

Na vzniku knihy se podílel kolektiv autorů z Masarykovy univerzity, Vysokého učení technického v Brně, společnosti Monet+ a dalších institucí pod vedením V. Matyáše a J. Krhovjáka.

Doc. RNDr. **Vašek Matyáš**, M. Sc., Ph.D. působí na Fakultě informatiky Masarykovy univerzity. Je vedoucím Katedry počítačových systémů a komunikací. Věnuje se aplikované kryptografii, bezpečnosti IT a ochraně informačního soukromí. Podílel se na výzkumu a vývoji pro akademické, průmyslové i státní instituce v České republice, Velké Británii, Irsku, Švýcarsku a Kanadě; na vývoji Společných kritérií a norem ISO/IEC. Je členem redakční rady časopisu Data Security Management.

Mgr. et Mgr. **Jan Krhovják** je PhD studentem Fakulty informatiky Masarykovy univerzity. Zabývá se bezpečností v IT. Mezi hlavní oblasti jeho zájmu patří bezpečný (kryptografický) hardware, bezpečnost v mobilních výpočetních prostředích a generování kryptografického materiálu z hesel a náhodných či pseudonáhodných sekvencí.

Dalšími autory jsou:  
Mgr. **Václav Lorenc**, Mgr. **Marek Kumpošt**, Ing. Mgr. **Zdeněk Říha**, Ph.D., Doc. Ing. **Daniel Cvrček**, Ph.D., Doc. Ing. **Jan Staudek**, CSc., Doc. Dr. Ing. **Petr Hanáček**, Ing. **Pavel Hendrych**, Ing. **Miroslav Janda**, Mgr. **Vlastimil Holer**, Mgr. **Kamil Malinka**, Mgr. **Petr Švenda**, Mgr. **Andriy Stetsko**.

„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.“

RNDr. Vojtěch Jákl,  
Univerzita Karlova, Praha

„Tematicky je kniha unikátní, v dané oblasti nebylo dosud nic napsáno na žádné vysoké škole v České republice.

Knih je nabitá hodnotnými informacemi; dobře se čtou a efektivně jsou v nich využívány faktografické tabulky a ilustrativní obrázky. V publikaci byly uplatněny zkušenosti autorů ze zahraničních působení i konkrétní informace získané ve výzkumu a různých experimentech prováděných v České republice“.

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

Vašek Matyáš, Jan Krhovják a kolektiv Autorizace elektronických transakcí a autentizace dat i uživatelů

# Autorizace elektronických transakcí a autentizace dat i uživatelů

Vašek Matyáš  
Jan Krhovják  
a kolektiv

MASARYKOVA UNIVERZITA

Publikace je mimořádná v tom, že pokrývá kompletně základní problematiku metod a technologií používaných při autentizaci uživatelů i dat a autorizaci při elektronických platebních transakcích.

První kapitola seznamuje čtenáře se základní terminologií z oblasti autentizace (včetně srozumitelného popisu biometrické autentizace) a autorizace. Závěr kapitoly obsahuje první z cenných partií této knihy 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 knihy je věnována 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 mechanismů. Zvláště cenná je analýza bezpečnosti používání čipových karet tohoto typu v praxi. 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 bankovníctví (internet-banking, tele-banking, ...). 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 zneužití platebních terminálů.

Poslední rozsáhlá kapitola je věnována velice podrobnému přehledu technik, kterými výrobci karet na známé útoky reagují.