FAKULTA EKONOMICKÁ
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI

Katedra ekonomie a kvantitativních metod

Oponentský posudek disertační práce

Autor práce: **Ing. Monika Borkovcová**

Název práce: **ANALÝZA A OPTIMALIZACE PŘÍSTUPOVÝCH OPRÁVNĚNÍ A MODELOVÁNÍ UŽIVATELSKÝCH ROLÍ**

Cíle práce včetně podcílů jsou přehledně definovány. Jako hlavní cíl si autorka vytýčila nalezení společných vzorců chování uživatelů v životním cyklu jejích identit a uživatelských přístupů na základě analýzy různých případových studií. K tomu je využita rozšířená formalizace popisu identit a definice odpovídajících přístupů. Tato formalizace je poté základem pro návrh a implementaci relevantních algoritmů.

Obsah a struktura práce

Disertační práce je členěna do 6 kapitol. V rešeršní části autorka popisuje různé přístupy k řízení informačních technologií, formuluje základní pravidla bezpečnosti a nakonec se soustředí na základní popis Role-Bassed Access Control (RBAC) jako hlavní řešení volitelného a povinného řízení přístupů. Klasifikuje různé modely systému RBAC a formálně specifikuje RBAC pomocí Z notace v syntaxi ANSI-RBAC. V této formalizaci se autorka dopouští drobných nepřesností, které však nemají větší vliv na pochopení definice komponent, ani principu hierarchického a omezujícího RBAC.

Součástí rešeršní části by mohla být i kritická diskuse, ze které vyplyne i vlastní přínos autorky práce k řešení dané problematiky. Toto není v práci zcela jasně uvedeno.

Práci by jistě prospěla explicitně a souhrnně popsaná metodika řešení problému. Tato metodika by podpořila také lepší provázanost mezi jednotlivými kapitolami.

Jedna ze stěžejních částí práce se zabývá formalizací popisů definice a pravidel pro práci s rolemi, které definují oprávnění pro přístup k vybraným prostředkům. Uvedené definice v podobě axiomů, které popisují význam navržených predikátů, jsou výchozím bodem ke konstrukci funkcí realizujících požadované operace propojení rolí a identit přes vybrané atributy. To vše tvoří rámec maximalizační úlohy ke konstrukci množiny rolí dané kardinality pokrývající maximální počet identit, stejně minimalizační úlohy hledající minimální počet rolí, které pokrývají zadanou množinu identit. Vytvořené axiomy jsou velmi precizně zpracovány. Autorce lze pouze doporučit zpřesnit a ujasnit slovní popis jednotlivých axiomů, popř. definovaných úloh zejména s ohledem na použití množin objektů a objektu z množiny objektů (např. account vs. accounts), dále lze věnovat více pozornosti přesné syntaxi pravidel a pořadí použitých definic (např. hojně používanou definici DOM najdeme až v následujících podkapitolách v popisu převodu na kvantifikovanou booleovskou proměnnou, BI predikát

není definován vůbec). Toto není vždy i s ohledem na precizní popis ostatních objektů a pravidel zcela přesné a tím i ne zcela pochopitelné. Nicméně uvedené nepřesnosti nemají vliv na celkové pochopení významu a funkce použitých axiomů.

V další části se práce zabývá popisem návrhových implementačních vzorů diskutovaných autorizačních systémů a jejich provázáním s výstupními katalogy uživatelských rolí získanými aplikací navržených maximalizačních a minimalizačních algoritmů. Popsané propojení je výchozím bodem pro praktické nasazení v typově různých organizacích z realizovaných případových studií. S ohledem na způsob popisu a použité prostředky není deklarované propojení z předloženého textu vždy zcela zřejmé.

V poslední části se práce zabývá výstupy z realizovaných případových studií, které mimo jiné popisují častý nesoulad mezi pracovní náplní uživatelů a jejich systémovými oprávněními. Současně řeší s využitím změnového vektoru udržitelnost požadovaného katalogu rolí a souladu mezi pracovními a systémovými rolemi uživatele během jeho životního cyklu.

Obě dvě poslední části působí ve srovnání s řešením problematiky efektivního pokrytí rolemi spíše jako doplněk a zejména implementace navržených algoritmů do systémů organizací z případových studií může být popsána šířeji a jasněji.

Úroveň zpracování práce, přínos práce

Práce je psána odborným jazykem, který odpovídá problematice práce. Na několika místech nevhodné formulace, nesprávně použité slovní tvary, jiná slova vnucena automatickou korekcí textu a chybějící předložky snižují srozumitelnost a stěžují pochopení textu. Po grafické stránce je práce zpracována v souladu s požadavky na práci kladenými. Přínosem práce je rozšíření formalizace popisu autorizačních systémů. Dalším přínosem je návrh a implementace algoritmů efektivního pokrytí uživatelských identit rolemi, vycházejících z navržené formalizace. Za přínos lze též považovat identifikaci slabin a nevýhod používaných autorizačních systémů v různých organizacích i návrh řešení udržitelnosti relevance nastavených oprávnění s ohledem na životní cyklus organizace i zaměstnance.

Formální náležitosti práce

S ohledem na obtížnost zvoleného téma a na srozumitelnost textu nejsou všechny kapitoly zcela vyvážené. Některé z nich jsou psány srozumitelným a přehledným jazykem, jiné naopak zkratkovitě bez detailnějšího objasnění popisované problematiky. Práci by neuškodilo již zmíněné srozumitelnější provázání obsahu 2. kapitoly s obsahem 3. a 4. kapitoly.

Způsob naplnění cílů práce

Cíle i dílčí cíle práce jsou na začátku práce jasně a přehledně definovány. Naplnění některých z nich je možné v textu práce jasně identifikovat, naplnění jiných lze někdy pouze vytušit. K větší přehlednosti plnění jednotlivých cílů by jistě přispěla samostatná část práce, která by

popsala metodiku řešení vytyčených cílů. I přes uvedené lze konstatovat, že hlavní cíl práce a všechny dílčí cíle byly splněny.

Celkově lze konstatovat, že předložená práce splňuje svým obsahem i zpracováním požadavky kladené na disertační práci. Práci hodnotím kladně a doporučuji ji k obhajobě.

Otázky

1. Lze dané problémy řešit deklarativním přístupem např. v Prologu? Lze popsat navržené axiomy striktně pomocí predikátové logiky 1. řádu? Je možné popsané úlohy takto řešit v reálném čase?
2. Proč nebyl použit pro formalizaci správy identit zápis predikátové logiky 1. řádu, která má blíže k formálnímu popisu implementace SAT algoritmu?
3. Jakým způsobem je realizováno propojení navržených „pokrývacích" algoritmů a implementace návrhových vzorů RBAC s ohledem na jednotlivé organizace z případových studií?

5. 12. 2016

doc. RNDr. Mikuláš Gangur, Ph.D.