Posudek oponenta diplomové práce

Jakub Kučera: Perspektivní bezpečnostní metody pro přímé bankovní kanály

Předložená diplomová práce (DP) se zabývá problematikou bezpečnosti v oblasti bankovnictví. Cílem práce je provedení analýzy bezpečnostních metod, dále pak navrhnout a implementovat systém pro monitorování chování uživatelů v oblasti bankovnictví. Zadavatelem práce je firma Logica Czech Republic, s.r.o.

Teoretická část obsahuje nejdříve popis metod a kanálů přímého bankovnictví. Dále jsou popsány základní techniky pro zajištění bezpečnosti přímého bankovnictví. Banky dnes používají pro komunikaci s klienty převážně protokol TLS (případně SSL) a tyto dva protokoly jsou klíčové pro přímé bankovnictví. V této části práce bych proto očekával jejich popis. V práci jsem našel pouze zmínku o protokolu SSL bez popisu. V další části autor popisuje základní útoky na přímé bankovnictví. Diplomant pokračuje popisem bezpečnostních metod v přímých bankovních kanálech. Po přečtení této části ale zjistíme, že se autor omezil pouze na způsoby autentizace. Na druhou stranu se některé autentizační metody (ECG, EEG, hlas, apod.) netýkají bankovního sektoru a mohly by být podle mého názoru vypuštěny. Zde mě překvapila vložená podkapitola „2.3.1.2 Autentizační metody použité v ČR". Většina metod popsaných v předchozím textu je používána v ČR a demonstrována i ukázkami v českém prostředí (viz např. obr 4 a 6), proč tedy vkládáte tuhle kapitolu? V poslední sekci teoretické části diplomant popisuje systémy pro detekci podvodného chování.

Práce pokračuje kapitolou 3. - Praktická část. Autor nejdříve definuje metriky pro hodnocení autentizačních metod. Kompletní seznam kritérií je velmi obsáhlý, propracovaný a složitý (viz příloha 7.1) a je zjevné, že jeho příprava zabrala dost času. Jako nedostatek zde vidím, že hodnotící kritéria jsou velmi subjektivní a nejsem si jist, jakou mají vypovídající hodnotu. Uvítal bych zde alespoň větší zdůvodnění navrhovaných parametrů. Co Vás vedlo k tomu, že parametry mohou nabývat hodnot 1-5? Parametry metrik jsou váhově ohodnoceny, součet vah je vždy 10. Co Vás vedlo ke stanovení této hodnoty? Myslíte si, že všechny metriky mají stejnou váhu (např. síla autentizace vs. další aspekty)? Dále autor analyzuje vybrané autentizační metody za použití navržených metrik. Zde se mi jeví jako nadbytečná grafická reprezentace výsledku a naprosto dostatečné bych viděl výsledky v podobě tabulky. Na konci kapitoly porovnáváte jednotlivé metody na základě vypočítané průměrné hodnoty z daných metrik. Myslíte si, že je aritmetický průměr ideální hodnota pro porovnání kvality jednotlivých metod?

Práce pokračuje návrhem a implementací systému pro monitorování uživatelů. Během prezentace byla ověřena funkčnost systému na množině ukázkových scénářů. K implementační části nemám připomínky, jen bych chtěl uvést, že návrh a implementace systému byla podle mého názoru velmi časově náročná. Co zde ale postrádám je srovnání Vašich výsledků s podobnými systémy.

Průvodní dokument má převážně přehlednou strukturu, jen některé části v teoretické části se zdají lehce chaotické: proč nespojit kapitoly 2.2 a 2.3, když jde podle mého názoru o totéž? Proč uvádět kapitolu 2.3.1.2 (viz výše). Dokument obsahuje několik faktických chyb, řadu nepřesností a překlepů a bohužel i několik hrubých chyb. Kladně hodnotím vytvořený přehled termínů a zkratek, který čtenáři usnadní orientaci v práci samotné, bohužel ale neobsahuje všechny použité zkratky. Co mě dále v dokumentu chybí je popis instalace systému a uživatelská příručka vč. definice scénářů. Obsah přiloženého CD má logickou strukturu, zdrojové kódy jsou čitelné, přiměřeně komentované.

Předložená diplomová práce i přes výše uvedené nedostatky splňuje zadání. Autor zde prokázal, že dokáže řešit zadané problémy. Práci doporučuji k obhajobě a hodnotím klasifikačním stupněm

„dobře"

Ing. Pavel Král, Ph.D.
oponent DP

V Plzni 5. června 2012

Otázky: Viz posudek.