„Jedná se o zcela ojedinělou a výjimečnou publikaci. Obsahuje téměř kompletní přehled metod a technologií používaných při autentizaci a autorizaci používaných při elektronických platebních transakcích.

Na závěr první kapitoly, která seznamuje čtenáře se základní terminologií z oblasti autentizace (včetně srozumitelného popisu biometrické autentizace) a autorizace, je první z cenných partií této příručky s konkrétním popisem a zejména kritikou současného stavu (ne)bezpečnosti platebních systémů.

Stejnou přednost má i druhá kapitola. Přehled základních metod autentizace obsahuje i fundovaný popis biometrické autentizace a krátkou zmínku o jedné z více faktorových autentizací. Následující popis autentizace pomocí certifikátů je speciálně zaměřen právě na platební transakce. Podobně je orientován i úvod do problematiky bezpečného hardwaru s popisem kryptografických modulů, příslušnými bezpečnostními požadavky a konečně cenným přehledem útoků na bezpečný hardware a to jak logickým, tak i fyzickým, včetně klasifikace útočníků podle jejich schopností a možností a včetně popisu několika vybraných příkladů a hlavních technik útoků.

Hlavní část publikace je pochopitelně věnována vlastní autorizaci platebních transakcí. Po klasifikaci elektronických plateb, způsobů autorizace bankovních operací a systémů pro podporu karetních plateb následuje popis specifikace EMV (Europay-Mastercard-Visa) a příslušných bezpečnostních mechanizmů. Zvláště cenná je analýza bezpečnosti používání čipových karet tohoto typu v praxi. Zde uvedené slabiny tohoto systému a doporučení pro jejich odstranění jsou založeny hlavně na několikaletých zkušenostech z jejich používání ve Velké Británii. Analýza je oboustranná, tj. jak z pohledu bank, tak i z pohledu zákazníka,a je doplněna popisem dnes již klasického brněnského experimentu. Zvláštní pozornost je věnována platebním transakcím

Další kapitola je srozumitelným popisem elektronického bankovnictví (internet-banking, tele-banking,…). A opět po popisu základních principů a analýze slabých míst následuje zajímavý přehled možných útoků z pohledu uživatelů. Ten postupně graduje až k popisu více i méně známých způsobů znuežití platebních terminálů.

Samotný popis různých typů útoků by ale byl velice pesimistickým závěrem skript. Naštěstí je poslední rozsáhlá kapitola věnována velice podrobnému přehledu technik, kterými výrobci karet na známé útoky reagují. Snad jen větší zdůraznění typů útoků a prostředí, resp. situace, pro které jsou jednotlivé obranné techniky navrhovány, chybí k úplné dokonalosti.

Celá publikace obsahuje velké množství fundovaných informací, která takto pohromadě nelze asi nikde jinde nalézt. Vzhledem k objemu těchto velmi užitečných informací by bylo záhodno, aby se z publikace časem vyvinula objemnější monografie – základní učebnice pro obor informační bepečnosti.“

V. J. Jákl, Univerzita Karlova