Posudek diplomové práce

Matematicko-fyzikální fakulta Univerzity Karlovy

Autor práce	Jiří Smolík		
Název práce	Důvěryhodná proxy v SSL/TLS spojení		
Rok odevzdání	2017		
Studijní program	Informatika	**Studijní obor**	Diskrétní modely a algoritmy

Autor posudku	Libor Forst	**Role**	Vedoucí
Pracoviště	SISAL		

Text posudku:

Zadání této práce vycházelo z praxe. Jeho záměrem bylo podrobně prozkoumat, jaké existují možnosti pro implementaci tzv. "rozlamování" zabezpečeného spojení (SSL/TLS), resp. zjistit, zda jdou překonat obtíže, které současná řešení překonat nedokážou. Předpokladem bylo, že výsledkem bude jednak analýza problému a jednak implementace, která zahrne řešení, jež analýza předurčí k úspešné implementaci. Analýza přitom vyústí v text, který bude vlastně přehledným a srozumitelným způsobem vysvětlovat, která řešení vhodná nebyla a která ano.

Diplomant se s vervou pustil do studia, a když analýzu dokončil, rozhodl se v rámci oficiálního zadání vydat se poněkud jiným směrem a místo implementace, která by jistě nemohla pokrýt všechna slabá místa, zvolil rošíření protokolu, které by se těmto slabým místům vyhnulo. Ovšem takovéhle komplexní řešení vyžaduje také daleko komplexnější analýzu. Diplomant ji (potud, pokud jsem to schopen posoudit) opravdu dokonale udělal (patří v této chvíli nejspíše k nejvzdělanějším odborníkům na problematiku u nás), a to dokonce včetně právních dopadů, ale přetavit ji v text, který by to dostatečně prokázal, už tak dokonale nesvedl. Navíc se tím dostala na vedlejší kolej i implementace, ačkoli se v této variantě zmenšila vlastně na pouhý proof-of-concept, a je na ní vidět míra pozornosti, kterou jí diplomant věnoval. Vcelku chápu, že myšlenka zavést celosvětově používané rozšíření je velmi lákavá a ambiciózní, ale osud takového nápadu je v této chvíli z mnoha důvodů velmi nejasný. Očekával bych ovšem, že součástí takto modifikovaného zadání bude i návrh patřičného RFC.

První verze textu práce, kterou jsem viděl, měla ambice uspět spíše na Filosofické fakultě, bylo to vlastně beletristické dílo, v němž se pod nánosem květných fabulací jen obtížně hledala fakta a jejich souvislosti. Pro čtenáře to bylo nesmírně obtížné, snadno se v textu ztrácel a v mnoha případech téměř nebylo možné se např. dobrat důvodů pro některá rozhodnutí . Nebylo jasné, zda je nějaké tvrzení zcela zřejmé, nebo plyne z nějaké jasné premisy o pár desítek stránek dříve, anebo se naopak důvody dozvíme o pár desítek stránek dále. Když se mi podařilo autora přimět k radikálnímu odbeletrizování a zcivilnění textu, doufal jsem, že i toto předivo souvislostí jasně vykrystalizuje. To se, ale povedlo jen zčásti. Odevzdaný text je o několik řádů lepší, ale mnohé nešvary v něm stále přetrvávají, takže pořád platí, že jeho obsah je možná špičkový, ale díky formě to lze těžko posoudit. Chápu, že problematika je složitá, ale i složitá problematika se dá popsat tak, že čtenář dokáže sledovat jasnou linii výkladu a neztratí se v jejích odbočkách. Situaci hodně komplikuje i to, že v textu autor pracuje s obrovským množstvím zkratek a několikaslovných termínů, ale práce neobsahuje žádnou formu rejstříku, takže čtenář velmi snadno ztratí přehled o tom, která zkratka nebo termín je obecně známá (a pokud ji nezná, může ji někde mimo práci vyhledat) a kterou zavádí autor (a je třeba prolistovat sto stran, aby její definici čtenář našel).

Co se týče kódu, je třeba na něj opravdu nahlížet pouze jako na demostraci, že základní myšlenka rozšíření funguje. Neškodilo by mu věnovat přeci jen o trochu více práce a to i po formální stránce (dokumentace pro vývojáře, odlišení vlastní a přejaté práce atp.). Pokud by SW dílo mělo být stěžejní částí práce, nebylo by v této formě přípustné. Přijmeme-li ale fakt, že zde má jen demostrační charakter, je asi možné ho akceptovat.

Práci doporučuji k obhajobě.

Práci nenavrhuji na zvláštní ocenění.

Datum 18.1.17 **Podpis**