Politechnika Warszawska
Wydział Elektroniki i Technik Informacyjnych

Warszawa, 26 marca 2018 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 10 kwietnia 2018 r. publiczna obrona rozprawy doktorskiej

mgr inż. Mariusza Sepczuka

temat: „Schemat zarządzania uwierzytelnieniem ze zmiennym poziomem bezpieczeństwa i oceną satysfakcji użytkownika”

promotor – prof. dr hab. inż. Zbigniew Kotulski z Politechniki Warszawskiej

recenzenci:
dr hab. inż. Bogdan Księżopolski z Uniwersytetu Marii Curie-Skłodowskiej
dr hab. inż. Grzegorz Kołaczek, prof. Politechniki Wrocławskiej

Obrona odbędzie się w dniu 10 kwietnia 2018 r. w sali 116 na Wydziale Elektroniki i Technik Informacyjnych – Gmach im. Janusza Groszkowskiego, Warszawa, ul. Nowowiejska 15/19; początek godz. 11.00 .

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 pracy: **mgr inż. Mariusz Sepczuk**

promotor pracy: **prof. dr hab. inż. Zbigniew Kotulski**

tytuł (+tytuł angielski): **Schemat zarządzania uwierzytelnieniem ze zmiennym poziomem bezpieczeństwa i oceną satysfakcji użytkownika** (**An authentication management schema with Quality of Protection and Quality of Experience**)

streszczenie

Współczesne zabezpieczenia usług internetowych są bardzo często przewymiarowane, tzn., że zapewniają poziom ochrony wyższy niż jest to faktycznie wymagane, co może skutkować np. wyczerpaniem się zasobów systemu. Inną kwestią jest to, że zastosowane metody zabezpieczeń nie uwzględniają potrzeb konkretnego użytkownika, a te mogą się znacznie różnić. Nasuwa się zatem spostrzeżenie, że fakt ten można wykorzystać przy dobieraniu właściwych mechanizmów bezpieczeństwa. Pierwszą linią obrony usługi przed nieautoryzowanym dostępem są mechanizmy uwierzytelnienia. Obecnie stosowana praktyka pozwala na trzykrotną próbę identyfikacji tożsamości osoby, po czym konto jest blokowane i wymagane są dodatkowe czynności i weryfikacje w celu przywrócenia jego aktywnego stanu. Wynika to z przyjętych reguł ochrony, które mają chronić przed atakami siłowymi. Pojawia się zatem pytanie, czy taka sytuacja może być zmieniona przy zachowani wymaganego poziomu ochrony.

W prezentowanej rozprawie doktorskiej zaproponowano nowy schemat zarządzania uwierzytelnieniem ze zmiennym poziomem bezpieczeństwa i oceną satysfakcji użytkownika. Pozwala on zapewniać odpowiedni poziom ochrony usługi (określany jako QoP – Quality of Protection), a równocześnie jest zorientowany na potrzeby użytkownika (QoE – Quality of Experience).

Dr hab. Bogdan Księżopolski
Instytut Informatyki
Wydział Matematyki, Fizyki i Informatyki
Uniwersytet Marii Curie-Skłodowskiej w Lublinie

Lublin, 1.03.2018 r.

Recenzja rozprawy doktorskiej

Tytuł : Schemat zarządzania uwierzytelnieniem ze zmiennym poziomem bezpieczeństwa i oceną satysfakcji użytkownika

Autor: mgr inż. Mariusz Sepczuk

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

Rozprawa doktorska dotyczy ważnego zagadnienia z zakresu zarządzania bezpieczeństwem informacji. Przedmiotem rozprawy jest stworzenie schematu uwierzytelnienia ze zmiennym poziomem bezpieczeństwa, która uwzględnia poziom satysfakcji użytkownika (QoE). Rozpatrywany temat jest ważny i aktualny z uwagi na rosnąca liczbę urządzeń z ograniczonymi zasobami oraz rozwój inteligentnych sieci 5G.

Tezą rozprawy jest skonstruowanie systemu, który będzie dobierał mechanizmy uwierzytelnienia, mając na względzie odczucia osoby, która będzie z niego korzystać. W celu potwierdzenia postawionej tezy określono trzy główne zadania badawcze. Pierwsze dotyczyło zbudowania modelu zarządzania uwierzytelnieniem biorącym pod uwagę kontekst użytkownika, poziom bezpieczeństwa oferowany przez mechanizm uwierzytelnienia i satysfakcję użytkownika. Drugie zadanie dotyczyło zbudowania rozszerzonego modelu zarządzania uwierzytelnieniem uwzględniającym poziom ryzyka. Trzecie zadanie polegało na

zaproponowaniu wykorzystania modelu w wybranych środowiskach sieciowych wraz z analizą warunków działania rozwiązania.

Oprócz głównych zadań badawczych przedstawiono trzy pomocnicze zadania badawcze. Pierwsze polegało na zbadaniu zależności końcowej wartości parametru QoE w wybranych mechanizmach uwierzytelnienia. Drugie dotyczyło zbadania zależności czynników wpływających na satysfakcję użytkownika w proponowanym mechanizmie zarządzania uwierzytelnieniem. Trzecie zadanie dotyczyło zbadania wpływu ryzyka związanego z wyborem danej metody identyfikacji w rozszerzonym modelu zarządzania uwierzytelnieniem.

Postawiona teza została sformułowana poprawnie, a jej wykazanie implikowało konieczność rozwiązania sformułowanych zadań badawczych oraz implementacji stosowych rozwiązań o stopniu złożoności adekwatnym do oczekiwanego poziomu prac doktorskich.

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

Analiza źródeł została zawarta głównie w rozdziale 2 oraz 3 rozprawy. W rozdziale 2 przedstawiono definicję usługi uwierzytelnienia wraz z jej charakterystyką oraz omówiono przykładowe protokoły uwierzytelnienia. Ta część ma charakter wprowadzenia w tematykę poruszoną w rozprawie. Analiza literatury światowej wraz z przedstawieniem aktualnego stanu wiedzy jest zawarta głównie w rozdziale 3. Zaprezentowany tam stan wiedzy prezentuje kolejno istotne zagadnienia dotyczące zadań badawczych określonych w rozprawie. Zagadnienia te dotyczą: poziomu ochrony mechanizmów bezpieczeństwa, bezpieczeństwa kontekstowego, systemów reputacji i zaufania oraz jakości usługi odbieranej przez użytkownika. Warto nadmienić, że tematyka dotycząca zarządzania bezpieczeństwem informacji zorientowana na użytkownika jest nadal nowym kierunkiem badań naukowych, dlatego literatura światowa w tej tematyce jest ograniczona. Przedłożona rozprawa doktorska obejmuje 91 pozycji bibliograficznych, które reprezentują poruszaną tematykę. Jest ona uporządkowana w kolejności alfabetycznej. Szczególnie wartościowe jest przedstawienie czterech zestawień systemów uwierzytelnienia (Tabele: 3.1, 3.2, 3.3, 3.4), które jasno i przekonywująco charakteryzują poszczególne rozwiązania.

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 stworzenia systemu, który będzie dobierał mechanizmy uwierzytelnienia, mając na względzie odczucia osoby, która będzie z niego korzystać, został rozwiązany. Zaproponowane rozwiązanie polegało na przygotowaniu modelu teoretycznego. W tym celu stworzono schemat zarzadzania uwierzytelnieniem, który opiera się na koncepcji drzewa decyzyjnego. Zaproponowany schemat uwzględnia czynniki związane z QoE towarzyszące procesowi uwierzytelnienia. Wśród nich wzięto pod uwagę zadowolenie z możliwości podjęcia kolejnej próby (brak zablokowania konta), dyskomfort z powodu nieudanej próby oraz satysfakcję z finalnego potwierdzenia tożsamości. Zaproponowany model uwierzytelnienia został następnie rozszerzony o czynnik dotyczący poziomu ryzyka dotyczącego wykonywanej akcji. Ryzyko określa niepewność, co do możliwości wystąpienia zdarzenia (kontekstu) mogącego mieć negatywny wpływ na proces uwierzytelnienia.

W celu weryfikacji stworzonego systemu zostały opracowane dwa środowiska testowe: środowisko mobilne oraz środowisko mgły obliczeniowej. W ramach środowiska mobilnego wykonano symulacje systemu, które uwzględniają poziom ochrony i poziom satysfakcji użytkownika. W ramach środowiska mgły obliczeniowej wzięto pod uwagę parametry: QoS, QoP i QoE przy niezmiennym kontekście wykonywane przez użytkownika akcji. Wykonane symulacje potwierdzają postawioną w rozprawie doktorskiej tezę. Biorąc pod uwagę powyższe, uważam, że Autor wykorzystał odpowiednie metody badawcze.

4. **Na czym polega problem 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?**

Najważniejszym oryginalnym osiągnięciem Autora jest opracowanie nowego schematu zarządzania uwierzytelnieniem opartym na poziomie ryzyka.

W celu określenia ryzyka wykonania danej akcji uwierzytelniania, Autor wprowadził wagę określającą wpływ danych kontekstowych na ten proces (SWOC). Następnie na podstawie danych historycznych dotyczących zachowania użytkownika określa

prawdopodobieństwo wystąpienia pewnego stanu, rozumianego jako kontekst (P(e)). Na podstawie wspomnianych parametrów określany jest minimalny poziom bezpieczeństwa (LOS) mierzony jakością zabezpieczeń (QoP) wymagany do wykonania procesu uwierzytelniania. W ramach utworzonego schematu istotnym elementem jest również wprowadzenie algorytmu korelacji danych kontekstowych historycznych z aktualnie analizowanymi danymi kontekstowymi. Algorytm ten wykorzystuje procedury przeglądania grafu w głąb (DFS), którego wynikiem jest określenie, czy analizowany kontekst jest zgodny z wcześniej określonymi profilami kontekstowymi. Rozszerzenie schematu uwierzytelnienia o czynnik ryzyka jest bardzo ciekawe i z punktu widzenia naukowego bardzo wartościowe. Warto również nadmienić, że zaproponowane rozszerzenie zostało pozytywnie przyjęte przez ekspertów w tej tematyce, schemat ten został opublikowany w renomowanym czasopiśmie z listy JCR - Computers & Security.

Innym oryginalnym wkładem Autora jest zaproponowanie modelu uwierzytelnienia, który uwzględnia czynniki towarzyszące podczas procesu uwierzytelnienia (QoE). Zaproponowany schemat dla określonych metod autentykacji określa ich jakość zabezpieczenia (QoP) oraz łączy te metody z satysfakcją użytkownika (QoE). Autor tworzy drzewa decyzyjne, które określają możliwe stany w ramach procesu autentykacji. Zaproponowany system wylicza dla poszczególnych ścieżek parametry: QoP, QoE oraz prawdopodobieństwo poprawnej autentykacji. Na podstawie tych parametrów dla poszczególnych ścieżek wykonywany jest proces wielokryterialnej optymalizacji w celu znalezienia najlepszej ścieżki zgodnie z określoną funkcją celu.

Innym wkładem Autora wartym zauważenia jest wykonanie badania zależności QoE oraz QoP dla wybranych mechanizmów uwierzytelnienia dla urządzenia mobilnego. W ramach badania wybrano jako metody autentykacji kod PIN (4-12 cyfr), skanowanie odcisku palca (1-4 palców) lub kombinację tych metod. Satysfakcję użytkownika badano przy pomocy skali MOS (1-5) i na tej podstawie określono zależności wartości QoE (skala MOS) i grupy wiekowej. Wyniki przeprowadzonego eksperymentu pokazują, że dla wieloczynnikowych metod autentykacji poziom satysfakcji użytkownika nie jest prostą średnią arytmetyczną, ale w dużej mierze zależy, czy któryś z czynników nie był dla użytkownika szczególnie uciążliwy.

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

Praca została zredagowana w sposób bardzo dobry. Autor wykazał się umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników. Zaproponowane schematy uwierzytelnienia zostały dobrze zilustrowane odpowiednimi przykładami. Mam pewne uwagi dotyczące rozdziału 8, w ramach którego zostały zaprezentowane wybrane środowiska zastosowania. Zostały tam przedstawione diagramy przepływów dla scenariuszy ilustrujących możliwość zastosowania zaproponowanych schematów autentykacji. Diagramy te zostały opisane, ale brakuje odwołania poszczególnych wykonywanych operacji do poszczególnych kroków na diagramie. Dodatkowo, zawarte w rozdziale 8 tabele z wynikami (Tabela 8.2-8.17) nie zostały opatrzone przykładowymi wyliczeniami, ich dodanie pomogłoby w analizie konkretnych przypadków. W ramach rozprawy doktorskiej zaprezentowano kilka modeli teoretycznych opisujących nowy schemat uwierzytelniania. Podstawowe pojęcia zostały wprowadzone w rozdziale 5 i zostały rozszerzane w rozdziale 6 i 7. Brakuje dodatku, który opisywałby pełną notację w ramach zaproponowanych rozwiązań. Pomocny był natomiast załączony wykaz skrótów, spisu rysunków, tabel, algorytmów oraz listingów.

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

W moim odczuciu zaprezentowane wyniki mają dwie słabości. Pierwsza z nich polega na tym, że większość parametrów zastosowanych w proponowanych schematach uwierzytelnienie jest ustalanych na podstawie wiedzy eksperckiej. Przykładem mogą być parametry określone w podstawowym modelu uwierzytelnienia dotyczące kontekstu (QoE, tabela II, s. 53) lub jakości zabezpieczeń (QoP, tabela VI, s.54). W rozszerzonym modelu uwzględniającym ryzyko w podobny, ekspercki sposób określane są na przykład wagi bezpieczeństwa opisujące kontekst (SWOC, Tabela 1-4, s.68). Myślę, że warto w przyszłych badaniach opracować metody wyznaczania wspomnianych parametrów w oparciu o dane ilościowe. Na podstawie danych ilościowych można by wówczas określić uniwersalne miary oceny parametrów QoE oraz QoP, które następnie stanowiłyby wzorzec dla innych rozwiązań opartych o podobne parametry jakościowe.

Druga słabość dotyczy braku weryfikacji zaproponowanych rozwiązań w rzeczywistym systemie teleinformatycznym. W pracy wykonano zestaw symulacji, które pokazują jaki rozkład mają poszczególne parametry i jaki mają one wpływ na końcowe funkcje oceny, ale brakuje uzasadnienia zastosowania poszczególnych parametrów. Dla przykładu parametr QoE w podstawowym schemacie uwierzytelnienia jest iloczynem parametru A oraz exp(Z), gdzie A jest parametrem, który ma na celu dostosowanie zachowania użytkownika (skala MOS:1-5), a Z jest uzależniony od stanu systemu na drzewie decyzyjnym (s.52). Dlaczego została użyta funkcja ekspotencjalna a nie inna funkcja? Czy rzeczywiście warto używać parametru A, a jeżeli tak to, czy skala 1-5 jest odpowiednia? Myślę, że przy pomocy metod eksperymentalnych można spróbować uzasadnić zastosowanie poszczególnych parametrów oraz funkcji.

Należy zauważyć, że wskazane uwagi nie wpływają w istotny sposób na moją merytoryczną pozytywną ocenę pracy jako całości. Ich uwzględnienie może okazać się przydatne w dalszej działalności naukowej doktoranta.

7. Jaka jest przydatność rozprawy dla nauk technicznych?

Przydatność uzyskanych wyników w naukach technicznych oceniam wysoko. Zaproponowane schematy uwierzytelnienia ze zmiennym poziomem bezpieczeństwa i oceną satysfakcji użytkownika pozwalają dostosować poziom bezpieczeństwa stosowanych metod autentykacji do prawdziwych wymagań systemowych, unikając nadmiarowego użycia zasobów. Warte podkreślenia jest, że Autor w ramach rozprawy doktorskiej przedstawił dwa potencjalne zastosowania nowych schematów, czyli środowisko mobilne oraz mgły obliczeniowej. Myślę, że zaprezentowane wyniki znajdą zainteresowanie w środowisku naukowym.

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.

Uważam, że rozprawa doktorska magistra Mariusza Sepczuka spełnia wymogi stawiane rozprawom doktorskim przez obowiązujące przepisy. Należy podkreślić, że część wyników rozprawy została już opublikowana w literaturze międzynarodowej, a w szczególności w renomowanym czasopiśmie Computers & Security indeksowanym w JCR.

Wrocław, 14.02.2018

Dr hab. inż. Grzegorz Kołaczek, prof. PWr
Katedra Informatyki
Wydział Informatyki i Zarządzania
Politechnika Wrocławska
ul. Wybrzeże Wyspiańskiego 27
50-370 Wrocław

Recenzja rozprawy doktorskiej

Autor: **mgr inż. Mariusz Sepczuk**
Tytuł: **„Schemat zarządzania uwierzytelnianiem ze zmiennym poziomem bezpieczeństwa i oceną satysfakcji użytkownika"**
Promotor: **prof. dr hab. inż. Zbigniew Kotulski**

Niniejsza opinia została przygotowana na prośbę Dziekana Wydziału Elektroniki i Technik Informacyjnych prof. dr hab. inż. Krzysztofa Zaremby z dnia 19.12.2017r.

1. Jakie zagadnienie naukowe jest rozpatrzone w pracy?

Recenzowana rozprawa dotyczy istotnego dla współczesnej informatyki zbioru zagadnień z zakresu bezpieczeństwa teleinformatycznego. Szczegółowym aspektem bezpieczeństwa, którego dotyczy rozprawa jest zadanie uwierzytelnienia użytkownika w systemie i analiza poziomu satysfakcji użytkownika z usług uwierzytelnienia świadczonych przez system. Celem pracy wskazanym przez autora przedłożonej rozprawy jest „stworzenie schematu zarządzania uwierzytelnieniem ze zmiennym poziomem bezpieczeństwa i oceną satysfakcji użytkownika, który będzie zapewniać odpowiedni poziom ochrony usługi, a równocześnie będzie zorientowany na użytkownika". Takie sformułowanie celu pozwala jednoznacznie określić problem badawczy podjęty w pracy. Należy zauważyć, iż sformułowanie celu badawczego w ujęciu zaproponowanym przez autora rozprawy jest relatywnie nowym podejściem do standardowego zbioru problemów charakterystycznych dla dziedziny bezpieczeństwa teleinformatycznego. Położenie w pracy akcentu na elementy związane z użytecznością w procesie gwarantowania wysokiego poziomu bezpieczeństwa nie jest czymś zupełnie nowym, nie mniej jednak jest to problem wciąż rzadko podejmowany jako temat badawczy. Przedłożona rozprawa ma charakter teoretyczny z elementami badań eksperymentalnych, które głównie mają na celu ilustrację własności opracowanych rozwiązań.

Należy również zauważyć, iż sformułowany przez autora rozprawy problem badawczy jest bardzo rozległy i ma charakter interdyscyplinarny oraz wpisuje się w obszar zagadnień naukowych przynależnych do dziedziny „interakcja człowiek-komputer" (ang. Human-Computer interaction). Pomimo istotnej roli czynników pozatechnicznych w podjętej tematyce badawczej, które uwidaczniają się zwłaszcza w kontekście analizy poziomu satysfakcji użytkownika (ang. Quality of Experience), autor ograniczył zakres pracy głównie do zadania opracowania ogólnej koncepcji schematu uwierzytelniania z uwzględnieniem czynnika

QoE. Przedstawiony schemat może być przedmiotem dalszych prac badawczych zarówno w kontekście technicznym (szczegółowa analiza środowisk wykonawczych, protokołów i mechanizmów uwierzytelnienia) oraz pozatechnicznym (aspekty psychologiczne, kognitywne, ekonomiczne).

2. Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł?

Trzeci rozdział recenzowanej rozprawy w całości został poświęcony analizie aktualnego stanu wiedzy i kierunków prac badawczych w zakresie zagadnień istotnych dla sformułowanej przez autora rozprawy tezy badawczej. Przedstawiono przegląd literatury i dokonano analizy stanu wiedzy oraz zastosowań wyników prac badawczych w zakresie metod oceny poziomu ochrony przy wykorzystaniu konkretnych mechanizmów bezpieczeństwa, rozwiązań z zakresu bezpieczeństwa kontekstowego oraz problematyki dotyczącej systemów zarządzania reputacją i zaufaniem w systemach informatycznych.

W rozprawie przedstawiono skrótowo najważniejsze kierunki rozwoju, osiągnięcia oraz problemy dla dziedziny badań podjętych przez autora na przykładzie wybranych publikacji naukowych z literatury światowej. Poza zwięzłym opisem istoty poszczególnych prac, doktorant przestawił wynik przeprowadzonej analizy w postaci syntetycznego zestawienia w formie trzech tabel. Zamiar autora był słuszny, nie mniej jednak sposób realizacji nie okazał się być najlepszy, gdyż umieszczone w tabelach podsumowanie w formie pojedynczych haseł nie jest zawsze jednoznaczne i czytelne (np. kolumna „ograniczenie" – wartość „użytkownik decyduje o ochronie"). Poza tym, opis umieszczony w tabeli nie jest zawsze do końca spójny z opisem w tekście rozdziału (np. praca Y.Mowafi [53] – w tabeli przedstawiono, iż realizowana jest jedynie usługa autentyczności, podczas gdy z opisu umieszczonego w tekście rozdziału wynika, iż przedstawione w pracy rozwiązanie koncentruje się na poufności i integralności).

Autor rozprawy odwołał się do 91 pozycji literaturowych, w tym 8 własnych i współautorskich. Wśród nich są referaty konferencyjne, artkuły w recenzowanych czasopismach, w tym w czasopiśmie notowanym na tzw. liście filadelfijskiej. Przedstawione wynik studiów literaturowych potwierdzają umiejętności korzystania z dostępnych źródeł wiedzy.

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

W recenzowanej pracy zostało przedstawione autorskie rozwiązanie problemu związanego z zarządzaniem uwierzytelnieniem z wykorzystaniem mechanizmów gwarantujących różny poziom ochrony (ang. Quality of Protection) oraz z uwzględnieniem sposobu postrzegania usług bezpieczeństwa przez użytkownika (ang. Quality of Experience). Zaproponowane rozwiązanie korzysta z algorytmu drzewa decyzyjnego, którego węzłami są dostępne mechanizmy uwierzytelnienia, a gałęzie definiują zdarzenia przejścia należące do jednego z trzech możliwych typów: wybór nowego mechanizmu uwierzytelnienia, ponowienie uwierzytelnienia, zakończenie procedury uwierzytelnienia.

Podstawowym założeniem przyjętym w rozprawie przez autora było założenie dotyczące istotnego wpływu kontekstu na poziom satysfakcji użytkownika usługi uwierzytelniającej oraz na poziom ryzyka. Autor dokonał analizy zaproponowanego rozwiązania z wykorzystaniem symulacji oraz badania eksperymentalnego z udziałem użytkowników. W świetle przedstawionych w pracy rezultatów teoretycznych oraz wyników eksperymentów należy uznać, iż autor użył właściwej metody dla przedstawionego zagadnienia badawczego.

4. Na czym polega oryginalność rozprawy?

Podstawowym oryginalnym rezultatem rozprawy jest zaproponowany przez autora schemat zarządzania uwierzytelnieniem zorientowany na użytkownika. Szczególnie interesujące jest przedstawione rozwiązanie problemu „maksymalnej liczby błędów" w trakcie realizacji procedury uwierzytelnienia użytkownika. Opracowany schemat uwierzytelnienia może znaleźć praktyczne zastosowanie w systemach informatycznych, dla których aspekt bezpieczeństwa, jak i elementy użyteczności są równie istotne (np. w sektorze usług finansowych). Przedstawione rozwiązanie problemu zarządzania uwierzytelnieniem jest unikalne i rozszerza stan wiedzy w dziedzinie badań nad użytecznością rozwiązań z dziedziny bezpieczeństwa teleinformatycznego. Potwierdzeniem znaczenia przedstawionej koncepcji może być również fakt, iż część z rezultatów przeprowadzonych prac badawczych została opublikowana w renomowanym czasopiśmie „Computers & Security" (IF=2.849, 2016r.).

5. Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników?

Autor przedstawił poprawnie i metodycznie wszystkie komponenty procesu projektowania i walidacji schematu zarządzania uwierzytelnieniem w systemach informatycznych. Ponadto poddano dyskusji i wykazano zasadność wykorzystania elementów kontekstu w procesie zarządzania uwierzytelnieniem. W części autorskiej pracy doktorant przedstawił opis wykonanych eksperymentów oraz rezultaty przeprowadzonej analizy otrzymanych wyników.

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

Uwagi ogólne

1. Zasadnicza część rozprawy prezentująca autorski dorobek doktoranta składa się z trzech artykułów, które zostały umieszczone w tekście rozprawy w całości, w oryginalnej postaci. Powoduje to powstanie w sposób naturalny pewnej nadmiarowości w tekście rozprawy (np. analiza stanu sztuki), lecz również przyczyniło się to do pojawienia się w pracy pewnych niespójności. Np. w rozdziale 5 wartość metryki oceny mechanizmu uwierzytelnienia jest wyliczana jako prosty iloczyn QuE i QuP, natomiast w rozdziale 6 pojawiają się wagi dla tych samych elementów metryki. Fakt współistnienia tych dwóch podejść oraz ewentualne różnice pomiędzy tymi podejściami nie został w tekście pracy skomentowany.
2. Artykuł w czasopiśmie czy też publikacja w materiałach konferencyjnych ze względu na swój charakter jest formą zwięzłą, gdzie narzucone są wymagania dotyczące objętości pracy, a przez to nie wszystkie szczegóły mogą zawsze być w sposób wystarczająco precyzyjny przedstawione i przedyskutowane. Przygotowując rozprawę można było spróbować poszerzyć materiał z publikacji o istotne szczegóły, na które zabrakło miejsca w oryginalnej pracy. Na przykład można byłoby w sposób bardziej wyczerpujący opisać sposób realizacji badań, których wyniki przedstawiono w rozdziałach 5-7. Bardziej szczegółowy opis dotyczący m.in. tego w jaki sposób dobierano osoby do badania, jak wyglądał scenariusz badawczy od strony użytkownika, czy badania były powtarzane na kilku grupach osób, jakie doświadczenie posiadały te osoby (rozdział 5). Takie uzupełnienie stanowiłoby dodatkowy walor przedłożonej rozprawy i dokumentowałoby umiejętności badawcze jak i warsztat pracy naukowej autora. W rozdziale 6 można byłoby

np. przedstawić dyskusję nad wartościami parametrów, szczegółową specyfikację formuł umieszczonych w oryginalnej publikacji, itp. Takie podejście umożliwiłoby nadanie większej spójności całej treści rozprawy oraz pozwoliłoby uniknąć pewnych niejednoznaczności (np. opisanych w Uwagi ogólne, pkt. 1).

3. Autor w sposób zamienny używa pojęć: model, mechanizm, metoda, schemat w kontekście uwierzytelnienia – co nie jest właściwym podejściem, gdyż w literaturze specjalistycznej te pojęcia są dobrze zdefiniowane i mają swój odrębny charakter i zakres zastosowania.
4. Autor w sposób zamienny używa pojęć identyfikacja i uwierzytelnienie. Zagadnienia te w sposób znaczący różnią się od siebie, o czym wspomina sam autor w rozdziale 2.1.
5. Część przedstawionych wniosków ma znamiona trywialności (np. poziom ryzyka zależy od wiedzy, rodzaju serwisu, metody uwierzytelnienia).
6. Istotne dla ewentualnego dalszego przebiegu badań jest pytanie: jak bardzo, lub też czy w ogóle wartość doświadczenia użytkownika powinna mieć wpływ na „adaptacyjny" dobór metody uwierzytelnienia. Czy „zły odbiór" metody uwierzytelnienia przez użytkownika jest wystarczającym powodem żeby ją zastąpić inną metodą dającą w konsekwencji niższy poziom bezpieczeństwa? Rozważając coraz bardziej wyrafinowane ataki, które coraz częściej realizowane są wieloetapowo (np. najpierw uzyskanie dostępu do skrzynki e-mail, w kolejnym kroku dostępu do portalu systemu bankowego, itd.) dają mocne przesłanki ku temu, iż zasada „najsłabszego ogniwa" powinna również być wzięta pod uwagę w procesie doboru metod uwierzytelnienia. Nie mniej jednak, przedłożona rozprawa bardzo dobrze koresponduje z innym paradygmatem bezpieczeństwa, a mianowicie z wymaganiem, iż mechanizmy bezpieczeństwa powinny być „przeźroczyste" dla użytkownika, a co za tym idzie, iż w procesie projektowania rozwiązań z dziedziny bezpieczeństwa, równie istotnym elementem jest rozważanie aspektów dotyczących sposobu odbioru zabezpieczeń przez użytkownika.

Uwagi szczegółowe

1. W pracy niestety nie udało się uniknąć potknięć językowych (np. „tezą pracy jest skonstruowanie systemu (...)" str.1; „zbadano zależność końcowej wartości parametru QoE (...)", „zbadano zależność czynników (...)" – od czego? str.2.; „zbadano wpływ ryzyka (...)" – na co? str.2.) i literówek (np. „Oczywiście nie są to *jedyna* rozwiązania (...)" str.15; „Drugi wariant jest dostępny do *momenty*, kiedy dostępne są do *użycie* mechanizmy uwierzytelniające (...)". str.101).
2. Rozdział 5. Założenie o liniowej zależności poziomu bezpieczeństwa od długości hasła jest zbyt dużym uproszczeniem i w ostateczności może wypaczyć końcowy wynik oceny przydatności metody uwierzytelnienia (w pracy przyjęto założenie, iż wydłużenie hasła o jeden znak powoduje wzrost QoP o jeden).
3. Rozdział 6. Dla wzoru (7) założono domyślnie, że $t_j>1$, co niekoniecznie musi być oczywiste. Dla ego samego wzoru czy QoP_{jFIN} jest funkcją QoP? Tak sugeruje użyta notacja i użycie symbolu nawiasów.
4. Rozdział 6. Czym jest „j" w QoE_{jFIN}? Indeksem? Elementem symbolu zmiennej? Jak zatem interpretować zapisy dla $QoE_{jFIN=1}$ (9) i QoE_{j-1FIN} dla (10)?

5. Rozdział 6. Rysunek 2. Górna „ścieżka" wskazuje na możliwość wielokrotnego wyboru tego samego mechanizmu uwierzytelnienia A_1. W szczególności można użyć tego mechanizmu więcej niż 3 razy. Czy jest to poprawna interpretacja w świetle przedstawionych w artykule założeń? Taka sama uwaga obowiązuje w odniesieniu do analogicznego rysunku w rozdziale 7.
6. Rozdział 6. Ocena wpływu zmian wartości parametru B w stosunku do zmian parametrów A1 i A2. Zmiana wartości zmiennych A jest sumarycznie na poziomie 0,44, podczas gdy zmiana wartości B na poziomie 0,2. Implikuje to oczywiste wnioski o wpływie zmian wartości tych parametrów na końcową wartość oceny.
7. Rozdział 7. Czy interpretacja parametru B jako wskaźnika korelacji wartości parametrów kontekstu nie jest pewnym nadużyciem? Z Algorytmu 1 wynika, iż bardziej zasadne jest traktowanie tego parametru jako wskaźnika obecności ścieżki w grafie.
8. Rozdział 7. „Moreover the scale is inverted (...) str.68" – nie jest to spójne z podanym przykładem i z wartościami w tabelach.
9. Rozdział 7. Czy wartość „typ użytkownika", ma pomagać w dobraniu odpowiedniego mechanizmu uwierzytelnienia dla użytkownika, czy też ma pomóc ochronić system przed atakiem („human skills and awareness of vulnerabilities increase a risk too")? Jeżeli rozważyć ten drugi aspekt, to skąd system czerpie wiedzę na temat typu użytkownika?
10. Rozdział 7. Rysunki 4-6 mają niezbyt szczęśliwie dobrane kolory. Nie zostało również opisane znaczenia kolorów, co utrudnia analizę.

7. Jaka jest przydatność rozprawy dla nauk technicznych?

Rozprawa stanowi istotny wkład do rozwoju badań nad rolą doświadczenia użytkownika w procesie gwarantowania bezpieczeństwa w systemach informatycznych. Otrzymane rezultaty charakteryzuje znacząca wartość praktyczna. Zaproponowany schemat może zostać wykorzystany w celu umożliwienia elastycznego i przyjaznego użytkownikom zarządzania procesem uwierzytelnienia. Autor przedstawił w pracy koncepcję zastosowania opracowanego schematu w środowisku mgły obliczeniowej. Jak to zostało już nadmienione w pkt.1. niniejszej recenzji, niezależnie od istotnych osiągnięć teoretycznych i praktycznych charakteryzujących recenzowaną pracę, praca może być traktowana również jako wstępny etap do poszerzonych badań nad rolą doświadczenia użytkownika systemów informatycznych w kontekście procesu zapewnienia wysokiego poziomu bezpieczeństwa. Dalsze poszukiwania tematów badawczych mogą odnosić się m.in. w sposób bardziej pogłębiony do problemów powstających na linii powiązań typu technika – użytkownik. Tego typu zagadnienia stanowią podstawową domenę badań dla coraz bardziej znaczącego nurtu prac z dziedziny interakcja człowiek-komputer.

8. Konkluzja

Doktorant wykazał się w recenzowanej rozprawie właściwie stosowanym aparatem matematycznym oraz dobrą znajomością aktualnej problematyki związanej z zarządzaniem uwierzytelnieniem w systemach informatycznych ze szczególnym uwzględnieniem aspektu zmienności poziomu bezpieczeństwa i oceny jakości doświadczenia odbiorców usług informatycznych. Dla przedstawionych zagadnień został sformułowany szereg interesujących i użytecznych metod analizy w tym przedstawione zostały wyniki badań symulacyjnych

uwzględniających różne wartości parametrów opisujących właściwości systemów uwierzytelniania i czynników kształtujących poziom odbioru jakości świadczonych usług.

Recenzowana rozprawa przedstawia rozwiązanie ważnego i oryginalnego problemu wzbogacając wiedzę dotyczącą bezpieczeństwa teleinformatycznego w zakresie zarządzania uwierzytelnieniem, a zawarte w niej wyniki badań wskazują również na możliwość wykorzystania przedawnionych metod w praktyce.

Przedstawione w punkcie 6. niniejszej recenzji uwagi nie mają wpływu na ostatecznie pozytywne wrażenie o przedłożonej rozprawie.

Biorąc powyższe pod uwagę stwierdzam, że praca mgr inż. Mariusza Sepczuka

pt. „Schemat zarządzania uwierzytelnieniem ze zmiennym poziomem bezpieczeństwa i oceną satysfakcji użytkownika" spełnia wymagania stawiane rozprawom doktorskim w świetle stosownej ustawy o stopniach naukowych i tytule naukowym. Wnoszę o jej przyjęcie i dopuszczenie do jej publicznej obrony.

Grzegorz Kołaczek