Posudek oponenta závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Bc. Václav Mach
Oponent práce: Ing. Jan Tomášek
Název práce: Zpracování a analýza logů roamingového systému eduroam
Obor: Počítačové systémy a sítě

Datum vytvoření: 20. 1. 2017

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:
Cílem práce byl návrh a implementace systému pro zpracování a analýzu logů roamingového systému eduroam. Zadání je unikátní snahou o analýzu logů s ohledem na detekci anomálií, chyb při ověřování uživatelů a identifikaci podezřelých událostí. Pokud je mi známo, podobný systém neexistuje. Existující systémy zpracovávají logy především kvůli statistice počtu proběhlých autentizací.

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:
Student po seznámení se s plnými i redukovanými logy eduroam systému implementoval systém pro ukládání redukovaných logů ve vhodně strukturované databázi. Nad databází vytvořil obecné REST API rozhraní pro dotazování se databáze. Úspěšně implementoval řadu statistik a reportů, ve formě tabulek, grafů a emailových zpráv. Nechybí rozhraní pro interaktivní práci se systémem, a tak lze systém využít k přípravě parametrizovaných grafů a k vyhledávání podkladů při řešení provozních incidentů. Detekce anomálií je na velmi dobré úrovni.

Od požadavku na analýzu trendů, které mohou signalizovat nefunkčnost služby, bylo upuštěno. Nepovedlo se určit metodu, která by překonala schopnosti detekce stávajícího testování pomocí aktivních dotazů centrálního end-to-end monitoringu eduroamu. Podklady pro analýzu se ale dále zpracovávají, takže se lze k této práci v případě potřeby rychle vrátit.

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:
Předložená písemná zpráva splňuje požadovaný rozsah.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*95 (A)*

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:
Práce je dobře rozčleněna od rozboru vstupních dat přes implementaci po popis uživatelského rozhraní, kde kladně hodnotím, že student nesklouzl k lacinému natažení práce pomocí nadměrného množství snímků uživatelského rozhraní. Zvlášť kladně hodnotím úvahu nad dalším možným rozvojem systému.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*

5. Formální úroveň práce *90 (A)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 12/2014, článek 3.

Komentář:
Jazyková i typografická úroveň je velmi dobrá, práce byla vypracována s náležitou péčí.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*

6. Práce se zdroji *90 (A)*

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:
Student cituje relevantní zdroje, citace se zdají být v souladu s citačními zvyklostmi a normami.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*

7. Hodnocení výsledků, publikační výstupy a ocenění *95 (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:
Stávající systémy zpracování redukovaných logů RADIUS serverů se zabývají zpracováním logů jen pro účely statistiky počtu autentizací. Systém etlog vytvořený v rámci této DP je v oblasti detekce anomálií celosvětově unikátní. Rozšířil statistiky, které má operátor české eduroam federace k dispozici, o přehled, jak které zapojené instituce edruoam využívají.

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:
Díky systému etlog byly úspěšně detekovány anomálie v podobě kompromitovaných uživatelských identit a uživatelské identity provozované v rozporu s pravidly roamingového systému eduroam. Systém umožnil odhalit nekompletní podklady o pokrytí ze strany zapojených institucí. Dále poskytuje dobré rozhraní pro dohledávání odcizených zařízení. Celkově etlog přinesl zjednodušení správy českého národního eduroamu.

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:
Bylo by možné rozšířit systém takovým způsobem, aby identifikoval konkrétní typ zařízení použitého k přístupu k internetu prostřednictvím eduroamu (iOS, Android, WindowsMobile atd.)?

Co by měl uživatel, který odcizil eduroam identitu, udělat, aby nebyl systémem etlog detekovatelný?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*

10. Celkové hodnocení *95 (A)*

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:
Student se dokázal vyrovnat s ne zcela přesným zadáním včetně nedostatků ve vstupních datech, které průběžně během své práce odhalil. Díky tomu byla řada nedostatků ve vstupních datech odstraněna. Vytvořený systém zjednodušuje správu českého národního eduroam RADIUSu. Celkově práci hodnotím velmi kladně.

Podpis oponenta práce: