RADA NAUKOWA DYSCYPLINY
INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA POLITECHNIKI WARSZAWSKIEJ

zaprasza na

PUBLICZNĄ OBRONĘ ROZPRAWY DOKTORSKIEJ

mgr. inż. Grzegorza Siewruka

która odbędzie się w dniu **6 kwietnia 2022 roku o godzinie 10:00** w trybie zdalnym

Temat rozprawy doktorskiej:

„ Orkiestracja narzędzi bezpieczeństwa w sieci operatora telekomunikacyjnego z wykorzystaniem technik uczenia maszynowego oraz metod przetwarzania języka naturalnego”

Promotor: dr hab. inż. Wojciech Mazurczyk - Politechnika Warszawska

Recenzenci: dr hab. inż. Zbigniew Piotrowski – Wojskowa Akademia Techniczna w Warszawie

dr hab. inż. Robert Burduk - Politechnika Wrocławska

dr hab. inż. Rafał Leszczyna – Politechnika Gdańska

* Obrona odbędzie się zdalnie na platformie MS Teams. Osoby zainteresowane uczestnictwem w obronie proszone są o zgłoszenie chęci uczestnictwa w formie elektronicznej na adres sekretarza komisji: dr hab. inż. Marcin Kowalczyk, prof. uczelni – email :

marcin.kowalczyk@pw.edu.pl do dnia 04.04.2022 do godz.12.00.

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://bip.pw.edu.pl/Postepowania-w-sprawie-nadania-stopnia-naukowego/Doktoraty/Wszczete-po-30-kwietnia-2019-r/Dyscyplina-informatyka-techniczna-i-telekomunikacja-dziedzina-nauk-inzynieryjno-technicznych/mgr-inz.-Grzegorz-Siewruk.

Przewodniczący Rady Naukowej Dyscypliny Informatyka Techniczna i Telekomunikacja Politechniki Warszawskiej

dr hab. inż. Jarosław Arabas

Streszczenie

Orkiestracja narzędzi bezpieczeństwa w sieci operatora telekomunikacyjnego z wykorzystaniem technik uczenia maszynowego oraz metod przetwarzania języka naturalnego

Coraz więcej zespołów wytwarzających oprogramowanie korzysta obecnie z rozwiązań pozwalających na automatyzację większości czynności, które jeszcze kilka lat temu były wykonywane manualnie. Tego typu zmiany pozwalają na zwiększenie elastyczności procesów wytwarzania oprogramowania oraz umożliwiają szybsze wdrażanie zmian w oprogramowaniu i ich udostępnianiu użytkownikowi końcowemu. Niestety prowadzi to również do pewnych niedogodności. Największą z nich jest problem z zapewnieniem bezpieczeństwa tak zbudowanemu procesowi, w którym kod źródłowy aplikacji może się zmieniać nawet kilkanaście razy dziennie. Do dyspozycji zespołów bezpieczeństwa jest różnego rodzaju oprogramowanie, pozwalające na wykonywanie skanów podatności (w tym modelu realizacją manualnych testów bezpieczeństwa nie jest możliwa z uwagi na wolumen zmian).

Niestety automatyczne wykonywanie skanów podatności wiąże się ze zgłaszaniem (przez narzędzia) bardzo dużej liczby naruszeń, które muszą być odpowiednio przeanalizowane. Zarządzanie podatnościami bezpieczeństwa raportowanymi przez różnego rodzaju oprogramowanie skanujące jest skomplikowanym i czasochłonnym zajęciem. Konkretne błędy bezpieczeństwa mogą mieć różny wpływ na system teleinformatyczny w zależności od kontekstu, w jakim on działa. Co więcej, liczba błędów zgłaszanych przez konkretne rozwiązania może być bardzo duża (od kilkuset do kilku tysięcy), co zdecydowanie utrudnia analizę oraz określanie odpowiednich priorytetów dotyczących tego, które błędy należy usunąć w pierwszej kolejności.

Aby rozwiązać przedstawione powyżej problemy, w niniejszej rozprawie przedstawiono koncepcję rozwiązania *Mixeway*, które zostało wdrożone w infrastrukturze rzeczywistego operatora telekomunikacyjnego. Wspomniany system jest odpowiedzialny za orkiestrację pracy narzędzi bezpieczeństwa oraz umożliwia klasyfikację wykrytych podatności. Wykorzystany w *Mixeway* klasyfikator został przygotowany w procesie nauczania opartego o rzeczywiste dane zbierane przez 12 miesięcy z produkcyjnie działających aplikacji. Zebrane zagrożenia klasyfikowane są do jednej z dwóch kategorii: konieczne do poprawy w badanym kontekście (ang. Confirmed and Relevant Vulnerability - CRV) oraz nieistotne w badanym kontekście (ang. Detected but Not Relevant Vulnerability - DRNV). Wyniki uzyskane przez opracowany system *Mixeway* pozwalają potwierdzić skuteczność przedstawionego rozwiązania w kontekście automatycznej weryfikacji zagrożeń w procesie dostarczania oprogramowania.

Słowa kluczowe: bezpieczeństwo IT, CICD, devsecops, uczenie maszynowe

dr hab. inż. Robert Burduk
Politechnika Wrocławska
Wydział Informatyki i Telekomunikacji
Ul. Wybrzeże Stanisława Wyspiańskiego 27
50-370 Wrocław

Wrocław, dnia 21.12.2021 r.

RECENZJA

rozprawy doktorskiej mgra inż. Grzegorza Siewruka

zatytułowanej: **„Orkiestracja narzędzi bezpieczeństwa w sieci operatora telekomunikacyjnego z wykorzystaniem technik uczenia maszynowego oraz metod przetwarzania języka naturalnego"**

Recenzja została sporządzona w związku z powołaniem przez Radę Naukową Dyscypliny Informatyka Techniczna i Telekomunikacja Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej, piszącego niniejszą recenzję, jako recenzenta rozprawy doktorskiej mgra inż. Grzegorza Siewruka pismem z dnia 25 października 2021 r.

Kryteria oceny dysertacji wynikają z przepisów zawartych w art. 187 Ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2021 r. poz. 478).

Problem badawczy i jego znaczenie

Zakres recenzowanej rozprawy dotyczy szerokiej i dynamicznie rozwijającej się problematyki bezpieczeństwa systemów informatycznych. W szczególności Doktorant koncentruje się na zagadnieniach dotyczących automatyzacji (orkiestracji) systemu informatycznego dedykowanego do zapewnienia bezpieczeństwa w łańcuchu dostarczania oprogramowania. W rozprawie zdefiniowano zagadnienie binarnej klasyfikacji nadzorowanej, który dotyczy wykrywania błędów krytycznych lub nieistotnych z punktu widzenia bezpieczeństwa oprogramowania. Problem badawczy recenzowanej rozprawy obejmuje zatem zakresem automatyzację procesów występujących w systemach informatycznych oraz wykorzystanie metod uczenia maszynowego w tworzeniu modelu predykcyjnego.

W rozprawie sformułowano hipotezę badawczą, która zakłada, że wykorzystanie w procesie automatyzacji narzędzi bezpieczeństwa metod uczenia maszynowego może skutkować trafniejszym wskazaniem, które podatności bezpieczeństwa powinny być

poprawiane przez zespół programistów. Postawiona hipoteza badawcza nie budzi zastrzeżeń i jednocześnie definiuje szczegółowe cele badawcze dysertacji. Jednym z celów jest zastosowanie opracowanych wyników badań w sferze gospodarczej, którą jest system informatyczny operatora telekomunikacyjnego. Eksperymentalna weryfikacja postawionej hipotezy badawczej została wykonana z wykorzystaniem rzeczywistego zbioru danych zawierającego 53665 obiekty uczące zebrane z produkcyjnie działających aplikacji.

Tematyka podjęta przez mgra inż. Grzegorza Siewruka jest interesująca, w pełni uzasadniona i odpowiada na wyzwania współczesnej informatyki dotyczące cyberbezpieczeństwa, automatyzacji procesów w systemach informatycznych oraz wykorzystania metod uczenia maszynowego. Recenzowana rozprawa bez wątpienia podejmuje wątek badawczy mieszczący się w zakresie dyscypliny Informatyka Techniczna i Telekomunikacja.

Struktura pracy oraz wiedza Autora

Recenzowana praca została napisana w języku polskim i liczy 105 stron maszynopisu. Składa się z sześciu rozdziałów merytorycznych, wprowadzenia, podsumowania, bibliografii, listy skrótów, spisu tabel, spisu rysunków, załączników, streszczenia w języku polskim oraz angielskim. Rozdział nr 1 przedstawia kolejno: motywację dotyczącą podjęcia tematyki badawczej, sformułowaną hipotezę badawczą, cele pracy oraz strukturę dysertacji. Lista publikacji mgra inż. Grzegorza Siewruka wraz z informacją o uzyskanych nagrodach znajduje się przed wspomnianym rozdziałem.

Rozdział 2 zawiera wprowadzenie do problematyki cyberbepieczeństwa oraz wykorzystania metod uczenia maszynowego do detekcji anomalii lub ataków sieciowych. W szczególności Autor przedstawił zagadnienia związane z systemami wykrywania włamań, automatyzacji (orkiestracji) procesów zachodzących w systemach informatycznych oraz omówił wykorzystanie uczenia nadzorowanego w predykcji podatności bezpieczeństwa. Rozdział 2 zakończony jest podsumowaniem, w którym przedstawiono zalety opracowanego w pracy systemu o nazwie *Mixeway* służącego automatyzacji narzędzi bezpieczeństwa działających w łańcuchu dostarczania oprogramowania w kontekście cech innych systemów, o zbliżonych funkcjonalnościach, znanych z literatury tematu.

Rozdział 3 dysertacji przedstawia metodyki dotyczące prowadzenia projektów (model kaskadowy oraz zwinny wywodzący się z manifestu zwinnego wytwarzania oprogramowania) wraz z łańcuchem dostarczania oprogramowania w koncepcji ciągłej integracji i wdrażania.

Wykorzystane w badaniach eksperymentalnych metody uczenia maszynowego, takie jak sieci neuronowe, las losowy oraz maszyna wektorów nośnych zostały przedstawione w Rozdziale 4. Dodatkowo Autor dysertacji w punkcie 4.4 opisał skrótowo problematykę przetwarzania języka naturalnego.

Rozdział 5 recenzowanej rozprawy przedstawia architekturę opracowaną przez Doktoranta, której celem jest automatyzacja procesów bezpieczeństwa działających w koncepcji ciągłej integracji i wdrażania oprogramowania. Autorska architektura została nazwana *Mixeway* i składa się z trzech modułów: wykrywania zasobów, zarządzania skandami bezpieczeństwa oraz korelacji wyników. Poszczególne punkty Rozdziału 5 opisują logiczne elementy oraz powiązania między tymi elementami. Opracowane rozwiązanie wykorzystuje język Java, w szczególności „platformę programistyczną dla platformy programistycznej" tego języka jaką jest *Spring Boot*, który pozwala na tworzenie spójnego oprogramowania z wykorzystaniem predefiniowanej konfiguracji wraz z kontrolerem aplikacji. Rozdział 5 przedstawia również w syntetyczny sposób wynik działania systemu *Mixeway* w środowisku systemu informatycznego operatora telekomunikacyjnego, który udostępnił dane do przeprowadzenia badań eksperymentalnych. Wyniki zawarte w omawianym rozdziale dotyczą takich wskaźników jak liczba wykonanych skanowań oraz czas dostarczania wyników z przeprowadzonych skanowań.

Rozdział 6 opisuje etapy wykonanych badań eksperymentalnych, które pozwoliły na zastosowanie metod uczenia maszynowego w proponowanym przez Doktoranta systemie *Mixeway*. W szczególności mgr inż. Grzegorz Siewruk przedstawił zbiór uczący, który był wykorzystywany do budowy modeli klasyfikacyjnych wraz z ustaleniem hiperparametrów metod uczenia nadzorowanego wykorzystanych w badaniach eksperymentalnych. W punkcie 6.3 Doktorant przestawił proces inżynierii cech, który był niezbędny w etapie przetwarzania wstępnego danych typu tekstowego.

Wyniki badań eksperymentalnych, uwzględniające różne miary jakości klasyfikacji zostały przedstawione w Rozdziale 7. Wykorzystane metryki dotyczą problemu binarnej klasyfikacji, który w recenzowanej rozprawie miał na celu przypisanie jednej z etykiet klas: błąd wymagający poprawy lub błąd nieistotny. Rozdział 7 zawiera również syntetyczny opis wraz z dyskusją wyników wdrożenia systemu *Mixeway* w strukturze systemów informatycznych operatora telekomunikacyjnego.

Recenzowaną dysertację kończy rozdział 8, który jest podsumowaniem wyników pracy badawczej mgra inż. Grzegorza Siewruka. Niniejszy rozdział zawiera również propozycję dalszych prac badawczych.

Spis literatury liczy 132 pozycje. Cytowane prace dobrane są prawidłowo i odnoszą się do omawianych w pracy problemów.

Praca napisana jest bardzo starannie pod względem edycyjnym, a błędów redakcyjnych lub językowych jest niewiele. Często występujący błąd redakcyjny to tzw. „wiszący znak" (występujący np. na stronie 92 sześciokrotnie). Inne błędy to „ ... kart płatniczych. [117]." na stronie 70, czy też „..., które pozwalają zapewnienie ..." na stronie 75.

Wkład Autora — oryginalne osiągnięcia

Wkład Autora w rozwój dyscypliny Informatyka Techniczna i Telekomunikacja dotyczy: opracowania systemu o nazwie *Mixaway*, którego celem jest automatyzacja (orkiestracja) procesów bezpieczeństwa w łańcuchu dostarczania oprogramowania wraz z badaniami eksperymentalnymi dotyczącymi wykorzystania metod uczenia nadzorowanego do klasyfikacji błędów oprogramowania. Wkład utylitarny związany jest natomiast z zastosowaniem wyników badań Doktoranta w infrastrukturze informatycznej operatora telekomunikacyjnego.

Oryginalne osiągnięcia mgra inż. Grzegorza Siewruka przedstawione w dysertacji to:

1. Opracowanie systemu *Mixaway*, który składa się z trzech modułów (wykrywania zasobów, zarządzania skanami bezpieczeństwa oraz korelacji wyników). Proponowany system stanowi warstwę pośredniczącą między skanerami podatności a procesami wykonywanymi w działach rozwoju oprogramowania oraz operacji. System Mixaway pozwala na dodanie mechanizmów bezpieczeństwa do łańcucha dostarczania oprogramowania działającego w koncepcji ciągłej integracji i wdrażania. Jednocześnie automatyzuje procesy zachodzące pomiędzy wymienionymi wcześniej warstwami.
2. Wykonanie bardzo szerokiego zestawu eksperymentów komputerowych mających na celu weryfikację postawionej hipotezy badawczej. W szczególności Autor analizował wykorzystanie trzech różnych metod uczenia nadzorowanego (las losowy, sieć neuronowa, maszyna wektorów nośnych) jako klasyfikatorów identyfikujących typ błędu oprogramowania.
3. Wdrożenie z sukcesem, potwierdzonym dwoma nagrodami branżowymi, zaproponowanego systemu *Mixaway* w sferze gospodarczej jaką jest infrastruktura informatyczna operatora telekomunikacyjnego.

4. Udostepnienie opracowanego systemu *Mixaway* w serwisie GitHub na zasadzie licencji GPL-3.0. Liczba udokumentowanych pobrań oraz zarejestrowanych użytkowników świadczy o zainteresowaniu społeczności IT opracowanym systemem *Mixaway*.

Recenzowana praca ma charakter koncepcyjno-eksperymentalny. Mgr inż. Grzegorz Siewruk zaproponował rozwiązanie problemu zdefiniowanego przez operatora telekomunikacyjnego. Uzyskane przez Autora rezultaty badań eksperymentalnych potwierdzają postawioną na wstępnie pracy tezę badawczą, a opracowany przed Doktoranta system *Mixeway* został z powodzeniem wdrożony infrastrukturze informatycznej operatora telekomunikacyjnego.

Uwagi krytyczne i dyskusje

Metryki jakości klasyfikacji, które są wykorzystane do analizy wyników to precyzja, dokładność, czułość oraz średnia harmoniczna precyzji oraz czułości (F1). W Rozdziale 6 oraz 7 wykorzystywana jest do analizy wyników również funkcja strat. Autor rozprawy nie przedstawił jaka funkcja strat została przyjęta w badaniach eksperymentalnych (np. logistyczna, kwadratowa, zero-jedynkowa), oraz jaki jest związek między funkcją strat a metrykami jakości klasyfikacji, których wartości wyliczane są z macierzy pomyłek. Dobór hiperaprametrów algorytmu las losowy dokonany jest z wykorzystaniem metryki dokładności, natomiast algorytmu typu sieć neuronowa z wykorzystaniem wartości funkcji strat. Czy zatem otrzymane wyniki są porównywalne? Inną wątpliwość budzi stwierdzenie Autora dysertacji znajdujące sią na stronie 73 – „Wpływ zamiany danego parametru na dokładność działania predykcji nie jest przedmiotem niniejszej rozprawy". Jaki był zatem cel doboru hiperparametrów?

W punkcie dotyczącym opisu wykorzystanych danych (6.2) Doktorant wspomina o rozkładzie wartości dwóch etykiet klas. Treść przedstawiona w tym punkcie nie wyjaśnia czy jest to rozkład *a priori* etykiet klas. Dodatkowo na Rys. 6.2 używane są opisy „Potwierdzone" oraz „Nie potwierdzone". Czy te opisy są tożsame z etykietami klas, które dotyczą tzw. podatności istotnej lub nieistotnej?

W przeprowadzonych badaniach eksperymentalnych dokonano podziału pierwotnego zbioru danych na podzbiory wykorzystywane w uczeniu nadzorowanym. Opis dotyczący metody walidacji jest nieprecyzyjny, ponieważ nie wskazuje konkretnej metody. Zawiera jedynie stwierdzenie, że zapewniono różnorodność w podziale na zbiór uczący oraz testowy.

Dodatkowe pytanie, które pojawia się w tym miejscu dotyczy zbioru walidacyjnego. Czy tego typu zbiór był wykorzystany do ustalania hiperaprametrów poszczególnych algorytmów?

Eksperymenty zostały wykonane dwudziestokrotnie, o czym wspomina Autor dysertacji na stronie 79. Krótki komentarz wskazuje, że rozrzut uzyskanych wyników mieści się w granicach 1%. Przedstawienie wartości statystyk opisowych dla wielokrotnie powtórzonych eksperymentów niewątpliwie rozszerzyłoby możliwości interpretacji otrzymanych wyników.

W punkcie przedstawiającym wyniki badań eksperymentalnych (7.1) Autor dysertacji wykorzystuje „zmanipulowany" zbiór danych. Opis dotyczący „manipulacji" jest nieprecyzyjny. Czy badana zmiana dotyczyła nieprawidłowego przypisania etykiet klas w zbiorze uczącym? Znacznie bardziej interesujące byłyby badania uwzględniające różnego rodzaje zmiany w charakterystykach danych, czyli badania wykorzystujące tzw. dryft koncepcji. Zmiana charakterystyki danych uczących może mieć charakter dynamiczny i dotyczyć różnych cech danych a nie polegać tylko na nieprawidłowym określeniu etykiety klasy w zbiorze uczącym.

W punkcie 5.1.3 Autor przy opisie akronimów CVR oraz DNRV używa słowa „metryka". W dalszej części pracy wspomniane akronimy odpowiadają natomiast etykietom klas.

Podsumowanie

Reasumując stwierdzam, iż mgr inż. Grzegorz Siewruk posiada ogólną wiedzę teoretyczną w zakresie metod uczenia maszynowego, cyberbezpieczeństwa oraz projektowania i wdrażania systemów informatycznych, które mieszczą się w dyscyplinie Informatyka Techniczna i Telekomunikacja. Lektura dysertacji pozwala stwierdzić, że Autor zaprezentował na jej łamach umiejętność samodzielnego prowadzenia pracy naukowej, której efekty pozwoliły na opracowanie systemu *Mixeway* wraz z eksperymentalnym sprawdzeniem jego skuteczności. Dodatkowo treść dysertacji jednoznacznie wskazuje na zastosowanie wyników badań naukowych mgra inż. Grzegorz Siewruka w sferze gospodarczej jaką jest infrastruktura informatyczna operatora telekomunikacyjnego.

Wobec powyższego, recenzowana praca spełnia wymagania zdefiniowane przez artykuł 187 Ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2021 r. poz. 478). Konkludując, wnoszę o przyjęcie rozprawy oraz dopuszczenie mgra inż. Grzegorza Siewruka do publicznej obrony.

R. Rudnik

Gdańsk, 15 listopada 2021

Dr hab. inż. Rafał Leszczyna
Politechnika Gdańska
Wydział Zarządzania i Ekonomii
rle@zie.pg.edu.pl

Recenzja rozprawy doktorskiej

mgr inż. Grzegorza Siewruka

pt. „Orkiestracja narzędzi bezpieczeństwa w sieci operatora telekomunikacyjnego z wykorzystaniem technik uczenia maszynowego oraz metod przetwarzania języka naturalnego"

Promotor dr hab. inż. Wojciech Mazurczyk, Politechnika Warszawska

Promotor pomocniczy dr inż. Adrian Marzecki

1. Wprowadzenie

Niniejsza recenzja rozprawy doktorskiej, której Autorem jest mgr inż. Grzegorz Siewruk, została wykonana w oparciu o uchwałę Rady Naukowej Dyscypliny Informatyka Techniczna i Telekomunikacja Politechniki Warszawskiej (Uchwała nr 181/2021) z dnia 14 września 2021 roku podpisaną przez dr hab. inż. Jarosława Arabasa oraz dr hab. inż. Artura Janickiego. Uchwała ta wskazuje mnie jako recenzenta w komisji doktorskiej w postępowaniu w sprawie nadania stopnia doktora mgr. inż. Grzegorzowi Siewrukowi.

Promotorem niniejszej rozprawy jest dr hab. inż. Wojciech Mazurczyk, profesor Politechniki Warszawskiej. Promotorem pomocniczym jest dr inż. Adrian Marzecki.

2. Podejmowane zagadnienia naukowe

Recenzowana rozprawa doktorska dotyczy zastosowań technik uczenia maszynowego oraz metod przetwarzania języka naturalnego w procesie rozwijania bezpiecznego oprogramowania.

Teza rozprawy oraz jej główne cele zostały przedstawione w rozdziale 1.2. Cele pracy, sformułowane poprawnie oraz spójne z tezą pracy, związane są z (i) eksperymentalną

analizą algorytmów uczenia maszynowego pod kątem możliwości ich zastosowania w procesie wytwarzania bezpiecznego oprogramowania; (ii) zaprojektowaniem i implementacją rozwiązania wspomagającego automatyczne zarządzanie (orkiestrację) narzędzi bezpieczeństwa i proces decyzyjny wdrażania oprogramowania; (iii) wdrożeniem tego rozwiązania; (iv) oraz udowodnieniem jego skuteczności.

3. Zawartość rozprawy

Przedstawiona do recenzji praca zawiera streszczenie, streszczenie w języku angielskim, spis treści, wykaz publikacji, prezentacji i nagród związanych z tematyką rozprawy, listę skrótów, spis tabel, spis rysunków, wprowadzenie, osiem numerowanych rozdziałów, spis pozycji literatury oraz trzy załączniki zawierające instrukcję uruchomienia systemu oraz kopie dyplomów związanych z przedstawionym rozwiązaniem.

Całość rozprawy napisana jest w języku polskim, z wyjątkiem wspomnianego streszczenia w języku angielskim.

Układ i zawartość rozdziałów merytorycznych jest zasadniczo poprawna.

W pierwszym rozdziale (Wprowadzenie) Autor zarysowuje tematykę doktoratu oraz ogólnie przedstawia podjętą problematykę badawczą. Opisane są tutaj też cele i teza rozprawy a także układ pracy.

Rozdziały 2-4 przedstawiają kontekst prowadzonych przez Autora badań, począwszy od obszarów cyberbezpieczeństwa w których wykorzystywane są algorytmy uczenia maszynowego (rozdział 2). W rozdziale trzecim przedstawiono podstawowe modele wytwarzania oprogramowania i problematyce cyberbezpieczeństwa w procesie dostarczania oprogramowania. Natomiast rozdział 4 dedykowany jest wybranym algorytmom uczenia maszynowego oraz technikom przetwarzania języka naturalnego. Poziom szczegółowości opisów nie jest jednorodny. Może zastanawiać dlaczego niektórym zagadnieniom Autor poświęca więcej uwagi, innym mniej a także motywacje stojące za decyzjami dotyczącymi kategorii istniejących rozwiązań. Piszę o tym szerzej w części zatytułowanej „Uwagi dyskusyjne" niniejszej recenzji.

Opis zaproponowanego przez Autora rozwiązania Mixaway oraz związanych z nim badań i eksperymentów rozpoczyna się w rozdziale 5. To tutaj Autor opisuje architekturę Mixaway oraz główne etapy wdrożenia rozwiązania. W rozdziale 6, zatytułowanym „Metodyka badawcza", Autor przedstawia badania eksperymentalne służące do wybrania algorytmu maszynowego do implementacji w rozwiązaniu. Wyniki eksperymentów przedstawiono w rozdziale 7, zatytułowanym „Wyniki badań eksperymentalnych". W tym samym rozdziale znajduje się opis rezultatów uzyskanych dzięki wdrożeniu w rozwiązania.

Bibliografia zawiera 132 pozycje. Są to w przeważającej części artykuły i dokumenty opublikowane w ciągu ostatnich kilku lat. Obok nich znajdują się podstawowe, starsze publikacje z obszarów poruszanych przez Autora. Analiza literatury jest dość szeroka i Autor przedstawia w niej trafne wnioski, co generalnie świadczy o dobrym rozpoznaniu wiedzy w dziedzinie. Pozostałem komentarze dotyczące analizy literatury przedstawiłem w rozdziale „Uwagi dyskusyjne" niniejszej recenzji.

4. Stopień realizacji celów rozprawy

Wszystkie cele rozprawy zostały osiągnięte.

Autor zaproponował system Mixaway wspomagający zarządzanie automatycznymi testami bezpieczeństwa w (wysoce) rozproszonym środowisku wytwarzania oprogramowania, integrującym m.in. zasoby udostępniane w chmurach zewnętrznych. Przeprowadzone badania eksperymentalne pozwoliły Autorowi opracować moduł korelujący wyniki z pomocą technik uczenia maszynowego oraz metod przetwarzania języka naturalnego. Zaprojektowane i zrealizowane rozwiązanie zostało wdrożone w infrastrukturze Orange Polska a o powodzeniu wdrożenia mogą świadczyć uzyskane nagrody przedsiębiorstwa tj. Nagroda szefa funkcji Sieć i Technologie 2019 oraz Security & Privacy Awards 2021. Ponadto system został udostępniony na zasadach licencji otwartego oprogramowania na platformie GitHub skąd pobrano go oraz zainstalowano już ponad 16 000 razy. **Fakty te oceniam bardzo pozytywnie.**

Skuteczność systemu została zweryfikowana eksperymentalnie (analiza modeli uczenia maszynowego w oparciu o zbiór danych pochodzących z infrastruktury rzeczywistego operatora telekomunikacyjnego). oraz na podstawie obserwacji efektów pracy wdrożonego środowiska.

Realizacja celów pracy pozwoliła dowieść jej tezę.

5. Przydatność zaproponowanego rozwiązania w sferze gospodarczej

Zaproponowany przez Autora system Mixaway został wdrożony w sieci operatora telekomunikacyjnego Orange Polska i włączony do procesu dostarczania oprogramowania stu trzydziestu aplikacji. Wpłynęło to na poprawę jakości i skuteczności procesów wytwarzania oprogramowania firmy o czym świadczą wielomiesięczne obserwacje wspieranych przez Mixaway projektów prowadzonych w przedsiębiorstwie. Takie efekty znalazły uznanie w prestiżowych nagrodach przyznanych na poziomie międzynarodowym Grupy Orange oraz przez Orange Polska. Powyższe fakty jednoznacznie potwierdzają wysoką przydatność i praktyczne zastosowanie zaproponowanego rozwiązania w sferze gospodarczej.

Ponadto system jest dostępny na zasadach licencji otwartego oprogramowania na platformie GitHub. Dzięki temu mogą z niego skorzystać także inne przedsiębiorstwa oraz użytkownicy indywidualni. W serwisie GitHub dostępna jest informacja o ponad szesnastu tysięcy pobrań i instalacji oprogramowania Mixeway.

6. Oryginalność rozwiązania

Recenzowana rozprawa doktorska opisuje oryginalne rozwiązanie w zakresie zastosowania wyników własnych badań naukowych w sferze gospodarczej. W porównaniu z innymi rozwiązaniami opisywanymi w literaturze, system Mixaway, zaproponowany przez Autora, wykorzystuje potencjalne i niepotwierdzone podatności bezpieczeństwa, które zostały zebrane przy pomocy automatycznych skanerów. Ponadto, system posiada możliwość zdalnej kontroli uruchamianych testów podatności co umożliwia automatyzację całego procesu. Ciekawą stroną naukową jest też

wprowadzenie technik uczenia maszynowego do wspomagania decyzji w procesie wytwarzania bezpiecznego oprogramowania.

7. Uwagi dyskusyjne

Autor osiągnął postawione cele rozprawy, udowodnił sformułowaną tezę oraz przeprowadził poprawną ewaluację eksperymentalną. Dołożył też wszelkiej staranności, aby zapewnić poprawność pracy pod względem merytorycznym i redakcyjnym. Poniżej przedstawiam aspekty dyskusyjne, które napotkałem podczas analizy rozprawy.

- Na początku rozdziału 2.1 Autor pisze: „Aplikacje wykorzystujące algorytmy ML w domenie bezpieczeństwa sieciowego mogą być sklasyfikowane do następujących kategorii (na podstawie podziału zaproponowanego w [17]): systemy wykrywania anomalii/włamań oraz ochrona urządzeń końcowych". – Taki podział, na dwie kategorie jest dyskusyjny. Na przykład, jak zgodnie z tą klasyfikacją rozpatrywać fakt, że systemy wykrywania włamań bazujące na detekcji anomalii wykorzystywane są również w ochronie urządzeń końcowych? Poprawności przedstawionej kategoryzacji algorytmów uczenia maszynowego nie wzmacnia fakt, że została ona przedstawiona w artykule ([17]) opublikowanym w serwisie internetowym nie wymagającym recenzji. Jednocześnie należy podkreślić, że główny obszar badań, w którym usytuowana jest praca, czyli orkiestracji narzędzi bezpieczeństwa, został przybliżony w oparciu o rzetelne i wiarygodne źródła wiedzy naukowej ([31]).

- Druga uwaga dotyczy kwestii wyboru przez Autora dwóch spośród pięciu kategorii przedstawionych w artykule [17] bez podania uzasadnienia tego wyboru.

- Zastanawia również dlaczego w części poświęconej rozwiązaniom komercyjnym przedstawiono wyłącznie jedno takie rozwiązanie.

- Z pewnością wartość części pracy związanej z analizą literatury podwyższyłoby przeprowadzenie tego procesu w sposób systematyczny, z wykorzystaniem ugruntowanej metody. W ten sposób zapewnia się gwarancje wysokiej kompletności i uporządkowania. Przykładem systematycznych analiz mogą być te przedstawione w artykułach oznaczonych identyfikatorami DOI: 10.1016/j.compeleceng.2017.11.027 i 10.1016/j.infsof.2013.07.010.

- Nie jest jasne dlaczego rozdział 6 poświęcony opisowi procesu został opatrzony tytułem „Metodyka badawcza", chociaż w treści opisano eksperymenty wykonane przez Autora. W tym środowisko eksperymentalne, wykorzystywane zbiory danych, algorytmy i czynności.

- Również tytuł rozdziału siódmego nie w pełni trafnie oddaje jego treść. Przedstawiono tutaj nie tylko wyniki eksperymentów, ale również praktyczne rezultaty pochodzące z wdrożenia.

- W rozdziale 7.2 nie jest do końca jasne dlaczego Autor najpierw skazuje wartość spadku odrzuceń wdrożenia równą 5% a dalej odwołuje się do wartości 9% omawiając czynniki jakie przyczyniły się do zmniejszenia liczby odrzuceń.

- Także wyjaśnienie w ostatnim akapicie wprowadzenia do rozdziału 7 mające uzasadnić pominięcie dyskusji metryk takich jak odsetek wyników fałszywie negatywnych czy odsetek wyników fałszywie pozytywnych wymagałoby rozszerzenia. W moim odczuciu przedstawienie i omówienie tych metryk stanowiłoby cenną informację w pracy.

Należy zaznaczyć, że wymienione powyżej (w większości drobne) uwagi nie pomniejszają wartości naukowej oraz przydatności i oryginalności rozprawy.

8. Podsumowanie

Przedstawiona do recenzji rozprawa doktorska spełnia ustawowe wymagania stawiane rozprawom doktorskim.

Na tej podstawie wnioskuję o jej dopuszczenie do publicznej obrony w postępowaniu w sprawie nadania stopnia doktora.

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 implementację rozwiązania, które orkiestruje pracę 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) **wybitnie dobra, zasługująca na wyróżnienie.**

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.

podpis