ČVUT v Praze - Fakulta elektrotechnická
katedra telekomunikační techniky
Praha 6 - Dejvice, Technická 2, 166 27
tel: 224352100 (2103, 2070)

Posudek oponenta diplomové práce

Název diplomové práce: Autentizační mechanismy v heterogenních sítích

Jméno a příjmení studenta: Bc. Jiří Tišler

Jméno a příjmení oponenta diplomové práce včetně titulů a pracoviště:
Ing. et Ing. Pavel Schlitter, Ph.D., SITEL, spol. s r.o.

1) Náročnost zadání:
__ velmi vysoká
X vysoká
__ průměrná
__ podprůměrná

2) Zvolené metody a postupy při řešení práce:
__ výborné
X velmi dobré
__ dobré
__ uspokojivé
__ dostatečné
__ nedostatečné

3) Správnost názvosloví:
__ výborná
X velmi dobrá
__ dobrá
__ uspokojivá
__ dostatečná
__ nedostatečná

4) Správnost předložených výsledků:
__ výborná
X velmi dobrá
__ dobrá
__ uspokojivá
__ dostatečná
__ nedostatečná

5) Odborná úroveň:
__ výborná
__ velmi dobrá
X dobrá
__ uspokojivá
__ dostatečná
__ nedostatečná

6) Jazyková a textová úroveň:
__ výborná
__ velmi dobrá
__ dobrá
X uspokojivá
__ dostatečná
__ nedostatečná

7) Grafická úprava:
__ výborná
__ velmi dobrá
__ dobrá
__ uspokojivá
X dostatečná
__ nedostatečná

8) Student splnil zadání:
X úplně
__ částečně
__ nesplnil

9) Dosažené výsledky, vlastní přínos a praktická využitelnost práce*: Student v práci popsal možnosti přihlašování v sítích využívajících různé autentizační mechanismy a zdroje identit (AD, Kerneros, OpenLDAP). V praktické části navrhl a zrealizoval systém jednotné správy uživatelů na Katedře telekomunikační techniky včetně vytvoření skriptu pro synchronizaci fakultní LDAP databáze uživatelů s katedrálním AD.

10) Připomínky k práci*: Práce jako celek působí velmi syrovým dojmem, zřejmě byla psána na poslední chvíli a nezbyl čas na nezbytné korekce. V práci lze nalézt celou řadu míst, která toto dokreslují: Nesystematický přepis zkratek – str. 6 „a kol." a „et al". Obrázky (3.3.5-3.3.10) jsou jednak nepřehledné a dále i nekvalitní. Psaní šipek pomocí „pomlčky a špičaté závorky ->" svědčí o nezvládnutí správných typografických návyků. Seznam zkratek neobsahuje všechny v textu používané zkratky např.: OU, DN, CSV, UID, NAP…

11) Otázky ke studentovi vztahující se k práci (budou zodpovězeny při obhajobě)*:
Viz druhá stranu posudku.

Doporučení k obhajobě: X doporučuji __ nedoporučuji

Klasifikace diplomové práce:

__ A - výborně (1,0)
__ B - velmi dobře (1,5)
__ C - dobře (2,0)
X D - uspokojivě (2,5)
__ E - dostatečně (3,0)
__ F - nedostatečně (4,0)

Datum: 24.5.2015 **Podpis:**

__ zaškrtněte odpovídající odpověď
* v případě nedostatku místa použijte zadní stranu formuláře

11) Otázky pro studenta:

1) Na straně 7 je uvedeno: „Kombinace UPN a uživatelského hesla je stanicí zahashována jednosměrnou hashovací funkcí…“ Jaké tři základní požadavky musí splňovat standardně používané kryptografické hashovací funkce např. SHA-1? Používají se v praxi kryptografické hashovací funkce, které nejsou jednosměrné?
2) Objasněte vztah AS a TGS v rámci protokolu Kerberos. Na straně 6 je v posledním odstavci napsáno: „ Obr. 3.3.3 představuje Kerberos server, který slouží jako Key Distribution Center (KDC), kde běží autentizační služby (AS), jako např. Ticket-Granting Service“. Tato věta budí dojem, jako by TGS byl jednou z možností, jak zrealizovat AS.
3) Na straně 13 jsou definovány možné vztahy mezi doménami, kde jedním z kritérií je tzv. tranzitivnost vazby. Demonstrujte na příkladu obousměrnou netranztivní vazbu mezi doménami.

__ zaškrtněte odpovídající odpověď
* v případě nedostatku místa použijte zadní stranu formuláře