MASARYKOVA UNIVERZITA
FAKULTA INFORMATIKY
Botanická 68a
602 00 Brno
Tel: +420-549 49 1810
Fax: +420-549 49 1820
http://www.fi.muni.cz/

Posudek oponenta disertační práce:

Autentizační mechanismy v distribuovaném prostředí a jejich aplikace

Autor: **Mgr. Jindřich Jelínek**

Ve své disertační práci se Mgr. Jindřich Jelínek zabývá problematikou distribuovaných sítí založených na autentizaci s protojkolem RADIUS. Autor přestavuje svůj návrh vylepšení založený na využití všech dostupných informací. Tento návrh namodeloval v prosředí Petriho sítí a na simulaci změřil základní charakteristiky nového protokolu. Dále se zabýval svým návrhem z pohledu bezpečnosti sítě na systémové úrovni.

Úvodní část obsahuje obecný úvod do problematiky včetně definice základních pojmů, úvodu do bezpečnosti a základních informací o síti eduroam. Zde bych přivítala, kdyby se autor zabýval nejemon pojmy na vysoké úrovni abstrakce, ale využil toho, že eduroam je rozsáhlá síť využívana v mnoha organizacích v různých zemích po relativně dlouhé časové období a tedy existuje reálná zkušenost s jejím provozováním. Byla bych ráda, kdyby autor u obhajoby doplnil a zmínil, zdali jsou v komunitě provozovatelů a uživatelů popsány případy, kdy stávající protokol selhal a zdali to vedlo k bezpečnostním incidentům. Za ním následuje popis cílů disertační práce, proti kterým nic nenamítám. V následující části s názvem Teoretické poznatky se autor opět obecně zabývá autentizačními protokoly popisem protokolu RADIUS. Kapitola 5 obsahuje vlastní jádro disertační práce a sice návrh inovace protokolu. Autor popisuje experimentální síť, simulaci stávajícího protokolu a nový protokol. K této části se váže můj další dotaz. Zvažoval autor formální popis protokolu a jeho následnou verifikaci? Pokud ano, proč se rozhodl od toho upustit? Povětšinou verbální popis je rovněž korektním řešením zvláště, pokud by autor měl ambice prosadit zveřejnění svého protokolu formou RFC. Udělal autor tímto směrem nějaký pokus? Experimentální část a měření nasimulováného protokolu považuji za zdařilé. Šestá kapitola obsahuje hodnocení návrhu z hlediska bezpečnosti a nemám k ní připomínky. Na závěr autror věcně hodnotí dosažené výsledky. Zde by mě zajímalo, jakým způsobem autor informoval o své práci odpovídající komunitu a jak byla jeho práce přijata.

Kromě dotazů s připomínek ve výše uvedeném textu mam k práci následující:

- Práce je psána v českém jazyce a to omezuje okruh potenciálních čtenářů.
- Práce obsahuje překlepy (např.str. 21, podkapitola 4.1, 4. řádek) a větší množství prohřešků v sazbě (např. jednopísemné předložky na konci řádků), což u disertační práce vnímám jako nedostatek.
- Publikační činnost autora představuje celkem 2 příspěvky na doktorandských konferencích v ČR, 3 příspěvky v angl. jazyce na konferencích na Slovensku a jeden příspěvek nesouvisející s tématem z roku 2005 na doktorandské konferenci opět v ČR. Chybí

mi buď publikace v časopisu (nejlépe impaktovaném) nebo na kvalitní mezinárodní konferenci.

- Chybí mi zmínky o využití této práce v praxi.

Na závěr konstatuji, že autor v textu disertační práce prokázal, že rozumí problematice, že je schopen isamostatně navrhnout a zpracovat dané téma. Pokud jeho publikační aktivity odpovídají kvantitou i kvalitou požadavkům pracoviště a pokud adekvátně odpoví na dotazy uvedené v posudku, doporučuji tuto disertační práci k přijetí.

V Brně 1. března 2016

Doc. RNDr. Eva Hladká, Ph. D.

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta informačních technologií
katedra počítačových systémů

Posudek oponenta dizertační práce

Mgr. Jindřicha Jelínka

Autentifikační mechanismy v distribuovaném prostředí a jejich aplikace

Doktorská dizertační práce Mgr. Jindřicha Jelínka je věnována autentifikaci v distribuovaném prostředí. Jedním z cílů je návrh a simulace chování algoritmů dovolujích doplnění domovského autentizačního serveru o alternativní autentizační servery zastoupujících domovský server při jeho výpadku nebo při výpadku komunikace s ním.

Druhým cílem práce bylo vylepšení autentizačního protokolu RADIUS. které dovolí zvýšit bezpečnost autentizace v distribuovanných sítích s federativní autentizací.

Nejpodrobnější částí dizertační práce je kapitola 5 věnováná návrhu modifikovaného protokolu RADIUS, opírajícího se o využití alternativních autentizačních serverů. Popis algoritmu se plně opírá o Colored Petriho sítě (CPN) a chování algoritmu je ověřeno prostřednictvím systému CPN Tools. Primárním parametrem testů je spolehlivost přenosu v síti propojující jednotlivé prvky, z hlediska rozsahu uvažovaných hodnot je zřejmě jako použitý komunikační protokol uvažován UDP. Vliv ostatních parametrů, jako jsou počet autentizačních serverů, doba platnosti autentizačních záznamů v cache pamětech a omezení kapacity cache pamětí a rozsahu vstupních požadavků, zůstává při simulace stranou (důvodem jsou zřejmě schopnosti systému CPN Tools).

Na druhou stranu, pro omezený rozsah vstupních parametrů jsou simulací prostřednictvím modelu v CPN Tools získány výsledky v oblastech úspěšnosti dotazu, počtu přenášených paketů a doby odezvy na požadavek o autentizaci.

Druhým přínosem dizertační práce je návrh technologie dovolující zajistit bezpečnost distribuce autentizačních informací mezi autentizační servery distribuovaného autentizačního systému. Této oblasti je věnována kapitola 6, ve které se Mgr. Jindřich Jelínek věnuje návrhu rozšíření funkce pro účtování (Accounting Service) služby protokolu RADIUS o obranný mechanismus proti průniku (IDS Intrusion Detection System)

Klíčovým přínosem práce je v této části doplnění protokolu RADIUS o zprávy sloužící specificky bezpečnostním funkcím, tedy zprávy Security-Message a jimi předávané atributy. Jde o zprávy vyměňované mezi autentifikačními servery v sítích federace dovolující regulovat přístup klientů k poskytovaným službám. Jejich využití v konkrétních vzorových příkladech struktury federativního autentizačního systému ale zůstává mimo rozsah textu dizertační práce.

Bezpečnostní politiky orientované na klienty a služby (podkapitola 6.6) jsou zmiňovány spíše zkratkovitě, i když jejich vztah k autentifikačním funkcím je poměrně významný.

V tomto odstavci uvádím některé připomínky k nejasnostem v publikaci práce, které bych potřeboval v průběhu obhajoby vysvětlit:

- Využití Petriho sítí (konkrétně CPN) pro modelování chování distribuovaného výpočtu odpovídá požadavkům, určitou nevýhodou je ovšem fakt, že stavový prostor pokrytý takovým modelem je rozsáhlejší, než stavový prostor modelovaného systému a v určitých případech může ovlivnit statistické výsledky (což však pro model algoritmů RADIUS možná neplatí).
- Výsledky hodnocení úspěšnosti (graf 1 na str. 59) evidentně vycházejí ze schopnosti modifikovaného algoritmu RADIUS zajistit autentizaci i při výpadku domovského serveru servery alternativními. Graf ovšem ukazuje zajímavé výsledky, které jsou (pro SimplAdj) pravděpodobně důsledkem aktualizace dat na domovském serveru, zatímco v jeho alternativách zůstává kopie autentizačních dat po určitou dobu zachována.

- Svými výsledky hodnocení časové odezvy autentizace (graf 2 na str. 60) sice odpovídá předpokladům o době odpovědi v systémech s více autentizačními servery a různými strategiemi rozhodování (adjudikace), není však zřejmé, jak bylo hodnot (Time Units) při modelování systémem CPN Tools dosaženo.
- Výraznější je i vyhodnocení počtu přenesených paketů, a to jak získaných simulací (graf 3 na str. 61), tak vyjadřujících počet přenesených paketů při vyšším počtu alternativních autentizačních serverů (graf 4 na str. 61). S hodnotami v grafech na str.61 zřejmě souvisí i střední hodnoty z menšího množství pokusů (5) a výsledky autentizace Accept a Reject na str. 62 a 63. Vyhodnocení těchto výsledků by bylo vhodné spojit s modelem podle obr.19 (str. 46), který evidentně využívá prvku Radius1 jako domovského autentikačního serveru a jeho výpadkem zcela odřízne servery alternativní.

Celkově, a to i přes připomínky, které jsem uvedl k předkládanému textu, konstatuji, že dizertační práce dobře prokazuje schopnost samostatné vědecké práce jejího autora Mgr. Jindřicha Jelínka, řeší velice zajímavou problematiku, a výsledky, kterých autor dosáhl, mohou být zajímavé pro jeho další výzkumnou činnost. Doufám, že krátká prezentace Mgr. Jindřicha Jelínka bude věnována výše uvedeným otázkám.

Práci ve smyslu zákona 111/98 Sb. doporučuji přijmout k obhajobě s cílem získání titulu PhD. v oboru Technická kybernetika na Fakultě mechatroniky, informatiky a mezioborových studií Technické univerzity v Liberci.

V Praze dne 30. prosince 2015

doc. Ing. Jan Janeček, CSc.

PŘEHLED PUBLIKAČNÍ ČINNOSTI AUTORA – 2015

[A] Jelinek J., Satrapa P., Fiser J.: Experimental Issues of the Model of the Enhanced RADIUS Protocol, In: Proceedings of 12th International Workshop of Electronics, Control, Measurement, Signals and their application to Mechatronics ECMSM2015, Liberec, 2015

[B] Jelínek J., Satrapa P.: Návrh inovace protokolu RADIUS z hlediska bezpečnosti, In: sborník příspěvků 12. ročníku doktoradské konference, Hradec Králové, 2012, ISBN 978-80-7435-185-3

[C] Jelínek J., Satrapa P.: Návrh inovace protokolu RADIUS z hlediska bezpečnosti, příspěvek na 12. ročníku doktoradské konference, Hradec Králové, 10. 5. 2012

[D] Jelinek J., Satrapa P., Fiser J.: Simulation of enhanced RADIUS protocol in Colored Petri nets, In: Proceedings of 11th International Scientific Conference Informatics 2011, Rožňava, ISBN 978-80-89284-94-8

[E] Jelinek J., Satrapa P., Fiser J.: Simulation of enhanced RADIUS protocol in Colored Petri nets, příspěvek na konferenci, Informatics 2011, 11th International Scientific Conference, Rožňava, 17. 11. 2011

[F] Jelinek J., Satrapa P.: Simulation of RADIUS protocol in Colored Petri nets, In: Proceedings of Networking 1 – Theory and Practice, ŽU Žilina, 2011, ISBN 978-80-554-0494-3

[G] Barilla J., Jelinek J., The Mathematical Model of the Chemical Phase of Radiobiological Mechanism, WDS05 Proceeding of Contributed Papers, Part III, 620-624, Praha 2005