Příloha k protokolu o SZZ č.

Vysoká škola: JU, Pedagogická fakulta

Katedra: informatiky

Datum odevzdání posudku: 18. 1. 2012

Student: Stanislav Čeleda

Aprobace: F-VTE-n, k

Vedoucí diplomové práce:

PhDr. Milan Novák, Ph.D.

POSUDEK DIPLOMOVÉ PRÁCE

Certifikáty a certifikační autority
(téma)

Předkládaná práce se zabývá problematikou certifikátů a certifikačních autorit se zaměřením na jejich implementaci do internetových systémů. Práce vychází z předpokladu, že neustálý rozvoj digitální komunikace, nahrazování papírových dokumentů elektronickými a stále vyšší počet osob využívající komunikační technologie, vyžaduje rozšíření moderních autentizačních metod. Autor si proto v této práci vytyčil cíl zejména zmapovat současný stav problematiky certifikátů a certifikačních autorit.

Autor práci rozdělil do dvou základních částí. První část je založena na analýze současné problematiky, kde jsou popsány v současné době dostupné autentizační mechanizmy od jednoduché autentizace pomocí hesla, přes autentizaci biometrickou až po vícefaktorovou. Rozsáhlejší část analýzy tvoří problematika digitálních certifikátů. Autor popisuje jednotlivé elementární vlastnosti možných certifikátů a uvádí jejich možné operace s nimi. Dále plynule navazují certifikační autority, jejich činnosti, je popsán proces vydávání certifikátů certifikační autoritou. Autor se zabývá také českými komerčními certifikačními autoritami a uvádí možnosti pro vytvoření autorit vlastních. Takto provedená analýza slouží jako vstup k porovnání jednotlivých certifikačních autorit. Zde je vidět autorova nejistota ve volbě metriky pro závěrečné hodnocení. Autor si zvolil váhy, které přiřazoval vybraným společným vlastnostem certifikačních autorit, ale již není jednoznačně uvedeno, na jakém základě tyto vlastnosti byly vybrány. Zda se jedná o zcela náhodnou volbu, autorův subjektivní pocit nebo byly stanoveny z provedené analýzy. Výsledky jsou uvedeny v přehledové tabulce a je nad nimi provedena diskuse s výsledným doporučením výběru autority a možné aplikace do systémů školského prostředí.

Ve druhé části se autor zabývá praktickou realizací šifrovaného spojení s použitím digitálního certifikátu mezi serverem a klientem za podpory protokolu SSL. Popisuje postupy tvorby certifikátu

certifikační autority a certifikátu serveru. Autor zde uvádí ověřené postupy pro vytvoření certifikátů v operačních systémech Linux a Windows.

Přestože lze autorovi vytknout nejasnosti v části práce zabývající se porovnáváním jednotlivých autorit a to zejména ve zvolené metrice, která není zcela průkaznou, lze práci považovat za velmi zdařilou. Typografická úroveň práce je dobrá a její výsledná podoba odpovídá nárokům kladeným na diplomovou práci.

Návrh na klasifikaci bakalářské práce: výborně

.....

Podpis vedoucího diplomové práce

V Č. Budějovicích dne 18. 1. 2012

Stupeň klasifikace	výborně	velmi dobře	dobře	nevyhověl