Doc dr hab. Marian Srebrny
Profesor Wyższej Szkoły Handlowej w Kielcach
Instytut Podstaw Informatyki PAN
Ordona 21, 01-237 Warszawa
marians@ipipan.waw.pl

Warszawa, 21.11.06

RECENZJA
rozprawy doktorskiej mgr Bogdana Księżopolskiego
pt. *Bezpieczeństwo i optymalizacja procesów realizowanych drogą elektroniczną*

Rozprawa mgr Bogdana Księżopolskiego poświęcona jest kryteriom projektowania systemów zabezpieczeń dużych procesów obliczeniowych. Przedmiotem rozprawy są zabezpieczenia dużych rozproszonych procesów obliczeniowych realizowanych przez oprogramowanie o wysokim stopniu złożoności - wielu uczestników, wiele możliwych współbieżnych zachowań. Procesy takie wymagają zabezpieczeń o rozmaitej mocy kryptograficznej. Niektóre praktyczne sytuacje wymagają bardzo solidnego, mocnego kryptograficznie systemu zabezpieczeń, inne niekoniecznie. Przykładami motywacyjnymi mogą tu być procesy obliczeniowe często spotykane obecnie w dziedzinie gospodarki elektronicznej; na przykład, e-aukcja, albo e-przetarg.

Na ogół koncentrujemy uwagę na pojedynczych mechanizmach zabezpieczeń - kryptograficznych algorytmach i modułach. Obecnie zwraca się coraz więcej uwagi na poprawność całości projektów systemów oprogramowania, nie tylko poszczególnych mechanizmów składowych. Recenzowana rozprawa jest w tym nowoczesnym nurcie badań.

Kiepska konstrukcja oprogramowania całego procesu może podważyć wiarygodność przyjętego systemu zabezpieczeń, nawet mimo wysokiej efektywności i mocy kryptograficznej poszczególnych składników. Nawet jeśli wszystkie składowe systemu zabezpieczeń działają poprawnie, nadal nie daje to gwarancji poprawności, wiarygodności całego systemu. Osłabienie odporności na potencjalne ataki może być rezultatem trudnych do przewidzenia przeplotów wykonań poszczególnych modułów oprogramowania. Projektowanie dużych systemów wymaga analizy interakcji pomiędzy poszczególnymi modułami kryptograficznymi, analizy całości procesu. Znane są liczne przykłady znalezienia luk w zabezpieczeniach nowo proponowanych w literaturze systemów oprogramowania. Patrz, na przykład: Boyd i Mao *Security issues for electronic auctions*, 2000; Franklin i Reiter *The design and implementation of a secure auction service*, 1996; Naor et al. *Privacy preserving auctions and mechanism design*, 1999; Boyd et al. *A Three Phased Schema for Sealed Bid Auction System Design*, 2000; Boyd et al. *Defining Security Services for Electronic Tendering*, 2004; J. Trevathan *Design issues for electronic auctions*, 2005.

Szczególnie interesującą linią badań są protokoły z zabezpieczeniami bez centrali, nazywanej trzecią stroną obdarzoną zaufaniem wszystkich uczestników procesu. (Patrz, na przykład, S. G. Stubblebine i P. F. Syverson *Fair On-line Auctions Without Special Trusted Parties*, 1999.)

Najważniejsze wyniki rozprawy dotyczą *skalowalności* projektów systemów zabezpieczeń Termin „skalowalność" nie jest właściwie zdefiniowany w rozprawie. Stosowany jest przez autora w nieco innym znaczeniu niż normalnie. Nie chodzi o możliwość skalowania systemów w sensie zwiększania/zmniejszania liczby uczestników, podprocesów albo

komputerów w systemie tylko o możliwe zestawy modułów oprogramowania zabezpieczającego. Na przykład, można zabezpieczać poufność dokumentów tylko przez szyfrowanie. Można dodatkowo do szyfrowania wymagać jeszcze jakiegoś rodzaju sumy kontrolnej tego dokumentu; otrzymywanej z ustalonej funkcji skrótu (ang. hash function). Dodatkowo, autor albo nadawca jakiegoś dokumentu może jeszcze własnym podpisem elektronicznym potwierdzać autentyczność i integralność tego dokumentu. I tak dalej. Każdy z tych mechanizmów zabezpieczających można realizować rozmaitymi algorytmami i modułami kryptograficznymi. Możliwość dobierania ich zestawów nazywana jest w tej rozprawie „skalowalnym bezpieczeństwem".

Zawartość rozprawy

Recenzowana rozprawa liczy 173 strony, składa się z siedmiu rozdziałów, dwóch dodatków oraz bibliografii zawierającej 123 pozycje.

W rozdziale pierwszym, po krótkim wprowadzeniu, przedstawiono główne cele rozprawy wraz z ich uzasadnieniem oraz przedstawiono strukturę pracy.

W rozdziale drugim zaprezentowano ogólną charakterystykę procesów realizowanych drogą elektroniczną, rodzaje usług elektronicznych oraz wymagania dotyczące ich zabezpieczeń.

W rozdziale trzecim przedstawiono ogólne informacje dotyczące ochrony informacji. Omówiono modele komunikacyjne, występujące w nich zagrożenia oraz wyodrębniono te zagrożenia, które są najważniejsze dla sprawnego działania infrastruktury teleinformatycznej. Następnie przeanalizowano zagadnienia związane z zabezpieczaniem procesów realizowanych drogą elektroniczną, a zwłaszcza usługi ochrony informacji oraz mechanizmy, moduły kryptograficzne, które je realizują. Wprowadzono pojęcie protokołów kryptograficznych i ich rodzajów. Na zakończenie rozdziału uzasadniono potrzebę stosowania „skalowalnego bezpieczeństwa" i przedstawiono przegląd literatury na temat głównego zagadnienia poruszanego w rozprawie, czyli metod realizujących skalowane bezpieczeństwo.

W rozdziale czwartym zaproponowano kilka równań dotyczących szacowania prawdopodobieństwa wystąpienia zagrożeń, nazywając to modelem realizującym skalowalne bezpieczeństwo. W szczególności opisano modele: obliczania prawdopodobieństwa zajścia incydentu, określenia wpływu udanego ataku na system oraz ogólny model skalowanego bezpieczeństwa, za pomocą którego obliczane są możliwe poziomy bezpieczeństwa. W tym rozdziale przedstawiono również schemat postępowania dla proponowanej metody wprowadzenia skalowanego bezpieczeństwa. Na zakończenie rozdziału przedstawiono ilustracyjny przykład zastosowania proponowanego schematu postępowania dla znanego protokołu SSL (w wersji 3.00).

W rozdziale piątym przedstawiono optymalizację zabezpieczeń protokołu elektronicznego przetargu z wykorzystaniem metodologii „skalowanego bezpieczeństwa". Rozdział zaczyna się od omówienia literatury na temat stanu wiedzy dotyczącej protokołów kryptograficznych realizujących elektroniczną formę przetargu. W dalszej jego części zaproponowany jest nowy protokół kryptograficzny realizujący elektroniczny przetarg. Głównym wynikiem przedstawionym w tym rozdziale jest zastosowanie utworzonego wcześniej modelu „skalowanego bezpieczeństwa" dla nowego protokołu e-przetargu.

W rozdziale szóstym zaprezentowano optymalizację mechanizmu rozstrzygnięcia przetargu dla nowego protokołu kryptograficznego realizującego e-przetarg, pozwalającą wyłączyć udział człowieka z procedury decyzyjnej.

Na zakończenie, w rozdziale siódmym podsumowano badania przedstawione w rozprawie oraz przedstawiono końcowe wnioski.

Rozprawa ma też dwa dodatki. Dodatek A zawiera opis implementacji jednego z podprotokołów zaproponowanego protokołu realizującego przetarg elektroniczny i jego testy wydajnościowe. Dodatek B przedstawia sieci sensorowe jako przykład możliwych zastosowań wykorzystujących pojęcie skalowanego bezpieczeństwa.

Wyniki

Zaproponowany został model skalowanego bezpieczeństwa, który w zależności od potencjalnego ryzyka systemu wyznacza potrzebny do tego poziom wiarygodności jego zabezpieczeń. Przedstawiony model składa się z następujących trzech składowych: model obliczania prawdopodobieństwa zajścia incydentu, model wpływu udanego ataku na system oraz model określający poszczególne poziomy zabezpieczeń dla danej wersji protokołu.

Zaprezentowano nowy protokół kryptograficzny realizujący elektroniczną formę przetargu. Na przykładzie tego protokołu autor zilustrował metodę skalowanego bezpieczeństwa. Proponowana metodologia skalowanego bezpieczeństwa została również zastosowana do znanego protokołu kryptograficznego SSL (w wersji 3.00).

Zaproponowany model teoretyczny skalowanego bezpieczeństwa został doprowadzony do postaci implementowalnej; zostało to osiągnięte dzięki zastosowaniu grafów, list wyborów (ang. checklist) oraz wprowadzeniu łatwo modyfikowalnych, intuicyjnych parametrów. Realizujący go moduł mógłby funkcjonować jako warstwa pośrednia między warstwą użytkownika (aplikacji) a warstwą systemu. Wierzchołki wspomnianych grafów etykietowane są poszczególnymi mechanizmami kryptograficznych zabezpieczeń, tzn. nazwami znanych szyfrów, funkcji skrótu, algorytmów podpisu cyfrowego itd. W taki sposób, że ścieżka grafu jest zestawem mechanizmów kryptograficznych.

Uwagi krytyczne

Nie widać w rozprawie oszacowania złożoności obliczeniowej ani dowodów poprawności. Zmiany w dużym, złożonym protokole mogą powodować istotny narzut obliczeniowy (ang. computational overhead) i komunikacyjny; tzn. mogą powodować istotne powiększenie rozmiaru protokołu, jego przestrzeni możliwych (osiągalnych) stanów, czasu wykonywania, niezbędnych zasobów pamięci. Dotyczy to w szczególności protokołów SSL, zabezpieczonej obsługi przetargu elektronicznego, sieci czujników. Protokół e-przetargu zaproponowany w rozdziale 5 rozprawy też wymaga oszacowania złożoności i dowodu poprawności. Bez dodatkowych założeń ograniczających zakres stosowania takiego protokołu w praktyce, można – jak sądzę – spodziewać się wykładniczo rosnącej liczby komunikatów informacji wymienianych w trakcie wykonywania takiego protokołu. Dotyczy to szczególnie protokołów aukcji wielokryterialnych.

Dobieranie zestawu zabezpieczeń protokołu SSL przeprowadzone jest „ręcznie" w części 4.7 rozprawy, ważne decyzje podejmuje człowiek, mimo deklarowanej możliwości

zautomatyzowania skalowaności. Dotyczy to też protokołu e-przetargu. Dla sieci czujników, model skalowanego bezpieczeństwa jest w rozprawie tylko zasygnalizowany jako interesujący pomysł.

Rys. 4.1 w części 4.2.1 jest właściwie sposobem zadania, zdefiniowania funkji L^Z przez podanie jej wykresu (trójwymiarowego, bowiem jest to dwuargumentowa funkcja od L i Z). Nie ma żadnego objaśnienia, dlaczego właśnie taki kształt ma ta powierzchnia. Podobne uwagi odnoszą się do kilku wzorów, które razem autor nazywa analitycznym modelem skalowanego bezpieczeństwa. Wzory te nie są wyprowadzone, tylko odzwierciedlają intuicje, symulacje i doświadczenie autora. Owe intuicje i symulacje nie są przytoczone w rozprawie.

Interesujące byłoby krótkie porównanie z najważniejszymi znanymi protokołami e-przetargu; na przykład, z krążącego od kilku lat i stale aktualizowanego przeglądu najważniejszych pozycji literatury z tego zakresu tematycznego: *Electronic auctions literature review* J. Trevathana. W Polsce najważniejsza wydaje się funkcjonująca obecnie z powodzeniem implementacja systemu e-przetargu Państwowej Wytwórni Papierów Wartościowych, PWPW.

Terminologia przyjęta w rozprawie wydaje się trochę myląca. Skalowalne bezpieczeństwo to raczej *elastyczność* (ang. *flexibility*) systemu, pozwalająca dobierać zestawy zabezpieczeń odpowiadające faktycznym potrzebom w danej rzeczywistej sytuacji. (Patrz, na przykład, J.D. Tygar et al. *A Flexible and Secure Auction Architecture Using Trusted Hardware*, 1991.)

Rozprawa napisana jest dość starannie i przejrzyście, choć nie jest pozbawiona błędów: literówek, błędów w interpunkcji itp. Trafiają się też błędy w oznaczeniach we wzorach ważnych dla merytorycznej dramaturgii rozprawy.

Powyższe uwagi krytyczne nie zmieniają ogólnej pozytywnej opinii o tej rozprawie

Konkluzja

Rozprawa spełnia wymagania stawiane rozprawom doktorskim w Polsce zgodnie z obowiązującą ustawą o stopniach i tytule naukowym. Wnoszę o dopuszczenie mgr Bogdana Księżopolskiego do dalszych etapów przewodu doktorskiego.