RADA NAUKOWA DYSCYPLINY

INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA POLITECHNIKI WARSZAWSKIEJ

zaprasza na

PUBLICZNĄ OBRONĘ ROZPRAWY DOKTORSKIEJ

mgr. inż. Marka Bogusława Janiszewskiego

która odbędzie się w dniu **27 listopada 2023 roku,** o godzinie **14:00** w trybie łączonym (stacjonarnie równolegle ze zdalnie)

Temat rozprawy:

„Metodyka oceny wiarygodności systemów zarządzania zaufaniem i reputacją”

Promotor: dr hab. inż. Krzysztof Szczypiorski, prof. uczelni – Politechnika Warszawska

Recenzenci: dr hab. inż. Piotr Chołda, prof. uczelni – Akademia Górniczo-Hutnicza

prof. dr hab. inż. Michał Choraś – Politechnika Bydgoska

Obrona odbędzie się w sali 478 **Wydziału Elektroniki i Technik Informacyjnych, ul. Nowowiejska 15/19** oraz jednocześnie zdalnie na platformie MS Teams. Osoby zainteresowane uczestnictwem w obronie w formie zdalnej proszone są o zgłoszenie chęci uczestnictwa w formie elektronicznej na adres sekretarza komisji: dr. hab. inż. Mariusz Rawski, prof. uczelni, email: mariusz.rawski@pw.edu.pl, do dnia 24.11.2023 r., godz. 23:59.

Z rozprawą doktorską i recenzjami można zapoznać się w Czytelni Biblioteki Głównej Politechniki Warszawskiej, Warszawa, Plac Politechniki 1.

Streszczenie rozprawy doktorskiej i recenzje są zamieszczone na stronie internetowej: https://www.bip.pw.edu.pl/Postepowania-w-sprawie-nadania-stopnia-naukowego/Doktoraty/Wszczete-do-30-kwietnia-2019-r/Dyscyplina-informatyka-techniczna-i-telekomunikacja-dziedzina-nauk-inzynieryjno-technicznych/mgr-inz.-Marek-Boguslaw-Janiszewski

Przewodniczący Rady Naukowej Dyscypliny
Informatyka Techniczna i Telekomunikacja
Politechniki Warszawskiej
dr hab. inż. Jarosław Arabas, prof. uczelni

METODYKA OCENY WIARYGODNOŚCI SYSTEMÓW ZARZĄDZANIA ZAUFANIEM I REPUTACJĄ

STRESZCZENIE

Systemy zarządzania zaufaniem i reputacją, jako mechanizmy miękkiego bezpieczeństwa, znajdują zastosowanie w wielu środowiskach teleinformatycznych. Systemy te, mimo że stanowią zabezpieczenie przeciwko atakom związanym ze świadczeniem nierzetelnych usług, to same mogą stać się celem specyficznych dla nich ataków. W związku z tym istnieje potrzeba kompleksowej oceny wiarygodności (rozumianej jako odporności na ataki) takich systemów. W niniejszej rozprawie przedstawiono ogólną ideę systemów zarządzania zaufaniem i reputacją, pojęcia z nimi związane, a także przykłady ich praktycznych zastosowań. Zawarto także przegląd stanu wiedzy w zakresie ataków na systemy zarządzania zaufaniem i reputacją oraz oceną ich wiarygodności, w tym odniesienie się do publikacji, wchodzących w polemikę z wcześniejszymi artykułami autora rozprawy, dotyczącymi tej tematyki. W pracy zaprezentowano metodykę oceny wiarygodności, bazującą na stworzonych od podstaw i przedstawionych w rozprawie modelach środowiska, systemów zarządzania zaufaniem i reputacją oraz ataków. W metodyce zdefiniowano miary wiarygodności, które mogą służyć ocenie odporności systemów na ataki, a także przedstawiono rodzaje i propozycje badań, które mogą zostać wykorzystane do ich ewaluacji. Zaprezentowano także propozycję metody pozwalającej na identyfikację nowego ataku przeciwko konkretnemu systemowi zarządzania zaufaniem i reputacją, który może być bardziej efektywny niż znane do tej pory ataki. Rozprawa zawiera także opis dedykowanego narzędzia stworzonego do ewaluacji wiarygodności systemów zarządzania zaufaniem i reputacją. W oparciu o stworzoną metodykę i narzędzie, zaprezentowano wyniki przeprowadzonych badań wybranego systemu oraz ocenę jego wiarygodności, co stanowi przykład praktycznego zastosowania modeli, metodyki i metody przedstawionych w niniejszej publikacji. W ramach podsumowania zostały zaprezentowane perspektywy kontynuacji badań, a także wskazane dotychczasowe publikacje autora dotyczące ataków na systemy zarządzania zaufaniem i reputacją oraz oceny ich wiarygodności.

Słowa kluczowe: *zaufanie, reputacja, ataki, systemy zarządzania zaufaniem i reputacją, systemy zaufania, systemy reputacyjne, mechanizmy miękkiego bezpieczeństwa*

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

AKADEMIA GÓRNICZO–HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE

Wydział Informatyki, Elektroniki i Telekomunikacji

INSTYTUT TELEKOMUNIKACJI

Dr hab. inż. Piotr CHOŁDA

Kraków, dn. 28 lipca 2023 r.

RECENZJA ROZPRAWY DOKTORSKIEJ

Tytuł rozprawy: Metodyka oceny wiarygodności systemów zarządzania zaufaniem i reputacją
Autor rozprawy: mgr inż. Marek Bogusław Janiszewski

1. WSTĘP

Recenzowana rozprawa powstała pod opieką promotorską dra hab. inż. Krzysztofa Szczypiorskiego, prof. PW. Praca liczy 254 strony i obejmuje Streszczenie (str. 5), Abstract (str. 7), Spis treści (str. 9-11), szereg rozdziałów: 1. Wprowadzenie (str. 13-16), 2. Systemy zarządzania zaufaniem i reputacją (str. 17-42), 3. Stan wiedzy w zakresie systemów TRM (str. 43-71), 4. Model środowiska, systemu TRM i ataku (str. 72-122), 5. Metodyka oceny wiarygodności systemów TRM (str. 123-158), 6. Badanie systemu TRM w oparciu o metodykę oceny wiarygodności (str. 159-215), 7. Podsumowanie i wnioski (str. 216-219). Pracę zamykają materiały uzupełniające: Bibliografia (str. 220-228), Załączniki (str. 229-250) zawierające wykaz używanych skrótów, wykaz oznaczeń, wybrane pojęcia stosowane w pracy, opis znanych ataków na systemy TRM i specyfikację techniczną narzędzia TRM-RET. Na koniec zamieszczono spisy rysunków i tabel. Poza angielskim streszczeniem Abstract praca została napisana w języku polskim.

2. CEL BADAŃ (W ODNIESIENIU DO TEZY ROZPRAWY). Jakie zagadnienie naukowe jest rozpatrzone w pracy (teza rozprawy) i czy zostało ono dostatecznie jasno sformułowane przez Autora?

Praca dotyczy systemów zarządzania zaufaniem oraz reputacją (TRM). Biorąc pod uwagę, że we współczesnych systemach teleinformatycznych wiele obiektów zarządzanych przez różnych użytkowników, instytucje itd. współpracuje ze sobą, a poziom jakości ich współpracy decyduje o wynikach, jest to zagadnienie o charakterze uniwersalnym i ważne. W przypadku ocenianej dysertacji Doktorant zajął się odpornością systemów TRM na specyficzne ataki, które mają na celu właśnie zaburzenie oceny zaufania/reputacji. Można nawet powiedzieć, że Doktorant w ramach pracy buduje coś na kształt ogólnej teorii takich systemów oraz ich odporności, co bez wątpienia jest ogromną zaletą dysertacji, gdyż prezentuje całościowe podejście do pewnego wybranego istotnego zagadnienia teleinformatycznego.

Akademia Górniczo–Hutnicza | Wydział Informatyki, Elektroniki i Telekomunikacji
Instytut Telekomunikacji
al. A. Mickiewicza 30, 30–059 Kraków,
tel. +48 12 617 39 37, fax +48 12 634 23 72
e–mail: kt@agh.edu.pl, www.agh.edu.pl

Samo zaufanie jest w pracy rozumiane jako kwestia wzajemnej oceny interakcji między agentami, bo podejście agentowe decyduje tutaj o zdefiniowaniu tego, co może się dziać w środowisku (dopiero agenty świadczą pewne usługi). Reputacja jest pojęciem nadbudowanym na zaufaniu i w ogólności oznacza jakieś jego zagregowanie.

Teza rozprawy brzmi następująco: „Metodyka oceny wiarygodności systemów zarządzania zaufaniem i reputacją umożliwia dokonanie jakościowej i ilościowej ewaluacji odporności tych systemów na ataki mające za cel zmanipulowanie generowanych wyników i podejmowanych decyzji. Stworzenie metodyki oceny wiarygodności jest możliwe w oparciu o opracowanie modelu środowiska, systemów zarządzania zaufaniem i reputacją oraz generycznego modelu ataku przeciwko tym systemom." Doktorant dowodzi tej ***jasno i precyzyjnie sformułowanej tezy***, konstruując właśnie tego rodzaju metodykę. Jest to poprawne założenie w odniesieniu do tezy mówiącej o możliwości dokonania czegoś. W ramach pracy doktorskiej ***teza ta zostaje istotnie udowodniona***, co uznaję za wartościowe, gdyż wprowadzenie możliwości ocena wiarygodności systemów TRM jest pożądane.

3. CHARAKTER ROZPRAWY. Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?

Praca ma ***charakter konstrukcyjny***, z pewnymi elementami teoretycznymi. Doktorant przede wszystkim opracował pewną metodykę konstrukcji i oceny systemów TRM, która jest nastawiona na ilościowe szacowanie wiarygodności tych systemów. Przydatności całej zaproponowanej metodyki (a nawet więcej, bo użyte podejście jest całościowe, poczynając od propozycji podstawowych definicji odnoszących się do TRM) Autor rozprawy dowodzi w sposób doświadczalny, z użyciem małych przykładów i jednego dużego przykładu ilustracyjnego (co pokazuje nie tylko przydatność, ale też sposób zastosowania metodyki).

Obecny w pracy element teoretyczny dotyczy przede wszystkim formalizacji różnych zagadnień związanych z systemami TRM (w tym z atakami na nie), chociaż w mojej ocenie sama formalizacja nie ma charakteru heurystycznego, który służyłby np. do dowiedzenia poprawności działania metodyki (za to wspomaga opis oraz zastosowania).

4. SPOSÓB PRZEPROWADZENIA ANALIZY ŹRÓDEŁ. SPOSÓB SFORMUŁOWANIA WNIOSKÓW WYNIKAJĄCYCH Z ANALIZY ŹRÓDEŁ. Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł (w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle) świadczący o dostatecznej wiedzy Autora. Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?

Analiza wiedzy zastanej oraz dostępnej literatury światowej została przeprowadzona przez Doktoranta w rozdz. 2 (tutaj głównie opis tła koncepcyjnego) oraz rozdz. 3 (właściwa analiza źródeł i stanu wiedzy, w tym zastosowań w przemyśle i biznesie). Oba rozdziały dowodzą ***dobrej orientacji Autora w obszarze, którego dotyczy praca***, jak również w zakresie zbliżonych do niego zagadnień szeroko pojętego bezpieczeństwa, ale również współczesnych systemów teleinformatycznych.

Bibliografia liczy 112 pozycji i w większości przypadków są to prace anglojęzyczne, funkcjonujące w obiegu międzynarodowym. W tej liczbie mieści się pewna grupa prac polskojęzycznych samego Doktoranta, ale jest zrozumiałe, że są one oczywiście cytowane jako podstawa rozprawy. Na początku rozdziału 3 Autor wylicza tematy, które brał pod uwagę jako podstawę wyboru tekstów do opisu literaturowego. Dobór jest jak najbardziej adekwatny do zagadnienia będącego przedmiotem rozprawy. Sama ***analiza źródeł jest więc wyczerpująca tematycznie*** i trzeba stwierdzić, że Doktorant z jednej strony trafnie charakteryzuje opisywane systemy, koncepcje itd., poprawnie i rzetelnie wyciąga z nich wnioski, a także wykazuje oryginalność swojego podejścia oraz podaje źródła inspiracji (a nawet niekiedy miejsca polemiczne z własnymi wcześniejszymi dokonaniami).

Niestety, trzeba tutaj krytycznie powiedzieć, że systematyczny opis literatury nie jest konsekwentny i wyczerpująco został wykonany w odniesieniu do stanu wiedzy sprzed ok. 10 lat, gdyż – z niezrozumiałych w sumie względów Doktorant cytuje bardzo mało źródeł z lat późniejszych (widzę ok. 18 cytowań pochodzący z lat 2016 i później, z czego część to prace samego Autora). Nawet pobieżna kwerenda w Google Scholar wskazuje, że w ciągu ostatnich lat powstały dziesiątki artykułów na temat systemów TRM, także odnoszących się do nowych paradygmatów sieciowych (np. IoT). Nie oznacza to, że wnioski wyciągnięte przez Doktoranta są nieprawidłowe, ale na pewno przegląd literatury nie jest pełny.

5. ROZWIĄZANIE PRZEDSTAWIONEGO ZADANIA, WŁAŚCIWOŚCI PRZYJĘTYCH METOD I ZAŁOŻEŃ. Czy Autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?

Tematyka rozprawy dotyczy, jak słusznie pisze Doktorant, zagadnień miękkiego bezpieczeństwa. Mimo to, można powiedzieć, że w ramach pracy Autor podjął się pewnego, pożądanego tutaj „utwardzenia" zagadnienia, wprowadzając formalizację problematyki. Wprawdzie formalizacja owa służy głównie rozjaśnieniu przedstawionych koncepcji oraz uprecyzyjnieniu opisu, a także umożliwia sprawniejsze użycia opracowanego przez Doktoranta systemu, a nie ma na celu np. automatycznego wnioskowania w sposób pewny, ale jest to na pewno krok w przód w zakresie konstrukcji systemów TRM.

Przedstawione zadanie, związane z określoną w tezie metodyką zostało przez Doktoranta rozbite na szereg podzagadnień, tj. Autor rozprawy raportuje następujące czynności: opracowanie modelu środowiska, w którym może być wykorzystywany system TRM (przedmiot rozdziału 4, ale faktem jest że również rozdział 2, który wprowadza tło koncepcyjne, zawiera niezbędne elementy formalizacji); opracowanie ogólnego modelu systemów TRM (również przedmiot rozdziału 4); opracowanie modelu ataków na systemy TRM oraz kryteriów oceny ich skuteczności w oparciu o generyczny model systemów TRM (również przedmiot rozdziału 4, ale także częściowo rozdziału 5); zaproponowanie metody pozwalającej na znalezienie najbardziej efektywnego ataku na określony system TRM (również przedmiot rozdziału 5); dokonanie opisu przykładowego systemu TRM w ramach opracowanego modelu oraz przeprowadzenie badań jego wiarygodności w oparciu o zaproponowaną metodykę (przedmiot rozdziału 6). Warto zwrócić uwagę, że Doktorant w ramach rozdziału 5 posłużył się koncepcją tzw. najbardziej efektywnego ataku, czyli swego rodzaju najbardziej pesymistycznego przypadku,

który ma być kamieniem probierczym wiarygodności badanego systemu (taki atak nie musi należeć do wcześniej zidentyfikowanych grup ataków, co daje dużo możliwości w analizie systemu). W ramach rozdziału 6 Doktorant przedstawił na podstawie samodzielnie skonstruowanego systemu TRM-RET, w jaki sposób można przewidywać wartości zdefiniowanych wcześniej miar wiarygodności zachowania przykładowego systemu. Bardzo cenne jest też zestawienie szerokiej grupy możliwych ataków, ich systematyzacja (także zgrabnie podsumowana w ramach załącznika 4) oraz sprawdzenie, jakie szkody mogą przynosić w przypadku badanego systemu TRM. W ogólności ***przyjęte podejście jest poprawne i zgodne ze sposobami postępowania przyjętymi w odniesieniu do tego rodzaju tematyki.***

Jeśli chodzi o wspomnianą formalizację zagadnienia, to samo jej użycie jest cenne i zasadniczo słuszne. Wprawdzie Doktorant nie przedstawia konsekwentnego systemu aksjomatycznego i gros formalizacji to raczej definicje niż wnioski formalne, a tym bardziej twierdzenia (chociaż Autor formułuje pewne własności, które mają charakter asercji), ale na pewno przyjęte podejście zwiększa zrozumiałość rozprawy. W odniesieniu do niektórych aspektów (jako roszczące sobie generyczność) wykazuje pewne słabości. W niektórych przypadkach miałem wątpliwości nt. przyjętego podejścia, na przykład:

- Drobne kwestie związane z formalizacją:
  - Definicja 5 „zaufania" na str. 23 niebezpiecznie ociera się o błędne koło ew. definiowanie ignotum per ignotum, gdyż użyto w niej słów „ufający", „zaufany", „relacja zaufania", „wartość zaufania". Takie uwikłanie niekoniecznie służy podniesieniu zrozumiałości.
  - Objaśnienie „częściowej addytywności" na str. 24: rozpisano je jako dwie odrębne implikacje; wydaje mi się że obie implikacje powinny być połączone koniunkcją (nie wykluczam, że taka była intencja Autora, ale niejasne jest dla mnie znaczenie użytego średnika).
  - Objaśnienie „niesymetryczności" rozpisane jako zaprzeczenie pewnej implikacji: przez użycie wartości *v* klaryfikacja ta wydaje się mówić więcej niż zwerbalizowane pojęcie „niesymetryczności" (jeśli *v* nie są tylko i jedynie wartościami zero-jedynkowymi, a chyba istotnie Doktorantowi chodziło o tego rodzaju generalizację, chociaż np. na str. 29 wspominany jest system binarny).
  - Definicja 9 „system TRM jest wiarygodny" zdaje się w sposób zero-jedynkowy definiować wiarygodność, ale nie jest jasne, jak odnosi się to do wielopoziomowych wartości zaufania *v*, które są definiowane w innych miejscach pracy.
- Zagadnienia koncepcyjne:
  - Na pochwałę zasługuje fakt, że Doktorant zwraca uwagę na ograniczenia sformułowanego modelu ogólnego systemów TRM. Na przykład idea systemu TRM zdaje się dotyczyć interakcji indywidualnych agentów ze sobą, trzeba jednak pamiętać, że współczesne systemy teleinformatyczne coraz bardziej zależą nawet nie od współpracy podzbioru agentów (o czym wspomina Autor w kontekście zastosowania systemu TRM w odniesieniu do systemów rutingu czy też w ramach dyskusji heterogeniczności agentów), ale nawet ich uporządkowanego podzbioru (jak w przypadku łańcucha usług sieciowych, NFC). Powstaje pytanie, czy

przedstawione koncepcje da się przyłożyć do tego rodzaju praktycznego i współczesnego kontekstu, albo na ile skomplikowane byłoby rozszerzenie proponowanych rozwiązań.

- Kilkukrotnie Autor zwraca uwagę na niemożliwość skonstruowania dokładnego rozwiązania problemu poszukiwania zachowania systemu TRM ze względu na wielość parametrów konfiguracyjnych (w odniesieniu do zachowań atakujących). Nie mam pewności, że Doktorant się myli, ale używane przez niego uzasadnienia nie zawsze są precyzyjne (np. na str. 150 i 154), a niekiedy są nietrafne. Np. w systemach optymalizacyjnych (a niektóre sformułowania, np. z funkcją celu, jak w przypadku funkcji zysku podanej w ramach wzorów 5.1 czy 5.2 wskazują że pewne aspekty działania systemów TRM, jak również ataków na nie, można traktować w tych kategoriach) sam fakt użycia bardzo dużej liczby wartości zmiennych decyzyjnych wcale nie musi świadczyć o istotnych trudnościach obliczeniowych w zakresie uzyskiwania rozwiązania dokładnego. Nawet nieskończona liczba potencjalnych wartości zmiennych wcale nie oznacza sama przez się dużej trudności (jak np. w przypadku programowania liniowego), a jeśli chodzi o niezaniedbywalną liczbę wartości dyskretnych, to trudność w ich przypadku często jest związana z faktem, że problem kombinatoryczny opisywany przez zmienne zawiera wiele wzajemnie wykluczających się warunków. Nie jest dla mnie oczywiste, że akurat taka sytuacja ma miejsce w przypadku opisywanych przez Doktoranta systemów TRM.

Uwagi te należy traktować raczej jako zaproszenie do dyskusji niż krytykę samego podejścia.

6. ORYGINALNOŚĆ ROZPRAWY, SAMODZIELNY DOROBEK AUTORA, POZYCJA ROZPRAWY W STOSUNKU DO STANU WIEDZY (POZIOM TECHNIKI) PREZENTOWANEGO W LITERATURZE ŚWIATOWEJ. Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek Autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?

W dużym stopniu dysertacja stanowi kompilację wcześniej opublikowanych oryginalnych materiałów badawczych (co nie jest wadą, a nawet stanowi zaletę, gdyż wyniki były już zapewne recenzowane i rafinowane). Doktorant opiera się na osiemnastu własnych pracach, w większości opublikowanych po angielsku. Moim zdaniem ***głównym osiągnięciem Autora doktoratu jest przedstawienie uogólnionego i sformalizowanego podejścia do konstrukcji systemów zaufania/reputacji TRM oraz przebadania najbardziej typowych ataków na tego rodzaju systemy***. Praca korzystnie sytuuje się na tle stanu wiedzy, tyle że Doktorant nie dokonał wyczerpującego przeglądu tej wiedzy w ciągu ostatnich kilku lat. Niemniej jednak użycie podejścia sformalizowanego zapewnia, że przedstawione wyniki mają uniwersalne zastosowanie.

7. **POPRAWNOŚĆ PRZEDSTAWIENIA UZYSKANYCH WYNIKÓW. Czy Autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników (zwięzłość, jasność, poprawność redakcyjna rozprawy)?**

Praca jest napisana w języku polskim w sposób poprawny i czytelny. Zdarzają się wprawdzie pewne potknięcia językowe i edycyjne, nie przeszkadzają one jednak w odbiorze pracy. ***Sposób przedstawienia wyników jest dobry*** i wskazuje na umiejętności prowadzenia prac badawczych oraz komunikowania ich wyników.

Tu kilka uwag krytycznych:

- W zasadzie kolejność literatury w doktoracie powinna być dostosowana do kolejności alfabetycznej (na podstawie pierwszego autora), a nie kolejności cytowania.
- W przypadku niektórych pozycji literaturowych brakuje informacji, co to właściwie za tekst (np. [5], [29], [37]).
- Drobne wady edycji, np. zgubione odstępy między cytowaniem a odnośnikiem literaturowym (str. 23) czy „przenikanie" języka angielskiego (najwyraźniej z publikacji obcojęzycznych, w których wcześniej raportowano rezultaty prac) do rysunków zamieszczonych w rozprawie pisanej w języku polskim (np. rysunek 12).
- Pewna liczba potknięć w odniesieniu do użycia języka polskiego:
    - nadużywanie słowa „stworzyć" i pochodnych (lepiej byłoby powiedzieć „opracować" itp.);
    - nadużywanie anglicyzmu „bazować" i pochodnych.

8. **SŁABE STRONY ROZPRAWY, JEJ GŁÓWNE WADY. Jakie są słabe strony rozprawy i jej główne wady?**

Praca ***nie ma słabych stron, które przekreślałyby jej ogólną wartość***. Natomiast można wskazać kilka nieco słabszych aspektów (zostały już zresztą one wspomniane wcześniej):

- Przegląd literatury nie jest konsekwentny – w zasadzie w sposób regularny zatrzymał się kilka lat temu, o ile się nie mylę w okolicach lat 2014-15; potem poza swoimi publikacjami Doktorant cytuje stosunkowo niewielką liczbę prac późniejszych. Jednak w każdym roku pojawiają się teksty na ten temat i nawet jeśli nie są adekwatne do koncepcji tej rozprawy należałoby przynajmniej je pobieżnie wspomnieć i podsumować.
- W przypadku skądinąd bardzo przydatnej formalizacji zagadnienia w odniesieniu do niektórych definicji (zaufanie czy częściowa addytywność) mam wątpliwości odnośnie poprawności. Również kilka aspektów koncepcyjnych (np. uzasadnienie złożoności obliczeniowej niektórych zagadnień związanych z TRM) wymagałoby lepszego doprecyzowania. W szczególności liczę na dyskusję tych zagadnień w trakcie publicznej obrony.

9. PRZYDATNOŚĆ ROZPRAWY DLA NAUK TECHNICZNYCH, PRZEMYSŁU, OBRONNOŚCI KRAJU ITP.

Praca jest ***przydatna dla nauk technicznych*** – w tym przypadku Informatyki Technicznej i Telekomunikacji głównie ze względu na rozbudowanie podejścia formalnego do systemów TRM. Ma też przydatność dla przemysłu teleinformatycznego, gdyż jej wyników można użyć do konstrukcji (a przynajmniej kontroli w pewnych aspektach) wszelkich systemów opartych na interakcji agentów, które używają koncepcji zaufania i jej pochodnych (reputacji) – co obecnie jest powszechną praktyką.

10. PODSUMOWANIE (CZY ROZPRAWA SPEŁNIA WYMAGANIA PRZEZ OBOWIĄZUJĄCE PRZEPISY)

Praca skupia się na istotnym z punktu widzenia użyteczności i ogólnego bezpieczeństwa zagadnieniu zapewniania zaufania i reputacji, przedstawiając przydatne podejście do konstrukcji systemów TRM oraz sprawdzania ich jakości (w aspekcie zaufania). Z tego punktu widzenia przedstawia oryginalne osiągnięcie w zakresie Informatyki Technicznej i Telekomunikacji. Doktorant wykazuje również znajomość systemów tego rodzaju oraz ogólnego kontekstu teleinformatyki (odwołuje się do różnego typu systemów czy technik przy okazji omawiania adekwatnych dla nich systemów TRM). Z tego względu stwierdzam bez wątpliwości, że rozprawa spełnia ***wymagania odnoszące się do obowiązujących przepisów*** w zakresie prac doktorskich (oryginalność i użyteczność rozwiązania oraz potwierdzona wiedza Doktoranta w przedmiotowym obszarze). Wnioskuję o dopuszczenie Doktoranta do dalszych etapów postępowania w zakresie procedury doktoryzacji.

11. OCENA ROZPRAWY. Do której z następujących kategorii Recenzent zalicza rozprawę (niepotrzebne skreślić)?

~~a. Nie spełniająca wymagań stawianych rozprawom doktorskim przez obowiązujące przepisy~~
~~b. Wymagająca wprowadzenia poprawek i ponownego recenzowania.~~
c. Spełniająca wymagania.
~~d. Spełniająca wymagania z wyraźnym nadmiarem.~~
~~e. Wybitnie dobra, zasługująca na wyróżnienie.~~

PODPIS ZAUFANY
PIOTR ARTUR
CHOŁDA
28.07.2023 14:36:45 [GMT+2]
Dokument podpisany elektronicznie
podpisem zaufanym

Piotr Chołda