NADRAČUNALNIŠTVO IN VARNO POSLOVANJE[1]

Niko Schlamberger

Poslovni sistemi se danes resno ukvarjajo z vprašanjem, kako zagotoviti varno elektronsko poslovanje. Odprte komunikacije, Internet in omreženi računalniki na že skoraj vsakem delovnem mestu so skrb za zaščito podatkov, ki se je še pred nekaj leti zdela kar pretirana, opravičile. Medtem so nas virusi, ki se razširjajo po računalniških mrežah, spametovali in previdneži izpred desetletja so danes videti skorajda lahkomiselni. Pregrade, kombinacije naprav in programov, ki naj bi onemogočile pristop do računalniških virov, so danes obvezen del vsakega komunikacijskega sistema. Skoraj neverjetno se zdi, da je bil v Združenih državah Amerike že pred več kot desetletjem sprejet standard za zaščito podatkov (Data Encryption Standard, DES), ki je v primerjavi s kasneje razvitimi načini razmeroma enostaven, je pa pomemben prvi korak. Eden od optimalnih algoritmov za kodiranje podatkov je RSA[2], ki omogoča razmeroma dobro zaščito pri dokaj enostavni uporabi. V Združenih državah Amerike (kje pa drugje) napisani program PGP[3] daje prav to: še kar dobro zaščito in s tem domnevno tudi varno poslovanje. Zaščita je celo tako dobra, da ga je ameriška vlada označila za strateški material in omejila njegovo distribucijo.

Varno poslovanje je tako poslovanje, pri katerem ne more priti do zlorab v nobeni fazi opravljanja poslovne transakcije. Ali je klasično poslovanje, torej tako, kjer funkcije, procesi in postopki niso informatizirani, varno? Seveda ne. O tem nas vsak dan znova poučijo črne kronike javnih občil. Pri informatiziranem poslovnem procesu je nezaupanje do varnosti poslovanja še večje, ker je ves proces izjemno hiter in poleg tega za večino neinformatikov tudi nepregleden. Da ta občutek ni zgolj preganjavica, nas prepričujejo vesti o zlorabah pri kupovanju na daljavo. To je verjetno tudi eden od močnih zadržkov, da se trgovalna središča ("Trade Point") le težko uveljavljajo, čeprav je pospeševanje poslovanja na daljavo njihovo glavno poslanstvo. Ali je informatizirano poslovanje lahko varno?

Obstaja mnenje, da je sintagma "varnost v Internetu" oksimoron. Zaščita, zanesljivost in nadzor pristopa do podatkov naj bi bili tehnološko nezdružljivi z javnimi omrežjem, katerega velikost in zapletenost naraščata z eksplozivno hitrostjo. Vendar so strokovnjaki, katerih področje dela je prav to: varnost v Internetu. Eden izmed njih je Dan Farmer, kralj omrežne zaščite, ki za svetovalni dan računa tudi 5.000 dolarjev in ki ga ameriški senat upošteva kot izvedenca pri razvijanju zaščite zveznih računalniških sistemov[4]. Sodeloval je pri razvoju programa SATAN, katerega del je podatkovna baza o programskih napakah v sistemih zaščite računalniških vozlišč. Z njeno pomočjo SATAN sistematično preizkuša vozlišča v omrežju, ali v njih obstajajo take luknje. Za razliko od drugih programov[5], ki preiskujejo domača omrežja, lahko SATAN brska po kateremkoli Internetovem računalniku. Farmer ima nekoliko nenavadne prijeme: nedavno tega je brez dovoljenja preiskal 1.700 Internetovih vozlišč v bankah, kreditnih družbah, časopisih, zveznih ustanovah in še kje. V poročilu, ki ga je objavil, je povedal, da sta okoli dve tretjini lokacij opremljeni s programi, ki vsebujejo napake in so dotični računalniki enostaven cilj za zlorabe. Kar 68 odstotkov lokacij v bankah in 70 odstotkov lokacij, ki jih vzdržujejo časopisi, je ranljivih, kar je presenečenje za povprečnega obiskovalca Interneta, za Farmerja pa niti ne. Meni, da bi utegnil biti odstotek nezaščitenih vozlišč celo večji. Seznama lokacij seveda ni objavil. Tudi sam se strinja z mnenji nekaterih, da je njegova metoda nekonvencionalna in nekakšno sivo področje računalniškega zanesenjaštva.

Zamislimo si, da bi želel nekdo dešifrirati sporočilo, zakodirano s pomočjo na algoritmu RSA zgrajenega programa RC5 podjetja Data Security. Tako zakodirano sporočilo naj bi bilo varno, saj bi bilo treba preizkusiti

1 *Prispevek povzema članek World Wide Widgets, Scientific American, maj 1997. Povezava s poslovanjem je dodana. Beseda "nadračunalništvo" je prevod ameriškega izraza "metacomputing".*

2 *Naziv algoritma so začetnice priimkov avtorjev, ki so ga razvili: Rivest, Shamir, Adelman.*

3 *Pretty Good Privacy*

4 *Scientific American, april 1997.*

5 *Eden od prvih takih je COPS D. Farmerja.*

kar 281 trilijonov mogočih ključev, da bi našli pravega. Ameriška državna agencija za varnost (National Security Agency, NSA) razpolaga z dovolj močnimi računalniki, da bi razbila kodo v sprejemljivem času, večina drugih pa ne. Najhitrejši današnji osebni računalnik bi to nalogo opravil približno v dveh letih. Vendar pa bi bilo mogoče z RC5 zakodirano sporočilo dekodirati bistveno prej in sicer tako, da bi se zbralo dovolj veliko število interesentov, na primer več tisoč, ki bi si reševanje naloge razdelili. Zamisel je presenetljivo preprosta: postopek iskanja ključa bi si razdelili in ga reševali istočasno. Vsak izmed njih bi dobil programček ("widget"), ki preizkuša zaporedje ključev tačas, ko je njegov računalnik prost. Ko bi preizkušanje končal, bi vsak udeleženec rezultat poslal nekemu centralnemu računalniku in od njega prejel nadaljnje ključe, ki naj jih preizkusi. V času reševanja problema bi računalniki delovali kot zmogljiv moderen superračunalnik. To se še ni zgodilo, vendar ni rečeno, da se tudi ne bo.

Zamisel je presenetljivo preprosta in sicer v reševanje nekega problema vpreči v mrežo povezane računalnike, ki so trenutno dovolj prosti. Pri nekaj deset računalnikih je taka ideja utopična, pri nekaj tisoč je vredna razmisleka, pri sto tisoč pa je vredno tudi že kaj narediti. Internet s sto tisoči računalniških vozlišč je danes za kaj takega tako rekoč naravna možnost. Že leta 1992 je bil ta koncept opisan in zdel se je tako izvedljiv, da je dobil tudi ime: metaračunalništvo. Prvi poizkusi, da bi močne računalnike povezali v nadračunalnik, so propadli in zanimanje je upadlo. Zanesenjaki metaračunalništva pa so se spet oglasili. V Internet je povezanih neprimerno več računalnikov kakor pred petimi leti in Java omogoča pisanje programov, ki se lahko izvajajo na prej nezdružljivih strojih. Niz nedavnih poizkusov navaja na misel, da nadračunalniki niso več daleč. Svetovno omrežje (World Wide Web) bi lahko delovalo tudi kot računalniško omrežje, na katero se lahko priključimo tako enostavno, kakor bi priključili električno napravo v vtičnico. Seveda je še kar nekaj nerešenih tehničnih problemov. Na primer: podatki bi morali biti zapisani na način, ki bi ga razumeli vsi udeleženi računalniki; naloga bi morala biti razdeljena tako, da bi jo računalniki reševali paralelno. So tudi ekonomske omejitve kot na primer ta, da je verjetno ceneje in hitreje računati na enem mestu kakor razpošiljati podatke sem in tja. Potem gre tudi za zaupanje med sodelujočimi: ali bi VISA ali IBM verjela, da udeleženi računalniki ne bodo škilili v podatke, ki jih obdelujejo? Ali imajo znanstveniki, ki distribuirajo reševanje problema, zagotovilo, da bo rezultat znan samo njim?

Nekateri od metaračunalniških projektov so vsaj deloma na postavljena vprašanja že odgovorili. Na kalifornijski univerzi v Berkeleyu je v teku projekt WebOS, pri katerem vdelajo URL-je (imena datotek, ki jih uporabljajo mrežni brkljalniki) v datoteke omrežne delovne postaje tako, da so dostopne prek omrežja. Na kalifornijski univerzi v Santa Barbari razvijajo program Javelin, ki je programski mešetar ("broker") za posredovanje med ponudniki procesorske moči in povpraševalci po njej. Kopije poslov, ki jih dobi mešetar v obliki programov Java, razpošlje naprej trenutno prostim računalnikom. Težava je le, da zaradi Jave taki programi ne morejo uporabiti diskovnega pomnilnika udeleženega stroja, kar reševanje problema omeji na procesorski pomnilnik. Ohrabrujoč je rezultat projekta Charlotte z univerze v New Yorku. Model magnetne interakcije, katerega reševanje je bilo razdeljeno med 10 računalnikov, je bil izračunan devetkrat hitreje, kakor bi bil sicer. Še več, rezultat je bil pravilen tudi tedaj, ko je bilo nekaj računalnikov namenoma ustavljenih.

Metaračunalništvo postaja realnost. Domačih osebnih računalnikov ne bo izpodrinilo takoj, tisti, ki znajo in zmorejo, pa bodo lahko Internetova vozlišča povezali v izjemno močan računalnik. Ali je elektronsko poslovanje potem sploh lahko varno? Varnega poslovanja ni. Analogno stališču Evropske komisije o računalniškem kriminalu ("Kar je prepovedano off-line, je prepovedano tudi on-line") bi lahko rekli: "Kar ni varno off-line, tudi ni varno on-line". Vendar pa ni bistveno to, ali je poslovanje varno ali ni, temveč to, ali je zaščiteno. Kakor klasično poslovanje pa je tudi elektronsko lahko in mora biti zavarovano. Poleg tega mora biti vrednost transakcije v razumnem razmerju s stroški, ki bi jih nekdo imel z vdiranjem v sistem. In končno, vsaj trenutno večina tistih, ki bi jih to zanimalo, ne razpolaga z dovolj močnim orodjem.

■