JADRANKO PETROVIĆ, dipl.inž.
RO "Josip Kraš"
Zagreb, Ravnice bb

Znanost u prometu
Stručni rad
UDK: 681.326
Primljeno: 13.02.1990.
Prihvaćeno: 24.09.1990.

ZAŠTITA PODATAKA I SOFTVERA U VEZI PROJEKTA DOCIMEL

SAŽETAK

Autor razmatra u radu problem zaštite podataka i softvera općenito, a s tim u vezi i posebno kod projekta DOCIMEL. Ukazuje na opasnosti tzv. virusa, tj. programa koji imaju sposobnost da se sami reproduciraju i zatim počinju svoju razornu aktivnost u računarskim sistemima. Obrazlaže se više načina zaštite od virusa, posebno kod DOCIMEL-a, koji će biti pristupačan velikom broju korisnika i kao takav još više ranjiv.

1. UVOD

Željeznice država-članica EZ postavile su si maksimu da 1.1.1991.g. zamijene klasični tovarni list s magnetskim zapisom. Projekt kojim se to treba ostvariti je DOCIMEL. Jedan od osnovnih problema koji sputava već sada primjenu DOCIMEL-a je adekvatna zaštita podataka i softvera, te odgovornost u vezi automatskog prenosa podataka. Moramo ovdje napomenuti da isticanje ovih problema nije specifičnost samo projekta DOCIMEL. Svjedoci smo raznoraznih kriminalnih radnji u području elektronske obrade podataka a koje se događaju u zemljama gdje je računarska tehnika i tehnologija daleko zakoračila u svakodnevnicu. Ne moramo ni govoriti kolike mogućnosti kriminalnih radnji pruža željeznički prijevoz roba, ako se isticani problemi ne riješe na zadovoljavajući način. Ne samo da bi željeznice mogle ostati bez vozarine za prijevoze roba, već na vrlo elegantni način i bez robe koju su preuzele na prijevoz, tj. da ju isporuče nepoželjnom primaocu.

No, radi jasnoće problema, mi ćemo razmotriti svaki problem posebno. U današnjoj informatici izdvajaju se sve veća i veća sredstva za razvoj zaštite podataka i softvera. Budući da sami podaci i softver predstavljaju vrijednost, a njih ima sve više u računarskim sistemima, razumljivo je da ih treba zaštititi. Problem je jedino što nijedna zaštita nije stopostotna, a ponekad za neke podatke vrijednost zaštite prelazi vrijednost samog podatka kojeg treba sačuvati. Teško je tu odrediti granicu ulaganja u zaštitu. Mjere zaštite u informatici koncentriraju se u tri pravca pa zaštita može biti softverska, hardverska ili kombinirana. Upotreba neke od tih zaštita zavisi od toga što treba štititi, koliko možemo uložiti u zaštitu i koliko će ta zaštita zapravo biti efikasna. Danas kad se računari spajaju u računarske mreže, a baze podataka se preklapaju, teško je zaštititi jedan takav složen informacijski sistem.

Računarske mreže možemo podijeliti u dva podsistema:
- podsisteme računara i terminala gdje računari mogu biti centralni računari velikog kapaciteta ili mali osobni računari, a terminali jednostavni "neinteligentni" pa sve do složenih "inteligentnih" terminalnih podsistema,
- prenosne podsisteme čiji je osnovni zadatak osiguranje ispravnog prenosa podataka između elemenata (računara i terminala) podsistema računara i terminala.

Sve strože mjere zaštite elektroničkih računskih centara pružaju malu mogućnost direktne zloupotrebe nad njihovim resursima u odnosu na komunikacijske mreže koje se sastoje od čitavog niza kablova, prekidača, modema, multipleksora itd.

Razina zaštite pristupu od podataka i drugih resursa bit će različita u različitim oblastima. U vojnim i mnogim finacijskim sistemima zahtijevat će se najviša razina sigurnosti, u drugim sistemima gotovo neće biti potrebna.

U svakom slučaju, potpunu sigurnost komunikacijskog sistema je nemoguće postići. Vrlo pouzdana zaštita od neovlaštenog dostupa do sadržaja podataka i njihove promjene postiže se postupkom šifriranja. Pri tome se koriste složeni algoritmi šifriranja, budući da je jednostavnije šifre lako otkriti. U prenosu podataka postoje dva načina šifriranja i to transformacija bita na bit ili čitavog bloka. Poruka koja se šifrira ima veliku redundanciju, budući da je obično ključ šifriranja veliki kao i sam tekst, a on se prenosi zajedno sa porukom.

Šifriranje može biti softversko u samom računaru ili hardversko sa posebnim uređajima (enkriptor/dekriptor), koji se stavljaju na digitalni izlaz (ulaz) podataka između računara i modema.

Osim sprečavanja, otkrivanja i promjene sadržaja poruka zaštita komunikacija ima još zadatak sprečavanja analize prometa, otkrivanje promjena u redoslijedu poruka, otkrivanje onemogućavanja usluga, te otkrivanje pokušaja neovlaštenog uspostavljanja veza.

Jedan od načina zaštite analize prometa je u kontinuiranom slanju poruka. Ako nema podataka koji se razmjenjuju, šalju se tzv. prazne poruke, čime se onemogućava analiziranje stvarnog prometa. Analiza dužine poruka se sprečava dodavanjem bitova ili znakova poruci

ispred i iza stvarnog teksta.

Postizanje ostalih ciljeva zaštite može se riješititi protokolima komuniciranja viših razina.

Zaštitu podsistema računara i terminala treba izvesti već kod projektiranja jednog takvog računskog sistema ili izrade odgovarajućeg sistema softvera za neki računar. Pri tome bi projektanti trebali voditi računa da dotični budu što manje ranjivi.

Složenost informacijskog sistema je, uglavnom, ugrađena u njegovom softveru da bi hardver mogao da bude jednostavniji i sastavljen od standardnih jedinica, kao što su mikroprocesori i memorijalni čipovi. Odlika je softvera da može biti izmijenjen i za vrijeme razvoja i poslije toga, da bi sistem dobio nove osobine. Ovakva fleksibilnost je s druge strane prijetnja sigurnosti računarskog sistema, pogotovo kad postoje "MAIN-FRAME" računari sa svojim složenim operativnim sistemom, koji se nikada ne mogu potpuno razumjeti.

Jedna od najpoznatijih zaštita nekog sistema je pristup dotičnom preko lozinke (password). Na prvi pogled čini se nemogućim ući u taj sistem bez lozinke. To je kao da pokušamo ući u zaključanu kuću bez ključa. Ali ako razmislimo malo bolje shvatit ćemo, da to i nije nemoguće. Može se pokušati ući kroz neki otvoreni prozor, ili pozvati majstora da dotična vrata otključa.

Za sistem to izgleda slično. Koliko puta zna terminal da ostane priključen na sistem, a korisnik otiđe za "trenutak" na kavu, telefon ili sl,. Ništa lakše za nekoga sa lošim namjerama da za nekoliko minuta obavi brisanje, mijenjanje ili da sazna određene podatke.

Ući u sistem bez znanja lozinke ponekad također nije teško. Istraživanja su pokazala da lozinku najčešće zna više ljudi, da se mijenja prije određenog vremena (pogotovo to vrijedi za lozinke sa posebnim ovlaštenjima), da osoblje zna napustiti firmu, a njegova lozinka ostaje ista još godinama. Također, prilikom izbora lozinki firme su neoprezne i nedosjetljive pa čovjek sa iskustvom može za nekoliko minuta provaliti u većinu sistema. Uglavnom, u svakoj državi koristi se nekoliko stalnih riječi za lozinku. S druge strane, danas postoje kućni računari uz čiju pomoć možemo također relativno brzo otkriti lozinku. Takav računar priključen na veliki sistem generira različite lozinke sve dok ne naleti na pravu i ne uđe u veliki sistem.

U novim operacijskim sistemima jedna od zaštite od takvog pristupa je ograničenost pokušaja pogrešnog unosa lozinke ili u eksponencijalnom rastu vremena odziva za svaki novi krivi pokušaj unosa lozinke.

Jedan od značajnih faktora zaštite sistema je i odabir odgovarajućih ljudi koji će se baviti sistemom u upotrebi. To se prvenstveno odnosi na sistem-administratore i administratore baze podataka. Ti ljudi imaju privilegiran status pristupa sistemu. Takva jedna osoba može uraditi na sistemu gotovo sve što hoće. Dakle, kod odabira ljudi za taj posao treba voditi računa da su to pouzdani i sposobni ljudi za taj posao, budući da pouzdan ali nesposoban čovjek na takvom mjestu može isto tako uraditi puno štete.

Danas se nad računarskim programima i mrežama širi velika epidemija virusa koji su preplavili SAD, a i po Evropi se šire velikom brzinom. Američka CVIA (Computer Virus Industry Asociation) primila je 1988.g. 25 tisuća zahtjeva za pomoć i informaciju pri razobličavanju misterioznih virusa koji uništavaju podatke.

Amerikanci razlikuju različite tipove virusa, te su ih prema njihovom ponašanju i djelovanju na računare nazvali različitim imenima (crvi, trojanski konji i sl.).

Virusi su u suštini programi koji su sposobni da se autoreproduciraju, inficiraju ostale nezaražene programe, ta da nakon određenog vremena ili broja kopija počnu svoju ubilačku akciju. Ta akcija se očituje u gubljenju datoteka, disk se inicijalizira sam od sebe, ponekad se izbriše memorija i slično.

Početak virusa seže u sredinu 70-ih godina. Tada se pojavila verzija računarske igre "Core Wars" od A.K.Dewdneya. U toj igri sudjeluju dva programa koji jure jedan drugog po memoriji i nastoje izbrisati protivnika. Usput postavljaju numeričke bombe po susjednim lokacijama, kopiraju sami sebe na druge lokacije, negdje se zaustavljaju i liječe svoje rane. Kraj igre u potpunosti ovisi od samih programa i od toga koji je prvi napadnut na ranjivom području. Dakle, osnovna ideja je da svakim pokretanjem programa on sam sebe autoreproducira i raširi se preko računarske mreže, a to je zajednička odlika svih virusa.

Kako je jednostavno napisati program za brisanje ili za kopiranje samog sebe vidjet ćemo na dva slijedeća primjera.

Program za brisanje memorija je vrlo lako napisati u nekom asamblerskom kodu na osnovu slijedećeg principa.

```
LOK1    ADD     1   BR1
        MOVE    0   (BR1)
        JMP     LOK1
BR1     4
```

Na početku povećavamo vrijednost lokalnog brojača za 1 (inicijalna vrijednost je 4). Upisujemo nulu u memorijsku lokaciju koja se nalazi u lokaciji BR1. Sa instrukcijom JMP, zatvaramo program u beskonačnu petlju i time upisujemo nule u cijelu memoriju.

Princip programa koji kopira samog sebe po cijeloj memoriji izgleda ovako:

```
LOK1    MOVE    10      C
LOk2    MOVE    (BR1)   (BR2)
        ADD     1       BR1
        ADD     1       BR2
        DEC     C       LOK2
        MOVE    BR3     BR1
```

```
        JMP     LOK1
BR1     LOK1
BR2     LOK3
BR3     LOK1
LOK3
```

Prvom instrukcijom daje se nalog koliko će redaka kopirati. Nakon toga premješta vrijednost prvog retka programa na lokaciju u memoriji čija se adresa nalazi pohranjena u lokaciji BR2. U slijedeća dva koraka program sprema prenos na slijedeći red programa. Provjera da li je sve prenešeno. U slučaju da nije, ponovo izvodi dio programa od lokacije LOK2. Kada je sve prenešeno vraća ponovo staru početnu adresu programa i slijedećim instrukcijama vraća se na početak programa u drugu memorijalnu lokaciju.

Virusi su veoma opasni programi u današnjem svijetu računara i automatiziranih podržanih procesa. Mogli bi odjednom da zaustave sav promet i bankovni transfer, mogli bi da se zagube bez podataka itd. Najglasovitiji slučaj je bio onaj s mrežom ARPA (The Advanced Research Project Agency), kojom se koristi i Pentagon, a koja povezuje desetke sveučilišta, istraživačkih laboratorija i znanstvenih instituta. Takav jedan program se autoreproducirao i napunio memoriju sistema samo sa sobom, te je ta mreža bila blokirana nekoliko dana. Ni IBM nije ostao pošteđen virusa. Njegovu mrežu za transmisiju podatka napao je prošle godine virus ubačen s božićnom porukom.

To je samo primjer da programa koji u sebi nose virus ima svih vrsta od javnih ili pomoćnih koji su besplatni, do specijalnih sistematskih koji se krišom prekopiraju od prijatelja. Takvi se programi prilikom svakog pokretanja sistema aktiviraju i inficiraju ostale sistemske programe koji još nisu inficirani. Tako se virus nanovo rasprostire i ako smo priključeni u računarsku mrežu, rasprostire se i na druge računare. Virus može da ima vremensku kontrolu i da se pojavi samo u određenom danu i satu, a zatim se izbriše ili opet zaspi.

Kako se zaštititi od virusa? Najbolji način je ne uključivati se u računarsku mrežu, imati samo svoj legalno kupljen softver, ne pasti pod utjecaj prijatelja i ne instalirati neki novi softver koji ne poznajemo dobro i ne znamo na koji ga je način prijatelj dobio. Također je poželjno nabaviti i nekoliko programa koji služe kao cjepivo protiv virusa. Ti programi provjeravaju sumnjive programe prije nego ih računar upotrebi i ako nađu dijelove računarskog koda koji nevin program ne bi smio imati, brišu ga. Međutim, ni jedan dosadašnji takav program nije u potpunosti pouzdan i svestran iz jednostavnog razloga što ima puno različitih virusa, napravljenih na različite načine.

Sistem DOCIMEL u svojoj zamisli mora biti pristupačan velikom krugu korisnika i to ne samo željezničkih. Ovo povećava dostupnost do sistema praktički neograničenom broju ljudi, a to znači i onima čiji je cilj besplatna vozarina, otuđenje pošiljaka itd. Iz iznijetoga se vidi koliko je računarski sistem ranjiv. Očito da se mora pronaći zaštita prije nego što tovarni list bude u potpunosti zamijenjen elektronskim zapisom.

SUMMARY

PROTECTION OF DATA AND SOFTWARE WITH REFERENCE TO THE DOCIMEL PROJECT

The author deals with the issue of protection of data and software in general and with particular reference to the DOCIMEL Project. Ther author discusses the problem of the so called virus i.e. the programs capable of reproducing themselves and starting their destructive activity in computer systems. The author exposes a number of protection methods in fighting virus with particular reference to the DOCIMEL Project that will be available for access to a large number of users and as such more vulnerable than others.