Predgovor

Dugo smo razmišljali o tome kakav treba da bude predgovor za ovu knjigu. Ne sviđaju nam se uobičajeni i standardni predgovori, a ne znamo kako će biti prihvaćeno neobičnije rešenje. Sigurnost ne trpi uštogljen pristup. Opet, neki iskusni autori su rekli da se predgovor i zaključak pišu na kraju pisanja knjige, kad se vidi kako ona otprilike treba da izgleda. Tako i činimo. Knjigu počinjemo navođenjem zanimljivog razgovora koji otvara pitanja obrađena u knjizi, a koji je vodio jedan od autora knjige pre skoro deset godina. Tada su banke počele da otvaraju svoja vrata pristupu preko Interneta, što znači da je započela era elektronske trgovine. Rukovodilac ugledne finansijske institucije – koga ćemo zvati Direktor XY – čuo je kojom se oblašću autor ZW bavi, pa ga je pozvao da popričaju o mogućoj saradnji. Deo razgovora tekao je otprilike ovako (izmenenjeni su mnogi detalji radi očuvanja privatnosti i u želji da se niko ne prepozna u ovoj priči):

- *Direktor XY:* Čuo sam da je sada trend u svetu da se korisnicima omogućava da preko Interneta gledaju stanje računa, plaćaju, kupuju?
- *Autor ZW:* Da, dobro ste čuli, i taj trend će se nastaviti. Treba da razmislite i da budete među prvima kod nas u tom pogledu.
- *Direktor XY:* Ali kako, zar to nije nesigurno. Pa neko će da napravi rusvaj, prebaciće pare na drugi račun, uništiće nas. Pući će bruka, reputacija će biti ugrožena.
- *Autor ZW:* Da, to je realna opasnost. Morate da vodite računa o zaštiti podataka i sigurnosti.
- *Direktor XY:* Pa kako, kako da budem siguran da se to neće desiti? Šta treba da kupim za to. Neki hardver, softver? Možete li mi predložiti?
- *Autor ZW:* Pa... stvar nije tako jednostavna... znate.
- *Direktor XY:* Hm... znam da nije jednostavna, znam da to košta. Ali izašao bih na upravni odbor, mi bismo odvojili novac da kupimo šta nam treba.
- *Autor ZW:* Hm... pa to jeste, ali nije samo to. Treba tu još stvari jer sigurnost nije nešto što se kupuje tako lako.
- *Direktor XY:* Čekajte... kako to mislite, kako ne može da se kupi?
- *Autor ZW:* Pa znate, trebaju vam i ljudi koji se u to razumeju, trebaju vam procesi, procedure. Sigurnost nije ni proizvod ni usluga, ni aktivnost, ni završno stanje – već sve to i još ponešto.
- *Direktor XY*: Hm... kako sad to? Možete li mi to reći jednostavnije, znate, ja nisam tehničke struke.

- *Autor ZW:* Pa ne morate biti tehničke struke. Vi ste bankar. Recite mi kako ste zaštitili svoj stan i auto?
- *Direktor XY:* Imam alarm i osigurao sam se kod osiguravajućeg društva.
- *Autor ZW:* A kako ste osigurali filijale svoje banke, kako centralu?
- *Direktor XY:* Imam obezbeđenje (ljude koji čuvaju), imamo ponegde kamere, imamo dugme za uzbunu, povremeno organizujemo obuku za ljude, imamo još neke sisteme.
- *Autor ZW:* Da li mislite da ste sigurni, tj. da li ste sigurni da vam niko neće obiti stan, ukrasti auto, opljačkati banku i pored svih tih mera?
- *Direktor XY:* Hm... pa nadam se da neće. Ali... nisam siguran, može da se desi. Može.
- *Autor ZW:* Eto odgovora, i ovde nikada nećete biti sigurni.
- *Direktor XY:* Hm... vidiš, da. Znači, ozbiljna stvar je u pitanju.
- *Autor ZW:* Da vrlo ozbiljna i trajna. Trebaju vam mnoge stvari da biste bili sigurni, ali nikad nećete biti 100% sigurni da ste sigurni.
- *Direktor XY:* A ljudi? Gde da nađem kadrove koji se u to razumeju, koja škola ih školuje?
- *Autor ZW:* Hm... teško pitanje; na raznim mestima ljudi pomalo uče o tome, ali u ovom trenutku... nesistematično i nedovoljno, čini mi se.
- *Direktor XY:* A ovi hakeri, mogu li oni pomoći?
- *Autor ZW:* I mogu i ne mogu. Zavisi koji i kakvi. Neki vole da budu destruktivni, neki vole da pomognu. Ima ih raznih.
- *Direktor XY:* Znači moram da pazim koje uzimam.
- *Autor ZW:* Pa... da, i to dobro da pazite.
- *Direktor XY:* A kako da znam da će baš da napadnu moju banku. I kada i kako će da je napadnu, kada je najveći rizik? I koliki je rizik?
- *Autor ZW:* Da, vama treba i procena rizika.
- *Direktor XY:* Mogu li moji ljudi iznutra da mi naprave problem, neko je recimo nezadovoljan platom ili recimo ode iz firme i hoće zbog nečega da se sveti.
- *Autor ZW:* Da, itekako. I to je čest slučaj.
- *Direktor XY:* Ima li knjigâ o tome, da se malo obrazujem?
- *Autor ZW:* Ima dobrih stranih knjiga, uglavnom na engleskom.
- *Direktor XY:* Ali ja ne znam engleski, učio sam ruski u školi i pomalo znam francuski.
- *Autor ZW:* Pa... spremamo se da napišemo knjigu na srpskom... Dobra ideja...

Ovaj razgovor je podstakao mnoga razmišljanja o sigurnosti. Nekada su se ovim problemima bavile vojska, diplomatija, policija, vlade. Sada to postaje problem svih, pa i privatnih lica koja obavljaju bankarske transakcije sa svog računa ili

kupuju preko Interneta. Da, to je večita borba lopova i policajaca. Večita borba interesa i suprotstavljenih strana. Onaj ko se opusti u toj borbi, rizikuje da izgubi. Napadač ima brojne prednosti, a najveća prednost je faktor iznenađenja, tj. mogućnost izbora vremena, mesta i načina napada. Onaj ko brani neki sistem mora da bude spreman uvek, na svakom mestu i za sve načine napada. To je neravnopravna borba, slična borbi u ratu. Poseban problem je nepoznavanje oblasti i nedostatak kadra. Kadrove su školovale samo vojska i policija (barem kod nas) i to na indirektan način. U međuvremenu su to počeli da rade i „obični" civilni fakulteti, prateći potrebe industrije i različitih institucija i organizacija. Računarski sistemi i mreže postali su važan (često i najvažniji) deo infrastrukture mnogih proizvodnih, upravnih, finansijskih i vojnih sistema. Ugrožavanje njihove sigurnosti, tj. neovlašćeno pregledanje, menjanje ili oštećivanje podataka, programa, servera, radnih stanica, prenosnih puteva ili drugih resursa, opasnost je s kojom se susreću gotovo svi koji su na bilo kakav način uključeni u razvoj, uvođenje, upotrebu ili održavanje ovakvih sistema.

Kome je namenjena ova knjiga (ili „da li je ova knjiga za mene?")

Osnovni deo ove knjige je rezultat predavanja i vežbi iz predmeta Sigurnost računarskih mreža koja se drže u Višoj elektrotehničkoj školi u Beogradu. Knjiga je prvobitno bila namenjena studentima koji prate nastavu iz tog predmeta, kako bi se osposobili za izvršavanje praktičnih zadataka koji ih čekaju po završetku studija. Kasnije smo ustanovili da je ovakva literatura potrebna i mnogim inženjerima, tehničarima, administratorima, programerima i običnim korisnicima računara – dakle, svima koji se profesionalno ili amaterski bave računarima i računarskim mrežama, a žele da shvate problem sigurnosti. Iako većim delom prati predavanja iz predmeta Sigurnost računarskih mreža, knjiga sadrži šira objašnjenja nekih tema, kao i dodatne teme koje se ne izlažu na predavanjima.

U ovoj knjizi nećete naći uputstva za pisanje virusa, crva i trojanskih konja, postupna objašnjenja za pljačkanje bankomata i krađu podataka s komšijinog računara. Knjiga od vas neće napraviti vrhunskog kriptoanalitičara ili hakera s crnim šeširom, tj. osobu koja može zaobići mrežnu barijeru i upasti u tuđu mrežu. Razlozi zbog kojih smo se odlučili na takav korak su sledeći:

[1] Nijedna knjiga iz ove oblasti ne može da obradi sve teme i dileme, pa smo sigurni da ćete se zapitati zašto ovde nema ni reči o „tome i tome". Odgovor je: „Zato što bi u tom slučaju knjigu bilo teško nositi". Područje sigurnosti je toliko široko da je vrlo teško napraviti ispravan izbor tema o kojima treba pisati. Ono što je nekome vrlo važno, drugome može biti skoro beznačajno i obrnuto.

[2] Pisali smo s namerom da vas uvedemo u područje sigurnosti, predstavimo osnovne sigurnosne usluge i zaštitne mehanizme i da vas obučimo kako da zaštitite svoj računar, mrežu, izvorni kôd ili bazu podataka. Jednostavnije – cilj nam je bio da čitaoce naučimo kako da zaštite svoju imovinu, a ne kako da napadaju tuđu. Ukoliko želite da zloupotrebite stečena znanja, preporučujemo da najpre pročitate pravne aspekte opisane u 14. poglavlju (da, crni šešir vas može odvesti u zatvor) i dobro razmislite da li vam se zaista isplati da to radite. Autori se u svakom slučaju ograđuju od mogućih zloupotreba znanja koje čitaoci steknu i ne mogu da prihvate nikakvu odgovornost za eventualne posledice takvih zloupotreba.

Odricanje od odgovornosti

Prilikom pripreme ove knjige, korišćena je raznovrsna literatura u „papirnom“ i elektronskom obliku (sa Interneta). Autori su učinili sve napore da podaci koji su izneti u knjizi budu tačni i da se izbegnu greške. Iako su autori sve opisane postupke, algoritme i metode proverili praktično i/ili pomoću više različitih izvora, moguće je da u knjizi postoje izvesni previdi, nepreciznosti i nepravilnosti. Izdavač i autori ne prihvataju bilo kakvu odgovornost za eventualne greške i omaške, kao ni za posledice koje mogu nastati zbog primene saznanja iz ove knjige ukoliko se kasnije ispostavi da su netačna.

Autori takođe upozoravaju da se saznanja stečena proučavanjem ove knjige mogu primeniti destruktivno. Od naših studenata i drugih čitalaca ove knjige zahtevamo da saznanja isključivo primene za odbranu, a nikako za napad (osim strogo kontrolisanih napada u cilju provere sigurnosti). Takođe, upozoravamo da se neka dostignuća navedena u ovoj knjizi ne smeju proveravati u proizvodnim i poslovnim okruženjima, tj. u okruženjima u kojima se primenom ovih mera može naneti bilo kakva šteta. Svi eksperimenti i probe namenjeni su isključivo za laboratorijsko tj. ispitno okruženje.

Autori su prilikom pisanja knjige pokušali da budu u toku s najnovijim dešavanjima u oblasti sigurnosti i u oblasti savremenih tehnologija. Međutim, sigurnost je oblast koja se stalno razvija. To znači da će s vremenom softver opisan u ovoj knjizi zastareti, da će postojati novije verzije koje ovde nisu pomenute (na primer, moguće je da u vreme dok čitate knjigu bude aktuelna verzija 6 programa True Crypt) ili da će prestati da se razvija, i da će neki algoritmi, postupci ili metode biti izmenjeni ili zamenjeni novima (na primer, NIST je objavio konkurs za novu heš funkciju koja treba da postane zvanični heš standard). Slično, neke Web stranice će biti uklonjene ili izmenjene, a *on-line* resursi nedostupni ili zamenjeni novim. Autori ne mogu prihvatiti odgovornost za sadržaje i/ili nedostupnost resursa na koje ova knjiga upućuje.

Da pojednostavimo – autori se ograđuju od:

- zloupotreba znanja koja su stekli čitaoci
- neugodnosti koje mogu nastati prilikom primene stečenih znanja
- nepravilnog korišćenja saznanja stečenih iz ove knjige
- posledica nepreciznosti i/ili grešaka u ovoj knjizi
- sadržaja resursa (Web stranice, knjige, softver, hardver) na koje ova knjiga upućuje, i mogućih posledica bilo kakve upotrebe tih resursaa

Zahvalnosti

Zahvaljujemo svima koji su nam na bilo kakav način pomogli prilikom izrade ove knjige. Posebno se zahvaljujemo našim studentima koji su ukazivali na nejasnoće i propuste u našim prethodnim izdanjima, i tako su pomogli da tekst poboljšamo i učinimo jasnijim i razumljivijim, i da otklonimo greške i nepreciznosti. Neki od naših studenata pomogli su tako što su ukazali na zanimljive resurse i izvore, i tako što su delovi njihovih seminarskih i diplomskih radova iskorišćeni pri obradi nekih tema.

Knjiga je napisana u paketu OpenOffice.org (`http://http://www.openoffice.org/`). Vektorske slike su rađene pomoću programa Inkscape (`http://www.inkscape.org/`) i DIA (`http://www.gnome.org/projects/dia/`). Rasterske slike su retuširane u programu GIMP (`http://www.gimp.org/`). Navedeni programi su besplatni, postoje verzije za Linux i Windows i mogu se preuzeti sa Interneta. Na ilustracijama su korišćeni šabloni iz programskog paketa Microsoft Visio 2003 i familija fontova Franklin Gothic. U knjizi su korišćeni fontovi: Franklin Gothic, Birka, Letter Gothic Pitch i Symbol. Nemanja Maček koristi OpenSuSE distribuciju Linuxa (`http://www.opensuse.org/`). Autori se zahvaljuju svima koji su zaslužni za razvoj besplatnog softvera i softvera sa otvorenim kodom, kao i onima što su obezbedili besplatne resurse koji su na neki način iskorišćeni u pripremi ove knjige ili pomenuti u ovoj knjizi. Hvala svima!

Autori