Рачунарство и друштво
2015/2016

Сигурност рачунара и мрежа

Александар Картељ
aleksandar.kartelj@gmail.com

Рачунарска гимназија

Битни аспекти

- Да ли је реално да у филму „Умри мушки“ терористи преузму контролу над уличном расветом, системом за гас и електричне енергије?
- Проблематични аспекти:
  - Хакери
  - Малвер
  - Сајбер криминал и сајбер напади
  - Онлајн гласање

Хакери

- Оригинално значење речи хакер – онај који истражује, преузима ризик.
- MIT клуб за моделовање железница 1950-их.
- Најоданији чланови су остајали целу ноћ да побољшавају велики модел железнице испијајући велике количине Кока-Коле.
- „Хак“ је за њих представљало унапређење модела и реч „хакер“ је била знак поштовања.
- Крајем 1950-их неки од хакера су завршили курсеве програмирања... Остало је историја...

Хакери - ширење

- Неки филмови су допринели ширењу идеје за хакерисањем, нпр. Ратне игре из 1983.
- Данас су хакери најчешће они који покушавају да добију неауторизовани злонамерни приступ рачунарима и рачунарским мрежама.
- Приступи:
  1. Погађање корисничког имена и шифре. Када је ово могуће?
  2. Прислушкивање, „гледање изнад рамена“ (енг. eavesdropping)
  3. Претраживање смећа - неке фирме не уништавају папирно смеће – како се ово може искористити?
  4. Социјални инжењеринг – погодан у већим компанијама. Нпр. Вас назове на послу и представи се као шеф вашег шефа.

Казне за хакерисање

- Кажњиве активности:
  - Пренос кода (вируса, црва)
  - Неауторизовани приступ туђим налозима (чак и када нема приступа датотекама)
  - Пренос поверљивих владиних информација
  - Трговина шифрама
  - Рачунарске преваре
  - Рачунарске уцене
- У Америци је максимална казна 20 година затвора и 250.000$.
- У Србији су ниже казне, а најчешћи облик преваре је Нигеријска превара.

Анализа случаја - Firesheep

- Већина Интернет (http) саобраћаја није шифрована, а само неки критични делови нпр. логовање, приступ плаћањима итд. Јесу (https). Зашто није све?
- Бежичне мреже су посебно проблематичне јер је реч о радио сигналу који може бити пресретнут.
- „Sidejacking“ је вид злоупотребе у којем се прислушкује пренос у оквиру WiFi мреже и узима колачић који корисник добија од сајта.

Анализа случаја - Firesheep

- Проблем са многим сајтовима је што иако имају шифровану комуникацију при ауторизацији, колачићи нису шифровани.
- Ерик Батлер је 2010. направио екстензију за Firefox под називом Firesheep:
  - Након клика на дугме „Start capturing“ корисник би видео списак свих људи који користи WiFi у близини и сајтове које су посетили.
  - Кликом на неко име и одговарајући сајт он би приступио датом систему ауторизован као прави корисник.
- Шта мислите, зашто је Батлер то урадио?
- Да ли је то што је урадио било етички?

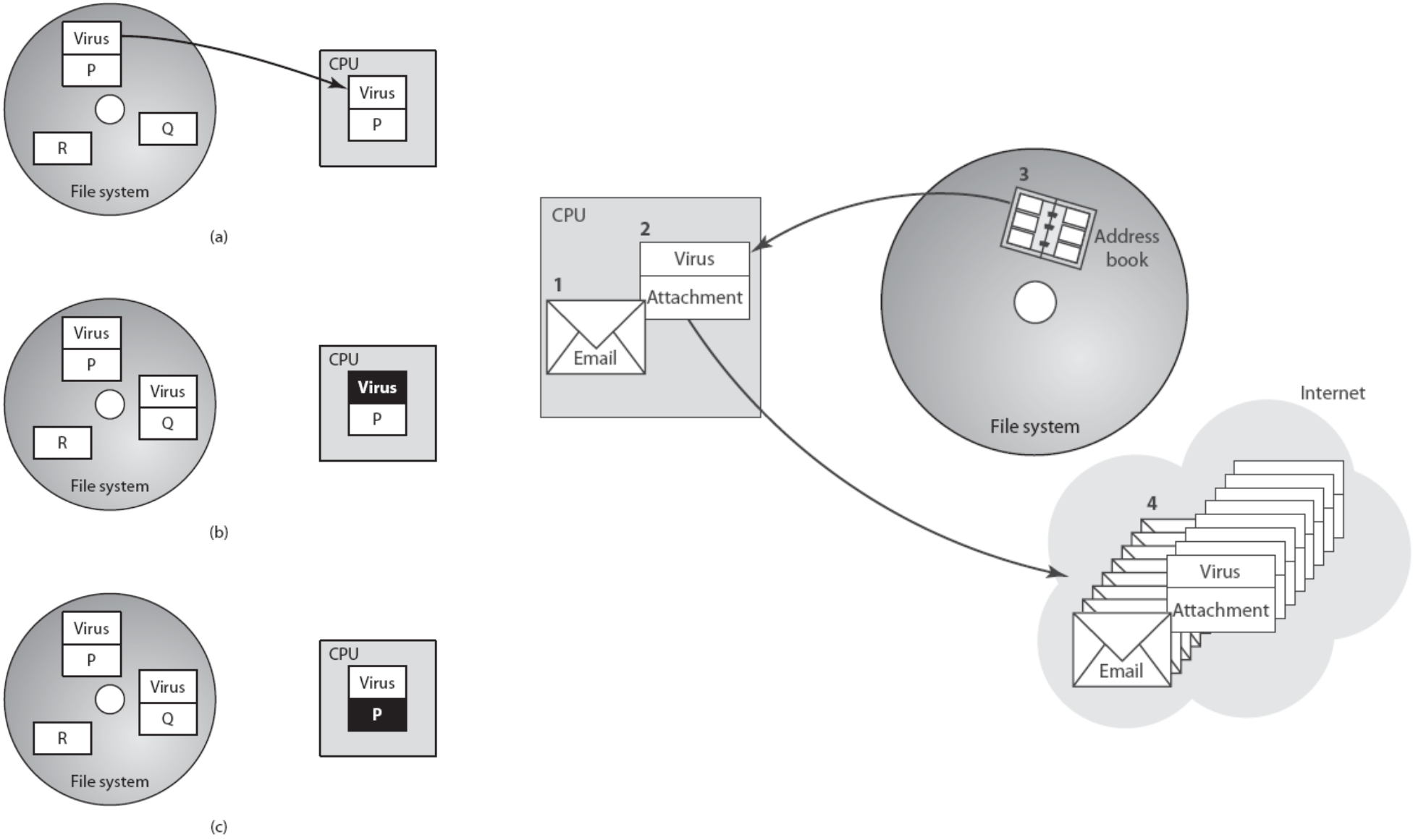
Малвер

- Злонамерни програми који се инфилтрирају на Ваш рачунар:
- Шта могу да раде након тога:
  - Ништа специјално, троше процесорско време.
  - Уништавају битне датотеке.
  - Преузимају контролу над рачунаром:
    - Користе Ваш рачунар као репозиторијум за украдене картице.
    - Ваш рачунар симулира веб сервер за порнографски материјал.
    - Ваш рачунар врши нападе на друге рачунаре у циљу добијања права приступа (енг. denial-of-service attack).

Вируси и црви

- Вирус је самореплицирајући програм који се налази у оквиру неког домаћина (другог програма).
- Када се покрене инсталација домаћина, најпре се покрене вирус и пронађе другог домаћина у Вашем рачунару и њега инфицира.
- Могу се преносити и путем имејл додатака (енг. attachment)
  - Већина имејл клијената ово спречава.
- Неки вируси могу бити релативно безопасни и само заузимати меморију и трошити процесор.
- Други могу брисати датоеке и слично.

Вирус – инфилтрација и ширење

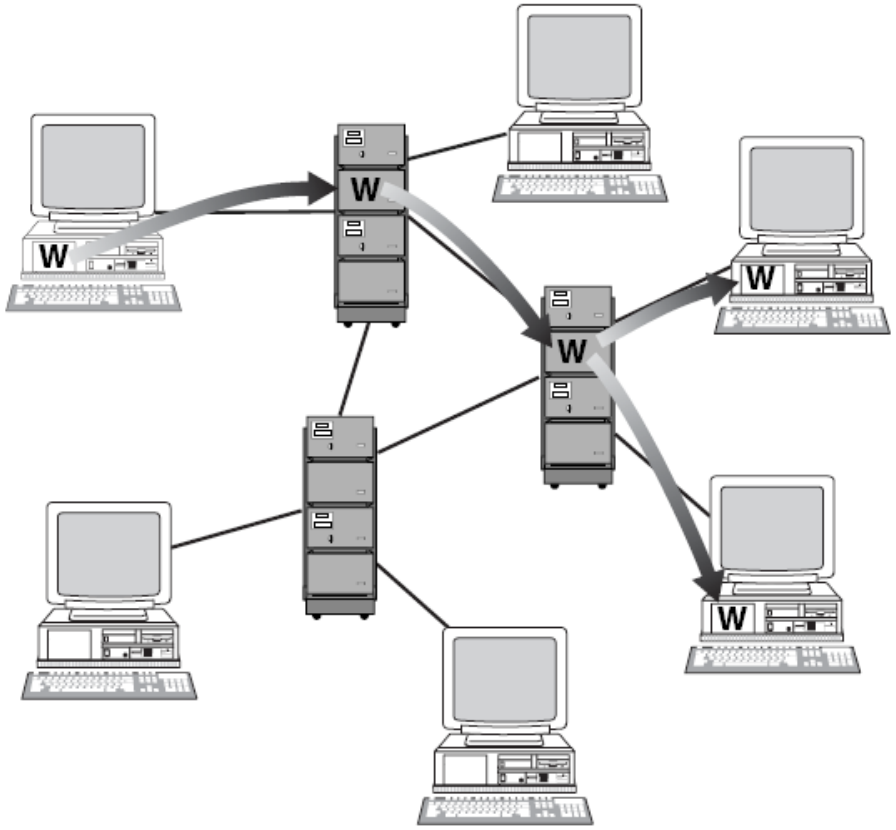


Антивирус програми

- Јако је битно да буду ажурни.
- Већина инфекција вирусима се дешава због неажурног антивирус софтвера.
- Стално се појављују нови типови вируса.
- Постоје и лажни антивирус програми.

Црви

- Програм који проналази сигурносне пропусте у рачунарској мрежи и шири се.



Роберт Морис

- Роберт Морис је почео да учи Unix још када је био у основној школи. Његов отац је радио у Беловим лабораторијама и они су имали приступ пословним рачунарима од куће.
- Убрзо је Морис открио сигурносне пропусте у Unix-у па је могао нпр. да чита мејлове других људи у мрежи и слично.
- Као студент основних студија на Харварду постао је познат као стручњак за Unix и убрзо су га запослили у Беловим лабораторијама.
- Стално је правио шале на Харварду, нпр. убацио је да пре логовања студенти морају да одговоре на питање које поставља Oracle, а након тога да и сами поставе питање. Наравно није постојао Oracle, само су једни другима постављали питања.

Интернет црв – Роберт Морис

- Када је био на постдипломским студијама на Cornell-у постао је опседнут прављењем црва који ће пробити Unix сигурност.
- Његова листа жеља је била следећа:
  - Инфицирај 3 машине по локалној мрежи
  - Користи CPU само ако је слободан
  - Избегавај споријe машине
  - „Проваљуј“ шифре у циљу ширења на друге рачунаре
- Циљ црва није био да оштети рачунар, већ да увиди на колико максимално рачунара може да се прошири!

Интернет црв - лансирање

- Морис је лансирао Интернет црва 2. новембра 1988. године у MIT лабораторијама.
- Црв је на неколико дана онеспособио већину тада доступних рачунара (Интернет је тада укључивао махом универзитете).
- Морис је касније избачен са Cornell-a и осуђен на 3 године условно и новчану казну.
- Да ли је Морис био етичан?

Други познати црви

- 2004. SASSER
  - 18 милиона инфекција.
  - Изазивао гашење рачунара – велики проблем за авиокомпаније, железнице и слично.
  - Кривац – седамнаестогодишњак, немац.
- 2008. Conficker
  - Око 15 милиона инфекција укључујући и добар део војне Интернет мреже у Француској, Енглеској итд.
  - Ширење по рачунарима који нису имали последњи Microsoft Update.
  - Кривац није откривен.

Други видови малвера

- Cross-side scripting
  - Убацивање страног програма у Веб сајт
- Навођено преузимање (drive-by download)
  - Преузимање малвера јер корисник мисли да је то нешто друго (искаче попуп, лажни резултат гугл претраге и слично)
- Тројански коњ
  - Инфилтира се и потом нпр. преузима шифре за рачунарске игре итд.
- Rootkits
- Spyware, Adware...

Сајбер напади

- Економска корист од Интернета неколико хиљада милијарди годишње и расте.
- Ово чини Интернет примамљивим за организовани криминал.
- Типови напада:
  - Пецање и пецање штапом (phishing and spear phishing)
  - Убацивање SQL кода (SQL injection)
  - DoS и DDoS

Пецање

- Нападач шаље милионе мејлова са информацијом да је кориснички налог
на нпр. Амазону компромитован.
- Ту је и лажни линк ка „Амазону“ који корисник кликне.
- Корисник бива преусмерен на
лажну страницу „Амазона“ и ауторизује се.
- Наравно, то је само маска сајта и он је заправо одао своје информације:
налог и корисничко име
- Неколико стотина хиљада успешних напада пецањем годишње.
- Пецање штапом – варијанта са циљањем одређене групе корисника нпр. старијих особа.

Убацивање SQL кода

- Убацивање SQL кода у текстуално поље за унос нпр. налога или шифре.
- Већина познатих Интернет сајтова има заштиту против овога.
- Пример – кориснички унос за претрагу:

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

- Шта ако се унесе у текстуално поље "464 or 1=1 “
- Добија се:

```
txtSQL = "SELECT * FROM Users WHERE UserId = 464 or 1=1
```

DoS (denial of service)

- Циљ није крађа података већ онеспособљавање рачунарског система (сервера).
- Сервер бива нападнут појединачно или симултано од стране других система.
- Истовремено се пошаљу хиљаде захтева што систем не може да подржи и слично.
- DDoS – дистрибуирана варијанта овог напада

Сајбер криминал

- Продаја малициозног софтвера (малвера) на илегалним аукцијама оном ко највише понуди.
- Једна машина инфицирана Adware софтвером донесе у просеку 1$ месечно:
  - Закон великих бројева!
- Логери за тастатуру – јако опасни софтвери:
  - Крађа кредитних картица
  - Злоупотреба плаћених услуга

Сајбер инцидент - Blue Security

- 2006. Израелска компанија Blue Security:
  - Анти-спам систем који инсталирате и када Вам стигне порука најпре бива проверена од сервера.
  - Ако сервер потврди да није спам пропушта поруку ка примаоцу.
  - У супротном се шаље порука упозорења пошиљаоцу односно „спамеру“.
  - Ово је врло брзо „затрпало“ сандучиће спамера и многи су одустали од напада на Blue Security кориснике.
- Међутим група спамера није одустала и наставила је још жешће DDoS нападе на Blue Security.
- Наравно, Blue Security је ускоро пропао.

Сајбер инцидент – Алберта Гонзалес

- 2010. Алберта Гонзалес је осуђена на 20 година затвора.
- Разлог: SQL убацивање кода којим је украла 130 милиона кредитних картица.
- Највише је било проневера на дебитним онлајн картицама које се често дају као купони.
- Штета од око 130 милона долара.

Политички мотивисани напади

- Естонија је одлучила 2007. године да измести статуу руског војника из Талина, главног града.
- Овај потез је оцењен као непопуларан међу руским становништвом и у Русији генерално.
- Последица је да су Руси извели DDoS нападе невиђених размера на сајтове Естоније.
- Око милион рачунара је било укључено у напад на:
  - Јавне установе
  - Владине системе и системе војске
  - Банке итд.
- Сличне ствари су се дешавале и у Грузији, Јужној Кореји, Тибету итд.

Онлајн гласање

- Због многобројних неправилности са „папирним“ гласањем многе земље су започеле праксу гласања на електронским машинама.
- У неким деловима Америке, попут Аљаске је уведено онлајн гласање.
- Естонија је била прва држава која је увела гласање на нивоу гласања за парламент и локалну управу.
- За и против онлајн гласања – дискусија?