



ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra počítačů

POSUDEK VEDOUCÍHO DIPLOMOVÉ PRÁCE

Autor: Daniel Slavík
Název práce: Jednotná autentizace v prostředí UNIX pomocí Public-key infrastructure
Vedoucí práce: Ing. Jan Kubr

Zaměření: *teoretické* | **praktické** | *experimentální* | *průzkumové* | *výukové*

Závěrečná práce se zabývá bezpečným přihlašováním na servery s OS Linux/Unix prostřednictvím aplikace ssh. Autor navrhl postup přihlašování a implementoval proof of concept pro ověření implementovatelnosti navrženého řešení.

Dodržení zadání: *odchýlené* | **převážné** | *úplné* | *přesážené*

Vzniklá aplikace splňuje požadavky zadání. Výsledkem práce mohla být již beta verze aplikace.

Studijní náročnost: *A – velmi velká* | *B – značná* | **C – střední** | *D – mírná* | *E – malá* | *F – nízká*

Technická pracnost: *A – velmi velká* | *B – značná* | **C – střední** | *D – mírná* | *E – malá* | *F – nízká*

Dosažené výsledky a jejich přínos:

A – vynikající | *B – značné* | *C – dobré* | **D – uspokojivé** | *E – dostatečné* | *F – nedostatečné*

Uspokojivé jsou všechny části práce (analýza, implementace a testování). V analýze mi chybí jasné zhodnocení stávajících produktů. Produkty jsou v krátkosti popsány a jejich klíčové vlastnosti jsou shrnuty v tabulce, ale celkové zhodnocení je ponecháno na čtenáři. V analýze chybí jasná definice požadavků kladených na vznikající aplikaci. Implementace se omezuje pouze na proof of concept. Testování bylo provedeno, ale chybí popis testovacích scénářů, očekávaných výsledků a skutečných výstupů.

Orientace v problematice:

A – výborná | **B – velmi dobrá** | *C – dobrá* | *D – uspokojivá* | *E – dostatečná* | *F – nedostatečná*

Analýza problému a implementace:

A – výborná | *B – velmi dobrá* | *C – dobrá* | **D – uspokojivá** | *E – dostatečná* | *F – nedostatečná*

Žádám autora aby vysvětlil srovnání z kap. 3.2.3. Co je výstupem uvedeného vzorce? Co zobrazuje uvedený graf?

Passphrase se posílá na server nezašifrovaná viz str. 41 (neoznačená)?

Bude možné s aplikací použít Open ssh, které je velmi často používané na OS Linux, i když není uvedeno v kap. 4.9.1.1?

Hodnocení formální stránky:

A – výborné | B – velmi dobré | C – dobré | D – uspokojivé | E – dostatečné | F – nedostatečné

<i>struktura:</i>	dobrá
<i>jazyk:</i>	český
<i>srozumitelnost:</i>	uspokojivá
<i>styl:</i>	množství chyb a překlepů je na hranici akceptovatelnosti
<i>úprava:</i>	uspokojivá
<i>literární reference:</i>	dostatečné

Práce obsahuje velké množství chyb a překlepů. Obrázky jsou velmi často rozmazané. Srozumitelnost textu omezuje absence jasných závěrů jednotlivých kapitol. Autor v textu téměř nepoužívá literární reference viz str. 39 a chybějící odkaz na ČSN ISO/IEC 13888 uvedenou v literatuře. Norma ITU-X.509 z kap. 2.1.není uvedena v literatuře. Popisky obrázků nepomáhají s pochopením, co obrázek zobrazuje.

Aktivita a samostatnost studenta v průběhu řešení:

A – výborná | B – velmi dobrá | C – dobrá | D – uspokojivá | E – dostatečná | F – nedostatečná

Student pracoval zcela samostatně. Během práce proběhlo minimum konzultací. Připomínky vedoucího se snažil do práce zapracovat.

Závěr:

Celkově se jedná o uspokojivou práci, která nedosáhla původního očekávání. Navržený přístup řešení autentizace je unikátní, ale je nutné jej podrobit hlubší analýze a diskusi, což textová část práce neusnadňuje. Je škoda, že nevznikla alespoň beta verze aplikace, která by se dala otestovat ve zkušebním provozu.

Předloženou diplomovou práci hodnotím známkou:

D – uspokojivě

V Praze dne 12.1.2015

Ing. Jan Kubr