Warszawa, 8 stycznia 2017

prof. UKSW, dr hab. Mirosław Kurkowski
Instytut Informatyki
Uniwersytet kard. St. Wyszyńskiego
w Warszawie

Recenzja Rozprawy Doktorskiej mgra inż. Tomasza Klasy

Model referencyjny zintegrowanego systemu monitorowania bezpieczeństwa informacji w organizacjach wirtualnych

Promotor: dr hab. inż. Imed El Fray

Niniejsza recenzja została sporządzona na prośbę Dziekana Wydziału Informatyki Zachodniopomorskiego Uniwersytetu Technologicznego dra hab. inż. Jerzego Pejasia. Praca ogólnie rzecz biorąc dotyczy metod ochrony danych w systemach/środowiskach dynamicznie zmieniających swoją strukturę.

Wprowadzenie

Nie bez powodu mówi sie, że informacja jest obecnie najbardziej cennym towarem na świecie. Można śmiało powiedzieć, ze dzisiaj w dobie tzw. społeczeństwa informacyjnego, sukcesy i porażki w wielu dziedzinach życia uzależnione są od posiadania lub braku informacji. W skomputeryzowanym świecie informacje wymieniane są szybko i w ogromnej ilości, o jakiej kilkadziesiąt lat temu nikt nie mógł marzyć. Problem bezpieczeństwa informacji jest więc jednym z najważniejszych obecnie problemów świata, rozprawa dotyczy więc jednego z najbardziej aktualnych i poważnych problemów z jakimi boryka się rzeczywistość.

Rozważania zawarte w rozprawie są kontynuacją badań nad problemem bezpieczeństwa informacji w różnego typu przedsiębiorstwach/organizacjach. Od pewnego czasu prowadzone są na ten temat prace badawcze, jednak zmieniające się warunki funkcjonowania firm/organizacji powodują coraz to nowe uwarunkowania zmieniające wciąż bazowe parametry rozważań. Praca mgra inż. Tomasza Klasy przedstawia rozwiązania w omawianym zakresie dla jednego z najnowszych typów organizacji, a mianowicie struktur nazywanych wirtualnymi, gdzie ze względu na dużą dynamikę zmian w strukturze i modelu ich działania, zapewnienie bezpieczeństwa informacji jest utrudnione.

W odpowiednio dużych organizacjach wirtualnych okresy pomiędzy zmianami mającymi znaczny wpływ na ich strukturę mogą być krótsze niż przeciętny czas trwania audytu bezpieczeństwa. Powoduje to problem możliwości permanentnego braku odpowiedniego monitoringu bezpieczeństwa informacji w organizacji. Całkowicie zasadne

jest zatem prowadzenie badań nad metodami monitorowania bezpieczeństwa uwzględniających wymagania i możliwości (ograniczenia) systemu informacyjnego organizacji wirtualnej.

Badania takie prowadzone są w ostatnich latach. Powstało wiele opracowań w tym zakresie. Jednak należy podkreślić, że proponowane w tych pracach rozwiązania nie tworzą, jak do tej pory, spójnej całości. Rozważane są metody skupiające się na przykład na zapewnieniu odpowiedniego poziomu zaufania, inne podkreślają rolę zapewnienia bezpiecznego dostępu do informacji. Istnieją także prace skierowane na wykrywanie anomalii w pracy organizacji wirtualnych. Biorąc pod uwagę powyższe podjęcie próby wyznaczenia modelu zintegrowanego systemu monitorowania bezpieczeństwa organizacji wirtualnej jest całkowicie uzasadnione.

Zawartość Rozprawy

Przedstawiona do recenzji praca liczy 161 stron, nie licząc stron zawierających spisu treści oraz bibliografii. W mojej opinii rozprawa została napisana starannie i przejrzyście, a jej układ nie budzi zastrzeżeń.

Postawiona w dysertacji **teza** brzmi: *przez dobór parametrów i metod monitorowania zasobów w sposób odpowiadający aktualnym potrzebom i oczekiwaniom organizacji, możliwe jest ograniczenie obciążenia systemu zadaniami związanymi z monitorowaniem przy zachowaniu akceptowalnej skuteczności*.

Celem zaproponowanym w **pracy** jest: *opracowanie modelu referencyjnego zintegrowanego systemu monitorowania bezpieczeństwa informacji w systemach informacyjnych organizacji wirtualnych*.

W rozdziale pierwszym opisano tło badanej problematyki. Przedstawiono i określono podstawowe pojęcia związane z omawianymi zagadnieniami: ryzyko, poufność, integralność, dostępność, spójność danych, czy zaufanie. Zdefiniowano proces i sposoby monitorowania bezpieczeństwa informacji. Omówiono metody gromadzenia danych na potrzeby monitorowania bezpieczeństwa. Przedstawiono znane metody identyfikacji anomalii i wnioskowania o stanie bezpieczeństwa systemu. Na potrzeby dalszych rozważań przedstawiono różne określenia oraz scharakteryzowano organizacje wirtualne. Określono również typowe dla nich zagrożenia związane z bezpieczeństwem informacji. Podano i przeanalizowano znane rozwiązania monitorowania bezpieczeństwa systemu informacyjnego organizacji wirtualnej.

Rozdział drugi przedstawia najważniejsze i istotne z punktu widzenia dalszych rozważań komponenty zintegrowanego systemu monitorowania bezpieczeństwa. Podano

również uogólniony model jego działania. Zaproponowano ponadto nową metodę doboru schematu/algorytmu ogólnego monitorowania, która uwzględnia ograniczenia techniczne i organizacyjne rozważanych struktur. Schemat ten stanowi kanwę dla późniejszych rozważań. Określa metodę gromadzenia danych i weryfikację ich kompletności. Również w oparciu o powyższy schemat przeprowadzane jest wnioskowanie o zaistniałych anomaliach oraz ich ocena. Opisano także proces doboru parametrów monitorowania bezpieczeństwa informacji oraz osobno metody doboru sposobu ich kontroli. Omówiono także problemy związane z gromadzeniem danych. Przedstawiono i przedyskutowano nowy model retencji danych, gdzie uwzględniono sposób ich reprezentacji oraz aktualizacji. Opisano metody komunikacji i uwierzytelniania w proponowanych strukturach. Na końcu rozdziału omówiono ostatni etap procesu monitorowania bezpieczeństwa informacji, jakim jest wnioskowanie z uzyskanych i przetworzonych danych.

Rozdział trzeci zawiera próbę wieloaspektowej weryfikacji jakości opisanego w rozprawie nowego modelu. Przedstawiono weryfikację algorytmu doboru planu monitorowania. Zastosowano tutaj nową metodę wyznaczania listy parametrów przeznaczonych do monitorowania oraz sposobu ich kontroli. Przeprowadzono także próbę weryfikacji poziomu bezpieczeństwa zaproponowanych protokołów uwierzytelniania oraz nawiązywania sesji, a także samego procesu komunikacji. Przedstawiono również weryfikację wydajności nowego sposobu organizacji danych. Pokazano, że zaproponowana metoda wymaga znacznie mniejszej transmisji danych w porównaniu z innymi metodami. Ostatni podrozdział przedstawia działanie przedstawionego w rozprawie algorytmu wnioskowania na przykładzie dwóch organizacji. Zaprezentowane wyniki oparto o rzeczywiste dane. Na koniec dokonano uzasadnienia wykazania postawionej tezy i osiągnięcia celu rozprawy.

Opinia merytoryczna rozprawy

Jak napisałem wcześniej, w mojej ocenie rozprawa została napisana starannie i przejrzyście, a jej układ jest właściwy. Dokonane w pierwszym rozdziale wprowadzenie w problematykę oraz przedstawienie rozważanych dalej pojęć i problemów zostało wykonane w sposób przystępny i wyczerpujący. Można podkreślić staranne i kompletne przedstawianie kolejno wprowadzanych zagadnień i problemów przez doktoranta. Moim zdaniem autor właściwie i wyczerpująco, ze względu na późniejsze rozważania, zaprezentował dotychczasowe rozwiązania w zakresie ochrony danych w organizacjach. Następnie kolejno określił rodzaj badanych organizacji (organizacji wirtualnych) i przedstawił zaproponowane wcześniej metody monitorowania informacji w tych organizacjach. Dzięki

takiemu układowi pracy czytelnik zostaje odpowiednio wprowadzony w późniejsze rozważania.

Rozdział drugi przedstawia wkład autora w badaną problematykę. Zaproponowano kompleksowy system monitorowania bezpieczeństwa informacji dostosowując go do nietypowych w ogólności warunków pracy organizacji wirtualnych. W porównaniu z innymi pracami na ten temat uwzględniono wiele istotnych czynników mających wpływ. Tę część rozprawy uważam za bardzo ważną i oceniam wysoko.

Rozdział trzeci zawiera próbę weryfikacji jakości wprowadzonych wcześniej rozwiązań. Weryfikacja jakości systemów jest w ogólności problemem bardzo złożonym. W mojej ocenie autor poradził sobie dobrze z wyzwaniami jakie sobie postawił w tej części rozprawy. Zastosował tutaj różne techniki od wnioskowania formalnego z użyciem logiki do badań nad rzeczywistymi danymi z dwóch organizacji. Niestety stosowana do weryfikacji zaproponowanych protokołów logika BAN nie jest w pełni wiarygodna, gdyż znanych jest kilka przypadków pozytywnego zweryfikowania przez tę logikę protokołów zawierających błędy. Można sądzić, że nietrudno będzie zweryfikować proponowane w rozprawie protokoły przy pomocy najnowszych i uznanych narzędzi weryfikacji modelowej do czego zachęcam autora rozprawy.

Uwagi polemiczne i krytyczne

W mojej ocenie najsłabszą stroną pracy są matematyczne formalizacje proponowanych rozwiązań oraz metodologiczne nieścisłości oraz błędy. Choć praca broniona jest w dziedzinie nauk technicznych, to jednak wydaje się, że doktorant powinien więcej uwagi zwrócić na poprawność i adekwatność formuł matematycznych zawartych w rozprawie.

W recenzji zwracam uwagę na następujące, moim zdaniem najważniejsze, kwestie:

1. Uważam, że nie do końca wyraźnie sformułowana jest zależność między tezą a celem pracy. Czytając tezę można wywnioskować, że rozprawa ma głównie wykazać, że „*Przez dobór parametrów i metod monitorowania zasobów (...)* ***możliwe jest ograniczenie obciążenia systemu…***”. Natomiast celem pracy jest wyraźnie: „***opracowanie modelu*** *(…)* ***systemu monitorowania bezpieczeństwa informacji*** *w systemach informacyjnych organizacji wirtualnych*”. Wydaje się, że w sformułowaniu tezy powinna znaleźć się informacja o zastosowaniu proponowanych metod do organizacji wirtualnych oraz o kompleksowości proponowanych rozwiązań. W opisie celu natomiast powinna być wzmianka, jak zrealizowanie go ma się do wykazania stawianej w pracy tezy. Oczywiście

czytelnik może to wszystko wywnioskować nawet już ze Wstępu, ale czytelniej byłoby, gdyby napisane to było wprost.

2. W mojej ocenie autor zbyt często i czasem niewłaściwie używa pojęcia definicji. Na przykład na stronie 10 przeczytać można, że: „*Dostępność oznacza zapewnienie niezawodnego i bezzwłocznego dostępu do informacji*… Następnie czytamy, że jest to definicja tego pojęcia, z której wynika, że „*informacje muszą być dostępne*". Pomijając dyskusję, czy *dostępność* można definiować przez *dostęp* można się zastanowić, czy w ogóle takie sformułowanie jest potrzebne dla prowadzenia rozważań w tym fragmencie rozprawy.
3. Na stronie 11tej napisano: „*Pojęciem blisko związanym z bezpieczeństwem jest ryzyko. Zależność ta kształtuje się w ten sposób, że wzrost ryzyka zwykle współistnieje z pogorszeniem bezpieczeństwa i ma charakter uniwersalny*." Skoro charakter tej zależności jest uniwersalny, to chyba jednak wzrost ryzyka *zawsze* współistnieje z pogorszeniem bezpieczeństwa.
4. Nie wiem, czy opisana na stronie 11tej „*materializacja ryzyka*" jest pojęciem powszechnie stosowanym w literaturze, ale jednak razi ono nieco czytelnika. Może jednak lepiej byłoby napisać: *Zaistnienie niepożądanej sytuacji związanej z … ryzykiem*.
5. Sądzę, że fragment na stronie 15: *„(…) problemem ERM jest wykładniczo rosnąca złożoność obliczeniowa – z każdym (…) rodzajem ryzyka rośnie liczba możliwych do zastosowania rozwiązań*" powinien brzmieć: *„(…) problemem ERM jest wykładnicza złożoność obliczeniowa stosowanych algorytmów, gdyż z każdym (…) rodzajem ryzyka wykładniczo rośnie liczba koniecznych do przeprowadzenia obliczeń.*"
6. Na stronie 24 w tabeli 1 pokazano, że rozwiązanie XCCDF jest uniwersalne dla podanych obszarów zastosowania. Jednak zdanie następne informuje, że: „*Z (…) analizy (…) wynika, że żadne z nich nie jest wystarczająco uniwersalne…*". Brak komentarza lub pomyłka.
7. W przedstawionym na stronie 37 wzorze na wyznaczanie priorytetu ryzyka (RPN) odpowiednie współczynniki są przez siebie przemnażane. Czy przypadek S=10, O=10 oraz D=0, a więc RPN=0 adekwatnie opisuje sytuację?
8. Na stronie 38 jest w mojej ocenie zawarta bardzo kontrowersyjna informacja: „*Modele formalne (…) stanowią próbę reprezentacji systemu (…). Ich podstawą jest model matematyczny, np. oparty o teorię grafów lub logikę stanów. (…) Istotną zaletą (…) jest fakt, że możliwa jest matematyczna weryfikacja poprawności i ograniczeń takich modeli. Jednocześnie, jest to przyczyną zwiększonej czasochłonności implementacji modelu w organizacji.*" Po pierwsze matematyczna, formalna weryfikacja poprawności, czy

ograniczeń modelu wymaga jakiegoś punktu odniesienia, najlepiej odpowiedniego metasystemu, ale również sformalizowanego. Takich raczej nie ma. Może chodziło jednak o *matematyczną weryfikację własności (poprawności?) w takich modelach??* Natomiast sama implementacja modelu nie musi być czasochłonna. Najczęściej czasochłonne są obliczenia wymagające przeszukania wykładniczo dużych struktur.

9. Wzory (6) i (7) na str. 55 powinny być lepiej opisane przez wprowadzenie odpowiednich oznaczeń i zależności.

10. We wzorze (8) nie wiadomo co to jest parametr *c* w wyrażeniu $\frac{c}{\frac{T}{j_{out}}}$.

11. Zapisy w wielu miejscach pracy w stylu „$bp_i \in BP\{bp_1, bp_2, \ldots, bp_n\}$" są wykonane bardzo nieszczęśliwie. Powinno być: „$bp_i \in BP = \{ bp_1, bp_2, \ldots, bp_n \}$, dla i = 1,…, n", lub lepiej: „$bp_i \in BP$ dla i = 1,…, n, gdzie $BP = \{ bp_1, bp_2, \ldots, bp_n \}$".

12. Zapis „*Zasób = {Zasób*, Zasób*, … }"* na stronie 76 sugeruje wielozbiór. Intencja autora była jednak inna. Powinno być *Zasób = {*$Zasób_1$**,* $Zasób_2$**, …,* $Zasób_n$** }*.

13. Zapis na stronie 76 *Zabezpieczenie*=zabezpieczenie(Zasób*)* ma przedstawiać relację między zasobem a zabezpieczeniem (?) (podobnie dalej *Parametr*=parametr(Zabezpieczenie*)).* W zasadzie jednak matematycznie nic nie oznacza. Brak jest określenia formalnego relacji. Zapis przypomina zapis funkcyjny mówiący, że ogólne *Zabezpieczenie** jest funkcją *Zasobu**.

14. Protokół zaproponowany na stronie 82 mógłby być opisany.

15. Na stronie 93 napisano: „*Następnie zdefiniowano autorską funkcję kryterialną* W_L *(ocena wpływu zmian na lokalną ocenę bezpieczeństwa informacji), za pomocą następującego wzoru:* $W = f(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$". Indeks *L* przy W_L to pewnie pomyłka. Gorzej, że podana zależność nie jest wzorem funkcji a jedynie informuje nieformalnie o liczbie jej argumentów. Brak klarownej informacji o dziedzinie funkcji oraz określeniu obliczania jej wartości. Kolejne zmienne to chyba odpowiednie współczynniki?

16. Przedstawienie wartości zmiennych na stronie 94 w postaci tabel i wykresów jest niejasne.

17. Na stronie 99 autor podstawia w miejsce „*ryzyka całkowitego"* „*system informacyjny"*.

18. Na stronie 125 autor rozpoczął weryfikację poprawności zaproponowanych w rozprawie protokołów przy pomocy logiki BAN. Logika ta jest pierwszą z logik zaproponowanych do weryfikacji protokołów. Jak napisałem wcześniej są jednak przypadki pozytywnej weryfikacji błędnych protokołów przez wnioskowanie syntaktyczne z wykorzystaniem systemu dedukcyjnego tej logiki. Również z formalnego punktu widzenia logika ta

posiada wiele mankamentów, nie ma jasno określonej semantyki, a jej system dedukcyjny jest niespójny. Myślę, że protokoły proponowane w rozprawie powinny być również zweryfikowane przez jakieś narzędzie z grupy tzw. model-checkerów, czyli narzędzi weryfikacji modelowej.

Uwagi redakcyjne

Jak każda rozprawa naukowa również recenzowana pozycja nie jest wolna od niedociągnięć, pomyłek, czy błędów natury redakcyjnej. Trzeba jednak zaznaczyć, że moim zdaniem rozprawa mgra inż. Klasy zawiera znacznie mniej takich pomyłek niż inne, znane mi, rozprawy. Poniżej zamieszczam listę przykładowych pomyłek/błędów.

- str. 9 - „…*istniała con najmniej*…”,
- str. 11 – „*W pierwszej chwili więcej użytkowników jest korzystne (większe przychody)*”,
- str. 12 - Po fragmencie: „…*proces zarządzania (…) dzieli się na*:” wypunktowanie powinno być pisane w bierniku,
- W rozprawie cytuje się prace polskich autorów. Sądzę, że ich nazwiska powinny być pisane zgodnie z językiem polskim. Np. Kołaczek, nie Kolaczek, Księżopolski, nie Ksiezopolski etc.,
- str. 53 – wzór: $\overline{\overline{\Omega}} = p_{(1)} * p_{(2)} * p_{(3)} * \ldots * p_{(n-1)} * p_{(n)} = p^n$ powinien chyba wyglądać tak: $\overline{\overline{\Omega}} = \underbrace{p * p * \ldots * p * p}_{n-razy} = p^n$, do oznaczenia iloczynu dobrze byłoby chyba używać normalnej kropki: $\overline{\overline{\Omega}} = \underbrace{p \cdot p \cdot \ldots \cdot p \cdot p}_{n-razy} = p^n$,
- rysunek 12 na stronie 61, potem 13, 14 na kolejnych stronach i im podobne są mało czytelne,
- str. 81 – „*model konwersji opiera się założenie, że*”,
- dobrze byłoby w Bibliografii ujednolicić pisownię autorów.

Wnioski końcowe

Biorąc pod uwagę zawartość przedstawionej przez mgra inż. Tomasza Klasę rozprawy stwierdzam, że moim zdaniem, praca ta spełnia wymagania stawiane rozprawom doktorskim przez obowiązującą aktualnie w Polsce Ustawę o Stopniach i Tytule Naukowym. Stawiam zatem wniosek o dopuszczenie jej do dalszych etapów przewodu doktorskiego prowadzonego przez Radę Wydziału Informatyki ZUT w dziedzinie nauk technicznych w dyscyplinie informatyka.