prof. dr hab. inż. Aleksander Byrski
Instytut Informatyki
Akademia Górniczo-Hutnicza
im. Stanisława Staszica w Krakowie
Al. Mickiewicza 30, 30-059 Kraków
olekb@agh.edu.pl

Kraków 28.10.2022

Recenzja rozprawy doktorskiej pt. "Rozproszone metody ukrywania informacji w sieciach" opracowanej przez mgr inż. Jędrzeja Bieniasza, asystenta w Instytucie Telekomunikacji, Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej

Mgr inż. Jędrzej Bieniasz (dalej "Doktorant") przedstawił do oceny rozprawę doktorską w formie cyklu następujących artykułów:

- [A1] Bieniasz, J., & Szczypiorski, K. (2017). SocialStegDisc: Application of steganography in social networks to create a file system. 2017 3rd Internatio- nal Conference on Frontiers of Signal Processing (ICFSP), 2017, pp. 76-80. DOI: https://doi.org/10.1109/ICFSP.2017.8097145. Rodzaj publikacji: materiały pokonferencyjne (IF: –; liczba cytowań: 7) Punktacja MEiN: 20
- [A2] Bieniasz, J., & Szczypiorski, K. (2019). Methods for Information Hiding in Open Social Networks. Journal of Universal Computer Science, 25(2), 74-97. DOI: https://doi.org/10.3217/jucs-025-02-0074. Rodzaj publikacji: artykuł w czasopiśmie (IF: 1.139; liczba cytowań: 2) Punktacja MEiN: 40
- [A3] Bieniasz, J., & Szczypiorski, K. (2019). Steganography Techniques for Command and Control (C2) Channels. In Botnets. Architectures, Countermeasu- res, and Challenges. (pp. 189-216). CRC Press. DOI: https://doi.org/10.1201/ 9780429329913-5. Rodzaj publikacji: rozdział w monografii (IF: –; liczba cytowań: 0) Punktacja MEiN: 50
- [A4] Bieniasz, J., Stepkowska, 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. DOI: https://doi.org/ 10.3217/jucs-025-09-1109 Rodzaj publikacji: artykuł w czasopiśmie (IF: 1.139; liczba cytowań: 7) Punktacja MEiN: 40
- [A5] Bieniasz, J., & Szczypiorski, K. (2021). Dataset Generation for Develop- ment of Multi-Node Cyber Threat Detection Systems. Electronics. 2021; 10(21):2711. DOI: https://doi.org/10.3390/electronics10212711. Rodzaj publikacji: artykuł w czasopiśmie (IF: 2.937; liczba cytowań: 1) Punktacja MEiN: 100
- [A6] Bieniasz, J., & Szczypiorski, K. (2018). Towards Empowering Cyber Attack Resiliency Using Steganography. 2018 4th International Conference on Fron- tiers of Signal Processing (ICFSP), 2018, pp. 24-28. DOI: https://doi.org/10. 1109/ICFSP.2018.8552068. Rodzaj publikacji: materiały pokonferencyjne (IF: –; liczba cytowań: 1) Punktacja MEiN: 20
- [A7] Bieniasz, J., Bąk, P., & Szczypiorski, K. (2022). StegFog: Distributed Steganography Applied To Cyber Resiliency In Multi Node Environments. IEEE Access,

2022. DOI: https://doi.org/10.1109/ACCESS.2022.3199749. Rodzaj publikacji: artykuł w czasopiśmie (IF: 3.476; liczba cytowań: 0) Punktacja MEiN: 100.

Wspomniane artykuły stanowią najważniejszą część 175-stronicowego manuskryptu. Manuskrypt zaczyna część wstępna zawierająca sformułowanie następującego celu pracy: przeprowadzenie badań teoretycznych i praktycznych w zakresie różnych aspektów rozproszonych metod ukrywania informacji w sieciach zgodnie z nowoczesnym podejściem do budowy zdolności do wykrywania i reagowania na cyberzagrożenia w oparciu na wiedzy i danych.

Po części wstępnej zamieszczono dokładny przewodnik po treści załączonych artykułów, przedstawiający najważniejsze osiągnięcia w nich zamieszczone. Manuskrypt zawiera również CV naukowe Doktoranta, co ułatwia ocenę, mimo tego iż nie jest wymagane przez obowiązujące akty prawne. Doktorant zamieścił również oświadczenia współautorów odnośnie kontrybucji do poszczególnych artykułów zarówno w formie szacowania procentowego wkładu pracy jak i podając merytoryczne aspekty przypadające na poszczególnych współautorów. Zamieszczone oświadczenia utwierdzają w przekonaniu, że Doktorant pełnił rolę wiodącą we wszystkich przedstawionych w cyklu pracach naukowych.

Steganografia a w szczególności w wydaniu prezentowanym przez Doktoranta jest niezmiernie ciekawym i niewątpliwie posiadającym wysoki potencjał zastosowania tematem badawczym. Przechowywanie wrażliwych danych w sposób ukryty, docelowo niewykrywalny w obszarze tak bardzo otwartym dla każdego, jakim są sieci komputerowe a nawet społeczne, niewątpliwie jest i będzie atrakcyjne zarówno dla osób mających w planach zarówno legalne (ukrywanie wrażliwych danych np. przez upoważnione służby) jak i nielegalne (np. komunikacja systemów biorących udział np. w atakach w cyberprzestrzeni) wykorzystanie tego typu narzędzi. Dlatego jednocześnie ważne jest opracowanie metod ukrywania danych jak i metod wykrywania tego typu działań - dokładnie w ten obszar wpisuje się przedstawiona do recenzji rozprawa.

W ramach przedstawionego do oceny cyklu artykułów, Doktorant badał naturę rozproszonych metod steganografii (artykuły [A1] i [A2]) w ramach których m.in. opracował autorski system plików o nazwie SocialStegDisc rozszerzając koncepcję StegHash opracowaną wcześniej przez jego Promotora, wprowadzając sekwencję bloków oraz definiując możliwości operacji na plikach wraz z przeprowadzeniem niezbędnych analiz i testów a także ewaluacji cechy niewykrywalności systemu, rozważając również możliwość zastosowania zaproponowanego rozwiązania jako jednej z metod cyberodporności systemu. Artykuły te można określić jako najważniejsze w cyklu, w szczególności prezentujące najistotniejsze osiągnięcia Doktoranta.

W [A3] Doktorant skupia się na analizie stanu wiedzy dotyczącej wykorzystywania steganografii do komunikacji Command and Control wraz z przeglądem metod jej wykrywania i zapobiegania, odniesienie wykorzystania steganografii do realizacji kanałów C2 w ramach metodyk modelowania zagrożeń, a także podsumowuje on najważniejsze znane ataki C&C z lat 2010-2018. Artykuł ten ma charakter przeglądowy i dowodzi szerokiej wiedzy Doktoranta w obszarze cyberbezpieczeństwa i steganografii.

W artykułach [A4] i [A5] opisana została realizacja procesu badań na danych na potrzeby detekcji metod steganografii rozproszonej - od stworzenia symulacji metod steganografii przez implementację prototypu systemu detekcji po referencyjne zastosowanie metod data science. W artykułach Doktorant stosuje systemy wieloagentowe jako podstawę wykrycia kanałów steganograficznych. Abstrahując od niedociągnięć w kontekście prezentacji samej istoty systemu wieloagentowego (odnoszę się do tej wady później) można ocenić te artykuły jako istotny komplement do artykułów [A1] i [A2], pokazujący osiągnięcia Autora w zbliżonym obszarze badań.

W artykułach [A6] i [A7] Doktorant koncentruje się na opracowaniu i przetestowaniu koncepcji nowatorskiego systemu komunikacyjnego StegFog (mającego działać w obszarze fog computing) łączącego trzy typy klasycznych podejść do steganografii w jeden system rozproszone steganografii dzieki przechowywaniu danych w obrazach, wykorzystaniu tekstu do zarządzania wskaźnikami do ukrytych danych oraz steganografię sieciową opracowanąna potrzeby realizacji ukrytej komunikacji. To kolejny element składający się na całościowy obraz wysokich umiejętności Doktoranta nie tylko w obszarze teorii ale również praktyki, pozwalający ponadto mieć duże nadzieje nie tylko na dalszą kontynuację badań, ale również na potencjalne wdrożenia.

Przedstawione artykuły składające się na rozprawę należy wysoko ocenić w kontekście bibliometrycznym - Doktorant mimo tego iż jest w zasadzie na początku swojej kariery naukowej, już może się pochwalić publikacjami w czasopismach notowanych na tzw. liście filadelfijskiej, niektóre o bliskim lub przekraczającym 3 współczynniku wpływu, tudzież punktowanymi powyżej 100 punktów wg obowiązującej punktacji MEiN - i to pełniąc w nich rolę wiodącą zgodnie z zamieszczonymi oświadczeniami. Stanowi to dobry prognostyk dla dalszej działalności naukowej Doktoranta i zachęca do realnej, bardzo wysokiej oceny jego osiągnięć.

Podsumowując, osiągnięcia badawcze Doktoranta raportowane w przewodniku, można wskazać w następujący sposób:

[D1] Stworzenie środowiska symulacji rozproszonych metod steganografii na potrzeby zbierania zestawów danych do ich analizy.

[D2] Opracowanie architektury rozwiązania i implementacja prototypu systemu wieloagentowego do monitorowania i wykrywania cyberzagrożeń wykorzystujących metody ukrywania informacji.

[D3] Zbadanie efektywności metod z obszaru data science do analizy i wykrywania symulowanych metod steganografii oraz zaproponowanie nowego algorytmu lub architektury przetwarzania danych do wykrywania steganografii.

[D4] Opracowanie koncepcji nowej metody steganograficznej o charakterze rozproszonym na potrzeby badania jej stosowalności, efektywności i cech charakterystycznych.

[D5] Usystematyzowanie wiedzy o cyberzagrożeniach związanych z rozproszonymi metodami steganografii, w tym poprzez zastosowanie metod modelowania cyberzagrożeń do budowania cyberobrony opartej na wiedzy i danych.

[D6] Zbadanie możliwości stosowania metod steganografii rozproszonej w kontekście obronnym - np. jako mechanizm bezpieczeństwa danych czy zapewnienia prywatności.

Po zapoznaniu się z planami, osiągnięciami i raportami wskazującymi jednoznacznie na realizację w.w. działań zawartymi we wspomnianych artykułach, stwierdzam, że Doktorant zajął się sprawą bardzo istotną, zrobił to w sposób kompetentny przeprowadzając szereg eksperymentów oraz analiz, nie tylko zakańczając pewien etap swojej pracy naukowej, ale wyznaczając punkt startowy dla szeregu ścieżek badawczych i rozwojowych, dla których niniejsza rozprawa może być punktem wyjścia.

Teraz chciałbym skoncentrować się na uwagach krytycznych i dyskusyjnych, które w przypadku ocenianej rozprawy nie zmieniają postrzegania jej całości w jakikolwiek sposób i nie umniejszają jej końcowej bardzo pozytywnej oceny.

1. Określenie celu pracy jest nie do końca precyzyjne, o wiele łatwiej byłoby ocenić kompletność pracy gdyby Doktorant pokusił się o sformułowanie tezy, której potem dowiódłby w swoich publikacjach i zaznaczył w przewodniku po nich, co należy do elementarnych kroków klasycznej metody naukowej. Byłbym zobowiązany gdyby Doktorant spróbował sformułować jednoznaczną tezę w czasie obrony i wskazał jej prawdziwość na podstawie wniosków z przedstawionych artykułów.
2. W artykule [A4] Doktorant wykorzystuje pojęcie agenta oraz systemu wieloagentowego, choć po lekturze można odczuć, że istotnie zastosowany został przez Doktoranta paradygmat agentowy do implementacji systemu monitoringu i detekcji zagrożeń - nie jest to w sposób precyzyjny pokazane w artykule. Proponuję przedyskutować w trakcie obrony algorytmy postępowania poszczególnych agentów (wysokopoziomowy pseudokod) z naciskiem na wykazanie autonomii i proaktywności.
3. Struktura łańcuchowa opracowanego przez Doktoranta dysku steganograficznego przypomina strukturę systemu blockchain - proponuje przedyskutować (jako potencjalną ścieżkę rozwoju systemu) możliwość zastosowania technologii blockchain w opracowanym systemie steganograficznym.
4. Chętnie usłyszałbym jak Doktorant ocenia możliwości wdrażania w modelu sprzedaży licencji lub open source zaproponowanych przez Doktoranta metod.
5. Język rozprawy jest poprawny tak samo oceniam skład wykonany w systemie LaTeX, w oczy rzucił mi się jeden błąd językowy który warto wskazać, otóż w podsumowaniu artykułów Doktorant używa sformułowania "stan sztuki" co jest bezpośrednim tłumaczeniem terminu angielskiego "state-of-the-art". W języku polskim raczej tłumaczy się ten termin jako "stan wiedzy".

Zgodnie z obowiązującą ustawą, rozprawa doktorska (...) powinna stanowić oryginalne rozwiązanie problemu naukowego (...) oraz wykazywać ogólną wiedzę teoretyczną kandydata w danej dyscyplinie naukowej (...) oraz umiejętność samodzielnego prowadzenia pracy naukowej (...). Stwierdzam, że przedstawiona do recenzji rozprawa spełnia przytoczone wymagania, gdyż opracował on szereg nowatorskich rozwiązań steganograficznych i przetestował ich charakterystyki, opracowane przez Doktoranta artykuły są poprawnie osadzone w literaturze tematu i świadczą o Jego szerokiej wiedzy fachowej (w tym jeden z nich ma charakter przeglądowy), zaś jego widoczne zaangażowanie w opracowanie wszystkich artykułów świadczy o tym, że jest gotowy do prowadzenia badań naukowych już raczej we współpracy z innymi naukowcami niż pod ich opieką.

Biorąc pod uwagę przytoczone powyżej obserwacje, zwracam się do Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Politechniki Warszawskiej z prośbą o dopuszczenie mgr inż. Jędrzeja Bieniasza do dalszych etapów postępowania w sprawie nadania stopnia doktora nauk technicznych. Ponadto, ze względu na wysoką jakość artykułów włączonych do cyklu (na 6 artykułów 3 z nich zostały opublikowane w czasopismach z tzw. impact factor), dużą samodzielność Doktoranta w realizacji badań, a także wysoką kreatywność i samodzielność w rozwiązywaniu postawionych problemów, rekomenduję wyróżnienie rozprawy.