Oponentní posudek diplomové práce

Petra Knapa

Zabezpečená výměna dat mezi počítači v nezabezpečeném prostředí

Diplomová práce se skládá ze dvou částí. První část se věnuje problematice zabezpečené komunikace. Druhá část se věnuje popisu praktické realizace tří hlavních komponent zabezpečené komunikace.

Diplomant využil znalosti získané studiem, ale ne úplně správně. Toto tvrzení bude zdůvodněno v nálezech, které jsou uvedeny v dále v tomto posudku.

Text v rešeršní části nejde příliš do hloubky, která by odpovídala druhému stupni vysokoškolského studia. Text rešeršní části je spíše na úrovni bakalářského studia.

Na přiloženém CD jsou uloženy zdrojové kódy a spustitelné „jar" soubory. Tyto „jar" soubory lze spustit a tím lze prokázat, že práce splnila hlavní cíl zadání.

Ke kvalitě textu mám tuto zásadní připomínku a to, že práce byla vytištěna na nějaké nekvalitní tiskárně. Totiž některé textové řádky mají vnitřní posun takovým způsobem, že to až znesnadňuje plynulé čtení. Kvalita textu, jeho srozumitelnost a přehlednost, je na průměrné úrovni a žádné zásadní pochybení z této strany diplomová práce neobsahuje.

Seznam nálezů:

1. Kapitola 6.1 Požadavky … obsahuje nevhodně definované požadavky, které obsahují pojmy: „… měla být …" nebo „… nesmí…". Toto bylo zjištěno i ostatních částech diplomové práce.
2. V práci je nesprávně používán pojem „objekt", přičemž se tím myslí třída. Toto chybné pojmenování tříd začíná již od kapitoly 6.3. Elementy označené jako ARWM a Handshake jsou třídami a ne objekty. Na Obr. 7 je použita kompozice v opačném směru, než jak ji vyučujeme. Dále na tomto diagramu jsou třídy, které jsou ve vztahu rodič-potomek, stejně pojmenovány. Což může způsobovat nedorozumění.
3. Na straně 29 je výpis kódu, který obsahuje toto `Handshake.KEY_PAIR = RSA.generatePair(4096).` Což podle konvenci Java znamená, že se do konstanty, mimo konstruktor, vkládá hodnota, tím pádem se nejedná o konstantu ale o veřejnou proměnnou. Přičemž v textu se tvrdí, že nový klíčový pár lze nastavit pro každou novou instanci a vzápětí v té samé větě se tvrdí, že ho lze nastavit jako statickou proměnnou.
4. Zásadní nález ke knihovně JavaCry je ten, že není k dispozici žádné objektivní ověření funkčnosti této knihovny. Chybí totiž jakékoliv testy, které by prokázaly, že spoj bude odolnější proti prolomení, jak je požadováno v zadání diplomové práce.
5. Dalším výhradou je, že knihovna JavaCry není navržena tzv. proti rozhraní, ale její použití je založeno pouze na implementačních třídách knihovny.
6. V textu práce a ani z obsahu na přiloženém CD není patrné, v jakém vývojovém prostředí byl produkt vyvíjen a pro jakou verzi Javy.

Z výše uvedených nálezů, je patrné se vyhotovená knihovna JavaCry byla ověřena pouze pomocí aplikačních programů. Proto ji nelze považovat za důvěryhodnou z hlediska její bezpečnost proti zneužití. Což potvrzuje samotný diplomant konstatování v závěru diplomové práce, že je potřeba

knihovnu JavaCry podrobit důkladnému testování. Toto je hlavní důvod návrhu sníženého klasifikačního stupně.

Otázky:

1. Proč nebyla použita metodika vývoje, která je známá pod názvem „řízení vývoje testy“? Znáte nějaké nástroje, které by takový vývoj umožňovaly?
2. Proč nebyla knihovna JavaCry navržena pomocí rozhraní? Kdyby byla, jaké by to přineslo výhody?

Práci **doporučují** k obhajobě a navrhuji klasifikační stupeň **velmi dobře**.

V Pardubicích 5. 6. 2014

Ing Karel Šimerda

KST-FEI-UPCE