Posudek oponenta diplomové práce

Práce: Kryptografická podpora pro aplikační server SAP
Autor: Vítězslav Fabian
Oponent: Martin Děcký

Práce obsahuje obecný přehled architektury knihovny implementující rozhraní GSS-API, přehled vhodných kryptografických mechanismů použitelných pro konkrétní implementaci, návrh autorova řešení s přihlédnutím k požadavkům aplikačního serveru SAP a závěrečnou diskuzi s evaluací dosažených cílů, srovnáním s jednou cizí proprietární implementací a výhledem do budoucna.

Text práce ukazuje autorův hluboký vhled jak do existujících kryptografických standardů a mechanismů, tak do obecné problematiky počítačové bezpečnosti. Navržený mechanismus PKIXM pro GSS-API knihovnu vhodně kombinuje existující standardy a implementace, samotný protokol je precizně definován v notaci ASN.1.

Práci lze vytknout občas až přílišnou stručnost. Ta se týká především programátorské dokumentace samotné implementace knihovny, která prakticky neexistuje (i přiložené zdrojové kódy obsahují velmi nedostačující množství dokumentačních komentářů). Také popis úskalí, která autor musel během vývoje pravděpodobně překonávat, by umožnil lépe docenit náročnost vykonané práce. Konečně srovnání popisované v kapitole 7.4 postrádá jakákoliv naměřená data (nebo alespoň odkaz na ně), takže závěr o datové propustnosti a časech působí značně nepodloženě.

Přes výše uvedené nedostatky lze práci hodnotit jako přínosnou. Navrhuji hodnotit ji známkou 1 – 2. Práci doporučuji k obhajobě.

V Praze, 1. září 2007.

Martin Děcký