Uzasadnienie wniosku o nagrodę Prezesa Rady Ministrów za osiągnięcia w zakresie działalności naukowej, w tym twórczości artystycznej lub działalności wdrożeniowej dr. hab. inż. Wojciecha Mazurczyka, prof. uczelni.
Tytuł dzieła*: Nowatorskie sposoby przeciwdziałania cyberzagrożeniom w sieciach teleinformatycznych*

Wojciech Mazurczyk otrzymał dyplom inżyniera w 2003 roku i magistra inżyniera w 2004 roku – oba na Politechnice Warszawskiej. W 2009 roku uzyskał stopień naukowy doktora nauk, a w 2014 roku stopień doktora habilitowanego w dziedzinie nauk technicznych w dyscyplinie Informatyka Techniczna i Telekomunikacja, również na Politechnice Warszawskiej. Od 2019 roku pełni funkcję profesora uczelni w Zakładzie Oprogramowania i Architektury Komputerów w Instytucie Informatyki Politechniki Warszawskiej.

W swojej działalności naukowej dr hab. inż. Wojciech Mazurczyk, prof. uczelni zajmuje się szeroko pojętą tematyką cyberbezpieczeństwa, w tym głównie analizą cyberzagrożeń oraz opracowywaniem nowatorskich sposobów im przeciwdziałania. Na Politechnice Warszawskiej jest kierownikiem Zespołu Bezpieczeństwa Systemów Komputerowych. W swoim dorobku ma ponad 200 publikacji, w tym 94 z tzw. listy filadelfijskiej (czasopisma posiadające współczynnik IF) oraz 64 w materiałach konferencji międzynarodowych. Był i jest także kierownikiem lub głównym wykonawcą grantów międzynarodowych ufundowanych m.in. przez Komisję Europejską (w ramach programów FP6, FP7 i H2020) oraz Armię USA jak i projektów krajowych (NCBR, NCN).

O jakości prowadzonych przez niego badań świadczy także to, że trzykrotnie został wskazany jako jeden z najczęściej cytowanych naukowców na świecie (Top 2% of Scientists) swojej dyscypliny naukowej na liście przygotowywanej przez Elsevier oraz Uniwersytet Stanforda za lata 2019, 2020 oraz 2021. Jest on także laureatem licznych nagród (w tym Prezesa Rady Ministrów za pracę doktorską, indywidualnych oraz zespołowych nagród Rektora PW – łącznie 7), oraz stypendiów (Ministra dla młodych wybitnych naukowców oraz prestiżowych organizacji m.in. FNP i NAWA). Odbywał również staże naukowe m.in. we Włoszech, Holandii, Hiszpanii i Niemczech.

Prowadzone przez Kandydata prace badawcze mają wymiar praktyczny i wdrożeniowy. Dr hab. inż. Wojciech Mazurczyk, prof. uczelni współpracuje z Europolem – prowadził tam szkolenia funkcjonariuszy i był członkiem Academic Advisory Network. Ponadto, opracowane rozwiązania naukowe znajdują także zastosowania praktyczne. Wiele z zaproponowanych przez dr. hab. inż. Wojciecha Mazurczyka, prof. uczelni metod detekcji zagrożeń zostało wykorzystanych w swoich produktach przez firmy będące partnerami w konsorcjach projektów europejskich. Dodatkowo, platforma Mixeway opracowana w ramach doktoratu wdrożeniowego obronionego z wyróżnieniem pod jego opieką została z sukcesem wdrożona w firmie Orange znacząco poprawiając wykrywalność różnego rodzaju podatności sieciowych oraz programowych. Za to rozwiązanie przyznano wiele nagród, w tym przez Ministerstwo Obrony Narodowej na najlepszy doktorat z dziedziny cyberbezpieczeństwa i kryptologii oraz jako najlepszy mechanizm bezpieczeństwa w 2022 r. w ramach całej grupy Orange. Wiele prac dyplomowych prowadzonych przez Kandydata kończy się wspólnymi artykułami naukowymi oraz nagrodami w konkursach organizowanych m.in. przez MON, organizację Institute4Science, czy firmę Intel.

Kluczowe publikacje dr. hab. inż. Wojciecha Mazurczyka, prof. uczelni w tematyce dzieła zgłoszonego do nagrody opublikowane w latach 2015–2022 (sumaryczny IF=101,394;

całkowita liczba punktów MEiN=3260) obejmują trzy obszary badawcze scharakteryzowane poniżej.

Obszar badawczy 1: Ukryte kanały sieciowe oraz sposoby ich wykrywania

Za najważniejsze osiągnięcie naukowe Kandydata należy uznać badania nad ukrytymi kanałami sieciowymi, w szczególności nad nowymi technikami ukrywania informacji, ich wykorzystaniem przez atakujących oraz nad sposobami ich wykrywania oraz przeciwdziałania. Jest pomysłodawcą i głównym autorem pierwszej książki o tej tematyce pt. Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures" wydanej przez prestiżowe wydawnictwo IEEE Press-Wiley. Dotychczas książka ta doczekała się prawie 300 cytowań. Pełnił on także rolę Co-Principal Investigator w projekcie CoCoDe (Covert Channels Detection) finansowanego przez Air Force Office of Scientific Research (AFOSR), USA.
Jest również pomysłodawcą i koordynatorem, stworzonej we współpracy z Europolem, inicjatywy CUIng (Criminal Use of Information Hiding), której celem jest podnoszenie świadomości dot. technik ukrywania informacji oraz integracja ekspertów pochodzących z różnych środowisk (naukowców, ekspertów z firm i instytucji). Obecnie w ramach CUIng współpracuje ponad 400 ekspertów z ponad 35 krajów z całego świata.

Wśród najważniejszych koncepcji naukowych w tej tematyce opracowanych przez dr. hab. inż. Wojciecha Mazurczyk, prof. uczelni należy wymienić m.in. koncepcję dynamicznego i adaptacyjnego strażnika, czyli elementu odpowiadającego za efektywne przeciwdziałanie zastosowania ukrytych kanałów sieciowych, kompleksowe analizy istniejących i nowych protokołów sieciowych pod kątem tych podatności (np. MQTT, IPv6, SCTP), wykorzystanie do detekcji rozwiązania eBPF (*Extended Berkeley Packet Filter*), technik uczenia maszynowego, czy charakterystyki zużycia energii na urządzeniach mobilnych. Przeprowadzone badania dotyczą zatem zarówno zagadnień związanych z testowaniem nowych technik ukrywania informacji, jak i nowych metod detekcji i przeciwdziałania. W ramach tego dorobku znajdują się także prace przeglądowe oraz zwiększające świadomość społeczeństwa i specjalistów związanych z tego typu zagrożeniami. Artykuły, w których zawarto przedstawione powyżej badania zostały opublikowane w prestiżowych czasopismach JCR m.in. *Future Generation Computer Systems, Computers & Security, IEEE Transactions on Information Forensics and Security, Communications of the ACM,* czy *IEEE Security and Privacy magazine,* itp.

Obszar badawczy 2: Analiza technik atakujących

Innym zagadnieniem badawczym, w którym dr hab. inż. Wojciech Mazurczyk, prof. uczelni ma ważne osiągnięcia naukowe jest analiza ataków sieciowych oraz opracowywanie efektywnych sposobów ich detekcji i blokowania. W ramach tej tematyki przeprowadzone zostały badania wielu rodzin jednego z obecnie najważniejszych zagrożeń, czyli *ransomware*. Uzyskane wyniki zostały przekazane m.in. polskiej Policji oraz przedstawione w siedzibie Europolu w Hadze. Zaproponowane zostały także praktyczne sposoby, które można wykorzystać w celu obrony przed nimi. Ponadto, analizowane były także techniki cyberrekonesansu, a także ruch generowany przez prawdziwe próbki złośliwego oprogramowania, dzięki czemu było możliwe określenie „odcisku palca" poszczególnych rodzin malware, jak i wskazanie anomalii z nim związanych. Przeprowadzone w tym obszarze badania mają także charakter praktyczny i przekładają się bezpośrednio na bezpieczeństwo sieci komputerowych. W jednej z prac naukowych przedstawionych do nagrody PRM przedstawiono metodę redukcji podatności sieciowych i programowych oraz opracowano

i zaprezentowano platformę Mixeway, która jest orkiestratorem bezpieczeństwa wykorzystującym techniki ML i NLP. Została ona z sukcesem wdrożona w firmie Orange znacząco poprawiając wykrywalność różnego rodzaju podatności. Rozwiązanie to jest dostępne publicznie na zasadach opensource i przyznano za nie nagrody m.in. Ministerstwa Obrony Narodowej oraz w konkursie w ramach całej grupy Orange.
Warto również dodać, że Kandydat brał także udział w projekcie europejskim w ramach programu Horizon 2020 – SIMARGL (Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware), gdzie razem z partnerami z innych krajów opracowywał nowatorskie rozwiązania detekcji i przeciwdziałania atakom na sieci teleinformatyczne.

Obszar badawczy 3: Mechanizmy zabezpieczeń w sieciach następnych generacji (5G/6G)

Dr hab. inż. Wojciech Mazurczyk, prof. uczelni opracował także szereg zabezpieczeń dedykowanych dla przyszłych sieci teleinformatycznych np. 5G/6G. Te metody przeciwdziałania zagrożeniom są oparte na nowoczesnych technologiach sieciowych takich jak programowalne sieci komputerowe – SDN (Software-Defined Networking) i często wykorzystują algorytmy uczenia maszynowego. W ramach europejskiego projektu IoRL (Internet of Radio Light), którego był kierownikiem rozwijał możliwości wykrywania różnego rodzaju ataków sieciowych (np. skanowania, ataków odmowy usługi, spoofingu) za pomocą specjalistycznych modułów bezpieczeństwa funkcjonujących na kontrolerze SDN. Natomiast techniki uczenia maszynowego były wykorzystywane w celu poprawienia skuteczności wykrywania ataków sieciowych lub sprawdzenia jak zmieni się zagrożenie w momencie, gdy atakujący będzie wyposażony w tego typu funkcjonalność.

W ramach wymienionych powyżej zagadnień naukowych Wojciech Mazurczyk jest także głównym organizatorem międzynarodowych workshopów takich jak ENS (Emerging Networks Security) oraz CUING (Criminal Use of Information Hiding), które od ponad 6 lat odbywają się razem z konferencją ARES (International Conference on Availability, Reliability and Security). Ponadto jest współorganizatorem także International Workshop on Traffic Measurements for Cybersecurity (WTMC), który odbywał się wraz z prestiżowymi konferencjami bezpieczeństwa m.in. *IEEE Security & Privacy, AsiaCCS* oraz *EuroIEEE Security & Privacy*.

Pan Wojciech Mazurczyk jest również członkiem redakcji wielu renomowanych czasopism naukowych. Jest redaktorem naczelnym czasopisma Journal of Cyber Security and Mobility. Od 2018 do 2021 roku pełnił rolę Associate Editor w czasopismie *IEEE Transactions on Information Forensics and Security*. Od 2018 do 2020 roku pełnił funkcję redaktora serii Mobile Communications and Networks, a w latach 2013–2018 był technicznym redaktorem współpracującym z czasopismem *IEEE Communications Magazine*.

Podsumowując dr hab. inż. Wojciech Mazurczyk, prof. uczelni opublikował dotąd ponad 200 artykułów naukowych w czasopismach oraz recenzowanych materiałach konferencyjnych, a jego prace są rozpoznawane w środowisku naukowym o czym świadczą parametry naukometryczne: H-index: 37, liczba cytowań: 5049 (wg Google Scholar z 23.03.2023r.). Świadczą o tym także zaproszenia do komitetów programowych prestiżowych konferencji międzynarodowych (m.in. IEEE Globecom, IEEE ICC, IEEE CNS, IEEE LCN, ARES), do recenzowania czy współprowadzenia prac doktorskich na zagranicznych uczelniach (Francja, USA) oraz do wygłaszania referatów plenarnych (keynote) na spotkaniach NATO i konferencjach we Włoszech, Niemczech i Chinach. Kandydat jest także zapraszany do oceny wniosków grantowych na całym świecie, w tym przez National Research Center for Applied Cybersecurity(ATHENE) w Niemczech, Polsko-Amerykańską Komisję Fulbrighta, czy National Science Foundation (NSF) z USA.