Oponentský posudek dizertační práce

Název práce: AUTENTIZACE S VYUŽITÍM LEHKÉ KRYPTOGRAFIE

Autor: Ing. Vlastimil Člupek

Oponent: Ing Stanislav Uchytil, Ph. D.

Obsahová strana práce

V současné době se telekomunikace stává součástí lidských životů prostřednictvím jednoúčelových chytrých blackboxu. Fenomén Internetu věcí je startující technické odvětví, které nás postupně začíná dokonale obklopovat. Proto je kladen důraz na nalezení nových bezpečných způsobů komunikace. Musí být navržena dostatečně robustní, ale zároveň výpočetně nenáročná. Poptávkou po principech a komunikačních protokolech se otevírá cele spektrum náročných návrhů a řešení přizpůsobených omezeným zdrojům IoT zařízení. V novém odvětví lehké kryptografie čeká spousta výzev k řešení.

Bezpečnost a nenáročnost na prostředky s dostatečným důrazem na autentizaci nízkonákladových zařízení je technicky a projektově náročné. Ing. Člupek úspěšně navrhl jednosměrný autentizační protokol se zabezpečeným přenosem dat. Dále navrhnul obousměrný autentizační protokol se zabezpečeným přenosem dat. V předposlední části práce realizoval návrh obousměrného autentizačního protokolu se zajištěním nepopiratelnosti. Poslední část práce popisuje provedení bezpečnostní analýzy u navržených protokolů.

Formální strana práce a studia

Dizertační práce Ing. Vlastimila Člupka má rozsah 113 stran textu včetně seznamu použitých symbolů a zkratek, literatury. Hlavní text je členěn na úvod popisující současný stav, cíle práce, tří části vlastního návrhu a diskuze. Odkazy z 226 různých citačních zdrojů svědčí o výborném rozsáhlém rozsahu nastudované problematiky. Práce je napsána srozumitelně a přehledně bez významných typografických a stylistických chyb.

Ing. Vlastimil Člupek během svého postgraduálního studia publikoval 2 autorské články v časopisech kategorie A (dle přiloženého Hodnoceni tvůrčích aktivit doktoranda), 9 spoluautorských prací v konferenčních sbornících. Všechny publikované práce jsou součástí předkládané disertační práce, čímž splňuje podmínku dostatečné publikační úrovně. Z předkládané práce a z celkové publikační aktivity je poznat hluboké znalosti v řešené problematice.

Otázky k obhajobě:

Na jakých konkrétních typech IoT zařízení je možné implementovat fyzicky neklonovatelné funkce?

Závěr

Za hlavní přínos práce považuji nalezení nových autentizačních protokolů jednosměrných i obousměrných, které jsou odolné vůči podvržené autorizaci a zároveň plní nedostatečný výpočetní výkon na straně IoT zařízení. Po prostudování všech dostupných materiálů **doporučuji předloženou disertační práci k obhajobě**.

V Brně 4.10.2016

Ing. Stanislav Uchytil, Ph.D.

Ing. S. Uchytil, Ph.D.