XXI Seminarium

ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE' 2011
Oddział Gdański PTETiS
Referat nr 13

MECHANIZM ZAPEWNIANIA WIARYGODNOŚCI STRON INTERNETOWYCH

Jerzy KACZMAREK[1], Michał WRÓBEL[2]

1. Wydział Elektroniki, Telekomunikacji i Informatyki, Politechnika Gdańska
   tel: (58) 347 26 82 fax: (58) 347 27 27 e-mail: jkacz@eti.pg.gda.pl
2. Wydział Elektroniki, Telekomunikacji i Informatyki, Politechnika Gdańska
   tel: (58) 347 10 37 fax: (58) 347 27 27 e-mail: wrobel@eti.pg.gda.pl

Streszczenie: Zapewnianie wiarygodności danych w Internecie to ważne zagadnienie współczesnej informatyki. Dynamiczny rozwój globalnej sieci komputerowej pociąga za sobą zarówno ogromne korzyści, jak i poważne zagrożenia. Jednym z zagrożeń jest brak wiarygodności stron internetowych zarówno z punktu widzenia wiarygodności dostawcy, jak również możliwości nieautoryzowanej zmiany treści. W artykule przedstawiono niektóre mechanizmy zapewniania wiarygodności stron WWW takie jak podpis cyfrowy, kryptograficzne podpisywanie mikrotreści czy pieczęcie kontrolne. Opisano wykonany system realizujący mechanizm pieczęci weryfikującej niezmienność treści, oparty na wyliczaniu kryptograficznej sumy kontrolnej pliku. Podano zasadę działania systemu oraz wybrane aspekty projektowe takie jak diagramy UML oraz interfejs użytkownika. Rozważono również skuteczność i praktyczną przydatność takiego rozwiązania.

Słowa kluczowe: wiarygodność, bezpieczeństwo, pieczęcie

1. WSTĘP

Internet staje się podstawowym źródłem dowolnego typu informacji oraz powszechnym sposobem przeprowadzania transakcji gospodarczych. Zapewnianie wiarygodności danych i transakcji internetowych to bardzo ważne zagadnienie współczesnej informatyki [1]. Zapewnienie wiarygodności można podzielić na bezpieczeństwo infrastruktury Internetu oraz wiarygodność przekazywanych i publikowanych danych.

Zagrożenia sieci Internet polegają na potencjalnej możliwości nielegalnego dostępu do zasobów, przekłamania w przekazywaniu danych czy podsłuchu transmisji. Istnieją możliwości kradzieży tożsamości zarówno indywidualnych użytkowników, jak również dużych firm, w tym banków. Bardzo groźne i trudne do wyeliminowania są ataki typu DoS (ang. Denial of Service) prowadzące do odmowy dostępu do wybranych serwerów w wyniku sztucznie wygenerowanego dużego ruchu w sieci.

Wiarygodność danych publikowanych w Internecie zależy od dwóch czynników. Pierwszy wynika z moralnego imperatywu podawania informacji prawdziwych. Warunek ten wcale nie jest dla wszystkich oczywisty ani bezwzględnie przestrzegany.

Drugim czynnikiem jest istniejąca realnie możliwość wrogiej, czy nieautoryzowanej zmiany treści stron internetowych. O tym, czy strona internetowa jest wiarygodna może zadecydować wiele czynników, zarówno technicznych, jak również psychologicznych, ponieważ jest to rodzaj przeświadczenia, że serwis jest godny zaufania. Można wyróżnić kilka czynników, które umacniają zaufanie do strony internetowej czy serwisu. Należą do nich znajomość i renoma firmy, której strona jest odwiedzana, profesjonalny wygląd serwisu, umieszczenie znaków firm poświadczających wiarygodność strony, poziom jakości interfejsu użytkownika, forum użytkowników i inne.

Użytkownicy w celu weryfikacji informacji znajdującej się na stronie internetowej powinni zawsze odpowiedzieć sobie na kilka podstawowych pytań takich jak: czy stronie zostały przyznane certyfikaty znanych instytucji, jaka jest opinia o posiadaczu strony, czy informacje mają podane źródła pochodzenia, czy strona jest dobrze zorganizowana, czy grafika prezentowana jest adekwatna do informacji wyświetlanej, kiedy została opublikowana strona, czy dane serwisu są uaktualniane, czy są linki do stron o podobnej tematyce. Powody powstawania zagrożeń wiarygodności serwisów internetowych wynikają w większości z nieostrożności użytkowników, błędów człowieka, zwłaszcza administratora, braku aktualizacji treści, złych systemów zabezpieczających oraz błędów w używanych aplikacjach.

Zagadnienie zapewniania bezpieczeństwa danych w Internecie jest przedmiotem licznych prac naukowych, teoretycznych oraz wdrożeniowych. Jednym z ciekawszych rozwiązań o dużej możliwości wdrożenia i perspektywach powszechnego zastosowania jest umieszczanie na stronach pieczęci weryfikujących. Pozwalają one użytkownikowi na sprawdzenie, czy treść strony nie uległa zmianie w sposób nieautoryzowany. Weryfikacja następuje na serwerze firmy świadczącej tego typu usługi. Firma taka powinna mieć profesjonalnie zabezpieczony system informatyczny, jak również posiadać certyfikaty bezpieczeństwa. Zasady działania wykonanego systemu realizującego pieczęcie weryfikacyjne oraz opis jego konstrukcji stanowi przedmiot tego artykułu.

Recenzent: Prof. dr hab. inż. Wojciech Jędruch – Wydział Elektroniki, Telekomunikacji i Informatyki Politechnika Gdańska

2. ZAPEWNIANIE WIARYGODNOŚCI

Metody zapewniania wiarygodności danych publikowanych w Internecie polegają na informowaniu użytkownika przeglądającego stronę, że jej wiarygodność jest kontrolowana przez niezależną od dostawcy informacji instytucję. Sposoby, jakimi użytkownik jest informowany o istnieniu takich mechanizmów zabezpieczających mogą być różne. Do najbardziej popularnych należą: pasek bezpieczeństwa (ang. security toolbar), podpis elektroniczny, kryptograficzny podpis mikrotreści, cyfrowy znak wodny oraz pieczęć wiarygodności.

Security toolbar to niewielki pasek informujący użytkownika, że wiarygodność strony została sprawdzona przez instytucje do tego powołane, jest pewnym sposobem ochrony użytkownika, przed groźnym a obecnie często stosowanym atakiem typu phishing [2]. Pasek bezpieczeństwa działa w oparciu o bazę danych budowaną i kontrolowaną przez instytucję realizującą tego typu usługę. Takich instytucji jest już obecnie kilka. W bazie danych powiązanej z paskiem bezpieczeństwa znajdują się informacje o stronach i serwisach bezpiecznych, fałszywych czy dobrze ocenianych przez użytkowników. Znajdują się również adresy URI serwisów o potwierdzonej przez niezależne instytucje wiarygodności. Podstawą działania takiego paska bezpieczeństwa są informacje o ocenie wiarygodności dostawcy danych internetowych. Wyniki klasyfikacji dostawców zależą od przyjętej metody oceny, od niej też zależy skuteczność tego mechanizmu.

Podpis elektroniczny jest stosunkowo skutecznym sposobem zapewniania, że dane publikowane nie zostały zmienione od chwili ich podpisania. Niemniej jednak nie zapewnia on wiarygodności danych i w tym sensie nie jest lepszy do security toolbar. Metoda podpisu elektronicznego opiera się na mechanizmie kryptografii. Używa się w nim klucza prywatnego do szyfrowania, a publiczny do odszyfrowania. W procesie podpisu elektronicznego uczestniczy niezależna instytucja, jaką jest urząd certyfikujący.

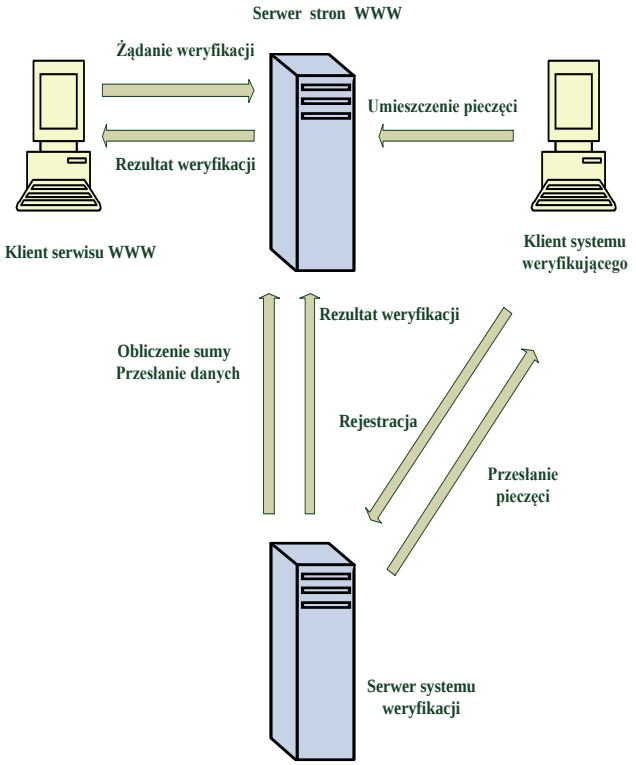
Kryptograficzne podpisywanie mikrotreści polega na dodaniu do strony internetowej dodatkowych informacji dotyczących struktury logicznej i semantycznej dokumentu. Struktura taka jest opisana w formie manifestu i może być odczytywana zarówno przez ludzi jak i przez systemy komputerowe działające w sieci semantycznej. Po opracowaniu mikrotreści jest ona kryptograficznie podpisywana. Metoda ta pozwala na zmiany w treści dokumentu również przez osoby inne niż autor dokumentu, ale jedynie w miejscach dozwolonych, wybranych uprzednio przez autora dokumentu.

Cyfrowe znaki wodne wykorzystywane są głównie w informacjach multimedialnych takich jak filmy, obrazy czy pliki audio. Ich zadaniem jest nie tylko zapewnianie wiarygodności i niezmienności danych, ale również kontrola ich udostępniania. Znaki wodne mogą zawierać dane o autorze pliku, informacje o możliwościach kopiowania, czy liczbie wykonanych kopii. Zasadniczą cechą znaków wodnych jest to, że są niezauważalne dla użytkownika.

Pieczęć wiarygodności, to widoczny na stronie internetowej symbol graficzny, po naciśnięciu, którego użytkownik uzyskuje pewność, że treść danej strony nie została zmieniona w sposób nieuprawniony. Wydaje się, że mechanizm pieczęci może być powszechnie wykorzystywany w przyszłości i dlatego zdecydowano się na podjęcie prac nad prototypem takiego systemu.

3. METODA PIECZĘCI WERYFIKACYJNEJ

Zasada działania systemu nakładania pieczęci na strony serwisów internetowych opiera się na istnieniu trzeciego podmiotu, sprawdzającego czy dane w serwisie dostawcy nie zostały zmienione w sposób nieautoryzowany. Użytkownikowi korzystającego z przeglądarki, wyświetlona zostaje pieczęć informująca, że dana strona internetowa ma mechanizmy sprawdzające jej wiarygodność. Klient ma możliwość naciśnięcia na umieszczony na stronie specjalny znaczek, co spowoduje uruchomienie mechanizmu weryfikacji. Sprawdzana jest wtedy w bazie danych instytucji weryfikującej integralność danych umieszczonych na stronie oglądanej przez użytkownika. Schemat działania mechanizmu pieczęci weryfikującej pokazano rysunku 1.



Rys. 1. Działanie systemu pieczęci weryfikującej

Kompletny działający system weryfikujący składa się z dwóch podsystemów. Najważniejszym z nich jest serwis dostarczany przez instytucję do tego powołaną. W bazie danych serwisu instytucji weryfikującej przechowywane są dane o treści stron internetowych publikowanych przez dostawcę danych. Informacje o zawartości stron zapisywane są w formie kryptograficznych sum kontrolnych zwaną wzorcem pliku.

Drugi podsystem umieszczony jest po stronie posiadacza serwisu internetowego. Oblicza on sumy kontrolne plików zawierających strony internetowe i przesyła je do systemu weryfikującego. Implementacja i język programowania, w jakim wykonany jest taki podsystem, zależą od środowiska programistycznego posiadacza serwisu internetowego.

Użytkownik przeglądający strony serwisu internetowego może zażądać sprawdzenia, czy treść strony nie uległa zmianie poprzez naciśnięcie symbolu pieczęci. Poprawna weryfikacja ma pozytywny aspekt psychologiczny, co jest dużą zaletą takich rozwiązań.

4. SYSTEM Z PIECZĘCIĄ WERYFIKACYJNĄ

Wykonanie systemu z pieczęcią weryfikacyjną wymagało podjęcia pewnych decyzji projektowych. Technologie, w jakich takie systemy mogą być wykonane są typowe dla zastosowań internetowych. Opisywany system wykonano w technologii Java.

Należy podjąć decyzję o sposobie wyznaczania skrótów kryptograficznych. Dane publikowane w Internecie przechowywane są na serwerach w formie plików. W plikach zawarte mogą być zarówno dane tekstowe jak również multimedialne. Powstaje, zatem problem jak wyznaczyć kryptograficzny skrót pliku, który zagwarantuje, że dane na stronie nie zostały zmienione w sposób nieuprawniony. Niestety do budowy skrótu kryptograficznego wykorzystywane są jedynie dane tekstowe. Metoda wyznaczania wzorca powinna charakteryzować się tym, że każda zmiana w pliku prowadzi zawsze do wygenerowania innego wzorca. Wygenerowanie zawartości pliku na podstawie wzorca ma być zadaniem obliczeniowo niewykonalnym. Operacja wyznaczania wzorca musi być wydajna, nawet dla dużych plików.

Najczęściej stosowanymi funkcjami skrótu kryptograficznego jest funkcja MD5 (ang. Message-Digest algorithm 5), oraz funkcja SHA1 (ang. Secure Hash Algorithm) i jej modyfikacje. Funkcja MD5 została wykorzystana w wykonanym systemie zapewniania wiarygodności stron z wykorzystaniem pieczęci.

Inną decyzją projektową jest wybranie formy graficznej pieczęci weryfikacyjnej. Może być ona dowolna, ale z uwagi na nazwę metody, opracowano znak w formie tradycyjnej pieczęci znanej ze starych historycznych dokumentów. Kształt pieczęci weryfikacyjnej przedstawiono na rysunku 2.

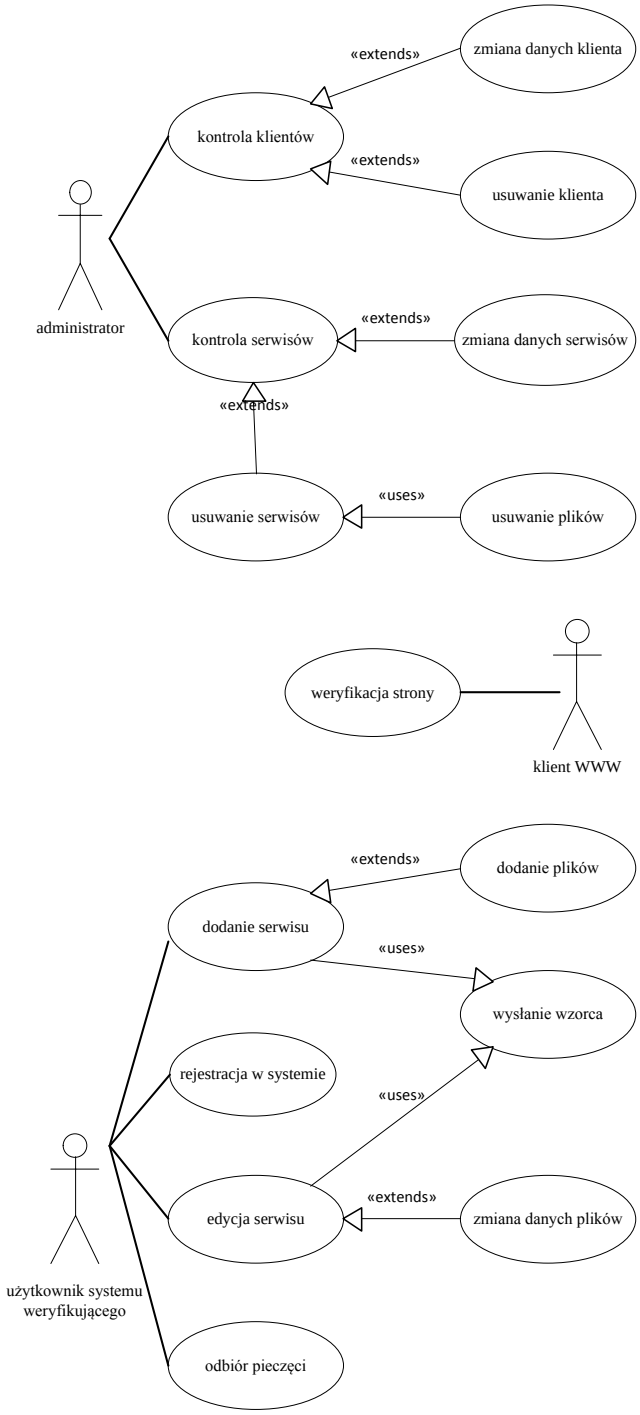
Rys. 2. Wzór pieczęci weryfikacyjnej

Pieczęć może mieć trzy kolory. Po uruchomieniu przez dowolnego użytkownika strony serwisu internetowego w przeglądarce, pieczęć na stronie ma kolor czarny. Jej naciśnięcie powoduje uruchomienie mechanizmu weryfikacji. Poprawna weryfikacja objawia się kolorem zielonym wewnątrz pieczęci, niepoprawna czerwonym. Zmiana kolorów jest również informacją dla użytkownika, że system zabezpieczający działa poprawnie.

4.1. Przypadki użycia systemu weryfikującego

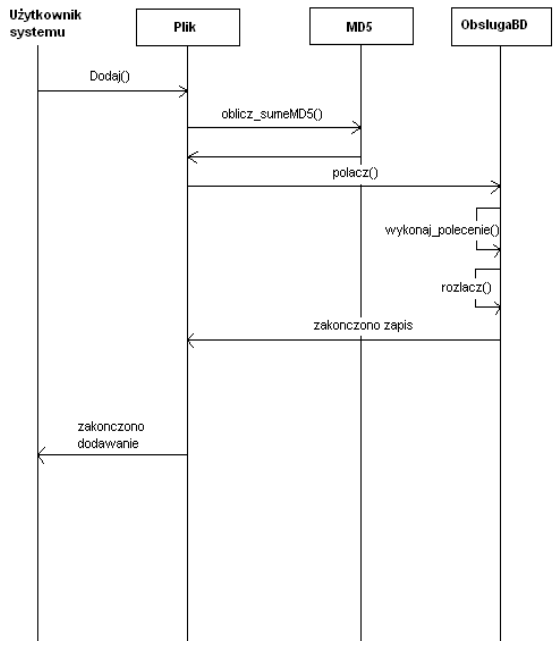
Przypadki użycia przedstawiono na rysunku 3. System weryfikacji stron internetowych z wykorzystaniem pieczęci ma trzech użytkowników. Należy do nich dowolny klient przeglądający strony internetowe, dostawca danych oraz administrator instytucji świadczącej usługi weryfikujące.

Zadania klienta internetowego sprowadzają się do sprawdzenia wiarygodności danych. Administrowanie serwerami firmy dostarczającej usługi weryfikujące polega na zarządzaniu klientami oraz na usuwaniu zbędnych i nieaktualnych danych. Ważnym zadaniem jest zapewnianie bezpieczeństwa serwerów z systemem pieczęci.



Rys.3. Przypadki użycia systemu weryfikującego

Najbardziej złożone są działania użytkownika systemu weryfikującego. Po rejestracji i uzyskaniu dostępu do usługi weryfikacyjnej, otrzymuje on możliwości logowania się i dokonywania zmian danych o swoim serwisie internetowym, w bazie danych umieszczonej na serwerze weryfikującym. Po każdorazowej zmianie ważnych danych w swoim serwisie dokonuje on obliczania skrótów kryptograficznych, przekazuje je do systemu i odbiera nową pieczęć weryfikującą. Działania użytkownika serwisu charakteryzują się tym, że ma on dostęp do bazy danych i dokonuje zmian swoich danych na serwerze instytucji samodzielnie. Diagram czynności użytkownika systemu weryfikującego w notacji UML przedstawiono na rysunku 4.



Rys.4 Diagram czynności użytkownika systemu

Użytkownik systemu każdorazowo po zmianie danych w swoim serwisie internetowym dokonuje modyfikacji danych w bazie danych instytucji weryfikującej. Poprawne działanie całego systemu weryfikującego wymaga zatem określonego nakładu pracy. Jest to pewna wada takiego rozwiązania jednak, w przypadku ważnych danych, których nieautoryzowana modyfikacja może prowadzić do poważnych konsekwencji i strat, takie działanie jest uzasadnione. Zmniejszenie nakładu pracy można dokonać poprzez wybór tylko niektórych danych podlegających ochronie oraz poprzez wybór niektórych stron w ramach całego serwisu, które podlegają weryfikacji. Należy również podkreślić, że takie systemy weryfikujące przeznaczone są dla profesjonalnych serwisów publikujących istotne dane zwłaszcza dla takich, których dane są przetwarzane przez inne systemy i podejmowane są na ich podstawie ważne decyzje o znaczących konsekwencjach. Trudno sobie wyobrazić konsekwencje nieautoryzowanych zmian danych w serwisach rządowych, militarnych, lotniczych, finansowych czy bankowych.

5. WNIOSKI KOŃCOWE

Zapewnienie wiarygodności danych internetowych to obecnie coraz poważniejszy problem, który wymaga nowych skutecznych rozwiązań [3,4]. Rozwój systemów do automatycznego przetwarzania informacji oraz budowa sieci semantycznej doprowadzi do wzrostu znaczenia zapewniania wiarygodności danych. Jedną z technicznych możliwości zapewniania wiarygodności danych internetowych są systemy przydzielające pieczecie weryfikujące. Ich poprawne działanie wymaga jednak firm świadczących usługi weryfikujące oraz nadzoru nad tymi firmami ze strony niezależnych instytucji. Możliwości systemów z pieczęciami weryfikującymi są bardzo duże, a same systemy nie są złożone techniczne czy programistycznie. Opisany w artykule system charakteryzuje się niezbyt dużą złożonością, ponieważ zawiera zaledwie 2000 wierszy kodu. Poprawne działanie takich systemów zależy jednak nie od wyboru nowoczesnych technologii i poprawności wykonania aplikacji, ale od konsekwencji w zgłaszaniu zmian treści stron przez administratora serwisu do systemu weryfikującego. Należy przypuszczać, że wykorzystywanie systemów weryfikujących dane internetowe będzie w przyszłości coraz popularniejsze.

Praca naukowa finansowana ze środków na naukę w latach 2009-2012 jako projekt badawczy nr N N519 172337.

5. BIBLIOGRAFIA

1. Witold Andrzejewski, Maciej Zakrzewicz: 'Problematyka bezpieczeństwa usług Web Services', Materiały PLOUG: Projektowanie i implementacja architektur zorientowanych na usługi, Warszawa, 2006.
2. M. Wu, C. Miller: Do Security Toolbars Actually Prevent Phishing Attacks, CHI, April 22-27, Montreal, Canada, 2006.
3. Y.Gil, D. Artz Towards Content Trust of Web Resources, WWW May 23-26 Edinburgh, 2006.
4. A. Herzberg, A. Jbara: Security and Identification Indicators for Browsers Against Spoofing and Phishing Attacks, ACM Transaction On Internet Technology Vol. 8, No.4, 2008.

A DEPENDABILITY ASSURANCE METHOD FOR WEB APPLICATIONS

Key-words: dependability, security, seals

Dependability assurance of internet-based information is an important issue that concerns both information supplier and the information itself. The paper overviews selected mechanisms of web page dependability assurance including: digital signatures, cryptographic signatures of micro information and security seals. Additionally, the paper describes a developed system that supplies a control seal mechanism that verifies integrity using cryptographic sum of file contents. We present main elements of system operation and selected design components, including UML diagrams and user interface.