Dr hab. Rafał Różycki, prof. PP
Instytut Informatyki
Politechnika Poznańska
ul. Piotrowo 2, 60-965 Poznań
rafal.rozycki@put.poznan.pl

Poznań, 20.09.2024

Recenzja rozprawy doktorskiej

mjr. mgr. inż. Artura Stachurskiego
p.t.: *Model i metoda prognozowania podatności oprogramowania na zagrożenia w cyberprzestrzeni*

będącej podstawą o ubieganie się o nadanie stopnia naukowego doktora w dyscyplinie naukowej informatyka techniczna i telekomunikacja.

Niniejsza recenzja została przygotowana w odpowiedzi na uchwałę nr 29/RDN ITiT/2024 Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego z dnia 9 lipca 2024 r. w sprawie wyznaczenia recenzentów rozprawy doktorskiej mjr. Mgr. inż. Artura Stachurskiego - absolwenta studiów III stopnia.

Postępowanie odbywa się na podstawie art. 14, ust. 2, pkt. 2 i art. 20 ust. 5 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz.U. z 2017 r. poz.17889 z późn. zm.), art. 6, ust. 1 i 3 rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 19.01.2018 r. w sprawie szczegółowego trybu i warunków przeprowadzania czynności w przewodzie doktorskim, w postępowaniu habilitacyjnym oraz w postępowaniu o nadanie tytułu profesora (Dz.U. z 2018 r. poz.1669, z późn. zm.).

1. Ogólna charakterystyka rozprawy

Do recenzji przedstawiono rozprawę doktorską wydaną w roku 2024 nakładem wydawnictwa Wojskowej Akademii Technicznej. Jedynym autorem pracy jest Doktorant – mjr mgr inż. Artur Stachurski, nad którym opiekę promotorską sprawowali dr hab. inż. Andrzej Najgebauer, prof.WAT oraz płk dr inż. Rafał Kasprzyk. Praca napisana jest po polsku.

2. Cel i zakres rozprawy

Przedstawiona do oceny rozprawa obejmuje wyniki badań z zakresu cyberbezpieczeństwa, a więc obejmuje zagadnienia, które współcześnie mają kluczowe znaczenie dla zapewnienia poprawnego funkcjonowania tzw. cyberprzestrzeni.

Autor swoje zainteresowania badawcze koncentruje na opracowaniu innowacyjnego modelu i dopasowanej do niego metody szacowania podatności oprogramowania na zagrożenia, które w cyberprzestrzeni występują. Jak Autor sam wskazuje, rozważania ograniczone są jedynie do wykrywania podatności dla oprogramowania dedykowanego, stale rozwijanego, dla którego zakłada się, że zebrane informacje o podatnościach są w dużej mierze wynikiem przeprowadzenia szerokich testów bezpieczeństwa.
Mimo tak zarysowanego zakresu pracy, rozprawa wpisuje się w szeroki zakres badań, których celem jest opracowanie metod i narzędzi wykrywania, przeciwdziałania i niwelowania skutków cyberzagrożeń.

3. Teza rozprawy

Autor stawia w swojej pracy następującą tezę:
„Opracowanie modelu i metody prognozowania podatności oprogramowania na zagrożenia w cyberprzestrzeni pozwala na racjonalne kształtowanie poziomu bezpieczeństwa oprogramowania."

4. Układ rozprawy

Obok Wstępu i Podsumowania praca zawiera pięć rozdziałów, Bibliografię, Wykazy tabel i rysunków oraz trzy załączniki.
We Wstępie zarysowany jest kontekst i cel prowadzonych badań, trafnie wskazujący na ich wagę. Na kilku przykładach cyberataków, Doktorant doszukuje się ich przyczyny w powszechnym występowaniu podatności oprogramowania na zagrożenia w cyberprzestrzeni.
W Rozdziale 1 Doktorant obszernie charakteryzuje obszar badań. Bardzo wartościowe wydaje się podanie precyzyjnych definicji pojęć, które często niepoprawnie używane są zamiennie, np. zagrożenie – podatność, incydent – atak. Ponadto przytoczone są znane z literatury taksonomie podatności, opisany cykl życia podatności oprogramowania i zebrane w czytelne zestawienie dane dotyczące liczby występujących podatności na przestrzeni kilku wybranych lat.
Rozdział 2 stanowi cenny i bardzo starannie przygotowany przegląd znanych z literatury modeli i metod analizy i prognozowania podatności oprogramowania. Układ i prezentacja zebranego materiału świadczą o dobrym rozeznaniu Doktoranta w przedmiotowym obszarze badań.
Rozdział 3 jest kluczowy zawiera bowiem opis oryginalnych modeli prognozowania podatności oprogramowania. Zaproponowany ogólny model wykrywania podatności bazuje na czterostanowym łańcuchu Markowa, o szczegółowo opisanych stanach (tzw. stanach bazowych) i interpretacji potencjalnych przejść między nimi. Autor wskazuje na zalety takiego podejścia, a wśród nich na: naturalne odwzorowanie sekwencyjnej natury rozwoju oprogramowania, praktycznie uzasadnionej możliwości predykcji stanów przyszłych na bazie stanu bieżącego, prostotę finalnego modelu. Rozwinięciem modelu ogólnego jest model, w którym dodatkowo dopuszcza się działania profilaktyczno-naprawcze, co znajduje odwzorowanie w uwzględnieniu dwóch dodatkowych przejść we wcześniej zaproponowanym czterostanowym łańcuchu Markowa. Oba modele rozwija się do postaci szczegółowej uwzględniając tzw. przejścia wielokrokowe między stanami bazowymi. Zastosowany model szczegółowy bez działań profilaktyczno-naprawczych pozwala obliczyć poziom bezpieczeństwa oprogramowania i intensywność wykrywania krytycznych podatności oprogramowania. Dzięki szczegółowemu modelowi z działaniami profilaktyczno-naprawczymi jesteśmy w stanie ocenić czy działania profilaktyczno-naprawcze są skuteczne. Rozdział kończy czytelnie zaprezentowany przykład obliczeniowy, w którym wykorzystano pojedynczy, ale bogaty zestaw danych rzeczywistych.

Rozdział 4 prezentuje oryginalne osiągnięcia Doktoranta z zakresu klasyfikacji podatności na podstawie danych historycznych pozyskiwanych z dedykowanych baz. Autor wykorzystuje tu walidację krzyżową i cztery znane z literatury metody klasyfikacji. Swoje podejście ilustruje przykładem obliczeniowym bazującym na danych rzeczywistych.
Rozdział 5 zawiera istotną wartość dodaną do zaproponowanych w poprzednich rozdziałach modeli i metod. Stanowi on opis oryginalnego oprogramowania, w którym zaproponowane podejścia zaimplementowano. Wygodny interfejs graficzny oraz pełna automatyzacja obliczeń, pozwalają prześledzić prognozowanie podatności oprogramowania i działanie wybranych modeli klasyfikacji dla różnych danych wejściowych.
Struktura pracy jest bez zarzutu – właściwie prezentuje zgromadzony materiał badawczy.

5. Uwagi merytoryczne

5.1. Przyjęta teza rozprawy ma charakter zbyt ogólny. Domyślam się, że nie było intencją Autora wykazywanie, że do racjonalnego kształtowania poziomu bezpieczeństwa oprogramowania wystarczy opracowanie jakiegokolwiek modelu i metody prognozowania podatności oprogramowania na zagrożenia w cyberprzestrzeni. Prawdopodobnie zamiarem autora było wskazać użyteczność w tym zakresie własnego, autorskiego rozwiązania, przedstawionego w rozprawie.

5.2. W punkcie 3.1.2 Autor zamieszcza dwa twierdzenia (Twierdzenie 3 i Twierdzenie 4). Nie jest jasne, czy są one oryginalnym wkładem Doktoranta, czy też zostały zaczerpnięte z innych prac. W pierwszym przypadku należałoby przeprowadzić dowód sformułowanego twierdzenia. Być może jest jednak tak, że nie są to jednak twierdzenia, a raczej definicje pojęć „prawdopodobieństwo dojścia" i „średnie czasy dojścia".

5.2. W punkcie 3.5 wprowadzono pewien zabieg natury numerycznej (tzw. "zaburzenie przejścia"), dzięki któremu udało się uniknąć osobliwości macierzy przejść. Czy można przedstawić praktyczną interpretację zastosowanego podejścia? Jaki wpływ na obliczane dzięki proponowanym modelom miary miałaby zmiana przyjętej perturbacji (o wartości 0,001) na wartość wyższą?

5.3. W przykładzie obliczeniowym dotyczącym klasyfikacji podatności (pkt. 4.3) niepokoi swoboda z jaką Autor decyduje o tym, którą walidację krzyżową (dla jakiej wartości k) wskazać jako najlepszą. Jest to *de facto* problem wielokryterialny (co najmniej dwukryterialny) i należałoby tu zaproponować jakąś prostą, ale matematycznie jednoznaczną metrykę oceny.

5.4. Niezręcznie brzmi komentarz do równań (4.17) i (4.18): „Jeśli powyższe równanie przyjmuje wartości dodatnie…". Równanie nie może przyjmować wartości!

5.5. W punkcie 4.4, na bazie przeprowadzonych obliczeń, podejmowana jest próba wskazania optymalnego modelu klasyfikacji. Warto w tym miejscu podkreślić, że wybrany w ten sposób model jest najlepszy tylko dla zestawu danych użytych do obliczeń, nie ma on charakteru optimum globalnego.

6. Strona redakcyjna rozprawy

Recenzowana rozprawa od strony redakcyjnej jest przygotowana bardzo starannie. Jak każda tak obszerna praca - tak i ona - nie jest wolna od pewnych mankamentów. Dziwi brak streszczenia pracy przygotowanego w języku angielskim. Streszczenie takie wydaje się niezbędnym minimum do szerszego popularyzowania innowacyjnego charakteru przeprowadzonych badań.
W pracy występują też nieliczne błędy językowe i literowe. Ponadto brakuje odnośników w tekście do niektórych rysunków. Na licznych rysunkach w Rozdziale 4 brakuje opisu jednej z osi, ponadto w miejsce wykresów punktowych (wartości *Error rate* dla całkowitych wartości k), prezentowane są wykresy liniowe.
Zaletą pracy jest bez wątpienia poprawność stylistyczna prezentowanego materiału.

7. Wniosek końcowy

Zaprezentowany w rozprawie oryginalny wkład badawczy Doktoranta jest bardzo ciekawy i celnie adresujący wyzwania współczesnej cyberprzestrzeni. Przedstawiona do oceny praca jest rzetelnym kompendium wiedzy na temat oceny podatności oprogramowania. Proponując własne modele i metody, Autor dobitnie wykazał swoje ponadprzeciętne kompetencje z zakresu zastosowań metod statystycznych. Jego warsztat badawczy można uznać za dojrzały i dobrze rokujący w perspektywie kontynuowania podjętych badań.
Do głównych osiągnięć Doktoranta zaliczam:
- przygotowanie wyczerpującego przeglądu literatury pod kątem metod analizy i prognozowania podatności oprogramowania;
- opracowanie oryginalnych modeli wykrywania podatności oprogramowania (użytecznych w zakresie przyjętym przez Autora);
- opracowanie oryginalnej metody wyznaczania intensywności wykrywania krytycznych podatności oprogramowania;
- opracowanie oryginalnej metody oceny poziomu bezpieczeństwa oprogramowania;
- opracowanie oryginalnej metody oceny skuteczności działań profilaktyczno-naprawczych w zakresie eliminacji podatności oprogramowania;
- przygotowanie zaawansowanego oprogramowania do praktycznej weryfikacji zaproponowanych podejść.

W związku z powyższym uznaję recenzowaną rozprawę za osiągniecie w pełni spełniające wymogi odpowiednich przepisów i wystarczające do skierowania wniosku mjr. mgr. inż. Artura Stachurskiego, o nadanie stopnia naukowego doktora w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja do kolejnych etapów postępowania.

Dr hab. inż. Rafał Różycki, prof. PP