dr hab. inż. Jerzy Konorski, prof. nadzw. PG
Politechnika Gdańska
Wydział Elektroniki, Telekomunikacji i Informatyki
Katedra Teleinformatyki

Gdańsk, 23.03.2018

Recenzja rozprawy doktorskiej mgr. inż. Tytusa Kurka
pt. "*Metody zapewniania poufności polityki bezpieczeństwa przy realizacji usług bezpieczeństwa w chmurze obliczeniowej*"

Tematem recenzowanej rozprawy doktorskiej są zagadnienia eksportu usług bezpieczeństwa z sieci klienta do chmury publicznej w ramach modelu biznesowego znanego jako *Security as a Service* (SecaaS) oraz próby systematycznego zapewniania prywatności polityki bezpieczeństwa klienta. Jest to atrakcyjny obszar badawczy, zarówno z uwagi na rosnące znaczenie architektur chmurowych (w rozprawie przytacza się przekonujące przykłady i dane ilustrujące tę tezę), jak i na rysujące się tutaj wyzwania naukowe (w uproszczeniu idzie bowiem o efektywne wykonywanie operacji na nieznanych danych). Wykorzystując możliwość zawartą w obowiązującej ustawie o stopniach naukowych Doktorant przedstawia rozprawę w formie monotematycznego cyklu publikacji z lat 2015-2017, opatrzonego autoreferatem zawierającym ich dane bibliograficzne oraz wskaźniki bibliometryczne Doktoranta, a także uzasadnienie ważności podjętej tematyki, zarys podejścia do problemu oraz streszczenie głównych pomysłów oryginalnych. Na podstawie autoreferatu oraz części przeglądowych w poszczególnych publikacjach można ocenić, że Doktorant posiada wystarczającą wiedzę i umiejętności informatyczne dla prowadzenia badań naukowych w tematyce rozprawy.

Na pięć publikacji wchodzących w skład cyklu jedna jest samodzielnego autorstwa Doktoranta, zaś w pozostałych występuje on jako jeden z 3 lub 4 współautorów. Trzy są artykułami w czasopismach z listy JCR o średnich (jak na dyscyplinę informatyka) współczynnikach wpływu, zaś dwie są referatami konferencyjnymi zamieszczonymi w czasopiśmie krajowym i w zagranicznym wydawnictwie zbiorowym. Artykuł samodzielny ma charakter przeglądowy, pozostałe zaś – przyczynkowy. Poniżej zamieszczone jest krótkie krytyczne omówienie każdego z nich.

Omówienie cyklu publikacji

Artykuł [A1] (z zachowaniem numeracji w p. 1 Autoreferatu) jako jedyny jest samodzielnego autorstwa Doktoranta. Opublikowany został w krajowym czasopiśmie *Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne*. Nie zawiera wyników oryginalnych, a jedynie wprowadzenie do tematyki rozprawy, przegląd najważniejszych pozycji literatury oraz szkic podejścia rozwijanego w rozprawie. Można tam znaleźć podstawowe informacje o modelu SecaaS i jego implementacjach w architekturach chmurowych, dyskusję na temat potrzeby ochrony prywatności polityki bezpieczeństwa klienta, skrótowe omówienie istniejących uniwersalnych rozwiązań kryptograficznych (w tym opartych na szyfrowaniu homomorficznym) oraz rozwiązań swoistych względem usług bezpieczeństwa, a także ich porównanie z punktu widzenia wymagań, wydajności i zastosowań. W końcowej części artykułu Doktorant formułuje postulaty pod adresem "ultymatywnej" ochrony prywatności polityki bezpieczeństwa i przedstawia wizję rozwiązań w hybrydowych architekturach chmurowych, streszczając zwięźle niektóre z wyników rozprawy.

Artykuł [A2] autorstwa Doktoranta i dwóch współpracowników jest główną pracą analityczną wchodzącą w skład rozprawy. Został opublikowany w *Int. J. of Information Security*, stosunkowo wysokopunktowanym czasopiśmie z listy JCR i według załączonych oświadczeń twórczy udział Doktoranta wynosi 60%. Artykuł posiada już kilka cytowań obcych w bazie Google Scholar i został wyróżniony przez *ACM Computing Reviews* umieszczeniem wśród najbardziej interesujących prac w zakresie inżynierii obliczeń za 2016 rok. W ramach modelu SecaaS Autorzy przedstawiają koncepcję hybrydowej chmury obliczeniowej dla sieci IP opartej na anonimizacji polityki bezpieczeństwa klienta poprzez zastąpienie specyfikacji list kontroli dostępu specjalnymi strukturami danych zwanymi *filtrami Blooma*. Z uwagi na nieodłączne dla takich filtrów błędy klasyfikacji (fałszywe alarmy) bezpośredni odczyt polityki bezpieczeństwa jest utrudniony. Co prawda w ogólności stosowanie hybrydowych chmur obliczeniowych staje się powszechnym trendem, zaś w szczególności pomysł zastosowania filtrów Blooma wysunęli kilka lat wcześniej dwaj inni badacze, Khakpour i Liu, nazywając go *Ladon*, jednak zasługą Autorów jest zwrócenie uwagi na podatność tego rozwiązania na ataki analizy ruchu. Chodzi o możliwość identyfikacji polityki bezpieczeństwa klienta w drodze dostatecznie długotrwałego procesu uczenia wykorzystującego obserwacje strumienia pakietów IP zaakceptowanych jako dozwolonych z punktu widzenia polityki klienta. Nasuwa się więc konieczność zarezerwowania fazy akceptacji pakietów dla chmury prywatnej, posadowionej w sieci klienta z zainstalowaną funkcją zapory ogniowej, a zarazem odciążenia klienta od obliczeniowo intensywnej fazy analizy głównego składnika ruchu wejściowego, jaki stanowią pakiety niedozwolone; faza ta realizowana jest przez chmurę publiczną, z reguły posadowioną u dostawcy usług internetowych klienta. Zaproponowano, by zamiast dążenia do jednoznaczności decyzji o akceptacji pakietów w chmurze publicznej poprzez zwielokrotnienie filtrów Blooma, tak jak to ma miejsce w rozwiązaniu *Ladon*, postąpić odwrotnie: wymuszać niejednoznaczne decyzje dla pakietów dozwolonych, pozbawiając je w ten sposób wartości informacyjnej zarówno dla samej chmury publicznej, jak i dla ewentualnego obserwatora na trasie chmura publiczna-chmura prywatna. Rozwiązanie takie nazwano *Ladon Hybrid Cloud* (LHC); z pewnością można je uznać za innowacyjne, zaś cały artykuł za wartościowy przyczynek do badań nad modelem SecaaS.

Przedmiotem analizy jest wymienność pomiędzy trzema charakterystykami rozwiązania LHC: wydajności obliczeniowej (mierzonej stosunkiem wielkości ruchu na wejściu i na wyjściu publicznej chmury obliczeniowej), ryzykiem przeciążenia prywatnej chmury obliczeniowej oraz skuteczności anonimizacji polityki bezpieczeństwa. Dwie pierwsze charakterystyki wydają się być ze sobą związane niemal wprost – duże wartości tej pierwszej oznaczają bowiem, że znaczna część pakietów niedozwolonych zostanie odrzucona w chmurze publicznej, odciążając w ten sposób chmurę prywatną. Zarazem przeciążenie chmury prywatnej stanowi poważne utrudnienia w pracy klienta, podczas gdy wydajność chmury publicznej sama w sobie nie przekłada się na percepcję klienta; np. trudno wyobrazić sobie, by cena usług chmury zależała od wydajności, skoro ta przesądzana jest przez klienta – poprzez politykę bezpieczeństwa (z której wynika udział pakietów dozwolonych) i strukturę filtrów Blooma (z której wynika prawdopodobieństwo niejednoznacznych decyzji). Być może zatem wystarczyłoby analizować jedynie ryzyko przeciążenia prywatnej chmury obliczeniowej. Odnośnie trzeciej z wymienionych charakterystyk Autorzy przyznają, że ilościowe badania są trudne i możliwe jest jedynie wnioskowanie pośrednie, częściowo wynikające także z przeprowadzonych eksperymentów z konkretnymi politykami bezpieczeństwa w rzeczywistym środowisku sieciowym. Tymczasem bardzo interesującym wyzwaniem naukowym byłaby tu próba sformułowania gwarancji co do niemożliwości odtworzenia w określonym czasie polityki bezpieczeństwa klienta przez właściciela chmury publicznej, bądź obserwatora na trasie niezaufanego łącza pomiędzy chmurami publiczną i prywatną, przy użyciu algorytmów o zadanym poziomie inteligencji i złożoności (warto zauważyć, że wystarczająca może okazać się tutaj analiza cech nieobecnych w łączu pakietów niedozwolonych). Rozważania na ten temat w końcówce p. 4.1 artykułu, skądinąd zdroworozsądkowe, są mało precyzyjne.

Przeprowadzona w artykule analiza probabilistyczna jest nietrudna i zasadniczo poprawna (również w świetle porównania z wynikami eksperymentalnymi), choć niewolna jest od kilku usterek.

Wyprowadzenie wzoru (4) jest niepotrzebnie rozwlekłe. We wzorze (11) zastępowanie ilorazu wielkości losowych przez iloraz ich kwantyli w sytuacji nieznajomości rozkładów wymaga co najmniej obszerniejszego komentarza. Wzór (15) pozostawiony jest w postaci niekompletnej, gdyż – skoro R i U można chyba uznać na zmienne wolne – nie określa granicznej wartości p dla zakresu dużych obciążeń chmury publicznej; przypuszczalnie chodzi o niemożność doboru p w tym zakresie, co można uznać za mankament proponowanego rozwiązania. Rozumowanie prowadzące do wzoru (18) jest niekonsekwentne: skoro na danym poziomie diagramu filtrów Blooma koincydencja wszystkich fałszywych alarmów jest niemożliwa, to trudno działanie tych filtrów uznać za statystycznie niezależne, więc wzór (18) nie ma uzasadnienia. Być może stanowi on dobre przybliżenie dla dużych wartości parametrów filtrów Blooma (podobnie jak często przyjmowany w praktycznych analizach wzór (21)), lecz dla ścisłości wywodu konieczne jest jakieś wyjaśnienie. Nienaturalne jest doprowadzenie analizy do wzoru (19) przyjmując liczbę poziomów $J = 5$, gdy kolejny wzór dla dowolnego J jest zupełnie analogiczny. Ciekawym uzupełnieniem analizy probabilistycznej byłaby deterministyczna analiza algorytmu modyfikującego strukturę filtrów Blooma na najniższym poziomie diagramu tak, by uniemożliwić jednoznaczne decyzje dla pakietów dozwolonych przez politykę bezpieczeństwa klienta. Na ten temat czytelnik znajduje jedynie wzmiankę na końcu str. 32 oraz na str. 38 i 40 dość ogólny opis "generatora", tj. programu modyfikującego strukturę filtrów Blooma stosownie do założonego prawdopodobieństwa niejednoznacznej decyzji, wraz z oceną nakładów obliczeniowych. Można sądzić, że podstawą modyfikacji są zależności od parametrów liczbowych wynikające ze wzorów (20) i (21), ale nie wiadomo, czy sama struktura składowych funkcji skrótu ma istotne znaczenie i czy proces modyfikacji daje się systematycznie optymalizować.

Pomimo swych niedoskonałości przedstawiona analiza spełnia swą rolę, tj. dostarcza teoretycznej podbudowy projektowania parametrów anonimizacji polityki bezpieczeństwa klienta. Na podkreślenie zasługuje staranna, choć z konieczności ograniczona co do liczby rozpatrywanych polityk bezpieczeństwa weryfikacja eksperymentalna (symulacyjna) w warunkach rzeczywistego środowiska sieciowego, a także konstrukcja odpowiednich narzędzi programowych. W zakończeniu artykułu trafnie wskazuje się na ograniczenia rozwiązania LHC, w szczególności możliwość identyfikacji polityki bezpieczeństwa klienta na podstawie ruchu potwierdzeń warstwy transportowej, szkicując środki zaradcze o charakterze dywersyfikacyjnym, kryptograficznym, bądź maskującym. Należałoby do nich chyba dodać mechanizmy typu *proxy TCP*, o ile jakość łącza pomiędzy chmurą publiczną i prywatną można przyjąć jako dostatecznie wysoką. Ograniczenie rozwiązania LHC jest ogólniejszej natury: nie nadaje się ono do kontekstowo zorientowanego wykrywania zagrożeń, np. działań niezgodnych z maszynami stanów standardowych protokołów komunikacyjnych, a są to częste wektory ataku. Wyklucza to także typowe algorytmy wykrywania anomalii.

Powyższe omówienie można zakończyć dwiema uwagami krytycznymi, które mają zastosowanie również do kolejnych artykułów przedstawionego cyklu. W warstwie motywacyjnej bardzo brakuje formalnego modelu intruza oraz przykładów scenariuszy ataków. W warstwie koncepcyjnej można dostrzec pewien brak konsekwencji: skoro chmurę publiczną traktuje się jako potencjalnego intruza, skąd pewność, że będzie ona wiernie realizować zaprojektowane algorytmy? Co jeśli np. będzie ona systematycznie kierować do chmury prywatnej część pakietów IP odrzuconych przez filtry Blooma? Dla wykrywania tego chmura prywatna powinna właściwie kopiować obliczenia chmury publicznej, byłby to więc skuteczny atak DoS.

Artykuł [A3], który posiada trzech współautorów z udziałem twórczym Doktoranta ocenianym na 60%, opublikowany został w markowym, średniopunktowanym czasopiśmie z listy *JCR Security and Communication Networks* i także doczekał się już cytowań. Dotyczy on eksportu usług wykrywania włamań (*Intrusion Detection Systems*, IDS) do chmury publicznej przy zarezerwowaniu części operacji dla chmury prywatnej w sieci klienta. Podobnie jak w omawianym wyżej artykule [A2], problem prywatności polityki bezpieczeństwa klienta wiąże się z koniecznością eksportu do chmury publicznej listy istotnych dla klienta sygnatur zagrożeń oraz niedozwolonych kombinacji parametrów protokołu IP. Autorzy proponują trzy wedle swej oceny przełomowe roz-

wiązania tego problemu, których wspólnym mianownikiem jest przeniesienie czynności intensywnych obliczeniowo oraz zarządczych (głównie dopasowywania i uaktualniania sygnatur) do chmury publicznej z zachowaniem po stronie chmury prywatnej decyzji o akceptacjach poszczególnych pakietów, jako niosących bezpośrednio lub pośrednio informacje o polityce bezpieczeństwa klienta. Zadaniem projektanta jest w tej sytuacji odpowiednie wyważenie nakładów obliczeniowych ponoszonych przez klienta i chmurę publiczną, a także narzutu komunikacyjnego na łączu pomiędzy chmurami publiczną i prywatną.

Najprostsze z zaproponowanych rozwiązań zakłada wykonanie wstępnego odsiewu pakietów podejrzanych w chmurze publicznej w oparciu o globalną listę sygnatur zagrożeń, bez znajomości listy sygnatur specyficznej dla klienta. Następnie pakiety podejrzane badane są w chmurze prywatnej. Wymaga to uruchomienia po stronie sieci klienta obliczeniowo kosztownych operacji IDS typu dopasowywania wzorców. Na drugim biegunie znajduje się rozwiązanie polegające na dogłębnej analizie każdego pakietu w chmurze publicznej i zaopatrzenie go w listę wszystkich dopasowanych sygnatur, którą następnie klient może jedynie przeszukać pod kątem istotnych z jego punktu widzenia. Dla uniknięcia zbędnych opóźnień w dostarczaniu pakietów do klienta listy sygnatur wraz z nagłówkami pakietów danych przekazywane są odrębnie jako pakiety kontrolne, a następnie analizowane w chmurze prywatnej niezależnie od dostarczania pakietów. Rozwiązanie to znacznie redukuje nakłady obliczeniowe po stronie sieci klienta, zarazem uniemożliwiając – w przeciwieństwie do pierwszego rozwiązania – migrację do funkcji *Intrusion Prevention System* (IPS), tj. identyfikację i ewentualne wstrzymanie dostarczenia pakietu danych po wykryciu w jego nagłówku istotnej dla klienta sygnatury. Zaproponowano także rozwiązanie pośrednie, które umożliwia skojarzenie istotnej dla klienta sygnatury z konkretnym pakietem danych i podjęcie stosownych akcji prewencyjnych – tj. migrację do funkcji IPS – dzięki przekazywaniu w pakiecie kontrolnym skrótu całego pakietu danych (według uzgodnionej pomiędzy klientem a chmurą publiczną funkcji skrótu) zamiast tylko jego nagłówka. Autorzy przedstawiają to rozwiązanie, zarazem dochodząc do wniosku, że nie posiada ono żadnych zalet w stosunku do pozostałych rozwiązań, co jest nieco zaskakujące. Prawdopodobnie zalety można dopatrzyć się w połączeniu redukcji nakładów obliczeniowych po stronie klienta z możliwością migracji do IPS. Zwiększone bezpieczeństwo tego rozwiązania polega także na pozostawieniu (nieskomplikowanej) analizy parametrów protokołu IP po stronie klienta, co jednak dodatkowo wymaga dopasowania nagłówków wyodrębnionych z otrzymanych pakietów danych do skrótów pakietów danych otrzymanych w pakietach kontrolnych.

Artykuł ma charakter opisowo-eksperymentalny z elementami porównawczej analizy jakościowej prowadzącej do tabel II i III, stanowiących dla projektanta chmurowych rozwiązań IDS dobry materiał do oceny przydatności zaproponowanych rozwiązań. Starannie opracowana część eksperymentalna pozwoliła na realistyczną ocenę czasów realizacji poszczególnych operacji obliczeniowych wymaganych przez wszystkie zaproponowane rozwiązania; implementacja w języku Python została uruchomiona w otoczeniu gotowego narzędzia do dopasowywania sygnatur *Snort*. Punkty 4 i 5 artykułu stanowią z pewnością jego mocne strony; same zaproponowane rozwiązania także można ocenić jako innowacyjne, choć od strony koncepcyjnej wydają się dość naturalne – można je zakwalifikować jako typowe działania maskujące.

Artykuł [A4] jest referatem konferencyjnym opublikowanym przez wydawnictwo Springer w serii *Communications in Computer and Information Science*. Doktorant jest jednym z czterech współautorów z deklarowanym udziałem twórczym 70%. Artykuł kontynuuje linię badań zapoczątkowaną w 2007 roku przez Goudę i Liu, zmierzających do specyfikacji usług zapory ogniowej w postaci diagramów decyzyjnych. Głównym celem artykułu jest sformułowanie matematycznych ram opisu uniwersalnej polityki IPS w przypadku, gdy polityka ta ma charakter bezstanowy i pozwala się przedstawić w postaci zestawu reguł decyzyjnych. Pomimo tych ograniczeń zamierzenie należy uznać za przydatne dla konstruowania instancji IPS w hybrydowych systemach chmurowych. Z "estetycznego" punktu widzenia w artykule brakuje próby formalnego zakreślenia rozważanej klasy polityk IPS, choć przytaczane przykłady dają pogląd, jak można to zrobić. Wychodząc z założenia że bezstanową politykę IPS można wyspecyfikować poprzez reguły kla-

syfikacji pakietów, sygnatury zagrożeń i zbiory akcji prewencyjnych, Autorzy przedstawiają dwa kluczowe wyniki: po pierwsze, sposób opisu polityki IPS przy pomocy diagramu decyzyjnego w postaci drzewa ważonego z zachowaniem warunków pozwalających przekształcić je w wewnętrznie spójny, wyczerpujący i zwarty zestaw reguł decyzyjnych (zgodnie ze znanymi wymaganiami formalnymi stosowanymi przy redukcji drzew decyzyjnych do binarnych diagramów decyzyjnych), zaś po drugie, algorytm otrzymywania takiego diagramu na podstawie wejściowej specyfikacji polityki IPS. W odniesieniu do tego algorytmu można wysunąć kilka zastrzeżeń, np. nieprecyzyjne sformułowania w punktach 3 i 4 (np. co oznacza "zawieranie elementów reguł"?). Nie podano formalnego dowodu na to, że algorytm zawsze kończy się sukcesem, a byłoby to istotne wzmocnienie poznawczego pierwiastka pracy; w szczególności nie skomentowano, czy niespełnienie warunku zwartości w danym kroku skutkuje zamianą kolejności testowania pól F_j. Bardzo przydatny byłby przykład obliczeniowy, który rozwiewałby te wątpliwości. Tę część pracy kończy naturalny algorytm wyznaczania ścieżki decyzyjnej dla pakietu o danej zawartości pól podlegających klasyfikacji.

Omawiany artykuł w pewnym sensie stanowi odstępstwo od zasadniczego nurtu badań rozprawy, gdyż nie dotyczy bezpośrednio anonimizacji polityki bezpieczeństwa klienta w modelu SecaaS, lecz efektywności obliczeniowej usługi IPS przy wykorzystaniu diagramu decyzyjnego w porównaniu do klasycznej specyfikacji w postaci zestawu reguł dopasowywania sygnatur. Przewaga diagramu decyzyjnego opartego na przedstawionym modelu matematycznym zostaje zademonstrowana eksperymentalnie przy pomocy implementacji obu algorytmów w języku Python i symulacji ich działania realizującego usługę IPS w zbliżonym do rzeczywistego środowisku ruchu IP. Czas obliczeń z wykorzystaniem diagramu decyzyjnego jest tu wielokrotnie niższy, przy czym przewaga ta maleje ze wzrostem udziału pakietów nieprzedstawiających zagrożenia, z uwagi na możliwość częstszego pomijania testów w podejściu klasycznym, a z drugiej strony na bezwarunkową konieczność wykonywania pewnych testów na diagramie decyzyjnym. Są to cenne obserwacje, gdyż dokumentują ilościowy pożytek z redukcji drzew decyzyjnych w kontekście usług IPS. Pośredni związek z zagadnieniami anonimizacji polityki bezpieczeństwa widoczny jest w punkcie 4.1 artykułu: ponieważ diagramy decyzyjne otrzymywane są w postaci drzew, można do nich zastosować podobne do przedstawionego w artykule [A2] podejście zastępowania fragmentów diagramu decyzyjnego przez filtry Blooma i wymuszania w chmurze publicznej niejednoznacznych decyzji o dopasowaniu sygnatur dla pakietów nieprzedstawiających zagrożenia. Utrudnia to analizę ruchu pakietów na łączu pomiędzy chmurą publiczną a klientem.

Artykuł [A5], ostatni w przedstawionym cyklu, został opublikowany w *Int. J. of Network Management*, średniopunktowanym czasopiśmie z listy JCR. Posiada on czterech współautorów, zaś deklarowany udział twórczy Doktoranta wynosi 60%. Praca stanowi bardzo właściwe zwieńczenie cyklu, gdyż uogólnia i rozwija idee przedstawione w poprzednich artykułach (a także we wcześniejszych pracach innych badaczy), proponując dla hybrydowych rozwiązań chmurowych uniwersalną platformę anonimizacji polityki bezpieczeństwa klienta w modelu SecaaS pod nazwą UNIPRIV. Jak przedtem, klasa usług bezpieczeństwa ograniczona jest do specyfikacji w postaci drzew decyzyjnych, przy czym istotne podane przykłady dotyczą zwłaszcza usług IPS. Anonimizacja polityki bezpieczeństwa odbywa się tu poprzez ukrycie reguł klasyfikacji pakietów IP i sygnatur zagrożeń z wykorzystaniem techniki filtrów Blooma oraz poprzez zaszyfrowanie opisów akcji prewencyjnych z użyciem szyfru monoalfabetycznego, którego klucz znany jest jedynie klientowi. Wymagane jest ponadto uzgodnienie pomiędzy chmurą publiczną a klientem wspólnego sekretnego hasła dla celów uwierzytelniania przesłanych do chmury prywatnej pakietów IP. Samo przesłanie pakietu wykorzystuje mechanizm podobny do HMAC (*hash-based message authentication code*): do pakietu dodawany jest skrót konkatenacji tego pakietu, zaszyfrowanego opisu wyznaczonej akcji prewencyjnej oraz sekretnego hasła. Umożliwia to klientowi porównanie otrzymanego skrótu z lokalnie wyliczonymi skrótami odpowiadającymi różnym możliwym akcjom prewencyjnym. (Niezbędne byłoby chyba też dodatnie etykiety czasowej dla uniknięcia ataków typu *replay*.) Autorzy pokazują eksperymentalnie, że pomimo uruchomienia po stronie klienta dodatkowych mechanizmów szyfrowania i funkcji skrótu platforma UNIPRIV w dalszym ciągu pozwala znacznie odciążyć obliczeniowo chmurę prywatną. Natomiast narzuty

komunikacyjne wynikające z dołączania skrótów pakietów danych można ocenić jako znaczące – z tabeli 2 wynika, że w zależności od typu funkcji skrótu i rozmiaru pakietów dochodzi on do 80%. Zastosowanie funkcji skrótu jest oczywiście uzasadnione z uwagi na niebezpieczeństwo kryptoanalizy klucza szyfru monoalfabetycznego klienta, choć wiąże się z możliwymi kolizjami po stronie klienta, które proponuje się rozwiązywać przez ignorowanie wywołujących je pakietów. Można się zastanawiać, czy nie stwarza to chmurze publicznej – konsekwentnie traktowanej jako potencjalny intruz – okazji do generacji sztucznych pakietów wywołujących kolizje, tj. zachowań analogicznych do ataków typu dnia urodzin, zwłaszcza gdy diagramy decyzyjne mają wiele liści (zaszyfrowanych akcji prewencyjnych).

Podsumowanie

Za najważniejsze osiągnięcia recenzowanej rozprawy, rozwijające różne wcześniejsze koncepcje innych badaczy i obudowane starannymi badaniami implementacyjnymi i eksperymentalnymi, można uznać propozycje:

- metodę ochrony prywatności polityki bezpieczeństwa klienta sieci IP w modelu SecaaS z wykorzystaniem zmodyfikowanych filtrów Blooma, utrudniającą ataki analizy ruchu (wraz z probabilistyczną oceną tego rozwiązania),
- metod organizacji eksportu niektórych typów usług IDS w hybrydowej architekturze chmurowej z zachowaniem prywatności polityki bezpieczeństwa klienta,
- formalizmu matematycznego prowadzącego do specyfikacji polityki IPS w postaci drzewiastego diagramu decyzyjnego, oraz
- metody ochrony prywatności polityki bezpieczeństwa klienta zorientowanej na usługi IPS z wykorzystaniem szyfrowania opisów akcji prewencyjnych i dopasowywaniu skrótów pakietów IP w mechanizmie typu HMAC.

Ponadto zaletami rozprawy są niewątpliwie: aktualność tematyki hybrydowych architektur chmurowych, zademonstrowane przez Doktoranta umiejętności eksperymentalne, bardzo staranna redakcja rozprawy oraz fakt opublikowania wyników rozprawy w trzech czasopismach z listy JCR, przy czym we wszystkich przypadkach potwierdzony oświadczeniami współautorów udział twórczy Doktoranta wynosi 60%, czyli jest decydujący.

Do wad rozprawy można zaliczyć rozmaite usterki wzmiankowane w powyższym omówieniu cyklu artykułów oraz brak samodzielnych publikacji przyczynkowych.

Konkluzja

Analiza zalet i wad rozprawy skłania do wniosku, że te pierwsze zdecydowanie przeważają. Recenzowana rozprawa mgr. inż. Tytusa Kurka przedstawia szereg innowacyjnych rozwinięć istniejącego stanu wiedzy i dokumentuje zdolność Doktoranta do skutecznego prowadzenia badań naukowych. Stwierdzam zatem, że spełnia ona wymagania obowiązującej ustawy o stopniach i tytułach naukowych i wnoszę o jej dopuszczenie do publicznej obrony. Spełnione jest ponadto przyjęte przez jednostkę prowadzącą przewód doktorski kryterium formalne wyróżniania rozpraw doktorskich w postaci współautorstwa przynajmniej dwóch publikacji w czasopiśmie na liście A MNiSW. W mojej ocenie rozprawa zasługuje na to także ze względu na swą merytoryczna zawartość, zwłaszcza cenne pomysły przedstawione w artykułach [A2] i [A5] oraz ich pomyślną weryfikację eksperymentalną. Stawiam więc wniosek o wyróżnienie rozprawy, uzależniając późniejsze podtrzymanie go od spełnienia innych kryteriów i przebiegu publicznej obrony.