Warszawa, dn. 01.02.2022 r.

Dr hab. inż. Zbigniew Piotrowski, prof. WAT

Wojskowa Akademia Techniczna
Wydział Elektroniki
ul. Gen. S. Kaliskiego 2,
00-908 Warszawa

# RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY NAUKOWEJ DYSCYPLINY INFORATYKA TECHNICZNA I TELEKOMUNIKACJA POLITECHNIKI WARSZAWSKIEJ

**Tytuł rozprawy:** **Orkiestracja narzędzi bezpieczeństwa w sieci operatora telekomunikacyjnego z wykorzystaniem technik uczenia maszynowego oraz metod przetwarzania języka naturalnego.**

**Autor rozprawy:** **mgr inż. Grzegorz Siewruk**

1. **Jakie zagadnienie naukowe jest rozpatrzone w pracy (teza rozprawy) i czy zostało ono dostatecznie jasno sformułowane przez Autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, itd.) ?**

Rozprawa autorstwa Pana mgr inż. Grzegorza Siewruka, stanowi wynik jego prac nad doktoratem wdrożeniowym. Rozprawa ma charakter doświadczalny i jednocześnie praktyczny bo potwierdzony rzeczywistym wdrożeniem systemu o nazwie Mixeway do procesu dostarczania oprogramowania w firmie telekomunikacyjnej.

W przedłożonej do recenzji pracy, zostały poddane analizie mechanizmy uczenia maszynowego do klasyfikacji podatności bezpieczeństwa w oprogramowaniu. Do wykrywania podatności w bezpieczeństwie oprogramowania, wykorzystano skanery działające zarówno statycznie jak i dynamicznie. Skanery te wykrywają błędy w oprogramowaniu. Wykryte błędy są zbiorem wejściowym, który następnie jest ręcznie dzielony na dwie grupy. Pierwszą grupą są potwierdzone podatności, które powinny być poprawione a drugą grupę stanowią te potwierdzone podatności które nie są istotne. Do klasyfikacji wykorzystano również metody przetwarzania języka naturalnego. Klasyfikator wynikowy został wdrożony jako część systemu odpowiadającego za orkiestrację narzędzi bezpieczeństwa w procesie wytwarzania oprogramowania.

Doktorant wyartykułował, na stronie nr 20 recenzowanego opracowania, cztery cele rozprawy:

Cel pierwszy: eksperymentalne porównanie dokładności algorytmów uczenia maszynowego wykorzystując techniki przetwarzania języka naturalnego pod kątem możliwości ich wykorzystania w celu wsparcia procesów związanych z zapewnieniem bezpieczeństwa w łańcuchu dostarczania oprogramowania.

Cel drugi: zaprojektowanie oraz implementacje, rozwiązania, które orkiestruje prace, narzędzi bezpieczeństwa takich jak skanery podatności oraz wykorzystuje implementacje wybranego klasyfikatora w celu wsparcia procesu decyzyjnego dotyczącego wdrożenia oprogramowania.

Cel trzeci: wdrożenie rozwiązania w rzeczywistej sieci operatora telekomunikacyjnego.

Cel czwarty: udowodnienie skuteczności wdrożonego rozwiązania bazującego na danych historycznych.

W oparciu o powyższe cele rozprawy Doktorant postawił następującą tezę:

*"Możliwe jest stworzenie i wdrożenie w sieci operatora telekomunikacyjnego efektywnego systemu teleinformatycznego, który pełni rolę orkiestratora narzędzi bezpieczeństwa oraz wykorzystuje sieci neuronowe w celu określenia, które z wykrytych podatności są konieczne do poprawy przez zespoły programistyczne, co w rezultacie spowoduje wzrost liczby przeprowadzonych testów bezpieczeństwa oraz poprawi poziom zabezpieczeń projektu, w ramach którego zostanie uruchomiony".*

Stwierdzam, że zarówno cele rozprawy jak też sama jej teza zostały sformułowane poprawnie i jasno pod względem naukowym. Cele są powiązane ze sobą logicznie i stanową spójny proces dowodzenia tezy.

2. **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?**

W pracy wykazano 132 pozycje literaturowe nawiązujące swoją treścią do przedmiotu rozprawy. W ramach bibliografii wykazano również odnośniki do adresów url, które są przywoływane w pracy jako referencje tematycznie związane z poruszanymi zagadnieniami. W szczególności w rozdziale drugim, poświęconym przeglądowi istniejących rozwiązań, występuje wiele odnośników do aktualnych implementacji metod i klasyfikatorów podatności

bezpieczeństwa oprogramowania. Stwierdzam zatem, że dobór literatury oraz wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący.

3. **Czy Autor rozwiązał postawione zagadnienia? Czy użył do tego właściwych metod i czy przyjęte założenia są uzasadnione?**

W celu udowodnienia tezy, postawionej przez autora rozprawy, autor podzielił tę rozprawę na osiem rozdziałów.

Do grupy pierwszej tzw. opisowej i podsumowującej zastany stan techniki, zaliczam rozdziały: drugi, trzeci oraz czwarty. W tych to rozdziałach dokonano przeglądu istniejących rozwiązań orkiestracji narzędzi bezpieczeństwa, wykrywania i klasyfikacji podatności w bezpieczeństwie oprogramowania. Doktorant omówił metodyki prowadzenia projektów IT. Na potrzeby podsumowania algorytmów uczenia maszynowego autor rozprawy przedstawił ich klasyfikację w oparciu o takie algorytmy przetwarzania danych jak: las losowy, sieci neuronowe, maszynę wektorów nośnych. Autor rozprawy wspomniał również o metodach przetwarzania języka naturalnego.

Do grupy drugiej tzw. zasadniczej, stanowiącej o faktycznej wartości pracy, zaliczam rozdziały piąty, szósty, siódmy i ósmy. To właśnie w rozdziale piątym Doktorant opisał architekturę i sposób wdrożenia opracowanego przez siebie systemu Mixeway. W rozdziale szóstym w kolei Doktorant opisał metodykę badawczą a wyniki badań eksperymentalnych zawarł w rozdziale siódmym. Ósmy rozdział stanowi natomiast podsumowanie pracy.

Wynikiem pracy naukowej jest opracowanie i wdrożenie do procesu CI/CD oprogramowania Mixeway składającego się z trzech głównych modułów: wykrywania zasobów, zarządzania skanami bezpieczeństwa oraz korelacji wyników. Warto przy tym zaznaczyć że oprogramowanie jest udostępnione publicznie w formie otwartego kodu źródłowego na serwisach: GitHub oraz Docker Hub. System w swojej architekturze został podzielony na trzy elementy logiczne. Interfejs GUI wykorzystujący technologię Angular, oraz serwer aplikacyjny Nginx stanowi pierwszy blok logiczny. Drugim blokiem jest element logiki biznesowej na bazie Technologii Spring Boot. Trzecim elementem systemu jest baza danych PostgreSQL oraz sejf na hasła Hashicorp Vault. System posiada wtyczki programowe integrujące skanery statyczne (*Microfocus Fortify, Checkmarx*), skanery dynamiczne (*Burp Enterprose Edition, Acunetix*), skanery sieciowe (*Nessus Professional, Nexpose, Greenbone Vulnerability Manager*) oraz skanery bibliotek (*OWASP Dependency Track*). Doktorant wprowadził metrykę CRV do podejmowania decyzji dotyczącej selekcji zgłoszonych błędów

klasyfikującą do poprawy w testowanym oprogramowaniu oraz metrykę DNRV dla klasyfikacji nieistotnych błędów. Istotną częścią oprogramowania jest model korelacji wyników wykorzystujący model sieci neuronowej. Bramka bezpieczeństwa jest z kolei elementem udostępniającym informację czy testowana aplikacja spełnia przyjętą politykę bezpieczeństwa.

Przyjęte zasady i założenia oparte o reguły polityk bezpieczeństwa oraz modułowy charakter oprogramowania polegający na wymianie lub dobudowywaniu np. kolejnych skanerów bezpieczeństwa, są poprawne i zgodne ze standardami tworzenia oprogramowania jako elementu procesu CD/CI.

Doktorant podzielił wdrożenie systemu Mixeway na pięć etapów, których realizacja precyzyjnie wyznaczała tempo i zakres prac projektowych. Do tych etapów Doktorant zaliczył: opracowanie procedury zarządzania podatnościami, wdrożenie modułu detekcji zasobów, wdrożenie modułu zarządzania testami bezpieczeństwa, opracowanie i wdrożenie modułu korelacji wyników oraz wdrożenie bramki bezpieczeństwa w łańcuchu dostarczania oprogramowania. Przeprowadzona przez Doktoranta analiza stanu przed i po wdrożeniu systemu Mixaway w środowisku operatora telekomunikacyjnego wyraźnie wskazuje na zdecydowane zwiększenia liczby przeprowadzonych testów sieciowych, statycznych SAST, dynamicznych DAST oraz testów OpenSource. Ponadto, dzięki wdrożeniu Mixaway zdecydowanie zwiększono zasoby objęte testami podatności pod względem testowanych aplikacji internetowych oraz pod względem testowanych repozytoriów kodu źródłowego.

Doktorant przeprowadził badania na podstawie których:

1. Opracował klasyfikatory na bazie modeli przygotowanych za pomocą SVM, sieci neuronowych oraz lasu losowego.
2. Porównał wartości podstawowych metryk dla opracowanych klasyfikatorów.
3. Zaprojektował i zrealizował prototyp aplikacji implementującej wybrany algorytm jako jeden z komponentów systemu Mixaway zawarty w module korelacji wyników.

Przyjęta metodyka badawcza jest zgodna z kanonem tworzenia oprogramowania zawiewającego eksperymentalne moduły klasyfikacji podatności. W świetle przedstawionych wyników należy stwierdzić, że autor rozwiązał postawione w pracy zagadnienia badawcze które przyniosły, potwierdzony eksperymentalnie, efekt opisany wynikami eksperymentów.

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

Praca jest oryginalna i posiada wiele elementów świadczących o jej wartości naukowej w zastosowaniu praktycznym. Autor samodzielnie opracował koncepcję oraz zaimplementował i przetestował system Mixaway do orkiestracji narzędziami skanowania błędów w oprogramowaniu w procedurze CD/DI. Autor zaproponował klasyfikatory metod uczenia maszynowego w tym na bazie sieci neuronowej, które pozwalają na automatyzację i poprawną klasyfikację wykrytej podatności. W procedurze przetwarzania wstępnego danych wejściowych autor rozprawy wykorzystał elementy technik przetwarzania języka naturalnego w formie tokenizacji danych. Doktorant wybrał hiperparametry algorytmów uczenia maszynowego zaadoptowanych do klasyfikacji podatności za pomocą dostrajania. W przypadku wariantów sieci neuronowych NN, CNN, RNN LSTM oraz RNN była to liczba warstw sieci oraz funkcja aktywacji i normalizacji, w przypadku algorytmu SVM była to funkcja jądra, parametr gamma funkcji jądra i parametr normalizacyjny C, natomiast w przypadku algorytmu Lasu Losowego była to liczba drzew, kryterium podziału, maksymalna głębokość drzewa oraz minimalna liczba przykładów dla konkretnego podziału.

Oryginalność rozprawy, w moim rozumieniu, polega tutaj na automatyzacji procesu klasyfikacji potwierdzonych przypadków naruszeń bezpieczeństwa w formie błędów wykrywanych na wczesnym etapie procedury CD/CI za pomocą metod uczenia maszynowego. Na podstawie opracowanych wyników eksperymentów przytoczonych w rozdziale 7, w zagadnieniu klasyfikacji podatności bezpieczeństwa najkorzystniejsze wyniki przyniosło zastosowanie algorytmów: Lasu Losowego, Rekurencyjnej Sieci Neuronowej LSTM oraz Konwolucyjnej Sieci Neuronowej. Skuteczna klasyfikacja przypadków jako potwierdzonych i skierowanych do poprawy CRV (ang. *Confirmed and Relevant Vulnerbility*) oraz przypadków wykrytych ale nieistotnych pod względem poprawy (DNRV – ang. *Detected but Not Relevant Vulnerability*), jak również niewielki odsetek fałszywych alarmów osiągnięty w procesie dostrajania wdrożonego oprogramowania, potwierdza zasadność opracowanych modeli klasyfikatorów.

5. **Czy autor wykazał umiejętności poprawnego i przekonywającego przedstawienia uzyskanych przez siebie wyników (zwięzłość, jasność, poprawność redakcyjna rozprawy) ?**

Rozprawa jest poprawnie zorganizowana tematycznie i stanowi logiczny ciąg dowodzenia tezy. W szczególności opis zaimplementowanego systemu Mixeway w rozdziale piątym oraz wyniki badań eksperymentalnych w rozdziale siódmym, zostały opisane przez autora w sposób jasny z obszernym komentarzem i zastosowaniem języka opisu technicznego. Zastosowane metryki oraz przedstawione w pracy ich wartości jako wyniki eksperymentów są czytelne i dokładnie omówione. Autor tym samym wykazał umiejętności poprawnego i przekonywującego merytorycznie przedstawienia uzyskanych przez siebie wyników. Praca jest poprawnie zredagowana i nie natrafiłem podczas jej recenzji na błędy edycyjne.

Warto nadmienić, że wyniki pracy zostały opublikowane w dwóch periodykach naukowych:

1. Siewruk G, MazurczykW. Context-Aware Software Vulnerability Classification using Machine Learning. IEEE Access. 2021 Apr 23.
2. Siewruk G,MazurczykW, Karpiński A. Security Assurance in DevOpsMethodologies and Related Environments. International Journal of Electronics and Telecommunications.2019May 19;65(2):211-6.

oraz zostały wygłoszone na trzech konferencjach:

1. Siewruk G. O tym jak (nie)łatwo dodać Sec do Dev(Sec)Ops w świecie telco. PLNOG19.Kraków 2019.
2. Siewruk G. O tym jak mało jest Sec w Dev(Sec)Ops podczas testów aplikacji. WTH19.Warszawa 2019.
3. Siewruk G. Klasyfikacja podatności jako weryfikacja w procesach automatycznego dostarczania oprogramowania. Advanced Threat Summit. Warszawa 2020.

Wyniki pracy zostały również opisane w prasie:

1. Orange Funds New CI/CD Security Tool, HardenStance Briefing, 2020.

Warto również odnotować nagrody jakie autor uzyskał za wdrożone oprogramowanie Mixeway:

1. Nagroda szefa funkcji Sieć i Technologie 2019 - przyznawana raz w roku za bardzo dobre wyniki lub wyjątkowe postawy w projektach o największym znaczeniu dla realizacji rocznych celów danej funkcji. Przyznawana przez Członka

Zarządu ds. Sieci i Technologii Orange Polska.

2. Security & Privacy Awards 2021 - Coroczny konkurs nagradzający najlepsze rozwiązania, wpływające na bezpieczeństwo w Grupie Orange. Nagroda przyznawana jest przez jury, na którego czele stoi dyrektor wykonawczy ds. Strategii i Cyberbezpieczeństwa Grupy Orange.

**6. Jakie są słabe strony rozprawy i jej główne wady ?**

W pracy zabrakło wyraźnego rozróżnienia na którym etapie jest realizowana procedura automatyzacji wykrywania podatności. Z treści pracy wynika, że orkiestracja skanerami bezpieczeństwa wyzwala automatyczne procesy skanowania podatności natomiast klasyfikacja odbywa się przez wykorzystanie modułów uczenia maszynowego. Na str. 19 rozprawy autor napisał, że „Stworzony zestaw danych zostanie ręcznie podzielony na dwie grupy – podatności które są potwierdzone i powinny być poprawione (ang. *Confirmed and Relevant Vulnerability* - CRV) oraz wykryte ale nieistotne (ang. *Detected but not Relevant Vulnerability* - DNRV). Ponadto, zaznaczono również, że to operator dokonuje finalnej klasyfikacji czy mamy do czynienia z fałszywie pozytywnymi (FP) przypadkami czy też nie. W przypadku pomyłki systemu jako FP i rozstrzygniętego przez operatora, wynik taki jest zwracany jako brak błędu z powrotem do maszyny uczącej tym samym zmniejszając liczbę generowanych przez system fałszywie pozytywnych przypadków.

Przydatne na potrzeby udokumentowania skuteczności działania systemu Mixeway byłoby również przedstawienie wykresów obrazujących efektywność detekcji CRC/DNRV w funkcji wykrytej liczby podatności. Warto byłoby również w pracy wyraźnie podsumować w jakich etapach wykorzystano technikę przetwarzania języka naturalnego. Recenzent dopatrzył się wykorzystania tej techniki na potrzeby wstępnego przetwarzania danych na etapie tokenizacji danych.

**7. Jaka jest przydatność rozprawy dla nauk technicznych?**

Wyniki rozprawy zostały wdrożone do praktyki gospodarczej operatora telekomunikacyjnego w formie zaimplementowanego systemu Mixeway. System podniósł w sposób zdecydowany bezpieczeństwo dostarczania oprogramowania w procesie CD/CI, poprzez masową eksplorację aplikacji internetowych i repozytoriów kodu źródłowego z wykorzystaniem testów podatności sieciowych, statycznych, dynamicznych oraz testów OpenSource. O braku na rynku podobnej klasy rozwiązań może świadczyć duża liczba pobrań tego oprogramowania z platformy do współdzielenia kodu GitHub. System został udostępniony na tej platformie na zasadzie licencji GPL-3.0.

Treść rozprawy może stawność dobry zaczyn do kolejnych implementacji opartych o metody uczenia maszynowego na potrzeby skanerów bezpieczeństwa systemów sieci definiowanych programowo. Wyniki badań nad algorytmami uczenia maszynowego mogą być też dobrą podstawą do opracowania automatycznych i skutecznych sposób detekcji i predykcji ataków przeprowadzanych na zasoby sieci komputerowych.

8. **Do której z następujących kategorii Recenzent zalicza rozprawę:**
   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) <u>wybitnie dobra, zasługująca na wyróżnienie.</u>**

**Wniosek**

Biorąc pod uwagę przedstawioną przez Doktoranta mgr inż. Grzegorza Siewruka rozprawę stwierdzam, że spełnia ona wymagania stawiane rozprawom doktorskim przez obowiązującą Ustawę o stopniach i tytule naukowym, i wnioskuję o dopuszczenie jej do publicznej obrony. Uważam tę pracę za przykład bardzo dobrze wykonanego doktoratu wdrożeniowego z potwierdzoną praktyczną implementacją opracowanej metody oraz jej udokumentowanymi efektami w procesie wytwarzania oprogramowania. Według mnie praca zasługuje na wyróżnienie.

Wojciech Kmiecik

.....

podpis