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