„Kniha o rozsahu 130 stran kompletně pokrývá základní problematiku metod a technologií používaných při autentizaci a autorizaci používaných při elektronických platebních transakcích. Zpracována byla kolektivem 13 odborníků. Literatura psaná tolika autory obvykle trpí stylistickou nevyvážeností textu, zde byla různorodost autorů sjednocena tak, že příručka tento nedostatek nemá. Tematicky je unikátní, v oblasti počítačové bezpečnosti v České republice nebyl dosud obdobný titul zpracován.

První kapitola uvádí základní terminologii v dané vědní oblasti a seznamuje se základními problémy, které je v ní třeba řešit. Správně klade důraz na vysvětlení rozdílu mezi autentizací a autorizací. Již od této úvodní kapitole se až úzkostlivě dbá na používání správných a přesných pojmů a termínů (v příručce se například nevyskytuje dnes často používaný verbální paskvil autentifikace).

Druhá kapitola je věnována trendům vývoje autentizačních metod. Uživatelé se v ní dozví řadu informací: principy slabé a silné autentizace uživatelů, jak hesla ukládat, co jsou jednorázová hesla, autentizační tokeny, třífaktorová autentizace i certifikáty, jaké jsou výhody a nevýhody čipových karet i autentizačních kalkulátorů a jak souvisejí biometriky s kryptografií. Pro popis základních autentizačních protokolů včetně Kerberosu byly použity formální metody, samotné kryptografické operce nejsou v příručce popisovány, implicitně se předpokládá jejich znalost čtenářem. Tyto znalosti mu zde prakticky ilustrují údaje o časových průbězích různých kryptografických operací potřebných pro čipovou kartu k výpočtu podpisů a jejich verifikací. Velká část kapitoly je věnována bezpečnostnímu hardwaru. S hlubokou znalostí věci jsou zde shrnuty bezpečnostní požadavky na kryptografické moduly, srovnány příslušné normy a podrobně klasifikovány útoky na bezpečnostní hardware a hodnocena odolnost běžného hardwaru proti různým třídám útoků.

Jádrem práce je třetí kapitola, věnovaná současným řešením autorizace některých platebních operací. Svědčí o tom i její rozsah skoro čtyřiceti stránek. Jsou zde klasifikovány elektronické platby, popsány způsoby autorizace bankovních operací a systémů pro podporu karetních plateb a uvedena specifikace EMV (Europay-Mastercard-Visa) a příslušných bezpečnostních mechanizmů. Mimořádně kvalitně je zde provedena analýza bezpečnosti používání čipových karet tohoto typu v praxi. Při rozboru slabin zde byly velmi dobře využity zkušenosti ze zahraničních studií a stáží (například na str. 60). Atraktivnost příručky jistě zvýší přehled konkrétních autentizačních metod používaných v bankovnictví ČR a popisy praktických experimentů při testování PIN-mailerů používaných čtyřmi českými bankami.

Čtvrtou, závěrečnou kapitolou výklad příručky graduje – čtenář se dozví aktuální metody zvyšování stupně kontroly a zabezpečení transakcí, jak vlastnosti karet a terminálů vylepšovat a testovat a jak realizovat změny v zaužívaných postupech u plateb.

Celkově hodnotím příručku velmi pozitivně; je nabita hodnotnými informacemi, dobře se čte a efektivně jsou v ní využívány faktografických tabulky a ilustrativní obrázky. V příručce byly uplatněny zkušenosti autorů ze zahraničních působení i konkrétní informace získané ve výzkumu a různých experimentech prováděných v České republice. Doporučuji, aby v budoucnu byla na základě oponovaného materiálu zpracována celostátní učebnice.“

Doc. Ing. Jaroslav Dočkal,CSc., Univerzita obrany, Brno