ЗАШТИТА ПОДАТАКА

ЗАШТИТА СИСТЕМА

Злонамеран софтвер

Преглед

- Биће објашњено:
  - Злонамеран софтвер
  - Вируси
  - Црви
  - Заштита од вируса

Вируси

- Најсофистицираније врста напада на рачунарске системе.
- Програми који искоришћавају слабе тачке система.
- Добили доста публицитета током година.
- Помињу се у вестима, новинама, чак и у филмовима научне фантастике (често се преувеличавају).

Злонамерни програми

- вирус - закачи се за неки програм и пропагира копије самог себе другим програмима
- црв (worm) - програм који пропагира своје копије другим рачунарима
- логичка бомба - окида неку акцију, када се испуне одређени услови
- тројански коњ - програм који садржи неочекиване додатне функционалности
- задња врата (backdoor, trapdoor) - модификација програма која дозвољава неауторизовани приступ некој функционалности

Злонамерни програми (2)

- експлоататори (exploits) - код који се концентрише на једну слабу тачку система
- downloaders - програм који инсталира додатне ставке на машину која је нападнута
- спамери - програми који шаљу огромне количине електронских порука
- зомбији - програм који се активира на погођеној машини и који напада друге машине
- Деле се на оне којима је потребан програм домаћин (вируси, задња врата, логичке бомбе) и на оне који су самоодрживи (црв, зомби).
- Друга подела је на оне који се реплицирају (црв, вирус) и на оне који се не реплицирају (логичка бомба).

Задња врата

- тајна тачка приступа програму
- омогућава онима који знају за њих, заобилажење регуларних сигурносних процедура
- често их користе програмери у току развоја софтвера, ради дебаговања и тестирања програма
- представљају код који препознаје неку секвенцу карактера, и сл.
- постају претња када остану у програму који уђе у продукцију, јер олакшавају посао нападачима
- јако их је тешко блокирати на нивоу оперативног система
- тако да се сигурност у односу на ову претњу мора тражити у добром развоју софтвера

Логичка бомба

- једна од најстаријих врста злонамерног софтвера
- представља код који је уграђен у неки легитиман програм
- активира се када се испуне одређени услови
  - нпр. одсуство/присуство неког фајла
  - одређени дан у недељи
  - одређени датум и време
  - одређени корисник
- када се активира најчешће оштећује систем
  - модификује или брише податке

Тројански коњ

- програм са скривеним бочним ефектима
- обично је на први поглед атрактиван
  - нпр. игра, унапређење неке игре или неког програма, итд.
- када се покрене извршава неке додатне задатке
  - омогућава нападачима да индиректно дођу до приступа који немају директно
- често се користи за пропагацију вируса или црва или за инсталацију задњих врата
- или једноставно за уништавање података

Тројански коњ (2)

- Пример 1: добијање приступа фајловима других корисника у мрежи.
- Пример 2: Тројански коњ који би био тежак за детекцију је програмски преводилац (compiler) који је модификован тако да убацује додатни код у програме док се преводе. Не може бити детектован анализом изворног кода.

Зомби

- програм који у тајности преузима контролу над другим умреженим рачунаром
- затим га користи да индиректно лансира нове нападе на друге рачунаре, са рачунара који је заузео
- често се користи за лансирање DOS напада
- користи познате недостатке у мрежним системима

Вируси

- представљају део самореплицирајућег кода прикаченог за неки други код
  - назив на основу биолошких вируса
- може да ради све што раде и остали програми
- једина разлика је у томе што се закачи за неки програм и ради у тајности када се покрене програм домаћин
- када се једанпут покрене, вирус може да извршава било коју функцију, укључујући и брисање фајлова или програма

Фазе код вируса

- постоје четири фазе кроз које типичан вирус пролази:
  - неактивна фаза (dormant) – вирус је беспослен и чека на неки догађај да би се активирао (немају сви вируси ову фазу)
  - фаза пропагације (propagation) – вирус поставља идентичну копију себе у друге програме или на специфична места на диску
  - фаза окидања (triggering) – активира се вирус да би извршио функционалност за коју је био намењен
  - фаза извршавања (execution) – извршава се функционалност, која може бити безазлена, као што је порука на екрану, или може бити деструктивна, као што је брисање програма и података
- већина вируса извршава своје задатке на начин који је специфичан за ОС, а понекад чак специфичан и за хардвер, тако да су они дизајнирани да искористе детаље и мане конкретних система

Структура вируса

- Заражени програм почиње тако што извршава код вируса.
- Прва линија кода је скок на главни програм вируса.
- Друга линија кода је специјална ознака коју вирус користи да би установио да ли је потенцијални програм-жртва већ био заражен са тим вирусом.
- Када се програм покрене контрола се одмах предаје главном програму вируса.
- Вирус прво тражи незаражене извршне програме и зарази их.
- Затим, вирус извршава неку акцију, која је обично штетна за систем.
- Акција може да се изврши сваки пут када се покрене програм, или може да буде логичка бомба.
- Коначно, вирус предаје контролу оригиналном програму.
- Ако је фаза пропагације разумно дуга, корисник неће приметити разлику између нормалног и зараженог извршавања програма.

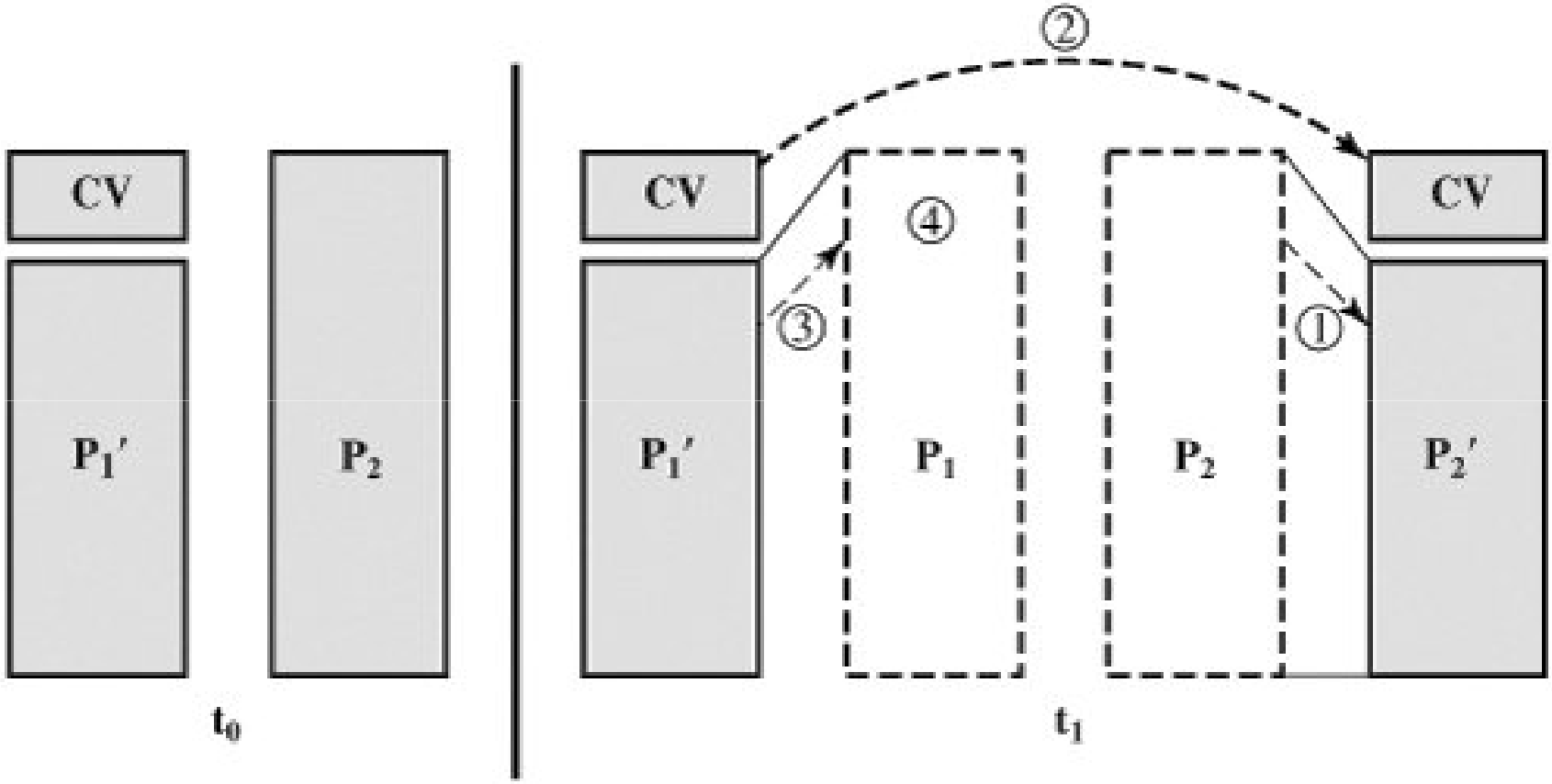
Структура вируса (2)

```
      program V :=

{goto main;
      1234567;

      subroutine infect-executable :=
            {loop:
            file := get-random-executable-file;
            if (second-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:

}
```

Структура вируса (3)

- Претходно описани вирус је лако детектовати, јер је величина зараженог програма већа од величине оригиналног програма.
- Овакви проблеми се могу избећи уколико се заражени програм компресује тако да буде исте величине као оригинални програм.

Структура вируса (4)



- P1, P2 - оригинал; P1', P2' - компресовано; CV- вирус

Иницијална инфекција

- Једном када се вирус нађе у систему у позицији је да зарази друге програме.
- Вирусна инфекција би могла у потпуности бити избегнута уколико вирус уопште не би имао приступ систему.
- Нажалост, превенција је изузетно тешка с обзиром да било који програм који долази ван система може бити заражен вирусом.
- Тако да би једини начин да се избегне могућност заразе вирусом био да се сав софтвер који се користи на неком систему и развија на том истом систему. Ако ово није испоштовано систем је рањив за нападе вируса.

Типови вируса

- паразитски вируси (parasitic virus) - прикачи се за извршни програм и када се програм покрене шаље своје копије на друге извршне програме
- вирус становник меморије (memory-resident virus) - настани се у оперативној меморији као део неког програма који се извршава и одатле напада сваки програм који се извршава
- boot sector вирус - настани boot сектор диска и шири се када се систем подиже
- невидљиви вирус (stealth virus) - дизајниран тако да се сакрије од антивирус програма (предузима одређене радње како би то постигао, нпр. компресија, враћање незаражене верзије програма када се приступа зараженом делу диска, ...)
- полиморфни вирус (polymorphic virus) - мутира након сваке инфекције, па отежава откривање детекцијом потписа вируса (убацује насумичне инструкције, мења редослед инструкција, шифрује део кода сваки пут са различитим кључем,...)
- метаморфни вирус (metamorphic virus) - као и претходни мутира након сваке инфекције, али се пише сваки пут испочетка, па тиме додатно отежава детекцију, а може да мења и своје понашање (користи неколико шаблона понашања)

Макро вируси

- Доминантна група вируса средином 90-их година.
- Макро вируси су опасни из неколико разлога:
  - платформски независан. Практично, сви макро вируси нападају Microsoft Word документе. Сваки систем који подржава Word може бити нападнут.
  - нападају документе, а не извршне програме. Већина информација које рачунар добија су у форми докумената.
  - лако се шире. Чест метод је електронска пошта.
- користе предности офис апликација, а највише макрое.
- макро је извршни програм који је уграђен у неки документ
- користи се да би се аутоматизовале акције које се често понављају
- за макрое се користе основни програмски језици (Basic,...)
- дешинише се секвенца акција која се покреће неким функцијским дугметом или неком комбинацијом дирки тастатуре
- новија издања Word-а пружају заштиту од макро вируса, тако што упозоравају кориснике на фајлове који би могли бити претња.

Email вируси

- у почетку су се ширили кроз додатке у порукама електронске поште
- додаци су садржали макро вирусе, који су се активирали када би корисник отворио додатак и
  - слали исту поруку на све адресе из адресара зараженог
  - чинили штету локално
- затим су се побољшали, па је било довољно само отворити поруку да би вирус заразио машину (почели су да раде са скрипт језицима, које су подржавали агенти електронске поште)
- Овим методом вируси су почели да се шире драстично већим брзинама и морала је да се обезбеди много боља заштита.

Црви

- реплицира се, али не омета програме
- шири се кроз мрежу, потпуно аутоматски и независно од корисника
- када се једном прошири по систему може да се користи да се убаци тројански коњ, да се постави логичка бомба, да се направи зомби за даље нападе
- за репликацију користи неки од мрежних сервиса, нпр:
  - електронску пошту - шаље копије себе другим рачунарима
  - удаљено извршавање - извршава своју копију на удаљеном рачунару
  - удаљено логовање на систем - улогује се као корисник и затим прекопира себе са једног система на други

Фазе код црва

- црв има исте фазе као вирус:
  - неактиван
  - пропагација
    - тражи друге системе које може да зарази
    - успостави везу са циљним удаљеним системом
    - копира сам себе на удаљени систем и покрене копију
  - окидање
  - извршавање
- Тешки су за спречавање

Morris - ов црв

- најпознатији класични црв
- пустио га је на интернет Robert Morris 1998. године
- нападао је Unix системе
- користио је неколико техника пропагације
  - разбијање шифре помоћу локалног фајла са шифрама
  - експлоатисао је *bug* у *finger* протоколу, који даје локацију удаљеног корисника
  - експлоатисао је задња врата у протоколу за слање и пријем порука електронске поште
- ако би било који напад успео, онда се реплицирао

Скорашњи напади црвима

- од 2001 па на овамо почињу да се појављују нове врсте црва
- **Code Red**
  - користи *bug* у Microsoft Internet Information Server (IIS) за продор у систем и ширење
  - испробава различите IP адресе корисника да види да ли је на њима покренут IIS
  - једно време не ради ништа и онда одједном напада неки рачунар са свих осталих
  - други талас је заразио скоро 360 000 сервера за 14 сати
- **Code Red 2**
  - унапређен, са инсталираним задњим вратима, које су омогућавале хакеру да усмерава напад
- **Nimda**
  - користи вишеструке технике упада
    - email, shares, web client, IIS, Code Red 2 backdoor
- **SQL Slammer**
  - 2003.
- **Mydoom**
  - 2004., масовно слање електронском поштом

Заштита од вируса

- напади вируса искоришћавају недостатак контроле интегритета у системима
- да би се одбранили од таквих напада морамо додати такве контроле
- технике које се користе су:
  - **превенција (prevention)** - не дозволити вирусима да уђу у систем (идеално, али немогуће, ипак смањује број успешних напада)
  - **детекција (detection)** - установити инфекцију и лоцирати вирус
  - **идентификација (identification)** - када се детектује вирус, потребно га је идентификовати
  - **уклањање (removal)** - када се идентификује, вирус треба уклонити из свих заражених програма и вратити их у оригинално стање
- ако детекција успе, али не и идентификација и уклањање, онда је решење обрисати такав програм и поновно инсталирати незаражену верзију

Генерације антивирус софтвера

- **прва генерација (simple scanners)**
  - скенери који користе потпис вируса да идентификују вирус
  - или користе промену у величини програма
  - могу детектовати само познате вирусе
- **друга генерација (heuristic scanners)**
  - користе хеуристике да уоче инфекције вирусима (нпр. почетак петље за енкрипцију у полиморфним вирусима)
  - или користе вредности за проверу интегритета оригиналног програма (checksum) да уоче промене (за вирусе који измене и checksum, може се користити шифрована хеш вредност)
- **трећа генерација (activity traps)**
  - програми који се налазе у оперативној меморији и идентификују вирусе према њиховим акцијама
- **четврта генерација (full-featured protection)**
  - пакети са различитим техникама антивирус програма
  - нпр. скенирање и праћење активности, контроле приступа

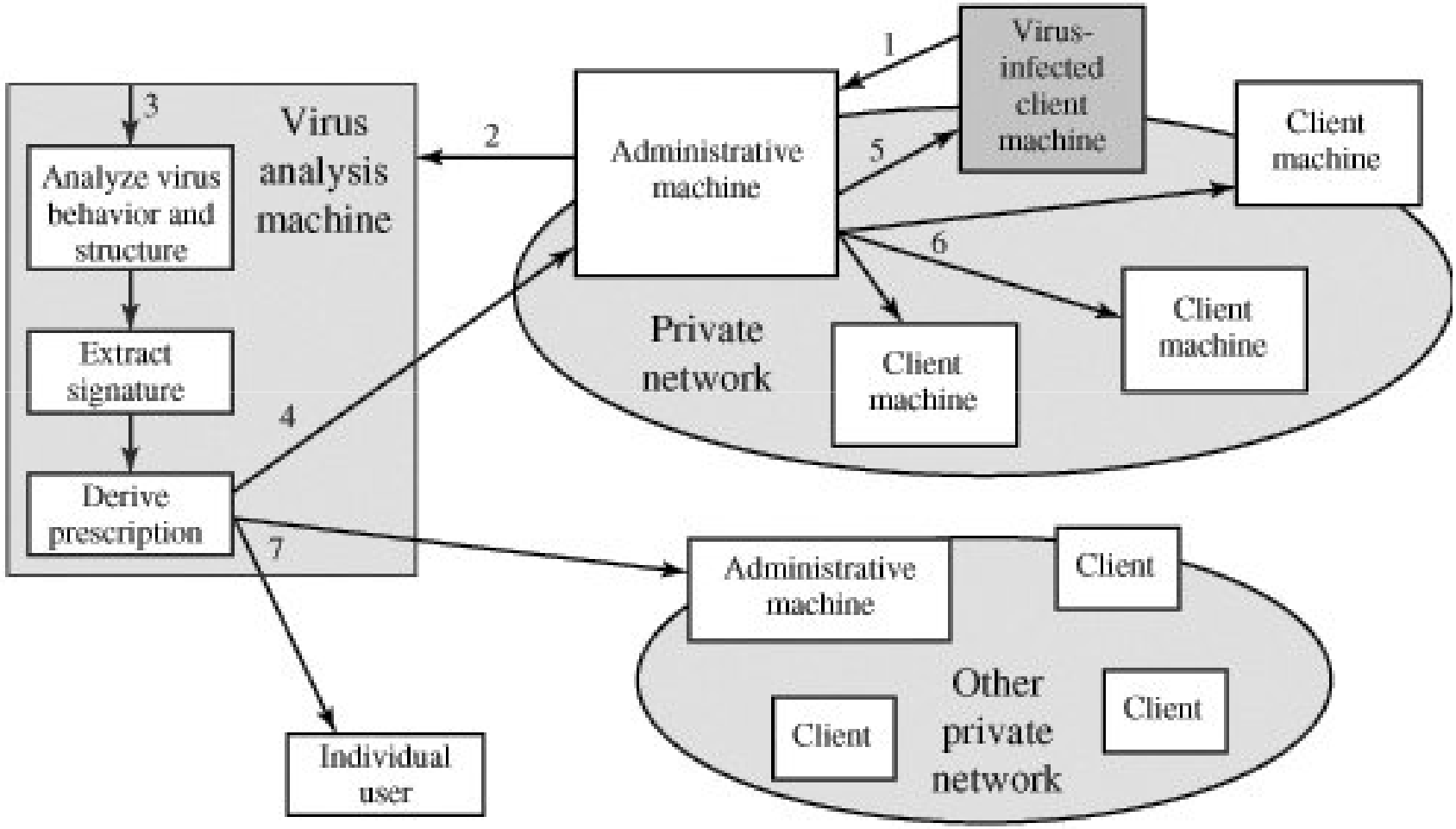
Напредне антивирус технике

- Генеричка декрипција пружа могућност детектовања софистицираних полиморфних вируса, на безбедан начин, без значајног успоравања система.
- Користи се GD скенер, који обухвата:
  - Емулатор процесора,
  - Скенер потписа вируса и
  - Модул за контролу симулације.
- Како је код полиморфних вируса део кода вируса шифорван, приликом покретања сваког програма, модул за контролу симулације најпре покреће код на емулатору процесора и уколико наиђе на део који представља дешифровање, чека док се вирус не разоткрије и тада га идентификује и уклања.
- Током овог процеса вирус не може нанети штету систему, јер се не извршава на рачунару, већ на емулатору.
- Најкомпликованија одлука приликом дизајна оваквог система је колико дуго треба програм извршавати на емулатору.

Напредне антивирус технике

- дигитални имуни систем (IBM)
  - праћење програма на сваком рачунару организације и слање копије сваког сумњивог програма административној машини
  - административна машина шифрује узорак и шаље га централној машини за анализу вируса
  - ова машина ствара окружење у коме је безбедно покренути заражени програм. Користи се емулација. Ова машина затим издаје рецепт за идентификацију и уклањање вируса
  - рецепт се шаље назад административној машини
  - административна машина прослеђује рецепт зараженој машини
  - рецепт се прослеђује и осталим клијентима у оквиру организације
  - клијенти широм света добијају редовна ажурирања антивируса, која их штите од нових вируса.

Дигитални имуни систем



Софтвер за блокирање понашања

- интегрише се са оперативним системом и прати понашање програма у реалном времену
- затим блокира потенцијално опасно понашање, пре него што такво понашање успе да се одрази на систем
- понашање које се прати укључује:
  - рад са фајлом, форматирање дискова, модификација логике извршних фајлова и макроа, модификација критичних системских подешавања, покретање мрежне комуникације
- ако установи да је неко понашање опасно, може да га блокира у реалном времену и да прекине софтвер који га је изазвао, или да тражи допуштење од корисника да се изврши тај програм
- ова техника је у предности у односу на детекторе злонамерног софтвера, јер како год добро да је вирус сакривен, мораће кад тад да упути исправно дефинисан захтев оперативном систему и ако софтвер за блокирање понашања може да пресретне сваки овакав захтев, онда он може и да заштити систем од сваког вируса.
- али мана овог приступа је што злонамерни софтвер мора да се покрене да би се детектовао и зауставио, а у том времену између покретања и детектовања он може да направи доста штете систему, нпр. упућујући захтеве оперативном систему, који нису опасни, али праве штету (померање фајлова)