Posudek oponenta

Dizertační práce: Analýza a optimalizace datové komunikace pro telemetrické systémy v energetice

Autor: Ing. Radek Fujidiak

Oponent: Doc. RNDr. Tomáš Pitner, Ph.D.

Disertační práce si klade za cíl navrhnout optimalizační přístupy pro zabezpečení komunikace telemetrických systémů v energetice. Z tohoto pohledu je samotný název příliš obecný, neboť zaměření na bezpečnost explicitně nezmiňuje, to však není podstatné z hlediska splnění cílů.

V úvodu práce diskutuje současné problémy informační bezpečnosti, a metody, které vedou k jejímu zajištění. Soustředí se na oblast, kde jsou využívána zařízení s omezenými zdroji – především výpočetní výkon, operační paměť, a to často ve vazbě na omezenou kapacitu napájení (potřebu dlouhého provozu bez externího napájení). Zde v úvodu, resp. motivační části bých uváděl podrobnější rozbor architektur a funkcí inteligentních sítí v zvolené doméně, tzv. energetické, resp. distribuční, jelikož to zdále nezahrnuje jen telemetrii v úzkém slova smyslu. To by umožnilo přesněji definovat jejich mírné-funkční požadavky vč. bezpečnosti (ale také rychlost, dostupnost, robustnost, nákladovost, vůči ním že se potom optimalizuje).

V úvodní kapitole autor poměrně přehledně popisuje i právní prostředí, a to nejen české, ale i evropské (EU), resp. obecné trendy – např. v ochraně osobních údajů, což je s kyberbezpečnosti často v (přijimajícím zdánlivěm) konfliktu. Výčet tří předpisů/strategií (GDPR, zákon o kyberbezpečnosti a EU 20-20-20) pokrývá sice to hlavní, ale ne jediné. Příjemnějším je podstatně ještě zákon o krizovém řízení z hlediska pojmut kritická infrastruktura, ale i další – kodyšny ENTSO-E, energetický zákon, zákon o elektronických komunikacích, nově i zákon o opatřeních ke snížení nákladů na budování vysokorychlostních sítí elektronických komunikací, dále vyhlášky a stanoviska ERÚ, případně zákon o ochraně útajovaných informací. Jedná se však o práci v oboru teleinformatika a pro stanovení motivace a cílů není detailní právní rozbor zásadní.

Hlavní část dizertační práce je následně věnována návrhu a optimalizaci vlastního hybridního kryptosystému. Jedná se o řešení, které dle autora nenaplňuje pouze jeden bezpečnostní princip (např. pouze autentičnost), nýbrž o řešení, které nabízí všechny požadované principy informační bezpečnosti v energetice. Je provedena analýza dnešních řešení, které jsou následně evaluovány vlastními měřeními i pomocí současné aktuální literatury. Tato část je celkově poměrně podstatná – autor dohledává, zda a kde v původní literatuře jsou opravdu závěry reprodukovatelné a přesvědčivé – a dopisuje k závěru, že často tomu tak nebyvá.

Návrh je logicky postaven na kombinaci symetrických a asymetrických kryptografických algoritmů. Jedná se o kombinaci symetrických blokových algoritmů elektronické kódu knihy (ECB), zajišťující autentičnost a integritu pomocí náhodných klíčů, řešení šifrovaného textu zajišťující důvěrnost, společně s algoritmem Diffie-Hellman nad eliptickými křivkami zajišťující bezpečnou distribuci a výměnu symetrických tajných klíčů.


Nakonec jsou představeny originální výsledky výzkumu, který se zabýval vhodnou volbou křivek a studii jejich doménových parametrů z pohledu vztahu velikosti k rychlosti operaci nad křivkou.


Ohebně vlastní tvory, autor sepsal či se podílel na sepsání dostatku publikací, včetně kvalitních časopiseckých, kde impact factor dosahoval v oboru „obvyklých“ hodnot, tedy sice většinou pod 1, ale nezaznádatabelných. Všechny klíčové publikace jsou přímo relevantní k tématu disertace. Student neuvádí své podíly a všechny jsou ve spoluautorství, prosím tedy o komentář, jaký a v čem byl podíl autora – nejen
v sepsování výsledků, ale příp. i vedení dílčích výzkumných týmů, studentů, studentských prací a projektů atd. Toto proslužím u obhajoby napravit, stáči u hlavních prací.

Na jednotlivé články autora jsou v Google Scholar řádově jednotky ohlasů, celkově pak desítky. Slibně vypadá citovanost u článku, který pokrývá téma úzce související s disertací (byť ne 100%), a věnuje se kryptografii pro IoT. Celkově jsou hlavní publikované články k tématu disertace dostatečně relevantní.

Na práci hodnotím kultivování jazykového projevu, logickou výstavbu textu, dobrou byť stručnou argumentaci a čitivost textu. V textu se vyskytují gramatické chyby (skloňování přídavných jmen ve středním rodu u bohučeli i dosud překleplých a chybění většinou neohlášených kontrolou pravopisu) (nezprávný tvar slova, nesprávné psaní velkých písmen – Česká Republika místo republika). Text se rovněž dopouští přes použití kvalitního typografického nástroje drobných chyb, jako je užívání znaménka „minus“ ve smyslu rozdělovníku.

Možná je škoda, že text nevznikl v angličtině – řada publikací autora takových byla a rovněž disertace by se dala mezinárodně využít. Převzaté zdroje jako obrázky jsou řádně citované.

**Aktuálnost zvoleného tématu**

Téma práce je bezpochyby aktuální; zajištění fungování infrastuktury v energetice, kde je z povahy nutno zajistit bezpečné fungování a kde do budoucna bude stále větší část sítě kritickou infrastrukturou, resp. inteligentní síť, je extrémně důležitě a jakýkoli fundovaný ověřený původní přístup je přínosem. Současně je možné vyjít ze závěrů autora i v obecnější rovině aplikované kryptografie a využít přístupy jinde, kde je potřeba navrhovat kryptografický rámec/systém v prostředích s omezenými zdroji.

**Vzhledem k tématu a zpracování konstatuji, že práce spadá do doktorského studijního oboru Teleinformatika.**

**Splnění cílů disertační práce**

Disertační práce splnila vytčené cíle a předkládá je srozumitelnou formou s pouze menším nedostatky.

**Zvolené metody zpracování**


**Přínos pro další rozvoj vědy a techniky**

Doktorandovi se ve výzkumu a práci podařilo navrhnout kryptografický základ komplexního řešení pokrývající některé (ty podstatné) požadavky na bezpečnost.

Navržené schéma kryptografického zabezpečení komunikace je relativně jednoduché a aplikovatelné v prostředí, kde chybí výpočetní síla, paměťová kapacita i výkonné napájení, což je aspoň z části i situace v elektrických sítích, zejména v distribuci – chytré elektroměry, koncentrátoře atd.

Potřeby uváděné v cílech a motivací práce jsou nesporné. K praktickému uplatnění vede nicméně ještě nesmírně dlouhá cesta nejen z pohledu obtížnosti průniku do technologických řešení, která jsou již jíž děta vyvíjena a v provozu a jsou do nich nainvestovány velké objemy prostředků (firmare i hardware zařízení). Pro prosazení by bylo i třeba otestovat rozsáhlejší (hlavně co do počtu zařízení) systémy využívajících navržené kryptografie v alespoň laboratorním provozu.

Přínos je tedy jednoznačný hlavně v koncepční rovině – ohledně praktického nasazení by bylo třeba více času a jistě by se narazilo na zmíněné problémy se setrvačností výrobků, nedostatečné otestování nových přístupů atd.

**Kritický rozbor předností, nedostatků a připomínky**

Název práce mohl být explicitněji zaměřen na to, že je jedná o bezpečnostní aspekty komunikace. Rovněž zaměření na inteligentní síť v energetice mělo být i více podepřeno v úvodní části – lepší rozbor jejich
architektur a funkcí, z nichž plynou komunikační požadavky, klidně s tím, že by se autor věnoval jen telemetrické části, např. AMM a požadavkům na ně.

Úvodní část s popisem právních aspektů není na stejné úrovni jako části návazné. Zde bylo možné bud’to dopracovat vě. expertní konzultace v této oblasti nebo vynechat a nahradit odkazy na literaturu, hlavně k ochraně soukromí, z energetického práva, příp. standardy a doporučení v této oblasti.

Ohledně vlastního navrženého kryptosystému – a to se váže k požadavkům na něj – by nemělo chybět posouzení, jaký bude (by byl) výkonnostní přínos v reálných protokolech používaných v reálných telemetrických infrastrukturách (tedy AMM a standardy jako DLMS/COSEM vč. zabezpečení, příp. implementace IPsec).

Závěrečná drobná již zmíněná výtka jde na vrub pravopisným chybám a překlepům, těch je v textu celá řada, a to i v nadpisu. V textu jsou i chyby věcné, ale též spíše „překlepové“ charakteru, jako v definici kryptosystému (funkce E a D), neboť z dalšího je jasné, že to autor chápe správně.

Celkově uvedené nedostatky nepovažuji za klíčové a jsou vyváženy přínosy práce.

Při obhajobě práce doporučuji dizertantovi položit následující otázky:

- Tématem práce jsou telemetrické systémy v energetice, tedy zejména v distribuci elektřiny. Jsou v navržených postupech skutečně silná specifika pro tuto oblast nebo by je šlo přímo využít v jiných inteligentních sítích, příp. kde je ta hranice?
- Jaké lze očekávat odchylky ve výkonu celého systému, příp. jednotlivých algoritmů v případě využití jiného kontroléru než MSP430, např. obdobných jako v reálných zařízeních v inteligentní DS – chytré elektroměry, koncentrátoře? Srovnání s Raspberry Pi asi není adekvátní, nebo ano?
- Jaký byl podíl autora na hlavních dílech psaných převažně ve spolauautorství? Vedl autor „své“ dílčí tým(y) v rámci práce na projektu TACR?

Závěr:

Předložená dizertační práce pana Ing. Radka Fudiaka s názvem Analýza a optimalizace datové komunikace pro telemetrické systémy v energetice je v souladu s § 47 zákona č. 111/1998 Sb. o vysokých školách, a proto doporučuji předloženou dizertační práci k obhajobě.

V Brně 29.8.2017

Doc. RNDr. Tomáš Pitner, Ph.D. [Podpis]