dr hab. inż. Franciszek Seredyński
profesor
w Polsko-Japońskiej Wyższej Szkole Technik Komputerowych
ul. Koszykowa 86, 02-008 Warszawa

Warszawa, 10.09.2006

Recenzja

rozprawy doktorskiej mgr Bogdana Księżopolskiego nt.
Bezpieczeństwo i optymalizacja procesów realizowanych drogą elektroniczną

1. Problematyka naukowa oraz przedmiot rozprawy

Recenzowana praca poświęcona jest opracowaniu i zbadaniu skalowanego modelu analitycznego umożliwiającego sterowanie poziomem bezpieczeństwa usług elektronicznych w zależności od poziomu ryzyka wystąpienia nadużycia.

Zaawansowane technologie teleinformatyczne dają obecnie szerokie możliwości rozwoju przemysłu lub usług świadczonych przez instytucje publiczne. Aktualnie duży nacisk kładziony jest na rozwój powszechnie dostępnych usług informacyjnych nazywanych „e-anything", czyli e-urząd, e-pieniądze, e-bankowość. Wspomniane procesy realizowane są głównie drogą elektroniczną, dzięki czemu można zwiększyć ich powszechność, jednocześnie zmniejszając koszty.

Wprowadzenie tych usług w praktyce wiąże się z zagwarantowaniem odpowiedniego poziomu ochrony informacji przesyłanych między uczestnikami danej usługi. Wśród technologii teleinformatycznych oraz modułów kryptograficznych są takie, dzięki którym można zadbać o różne usługi ochrony informacji np.: poufność, integralność, niezaprzeczalność, anonimowość danych. Wszelkie działania na danych w obrębie danej usługi elektronicznej zawarte są w protokołach, które je realizują.

Istotnym problemem jest określenie poziomu ochrony informacji realizowanych usług w danym protokole. Każdorazowe użycie dowolnej usługi internetowej wiąże się z wymianą informacji, co w przypadku udanego ataku stanowi dodatkowe zagrożenie dla całego procesu.

Wybór mechanizmów bezpieczeństwa, które zapewniają stosowny poziom zabezpieczeń jest uzależniony między innymi od stworzonej koncepcji bezpieczeństwa. Wśród głównych komponentów, które są określane w procesie oceny ryzyka można wymienić: zasoby biorące udział w procesie, potencjalne zagrożenia dla zasobów, wrażliwość zasobów, skutki udanego ataku i zastosowane zabezpieczenia.

Konieczne jest ustalenie odpowiednich mechanizmów bezpieczeństwa, za pomocą których określane są poziomy bezpieczeństwa dla poszczególnych faz protokołu realizującego daną usługę.

Recenzowana praca dotyczy nowego podejścia w bezpieczeństwie usług sieciowych. Zaprojektowano model bezpieczeństwa umożliwiający sterowanie poziomem bezpieczeństwa. Zastosowanie tego modelu do procesu nawiązywania połączenia sieciowego przy użyciu protokołu SSL wymaga działań w czterech fazach. W pierwszej fazie następuje inicjalizacja modelu na którą składa się: zdefiniowanie mechanizmów bezpieczeństwa, wyliczenie wartości parametrów dla każdego z nich, utworzenie grafów bezpieczeństwa i przyporządkowanie wartości parametrów do wierzchołków grafu. Fazie druga polega na zdefiniowaniu protokołu kryptograficznego. W fazie trzeciej ustalane są parametry modelu skalowanego bezpieczeństwa dla rozpatrywanej wersji protokołu. Ostatnia faza wymaga obliczenia poziomu bezpieczeństwa dla wszystkich wersji protokołu.

Celem pracy było rozwiązanie następujących problemów:

- opracowanie skalowanego modelu analitycznego, który będzie mógł w optymalny sposób sterować poziomem bezpieczeństwa procesów realizowanych drogą elektroniczną
- stworzenie modeli, na podstawie których będzie można określić prawdopodobieństwo zajścia incydentu w procesach realizowanych drogą elektroniczną oraz wpływ danego ataku na bezpieczeństwo tego procesu
- ukazanie metod optymalizacji procesu elektronicznego poprzez wykorzystanie protokołu kryptograficznego zastosowanego w elektronicznej wersji przetargu.

2. Ocena rozprawy doktorskiej

2.1 Treść rozprawy

Praca składa się z 7 rozdziałów, 2 dodatków oraz bibliografii obejmującej ponad 120 pozycji. W pierwszej części, obejmującej rozdziały 1-2, autor wprowadza czytelnika do problematyki procesów realizowanych drogą elektroniczną i formułuje cel pracy. Druga część, obejmująca rozdziały 3-4, omawia problemy związane z bezpieczeństwem usług oraz przedstawia proponowany model analityczny realizujący skalowane bezpieczeństwo. Dodatkowo zaprezentowany jest przykład użycia modelu dla protokołu SSL v3.0. W trzeciej części pracy, obejmującej rozdziały 5-6, autor prezentuje model nowego protokołu kryptograficznego oraz sposób jego optymalizacji z wykorzystaniem analitycznego modelu skalowanego bezpieczeństwa. Ostatni rozdział zawiera podsumowanie. W dodatku A przedstawiono implementację podprotokołu certyfikacji składnika nowego protokołu kryptograficznego, natomiast dodatek B zawiera opis metody optymalizacji działania sieci sensorowych.

Rozdział 1 pracy zawiera wprowadzenie do problematyki bezpieczeństwa usług realizowanych drogą elektroniczną. Omówiono w nim, na ogólnym poziomie, istotne elementy od których uzależniony jest poziom bezpieczeństwa. Ponadto doktorant przedstawia cel pracy, omawia strukturę pracy doktorskiej oraz prezentuje spis używanych skrótów.

Rozdział 2 pracy traktuje o społeczeństwie informacyjnym, projektach rządowych, których celem jest rozwój społeczeństwa informacyjnego. Dalej, na ogólnym poziomie przedstawione są opisy

realizowanych projektów oraz przedsięwzięć komercyjnych. Zaprezentowano również czynniki, które hamują rozwój społeczeństwa informacyjnego.

Rozdział 3 opisuje elementy bezpieczeństwa informacji. Autor prezentuje modele komunikacji w sieciach komputerowych, co stanowi punkt wyjścia do zdefiniowania zagrożeń w procesach elektronicznych. W celu podkreslenia wagi problemu, posłużono się wynikami badań polskiego oddziału CERT monitorującego naruszenia ochrony informacji. Autor przybliżył znane usługi i mechanizmy ochrony informacji. Rozdział kończy się przeglądem literatury traktującej o skalowalności bezpieczeństwa. Przybliżone modele określają jedynie ryzyko ataku, brak jest natomiast modeli uwzględniających mechanizmy bezpieczeństwa, jakie należy stosować dla różnych poziomów ryzyka. W związku z tym, w pracy zaproponowano model bazujący na łatwo mierzalnych parametrach określających ryzyko wystąpienia zagrożenia z uwzględnieniem stosowanych mechanizmów bezpieczeństwa.

Rozdział 4 jest pierwszym rozdziałem pracy przedstawiający wyniki własne doktoranta. Prezentuje on proponowany model analityczny realizujący skalowane bezpieczeństwo. Autor przedstawił założenia modelu, zdefiniował szereg parametrów modelu oraz formuły matematyczne do wyliczania wartości tych parametrów. W rozdziale opisane są również poziomy zabezpieczeń, sposoby obliczania prawdopodobieństwa zajścia incydentu oraz jego wpływu na atakowany system. Istotnym elementem jest sposób obliczania poziomu bezpieczeństwa. Autor na koniec rozdziału przedstawia przykład zastosowania opracowanego modelu dla protokołu kryptograficznego SSL v.3.00.

Rozdział 5 zawiera opis metody optymalizacji nowego protokołu elektronicznego przetargu z wykorzystaniem modelu skalowanego bezpieczeństwa. Autor przedstawił typy aukcji Internetowych oraz wykorzystywane obecnie protokoły kryptograficzne realizujące aukcje przetargowe. Na bazie aktualnego stanu wiedzy, przedstawiono model nowego protokołu realizującego przetargi, który poddano optymalizacji ze względu na wydajność i dostępność stosując do tego celu zdefiniowany w rozdziale 4 model skalowany bezpieczeństwa. W rozdziale omówiono algorytm postępowania do poprawnego zastosowania modelu analitycznego do optymalizacji algorytmu.

W rozdziale 6 autor prezentuje automatyczny mechanizm rozstrzygania przetargów dla nowego protokołu kryptograficznego w oparciu o system wspomagania decyzji. Autor zaprezentował model wspomagania decyzji bazujący na programowaniu celowym. W pierwszym kroku podejmowana jest decyzja, w kroku drugim zwiększana jest jakość otrzymanych wyników. Rozdział zawiera wyniki eksperymentalne jako rezultat przeprowadzonych badań.

W rozdziale 7 przedstawiono podsumowanie oraz wskazano dalsze kierunki prac.

2.2 Najważniejsze wyniki uzyskane w rozprawie

Przedstawione w rozprawie wyniki w pełni realizują jej cel, zarówno w zakresie opracowania modelu skalowanego bezpieczeństwa jak i zastosowania go do protokołu kryptograficznego SSL v3.00. Otrzymane wyniki potwierdzają, że dzięki mechanizmom określającym poziom ryzyka można sterować poziomem bezpieczeństwa.

Do najważniejszych osiągnięć pracy można zaliczyć:

- opracowanie modelu analitycznego realizującego skalowane bezpieczeństwo uwzględniającego mechanizmy zabezpieczeń, pozwalającego na wybór zabezpieczeń w zależności od ryzyka wystąpienia włamania
- opracowanie nowego protokołu kryptograficznego realizującego elektroniczną formę przetargu
- zastosowanie zapronowanej koncepcji skalowanego bezpieczeństwa do wybranych protokołów kryptograficznych i pokazanie uzyteczności modelu skalowanego bezpieczeństwa
- opracowanie procedury optymalizacji usług elektronicznych mającą na celu zwiększenie wydajności i bezpieczeństwa usług elektronicznych

2.3 Uwagi krytyczne

Uwagi krytyczne odnoszące sie do merytorycznych aspektów pracy są następujące:

- duża liczba parametrów proponowanego modelu skalowanego bezpieczeństwa wymaga określenia ich wartości w sposób praktycznie subiektywny. Są to np. takie parametry jak (a) indywidualny wkład mechanizmu bezpieczeństwa do globalnej ochrony danych (tab. 4.1, str. 39), (b) parametr wrażliwości (str. 41), (c) wielkość zasobów zdobytych podczas udanego ataku (str. 43), (d) wymagany poziom wiedzy atakującego oraz wymagane koszty poniesione przez atakującego (str. 43), itp. Konsekwencją tego może być nieadekwatna do rzeczywistości ocena bezpieczeństwa szacowana przez proponowany model
- nie jest jasne na jakiej podstawie wykonano wykres przedstawiony na rys. 4.1 ukazujący zależność poziomu zabezpieczeń od parametrów. Rysunek ten nie poprzedza w pracy ewentualna zależność funkcyjna między parametrami a poziomem zabezpieczeń
- doktorant przedstawia w pracy szereg empirycznych wzorów (np. (4.2), (4.9), (4.10)) nie podając ich uzasadnienia merytorycznego, posiłkując się jedynie formułką, stwierdzającą, że zostały one opracowane 'na podstawie wiedzy w tej dziedzinie nauki ... oraz intuicji autora wspomaganej przez wiele przeprowadzonych testów' (str. 66)

Przestawione wyżej uwagi nie wpływają znacząco na moją pozytywną ocenę rozprawy.

2.4 Ocena redakcji rozprawy

Praca zredagowana jest przejrzyście, a wywód poprowadzony jest logicznie. Styl językowy pracy nie budzi zastrzeżeń. W trakcie czytania pracy zauważyłem kilka niedociągnięć redakcyjnych:

- na str. 33 jest 'zostały krótko opisana' zamiast 'zostały krótko opisane'
- na str. 38 jest 'Każdy mechanizmu bepieczeństwa' zamiast 'Każdy mechanizm bezpieczeństwa'
- na str. 39 jest 'zabezpieczenie' zamiast 'zabezpieczeniem'
- na str. 42 jest 'być zastosowany' zamiast 'być zastosowana'
- na str. 59 jest 'jaki wpływa na' zamiast 'jaki wpływ ma'
- na str. 60 jest 'danego element' zamiast 'danego elementu'
- na str. 66 jest 'W pierwszy' zamiast 'W pierwszym'
- na str. 98 jest 'wybrany' zamiast 'wybranych'

3. Konkluzja

Postawione w pracy cele zostały przez doktoranta osiagnięte. Zbudował on oryginalny model skalowalnego bezpieczeństwa usług elektronicznych i pokazał jego praktyczną przydatność. Wyniki pracy były przedstawiane na kilku międzynarodowych konferencjach i publikowane w materiałach tych konferencji, jak też były publikowane w krajowych czasopismach.

Podsumowując, uważam, że recenzowana rozprawa zawiera oryginalne i interesujące wyniki teoretyczne jak i praktyczne. Uzyskane wyniki stanowią znaczący wkład doktoranta do teorii i praktyki problematyki związanej z bezpieczeństwem usług realizowanych drogą elektroniczną.

Jestem przekonany, że wymagania stawiane rozprawom doktorskim przez obowiązującą Ustawę o Stopniach i Tytułach Naukowych zostały w pełni spełnione. Wnoszę więc o dopuszczenie mgr Bogdana Księżopolskiego do publicznej obrony jego pracy.