POLITECHNIKA
GDAŃSKA
WYDZIAŁ ELEKTRONIKI,
TELEKOMUNIKACJI I INFORMATYKI

Gdańsk, 14.12.2022 r.

Dr hab. inż. Jacek Rak, prof. PG
Wydział Elektroniki, Telekomunikacji i Informatyki
Politechnika Gdańska

Recenzja rozprawy doktorskiej

Tytuł: Rozproszone metody ukrywania informacji w sieciach

Autor: Mgr inż. Jędrzej Tadeusz Bieniasz

Rozprawa doktorska mgra inż. Jędrzeja Bieniasza analizuje problemy oraz przedstawia wyniki badań własnych związanych z rozproszonymi formami ukrywania informacji w sieciach teleinformatycznych. Problem jest niewątpliwie ważny i aktualny, gdyż analizowana przez Doktoranta steganografia sieciowa i rozproszona stanowi rzeczywiście obszar intensywnych badań naukowych w ostatnim okresie. Doktorant we wstępie pracy słusznie podkreśla, że steganograficzne metody ukrywania informacji mogą zostać wykorzystane zarówno w działaniach defensywnych, jak i ofensywnych, toteż zrozumienie ich charakterystyk (w kontekście możliwości wystąpienia potencjalnych ataków) stanowi z pewnością ważny etap poprzedzający konstrukcję rozwiązań z zakresu przeciwdziałania atakom – w szczególności wykorzystujących steganografię jako instrument działań ofensywnych. Efektywność metod obrony zależy w dużej mierze od dopasowania ich charakterystyk do sposobu działań atakujących.

Oceniana rozprawa doktorska składa się z sześciu rozdziałów napisanych w języku polskim, stanowiących wprowadzenie do zawartości załącznika A obejmującego siedem artykułów [A1]-[A7] napisanych w języku angielskim (jako że rozprawa została przygotowana w oparciu o cykl publikacji powiązanych tematycznie). Występujący w rozprawie drugi załącznik (B) zawiera oświadczenia współautorów powyższych siedmiu prac cyklu dotyczące procentowych wkładów autorów w powstanie tychże prac. Analizując zawartość załącznika B rozprawy, stwierdzam, że

JRak

udział Doktoranta na poziomie 60-75% jest znaczący i świadczy o wiodącym zaangażowaniu Doktoranta w powstanie tych prac.

1. Jaki jest problem naukowy rozprawy i czy został on trafnie i jasno sformułowany?

Celem pracy było opracowanie metod zwiększania poziomu cyberbezpieczeństwa (oraz ocena skuteczności tychże metod) w dwóch obszarach:

- detekcji cyberzagrożeń wykorzystujących rozproszone metody ukrywania informacji wraz z reagowaniem na nie,
- projektowania i wdrożenia mechanizmów ochrony wykorzystujących rozproszone metody ukrywania informacji.

Cel rozprawy został w pracy jasno zdefiniowany. Jest on niewątpliwie także trafny z uwagi na obserwowaną tendencję wzrostową w odniesieniu do liczby, skali, jak i różnorodności form ataków. Jak ukazuje zawartość rozprawy, cel ten został osiągnięty wielotorowo m.in. poprzez działania z zakresu:

- projektu i realizacji środowiska symulacyjnego z zakresu rozproszonych metod steganografii,
- konstrukcji prototypu systemu wieloagentowego służącego do wykrywania zagrożeń wykorzystujących technki steganograficzne,
- wykorzystania metod z obszaru inżynierii danych do wykrywania steganografii wraz z zaproponowaniem techniki przetwarzania danych w tym kontekście,
- projektu rozproszonej metody steganograficznej oraz weryfikacji jej cech charakterystycznych,
- pozyskania i klasyfikacji wiedzy dotyczącej cyberzagrożeń wykorzystujących rozproszone metody steganografii,
- analizy możliwości wykorzystania metod steganografii rozproszonej w kontekście ich zastosowania w aspekcie defensywnym.

Pomimo, że teza badawcza nie została w rozprawie zdefiniowana, jasno wyrażony cel rozprawy oraz zaprezentowane w rozprawie wyniki moim zdaniem rekompensują brak tejże tezy i dowodzą możliwości poprawy poziomu cyberbezpieczeństwa poprzez wykorzystanie rozwiązań proponowanych przez Doktoranta w rozprawie bazujących na steganografii.

2. Na czym polega oryginalny dorobek Autora i jakie jest znaczenie poznawcze lub przydatność praktyczna dla nauki bądź techniki?

Do oryginalnego dorobku ukazanego w ocenianej rozprawie należy moim zdaniem zaliczyć:

1) wyniki badań Doktoranta opisane w rozdziale 2 dotyczących realizacji metody steganograficznej dedykowanej otwartym sieciom społecznościowym szczegółowo opublikowane w pracach [A1] i [A2], a w szczególności:

   a. opracowanie koncepcji steganograficznego systemu plików SocialStegDisc wraz implementacją proof-of-concept,

   b. dokonanie analizy niezawodności i niewykrywalności systemu,

   c. dokonania analizy wpływu zastosowania tejże koncepcji w cyberprzestrzeni,

2) wyniki badań Doktoranta opisane w rozdziale 3 z obszaru wykrywania skutków działań rozproszonych metod ukrywania informacji zaprezentowane w pracach [A3]-[A5] obejmujące w szczególności:

   a. analizę stanu wiedzy z zakresu stosowania metod steganografii do ukrywania informacji w sieciach; zestawienie istniejących metod detekcji i przeciwdziałania kanałom Command&Control opisane w pracy [A3],

   b. propozycje metod detekcji anomalii w procesie śledzenia ścieżki realizacji ataku, w tym wykorzystujące metody uczenia maszynowego operujące na danych zebranych podczas realizacji scenariuszy symulacyjnych (ukazane w pracy [A4]),

   c. rozszerzenie koncepcji z pracy [A4] o mechanizm celowego opóźniania i tracenia pakietów opisany w pracy [A5],

3) rezultaty badań Doktoranta z zakresu defensywnych zastosowań steganografii rozproszonej (cyber deception) opublikowane w pracach [A6], [A7] dotyczące:

   a. opracowania mechanizmów steganograficznych opisanych w pracy [A6] dedykowanych koncepcji *cyberfog*, w tym w szczególności mechanizmu indeksacji realizującego ideę metody StegHash, mechanizmu dyspersji w oparciu o metodę SocialStegDisc,

   b. zaprojektowania architektury systemu w ujęciu warstwowym wraz z analizą teoretyczną szeregu aspektów z obszaru bezpieczeństwa, niezawodności oraz ogólnie rozumianej wydajności (także praca [A6]),

   c. opracowania systemu StegFog opisanego w pracy [A7], stanowiącego rozszerzenie koncepcji z artykułu [A6] m.in. w zakresie mechanizmów i protokołów realizujących zapis/odczyt danych ukrytych, ukryte powiadamianie o dostępności danych czy też ukryty routing do kolejnych fragmentów danych.

Ponadto, należy także pozytywnie ocenić przejrzystą strukturę rozprawy obejmującą rozdział 1 (wstęp ukazujący cel i zakres rozprawy), rozdział 2 podsumowujący wyniki badań Doktoranta w

obszarze realizacji rozproszonych metod ukrywania informacji, rozdział 3 podsumowujący uzyskane wyniki badań z zakresu wykrywania form ukrywania informacji, jak i rozdział 4 ukazujący wyniki badań Doktoranta w obszarze defensywnych zastosowań metod steganograficznych.

Powyższe osiągnięcia udokumentowane również poprzez dogłębną ewaluację charakterystyk w drodze analizy teoretycznej i symulacyjnej dowodzą łącznej realizacji celu rozprawy.

3. Czy Autor rozwiązał postawiony problem i czy użył do tego celu właściwych metod?

Analizując zawartość rozdziałów rozprawy doktorskiej mgra inż. Jędrzeja Bieniasza, w szczególności osiągnięć zaprezentowanych w rozdziałach 2-4 ukazujących wyniki opublikowane w pracach [A1]-[A7], uważam że Doktorant rozwiązał we właściwy sposób problem zdefiniowany w rozprawie dotyczący metodologii detekcji oraz ochrony przed atakami wykorzystującymi techniki steganograficzne.

W mojej ocenie, metodologia zastosowana przez Doktoranta w kolejnych etapach badań jest poprawna, odpowiada technikom stosowanym w badaniach naukowym, a stopień jej złożoności jest adekwatny do oczekiwań stawianym pracom na poziomie doktorskim.

Warto w tym miejscu podkreślić, że osiągnięcia badawcze Doktoranta opublikowane w:

- czterech artykułach w czasopismach z listy JCR (w tym w jednym artykule z roku 2022 w IEEE Access – 100 pkt, jednym artykule w czasopiśmie Electronics z roku 2021 – 100 pkt oraz dwóch artykułach w czasopiśmie Journal of Universal Computer Science z 2019 roku za 40 pkt każdy),
- jednym rozdziale monografii wydawnictwa CRC Press z roku 2019,
- sześciu artykułach w materiałach konferencji międzynarodowych w latach 2017-2020

oraz bardzo dobre (w odniesieniu do postępowań doktorskich) wartości parametrów bibliometrycznych (w tym indeksu Hirscha H=3, liczby cytowań wynoszącej 37 oraz łącznej liczby punktów MEiN związanych z siedemnastoma publikacjami Doktoranta wynoszącej 459 pkt.) łącznie dowodzą zdolności Doktoranta rozwiązywania problemów badawczych o istotnym znaczeniu na arenie międzynarodowej.

4. Jakie są słabsze strony rozprawy?

Analiza słabszych aspektów rozpraw przygotowanych w oparciu o cykl publikacji ma niewątpliwie odmienny charakter w porównaniu z rozprawami klasycznymi (tj. prac, których główną częścią nie są artykuły naukowe). Każdy z artykułów cyklu tworzący taką rozprawę, stanowi bowiem pewną zamkniętą całość poddaną uprzedniej recenzji przed ukazaniem się w czasopiśmie / materiałach konferencyjnych. W przypadku takich prac, potencjalne ograniczenia

merytoryczne mogą wynikać np. z odgórnych limitów liczby stron prac narzuconych przez wydawnictwo / organizatorów konferencji. Jedyną częścią rozprawy przygotowaną przez kandydatów podczas tworzenia rozprawy jest w takim przypadku ogólne wprowadzenie.

Oceniając rozprawę doktorską mgra inż. Jędrzeja Bieniasza nie zauważyłem istotnych uchybień zarówno w zakresie merytorycznym, jak i struktury siedmiu prac cyklu [A1]-[A7]. Forma przedstawiania osiągnięć w tych pracach jest co prawda zróżnicowana, lecz wynika ona z odmiennych standardów wydawniczych (szablonów).

Jako że prace [A1]-[A7] dotyczą wąskiego obszaru steganografii, wstępy tychże prac są dosyć podobne, co jest jednakże typowe w przypadku rozpraw składających się z cyklu prac. Jeśli traktować to jako wadę, to nie w odniesieniu do tejże konkretnej rozprawy doktorskiej, lecz ogólnie odnosząc tę uwagę ogólnie do systemowej koncepcji tworzenia prac w oparciu o zbiór publikacji. W takim przypadku umiejętności doktorantów w zakresie tworzenia rozpraw doktorskich można ocenić w zasadzie jedynie po jakości części wprowadzenia rozprawy.

W przypadku ocenianej rozprawy mgra Bieniasza wprowadzenie to składa się z sześciu rozdziałów o objętości łącznej ok. 50 stron. Moja ocena tejże części jest wysoka. Uważam, że została przygotowana bardzo dobrze pod względem struktury i zawartości merytorycznej. Zauważalne są sporadycznie drobne niedociągnięcia stylistyczne czy literówki, np.:

- na stronie 9: „metod podnoszenia cyberbezpieczeństwa" → „metod podnoszenia poziomu cyberbezpieczeństwa"
- na stronie 11: „IF: 1.056ui" → „IF: 1.056"

Warto byłoby poszerzyć badania o analizę dotyczącą stopnia niezawodności systemu sieciowego w obliczu ataków wykorzystujących steganografię, jak i analizę wpływu metod Doktoranta na niezawodność. Bezpieczeństwo i niezawodność są bowiem aspektami mającymi szereg powiązanych atrybutów jak choćby dostępność (ang. availability).

Powyższe uwagi w mojej ocenie nie rzutują na moją jednoznacznie pozytywną ocenę łączną rozprawy doktorskiej mgra inż. Jędrzeja Bieniasza.

5. Do której z następujących kategorii Recenzent zalicza rozprawę:

a/ nie spełniająca wymagań,
b/ wymagająca wprowadzenia poprawek i ponownego recenzowania,
c/ zadowalająco spełniająca wymagania,
d/ wykraczająca ponad poziom zadawalający (spełniająca wymagania z nadmiarem),
e/ wybitna?

Podsumowując, moja recenzja pracy doktorskiej mgra inż. Jędrzeja Bieniasza jest **pozytywna**. Zarówno wartość merytoryczna rozprawy jak i ranga wyników opublikowanych w siedmiu głównych pracach rozprawy (oznaczonych jako pozycje [A1]-[A7]) kwalifikują w mojej ocenie rozprawę mgra inż. Jędrzeja Bieniasza do kategorii **d/ wykraczająca ponad poziom zadawalający (spełniająca wymagania z nadmiarem)**.

Z uwagi na spełnione przez Doktoranta ustawowe wymagania, **wnoszę o dopuszczenie rozprawy doktorskiej mgra inż. Jędrzeja Bieniasza do publicznej obrony**. Ponadto, z uwagi na szereg znaczących publikacji Doktoranta, z których składa się oceniana rozprawa (w tym czterech prac z listy JCR o wiodącym udziale Doktoranta), wskazanych w sekcji 3 niniejszej recenzji, jak wobec szeregu nagród i wyróżnień, które Doktorant uzyskał w związku ze swoją pracą badawczą, opisanych na stronach 43-44 rozprawy, **wnoszę o wyróżnienie rozprawy**.

Jacek Rak