Prof. dr hab. inż. Zbigniew Kotulski,
Instytut Telekomunikacji Politechniki Warszawskiej

Warszawa, 25 czerwca 2014 r.

Recenzja rozprawy doktorskiej dla Rady Wydziału Informatyki Polsko-Japońskiej Wyższej Szkoły Technik Komputerowych

Tytuł rozprawy:

Cloud Computing and Digital Forensics Investigation: A Defensive Approach

Autor rozprawy: mgr Yucel Turel

1.Wstęp

Recenzja została przygotowana na wniosek Rady Wydziału Informatyki Polsko-Japońskiej Wyższej Szkoły Technik Komputerowych, na podstawie pisma Pani Dziekan Wydziału, dr Aldony Drabik, profesora PJWSTK, z dnia 13 czerwca 2014 roku.

Autor rozprawy doktorskiej, pan Yucel Turel, w latach 1991 – 1995 odbył studia w Southbank University w Londynie (Anglia), gdzie uzyskał tytuł zawodowy magistra (MSc) w dyscyplinie inżynierii systemów informacyjnych (Information System Engineering). Doktorant ma bogate doświadczenie zawodowe w zakresie zarządzania projektami informatycznymi, jak również pewne doświadczenie dydaktyczne (wykłady w zakresie programowania obiektowego w Niemczech oraz bezpieczeństwa teleinformatycznego i kryptografii w Państwowej Wyższej Szkole Informatyki i Przedsiębiorczości w Łomży). Pan mgr Yucel Turel odbywał studia doktoranckie początkowo w University of East London (w latach 2008-2010), a następnie w Polsko-Japońskiej Wyższej Szkole Technik Komputerowych (w latach 2010-2013). Doktorant jest autorem trzech publikacji, w tym jednej opublikowanej w

Przeglądzie Elektrotechnicznym (czasopismo z listy B) oraz jednej pracy, obejmującej główne wyniki uzyskane w rozprawie doktorskiej, złożonej do druku w czasopiśmie *Computing* wydawnictwa Springer. Z powyższych faktów wynika, że spełnione są formalne przesłanki przeprowadzenia przewodu doktorskiego wynikające z Ustawy z dnia 14 marca 2003 roku (z późniejszymi zmianami) o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki.

2. Zakres rozprawy doktorskiej

Tematyka rozprawy doktorskiej pana mgr Yucela Turela jest niezwykle aktualna i należy do obszaru technik informacyjnych prawdopodobnie najintensywniej badanego obecnie zarówno pod kątem architektury i zastosowań, jak i analizy zagadnień bezpieczeństwa. Należy przy tym podkreślić, że mimo tak intensywnych prac problematyka bezpieczeństwa w chmurze obliczeniowej (a to jest kluczowym elementem recenzowanej rozprawy doktorskiej) nie doczekała się jeszcze ugruntowanych standardów zabezpieczeń i rekomendacji wyspecjalizowanych organizacji międzynarodowych dotyczących dobrych praktyk z zakresu bezpieczeństwa. Dlatego też wszelkie propozycje nowych rozwiązań zabezpieczeń w chmurach obliczeniowych są nie tylko oczekiwane, ale też, w przypadku pozytywnej oceny specjalistów, mają szansę na praktyczne wdrożenie.

Rozprawa doktorska pana magistra Yucela Turela dotyczy wykorzystania metod śledczych (forensic methods) do zwiększenia bezpieczeństwa działania chmury obliczeniowej. Autor formułuje tezę, że wśród różnych możliwych metod śledczych stosowanych w chmurze obliczeniowej najbardziej skuteczne jest scentralizowane zbieranie zapisów działań użytkowników (logów) w celu ich analizy. Działanie takie ma służyć przede wszystkim wykrywaniu intruzów (nieuprawnionych użytkowników) i ich szkodliwych działań. W celu wykazania tej tezy Autor rozprawy zaproponował model architektury bezpieczeństwa realizujący powyższy schemat zabezpieczeń, zrealizował praktycznie system zabezpieczeń w sieci testowej i przeprowadził eksperymenty mające potwierdzić sformułowaną w pracy tezę. Badania pana magistra Yucela Turela maja zatem charakter teoretyczno-doświadczalny.

Rozprawa doktorska, łącznie z dodatkami i wszelkimi spisami, liczy 112 stron. Jest napisana w sposób charakterystyczny dla publikacji mających charakter specyfikacji technicznych lub norm, to znaczy zawiera wiele krótkich podrozdziałów odpowiadających

szczegółowym problemom omawianym w rozprawie. Taki sposób zapisu wynika zapewne z doświadczenia zawodowego doktoranta (wieloletnia praca w przemyśle). Jego zaletą jest możliwość precyzyjnego formułowania myśli (w formie stwierdzeń a nie długich prezentacji), co znacznie skraca tekst dokumentu, zarazem jednak wymaga od czytelnika dużej koncentracji podczas czytania tekstu. Rozprawa składa się z 8 rozdziałów oraz zawiera kilka dodatków. Rozdział pierwszy stanowi sformułowanie tematu badań oraz krótkie przedstawienie treści rozprawy. Rozdział 2 zawiera wstęp do pracy: obejmuje omówienie podstaw technologii chmury obliczeniowej, stosowane modele chmury oraz możliwości zastosowań tej technologii, w szczególności w funkcjonowaniu małych i średnich przedsiębiorstw (SME). W zamierzeniu Autora miał on być również przeglądem literatury dotyczącej obliczeń w chmurze, jednak tej roli nie spełnia on w dostateczny sposób (zawiera odnośniki do jedynie 9 pozycji literaturowych w całym rozdziale 2, dotyczące wielu wątków, nie tylko zagadnień podstawowych). W rozdziale trzecim omówiona została koncepcja realizacji chmury obliczeniowej w technologii wirtualizacji, stosowanego do tego oprogramowania, zalety takiego rozwiązania ale również i elementy ryzyka, jakie pojawiają się w takim rozwiązaniu. Rozdział 4 to omówienie podatności chmur obliczeniowych na ataki oraz scharakteryzowanie możliwych ataków. Rozdział ten kończy ogólną część rozprawy naświetlającą problematykę obliczeń w chmurze i ich bezpieczeństwa wynikającego z wykorzystanych technologii teleinformatycznych. Kolejny rozdział 5 zawiera opis koncepcji badań dotyczących śledzenia nadużyć w chmurze obliczeniowej, propozycję architektury systemu eksperymentalnego oraz omówienie wykorzystanych technologii informatycznych. Rozdział 6 jest szczegółowym opisem metod śledczych możliwych do wykorzystania w analizie bezpieczeństwa chmury obliczeniowej, stanowi zatem powrót do części opisowej pracy, tym razem jednak ściśle związanej z tematem badawczym rozprawy i jej tezą. Ostatnie dwa rozdziały rozprawy stanowią główny jej wynik badawczy. Rozdział 7 jest opisem autorskiego rozwiązania zapewniającego możliwość realizacji w chmurze obliczeniowej śledzenia zachowań użytkowników i rejestracji dowodów ich działań (w postaci logów) w celu późniejszej analizy. Z kolei rozdział 8 to opis przeprowadzonych badań eksperymentalnych i wskazania dotyczące praktycznego wykorzystania zaproponowanej metody badawczej. Prace doktorską uzupełniają: wykaz skrótów (w śladowej formie kilku linijek), wykaz publikacji własnych Autora oraz opis jego stażu dydaktycznego, wykaz cytowanej literatury składający się z 95 pozycji, a także dodatki: krótka informacja na temat stanu prawnego w Polsce i Europie dotyczącego zagadnień związanych z technologiami informacyjnymi (jest to opis bardzo ogólnikowy – 1 strona, nie nakreśla tematu w stopniu wystarczającym do bezpiecznego pod względem

prawnym prowadzenia metod śledczych w sieci) i kody źródłowe oprogramowania wykorzystanego przez doktoranta w badaniach eksperymentalnych.

3. Ocena ogólna rozprawy

Rozprawa doktorska pana magistra Yucela Turela ma dwojaki charakter. Z jednej strony jest wprowadzeniem do dziedziny kryminalistyki cyfrowej w chmurach obliczeniowych, z drugiej – jest prezentacją wyników własnych Autora dotyczących tej dziedziny. W obu tych zakresach spełnia ona swoja rolę, jednak zdaniem recenzenta brakuje w niej wyraźnie wyodrębnionego opisu stanu sztuki odnoszącego się nie do wszelkich aspektów funkcjonowanie chmury obliczeniowej i jej bezpieczeństwa, ale ściśle dotyczącego metod wykrywania i dokumentowania ataków w chmurze, czy choćby odesłania czytelnika do publikacji zewnętrznych o takich charakterze (znalazłem np. taką pracę: Farid Daryabar, Ali Dehghantanha, Nur Izura Udzir, Nor Fazlida binti Mohd Sani, Solahuddin bin Shamsuddin, Farhood Norouzizadeh, A Survey About Impacts of Cloud Computing on Digital Forensics, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(2): 77-94, The Society of Digital Information and Wireless Communications, 2013, ISSN 2305-0012). Tym niemniej, część opisowa rozprawy spełnia dobrze rolę ogólnego wstępu pozwalającego czytelnikowi zrozumieć cel i metodologię prowadzonych przez Autora badań.

Głównym wynikiem rozprawy jest propozycja architektury systemu centralnego zbierania logów pozwalająca wykrywać i dokumentować nielegalne działania intruzów w chmurze obliczeniowej działającej według każdego z oferowanych modeli chmury (PaaS, SaaS, IaaS). Architektura ta została zrealizowana w sieci eksperymentalnej i poddana testom uwzględniającym wybrane klasy ataków. Przeprowadzone badania wykazały funkcjonalność zaproponowanej architektury w zakresie przewidzianych scenariuszy i tym samym potwierdziły tezę rozprawy. Z tego punktu widzenia cel badań został osiągnięty. Odrębnym zagadnieniem jest to, czy zaproponowane rozwiązanie znajdzie szerszy oddźwięk w świecie. Obecnie nie ma jeszcze powszechnie obowiązujących standardów w zakresie metod kryminalistyki cyfrowej w chmurach obliczeniowych, więc każda nowa propozycja jest cenna jako krok prowadzący do ich opracowania. W tym miejscu można przedstawić zalety i wady proponowanego rozwiązania w kontekście ogólnych reguł funkcjonowania systemów teleinformatycznych.

Zaproponowany system centralny ma takie zalety jak:

- łatwiejszą ochronę danych niż system rozproszony, a przez to i łatwiejsze spełnienie wymogów prawnych ochrony danych wrażliwych (np. danych osobowych);

- Pewne informacje można uzyskać jedynie analizując globalnie system, a do tego potrzebny jest system centralny gromadzenia danych;
- Szybkie przetwarzanie danych i możliwość szybkiej reakcji na incydenty.

Ograniczeniem systemu może być efekt skali, czyli niemożność gromadzenia wszystkich informacji dla wielkich systemów i dużego natężenia ruchu, podatność jednego punktu centralnego na ataki lub zablokowanie. Możliwym przeciwdziałaniem tym zagrożeniom byłoby wykorzystanie schematów hierarchicznych i tworzenie centrów zapasowych.

Wyniki naukowe uzyskane w rozprawie są przedstawione zwięźle i poprawnie merytorycznie, rysunki są dobrze dobrane i na ogół starannie wykonane. Edycja pracy ma pewne drobne usterki omówione w następnym punkcie recenzji.

4. Uwagi szczegółowe

1. Użycie nazwy Kerberos do autorskiego systemu śledczego (str. 50, Kerberos (three-headed) forensic investigation model) jest niewłaściwe. W obszarze bezpieczeństwa technologii informacyjnych nazwa ta jest powszechnie używana do określenia protokołu centralnego uwierzytelnienia opracowanego w MIT w ramach Projektu Atena zapoczątkowanego w końcu lat 80-tych XX wieku, standaryzowanego (wersja 5) w RFC 1510 (zastąpione przez RFC 4120).

2. Do kilku rysunków zamieszczonych w pracy nie ma bezpośrednich odniesień. Do szeregu z nich są błędne odniesienia:
Strona 13, odnośnik do rys.2 (figure 2), powinno być 2.1,
Strona 31, odnośnik do rys. 3.2, powinno być 3.5,
Strona 40, odnośnik do rys. 1, powinno być 4.1,
Strona 65, odnośnik do rys. 4, powinno być 7.1,
Strona 67, odnośnik do rys. 17, powinno być 7.3.

3. Na stronie 33 (i w kilku innych miejscach) użyty jest zwrot „the internet" z małej litery dla określenia sieci Internet. Jest to błąd językowy: powszechną sieć Internet określamy nazwą własną (a więc z dużej litery), w przeciwieństwie do określenia różnych koncepcyjnych sieci komunikacyjnych nazywanych internetami (wówczas pisanymi z małej litery).

4. W rozprawie używanych jest wiele akronimów dla określenia różnych powtarzanych terminów z zakresu technologii informacyjnych. Jest to oczywiście typowy dla tej dziedziny

sposób prezentacji. W pracy wiele z takich skrótów nie zostało wyjaśnionych w żadnym miejscu (np. SOAP pojawiające się pierwszy raz na str. 15), inne zostały wyjaśnione już po ich pierwszym użyciu (np. IaaS, PaaS, SaaS pierwszy raz występują na str. 15, wyjaśnione są na str. 17). Wyjaśnienie rozwinięcia używanych akronimów przy ich pierwszym użyciu jest istotne, ponieważ często mają one wiele rozwinięć, także w obrębie tej samej dziedziny (w tym wypadku – technologii informacyjnych).

5. W nawiązaniu do poprzedniej uwagi, spis używanych skrótów (akronimów) jest szczątkowy, liczy jedynie 9 pozycji, a używanych jest w pracy kilkadziesiąt różnych skrótów. Brak takiego spisu nie ułatwia czytania pracy.

6. Na stronie 36, w podrozdziale 4.3, przedstawiono szyfrowanie jako metodę ochrony danych użytkownika, w tym danych przeznaczonych do współdzielenia z innymi użytkownikami chmury obliczeniowej. W podrozdziale tym brakuje jednak omówienia problematyki zarządzania tajnymi kluczami, w tym także sposobów współdzielenia kluczy dla zaszyfrowanych współdzielonych plików.

7. W tym samym rozdziale 4, przy okazji omawiania zagrożeń dla bezpieczeństwa danych w chmurze, przedstawiono ataki kryptoanalityczne (nazwane przez Autora niepoprawnie „cryptographic attacks" – powinno być „cryptanalytic attacks" lub ewentualnie „cryptological attacks"). Omówiono te ataki jedynie ze względu na zasób wiedzy posiadanej przez napastnika (i to też w sposób nie wyczerpujący zagadnienia, brak np. ataków adaptacyjnych, z zależnymi kluczami, ataków na podpisy cyfrowe). Nie przedstawiono klasyfikacji ataków ze względu na stosowane techniki obliczeniowe (np. analiza liniowa i różnicowa, ataki algebraiczne, itd.).

8. W rozdziale tym pominięto też całkowicie metody socjotechniczne (por. np. książki Kevina Mitnicka), prawdopodobnie najgroźniejsze w systemach ukierunkowanych na użytkownika, zwłaszcza użytkownika słabo przeszkolonego pod kątem bezpieczeństwa).

9. Wiele rysunków pochodzi z literatury lub jest opracowanych przez Autora rozprawy według wzorów pochodzących z literatury. W większości podpisów do tych rysunków nie podano źródła pochodzenia lub miejsca publikacji oryginału.

10. W pracy występują nieprecyzyjne lub błędne odesłania do innych podrozdziałów, np. na str. 71 podano odnośnik do „section 1.8". W pracy nie ma takiego podrozdziału.

5. Ocena końcowa

W swojej rozprawie doktorskiej pan magister Yucel Turel podjął się analizy zadania bardzo aktualnego i mającego duże znaczenie dla rozwoju współczesnych technik komputerowych. Tematyka prowadzonych przez doktoranta badań niesie w sobie duży potencjał naukowy, w tym także możliwości publikacji wartościowych prac. W zakresie publikacyjnym możliwości wynikające zarówno z podjętej tematyki prac badawczych, jak i z uzyskanych wyników zaprezentowanych w recenzowanej rozprawie, nie zostały przez doktoranta w pełni wykorzystane. Tym niemniej, teza doktorska sformułowana w pierwszym rozdziale rozprawy została potwierdzona poprzez badania teoretyczne i eksperymentalne, a cała rozprawa, będąca w dużym stopniu opracowaniem monograficznym dotyczącym bezpieczeństwa w chmurze obliczeniowej i cyfrowych metod śledczych potwierdza wysokie kompetencje doktoranta w dziedzinie ochrony informacji.

Reasumując, rozprawę doktorską pana magistra Yucela Turela oceniam pozytywnie. Uważam, że spełnia ona wymagania stawiane przez USTAWĘ z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki, Dz.U. z 2003 r. Nr 65, poz. 595; z późniejszymi zmianami, rozprawom doktorskim w dziedzinie nauk technicznych w dyscyplinie naukowej: informatyka i wnioskuję o jej dopuszczenie do publicznej obrony.

Zbigniew Kotulski

Kotulski