POLITECHNIKA WARSZAWSKA
Wydział Elektroniki i Technik Informacyjnych
Instytut Telekomunikacji
ZAKŁAD CYBERBEZPIECZEŃSTWA

ul. Nowowiejska 15/19, 00-665 Warszawa

Warszawa, 23.03.2018

dr hab. inż. **Krzysztof Szczypiorski**, prof. PW

RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY WYDZIAŁU INFORMATYKI, ELEKTRONIKI I TELEKOMUNIKACJI AKADEMII GÓRNICZO-HUTNICZEJ

Tytuł rozprawy: ***Methods of preserving confidentiality of security policies in the implementation of security services in cloud computing environments***

Autor rozprawy: mgr inż. **Tytus Kurek**

1. **Jakie zagadnienie naukowe jest rozpatrzone w pracy /teza rozprawy/ i czy zostało ono dostatecznie jasno sformułowane przez autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?**

   Praca obejmuje zagadnienia bezpieczeństwa w sieciach teleinformatycznych w szczególności dotyczące metod zapewnienia poufności polityki bezpieczeństwa przy realizacji usług ochrony informacji w chmurze obliczeniowej. Cyberbezpieczeństwo w technologiach chmurowych jest bardzo istotne przede wszystkim ze względu na stosunkowo młode i modne modele biznesowe, które zmieniły podejście do zarządzania usługami ochrony informacji. Omawiany przez Autora model biznesowy *Security-as-a-Service (SecaaS)* zakłada kooperację pomiędzy klientem a operatorem z wykorzystaniem chmury obliczeniowej, która pełni rolę „zdalnej sieciowej usługi" wspierającą klienta od strony zabezpieczeń spotykanych do tej pory przeważnie w sieciach klienckich.

   W autoreferacie Autor sprawnie opisał sześć własnych metod przedstawionych szczegółowo w przedłożonej do recenzji rozprawie. Jedna z zaproponowanych metod jest uniwersalna, natomiast pozostałe są dedykowane usługom takim jak firewall, IDS, IPS. Tezę pracy można ująć następująco: *istnieją metody zwiększające prywatność klienta korzystającego z usług w modelu SecaaS.* Rozprawa ma charakter teoretyczno-doświadczalny i jest oparta: na symulacjach komputerowych, a także w typowej dla nauk technicznych w dyscyplinie Telekomunikacji konwencji *„proof of concept"* (PoC) połączonej z badaniami wybranych cech implementacji.

2. **Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł / w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle /świadczący o dostatecznej wiedzy autora. Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?**

Rozprawa ma formę spójnego tematycznie zbioru pięciu artykułów (oznaczonych A1-A5). Każdy z pięciu artykułów wchodzący w skład rozprawy posiada stosowaną analizę stanu sztuki:

- A1 w istocie jest artykułem przeglądowym, którego trzonem jest rozdział 2 - A Survey,
- natomiast artykuły A2-A5 posiadają rozdziały 2 o identycznym tytule Related Work.

Dodatkowo wprowadzający do rozprawy autoreferat syntetycznie przedstawia tło badawcze dla każdego z zagadnień.

Wyciągnięte przez Autora wnioski są przekonywujące i jasne. Każdy z artykułów posiada jasne konkluzje, a ich synteza jest klarownie ujęta w autoreferacie.

3. **Czy autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?**

Autor rozwiązał postawione zagadnienia i użył właściwych do tego metody przy uzasadnionych założeniach są uzasadnione. W rozbiciu na poszczególne części pracy wygląda to następująco:

1. Artykuł A1 ma charakter przeglądowy i zawiera przegląd najważniejszych trendów w omawianej dziedzinie.

2. Artykuł A2 dotyczy usługi firewall i zawiera propozycję mechanizmu wprowadzającego niejednoznaczność, co do decyzji związanej z analizą pakietu w chmurze publicznej. Zaproponowano hybrydowy framework LHC (*Ladon Hybrid Cloud*) wymuszający aktywne wsparcie także w chmurze prywatnej. W artykule użyto metod matematycznych i symulacyjnych z poprawnymi założeniami.

3. Artykuł A3 dotyczy usługi IDS opartej na sygnaturach i zawiera propozycje trzech nowych metod. We wszystkich metodach kluczową rolę odgrywa usługa IDS w chmurze publicznej, wspierana wariantowo IDS w chmurze prywatnej (1 metoda), bądź bez wsparcia IDS, ale za to ze wsparciem modułów obliczeniowych (metody 2 i 3). W artykule użyto metod symulacyjnych z poprawnymi założeniami.

4. Artykuł A4 dotyczy usługi IPS i bazuje na wykorzystaniu struktury drzewa decyzyjnego jako formy zapisu polityki bezpieczeństwa. W artykule użyto metody *„proof of concept"* z poprawnymi założeniami.

5. Ostatni artykuł (A5) zawiera propozycję uniwersalnej metody, która może posłużyć do wsparcia większości usług realizowanych w modelu SecaaS

z wyłączeniem niektórych firewalli (typu *stateful*) i systemów wykrywania anomalii. Główną ideą jest separacja polityki bezpieczeństwa na część decyzyjną i obliczeniową. W artykule użyto metody *„proof of concept"* z poprawnymi założeniami.

4. **Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?**

   Oryginalność pracy wynika z udanego powiązania kilku dziedzin - cyberbezpieczeństwa, kryptologii oraz teleinformatyki, w tym inżynierii ruchu.

   Zaproponowane przez Autora sześć metod stanowi bardzo istotny wkład w stan sztuki w omawianej dziedzinie. Aspekty innowacyjności Autor podsumował w autoreferacie (Tabela 3 - strona 15) i z tym zestawieniem należy się zgodzić.

5. **Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników /zwięzłość, jasność, poprawność redakcyjna rozprawy/?**

   Redakcja pracy jest poprawna, a liczba błędów edytorskich nie odbiega od typowej. Artykuły wchodzące w skład rozprawy są bardzo spójne tematycznie. Warto zwrócić uwagę, że pozycje A2, A3 i A5 zostały opublikowane w czasopismach z IF (odpowiednio 1.915, 0.806 i 1.118), a także na to, że wszystkie pozycje zostały napisane w języku angielskim, co znacząco zwiększa zasięg odbiorców. Część z prac doczekała się już cytowań np. A3 - 7, A1 - 6 (wg *Google Scholar*).

6. **Jakie są słabe strony rozprawy i jej główne wady?**

   Słabymi stronami rozprawy są:

   - brak jasno sformułowanej tezy rozprawy,
   - cechy wynikające z przyjętej formy rozprawy w tym: 1) brak ujednoliconej bibliografii, 2) pewna nadmiarowość wynikająca z tego, że każdy artykuł jest osobnym dziełem,
   - brak listy skrótów.

   Wskazane słabe strony nie mają jednak wpływu na ostateczną ocenę merytoryczną pracy.

7. **Jaka jest przydatność rozprawy dla nauk technicznych?**

   Praca ma ogromny potencjał w zakresie komercjalizacji i stanowi modelowy przykład pracy, która ma zastosowanie zarówno naukowe, jak i praktyczne. Interesującym byłoby rozszerzenie artykułu A1 i opublikowanie go np. w jednym z flagowych czasopism IEEE.

8. **Do której z następujących kategorii Recenzent zalicza rozprawę:**

~~a/ nie spełniająca wymagań stawianych rozprawom doktorskim przez obowiązujące przepisy~~

~~b/ wymagająca wprowadzenia poprawek i ponownego recenzowania~~

~~c/ spełniająca wymagania~~

d/ spełniająca wymagania z wyraźnym nadmiarem

~~e/ wybitnie dobra, zasługująca na wyróżnienie~~