Politechnika Warszawska
Wydział Elektroniki i Technik Informacyjnych

Warszawa, 27 lutego 2019 r.

D z i e k a n a t

Uprzejmie informuję, że na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej odbędzie się w dniu 19 marca 2019 r. publiczna obrona rozprawy doktorskiej

Mgr. inż. Alberta Sitka

temat: „Kontekstowe zarządzanie bezpieczeństwem elektronicznych systemów płatniczych".

promotor – prof. dr hab. inż. Zbigniew Kotulski Wydział Elektroniki i Technik Informacyjnych Politechniki Warszawskiej

recenzenci:
dr hab. inż. Jerzy Konorski, prof. Politechniki Gdańskiej Wydziału Elektroniki, Telekomunikacji i Informatyki
dr hab. inż. Jerzy Pejaś Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Obrona odbędzie się w dniu 19 marca 2019 r. w sali 116 na Wydziale Elektroniki i Technik Informacyjnych – Gmach im. Janusza Groszkowskiego, Warszawa, ul. Nowowiejska 15/19; początek godz. 9.00

Po adresem: **www.elka.pw.edu.pl/Wydzial/Rada-Wydzialu/Harmonogram-obron-doktorskich-streszczenia-i-recenzje** zapewniony jest na stronie Wydziału dostęp do tekstów streszczenia rozprawy i recenzji, jak również do tekstu rozprawy umieszczonej w Bazie Wiedzy Politechniki Warszawskiej.

Dziekan

prof. dr hab. inż. Krzysztof Zaremba

Autor: mgr inż. Albert Sitek
Temat: Kontekstowe zarządzanie bezpieczeństwem elektronicznych systemów płatniczych
Promotor: prof. dr hab. inż. Zbigniew Kotulski

Streszczenie

Płatności elektroniczne wykorzystujące nowoczesne karty płatnicze zyskują ogromną popularność, głównie dzięki swojej prostocie, szybkości przetwarzania transakcji, bezpieczeństwu i szerokiej dostępności tej formy płatności. Codziennie na świecie przetwarzane są miliony transakcji. Przy tak dużej skali, każdy ułamek sekundy, potrzebny na przetworzenie transakcji, staje się bardzo istotny. Nic dziwnego, że agenci rozliczeniowi prześcigają się w optymalizacji procesu akceptacji kart. Niestety reguły przetwarzania transakcji są stałe (np. weryfikacja kodem PIN dla transakcji na kwotę powyżej 50 PLN w Polsce), niezależnie od historii transakcji posiadacza karty i całego kontekstu transakcyjnego.

Celem rozprawy jest wykazanie, że możliwe jest dynamiczne i kontekstowe sterowanie przebiegiem transakcji elektronicznej w celu zmniejszenia średniego czasu przetwarzania transakcji, przy zachowaniu akceptowalnego poziomu ryzyka.

Praca zawiera szczegółową analizę przebiegu transakcji płatniczych przeprowadzanych z wykorzystaniem stykowych i zbliżeniowych kart płatniczych. Zaprezentowano mechanizmy zabezpieczeń stosowane przy transakcjach elektronicznych oraz przedstawiono znane z literatury ataki na karty płatnicze.

W ramach rozprawy zaprojektowano kontekstowy system do zarządzania ryzykiem (Contextual Risk Management System, CRMS) dedykowany dla dużych sieci sprzedaży detalicznej, którego celem jest dynamiczne podejmowanie decyzji o sposobie weryfikacji posiadacza karty podczas transakcji. Do swojego działania wykorzystuje on m.in. autorski system reputacyjny określający reputację posiadacza karty na podstawie przebiegu jego historycznych transakcji. W celu przeprowadzenia weryfikacji zaproponowanego rozwiązania, zaprojektowano mechanizm służący do zbierania szczegółowych informacji o przebiegu transakcji płatniczych bezpośrednio z terminala. Mechanizm ten posłużył następnie do zebrania produkcyjnych danych transakcji z 68 terminali płatniczych należących do jednej z sieci sprzedaży detalicznej w Polsce. Tak zebrane dane poddano szczegółowej analizie oraz wykorzystano do przeprowadzenia symulacji działania pełnego rozwiązania.

Wyniki badań potwierdzają osiągnięcie celu rozprawy, prezentują zależności pomiędzy akceptowalnym stopniem ryzyka a potencjalnymi korzyściami i stratami - dla zebranej próbki danych produkcyjnych.

W ramach rozprawy przeprowadzono również analizę możliwości produkcyjnego wdrożenia systemu CRMS oraz jego wykorzystania jako elementu programu lojalnościowego wykorzystującego karty płatnicze (and. Card-Linked Loyalty), określając przy tym potencjalne korzyści płynące z takiego wdrożenia.

Gdańsk, 8.02.2019

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

KWESTIONARIUSZ-RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY WYDZIAŁU ELEKTRONIKI I TECHNIK INFORMACYJNYCH POLITECHNIKI WARSZAWSKIEJ

Tytuł rozprawy: ***Kontekstowe zarządzanie bezpieczeństwem elektronicznych systemów płatniczych***

Autor rozprawy: **mgr inż. Albert Sitek**

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 recenzowanej rozprawie doktorskiej przedstawiono próbę usprawnienia elektronicznych systemów płatniczych opartych na kartach stykowych i zbliżeniowych. Doktorant zauważa, że średni czas przetwarzania transakcji można zmniejszyć poprzez okazjonalną rezygnację z weryfikacji kodu PIN, uzasadnioną przebiegiem poprzednich transakcji na danej karcie. Istotne informacje wyekstrahowane z historii transakcji, zakodowane w postaci bieżącego poziomu reputacji karty, stanowią zmienną wejściową odpowiedniej reguły decyzyjnej. Przedmiotem projektowania jest tu zarówno konstrukcja samego systemu reputacyjnego, jak i reguły decyzyjnej zapewniającej pożądany charakter wymienności pomiędzy częstością rezygnacji z weryfikacji kodu PIN a ryzykiem oszustwa w przypadku realizacji transakcji fałszywą bądź kradzioną kartą. W efekcie proponuje się rozbudowę architektury systemu płatniczego o komponent nazwany *Contextual Risk Management System* (CRMS). Doktorant stawia tezę, że kontekstowe zarządzanie przebiegiem transakcji (w istocie: uwzględnianie bieżącego poziomu reputacji karty przez komponent CRMS) daje wymierny zysk czasu przetwarzania transakcji przy akceptowalnym ryzyku oszustwa. Z rozważań wstępnych można ponadto wywnioskować, że idzie przede wszystkim o usprawnienia pozwalające w szerokim zakresie regulować zakres zysku i ryzyka, tj. pozostawiające w ręku operatora systemu zestaw konfigurowalnych parametrów wpływających na proces decyzyjny. Jest to zamierzenie ambitne, gdyż współczesne systemy płatnicze obwarowane są szeregiem bardzo ścisłych wymagań oraz specyfikacji technicznych i organizacyjnych, które zawężają zakres możliwych do zrealizowania idei rozwiązań. Powyższe sformułowanie tezy jest jasne i poprawnie, jed-

nocześnie zapowiadając kierunek i metodologię badań: niezbędne są prace teoretyczne, których celem jest optymalny dobór zasad tworzenia i wykorzystywania reputacji karty, jak również eksperymenty weryfikujące te zasady na dużych zbiorach danych zebranych z rzeczywistych systemów płatniczych. Taki też, teoretyczno-eksperymentalny charakter ma rozprawa.

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?

Analizując techniczne możliwości realizacji swojej koncepcji systemu reputacyjnego Doktorant zapoznał się z obszerną literaturą i posiadł dogłębną wiedzę na temat bezpieczeństwa informacji, szczególnie w odniesieniu do elektronicznych systemów płatniczych. Bibliografia rozprawy zawiera 127 pozycji, wśród których można znaleźć m. in. publikacje akademickie dotyczące protokołów kryptograficznych, mechanizmów budowy reputacji i zaufania, czy mechanizmów ochrony informacji w systemach informatycznych, jak też opisy ich wdrożeń w systemach rozproszonych, sieciach komputerowych i aplikacjach internetowych, a także dużą liczbę opracowań standaryzacyjnych i dokumentów specyfikacyjnych organizacji płatniczych, wreszcie raporty bankowe, analizy biznesowe i materiały dotyczące metod zarządzania ryzykiem i analizy danych przy pomocy różnych narzędzi informatycznych. Być może bibliografię warto uzupełnić o nurt teoriogrowy przeciwdziałania przestępstwom przeciwko systemom płatniczym (por. np. Peng Liu, Lunquan Li, *A game theoretic approach for attack prediction*), lecz i tak jest ona wystarczająco bogata. W rozdziałach 2-4 rozprawy Doktorant dokonuje wyczerpującego (z punktu widzenia potrzeb swych badań) przeglądu architektur, sprzętu i procedur stosowanych przy płatnościach elektronicznych, zwracając głównie uwagę na płatności stykowe i zbliżeniowe, w następnej kolejności zaś omawia skrótowo niektóre znane rodzaje ataków na systemy płatności kartą oraz twarde i miękkie zabezpieczenia przed nimi, w tym bezpieczeństwo kontekstowe i systemy reputacyjne. Cennym uzupełnieniem są wydruki przykładowych struktur danych i przebiegów procedur. Ta część rozprawy sprawia bardzo dobre wrażenie i jest interesującą lekturą także dla niespecjalisty; stanowi ona zarazem solidną podbudowę dla części oryginalnej i umożliwia Autorowi przekonującą argumentację na rzecz: umiejscowienia proponowanego rozwiązania w architekturze systemu zobrazowanej na rysunku 2.1, niezbędnych – a jednocześnie możliwych do zrealizowania – modyfikacji przebiegu wymiany informacji w systemie oraz zastosowanych metod oceny. Autor prezentuje się tutaj jako osoba wysoce kompetentna w podjętej tematyce oraz świadoma potrzeby i możliwości jej twórczego rozwijania. (Drobna uwaga redakcyjna: doceniając zalety jednolitego stosowania terminów anglojęzycznych może jednak na potrzeby polskiego tekstu warto przetłumaczyć nazwy głównych aktorów systemu płatniczego, np. Posiadacz karty, Sprzedawca, Agent rozliczeniowy, Wydawca karty – odmiana przez przypadki słów takich jak *Merchant*, *Acquirer* czy *Issuer* jest trudna do zaakceptowania.)

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

Do opracowania autorskiego komponentu systemowego CRMS Doktorant podszedł systematycznie, rozpoczynając od przyjęcia rozsądnych założeń projektowych wynikających z analizy działania systemów płatniczych: komponent został posadowiony po stronie Sprzedawcy (*Merchant*), ingerencja w standardowy proces decyzyjny sprowadzona została do weryfikacji bądź rezygnacji z weryfikacji kodu PIN, zaś kontekst budujący reputację karty objął dane karty oraz kwotę i przebieg transakcji sformalizowany zgodnie z diagramem 6.1. Wszystkie te założenia są poprawnie i jasno uzasadnione. Następnym etapem było sformułowanie modelu matematycznego i wreszcie weryfikacja rozwiązania z użyciem zbioru rzeczywistych danych zebranych z systemu płatniczego w wybranych placówkach handlowych. Ta ostatnia czynność wymagała działań o charakterze organizacyjnym i informatycznym, związanych z implementacją bezpiecznego przesyłania raportów o dokonanych transakcjach z terminali płatniczych za pośrednictwem dedykowanych serwerów. Rezultatem było wyprodukowanie zbioru danych produkcyjnych, który sam w sobie stanowi znaczną wartość rozprawy, do wykorzystania w wielu pożytecznych badaniach statystycznych i marketingowych. W zgodzie z obowiązującym rozporządzeniem o ochronie danych osobowych (RODO) Doktorant zadbał o właściwą pseudonimizację danych z użyciem silnej funkcji skrótu i dystrybucji tajnego klucza. Opisana metodologia jest właściwa dla ewaluacji wielu proponowanych w literaturze mechanizmów budowy reputacji, gdzie zapis rzeczywistych decyzji systemu informatycznego porównuje się z tym, jaki powstałby przy wykorzystaniu danego mechanizmu budowy reputacji. Zadanie Doktoranta było tu nieco ułatwione dzięki "lokalnej" naturze reguły decyzyjnej – obecność CRMS nie ma bowiem wpływu na przebieg transakcji kartą i nie wprowadza zależności z transakcjami innymi kartami. Okoliczność ta umożliwia analizę zbioru danych *offline*, a wynika z końcowego etapu projektowania przedstawionego w rozdziale 10, gdzie Doktorant analizuje możliwości praktycznej implementacji swego rozwiązania i dochodzi do wniosku, że rezygnacja z weryfikacji kodu PIN odbywa się poprzez proste nadpisanie przez CRMS decyzji karty uzyskanej w ramach standardowej wymiany informacji z terminalem płatniczym zgodnie z diagramem 6.1.

Kluczową ilustracją osiągniętych rezultatów są rysunki 9.6-9.8, gdzie w skali całej badanej sieci placówek handlowych pokazuje się zależności zysku czasowego i możliwych strat finansowych od przyjętego poziomu ryzyka nieuczciwej transakcji. Widoczna (z zastrzeżeniami, o których poniżej) obecność zysku czasowego i redukcja możliwych strat, wyliczona szkicowo w rozprawie, świadczy o tym, że Doktorant poprawnie udowodnił postawioną tezę. W rozdziale 11 prezentowane są dodatkowo analogiczne wyliczenia przy założeniu, że proponowane rozwiązanie CRMS jest elementem hipotetycznego programu lojalnościowego. Tu także efekty jego ewentualnego wdrożenia okazują się pozytywne, co widać na rysunkach 11.2 i 11.3.

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?

W rozdziałach 1.2 i 12.1 Doktorant podsumowuje oryginalny dorobek rozprawy. W opinii recenzenta na plan pierwszy wysuwają się:

- zgromadzenie i analiza dużego zbioru danych produkcyjnych,

- propozycja systemu reputacyjnego i reguły decyzyjnej z progowym poziomem ryzyka dla określania potrzeby weryfikacji kodu PIN,
- integracja proponowanych rozwiązań w postaci komponentu CRMS i jego weryfikacja z użyciem zgromadzonych danych produkcyjnych.

Jak wspomniano, metodologia i realizacja gromadzenia zbioru danych produkcyjnych stanowią znaczące osiągnięcie praktyczne. Natomiast główny dorobek teoretyczny mieści się w obszarze analiz wymienności kosztów zabezpieczeń i ryzyka ich naruszenia; jest to opracowanie sposobu oceny przeszłych transakcji, naliczania na tej podstawie reputacji karty oraz wyznaczania ryzyka i związanej z nim progowej reguły decyzyjnej. Wszystkie te propozycje mają charakter heurystyczny, a najcenniejsza poznawczo wydaje się być pierwsza z nich – adekwatna ocena przebiegu transakcji z punktu widzenia ryzyka, jakie niesie, wynika bowiem z unikalnej wiedzy Autora w zakresie bezpieczeństwa systemów płatniczych. Sam system reputacyjny nie wykracza poza stan sztuki, oparty jest na ważonej sumie ocen z zanikającymi wagami i jedynym problemem badawczym pozostaje eksperymentalny dobór optymalnych wag. Interesujący aspekt systemu polega na tym, że badany osobnik (karta) sam przechowuje swoją niepodrabialną reputację, którą przedkłada w kolejnych interakcjach (transakcjach), podobnie jak w modelach zaczerpniętych z biologii teoretycznej (por. np. H. Ohtsuki, Y. Iwasa, *The leading eight: Social norms that can maintain cooperation by indirect reciprocity*). Zgodnie z podaną w rozdziale 4.3 klasyfikacją system reputacyjny określa się jako arytmetyczny. Jest to naturalnie klasyfikacja bardzo niepełna, z czego Autor na pewno zdaje sobie sprawę, gdyż zamieszcza w bibliografii aż 12 pozycji przeglądowych dotyczących systemów reputacyjnych. Proponowany system można by np. dodatkowo określić jako holistyczny i ograniczony do ocen bezpośrednich (bez rekomendacji). Podobnie rzecz wygląda, jeśli idzie o relacje do stanu wiedzy, w przypadku klasycznego wyznaczania ryzyka według wzoru (8.4), arbitralnie uzupełnionego o czynnik w przybliżeniu odwrotny do bieżącej reputacji karty. Arbitralność tego przepisu nie musi jednak być wadą, skoro przynosi pozytywne skutki opisane w rozdziale 9. Ogólnie, za dorobek teoretyczny rozprawy można uznać skuteczne zastosowanie stanu sztuki w zakresie budowy reputacji i zaufania, wzbogacone o specyfikę oceny elektronicznych transakcji płatniczych.

Swe oryginalne wyniki Doktorant od kilku lat publikuje na szerszych forach. W Bazie Wiedzy Politechniki Warszawskiej znajduje się jego 7 publikacji, w tym 5 artykułów w czasopismach z listy B MNiSzW (jeden z nich to publikacja samodzielna) oraz 2 referaty konferencyjne w materiałach wydawnictwa Springer. Publikacja ważniejszych wyników rozprawy może w najbliższym czasie powiększyć ten dorobek.

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

Rozprawa jest zredagowana bardzo starannie pod względem językowym, układu treści i jasności wywodu. Podział na 12 stosunkowo krótkich rozdziałów ułatwia lekturę i pozwala czytelnie wypunktować i rozgraniczyć omawiane zagadnienia. Duże partie tekstu czyta się z przyjemnością i zaciekawieniem. Na tym korzystnym tle wyróżniają się zwłaszcza: rozdział 2 (w którym Autor objaśnia zasady przeprowadzania i zabezpieczania elektronicznych transakcji płatniczych), rozdział 5 (w którym Autor logicznie uzasadnia wy-

magania, jakie stawia swemu rozwiązaniu i opisuje kroki prowadzące do jego realizacji), oraz rozdział 10 (w którym Autor analizuje praktyczne możliwości realizacji rozwiązania przy minimalizacji koniecznych zmian w istniejących systemach). Najwięcej elementów analitycznych zawierają rozdziały 6-9, które budzą kilka niżej omawianych zastrzeżeń co do czytelności wywodu i osiągniętych wyników. Pogarszają one w pewnym stopniu ogólnie pozytywną ocenę prezentacyjnej strony rozprawy. Nie podważają naturalnie merytorycznego dorobku Doktoranta.

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

Zapowiadane uwagi i zastrzeżenia w stosunku do rozdziałów 6-9 są następujące:

- str. 57: znaczenia skrótów zdarzeń w trakcie transakcji można się domyślić (nie ma ich w wykazie na str. 125), jednak lepiej byłoby je jawnie podać, najlepiej na diagramie 6.1; na diagramie tym w niektórych blokach występują literówki, brak natomiast czytelnego odniesienia to tabeli 6.1,
- str. 59: w kluczowym wzorze (6.1) zabrakło wyjaśnienia, czym jest $\bar{R}_{n-i}$ (czytelniej byłoby podać odpowiedni wzór na sumę ważoną z użyciem wag (6.2); wydaje się ponadto, że w oznaczeniu tym nie powinien występować bieżący indeks *i*,
- str. 59: skoro Autor uznał dobór wag zgodny ze wzorem (6.2) za optymalny w świetle wykonanych eksperymentów, to należałoby to uzasadnić wynikami uzyskanymi przy innych określeniach wag i jawnie sformułować kryterium doboru wag; brak takiej analizy porównawczej nasuwa obawy, że wyniki mogłyby znacząco różnić się dla różnych zbiorów danych produkcyjnych,
- str. 59: we wzorze (6.2) występuje komplementarna funkcja błędu posiadająca dwa parametry – czy wobec tego występujący we wzorze (6.1) parametr *N* (długość pamięci przeszłych transakcji) nie jest nadmiarowy?
- str. 76: dla czytelniejszej prezentacji należałoby jawnie podać sposób obliczania zysku czasowego (suma czasów transakcji, dla których CRMS zrezygnował z weryfikacji kodu PIN?)
- str. 76: nie została jasno przedstawiona ocena osiągniętego zysku czasowego – co oznacza przykładowe 200 godzin? przy ponad 1000000 transakcji oznacza to średnio ułamek sekundy na transakcję? z kolei z punktu widzenia placówki handlowej nie wiadomo, czy zysk kilkunastu godzin w przekroju 6 miesięcy implikuje zwiększenie obrotów – tak byłoby w warunkach nasycenia, lecz bez analizy kolejkowej chyba trudno to przesądzać,
- str. 77: na osi poziomej rysunku 7.10 powinien chyba być limit CVL,
- str. 81: co oznacza "powstanie wymiernych oszczędności [czasów transakcji], które finalnie przekładają się na pieniądze" – jaki jest model tego przełożenia?
- str. 85: wzór (8.1) określa "maksymalną, teoretyczną stratę per każda transakcja" – jak to rozumieć i czy nie chodzi tutaj o *średnią* stratę?
- str. 86: po co we wzorze (8.2) potrzebne są parametry *a* i *b*, skoro istotny jest jedynie ich iloraz? w dodatku kilka wierszy wyżej symbol *a* miał zupełnie inne znaczenie,
- str. 86: prawdopodobieństwo oszukańczej transakcji określane jest statycznie na podstawie dużego zbioru badanych transakcji (rozdział 8.3.3), zatem we wzorze (8.2) pełni jedynie rolę czynnika skalującego i z powodzeniem mogłoby być włączone do funkcji $f(R)$ wyrażonej wzorem (8.3); wydaje się przy tym nieintuicyjne, że prawdopodobieństwo to nie zależy od bieżącej wartości reputacji,

- str. 88: przyjęcie "dodatkowego współczynnika bezpieczeństwa" w wysokości 100 jest zupełnie arbitralne; jak to wpływa na wyniki w rozdziale 9?
- str. 90: jak wynika z rysunku 9.1, ocena nawet prawidłowo przebiegającej transakcji bez weryfikacji kodu PIN jest niska i powoduje spadek reputacji, co uzasadniono na str. 64; warto tu naszkicować idealny przebieg wartości reputacji – pozwoliłoby to lepiej ocenić wyniki testów 1-4 w rozdziale 6.2.2 i właściwie zrozumieć rysunek 9.6; zasadne jest też pytanie, czy proponowany system reputacyjny jest odporny na strategiczne zachowania posiadacza karty, np. ataki *on-off*,
- str. 92/93: kluczowy rysunek 9.6 pokazuje wykres zysków czasowych w funkcji przyjętego ryzyka, który narasta wolniej niż liniowo, co nie jest dokładnie objaśnione (prawdopodobnie spadek częstości przekraczania progu reguły decyzyjnej (8.5) jest częściowo kompensowany spadkiem średniej reputacji karty, por. poprzednia uwaga); wyraźnie brakuje refleksji nad znacznie ambitniejszym problemem badawczym – możliwościami "uliniowienia" wykresu, np. poprzez wzbogacenie kontekstu i zastąpienie bądź uzupełnienie systemu reputacyjnego przez mechanizm wykrywania anormalnych transakcji, w którym, w idealnym przypadku, seria rezygnacji z weryfikacji kodu PIN prawowitego posiadacza karty nie zmniejsza istotnie szans na kolejną rezygnację,
- str. 94: poważną słabością wyników przedstawionych na rysunkach 9.7 i 9.8 jest brak przepisu wyznaczania wartości na osiach pionowych; w szczególności nie jest jasne, o jakie koszty chodzi na rysunku 9.8,
- str. 95: jak rozumieć wniosek, że "wykorzystany system reputacyjny skutecznie redukuje potencjalne straty wynikające z wykorzystania systemu CRMS"?

7. Jaka jest przydatność rozprawy dla nauk technicznych?

Zaproponowana koncepcja komponentu CRMS, niezależnie od jego dalszych losów i wyżej wyrażonych zastrzeżeń, oraz opracowanie metodologii i realizacja gromadzenia zbiorów danych produkcyjnych o transakcjach płatniczych, wzbogacają stan sztuki w dziedzinie bezpieczeństwa rozproszonych systemów płatniczych o innowacyjne mechanizmy "miękkie" i dostarczają interesujących sposobów ich weryfikacji. Agregacja kontekstu transakcji do wartości reputacji, a także konstrukcja odpowiedniej reguły decyzyjnej są oryginalne i mogą być pomocne w środowiskach, gdzie weryfikacja uprawnień dostępu do zasobów jest kosztowna (np. wymaga uruchomienia procedur typu *Deep Packet Inspection* w sieci komputerowej) i może być z niewielkim ryzykiem pomijana.

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 nadmiarem
e/ wybitnie dobra, zasługująca na wyróżnienie

Wobec powyższego wnioskuję o dopuszczenie Doktoranta do dalszych etapów przewodu doktorskiego.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie
Katedra Inżynierii Oprogramowania
Wydział Informatyki

Szczecin, dn. 15 stycznia 2019 r.

dr hab. inż. Jerzy Pejaś
Katedra Inżynierii Oprogramowania
Wydział Informatyki
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

KWESTIONARIUSZ- RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY WYDZIAŁU ELEKTRONIKI I TECHNIK INFORMACYJNYCH POLITECHNIKI WARSZAWSKIEJ

Tytuł rozprawy: Kontekstowe zarządzanie bezpieczeństwem elektronicznych systemów płatniczych

Autor rozprawy: mgr inż. Albert Sitek

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)?**

   Recenzowana rozprawa doktorska jest mocno powiązana z problemami realizacji bezpiecznych transakcji elektronicznych z wykorzystaniem kart płatniczych. Nie dotyczy jednak zabezpieczeń na poziomie algorytmów i protokołów kryptograficznych ani też ataków kryptoanalitycznych na tego typu zabezpieczenia. Przy założeniu, że wymienione zabezpieczenia (tzw. zabezpieczenia twarde) są poprawnie dobrane i dobrze zaimplementowane autor skupia się w pracy na bezpieczeństwie kontekstowym transakcji realizowanych w systemach płatniczych. protokołów systemach płatniczych. O ile zabezpieczenia twarde cechuje niezmienność (statyczność) w dłuższym okresie, to zabezpieczenia kontekstowe mogą zmieniać się dynamicznie w czasie korzystania z usługi i adaptować się, na przykład, do oszacowanego poziomu ryzyka transakcji.

   W przypadku transakcji elektronicznych zabezpieczenia kontekstowe mogą mieć różną postać. Na przykład, w systemie płatniczym możliwe jest dostosowanie metody uwierzytelniania użytkownika karty płatniczej do poziomu ryzyka realizacji transakcji, na który istotny wpływ może mieć reputacja użytkownika. Możliwe jest także zrezygnowanie z uwierzytelniania wtedy, gdy nie spowoduje to podniesienia ryzyka transakcji powyżej wartości akceptowalnej i jej ponowne wymuszanie, gdy ryzyko

wzrośnie powyżej tej wartości. Realizacja zabezpieczeń kontekstowych wymaga „zanurzenia" ich w systemie kontekstowym, tj. takim, który w zależności od reputacji użytkownika dostarcza mu właściwej usługi oraz w czasie rzeczywistym dobiera odpowiednie zabezpieczenia do jej ochrony.

Wprowadzenie zabezpieczeń w systemach płatniczych ma wpływ m.in. na koszty ich realizacji i obsługi, na czas obsługi pojedynczej transakcji oraz obniżenie komfortu obsługi użytkownika. Stąd zastosowanie zabezpieczeń kontekstowych może mieć pozytywny wpływ na wymienione czynniki, o ile nie spowoduje to obniżenia poziomu bezpieczeństwa systemu płatniczego.

Na potrzeby pracy Dyplomant sformułował następującą tezę:

Możliwe jest dynamiczne i kontekstowe zarządzanie przebiegiem transakcji elektronicznych (stykowych i zbliżeniowych) pozwalające na redukcję średniego czasu przetwarzania transakcji przy zachowaniu akceptowalnego poziomu ryzyka.

Sformułowanie tezy zostało poprzedzone krótką dyskusją (rozdz. 1.1). Stąd można ją uznać za dostatecznie jasną, chociaż pewne wątpliwości budzi brak precyzyjnie zdefiniowanego pojęcia „średni czas przetwarzania transakcji". Nie wiadomo bowiem, czy chodzi o średni czas przetwarzania wszystkich transakcji w 18 sklepach, w jednym sklepie, w jednym terminalu, czy też transakcji jednego klienta. Zastrzeżenie to wydaje się o tyle zasadne, że autor w dalszej części nie posługuje ilościową oceną średniego czasu transakcji, ale skumulowanymi ocenami zredukowanego czasu obsługi transakcji dla pojedynczego klienta (np. str. 91) lub wszystkich transakcji (str. 93). Ponadto transakcje pojedynczego użytkownika wykonywane są sekwencyjnie, podczas gdy transakcje w sklepach i w ramach sklepu są zrównoleglone. Do uwagi tej odnoszę się także w pkt. 5 oraz 6 (c).

Rozprawa doktorska ma charakter doświadczalny i należy do obszaru stosowanych badań naukowych. Eksperymenty doświadczalne autor realizował w trybie offline na podstawie wcześniej zgromadzonych historycznych danych o transakcjach płatniczych. Z jednej strony jest to zaleta pracy (natychmiastowe potwierdzenie zaproponowanych idei i rozwiązań), z drugiej strony jest to wada, ponieważ zmusza do postawienia pytania na ile uzyskane wyniki są uniwersalne i można je odnieść do przypadku innych sieci sklepów oraz grup klientów.

Niezależnie od powyższych uwag problemy badawcze w zakresie kontekstowego zarządzania bezpieczeństwem mają duże znaczenie praktyczne i leżą w obszarze zainteresowań jednej z 10 najważniejszych perspektywicznych technologii informatycznych wskazanych w roku 2018 przez firmę Gartner[1].

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?

Recenzowana rozprawa składa się z dwunastu rozdziałów (w tym podsumowanie pracy), streszczenia (w języku angielskim i polskim), bibliografii obejmującej 128 pozycji

[1] Jest to technologia ciągłej adaptacyjnej oceny ryzyka i zaufania wymieniona w raporcie *Gartner Top 10 Strategic Technology Trends for 2018*, https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/

literaturowych, wykazu skrótów oraz spisu rysunków i tabel. Całość pracy obejmuje 131 stron. Wyniki własne autora przedstawione są w rozdziałach 5-12.

Analizowane przez autora źródła literaturowe można podzielić na trzy obszary wiedzy. Pierwszy z obszarów (przedstawiony w rozdz. 2) dotyczy omówienia specyfikacji technicznych protokołów wymiany informacji w transakcjach elektronicznych, terminali płatniczych oraz stykowych i bezstykowych kart EMV. Szczególną uwagę autor zwracał na protokoły uwierzytelniania posiadacza karty i terminala oraz możliwość definiowania limitów transakcji. Analizował także możliwości karty w zakresie podejmowania decyzji o obniżeniu lub podwyższeniu restrykcji nałożonych na transakcję. Pomimo dużego znaczenia przytaczanych informacji w dalszej części pracy autor nie podsumował ich i jednoznacznie nie wskazał ich związku oraz przydatności w udowodnieniu tezy pracy.

W drugim z obszarów wiedzy (rozdz. 3) omówione zostały podstawowe ataki na karty płatnicze. Ich znaczenie dla pracy jest czysto informacyjne. Autor nie wskazał, że zaproponowany w pracy system kontekstowego zarządzania chroni posiadacza karty przed omówionymi atakami. Oznacza to, że ten obszar wiedzy mógł być pominięty w pracy.

Najistotniejszym z punktu widzenia celu rozprawy jest analiza literatury z trzeciego obszaru dotyczącego bezpieczeństwa kontekstowego i systemów reputacyjnych (rozdz. 4). Analiza ta, chociaż krótka, odnosi się do reprezentatywnych idei i rozwiązań przedstawionych i opracowanych na przestrzeni ostatnich dwudziestu lat. W podsumowaniu analizy autor stwierdza, że bezpieczeństwo kontekstowe w zaproponowanym w pracy systemie CRMS zostanie oparte na kontekstowym uwierzytelnianiu posiadacza karty zależnym od jego reputacji.

Wadą przedstawianych opisów i analiz jest brak uzasadniania dokonywanych wyborów. Dobrym przykładem takiego braku jest podjęcie decyzji o oparciu kontekstowego uwierzytelniania na reputacji posiadacza karty.

Po pierwsze, nie wiadomo jak ma być uzależniane uwierzytelnianie od reputacji. Można jedynie domyślać się, że im wyższa reputacja posiadacza karty, to tym mniej restrykcyjne (rozbudowane) powinny być protokoły uwierzytelniania. Autor nie wskazuje jednak rozważanego zbioru protokołów.

Po drugie, nie wiadomo jak będzie obliczana reputacja posiadacza karty. W rozdz. 6.1.3 autor przyjmuje, że sposób obliczania reputacji można zaliczyć do tych, które są stosowne w arytmetycznych systemach reputacyjnych. Dlaczego jednak autor nie zastosował sposobów stosowanych w innych systemach reputacyjnych wymienionych w rozdz. 4.3?

Po trzecie, dlaczego kontekstowe uwierzytelnianie uzależniono tylko od reputacji posiadacza karty, a nie od innych czynników, np. reputacji sprzedawcy, czy też oceny bezpieczeństwa termnala?

Przywoływana w rozprawie literatura oraz omawiane na jej podstawie zagadnienia są dość rozległe i świadczą o dobrej, pogłębionej wiedzy autora. Konkluzja ta dotyczy zwłaszcza praktycznej wiedzy dotyczącej systemów płatności elektronicznych oraz wspierających ich specyfikacji technicznych. W pracy brakuje jednak informacji o systemach podobnych lub zbliżonych do systemu zaproponowanego w pracy.

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

W mojej ocenie, postawiony w pracy problem zaprojektowania kontekstowego zarządzania bezpieczeństwem elektronicznych systemów płatniczych został rozwiązany. Z dużym prawdopodobieństwem należy także uznać, że sformułowana teza pracy została uzasadniona.

Sformułowany problem ma bardzo silny praktyczny charakter i jego rozwiązanie polega na zaproponowaniu takiego przebiegu transakcji elektronicznej realizowanej przez posiadacza karty, aby przy zachowaniu akceptowalnego poziomu ryzyka zredukować średni czas realizacji transakcji. Rozwiązanie problemu jest mocno uzależnione od ograniczeń wynikających z rzeczywistego funkcjonowania i możliwości poszczególnych elementów systemu płatniczego, np. terminala, karty płatniczej. Ograniczenia te autor zredukował do trzech najistotniejszych:

- dostępny jest przynajmniej jeden czynnik, którego dynamiczna zmiana powinna wpływać na czas przetwarzania transakcji (w pracy rozważany był jeden czynnik: wysokość limitu transakcji bez konieczności uwierzytelniania posiadacza karty);
- doboru informacji kontekstowych, w tym przede wszystkim reputacji posiadacza karty;
- możliwość kontrolowania poziomu ryzyka transakcji.

Teoretycznie, najlepsze rozwiązanie postawionego problemu leży pomiędzy dwoma skrajnymi, oczywistymi rozwiązaniami:

- uwierzytelnianie posiadacza karty jest przeprowadzane podczas każdej transakcji; stąd średni czas transakcji jest maksymalny przy jednoczesnym minimalnym poziomie ryzyka transakcji;
- uwierzytelnianie posiadacza karty nie jest przeprowadzane podczas żadnej transakcji; średni czas transakcji jest minimalny przy jednoczesnym maksymalnym poziomie ryzyka transakcji.

Pośredniego rozwiązania problemu autor poszukiwał eksperymentalnie. Bardziej poprawne metodycznie byłoby podjęcie próby sformalizowania problemu zaprojektowania kontekstowego zarządzania bezpieczeństwem elektronicznych systemów płatniczych jako problemu optymalizacji zadania decyzyjnego z ograniczeniami. W przypadku optymalizacji jednokryterialnej minimalizowany byłby średni czas transakcji przy ograniczeniach nakładanych na akceptowalny poziom ryzyka oraz poziom transakcji bez uwierzytelniania posiadacza karty.

Pomijając możliwe problemy w sformalizowaniu zadania decyzyjnego zaletą takiego podejścia byłby uniwersalizm uzyskanego rozwiązania. W przypadku podejścia przyjętego przez autora, tj. zaproponowanie rozwiązania i jego symulacyjne weryfikowanie, może zawsze rodzić pytania, czy rozwiązanie to działa poprawnie także w warunkach, które nie były przedmiotem symulacji.

Niezależnie od powyższych zastrzeżeń należy stwierdzić, że przyjęta przez autora metoda rozwiązania sformułowanego problemu mieści się w grupie akceptowalnych rozwiązań. W takim jednak przypadku przydałoby się przedstawienie alternatywnych rozwiązań i porównanie ich z przyjętym rozwiązaniem.

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?**

Recenzowana pracę można zaliczyć do intensywnie rozwijanego obecnie nurtu metod zabezpieczeń adaptacyjnych polegających na analizowaniu zachowań i zdarzeń występujących w systemie, a następnie dostosowywaniu jego ochrony do przewidywanych zagrożeń. Dzięki takiemu podejściu możliwa jest ciągła ocena ryzyka i automatycznie kontrolowanie jego poziomu poprzez zwiększenie lub obniżenie siły mechanizmów zabezpieczających.

Zaproponowany w pracy system CRMS adaptuje się do bieżącego prawdopodobieństwa sfałszowania transakcji elektronicznej. Zgodnie z zależnością (8.2) można przyjąć, że bieżące prawdopodobieństwo jest równe:

$$p_{curr} = p * f(R)$$

przy czym dla $R = 0$ (minimalna reputacja) wartość funkcji f(0) wynosi $1/p$[2], zaś dla $R = R_{max}$ (maksymalna reputacja) $f(R) = 1$. Poziom reputacji wpływa więc na bieżące prawdopodobieństwo i tym samym pośrednio na bieżące ryzyko sfałszowania transakcji. Jeśli dodać do tego, że ryzyko to zależy także od kwoty bieżącej transakcji, to autor wskazał dwa czynniki ryzyka (wysokość transakcji i poziom reputacji), dla których można określić poziom tzw. ryzyka akceptowalnego i regułę podejmowania decyzji (rów. 8.5). Reguła ta pozwala finalnie na kontrolowanie poziomu zabezpieczeń poprzez zwiększenie lub obniżenie siły mechanizmów uwierzytelniania posiadacza karty.

Za najbardziej oryginalny element rozprawy uważam opracowanie wspomnianej wyżej reguły decyzyjnej opartej na zaproponowanym systemie oceny reputacji uzależnionej od zidentyfikowanych sposobów przeprowadzenia transakcji płatniczej. Finalna postać reguły jest raczej standardowa i nie wyróżnia się niczym na tle innych temu podobnych reguł. Oryginalny jest jednak sposób obliczania bieżącego ryzyka transakcji i adaptacyjne uzależnienie od niego sposobu uwierzytelniania posiadacza karty płatniczej.

Systemy oceny reputacji użytkownika mają szerokie zastosowania (niektóre z nich zostały wspomniane przez autora w rodz. 4.3). W systemach tych reputacja podmiotu zależy od wielu elementów, które wpływają na jej zmiany w czasie. Z tego powodu istotną częścią sposobu obliczania reputacji jest zdefiniowanie elementów wpływających na ocenę reputacji oraz zasady zanikania znaczenia ocen historycznych w czasie. Nie jest to zadanie trywialne, w szczególności w przypadku systemów transakcji płatniczych, z którym jednak autor poradził sobie dobrze, tj. poprawnie zidentyfikował elementy oceny (sposoby realizacji transakcji płatniczych) oraz podał sposób postarzania ocen historycznych. Szkoda jedynie, że autor nie zaproponował innego szacowania reputacji, opartego np. na zbiorach rozmytych[3].

Dodatkowym oryginalnym dorobkiem autora, także na tle aktualnego stanu wiedzy, jest zaproponowane w pracy wykorzystanie systemu CRMS w systemach lojalnościowych bazujących na kartach płatniczych. Lojalność mogłaby być w tym przypadku dodatkowym czynnikiem, który można by wziąć pod uwagę przy obliczaniu reputacji

---

2 W pracy przyjęto, że f(R = 0) = ∞, ale w szczególności wartością nieskończoną może być $1/p$.

3 Portmann, E., et al. *FORA – A fuzzy set based framework for online reputation management*, Fuzzy Sets and Systems, Vol. 269, 15, June 2015, pp. 90-114

użytkownika karty płatniczej. Autor wybrał jednak inny sposób uzasadnienia swojej propozycji, który nie jest w pełni przekonywujący.

Potwierdzeniem wartości i oryginalności wyników uzyskanych przez autora jest m.in. jeden artykuł opublikowany w czasopiśmie *EURASIP Journal on Information Security* (lista JCR), dwa artykuły w *Annales UMCS Informatica* oraz dwa artykuły w materiałach konferencjach wydanych w wydawnictwie Springer. Wszystkie artykuły zostały opublikowane w latach 2014-2018.

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

Autor dobrze porusza się w obszarze badań związanych z bezpieczeństwem kontekstowym oraz systemów reputacyjnych. Posiada dużą wiedzę praktyczną dotyczącą specyfikacji i norm elektronicznych systemów płatniczych, a także umiejętność wykorzystania jej w zaproponowanym systemie CRMS oraz przygotowania i przeprowadzenia licznych eksperymentów symulacyjnych.

Wyniki badań autor przedstawił w formie czytelnych rysunków[4] oraz komentarzy, podkreślających istotę uzyskanych wyników. Jest to o tyle istotne, że dowód poprawności tezy sformułowanej w rozdz. 1.2 jest całkowicie oparty na trzech eksperymentach dotyczących przygotowania i analizy statystycznej danych produkcyjnych, symulacyjnej weryfikacji CRMS w systemie płatniczym oraz możliwości jego wykorzystania w systemach lojalnościowych.

Wadą wyciąganych wniosków z eksperymentów jest brak zgodności z miarą jakości zawartą w tezie a wynikami eksperymentów przedstawianych na rysunkach i komentowanych w tekście pracy. Udowodnienie tezy wymaga pokazania, że zaproponowane rozwiązania pozwolą na zredukowanie średniego czasu przetwarzania transakcji. Podczas prezentowania wyników eksperymentów autor posługuje się sumarycznym zmniejszeniem czasu wykonania transakcji w wyniku zastosowania systemu CRMS). Prawdopodobnie w oparciu o dane zawarte pracy można obliczyć wartość redukcji średniego czasu, ale niestety nie wiadomo jak zostało zdefiniowane pojęcie średniego czasu przetwarzania transakcji.

Rozprawa jest napisana na dobrym poziomie językowym, zdania są zrozumiałe i poprawnie formułowane. Ponieważ cała praca jest napisana w języku polskim, to także w tym języku powinny być opisane także tabele i rysunki.

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

W pracy można wskazać słabsze miejsca i na tej podstawie sformułować pewne uwagi o charakterze dyskusyjnym. Są to:

(a) oceniana praca jest bardzo mocno powiązana z istniejącymi systemami płatności elektronicznych; z jednej strony jest to jej zaleta, ale z drugiej autor często uzasadnia swoje propozycje wynikami uzyskanymi na podstawie analizy danych rzeczywistych lub wykonywanych na ich podstawie symulacji; np. w ten sposób autor zdefiniował równanie (6.2), a następnie dobierał jego parametry; takie podejście można zaakceptować, ale w takim przypadku autor powinien ocenić uniwersalność

[4] Na najważniejszych rysunkach w rozdz. 9 brakuje jednak opisu osi odciętych, w tym jednostek miar

przedkładanych propozycji albo poprzez zastosowanie bardziej formalnego podejścia albo przynajmniej wykonanie eksperymentów dla innych zestawów danych, które nie były używane podczas „uczenia systemu";

(b) opis architektury CRMS (rozdz. 8) jest bardzo ogólny, przez co trudno jest ocenić jakie ryzyka niesie za sobą włączenie tego podsystemu do produkcyjnego systemu płatności elektronicznych; na przykład, gdzie są przechowywane oceny N poprzednich transakcji zrealizowanych za pomocą karty płatniczej? Na karcie płatniczej? W bazie danych systemu CRMS? Jeśli w bazie, to jak są chronione przed modyfikacją?

(c) z punktu widzenia sprzedawcy terminale płatnicze pracują równolegle; imponujący zysk czasu przedstawiony na str. 93 (od 58.5 godz. do 135.5 godz.) uzyskano prawdopodobnie przy założeniu, że wszystkie analizowane transakcje (w 18 sklepach i za pomocą 68 terminali) realizowane są sekwencyjnie; w rzeczywistości zysk ten jest zdecydowanie mniejszy; niejednoznaczna interpretacja uzyskanych wyników jest pochodną braku definicji średniego czasu zmniejszenia transakcji elektronicznych.

Do wad pracy należy zaliczyć także sygnalizowany już wcześniej brak uzasadniana przez autora swoich wyborów. Oprócz podanych już przykładów wada ta dotyczy także rozdz. 11.2, w którym autor nie uzasadnia wyboru maksymalnego poziomu ryzyka o wartości 0,10 zł, podczas gdy w rozdz. 9.2 analizowano poziomy ryzyka od 0,005 zł do 0,02 zł. Wskazanie i uzasadnienie sposobów podejmowania przez autora swoich decyzji z pewnością wpłynęłoby na jeszcze lepszy odbiór i ocenę pracy.

Dodatkowo, w pracy można znaleźć i wytknąć drobne usterki o charakterze błędów edycyjnych lub formalnych. Są to między innymi:

(a) wszystkie rysunki i tabele powinny być opisane w języku polskim;

(b) str. 41, rozdz. 3.2.2: niejasny opis ataku na uwierzytelnienie danych karty (DDA), zwłaszcza w kontekście opisu DDA podanego na stronie 23;

(c) str. 57, rozdz. 6.1.1, punkt 6.: czy chodzi o obciążenie procesora karty płatniczej? Jeśli tak, to jakie obliczenia wykonuje karta na rzecz systemu CRMS?

(d) str. 81, rozdz. 7.2.5: niektóre wnioski są oczywiste, np. jest to, że na rynku dominują karty stykowe i zbliżeniowe, zaś weryfikacja posiadacza karty wydłuża czas transakcji;

(e) str. 88: niepokoi swoboda w przyjmowaniu założeń bez uzasadnienia, np. dlaczego prawdopodobieństwo transakcji przemnożono przez przyjęty współczynnik bezpieczeństwa (?) o wartości 100;

(f) str. 89, wyliczenie czwarte: dla $R = 10$ wartość $f(R) \neq 1$;

(g) str. 92-93: brak opisu odciętych na rys. 9.4 – 9.6; dodatkowo na rys. 9.4 i 95 (oś rzędnych) jest napis *Numer*, powinno być *Number*

7. Jaka jest przydatność rozprawy dla nauk technicznych?

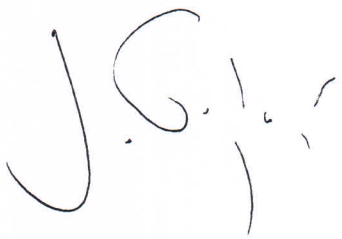
Niewątpliwie wyniki uzyskane w pracy mają duże praktyczne znaczenie i mogą stanowić istotne usprawnienie funkcjonujących na rynku systemów płatniczych. Ich rzeczywistą wartość można będzie w pełni ocenić jednak dopiero po wykonaniu dodatkowych eksperymentów w różnych środowiskach produkcyjnych i ocenie skuteczności działania oraz łatwości dostrojenia systemu CRMS do pracy w tych środowiskach.

Podstawowym wynikiem pracy jest system kontekstowego zarządzania bezpieczeństwem, który należy do obszaru silnie ostatnio rozwijanych technologii ciągłej adaptacyjnej oceny ryzyka i zaufania, wykorzystywanych następnie do automatycznego doboru właściwych mechanizmów zabezpieczających.

8. Do której z następujących kategorii Recenzent zalicza rozprawę?

Przedstawione powyżej uwagi merytoryczne i formalne obniżają moją ocenę pracy jako całości, ale nie podważają praktycznej przydatności zaproponowanych rozwiązań wbudowanych w system CRMS.

Uważam, że autor zrealizował cel rozprawy, przedstawił oryginalne rozwiązanie problemu badawczego w postaci projektowego opracowania systemu CRMS oraz wykazał się umiejętnościami i odpowiednim przygotowaniem do samodzielnej pracy naukowej w dyscyplinie informatyka. Na tej podstawie stwierdzam, że przedstawiona do oceny rozprawa doktorska mgra Alberta Sitka pt. „Kontekstowe zarządzanie bezpieczeństwem elektronicznych systemów płatniczych" **spełnia wymagania stawiane rozprawom doktorskim** w Ustawie *o stopniach naukowych i tytule naukowym* z dnia 14 marca 2003 roku (Dz. U. nr 65/2003, poz. 595 z późn. zmn.) i wnoszę o dopuszczenie jej autora do publicznej obrony.



Żołnierska 49, 71-210 Szczecin-Poland, Tel. (48-91) 449 56 62/55 52, Fax:. (48-91) 449 55 40,
NIP: 852-254-50-56, www.wi.zut.edu.pl