Bydgoszcz, 31.07.2023

Prof. dr hab. inż. Michał Choraś
Wydział Telekomunikacji, Informatyki i Elektrotechniki
Politechnika Bydgoska im. J.J. Śniadeckich, Bydgoszcz

Recenzja rozprawy doktorskiej

Metodyka oceny wiarygodności systemów zarządzania zaufaniem i reputacją,

której Autorem jest Pan

mgr inż. Marek Bogusław Janiszewski

realizowanej na Politechnice Warszawskiej

1. Wprowadzenie.

Niniejsza recenzja rozprawy doktorskiej, której Autorem jest Pan mgr inż. Marek Janiszewski, została wykonana na zlecenie Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Politechniki Warszawskiej (Uchwała nr 457/2023 z dnia 18 kwietnia 2023 r.) oraz na podstawie zawiadomienia o wyznaczeniu na Recenzenta w postępowaniu o nadanie stopnia doktora podpisanego przez Przewodniczącego RDN ITT Politechniki Warszawskiej Pana dr hab. inż. Jarosława Arabasa, profesora uczelni (z dnia 22 maja 2023).

Rozprawę odebrałem w czerwcu 2023 r., a recenzję wysłałem w wyznaczonym terminie w lipcu 2023 r.

Promotorem niniejszej rozprawy jest Pan dr hab. inż. Krzysztof Szczypiorski, prof. uczelni. Nie wyznaczono promotora pomocniczego. Praca doktorska składa się ze streszczenia, spisów, siedmiu rozdziałów, pięciu załączników oraz bibliografii.

Niniejsza recenzja (poza wprowadzeniem i wnioskiem) zawiera odpowiedzi na siedem pytań dotyczących rozprawy doktorskiej.

2. Jaki jest problem naukowy (teza) rozprawy? Czy został on trafnie i jasno sformułowany? Jaki charakter ma rozprawa?

Rozprawa, której Autorem jest Pan mgr inż. Marek Janiszewski, dotyczy metod ewaluacji systemów zarządzania zaufaniem i reputacją (tzw. systemów TRM (j.ang. *Trust and Reputation Management*)).

W szczególności Autor zajął się zagadnieniem ewaluacji oraz propozycją miar dla oceny wiarygodności systemów zarządzania zaufaniem i reputacją oraz problemem ataków na systemy zarządzania zaufaniem i reputacją.

Autor zaproponował, m.in:

- miary umożliwiające ocenę wiarygodności systemów TRM i ich porównywanie,
- szereg modeli (np. środowiska, systemu TRM oraz generycznych modeli ataków na systemy TRM),
- autorskie narzędzie TRM-RET.

Niniejsza praca naukowa ma charakter teoretyczny oraz koncepcyjno-eksperymentalny.

Problemy naukowe rozprawy zostały jasno i trafnie sformułowane, a także rozwiązane przez Autora.

Teza rozprawy znajduje się w rozdziale 1.2 na stronie 15. Poniżej tezy znajdują się cele szczegółowe rozprawy. Teza została potwierdzona przez Autora pracy w dalszych częściach rozprawy, a cele szczegółowe zostały osiągnięte.

3. Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł, w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle? Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?

Bardzo ciekawa i systematyczna analiza literatury została przeprowadzona w Rozdziale 3 „Stan wiedzy w zakresie systemów TRM". Do analizy stanu wiedzy, a w szczególności opisu praktycznych zastosowań systemów TRM należy zaliczyć także Rozdział 2 „Systemy zarządzania zaufaniem i reputacją".

W Rozdziale 2 Autor przedstawił ogólne pojęcia dotyczące jego rozprawy oraz wprowadził szereg przydatnych definicji. Na uznanie zasługuje podrozdział 2.7 „Zastosowania systemów TRM", w którym Autor przedstawił praktyczne i konkretne możliwości wykorzystania takich systemów. Natomiast w Rozdziale 3, Autor przedstawił szeroki i dobrze ustrukturyzowany przegląd prac naukowych i stan wiedzy w wielu aspektach związanych z pracą Autora (m.in. systemy TRM, modele systemów, ocena systemów, ataki na systemy TRM, taksonomie ataków, odporność na ataki, itp.).

Bardzo pozytywnie oceniam (zbyt rzadki w pracach doktorskich) podrozdział 3.5 „Podsumowanie przeglądu stanu wiedzy", w którym Autor dokonuje krytycznej analizy przeglądu literatury, wyciąga wnioski oraz motywuje swoje dalsze prace.

Sama bibliografia zawiera odpowiednią liczbę źródeł (112), ale niestety bardzo mało (zaledwie pięć) wspomnianych prac powstało po roku 2020 włącznie, co oceniam krytycznie.

Być może Autor rozprawy dokonał analizy i przeglądu literatury na wstępie swoich prac nad rozprawą i nie aktualizował już tej części wystarczająco często.

4. **Czy autor rozwiązał postawione zagadnienia? Czy użył do tego właściwych metod dowodząc, że posiadł umiejętności związane z metodyką i metodologią prowadzenia badań naukowych? Czy przyjęte założenia są uzasadnione?**

Generalnie, Autor w sposób odpowiedni rozwiązał problemy, których dotyczy rozprawa. Nie mam wątpliwości, iż Autor posiada wiedzę dot. zagadnień związanych z systemami TRM, a w szczególności ich modelowania, oceny wiarygodności oraz odporności na ataki. Autor posiada bogatą wiedzę dotyczącą modelowania oraz ewaluacji (w tym proponowania miar oceny wiarygodności) systemów TRM.

Przyjęte założenia są uzasadnione i merytorycznie poprawne, pomimo iż propozycje Autora są mocno heurystyczne.

Teza rozprawy została dowiedziona. Autor zaproponował oraz zaprezentował bardzo wiele miar, analiz oraz wyników symulacyjno-eksperymentalnych – jest to niewątpliwie dużą zaletą niniejszej rozprawy. Autor posiada duże umiejętności w konstruowaniu, analizie oraz wykorzystywaniu miar służących do ewaluacji wiarygodności i odporności (na ataki) systemów TRM.

5. **Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu nauki reprezentowanych przez literaturę światową?**

Autorskim i głównym elementem rozprawy jest propozycja oceny wiarygodności systemów TRM.

Głównymi osiągnięciami rozprawy oraz propozycjami Autora są:

- Opracowanie generycznego modelu środowiska, w którym działa system TRM,
- Opracowanie modelu systemów TRM,
- Opracowanie modeli ataków na systemy TRM,
- Zdefiniowanie miar wiarygodności systemów TRM,
- Opracowanie narzędzia TRM-RET służącego do badań eksperymentalnych,
- Opracowanie heurystycznej metody ataku na system TRM o nazwie MEAEM.

Autor wykonał szereg testów i prac eksperymentalnych w celu zbadania i porównania zaproponowanych miar wiarygodności systemów TRM, wkładając bardzo dużo pracy w tę część rozprawy oraz prezentując bogaty zestaw wyników i porównań (Rozdział 6 niniejszej rozprawy). Ponadto, Autor analizował wpływ różnorodnych ataków na systemy TRM.

Kolejnym pozytywnym elementem rozprawy jest propozycja narzędzia TRM-RET, które zostało wielokrotnie wykorzystane przez Autora w eksperymentach. Tym samym Autor wykazał się umiejętnościami programistycznymi oraz analitycznymi.

6. Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników? Jaka jest poprawność redakcyjna rozprawy?

Niniejsza rozprawa stanowi przykład profesjonalnie przygotowanej pracy doktorskiej. Praca napisana jest na wysokim poziomie edycyjnym oraz graficznym.

W pracy występują oczywiście drobne usterki, literówki i błędy językowe, ale jest ich niewiele i nie są znaczące. Dziwić może brak numeracji równań (standardowo z prawej strony równania), ale numerowane są definicje, w których równania są przedstawiane.

Te drobne usterki nie zmieniają ogólnej opinii o bardzo dobrym i profesjonalnym poziomie językowym i edycyjnym rozprawy.

7. Jakie są słabe strony rozprawy i jej główne wady?

Rolą recenzenta jest zauważenie ewentualnych niedociągnięć i mankamentów przedstawianej pracy, oraz zgłoszenie uwag, które mogą być pomocne i przydatne w dalszych pracach.

Uwagi krytyczne to między innymi:

- Autor przyjął założenie o stałym modelu środowiska i ogólnie o stałych modelach nie uwzględniających zmian w czasie oraz innych zmian rzeczywistych systemów. Rozumiem, że takie przyjęto założenie, ale warto było podjąć szerszą dyskusję o wpływie oraz wadach takiego podejścia.
- Model środowiska i systemu wydaje się bardzo ogólny i generyczny. Takie podejście ma swoje zalety, ale także i wady – znów brakuje mi szerszej dyskusji oraz przykładów dla konkretnych zastosowań i tzw. *use-cases*. Sądzę, że prace lepiej by się czytało, gdyby Autor wybrał do modelowania jeden/dwa konkretne rzeczywiste systemy (np. podobne do tych omówionych w Podrozdziale 2.7).
- Wiele z zaproponowanych przez Autora miar i podejść jest silnie heurystyczna. Brakuje uzasadnienia dla wielu miar oraz parametrów – często były one dobierane heurystycznie.
- Zbyt mało informacji Autor poświęcił praktycznym aspektom zaproponowanych miar: jakie mają konkretnie wartości, jak je skalować i normalizować (np. w przypadkach gdy część może mieć wartości małe, a część bardzo duże, jaki jest wpływ konkretnych miar itp.).
- Brakuje rozdziału (ewentualnie szerszej dyskusji) podważającego i testującego zaproponowane miary oraz ich dobór.

- Pewien niedosyt budzi sposób przedstawienia własnego narzędzia TRM-RET. Oczywiście pozytywnym elementem jest zaprojektowanie i wykonanie narzędzia programistycznego oraz ukazanie jego architektury, ale brakuje dokładnego pokazania jego zastosowania w pracy, oraz przykładowych widoków. Jak rozumiem, narzędzie nie posiada interfejsu graficznego przyjaznego dla użytkownika, a jego wykorzystanie wymaga jego dogłębnej znajomości lub treningu (i nie jest przyjazne/intuicyjne). Tym niemniej projekt oraz implementację narzędzia oceniam pozytywnie jako wartość dodaną niniejszej rozprawy.
- W pracy brakuje (to być może wynika tylko z moich zainteresowań) wykorzystania metod uczenia maszynowego, ale przede wszystkim szerszej dyskusji o potencjalnym wykorzystaniu takich metod jako alternatywy do zaprezentowanego podejścia.
- W pracy brakuje informacji na temat istotności statystycznej różnic między wynikami, parametrami.
- Większość wykorzystanych w przeglądzie literatury prac i artykułów ukazała się jeszcze przed rokiem 2020. Zaledwie pięć prac jest datowanych od roku 2020.

Uwagi krytyczne są często natury dyskursywnej. Zdaję sobie sprawę, że często uwagi dotyczą świadomych i przemyślanych wyborów Autora, więc nie zmieniają pozytywnej oceny pracy.

Generalnie, bardzo pozytywnie oceniam dobór tematu, bardzo przemyślaną i formalnie poprawną pracę oraz dużo pracy Doktoranta nad propozycjami modeli oraz częścią eksperymentalną niniejszej rozprawy.

Warto zauważyć, że Doktorant jest także współautorem kilku artykułów naukowych oraz wystąpień wymienionych na str. 218-219 niniejszej rozprawy w podrozdziale 7.2. Niniejszy dorobek jest zdecydowanie wystarczający na tym etapie kariery naukowej.

8. Jaka jest przydatność rozprawy dla nauk technicznych?

Praca dotyczy bardzo aktualnych i potrzebnych zagadnień nowoczesnej informatyki technicznej i telekomunikacji (zastosowania słusznie ukazano w Podrozdziale 2.7), a w szczególności analizy wiarygodności systemów TRM. Sądzę, iż temat niniejszej rozprawy będzie jeszcze zyskiwał na popularności oraz będzie ważną częścią szeroko rozumianego cyberbezpieczeństwa.

Niniejsza rozprawa i przedstawione metody mogą być szczególnie interesujące i przydatne dla podmiotów wykorzystujących systemy rekomendacji, systemy wspierania decyzji, aplikacje mobilne i internetowe, itp.

9. Wniosek

Biorąc pod uwagę przedstawioną przez Doktoranta rozprawę stwierdzam, że recenzowana praca **spełnia wymagania stawiane rozprawom doktorskim** przez obowiązujące przepisy.

Dlatego wnoszę o przyjęcie niniejszej rozprawy i **dopuszczenie** mgr inż. Marka Janiszewskiego do publicznej obrony.

Prof. dr hab. inż. Michał Chorąś