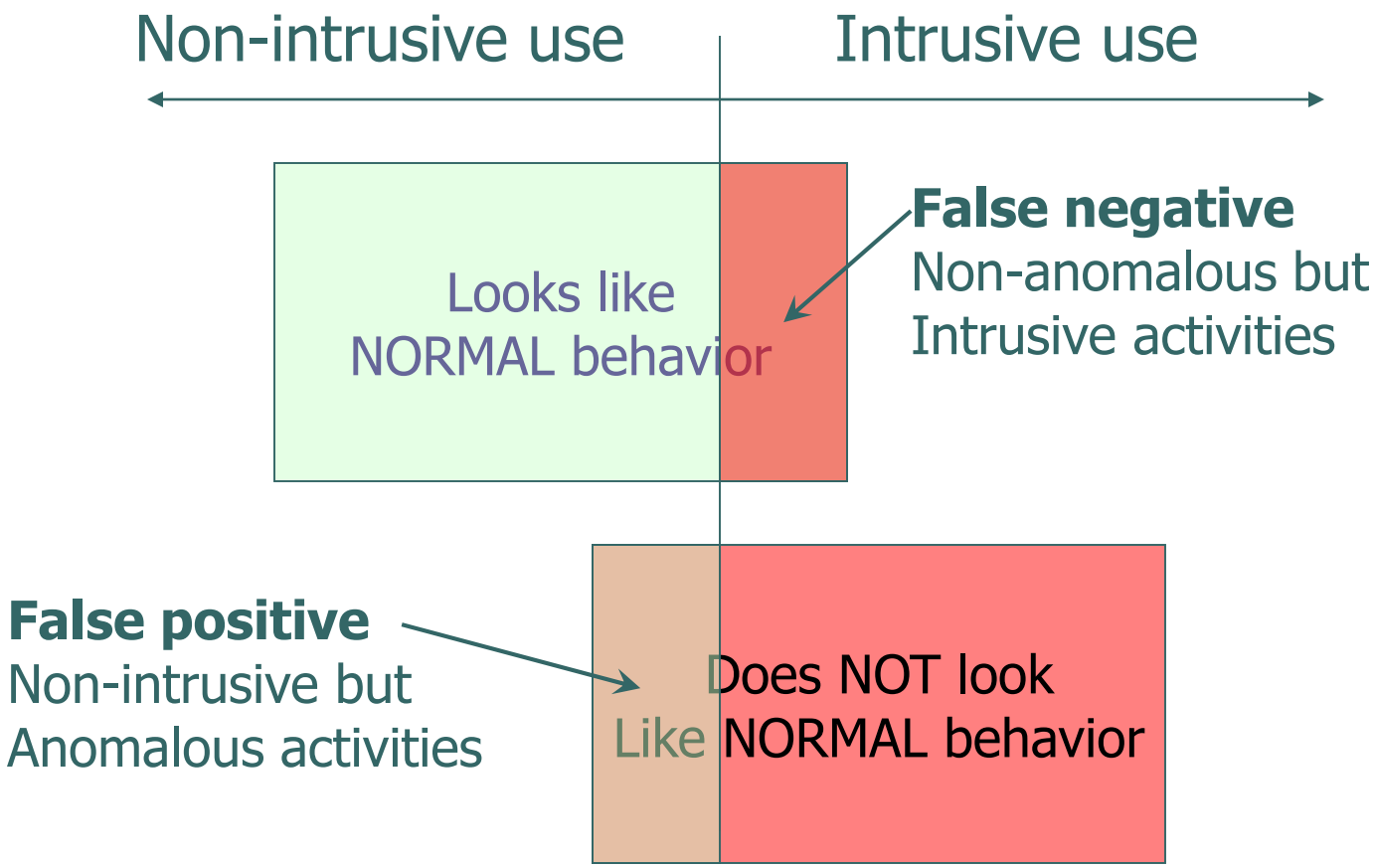
مبتنی بر این فرض می باشند که الگوی رفتاری نفوذکننده با کاربر مجاز متفاوت است

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

Behavior Profiles



False Positive vs. False Negative



تشخیص نفوذ

روشهای تشخیص نفوذ

- تشخیص آماری ناهنجاری(statistical anomaly): جمع آوری اطلاعات مربوط به رفتار کاربران مجاز در طول زمان، مشاهده 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 ناهنجاری توانایی تشخیص کاربران غیرمجاز(Masqueraderها) را دارند، ولی برای تشخیص کاربران مجاز خاطی(Misfeasorها) مناسب نیستند.
- روشهای تشخیص مبتنی بر قاعده 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 برمی گیرند.
- در واقع ورودی سیستم های تشخیص نفوذ محسوب می شوند.

تشخیص نفوذ

دو مکانیسم برای تولید آنها وجود دارد:

- رکوردهای بازرسی بومی(native): بخشی از کلیه OS های چندکاربره عمومی محسوب می شود
  - مزیت : عدم نیاز به نرم افزار ثبت رکورد جداگانه
  - ضعف : ممکن است همه اطلاعات موردنیاز امنیتی را شامل نشوند

- رکورد های 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

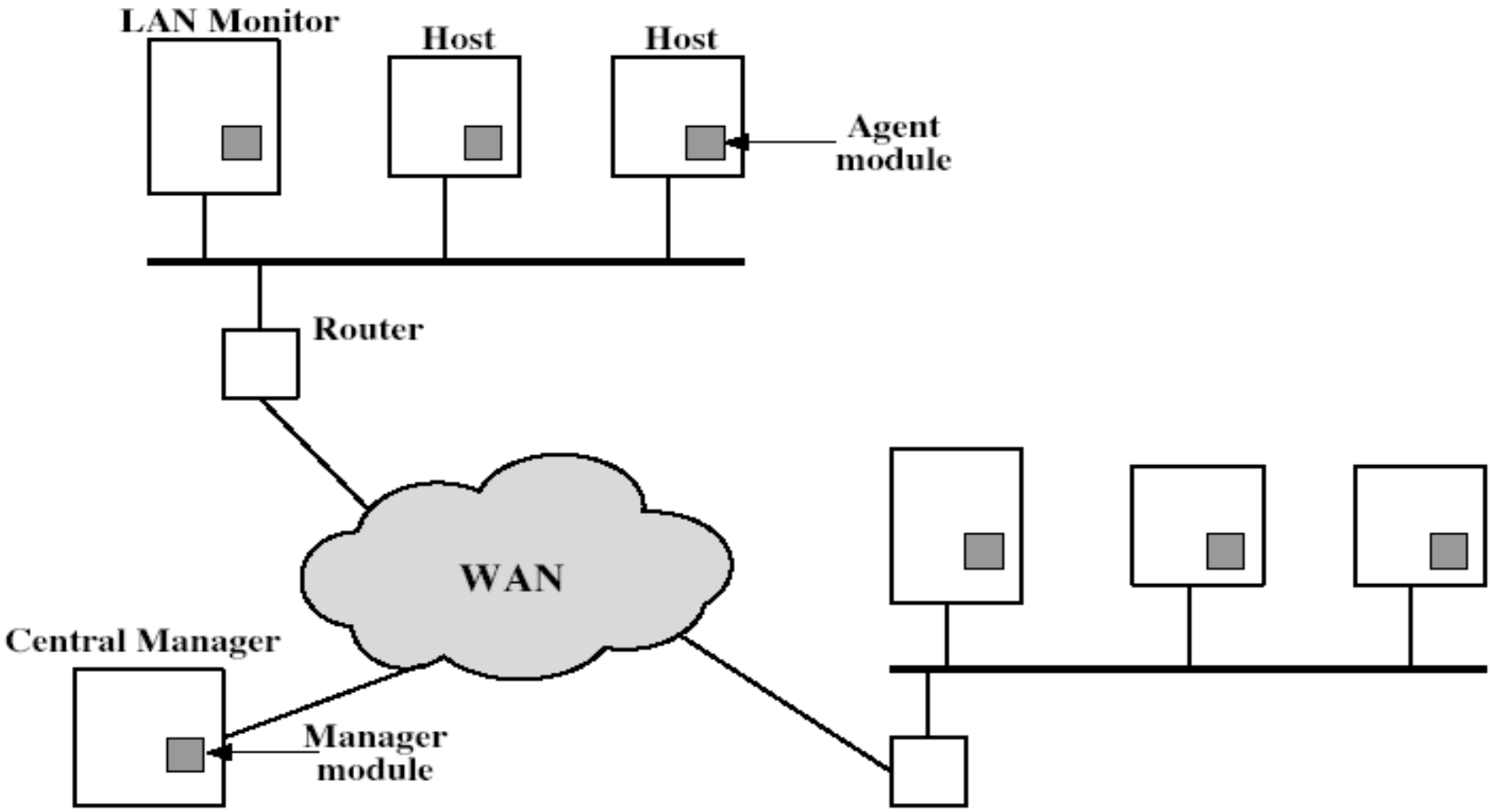
- تشخیص نفوذ توزیع شده
  - بصورت سنتی تاکید روی سیستمهای stand-alone بوده است
  - تشخیص نفوذ از طریق شبکه ها باید درنظر گرفته شود.
  - یک سیستم تشخیص نفوذ توزیع شده با مسائل زیر مواجه است
    - سروکار داشتن با فرمت های متفاوت رکوردها روی hostهای مختلف
    - انتقال رکوردها در شبکه و حفظ تمامیت و محرمانگی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

تشخیص نفوذ

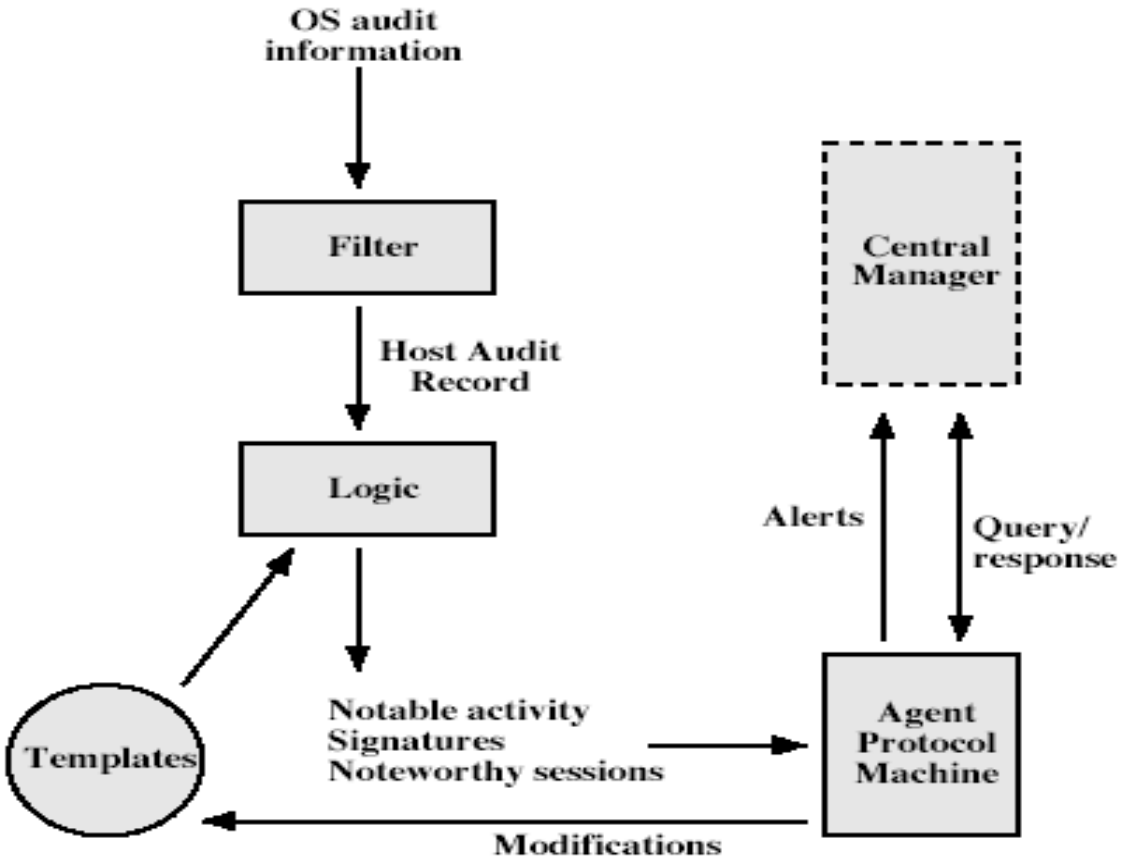
یک سیستم نمونه توزیع شده از اجزای زیر تشکیل شده است

- 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 میزبانها در LAN و ارسال آنها به مدیر مرکزی
- مدیر مرکزی : اطلاعات فوق را دریافت می کند و نفوذ را تشخیص می دهد.

Distributed Intrusion Detection - Architecture



Distributed Intrusion Detection – Agent Implementation



نرم افزارهای مخرب

نرم افزارهای مخرب

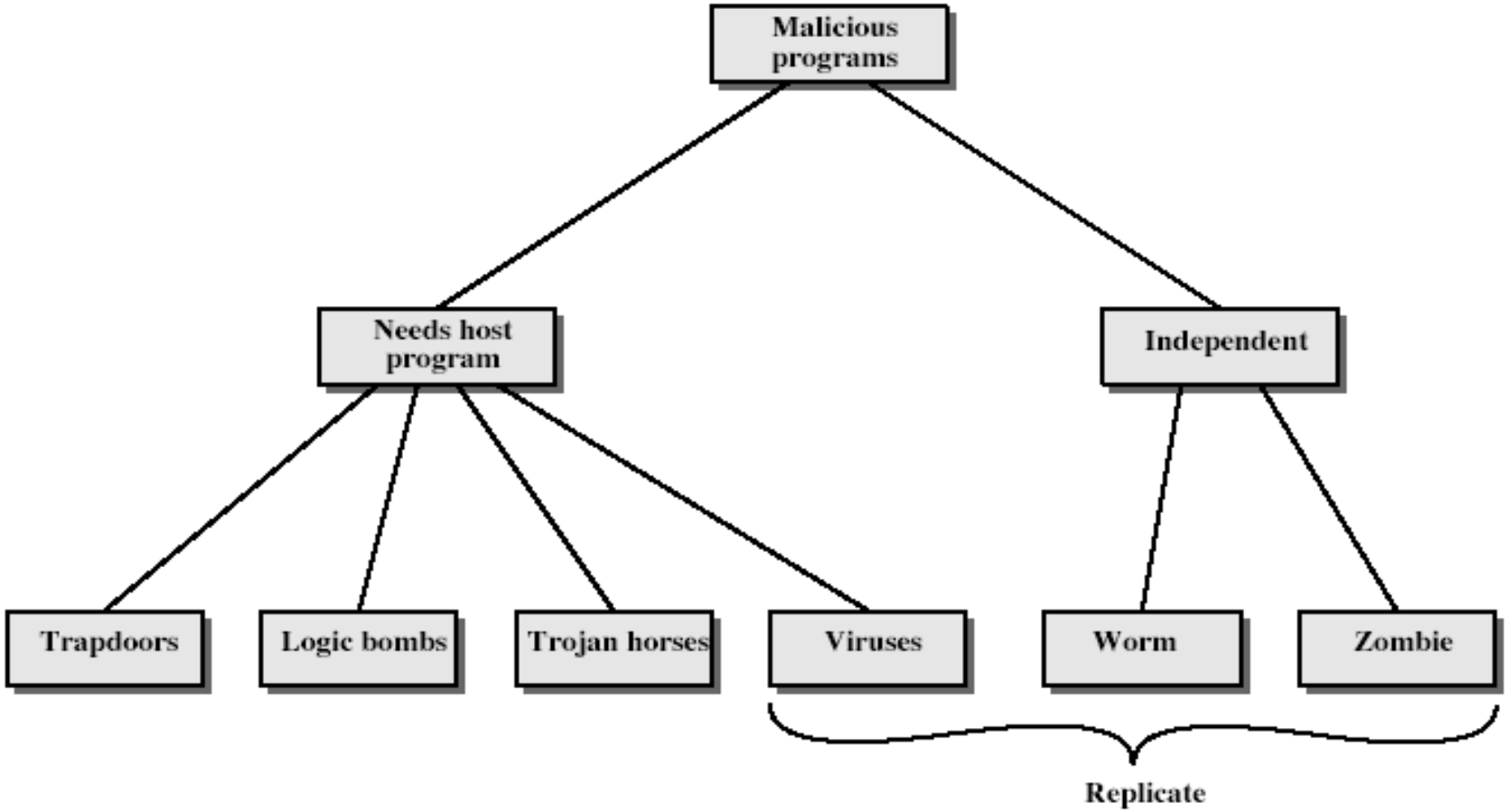
دسته بندی ۱ (بر اساس نیاز به برنامه های میزبان)

- آنهایی که برای اجرا به یک برنامه میزبان احتیاج دارند
- آنهایی که مستقلا اجرا می شوند

دسته بندی ۲ (بر اساس انتشار)

- نرم افزارهایی که منتشر نمی شوند
- نرم افزارهایی که یک کپی از خود را به برنامه ها یا سیستم های دیگر منتقل می کنند.

Malicious Software



نرم افزارهای مخرب

Trapdoors

- نوعی مدخل ورودی پنهانی در برنامه ها محسوب می شود
- عمدتا توسط تولیدکنندگان نرم افزار ایجاد شده اند(در هنگام تست و خطایابی)
- به اشخاص مطلع اجازه می دهد که روالهای امنیتی معمول را دور بزنند
- در صورت برطرف نشدن در محصول نهایی، نوعی خطر محسوب می شوند
- سد کردن آن از طریق OS بسیار مشکل می باشد

نرم افزارهای مخرب

Logic Bomb

- یکی از قدیمی ترین انواع نرم افزارهای مخرب محسوب می شود
- عبارت است از یک قطعه کد پنهانی در داخل یک برنامه مجاز
- این قطعه کد به شرط خاصی فعال می شود:
  - وجود یا عدم وجود فایل خاصی
  - در تاریخ/ساعت مشخص
  - کاربر خاص
- با فعال شدن معمولا عملیات تخریبی انجام می گیرد
  - تغییر یا حذف فایل(ها)

نرم افزارهای مخرب

Trojan Horse

- عبارت است از یک برنامه با اثرات جانبی مخفی
- در ظاهر برنامه جذاب و مفیدی به نظر می رسد
  - مثلا بازی یا نسخه بهبود یک نرم افزار
- در صورت اجرا یک سری اعمال اضافی را انجام می دهد
  - مثلا به نفوذگر اجازه دسترسی غیرمجاز به منبعی را می دهد
- اکثرا برای انتشار ویروس یا کرم و یا ایجاد یک backdoor بکار می رود

نرم افزارهای مخرب

Bacteria

- کاری بجز تکثیر خود به صورت نمایی انجام نمی دهد.
- ولی همین کار می تواند منجر به درگیر شدن همه منابع سیستم(پردازنده، حافظه و فضای دیسک سخت) تا سرحد مرگ شود!

نرم افزارهای مخرب

Viruses

- عبارت است از یک قطعه کد که توانایی تکثیر خود را داشته و به برنامه دیگری الحاق می شود
  - دستورات لازم برای تکثیر خود را به همراه دارد!
- در صورت آلوده شدن سیستم، یک نسخه مشابه ویروس اصلی به برنامه هایی که هنوز آلوده نشده اند، اضافه می شود.
- محیط شبکه محیط بسیار مناسبی برای انتشار ویروسها فراهم کرده است
  - گرچه انتشار آن وابسته به شبکه نیست

نرم افزارهای مخرب

فازهای عملکرد ویروسها

- غیرفعال(dormant) : در انتظار یک رخداد(event) بسرمی برد
- انتشار(propagation) : تولید یک کپی مشابه و آلوده کردن دیسکها/برنامه ها
- فعال شدن(triggering) : همزمان با رخداد یک event فعال می شود.
- اجرا(Execution) : اجرای کد مخرب ویروس

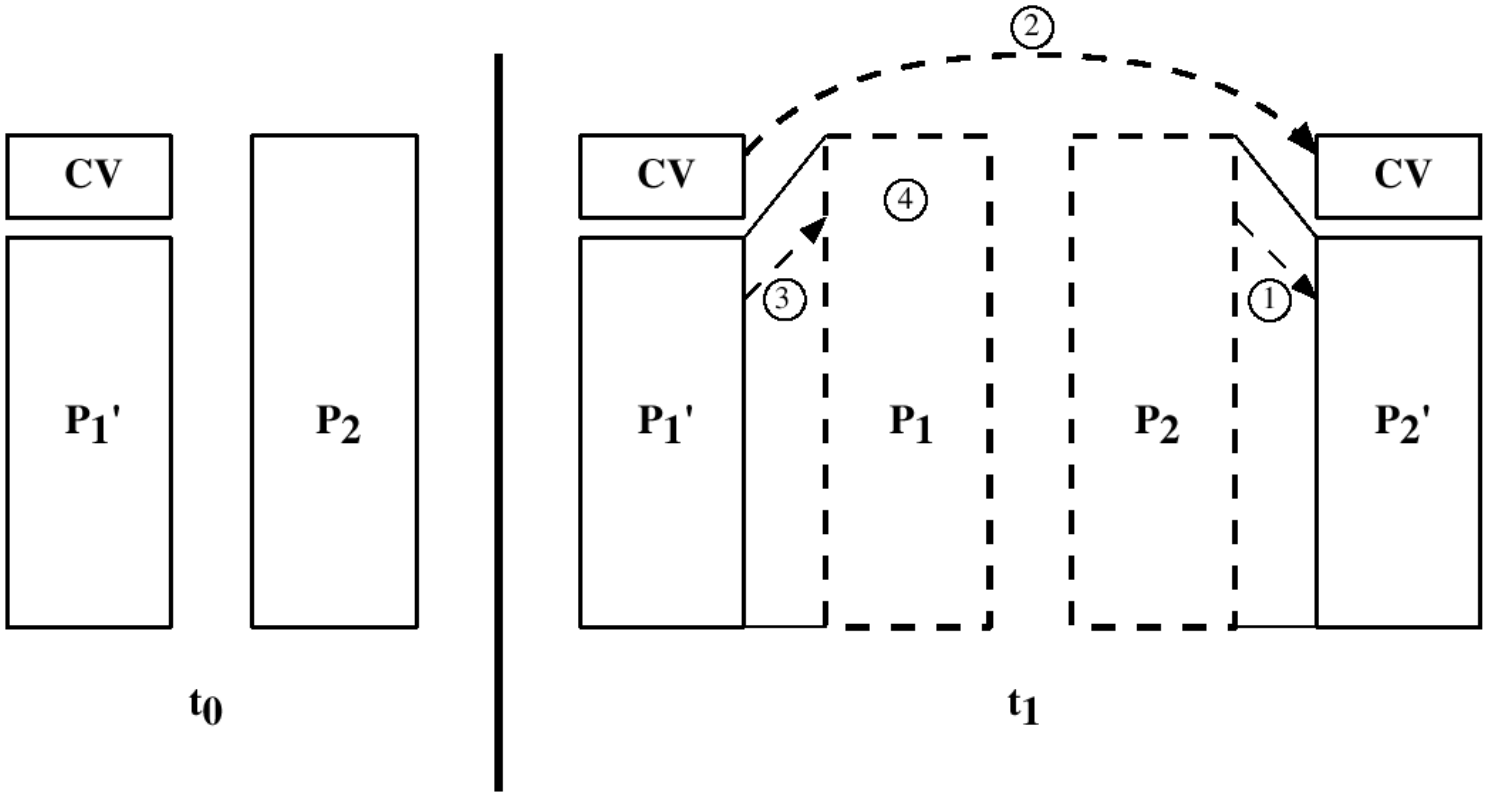
Virus Structure

```
        program V :=

{goto main;
        1234567;

            subroutine infect-executable :=
                {loop:
                file := get-random-executable-file;
                if (first-line-of-file = 1234567)
                        then goto loop
                        else prepend V to file; }

            subroutine do-damage :=
                {whatever damage is to be done}

            subroutine trigger-pulled :=
                {return true if some condition holds}

main:       main-program :=
                {infect-executable;
                if trigger-pulled then do-damage;
                goto next;}

next:

}
```

نرم افزارهای مخرب

- اگر حجم فایل آلوده شده از فایل اصلی بیشتر باشد، ویروس به سادگی قابل تشخیص است.
- باید به طریقی حجم فایل آلوده شده را بدون تغییر نگه داشت.
- به همین دلیل، ابتدا فایل فشرده شده و سپس کد ویروس به آن اضاف می شود.

ویروس فشرده شده : انتشار و اجرا



نرم افزارهای مخرب

انواع ویروسها(بر اساس روش حمله)

- انگلها(parasitic) : به یک فایل اجرایی دیگر متصل شده و در هنگام اجرای فایل آلوده شده، تکثیر می شوند
- مقیم حافظه(memory resident): در حافظه اصلی قرار گرفته و برنامه هایی که اجرا می شوند را آلوده می کنند
- سکتور راه اندازی(boot sector): سکتور بوت را آلوده کرده و به هنگام راه اندازی سیستم با دیسکت آلوده تکثیر می شوند

نرم افزارهای مخرب

انواع ویروسها(بر اساس روش حمله) ادامه ...

- پنهان(stealth) : بویژه برای مخفی شدن از دید ابزارهای تشخیص ویروس طراحی شده اند
- چند شکلی(polymorphic) : تکثیر نسخه های متفاوت به هنگام انتشار
  - این ویژگی تشخیص آنها بر اساس امضاء(signature) ویروس را مشکل می سازد.

نرم افزارهای مخرب

- **ویروس ماکرو(Macro Virus)**
  - عبارت است از یک ماکروی قابل اجرا که به یک فایل داده می چسبد(عموما به یک سند Word یا Excel)
  - کد ماکرو با رخداد event خاصی فعال می شود.
  - مستقل از سکو هستند(platform independent)
  - چون فایلهای داده ای را آلوده می کنند، تشخیص آنها مشکل تر است
  - تکثیر آنها آسان است(عموما از طریق Email)

نرم افزارهای مخرب

- **کرمها(Worms)**
  - تکثیر می شوند ولی برنامه های دیگر را آلوده نمی کنند
  - از طریق شبکه منتشر می شوند
    - کرم اینترنتی Morris در سال ۱۹۸۸ منجر به ایجاد CERT گردید!
  - پس از فعال شدن می توانند نقش ویروس را بازی کنند و یا یک اسب تراوا در داخل سیستم آلوده ایجاد کنند

نرم افزارهای مخرب

- کرم **Morris**
  - یکی از کرمهای مشهور قدیمی می باشد
  - در سال ۱۹۸۸ توسط Robert Morris انتشار یافت
  - سیستم عامل های Unix را مورد هدف قرار می داد
  - روشهای انتشار
    - دستیابی به فایل گذرواژه
    - استفاده از درب پشتی در کارگزار sendmail
  - در صورتی که حمله موفقیت آمیز باشد، خودش را تکثیر می کند

نرم افزارهای مخرب

- **Code Red**
  - از حفره موجود در MS IIS برای نفوذ و انتشار استفاده می کند
  - IP های تصادفی را امتحان می کند تا سیستمهایی را که IIS روی آنها در حال اجراست، پیدا کند.
  - باعث حمله عدم دسترسی(DoS) می شود.
  - موج دوم حمله توسط این کرم بیش از ۳۶۰۰۰۰ کارگزار را در ۱۴ ساعت آلوده کرد.
  - نسخه دوم این ویروس، Code Red 2، یک اسب تروجان روی دستگاه قربانی نصب می کند.

نرم افزارهای مخرب

- **Nimda**
  - یک کرم اینترنتی است که از مکانیسمهای مختلف برای انتشار استفاده می کند
    - انتشار از طریق پست الکترونیکی
    - اشتراک فایل ها روی شبکه
    - IIS ی که وصله های امنیتی روی آن اعمال نشده اند.
    - درب پشتی ایجاد شده توسط Code Red 2

نرم افزارهای مخرب

- **فاز عملکرد کرمها مشابه ویروسهاست**
  - Dormant
  - Propagation:
    - جستجو برای یافتن یک سیستم آلوده نشده
    - ایجاد ارتباط با سیستم جدید
    - تکثیر یک نسخه از خود روی سیستم جدید
  - Triggering
  - Execution

روشهای مقابله با ویروس

- **جلوگیری(Prevention) : جلوگیری از آلودگی سیستم به ویروس**
  - در عمل غیرممکن است
- **تشخیص(Detection) : تشخیص آلودگی و مکان آن**
- **شناسایی(Identification): مشخص کردن نوع ویروس**
- **از بین بردن(Removal): از بین بردن ویروس و بازگرداندن همه برنامه های آلوده شده به حالت اولیه**

روشهای مقابله با ویروس

نرم افزارهای ضدویروس

- نسل اول : پویشگر(scanner)های ساده
  - جستجوی امضاء ویروس یا تغییر طول فایل آلوده شده
- نسل دوم : پویشگرهای اکتشافی
  - تنها به امضاء ویروسها اکتفا نمی کردند
  - به دنبال الگوی قطعه کدهای آلوده کننده می گشتند.

روشهای مقابله با ویروس

نرم افزارهای ضدویروس(ادامه ...)

- نسل سوم : نظارت رفتاری(activity traps)
  - جستجوی ویروسها بر اساس فعالیت آنها
  - در حافظه مقیم می شوند و بعضی از الگوهای رفتاری رایج ویروسها را چک می کنند(مانند پویش فایلها)
- نسل چهارم : حفاظت ترکیبی
  - ترکیبی از مولفه های پوینده و نظارت رفتاری

روشهای مقابله با ویروس

رمزگشایی هوشمند(Generic Decryption)

- مبتنی براین واقعیت است که ویروسهای polymorphic برای انتشار باید رمزگشایی شوند
- فایلهای اجرایی از طریق پوینده GD اجرا می شوند
  - شبیه ساز CPU : کامپیوتر مجازی مبتنی بر نرم افزار
  - پوینده امضاء ویروس : کد اجرایی را برای یافتن امضاهای شناخته شده ویروسها جستجو می کند
  - ماجول کنترلی شبیه ساز : اجرای کد را کنترل می کند
- کد در حال اجرا آسیبی به سیستم نمی رساند
- بسیاری از آنتی ویروسها از این مکانیسم استفاده می کنند.

روشهای مقابله با ویروس

سیستم ایمنی دیجیتال(Digital Immune System)

- یک سیستم متمرکز برای تشخیص امضاء ویروسها و اعمال نسخه ضدویروس
- تشخیص ویروس توسط برنامه مانیتور در هر PC و ارسال آن برای ماشین Administration
- رمزنگاری نمونه و ارسال آن برای ماشین آنالیز
- اجرای کد در محیط شبیه سازی، جستجوی اثر ویروس و تجویز راهکار تشخیص و مبارزه با ویروس
- بازگشت نسخه به ماشین Administration
- ارسال نسخه به همه ماشینهای آلوده
- همه کاربران و ثبت نام کنندگان در این سیستم نسخه جدید را دریافت می کنند

جهت مطالعه بیشتر

- Denning, P. *Computers Under Attack: Intruders, Worms, and Viruses.* Addison-Wesley, 1990
- CERT Coordination Center (WEB Site)
- AntiVirus Online (IBM’s site)

یا ذالامن والامان

پایان

؟