Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK VEDOUCÍHO BAKALÁŘSKÉ PRÁCE

Jméno studenta: Daniel Ildža

Název práce: Šifrování komunikace v IP sítích

Autor posudku: Ing. Ondřej Hornig

Cíl práce: Cílem této bakalářské práce je obeznámit s možnostmi zabezpečení komunikace pomocí šifrování v IP sítích a navržení řešení pro zabezpečení datové komunikace v sítích energetické přenosové soustavy Smart Grid. Práce představuje referenční ISO/OSI model, Smart Grid, různé typy VPN a šifrovací algoritmy. V praktické části je popsán výběr vhodné VPN a určení požadavků na kryptografické metody pro použití k zabezpečení komunikace ve Smart Gridu na základě zákona o kybernetické bezpečnosti. Vzhledem ke zjištěným požadavkům je pak provedeno porovnání šifrovacích metod a je popsán jejich dopad na síťovou komunikaci.

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)			
	A	**C**	**E**	**F**
Práce svým zaměřením odpovídá studovanému oboru	☒	☐	☐	☐
Vymezení cíle a jeho naplnění	☒	☐	☐	☐
Zpracování teoretických aspektů tématu	☒	☐	☐	☐
Zpracování praktických aspektů tématu	☒	☐	☐	☐
Adekvátnost použitých metod, způsob jejich použití	☒	☐	☐	☐
Hloubka a správnost provedené analýzy	☒	☒	☐	☐
Práce s literaturou	☒	☐	☐	☐
Logická stavba a členění práce	☒	☐	☐	☐
Jazyková a terminologická úroveň	☐	☒	☐	☐
Formální úprava a náležitosti práce	☒	☐	☐	☐
Vlastní přínos studenta	☒	☒	☐	☐
Využitelnost výsledků práce v teorii (v praxi)	☒	☒	☐	☐

Dílčí připomínky a náměty:

Autor práce svůj postup pravidelně konzultoval, nemám žádné další připomínky.

Celkové posouzení práce a zdůvodnění výsledné známky:

Bakalářská práce se zabývá problematikou šifrování v počítačových sítí. Skládá se z 5 hlavních kapitol, z nichž první představuje úvod práce. Druhou kapitolu (teoretickou řást práce) člení autor na popis základních součástí ISO/OSI referenčního modelu, smart gridu a dále popisuje zabezpečení v sítích. V kapitole 2.4. se věnuje šifrovacím a hashovacím funkcím. Praktická část ve třetí kapitole pojednává o IPsecu a jeho možných nastaveních, která autor vzájemně porovnává. Poslední, pátá, kapitola představuje závěr práce se shrnutím dosažených výsledků.
Formální a stylistická úprava práce odpovídá platným metodickým pokynům pro vypracování závrečné práce. Obsahuje malé množství jazykových chyb. Práce je čtivá a vhodně doplněná obrázky a schématy. Autor pracoval převážně s hodnotnými a aktuálními zdroji, které vhodně využil v textu. Práce tak představuje kvalitní souhrn vytyčené problematiky
Cíle práce vytyčené byly naplněny. V praktické části student svým přínosem velmi zdařile představuje vybraný bezpečnostní problém a jeho vyřešení a popis považuji za velmi dobrý. Student velmi vhodně komponuje do práce aktuální zákonnou normu 181/2014 Sb. a předkládá ucelený souhrn doporučení včetně výkonových analýz na testovací topologii. Velmi kladně také hodnotím hluboký vhled do problematiky v teoretické části, kde jsou dopodrobna rozepsané jednotlivé šifrovací algoritmy.
Celkově je práce na vysoké úrovni a doporučuji ji k obhajobě.

Otázky k obhajobě:

Představte jednotlivé možnosti šifrování provozu vzhledem k jejich prolomitelnosti.
Jak je důležité pro IPsec tunely volit šifrovací klíče a interval jejich změny vzhledem k prolomitelnosti?

Práci doporučuji k obhajobě.

Navržená výsledná známka: A - výborně

V Hradci Králové**, dne** 15. května 2016

_____

podpis