

OBSAH

PŘEDMLUVA	7
1. ÚVOD DO PROBLEMATIKY	9
1.1 Autentizace uživatelů	9
1.1.1 Základní terminologie	9
1.1.2 Základní metody autentizace uživatelů	10
1.1.3 Ověření (držení) tajné informace použitím kryptografických protokolů	11
1.1.4 Řetězce důvěryhodných autorit	11
1.2 Autorizace finančních transakcí	12
1.3 Bezpečnost platebních systémů	13
2. TRENDY VÝVOJE AUTENTIZAČNÍCH METOD	15
2.1 Principy slabé a silné autentizace uživatelů	15
2.1.1 Hesla (jejich ukládání) a jednorázová hesla	16
2.1.2 Autentizační tokeny	19
2.1.3 Biometrie	21
2.1.4 Třífaktorová autentizace	25
2.1.5 Certifikáty	26
2.1.6 Protokoly výzva—odpověď a eskalační protokoly	27
2.2 Úvod do problematiky bezpečného hardwaru	32
2.2.1 Základní terminologie a pohled na bezpečnost	32
2.2.2 Vnitřní architektura HSM	35
2.2.3 Bezpečnostní požadavky na kryptografické moduly	38
2.3 Útoky na bezpečný hardware	42
2.3.1 Základní kategorizace jednotlivých útoků	42
2.3.2 Klasifikace útočníků a odolnost bezpečného hardwaru vůči útokům .	45
2.3.3 Vybrané techniky útoků na fyzickou bezpečnost	46
2.3.4 Vybrané techniky útoků na logickou bezpečnost	51
3. SOUČASNÁ ŘEŠENÍ AUTORIZACE NĚKTERÝCH PLATEBNÍCH TRANSAKČÍ	57
3.1 Elektronické platby	57
3.1.1 Rozdělení platebních karet	57
3.1.2 Elektronická peněženka	58
3.1.3 Přímé bankovníctví	61
3.1.4 Elektronický obchod	61
3.2 Autorizace bankovních operací	64

3.2.1	Podpis držitele karty	64
3.2.2	Autorizace pomocí PINu	64
3.2.3	Autorizace plateb pomocí elektronického podpisu na bázi PKI	65
3.2.4	Autorizace pomocí SMS jednorázového hesla	65
3.2.5	Autorizace pomocí biometrie	65
3.3	Systémy pro podporu karetních plateb	66
3.3.1	HSM, bankomaty a platební terminály	66
3.3.2	Základní architektura ATM a EFT sítí	67
3.3.3	Platební karty a základní používané autorizační metody	70
3.4	Bezpečnost platebních karet a přechod na EMV	71
3.4.1	Základní struktura specifikace EMV	71
3.4.2	Offline autentizace dat	72
3.4.3	Autentizace uživatelů	74
3.4.4	Automatická analýza rizik	75
3.4.5	Online autorizace transakcí	75
3.4.6	Certifikační autority	76
3.4.7	Bezpečnost EMV v praxi	76
3.4.8	Další bezpečnostní dopady EMV	77
3.4.9	Závěrečné zhodnocení	78
3.5	Internet-, GSM-, PDA- a TELE-bankovníctví	78
3.5.1	Základní přístupy používané bankami při autentizaci uživatelů	78
3.5.2	Dodatečné metody autorizace transakcí	81
3.5.3	Řešení elektronického bankovníctví v zahraničních bankách	83
3.6	Útoky na platební transakce z pohledu uživatelů	85
3.6.1	Nejčastější typy útoků	85
3.6.2	Experiment zabývající se autorizací bezhotovostních plateb	86
3.6.3	Bezpečnost PIN-mailerů a další aspekty autentizace	91
3.7	Problematika nedůvěryhodných terminálů/obchodníků	99
3.7.1	Dobré bezpečnostní zásady a znesnadňování útoků	101
4.	JAK NA ZVÝŠENÍ STUPNĚ KONTROLY A ZABEZPEČENÍ TRANSAKČÍ?	103
4.1	Vylepšování vlastností karet a terminálů	104
4.1.1	Použití nových technologií vedoucí ke zlepšení ochrany citlivých dat uložených na kartě	104
4.1.2	Důkladné testování karet v době návrhu	108
4.1.3	Použití lépe navržených kryptografických protokolů	110
4.2	Kombinované (super)tokeny	110
4.3	Aspekty pro realizaci změn v zaužívaných postupech u plateb	115
	POUŽITÁ LITERATURA	117
	REJSTRÍK	123