Płk dr hab. inż. Zbigniew Piotrowski, profesor WAT
Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego
Wydział Elektroniki
ul. Gen. S. Kaliskiego 2, 00-908 Warszawa
tel. 261839517

Warszawa dn., 28.12.2018 r.

KWESTIONARIUSZ - RECENZJA ROZPRAWY DOKTORSKIEJ DLA POLSKO-JAPOŃSKIEJ AKADEMII TECHNIK KOMPUTEROWYCH

Tytuł rozprawy:
Wieloaspektowe modelowanie rozproszonych ataków odmowy usługi dla architektury Internetu Rzeczy.

Autor rozprawy:
mgr Katarzyna Mazur

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)?

W przedstawionej do recenzji pracy doktorskiej mgr Katarzyny Mazur pt *„Wieloaspektowe modelowanie rozproszonych ataków odmowy usługi dla architektury Internetu Rzeczy"* jest możliwe odczytanie głównej tezy pracy mówiącej o tym, że wieloaspektowa analiza bezpieczeństwa systemów IoT (ang. *Internet of Things*), pozwala określić nowe zagrożenia dotyczące ataków typu DDoS (ang. *Distributed Denial of Service*). Teza ta jest wspierana postulatem, że wielopoziomowa analiza pozwala dobrać odpowiednie parametry sieci w celu minimalizacji skutków ataku przy jednoczesnej maksymalizacji żywotności sieci oraz zachowaniu odpowiedniego poziomu bezpieczeństwa.

Autorka skoncentrowała się w swojej pracy na wieloaspektowej analizie rozproszonych ataków odmowy usługi w środowisku Internetu Rzeczy i przedstawiła do oceny ściśle ze sobą powiązany tematycznie cykl czterech publikacji udowadniających postawioną tezę. Ponadto w przedstawionej do oceny pracy autorka omówiła poszczególne artykuły będące podstawą rozprawy wraz z ich wpływem na stan nauki w dziedzinie informatyki. Omówienie to zostało poprzedzone wprowadzeniem w którym scharakteryzowano problematykę Internetu Rzeczy oraz aktualny stan wiedzy w zakresie ataków DDoS. Założenia do pracy zostały sformułowane dostatecznie klarownie i przejrzyście. Praca ma charakter eksperymentalny.

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 w przeglądu źródeł sformułowano w sposób jasny i przekonywujący?

Biorąc pod uwagę analizę źródeł wykazanych w pracy stwierdzam, że dobór literatury specjalistycznej jest poprawny i dotyczy obszarów badawczych poruszanych w przedłożonej do recenzji pracy. Biografia składa się z 60 pozycji literaturowych w tym 31 referencji w formie adresów URL do zasobów w Internecie. Na uwagę zasługuje, wykazane w rozdziale 2 na str. 27, czterech publikacji autorki rozprawy mgr Katarzyny Mazur, w których jest ona głównym współautorem wymienionym na pierwszym miejscu wśród współautorów danej publikacji i które są związane bezpośrednio z tematem rozprawy i stanowią podstawę rozprawy. Wszystkie cztery publikacje są umieszczone w periodykach indeksowanych w prestiżowej bazie *Journal Citation Reports* (JCR). W tym należy wyszczególnić: *The Computer Journal, Oxford* (Impact Factor, IF za 2017 rok 0,792 pkt), *Sensors* (IF za 2017 rok 2,475 pkt), *Journal of Sensors* (IF za 2017 rok 2,057) oraz *Mathematical Problems in Engineering* (IF za 2017 rok 1,145 pkt).

Ponadto w rozdziale pierwszym pracy we Wprowadzeniu przywołano, na podstawie źródeł literaturowych, klasyfikację i charakterystykę ataków DDoS, ukazano historię rozwoju tego typu ataków sieciowych na infrastrukturę informatyczną firm i instytucji, podano również, na podstawie literatury tematu, w jaki sposób są modelowane i analizowane rozproszone ataki odmowy dostępu do usług. Przytoczone przez autorkę mgr Katarzynę Mazur przykłady użycia ataków DDoS oraz technik stosowanych w ich dystrybucji świadczą o jej dużej wiedzy na temat ataków rozproszonych oraz o skutkach ich przeprowadzania. Wnioski z przeglądu źródeł zostały sformułowane w sposób jasny i przekonywujący.

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

Teza pracy została dowiedziona przez wykonanie, zgodnie z wykazem na str. 13 pracy, czterech zadań badawczych. Pierwszym zadaniem było stworzenie metodologii służącej do pozyskiwania niezawodnych i wolnych od błędów pomiarowych danych statystycznych, które pozwalają określić ilościowo wpływ środków ochrony na jakość zabezpieczeń urządzeń wchodzących w skład Internetu Rzeczy. Drugim zadaniem badawczym było utworzenie modelu sieci WSN do monitorowania linii wysokonapięciowych oraz określenie potencjalnych zagorzeń związanych z procesem przetwarzania na dostępność takiego systemu. Trzecim zadaniem była wieloaspektowa analiza ataków DDoS typu flood w środowisku bezprzewodowej sieci sensorowej (ang. WSN), będącej jednym z najistotniejszych elementów IoT oraz ocena wydajności i żywotności atakowanej sieci. Ostatnim zadaniem postawionym w pracy było opracowanie systemu wspomagania decyzji, wraz ze schematem kompleksowej analizy, która może być wykorzystana do oceny różnych atrybutów złożonych, heterogenicznych systemów oraz analizą zarządzania kontrolą dostępu w systemach informatycznych, charakteryzujących się wysokim poziomem dynamiki, jakimi są środowiska IoT.

Autorka rozprawy mgr Katarzyna Mazur zauważyła, że w standardzie ISO/IEC 27004 brak jest metod weryfikacji poprawności uzyskanych wyników co oznacza w konsekwencji brak wiarygodności pomiarów. Utworzono zatem nową metodykę wykonywania pomiarów którą przedstawiono w pracy *„The Robust Measurement Method for Security Metrics Generation"*. W ten sposób poszerzono standardowy model wykonywania pomiarów o metody kontrolowania jakości pomiarów. W efekcie wyznaczane metryki są bardziej niezawodne ponieważ bazują na powtarzalnych pomiarach. Dzięki wprowadzeniu kontroli jakości pomiarów można walidować również środowisko w którym jest wykonywany pomiar. Sprawdzono poprawność zaproponowanego modelu wykonywania pomiarów do obliczenia współczynników wydajnościowych dla wybranych modułów kryptograficznych. Zaimplementowano narzędzie o nazwie CMTool (ang. *Crypto Metrics Tool*) do testowania wydajności prymitywów kryptograficznych oraz ich walidacji. Uzyskane wyniki charakteryzują się dokładnością i wiarygodnością. Metryki bezpieczeństwa zebrane za pomocą CMTool zostały wykorzystane do przeprowadzenia wieloaspektowych analiz ataków DDoS. Środowisko symulacyjne przygotowano z wykorzystaniem języka modelowania QoP-ML. Biorąc powyższe pod uwagę rozwiązano pierwsze z postawionych w pracy zadań. Warto podkreślić że zaproponowanie rozwiązanie, będące poszerzeniem standardu ISO/IEC 27004, może być wdrożone w środowisku Internetu Rzeczy.

W kolejnej pracy pt *„Secure ant Time-Aware Communication of Wireless Sensors Monitoring Overhead Transmission Lines"* autorka dokonała analizy warstwy percepcji IoT w środowisku smart grid. Warstwa ta jest istotna z punktu postrzegania architektury IoT ponieważ dostarcza standardy interfejsów a jednocześnie jest narażona na ataki. W pracy ukazano, że systemy monitorowania sieci energetycznych są jedną z realizacji koncepcji Internetu Rzeczy realizowaną w praktyce. Zaproponowano efektywną i bezpieczną metodę przesyłania danych zebranych przez bezprzewodową sieć sensorową w środowisku sieci energetycznej dla której rozwiązano problem opóźnień czasowych. Przy pomocy języka QoP-ML opracowano model sieci i wykonano jej analizę. Wybrano odpowiednią architekturę WSN z algorytmami trasowania połączeń w ten sposób zdecydowanie podnosząc parametr dostępności takiej sieci. Tym samym rozwiązano drugie z postawionych w pracy zadań.

Z kolei w pracy *„Multilevel Modeling of Distributed Denial of Service Attacks in Wireless Sensor Networks"* autorka rozprawy zaproponowała wieloaspektową analizę ataku DDoS przeprowadzoną w warstwie percepcji Internetu Rzeczy. Na podstawie badań opisanych w pracy określono nowy typ ataku jako opóźniony, rozproszony atak dostępu do usługi (ang. *Delayed Distributed Denial of Service DDDoS*). Ten typ ataku określono jako szczególnie niebezpieczny dla sieci sensorowych ze względu na wrażliwość zasobów energetycznych sieci WSN, a jego działanie można zaobserwować dopiero po pewnym czasie. Atak DDDoS wykryto z wykorzystaniem schematu analizy wieloaspektowej. Zatem można stwierdzić, że trzecie zadanie określone w pracy zostało poprawienie wykonane.

Wieloaspektowa analiza systemu realizującego zapytania do centrum danych na różnym poziomie bezpieczeństwa stała się kanwą publikacji pt *„On Security Management: Improving Energy Efficiency, Decreasing Negative Environmental Impact and Reducing Financial Costs for Data Centers"*. Postawione w pracy doktorskiej zadanie czwarte rozwiązano poprzez opracowanie zrębu systemu wspomagania decyzji zgodnie z koncepcją cyklu PDCA (ang. *plan-do-check-act*) zaproponowanego przez amerykańskiego statystyka Williama Edwardsa Deminga. Opracowany system składa się z pięciu etapów: definicji problemu, utworzenia modelu badanego środowiska, wieloaspektowej analizy bezpieczeństwa testowanego systemu, rekomendacji oraz wdrożenia. Warto zauważyć, że w etapie trzecim czyli w wieloaspektowej analizie zastosowano następujące analizy: czasową operacji wykonywanych w utworzonym modelu, energetyczną, jakości zabezpieczeń, ekonomiczną oraz analizę emisji dwutlenku węgla. Wszystkie wymienione pięć etapów systemu decyzyjnego wdrożono w ramach opracowanego systemu składającego się z serwerów świadczących określone usługi oraz urządzeń końcowych jako odbiorców tych usług.

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 rozprawy polega na zastosowaniu wieloaspektowej analizy złożonych systemów sieciowych pozwalającej na detekcję zagrożeń w architekturach systemów Internetu Rzeczy, które nie są podatne na wykrycie przez znane systemy analizy bezpieczeństwa. W szczególności można przytoczyć tutaj opisany w pracy fakt wykrycia opóźnionego, rozproszonego ataku odmowy usługi (DDDoS). Ponadto do oryginalnych cech rozprawy zaliczam również propozycję modyfikacji standardu ISO/IEC 27004 o fazę weryfikacji podstawowych wyników pomiarów wpływającej bezpośrednio na powtarzalność i wiarygodność wyznaczanych metryk badanego systemu.

Do samodzielnego i oryginalnego dorobku autorki należy zaliczyć wykonanie badań nad zaproponowanym systemem wieloaspektowej analizy oraz usprawnienie obowiązującego schematu detekcji zagrożeń o poszerzoną metodologię pomiaru determinantów bezpieczeństwa systemu o architekturze Internetu Rzeczy. Wyniki przeprowadzonej wieloaspektowej analizy systemu wpływają na określenie dostępności usług świadczonych przez badany system. Ponadto należy odnotować fakt dokonania rzetelnego przeglądu stanu wiedzy z zakresu rozproszonych ataków odmowy dostępu DDoS oraz wykrycie nowej formy ataku DDDoS. Niewątpliwie w/w aspekty pracy pozycjonują tę pracę jako wartościową i wnoszącą pożyteczny wkład w rozwój problematyki zabezpieczeń przed sieciowymi atakami rozproszonymi odmowy dostępu do usługi w systemach o architekturze Internetu Rzeczy. Warto podkreślić przy tym istotny naddatek publikacyjny wymagany przy rozprawach doktorskich. Mamy tutaj do czynienia z czterema publikacjami z listy JCR w których autorka rozprawy Pani mgr Katarzyna Mazur jest wymieniana na pierwszym miejscu wśród autorów artykułów.

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

Autorka w sposób zwięzły, jasny i przekonywujący opisała poszczególne etapy dowodzenia tezy rozprawy w formie wyników przeprowadzonych eksperymentów. Nie uniknęła ona jednak drobnego błędu edycyjnego na str 5 pracy. Tuż przed rodz. 1.3. znajduje się niedokończone zadanie.
Zdanie to można wykreślić ponieważ nie wpływa ono na treść akapitu.

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

Do głównych słabych stron rozprawy zaliczam:

1./ Brak wyraźnie wyartykułowanego przez autorkę mgr Katarzynę Mazur, na stronach Rozprawy Doktorskiej, jej wkładu własnego w zrealizowane oprogramowanie. W szczególności warto byłoby na kartach rozprawy rozstrzygnąć autorstwo narzędzia CMTool służącego do testowania wydajności prymitywów kryptograficznych oraz ich walidacji jak również algorytmów walidacyjnych opisanych w złączniku do artykułu *„The robust measurement method for security metrics generation”*. Recenzent przypuszcza, że skoro autorka rozprawy jest wymieniona na pierwszym miejscu jako autorka artykułu to miała ona największy wpływ na opracowanie w/w narzędzia i algorytmów, nie jest jasne natomiast czy są one jej samodzielnym wkładem w pracę doktorską.

2./ Nie jest określone wprost czy metody kontrolowania jakości pomiarów i ich walidacji są zbiorem otwartym czy też zamkniętym. Innymi słowy czy autorka rozprawy standaryzuje ustalony zbiór zalecanych metryk do walidacji danych pomiarowych ? Czy zaproponowane miary walidacji wyników pomiarowych są wystarczające do stwierdzenia o ich wiarygodności ?

7. Jaka jest przydatność rozprawy dla nauk technicznych?

Praca jest przydatna dla nauk technicznych jako kolejna iteracja procesu ewaluacji bezpieczeństwa w sieciach o architekturze Internetu Rzeczy. Zapisy w pracy stanowią pogłębioną analizę zagadnienia obrony przed rozproszonymi atakami odmowy dostępu do usługi wnosząc istotny praktyczny wkład w wykrywanie tego typu zagrożeń. Opracowanie innowacyjne scenariusze oraz algorytmy można bezpośrednio wykorzystać do obrony systemów teleinformatycznych w tym systemów krytycznych dla bezpieczeństwa państwa.

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

Biorąc pod uwagę powyższe wnioski i uwagi przedłożoną rozprawę mgr Katarzyny Mazur zaliczam jako **wybitnie dobrą zasługującą na wyróżnienie**.

.....
podpis