Oponentní posudek diplomové práce

MIKA, Pavel. Aplikace kryptografie v informačních systémech: Application of cryptography in information systems. Praha, 2013-08-XX. 64s. Diplomová práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí diplomové práce prof. RNDr. Jiří Ivánek, CSc.

Práce se věnuje kryptologii a informační bezpečnosti.

V 1. kapitole autor zavádí základní pojmy jako kryptosystém, šifrovací algoritmus, sdělovací kanál. 2. kapitola uvádí známé způsoby útoků na kryptosystémy.

Ve 3. kapitole autor probírá symetrické kryptosystémy. Přehledně shrnuje nejpoužívanější algoritmy DES, AES a Blowfish, u kterých uvádí i diskusi možných útoků.

Ve 4. kapitole autor obrací pozornost ke kryptosystémům asymetrickým. Nejprve přehledně prezentuje matematické principy těchto kryptosystémů a uvádí prostředky informační bezpečnosti, které jsou asymetrickou kryptografií podporované: elektronický podpis a navazující systém digitálních certifikátů jakožto prostředku pro zajištění důvěry a také protokol výměny tajného klíče.

Kapitolám 1-4 nelze nic vytknout. Dobře popisují známé a používané kryptosystémy, úroveň podrobnosti výkladu je pro účel práce naprosto vyhovující.

V 5. kapitole autor postupuje k výkladu pojmů informační bezpečnosti. Autor uvádí třístupňovou hierarchii: (1) bezpečnostní cíle, (2) bezpečnostní mechanismy a (3) kryptografické systémy. Uvádí přehledné schéma ilustrující, které bezpečnostní mechanismy lze použít pro naplnění jakých bezpečnostních cílů, a na druhé straně které bezpečnostní mechanismy jsou podporovány kterými kryptografickými systémy. V dalším výkladu autor dále diskutuje pojmy důvěrnost, dostupnost, integrita, autentizace, autorizace a nepopiratelnost, což jsou používané jak v kryptologii, tak v architektuře informačních systémů.

Zde je poněkud škoda, že práce neobsahuje žádný úvod ze strany informačních systémů. Bylo by tak zřejmější, jaký je charakter typických potřeb. Považuji to za nevyužitou příležitost, a to zejména vzhledem k příslibu, který je obsažen v názvu práce.

5. kapitola dále pokračuje stručným uvedením významných technických norem z oblasti kryptografie a informační bezpečnosti. Jde o dobře zpracovaný přehled.

V 6. kapitole autor přistupuje k hodnocení kryptografických algoritmů. Uvádí různá kritéria. V první části se soustředí výhradně na symetrické šifrovací algoritmy, u kterých uvažuje časovou náročnost, průchodnost, lavinový efekt a velikost paměti nutné pro implementaci algoritmu. Zde autor ponechává nejistotu, zda jde o velikost programového kódu v konkrétním programovacím jazyku, nebo o velikost operační paměti využívané algoritmem při jeho běhu. Druhá možnost je při hodnocení algoritmů obecně používanější.

Kapitola se dále věnuje dalším parametrům, jako jsou délka klíče, rok vytvoření algoritmu a doporučená délka klíče pro odolnost vůči různým kategoriím útočníkům. V kontextu aplikace kryptografických algoritmů v informačních

systémech jsou toto vlastnosti nejvýznamnější, neboť určují bezpečnostní životnost posuzovaného informačního systému.

Autor následně v oddíle 6.8 uvádí porovnání několika algoritmů na základě těchto vedlejších kritérií, přičemž se odvolává na dříve uvedené údaje. Tento oddíl má rozsah jedné půlstránky a sestává ze dvou krátkých odstavců. Jeho nadpis „Zhodnocení“ se jeví jako značně nepřesný. Není nikterak vymezen žádný kontext ani účel, se kterým by se k hodnocení přistupovalo. Není nijak odůvodněno, proč by autorem zvolená kritéria měla být rozhodující. Této části práce by evidentně prospěla dodatečná úvaha o východiscích, cílech a metodách, které by patrně vedly k významnému rozpracování. Autorovy schopnosti, které prokazuje na jiných místech práce, by na tento úkol nepochybně stačily.

V práci jsou citovány relevantní zdroje. Z technických norem jsou citovány patrně ty, které byly autorovi dostupné, což je v kontextu diplomové práce naprosto v pořádku. Jedinou výhradu mám k oddílu 6.6.2, kde je jen velmi vágně vymezena příslušná norma amerického normalizačního orgánu NIST, která specifikuje doporučené délky klíčů pro různé algoritmy.

Seznam použité literatury ve většině případů obsahuje reference dle normy ČSN ISO 690.

Nicméně seznam použité literatury čítající pouhých 32 položek je na hranici dostatečnosti. Odborné literatury pro oblast kryptologie a informační bezpečnosti existuje velké množství a znalosti lze čerpat z mnoha zdrojů. Práce, která si za cíl bere vyhodnocení a přitom nevychází z vlastních experimentů, by měla usilovat o používání údajů, které jsou ověřené, tj. např. potvrzené z více zdrojů.

Po stylistické stránce je práce zdařilá. Je psána spisovným jazykem, neobsahuje pravopisné chyby.

Výše uvedené výhrady k práci nejsou fatální. Její název je sice poněkud nadnesený, nicméně rozsah popsaný v abstraktu pokryt je a až na pokus o hodnocení algoritmů je zdařilý. Práci považuji za dostatečnou pro udělení magisterského titulu.
Navrhovaná známka: 2 (velmi dobře).

V Bruselu dne 9.9.2013

Dr. Jan Dvořák
Ústav informačních studií a knihovnictví FF UK