UVODNA REČ

RELJA JOVIĆ

Napad iPodova

MNOGO se dosad pisalo o pretnjama po bezbednost informatičkih sistema koje potiču od iPodova, digitalnih fotoaparata i USB memorijskih uređaja. Pošto se radi o uređajima za skladištenje podataka velikog kapaciteta, njihovi zlonamerni vlasnici (bilo da je reč o zaposlenima u vašem preduzeću ili o ljudima sa strane) mogu da se prikradu računarima, brzo preuzmu gomilu poverljivih dokumenata i potom se išunjaju iz zgrade – dok ste vi sve vreme mislili da samo uživaju u popularnim melodijama. Kradljivci mogu kompanijske tajne da iznesu i na SD kartici digitalnog fotoaparata, a ako su zaista podli mogu da izbrišu datoteke kako ne bi bile vidljive tokom nasumično obavljene inspekcije. Kada se vrate kući, pomoću programa za obnavljanje izbrisanih datoteka lako mogu da pristupe poverljivim podacima.

Dve funkcije koje to omogućavaju su Windowsov AutoRun i sposobnost periferijskih uređaja da koriste tzv. neposredan pristup memoriji (direct memory access, DMA).

AutoRun nije problem samo u Windowsu. Devedesetih godina prošloga veka, računari Macintosh su imali sličnu funkciju Autostart, koja je automatski pokretala datoteke programa QuickTime 2.0. U kompaniji Apple su uklonili tu funkciju iz operativnog sistema nakon što se virus nazvan Hong Kong proširio 1998. godine na hiljade računara. Operativni sistem Palm je takođe imao funkciju koja je svakom programu na SD kartici omogućavala da se automatski pokrene čim bi se kartice umetnula u ležište za proširenje.

Ova pretnja je stvarna i zloupotrebljavana je u velikoj meri. Kombinacija špijunskog softvera i administratorskog paketa (rootkit), koju je kompanija Sony Music prošle godine distributirala na milionima svojih kompakt diskova, instalirana je kao deo AutoRun skripta. Špijunski softver je tako bio instaliran na računarima pod Windowsom širom sveta.

Međutim, koliko god funkcija AutoRun bila loša, postoji pretnja koja je „ugrađena" u praktično svaki stoni računar i server što se danas koriste, a utiče na računare koji rade pod Windowsom, operativnim sistemom za Macintoshe i vrlo verovatno one koji rade pod Linuxom, pa čak i Solarisom. Ona se zasniva na neposrednom pristupu memoriji (DMA), a to je sastavni deo standarda FireWire i USB.

U osnovi postoje dva načina za prenošenje informacija između računarskih sistema i spoljnog sveta. Prvi je poznat kao programirani ulaz/izlaz (Programmed I/O, PIO), i za njega je karakteristično da centralna procesorska jedinica računara pažljivo kopira svaki bajt memorije i prenosi ga između spoljnjeg sveta i računara.

DMA, s druge strane, koristi „masovno" prenošenje podataka za premeštanje blokova informacija u memoriju računara i iz nje. U računarima koji koriste DMA, centralni procesor podešava prenošenje podataka i zatim se vraća izvršavanju ostalih poslova. Disk ili neki drugi uređaj koji podržava DMA sam aktivira prenošenje podataka kada za to postane spreman, a po obavljenom prenosu se centralnom procesoru šalje odgovarajuća poruka. Pošto su FireWire i USB projektovani u svrhu povezivanja brzih diskova, obe specifikacije imaju odredbe za DMA.

Mnogi stručnjaci za bezbednost računara uvideli su kolika je potencijalna opasnost od korišćenja DMA za napade preko FireWire ili USB veze u vidu „otvorenih vrata". Majkl Beker, Maksimilijan Dornzajf i Kristijan N. Klajn su na konferenciji CanSec West '05 prikazali zloupotrebu DMA očitavanja proizvoljne memorijske lokacije na računaru s FireWire interfejsom, a za to su koristili iPod koji radi pod Linuxom. Preko svog prilagođenog iPoda oni su preuzeli kopiju sadržaja ekrana računara žrtve – i to ne samo bez dozvole operativnog sistema već i bez njegovog saznanja!

Suštinski problem u osnovi svih ovih napada jeste činjenica da su programeri u Microsoftu, Appleu i drugim kompanijama verovali da je računarski hardver nesporno pouzdan. Projektanti nisu ni pretpostavljali da se iPod ili USB memorijski uređaj povezan s računarom može oteti kontroli i poslužiti za napad na računar – zato savremeni sistemi i nisu zaštićeni od napada te vrste.

U okruženju visokog stepena zaštite ima smisla „začepiti" USB i FireWire priključke, ali za većinu aplikacija korisnost tih tehnologija je verovatno vredna rizika. ■

Relja Jović je glavni i odgovorni urednik časopisa Mikro. *Njegove uvodne reči pročitajte na adresi www.mikro.co.yu/arhiva/relja.*