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** Softwarové systémy

Autor posudku	Dan Lukeš **Role** Oponent
Pracoviště	SISAL

Text posudku:

Autor práce prokázal, že se mu podařilo do dostatečné hloubky pochopit podstatné aspekty fungování SSL/TLS a už jen tím se v pozitivním slova smyslu vyčlenil do nepočetné skupiny odborníků na tuto oblast. Nepochybuji,. že bez ohledu na výsledek těchto obhajob nebude mít v budoucnosti žádný problém s kariérou.

Teoretická část návrhu úprav je jednou z možných funkčních variant řešení zadaného problému a rozhodně má potenciál být předložena IETF jako návrh standardu (samozřejmě až poté, co bude přepsána do formy vhodné pro tento účel). I navrhovaná úprava zdrojového kódu OpenSSL se jeví být funkční. Je ovšem třeba říct, že v rámci oponentského posudku lze posoudit především hlavní myšlenky předloženého návrhu a implementace. Kompletní analýza dopadu navrhovaných změn, zejména, zda některý konkrétní aspekt nevnáší do SSL/TLS nějakou chybu či nevytváří postranní kanál výrazně přesahuje možnosti oponentského posudku. Takového posouzení se ale návrh dočká od odborné věřejnosti, pokud bude návrh standardu předložen.

Naneštěstí má ale práce i vady.

Zatímco neformální vyjadřování je osvěžením, které zvyšuje čitelnost práce, autor opakovaně velmi neformálně přistupuje i k práci s fakty a k argumentaci obecně - což je přístup pro akademickou práci nevhodný.

Například autor opakovaně uvádí výroky, které nejsou v místě svého uvedení obecně pravdivé, aniž zmíní podmínky za nichž platné jsou (a není to zřejmé ani z kontextu). Čtenář neví zda navazující pasáže nejsou negativně ovlivněny vadným východiskem až do okamžiku kdy o řadu stránek či dokonce kapitol dál zjistí, že autor takové scénáře při kterých výrok neplatí z práce vyloučil. Případně se přízná, že o problému ví. Uvedu příkladmo jen dva z případů - na straně 113 zmiňuje použití kvalifikovaných certifikátů, aby teprve o šedesát řádek dál přiznal, že si je vědom, že takové použití je normami a legislativně zakázáno. A druhý - na stránce 16 dává při popisu TLS protokolu do souvislosti šifrování a autentizaci, přičemž tyto věci jsou ve skutečnosti na sobě obecně nezávislé, aby o devět stránek a několik kapitol dál uvedl, že scénáře, kdy spolu autentizace a šifrování nesouvisí z práce vyloučil. Podobných případů je tam ale větší množství, a značně znepřijemňují čtení práce.

Ještě nepříjemnější je, že autor na řadě míst rozebírá konkrétní problém tak, že vybere jeden scénář z mnoha možných, ten bez zdůvodnění označí za běžný/typický/převažující a na něm ukáže co ukázat chce. Se závěrem pak dál pracuje obecně, aniž by se vypořádal s existencí jiných scénářů - v lepším případě zmíní, že se dalšími variantami nebude zabývat kvůli rozsahu práce, z čehož není zrejmé, zda pro ně tvrzení platí (ale nebude se to zvlášť rozebírat), nebo jestli o platnosti tvrzení v těchto situaciích není nic známo. Čtenář je znovu při čtení dalšího textu ponechán v nejistotě co se platnosti východisek týče. Příkladů,

Text posudku:

nejvážnější je ale v samém závěru práce, kdy autor hodnotí bezpečnostní dopady navrhovaného řešení. Zabývá se ale jen pohledem klienta, kde to „vychází dobře", kdežto pohled serveru, kde by závěr byl podstatně méně příznivý, v podstatě vynechá. „Zájmy serveru" ostatně pomíjí i na některých dalších míst, kde se (zdánlivě obecně) vyjadřuje k bezpečnostním aspektům řešení. Argumentace autora tak nepůsobí vyváženě, místy budí spíš manipulativní dojem. Autor prostě „ví kam má v plánu dojít" a tomu podřizuje o čem se zmíní a co pomine. To mám za nejvážnější vadu textové části práce. Na základě zkušenosti s touto prací, na téma, kterému rozumím, bych měl problém důvěřovat budoucím pracem autora, na témata, kterým bych sám až tolik nerozuměl.

Ani implementace se nevyhnula některým velmi nešťastným rozhodnutím.

Autor se při provádění úprav původního kódu neomezil na změny související s prací a současně prováděl úpravy a opravy nesouvisející (opravy překlepů v cizích komentářích, změny ve formátování kódu, ...). To opravdu nepříjemně komplikuje práci kohokoliv, kdo by chtěl posoudit, zda úpravu nemají nějaký dopad na funkci a bezpečnost operací, které knihovna zajišťuje..

Neutěšený je stav dokumentace. Text zprávy sice obsahuje kapitolu *Dokumentace pro uživatele*, ta se ale věnuje pouze tomu, jak použít CLI testovací utilitu. Nenajdeme popis provedených změn, nebo alespoň popis změn API, takže prakticky není možné napsat vlastní aplikaci, která by upravenou knihovnu používala (zejména nově přidanou funkcionalitu). V kapitole *Dokumentace pro vývojáře* najdeme pouze popis jak přeložit zdrojový kód. Vývojová dokumentace (potřebná pro další vývoj, opravy chyb, portaci na novou verzi OpenSSL, ale i pro audit provedených změn) tak prakticky chybí. Implementace je tak spíš čistým *proof-of-concept* než referenční implementací, ze které by mohl někdo další vyjít. Autor se tak dostal na samou hranu zadání práce. Na druhou stranu, textová část je nadprůměrně rozsáhlá a její příprava si nepochybně vyžádala víc než běžné množství času. To snad částečně dovoluje „stručnou implementaci" omluvit.

Je velmi obtížné zaujmout jednoznačné stanovisko. Jádro práce je opravdu velmi dobré a autor se kvůli tomu stal odborníkem na oblast, které rozumí na světě jen poměrně úzký okruh specialistů. A v kontrastu s tím tu je vlastní text práce, který je rozsáhlý, ve výsledku obsahuje vše co je potřeba, ale je natolik neuspořádaný, že i pro odborníka je těžké sledovat (a verifikovat) tok autorových úvah. Žádnou část současného textu nelze přímo použít jako text budoucího návrhu standardu (což je autorův ambiciózní, a mě osobně velmi sympatický, cíl) a mám vážné obavy, že autor vůbec nebude schopen připravit exaktní a přísně strukturovaný text návrhu standardu. To už jsem se ale dostal mimo rozsah zadání práce.

Po zvážení všech okolností jsem se nakonec rozhodl práci k obhajobě doporučit. Kvůli nešťastné struktuře textové části ale nemohu navrhnout lepší známku než „3".

Práci doporučuji k obhajobě.

Práci nenavrhuji na zvláštní ocenění.

Datum 23.1.2017 **Podpis**

Digitally signed by Dan Lukeš
23.01.2017 19:06