Posudek diplomové práce
Jednotná autentizace v prostředí UNIX pomocí Public-key infrastructure

pana Bc.Daniela Slavíka (dále jen „student“)

Úkolem studenta bylo:

- **Analyzovat požadavky na jednotnou autentizaci ve větší společnosti.** Tuto část se snaží plnit kapitola 2, kde autor uvádí větší množství nepodložených faktů, kterých obecná platnost je diskutabilní. Nezdá se, že by provedl analýzu mezi rozumným počtem zástupců „větších společností“; uvádí zde dle mého názoru závěry, vyplývající z jeho zkušeností. Ve srovnání komerčních produktů není jasné, z čeho vznikl jejich výčet, navíc jsou srovnávány jen velice těžko srovnatelné produkty (či jejich části). V části „architektury centrální správy“ nesprávně používá pojem „man in the middle“, který se v praxi využívá pro označení bezpečnostních útoků.
- **Navrhnout a implementovat aplikaci řešící zabezpečený přístup na linux/unix systémy pomocí Public-key infrastructure (PKI)**. Návrh je postaven na použití dvou různých autentizačních prvků (klíčů), čímž student v podstatě zjednodušuje dnes běžnou vícefaktorovou autentizaci na autentizaci dvěma stejnými prvky, kterých zneužití se snaží zkomplikovat. Účelnost a použitelnost tohoto návrhu je diskutabilní a pro vyvození jednoznačného závěru by bylo potřeba intenzivního testování. Kladně hodnotím použití standartních prvků běžných v dnes dostupných unixových systémech.
  Implementace se omezuje na proof-of-concept řešení, kterého zprovoznění v práci není vůbec popsáno. Zvolené prostředí (Java) nepovažuji pro implementaci tohoto druhu aplikaci za standartní a tedy vhodně zvolené, očekával bych spíše implementaci v běžně dostupných prostředcích systému Unix (C/C++ či některý z běžných skriptovacích jazyků)
- **Vzniklou aplikaci otestujte.** Popis a výsledky testování (až na meditaci nad režií aplikace, která evidentně vychází z testování) v práci zcela chybí. Na externím médiu jsou dostupné obrazy pro testování laskavým čtenářem.

Z hlediska struktury je práce obvyklá a odpovídá zvyklostem absolventů naší katedry. Obsahuje velké množství chyb (překlepů, špatného skloňování, nesouhlas jednotného/množného čísla apod.). Závěr práce obsahuje impozantní seznam literatury, která ale v textu není odkazována (respektive minimálně). Autorství obrázků či ilustrací v práci není uvedeno vůbec i přesto, že některé jsou zjevně zkopírovány z internetu.

Práci doporučuji k obhajobě a hodnotím stupněm:
E-dostatečně

V Praze, 14.1.2015
Ing. Michal Medvecký
oponent diplomové práce