FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student: Petr Nohejl
Oponent práce: Mgr. Jakub Růžička
Název práce: Zabezpečení hlasovací aplikace Baletka
Obor: Bezpečnost a informační technologie

Datum vytvoření: 10. 6. 2018

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	*1=mimořádně náročné zadání,* *2=náročnější zadání,* ***3=průměrně náročné zadání,*** *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Náročnost zadání odpovídá požadavkům kladeným na bakalářskou práci.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. Splnění zadání	*1=zadání splněno,* ***2=zadání splněno s menšími výhradami,*** *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Cíle práce byly splněny. Výtku k bodu 3. ze zadání/projektu práce diskutuji níže, a sice v kontextu většího propojení teoretické a praktické části textu.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	***1=splňuje požadavky,*** *2=splňuje požadavky s menšími výhradami,* *3=splňuje požadavky s většími výhradami,* *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Rozsah textu překračuje požadavky kladené na bakalářskou práci. Zejména bych chtěl vyzdvihnout detailní analýzu zdrojového kódu (spojenou s bezpečnostním testováním) aplikace Baletka, kterou dále rozebírám v bodě 7. Naopak se zdá, že teoretická část není s částí praktickou části výrazně propojena, což dále diskutuji v bodě 4.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*70 (C)*

Popis kritéria:
Posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře.

Komentář:
Teoretické část práce v některých místech zachází do detailu, který sice čtenáři poskytuje zajímavé informace, ale přímo nesouvisí s tématem práce (resp. nejsou vyvozeny implikace pro bakalářskou práci jako takovou). Jako příklad uvádím pasáž "Jak je již zmíněno výše, ID-card používá framework JavaCard, který komunikuje pomocí APDU protokolu. APDU příkazy jsou posílány pomocí čtečky do karty (takzvané C-APDU), karta poté posílá zpět odpovědi (takzvané R-APDU). Specifikaci APDU protokolu můžeme najít ve standardu ISO 7816-4. Bližší specifikace ID-card je uvedena zde [6] a [7]." Byť se v bezpečnostní analýze aplikace Baletka místy objevují odkazy na část teoretickou, např. s poznatky z podkapitoly 'Audit elektronických volebních systémů' se v práci dále přímo nepracuje. S tím souvisí i poznámka, že z teoretické části není zjevné, zdali je hlavní záběr kladen na bezpečnost volebního systému, technickou specifikaci diskutovaného řešení, využití konkrétní technologie, nebo způsob testování těchto systémů. Zároveň by bylo možné v úvodu lépe definovat terminologii - např. elektronický X online, hlasovací X volební, systém X aplikace. K analýze elektronických volebních systémů vybraných států by mohla přibýt i diskuze hlasování malých uzavřených skupin (potenciálně zacílenější vzhledem k řešenému tématu).

Praktickou část mohu jenom chválit. Oceňuji zejména detailní analýzu zdrojového kódu i využitých knihoven (vč. poskytnuté dokumentace), která jistě zabrala velké množství času. Obsahová stránka a dokumentace praktické části je nespornou předností této bakalářské práce, za kterou by se nestyděl ani seniorní auditor zdrojového kódu.

V závěru práce je sice uvedeno, že rozsah analýzy nepokrýval server a databázi. Domnívám se však, že toto mohlo být definováno v samotném úvodu práce. Ať už v kontextu komponent (emailový server, operační systém atp.), vektorů útoku (útoky na webovou aplikaci, útoky webový prohlížeč uživatele, social engineering, ...), či ukotvení analýzy pomocí oborového standardu - např. klasifikace útoku (CAPEC atp.), či dle modelování hrozeb /analýzy rizik (STRIDE, DREAD, CVSS atp.). Téže mohlo dojít k otestování aplikace dle jednoho ze standardů/směrnic diskutovaných v teoretické části textu (resp. využít jejich relevantní části jako opory/frameworku pro vypracování části praktické).

Využitím některého z přístupů výše by došlo k lepšímu propojení teoretické část s částí praktickou. Je zjevné, že při už tak velkém rozsahu textu by na testy nad rámec těch provedených nezbyl čas. Nicméně, bez jasného teoretického ukotvení práce, dle mého názoru, nebyl splněn bod 3. ze zadání této bakalářské práce (celková analýza bezpečnostních aspektů aplikace Baletka), jelikož nebylo přesně definováno, co všechno celková analýza takové aplikace obnáší, a na jaká rizika se autor práce ve svém omezeném čase zaměřuje (byť nálezy analýzy jsou velmi cenné a praktická část práce byla zvládnuta skvěle - viz níže).

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*85 (B)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3.

Komentář:
Petr Nohejl mi poskytl veřejnou i neveřejnou část práce, v níž byly skryty potenciálně citlivé údaje. Přestože se jedná o profesionální jednání (zejména, ale ne výhradně, v komerční sféře), kterého si cením, v paralele ke známému principu se domnívám, že všechny v textu začerněné informace mohou být zveřejněny, jelikož aplikace by měla být bezpečná i za předpokladu, že její kód a konfigurace jsou veřejné (vyjma klíčů). V této souvislosti můžeme k otázkám v bodu 9. přidat i kritickou diskuzi toho, zdali není vhodné celou aplikaci zveřejnit jako open source.

Oceňuji průběžná shrnutí kapitol. Jeví se mi nicméně velmi obecná. Např. hned již několikrát diskutovaná úvodní kapitola "Elektronické volební systémy a principy jejich zabezpečení" mohla být završena shrnutím kritérií, podle kterých bude aplikace Baletka hodnocena (čímž by došlo i k většímu propojení teoretické a praktické části práce).

V textu se místy vyskytují gramatické chyby a hovorové výrazy.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*60 (D)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
K práci se zdroji mám větší výhrady. Množství citací je uvedeno ve formátu “více o této problematice lze nalézt v”, “následující část /celá tato sekce vychází především z” atp., kdy je obtížné rozlišit, zdali se jedná o přejatou myšlenku, vlastní názor, či kompilaci více zdrojů (je-li hlavním uvedeným zdrojem např. testovací příručka, není zjevné, zdali všechny její body byly v rámci testu ověřeny). Tyto citace zároveň na čtenáře mohou působit dojmem, že všechny relevantní informace nejsou v textu zmíněny, ale pro plné porozumění diskutovanému tématu a/nebo zvoleným metodám je třeba sáhnout po externích zdrojích (případně není zjevné, zdali jsou z hlediska řešeného problému podstatné - viz výše).

V literatuře se objevují především reference na standardy, blogové články, wiki a prezentace (online zdroje), ale v teoretické části je odkazována i článková tvorba. Hlavními zdroji pro praktickou část textu je oficiální bezpečnostní manuál frameworku Ruby on Rails (v němž je aplikace Baletka napsána) a slidy k prezentaci komerční firmy 3S Labs.

Rozumím, že výběr literatury byl z velké míry ovlivněn materiály, které tým za aplikací Baletka využil před zahájením jejího vývoje, nicméně ty vznikaly pro jinou potřebu než je bakalářská práce. Zacílení testování na hlasovací aplikaci Baletka je řešeno pouze na úrovni dopadů a doporučení k nalezeným zranitelnostem ve vztahu k procesu hlasování. Mohlo tedy dojít ke kompilaci a kritickému zhodnocení většího počtu zdrojů (vč. zdrojů odborných), případně více využívat zdrojů, jež se soustředí na elektronické hlasování (nebo naopak v teoretické části více diskutovat bezpečnost webových aplikací a následně diskuzi zacílit na aplikace pro hlasování), což by vedlo k výraznějšímu odlišení specifik testování hlasovací aplikace oproti testování libovolné jiné webové aplikace.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*100 (A)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Praktická část práce byla odvedena velmi poctivě/zodpovědně a rozhodně kvalitou přesahuje požadavky kladené na bakalářskou práci.

Petr Nohejl se detailně seznámil s aplikací Baletka, její architekturou a využitými technologiemi. Zároveň oceňuji (částečně i jakožto “protiváhu” ke komentáři okolo využité literatury výše) analýzu již proběhlých penetračních testů a materiálů, které mu tým za aplikací Baletka poskytl .

Nálezy analýzy byly využity pro zlepšení zabezpečení aplikace (přičemž byla nalezena minimálně jedna kritická zranitelnost). Autor na své nálezy v průběhu akademického roku pravidelně upozorňoval vývojaře aplikace, s nimiž úzce spolupracoval.

V návaznosti na teoretické ukotvení práce, okolo kterého soustředím svou hlavní kritiku textu, myslím, že by v samotném úvodu praktické části mohlo být uvedeno, o jaký bezpečnostní test /kombinaci testů se jedná (bezpečností audit kódu, skenování zranitelností, penetrační test, analýza rizik atp.). Pokud by využité metody byly stanoveny hned v úvodu, bylo by možné přímo v textu zhodnotit přednosti a limitace zvoleného přístupu, případně vyvodit náměty pro budoucí bezpečnostní testy a audity aplikace. Kontext/zasazení provedených testů do nějakého obecného rámce, případně schéma komponent aplikace, možných vektorů útoku a zdůraznění těch, kterými se práce zabývá, mi v textu chybí (není zcela jasně definované, jak je možné na analýzu studenta navázat).

Můj poslední komentář k tomuto bodu je pouze doplňující. Pro budoucí testování /analýzu kódu doporučuji využít některou z používaných metrik (např. coverage, risk density atp.) a závažnost zranitelnosti definovat dle standardizované škály (např. OWASP Risk Rating Methodology).

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Úsilí Petra Nohejla napomohlo k lepšímu zabezpečení aplikace Baletka. Na základě detailní analýzy zdrojového kódu nalezl problémy, které neodhalily proběhlé penetrační testy (jež tuto oblast neměly definovanou v rozsahu práce). Student své nálezy pravidelně konzultoval - po celý semestr přímo spolupracoval s vývojaři aplikace, případně v repozitáři aplikace proaktivně opravoval programový kód. Práce zároveň obsahuje návrhy pro nápravu odhalených zranitelností (ty zpravidla již byly implementovány v průběhu akademického roku).

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
Nakolik aplikace Baletka vyhovuje vybraným bezpečnostním standardům a směrnicím diskutovaným v Kapitole 1?

Jaký je rozdíl mezi automatickou a manuální analýzou kódu? Jaký je rozdíl mezi statickou a dynamickou analýzou kódu? Jaké metody a v jakém poměru byly využity ve Vašem konkrétním testování?

Srovnejte současnou "klasickou" architekturu aplikace Baletka se situací, kdy by byla opřena o technologii blockchain. Jaké výhody, nevýhody a implikace by využití této technologie znamenalo pro bezpečnost systému?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*85 (B)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Práci Petra Nohejla celkově hodnotím "B" ("velmi dobře"). Student věnoval velké množství času bezpečnostnímu testování a analýze zdrojového kódu aplikace Baletka, čímž se bezesporu zasloužil o její lepší zabezpečení, za což mu za celý tým aplikace Baletka patří velký dík! Přes skvělou praktickou část však v textu nebyly dodrženy některé náležitosti odborného textu - nejasná metodologie testování a teoretické ukotvení textu, malá propojenost teoretické a praktické části, vágnější citace. Přes velké množství komentářů/připomínek výše se však vůbec nedomnívám, že by se jednalo o špatný text (pouze jsem chtěl dát detailní zpětnou vazbu, aby diplomka už byla na výbornou).

Podpis oponenta práce: