Wrocław, 8 grudnia 2022

Prof. dr hab. inż. Krzysztof Walkowiak
Wydział Informatyki i Telekomunikacji
Politechnika Wrocławska

RECENZJA ROZPRAWY DOKTORSKIEJ
DLA RADY DYSCYPLINY INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA
POLITECHNIKI WARSZAWSKIEJ

Autor rozprawy doktorskiej: mgr inż. Jędrzej Bieniasz
Tytuł rozprawy doktorskiej: *„Rozproszone metody ukrywania informacji w sieciach”*
Promotor: dr hab. inż. Krzysztof Szczypiorski, prof. uczelni

1. Zakres i charakter rozprawy

Recenzowana rozprawa doktorska mgr inż. Jędrzeja Bieniasza dotyczy zagadnień związanych z bezpieczeństwem sieci teleinformatycznych, w szczególności rozprawa koncentruje się na problematyce cyberbezpieczeństwa i steganografii. Cyberbezpieczeństwo jest bardzo aktualnym i ważnym obszarem badawczym. Wynika to głównie z nieustannie rosnącej popularności różnych systemów informatycznych stosowanych w praktycznie każdym aspekcie ludzkiej aktywności i gospodarki. Dodatkowo w ostatnich latach obserwowany jest duży wzrost liczby różnorakich zagrożeń i ataków na systemy informatyczne mających związek z działaniami przestępczymi, także w sferze konfliktów międzynarodowych. Steganografia, w szczególności steganografia sieciowa i rozproszona w ciągu ostatnich dwóch dekad jest przedmiotem badań naukowych w obszarze cyberbezpieczeństwa. Głównym kierunkiem badań jest analiza możliwości zastosowania tych metod w różnych atakach na cyberbezpieczeństwo. Ponadto, raporty opisujące incydenty bezpieczeństwa komputerowego potwierdzają rosnącą skalę wykorzystania steganografii przez atakujących systemy informatyczne.

Recenzowana rozprawa doktorska jest przedstawiona jako cykl następujących siedmiu artykułów naukowych:

- Bieniasz, J., & Szczypiorski, K. (2017). SocialStegDisc: Application of steganography in social networks to create a file system. 2017 3rd International Conference on Frontiers of Signal Processing (ICFSP), 2017, pp. 76-80.
- Bieniasz, J., & Szczypiorski, K. (2019). Methods for Information Hiding in Open Social Networks. Journal of Universal Computer Science, 25(2), 74-97.

- Bieniasz, J., & Szczypiorski, K. (2019). Steganography Techniques for Command and Control (C2) Channels. In Botnets. Architectures, Countermeasures, and Challenges. (pp. 189-216). CRC Press.
- Bieniasz, J., Stępkowska, M., Janicki, A., & Szczypiorski, K. (2019). Mobile Agents for Detecting Network Attacks Using Timing Covert Channels. Journal of Universal Computer Science, 25(9), 1109-1130.
- Bieniasz, J., & Szczypiorski, K. (2021). Dataset Generation for Development of Multi-Node Cyber Threat Detection Systems. Electronics. 2021; 10(21).
- Bieniasz, J., & Szczypiorski, K. (2018). Towards Empowering Cyber Attack Resiliency Using Steganography. 2018 4th International Conference on Frontiers of Signal Processing (ICFSP), 2018, pp. 24-28.
- Bieniasz, J., Bąk, P., & Szczypiorski, K. (2022). StegFog: Distributed Steganography Applied To Cyber Resiliency In Multi Node Environments. IEEE Access, 2022.

Należy podkreślić, że wybrana tematyka rozprawy jest aktualnym obszarem badań poszerzającym dotychczas realizowane prace badawcze w zakresie cyberbezpieczeństwa i steganografii. Warto również zauważyć, że publikacje wchodzące w skład rozprawy zostały opublikowane w renomowanych czasopismach naukowych i w materiałach dobrych konferencji naukowych oraz uzyskały oddźwięk w środowisku naukowym potwierdzony cytowaniami.

2. Zawartość rozprawy

Rozprawa składa się z 6 rozdziałów oraz dwóch aneksów. Pierwszy rozdział to wprowadzenie przedstawiające motywację tematu rozprawy, cel rozprawy oraz opis podstawowych zagadnień związanych z tematyką rozprawy doktorskiej. Rozdziały 2-4 opisują badania nad: realizacją rozproszonych metod ukrywania informacji w sieciach, wykrywaniem rozproszonych metod ukrywania informacji w sieciach oraz defensywnymi zastosowaniami rozproszonych metod ukrywania informacji w sieciach przedstawionymi w artykułach naukowych wchodzących w skład rozprawy. W rozdziale 5 Doktorant przedstawił podsumowanie zrealizowanych badań. Rozdział 6 zawiera opis dorobku naukowego Doktoranta. Aneks A zawiera treść siedmiu artykułów naukowych wchodzących w skład rozprawy doktorskiej. Aneks B zawiera oświadczenia współautorów tych artykułów.

W mojej ocenie struktura rozprawy doktorskiej jest prawidłowa. Doktorant w logiczny i przejrzysty sposób przedstawił kolejne zagadnienia, co ułatwia lekturę i analizę zawartości rozprawy. Ponadto, pragnę podkreślić bardzo wysoką jakość rozprawy pod kątem językowym, stylistycznym i edycyjnym.

3. Poprawność i oryginalność postawionej tezy

Rozprawa nie zawiera precyzyjnego zdefiniowania tezy badawczej (ang. *research question*). Określony jest jedynie główny cel pracy sformułowany w następujący sposób:

"*Celem niniejszej rozprawy doktorskiej jest opracowanie i ocena skuteczności metod podnoszenia cyberbezpieczeństwa w kontekście dwóch obszarów zastosowania rozproszonych metod ukrywania informacji w sieciach:*
1. inteligentnego wykrywania i reagowania na cyberzagrożenia wykorzystujące rozproszone metody ukrywania informacji,
2. mechanizmów ochrony sieci opartych na rozproszonych metodach ukrywania informacji."

W mojej opinii cel rozprawy jest sformułowany w poprawny sposób. Mgr inż. Jędrzej Bieniasz na podstawie przeglądu literaturowego i własnej wiedzy prawidłowo określił zakres rozprawy doktorskiej, koncentrując się na aktualnych i ważnych zagadnieniach związanych z cyberbezpieczeństwem i steganografią.

Cel rozprawy został osiągnięty w rozprawie doktorskiej poprzez:

- Opracowanie, zaimplementowanie i ocenę rozszerzenia koncepcji steganograficznego systemu plików SocialStegDisc opartego o metodę StegHash, w tym w zakresie możliwości zastosowania metod StegHash i SocialStegDisc w rozwiązaniach bezpieczeństwa sieci zgodnych z koncepcją cyberfog.
- Opracowanie nowego sposobu modelowania komunikacji steganograficznej złośliwego oprogramowania za pomocą kanałów Command & Control.
- Opracowanie, zaimplementowanie i ocenę nowego rozwiązania dotyczącego detekcji metod ukrywania informacji przy zastosowaniu koncepcji systemów wieloagentowych, w tym w zakresie zdolności do wykrywania węzłów sieciowych stanowiących źródło ataków.
- Opracowanie i zaimplementowanie nowego systemu komunikacyjnego opartego o rozproszoną steganografię opartą na wcześniejszych metodach analizowanych przez Doktoranta – StegHash i SocialStegDisc oraz dopasowanie systemu do podejścia cyberfog.

Według mojej opinii mgr inż. Jędrzej Bieniasz w prawidłowy sposób określił cel badań oraz metody realizacji postawionego celu.

4. Analiza źródeł (w tym literatury światowej i stanu techniki) świadcząca o dostatecznej wiedzy autora w danej dyscyplinie naukowej

Rozprawa doktorska mgr inż. Jędrzeja Bieniasza dotyczy bieżących zagadnień związanych z cyberbezpieczeństwem. Doktorant przeprowadził dokładny przegląd literaturowy. Lista pozycji bibliograficznych umieszczona w pierwszej części rozprawy zawiera 57 publikacji naukowych. Ponadto, każda z siedmiu publikacji wchodzących w skład cyklu zawiera swój własny przegląd literatury dotyczącej tematyki danego artykułu. Wśród omówionych prac naukowych znajdują się najważniejsze prace związane z tematyką poruszaną w rozprawie, w szczególności z: cyberbezpieczeństwem, steganografią, zagrożeniami w zakresie cyberbezpieczeństwa, analityką danych, metodami uczenia maszynowego. Przedstawiony przegląd literaturowy stanowi dobre wprowadzenie do dalej przedstawionych oryginalnych koncepcji Doktoranta. Moim zdaniem,

Doktorant posiada odpowiednią wiedzę i znajomość współczesnej literatury z zakresu związanego z tematyka rozprawy.

5. Pozycja rozprawy w stosunku do stanu wiedzy i stanu techniki reprezentowanych przez literaturę światową

Tematyka rozprawy doktorskiej jest związana z aktualnie rozwijanymi kierunkami badań w zakresie cyberbezpieczeństwa. Zagadnienia dotyczące podniesienia bezpieczeństwa działania sieci teleinformatycznych, w tym w zakresie rozproszonych metod ukrywania informacji w sieciach są bardzo ważnym tematem badawczym. Wynika to z jednej strony z nieustannego wzrostu liczby różnego rodzaju cyberzagrożeń, a z drugiej strony z rosnącej popularności stosowania metod ukrywania informacji.

Rozważane w rozprawie cyberzagrożenia w obszarze steganografii i przeciwdziałanie tym zagrożeniom stanowi wyzwanie dla bardzo wielu instytucji i przedsiębiorstw. Doktorant w prawidłowy sposób określił zakres tematyczny rozprawy i następnie zaproponował właściwe metody rozwiązania postawionych problemów stosując koncepcje zgodne z aktualnym stanem wiedzy i techniki reprezentowanym w światowej literaturze. Na szczególne podkreślenie zasługuje zastosowanie metod uczenia maszynowego oraz uwzględnienie w realizowanych badaniach najnowszych trendów w zakresie cyberbezpieczeństwa, w tym *intelligence-driven cyber defense*, *intelligence-driven incident response*, *data-driven network intrusion detection*, *cybersecurity data science*, *big data analytics for information security*.

Należy zaakcentować, że wyniki przedstawione w rozprawie zostały zrealizowane w ramach projektów badawczo-rozwojowych dofinansowanych w programie CyberSecIdent Narodowego Centrum Badań i Rozwoju (NCBiR):

- Projekt „*Zaawansowane Laboratorium Kryminalistyki Śledczej*”, 2017–2019. Numer projektu CYBERSECIDENT/369234/I/NCBR/2017.
- Projekt „*Platforma detekcji anomalii sieciowych (PDAS)*”, 2017–2019. Numer projektu CYBERSECIDENT/369532/I/NCBR/2017.

6. Znaczenie uzyskanych wyników dla danej dyscypliny naukowej

Jako najważniejsze oryginalne osiągnięcia rozprawy doktorskiej mgr inż. Jędrzeja Bieniasza w dyscyplinie informatyka techniczna i telekomunikacja należy wymienić:

- Opracowanie koncepcji steganograficznego systemu plików SocialStegDisc, w którym mechanizm indeksacji danych jest rozszerzeniem rozwiązania StegHash. W ramach zrealizowanych badań:
    - Zdefiniowano steganograficzne metody realizacji podstawowych operacji klasycznego systemu plików, w tym tworzenie pliku, odczyt pliku, usuwanie pliku.
    - Zaimplementowano system SocialStegDisc w postaci proof-of-concept.

- Przeprowadzono wszechstronne analizy i testy systemu SocialStegDisc pod kątem różnych dodatkowych funkcjonalności, w tym: możliwości skalowania rozmiaru dysku, sposobu tworzenia sekretów, wydajności działania w realnym środowisku otwartej sieci społecznościowej.
- Opracowano ocenę różnych aspektów działania systemu, w tym:
  - w zakresie niewykrywalności i niezawodności systemu;
  - w zakresie procesów kryminalistyki śledczej;
  - w zakresie nierównomierność przestrzeni adresowej.
  - w zakresie możliwości wykorzystania systemu jako mechanizmu cyberodporności.

- Przeprowadzenie syntezy stanu wiedzy w zakresie stosowania metod steganografii do komunikacji typu C2 (ang. *Command & Control*). Rozważono różne metody, metody steganografii obejmujące stegnaografię multimedialną, sieciową oraz hybrydową, realizowaną jako metoda rozproszona. W ramach zrealizowanych badań:
  - Opracowano modele teoretyczne kanałów C2 wykorzystujących steganografię.
  - Przeanalizowano wykorzystania steganografii do realizacji kanałów C2 w ramach różnych metodyk modelowania cyberzagrożeń.
  - Opracowano przegląd możliwych metod wykrywania i przeciwdziałania kanałom C2 zabezpieczonym steganografią.
  - W oparciu o autorską taksonomię przeanalizowano cyberataki z lat 2010–2018, w których zastosowano kanały C2 wykorzystujące metody steganografii.
- Opracowanie koncepcji teorii obserwacji zmiany oraz metod monitorowania i detekcji kanałów steganograficznych w rozproszonych środowiskach teleinformatycznych z wykorzystaniem systemów wieloagentowych. Stosując opracowane metody można m.in. wykryć i śledzić kradzież danych w ramach komunikacji C2. Opracowane metody opierają się na wykrywaniu węzłów źródłowych realizowanych operacji, co umożliwia podjęcie odpowiednich działań, np. blokada ruchu sieciowego. W ramach zrealizowanych badań:
  - Opracowano syntezę stanu wiedzy w obszarze badań.
  - Opracowano scenariusze testowe w zakresie realizacji symulacji metod steganografii we wskazanym środowisku wraz ze sformułowaniem hipotez badawczych.
  - Opracowano metody analizy uzyskanych danych.
  - Zaimplementowano i zbadano jakość działania metod uczenia maszynowego.
  - Opracowanie oceny uzyskanych wyników oraz sformułowanie wniosków końcowych.
- Opracowanie koncepcji rozproszonego systemu steganograficznego dla urządzeń internetu rzeczy wykorzystującej mechanizmy StegHash i SocialStegDisc. System ma możliwość realizacji rozproszonej komunikacji kanałami steganograficznymi o charakterze hybrydowym, tj. łączącym steganografię komunikacyjną i steganografię przechowywania danych. W ramach zrealizowanych badań:

- Opracowano architekturę warstwową systemu. Każda z warstw zawiera, obok komponentu realizacji zadań podstawowych, uzupełniający komponent steganograficzny właściwy dla danej warstwy.
- Opracowano podstawowe mechanizmy steganograficzne dla komunikacji zgodne z koncepcją cyberfog, w tym:
  - mechanizm indeksacji wykorzystujący metodę StegHash;
  - mechanizm dyspersji wykorzystujący metodę SocialStegDisc;
  - rozszerzenie zbioru nośników ukrytych informacji poza materiały multimedialne;
  - możliwość zastosowania platform komunikacji steganograficznej np. TrustMAS.
- Opracowano założenia dla protokołu komunikacji i aspektów operacyjnych systemu końcowego.
- Analiza systemu pod kątem:
  - bezpieczeństwa;
  - niezawodności;
  - zużycia pamięci;
  - czasu działania.

- Opracowanie nowego system steganografii rozproszonej StegFog, bazującego na schemacie indeksowania wprowadzony przez StegHash. W ramach zrealizowanych badań:
  - Zaprojektowano architektury systemu.
  - Zdefiniowano podstawowe mechanizmu systemu StegFog w zakresie:
    - zapisywania i odczytywania danych ukrytych w systemie;
    - ukrytej notyfikacji o dostępności danych;
    - ukrytego routingu do kolejnych fragmentów danych;
    - mechanizmu adresacji kolejnych fragmentów danych.
  - Zaimplementowano prototyp systemu.
  - Analiza systemu pod kątem:
    - projektu architektury oraz zdefiniowanych protokołów;
    - bezpieczeństwa mechanizmu adresacji;
    - parametrów operacyjnych systemu, w tym czas działania, zużycie pamięci, przepływności steganograficznej.

Należy podkreślić, że opracowane w recenzowanej rozprawie koncepcje oraz uzyskane wyniki mają duże znaczenia praktyczne. Doktorant zdefiniował i następnie rozwiązał realne i aktualne problemy badawcze związany z cyberbezpieczeństwem w obszarze steganografii stosując wiele różnych narzędzi badawczych, w tym metody uczenia maszynowego.

7. Główne wady rozprawy, słabe stron wraz z krytycznymi uwagami szczegółowymi

Uwagi natury ogólnej:

- Brak przedstawienia tezy rozprawy (pytania badawczego), Doktorant nie sformułował głównej tezy rozprawy, sformułowany został jedynie główny cel rozprawy.
- W rozprawie brakuje próby generalizacji uzyskanych wyników w zakresie inteligentnego wykrywania i reagowania na cyberzagrożenia wykorzystujące rozproszone metody ukrywania informacji. Moim zdaniem brakuje szerszego spojrzenia na poszczególne zagrożenia i próby zaproponowania bardziej uogólnionych metod.
- W podsumowaniu nie przedstawiono propozycji dalszych prac badawczych stanowiących rozszerzenie osiągnięć uzyskanych w rozprawie.

Uwagi natury polemicznej:

- Czy w kontekście stosowania metod uczenia maszynowego do wykrywania przypadków użycia steganografii były rozważane niestacjonarne strumienie danych dotyczące przypadków gdy rozkłady statystyczne danych mogą ulec zmianie, zmuszając model do uwzględnienia ich dynamiki w trakcie eksploatacji? Zjawisko to nazywa się dryfem koncepcji (ang. *concept drift*).

8. Konkluzja

Recenzowana rozprawa stanowi oryginalne rozwiązanie jednoznacznie sformułowanego zagadnienia naukowego. Autor rozprawy mgr inż. Jędrzej Bieniasz w przekonujący sposób wykazał umiejętność samodzielnego prowadzenia badań naukowych, a także ich prawidłowej i wnikliwej interpretacji. Wymienione powyżej uwagi ogólne, polemiczne oraz szczegółowe nie mają znaczącego wpływu na pozytywną ocenę rozprawy. W związku z powyższym uważam, iż przedstawiona mi do recenzji rozprawa doktorska mgr inż. Jędrzeja Bieniasza spełnia wymogi zawarte w ustawie dnia 20 lipca 2018 r. *Prawo o szkolnictwie wyższym i nauce* i wnoszę o dopuszczenie jej do publicznej obrony.