BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 29, 2010

Projekt scentralizowanego, internetowego systemu rejestracji użytkowników

Piotr KWIATEK, Jan CHUDZIKIEWICZ

Instytut Teleinformatyki i Automatyki WAT,
ul. Gen. S. Kaliskiego 2, 00-908 Warszawa
piotr@kwiatek.org, jchudzikiewicz@wat.edu.pl

STRESZCZENIE: W artykule przedstawiono opis projektu oraz implementacji systemu rejestracji użytkowników w serwisie internetowym. Omówiono ideę zastosowania systemu jako scentralizowanego punktu uwierzytelniania i autoryzacji użytkowników w Internecie, a także aspekty bezpieczeństwa z tym związane. Przedstawiono przykład wdrożenia opracowanego rozwiązania.

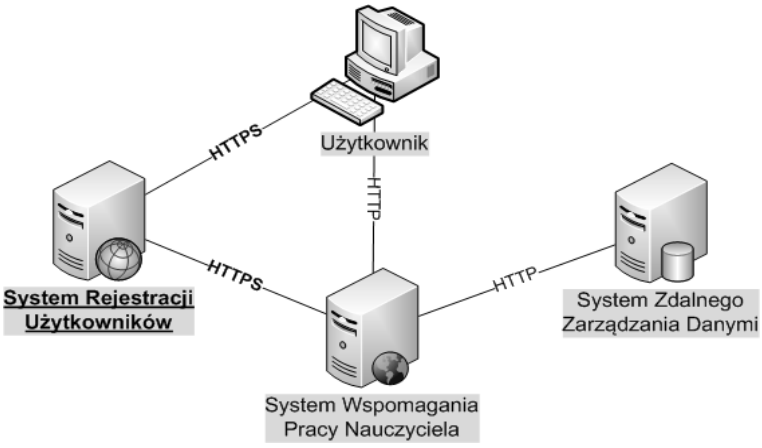
SŁOWA KLUCZOWE: uwierzytelnianie, autoryzacja, rejestracja użytkowników, bezpieczeństwo serwisów internetowych.

1. Wstęp

Logować się to rozpocząć pracę z systemem komputerowym o kontrolowanym dostępie przez podanie identyfikatora użytkownika i hasła. [1]. Na stronach internetowych jest to znany i powszechnie stosowany mechanizm potwierdzania tożsamości internauty. Na jednoznaczne odwzorowanie rzeczywistej tożsamości użytkownika w obiekt tożsamości w systemie pozwalają różne rodzaje mechanizmów uwierzytelniania. Warto zauważyć jednak, że koszt wykonania dobrej jakości modułu rejestracji, uwierzytelniania i autoryzacji w dużej mierze rośnie wraz z podnoszeniem jego poziomu bezpieczeństwa. Wydelegowanie wyżej wymienionych funkcji do specjalizowanego, autonomicznego systemu może przynieść wiele korzyści.

Celem budowy Systemu Rejestracji Użytkowników (SRU) było dostarczenie bezpiecznych mechanizmów zarządzania użytkownikami dla

Systemu Wspomagania Pracy Nauczyciela (SWPN) [3][4][7]. Na rys. 1 zaznaczono umiejscowienie SRU w relacji z pozostałymi aplikacjami współpracującymi z zaprojektowanym systemem. Technologią użytą do implementacji przedstawionych na rysunku aplikacji jest ASP.NET.



Rys. 1. Ogólny schemat powiązań pomiędzy aplikacjami

Początkową ideą była budowa SRU jako dedykowanego komponentu dla SWPN, jednak po dogłębnej analizie charakterystyki dziedziny oraz przeglądzie funkcji większości systemów uwierzytelniania powstała myśl o zbudowaniu niezależnego, autonomicznego systemu uwierzytelniania i autoryzacji. Jego zadaniem byłoby spełnianie nie tylko wszystkich wymagań stawianych przez aplikację SWPN, ale także umożliwienie wykorzystania jego usług do uwierzytelniania użytkowników oraz serwisów internetowych. Przyjęte rozwiązanie spełnia stawiane przez SWPN wymagania, dając dodatkowo możliwość zbudowania w oparciu o SRU centralnego punktu uwierzytelniania dla potrzeb np. szkoły, uczelni lub firmy.

2. Funkcje realizowane przez SRU

Głównym celem systemu jest zabezpieczenie wspieranej aplikacji przed nieautoryzowanym dostępem, podszywaniem się i pozyskiwaniem danych przez osoby postronne. Wspieraną aplikacją jest każdy serwis internetowy implementujący usługę uwierzytelnienia SRU, mający konto „serwisu internetowego" w bazie danych SRU. Serwis internetowy może przekazać do realizacji w SRU wszystkie obowiązki związane z bezpiecznym przechowywaniem i przekazywaniem poświadczeń oraz bezpiecznym uwierzytelnieniem i autoryzacją użytkownika.

2.1. Rejestracja nowego użytkownika

W aspekcie omawianego systemu tworzenie nowych kont użytkowników możemy realizować na dwa sposoby. Pierwszym jest udostępnienie anonimowym użytkownikom możliwości samodzielnego utworzenia konta w systemie poprzez wypełnienie formularza rejestracyjnego. Drugim sposobem tworzenia kont użytkowników jest przerzucenie tego obowiązku na administratora aplikacji klienckiej, czyli np. nauczyciela korzystającego z SWPN. Wybór scenariusza rejestracji nowego użytkownika nie jest trywialny, ponieważ każda z tych dróg przynosi inne korzyści, trudności i zagrożenia.

Realizacja pierwszego rozwiązania sprowadza się do udostępnienia formularza rejestracyjnego dla nieuwierzytelnionych internautów. Rozwiązanie to jest wygodne, ponieważ umożliwia błyskawiczne założenie konta oraz dostęp do docelowego serwisu internetowego. W przeciwieństwie do zdalnego tworzenia kont, użytkownik nie musi kontaktować się innymi sposobami z administratorem systemu w celu uzyskania danych potrzebnych do zalogowania się w systemie. Dzięki temu rozwiązaniu zyskujemy na czasie oraz odciążamy, z często żmudnej pracy, administratora systemu. Taki sposób realizacji tej funkcji wydaje się być dobry, jednak nie zapewnia wiarygodnego powiązania danej osoby z kontem w systemie.

Rozwiązanie zdalnego tworzenia kont zapewnia wiarygodność danych podanych w profilu konta. Uzyskuje się to, ponieważ administrator po założeniu konta, w momencie przekazywania użytkownikowi poświadczeń potrzebnych do zalogowania się w systemie, dokonuje potwierdzenia przynależności tej konkretnej osoby do nowo założonego konta. Warto jednak w tym przypadku zwrócić uwagę na kwestię bezpieczeństwa. Bardzo często zdarza się, że hasła i identyfikatory przekazywane są w niewystarczająco bezpieczny sposób, np. w wiadomościach e-mail zawierających hasła przesyłane w jawnej postaci lub po prostu na kartce papieru.

W celu spełnienia wszystkich wyżej wymienionych wymagań, w odniesieniu do różnych rozwiązań możliwych do zastosowania przy tworzeniu kont użytkowników, wybrano rozwiązanie hybrydowe. Polega ono na udostępnieniu dla anonimowych użytkowników formularza rejestracyjnego, zapewniającego szybki dostęp tylko do SRU zaraz po utworzeniu konta. Autoryzacja dostępu do współpracującego z SRU serwisu internetowego wymaga jednak aprobaty administratora tego serwisu, do którego użytkownik żąda dostępu. W tym momencie pozostaje tylko problem wiarygodności wprowadzonych przez internautę w formularzu rejestracyjnym danych. Administrator może opierać wiarygodność tych danych na wprowadzonym i potwierdzonym adresie e-mail lub musi skontaktować się w inny sposób z użytkownikiem w celu potwierdzenia podanych danych.

Autonomiczność SRU implikuje konieczność uwierzytelniania zarówno użytkowników, jak również aplikacji internetowych. Ponieważ nie istnieją żadne różnice w uwierzytelnianiu użytkownika i zewnętrznej aplikacji internetowej, postanowiono wykorzystać ten sam mechanizm, dostępny w ASP.NET, do uwierzytelniania zarówno kont użytkowników, jak i kont serwisów internetowych oraz zarządzania nimi. Konsekwencją tego jest konieczność wyboru rodzaju nowego konta podczas wypełniania formularza rejestracyjnego w celu nadania mu odpowiedniej roli w systemie.

2.2. Uwierzytelnienie i autoryzacja

SWPN jest rozwiązaniem umożliwiającym dostęp do stron WWW dla zamkniętej grupy użytkowników, dlatego też zadaniem SRU jest kontrola dostępu do całego serwisu. Oznacza to, że serwis internetowy nie udostępni żadnych treści użytkownikom nieuwierzytelnionym. Samo założenie konta w SRU pozwala tylko na uwierzytelnienia się w SRU. Mechanizm rejestracji wymaga weryfikacji adresu e-mail oraz określenia unikalnej nazwy użytkownika. Pozostałe dane nie mogą być wstępnie uznane za zgodne ze stanem faktycznym. O tym, czy posiadacz konta w SRU może mieć dostęp do wybranego serwisu internetowego, decyduje administrator tego serwisu. Dzięki udostępnionym usługom może on zezwolić lub zabronić na dostęp do swojej strony internetowej wybranym użytkownikom SRU. Dostęp do wybranego serwisu internetowego wymaga uwierzytelnienia i autoryzacji. Najpierw użytkownik potwierdza swoją tożsamość w SRU, co pozwala mu na uzyskanie dostępu do określonego serwisu. Następnie na podstawie tej uwierzytelnionej tożsamości udzielany jest mu dostęp do zasobów wybranego serwisu internetowego.

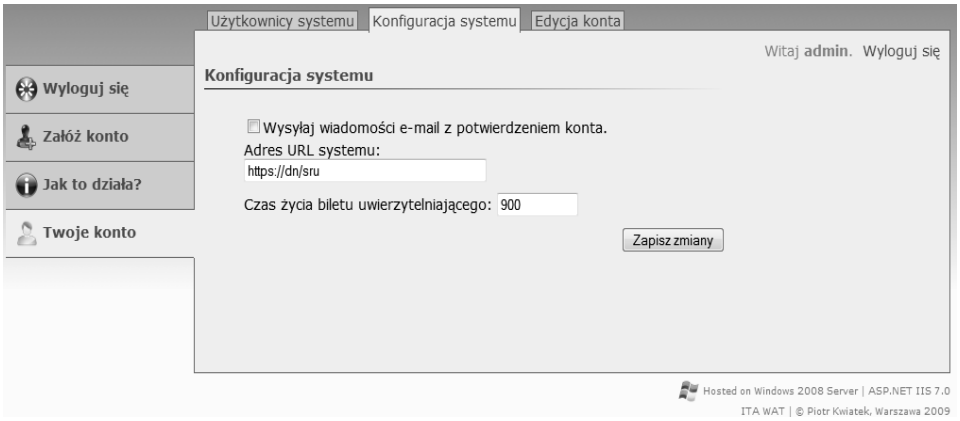
Proces uwierzytelniania musi także występować pomiędzy SRU i zewnętrznym serwisem internetowym. Dzięki mechanizmowi ról w ASP.NET możliwe jest uwierzytelnienie serwisu internetowego, bazując na poświadczeniach konta w SRU.

2.3. Role użytkowników SRU

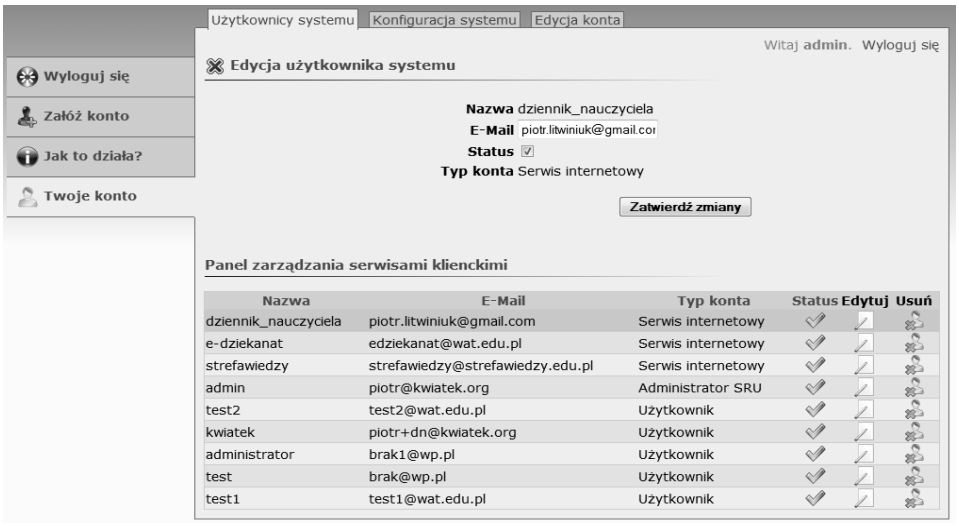
Uprawniony do korzystania z SRU użytkownik, czyli taki, który pomyślnie przechodzi proces logowania do systemu, podlega procesowi autoryzacji. System w zależności od rodzaju konta udostępnia różne części serwisu. W systemie występują trzy role: *rola administratora SRU*, *rola serwisu internetowego* oraz *rola użytkownika*.

Konto administratora SRU

Konto należące do roli administratora SRU ma uprawnienia do zarządzania wszystkimi profilami użytkowników założonych w systemie, czyli zarówno kontami użytkowników, jak i kontami serwisów internetowych. Po zalogowaniu się na takie konto, administrator ma do dyspozycji panel służący podstawowej konfiguracji systemu (rys. 2), a także ma prawo do zarządzania wszystkimi użytkownikami systemu (rys. 3). Może usuwać, aktywować, dezaktywować oraz edytować dowolne konta w systemie. Rolę administratora można przydzielić jedynie podczas specjalnej konfiguracji SRU.

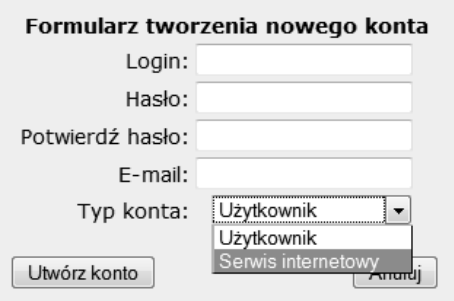


Rys. 2. Panel konfiguracji systemu administratora SRU



Rys. 3. Panel zarządzania użytkownikami systemu administratora SRU

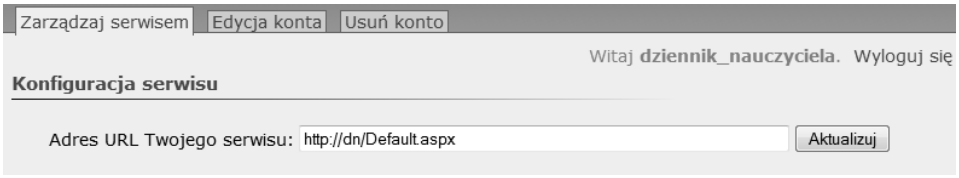
Kolejnymi dwiema rolami w systemie są: *rola użytkownika* oraz *rola serwisu internetowego*. Konto może przynależeć do dokładnie jednej z ról w danym momencie. Profile użytkowników należące do *roli użytkownika* lub *roli serwisu internetowego* nie są tak krytyczne w kwestii bezpieczeństwa jak konta z rolą administratora, dlatego też te typy kont, jak przedstawiono na rys. 4, mogą być wybierane samodzielnie przez internautę podczas wypełniania formularza rejestracyjnego.



Rys. 4. Formularz rejestracji nowego użytkownika

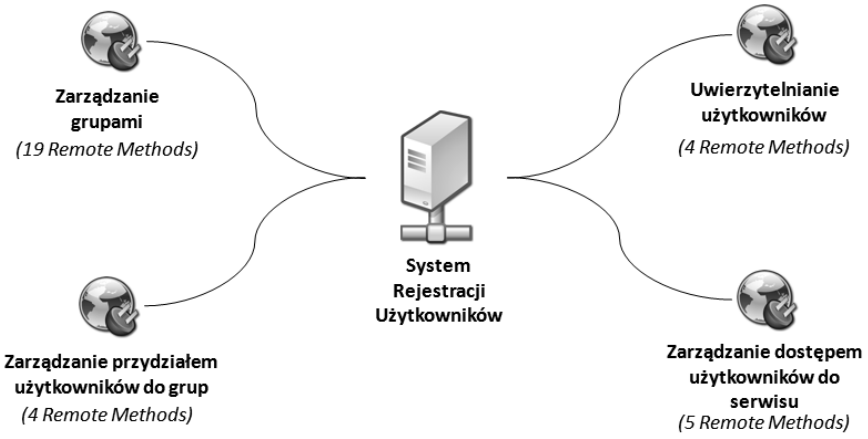
Konto serwisu internetowego

Konto serwisu internetowego służy do identyfikacji i uwierzytelnienia zewnętrznej aplikacji internetowej, implementującej mechanizm uwierzytelniania użytkowników SRU. Administrator serwisu internetowego, podczas korzystania z SRU, używając tych samych poświadczeń, może uwierzytelnić się w SRU przez stronę internetową systemu, jak również poprzez udostępniane usługi sieciowe. Pomyślne zalogowanie się do systemu, na konto serwisu internetowego przez stronę internetową, uprawnia jedynie do korzystania z formularza zmiany adresu URL danego serwisu, co zostało pokazane na rys. 5.



Rys. 5. Formularz rejestracji nowego konta w SRU

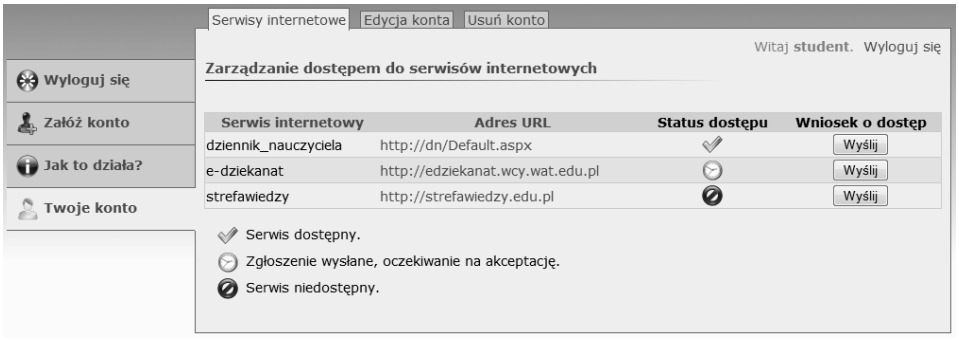
Większość funkcji oferowanych przez SRU dla serwisów internetowych dostępna jest z poziomu usług sieciowych „web service". Udostępniane usługi realizują zadania uwierzytelniania, autoryzacji, a także operacje związane z zarządzaniem użytkownikami i grupami. Ogólny schemat udostępnianych przez SRU metod zdalnych przedstawiono na rys. 6.



Rys. 6. Usługi sieciowe SRU dostępne dla serwisów internetowych

Konto użytkownika

Poświadczenia zwykłych użytkowników pozwalają na uwierzytelnienie się w SRU w celu zarządzania kontem oraz uwierzytelnienia się w zewnętrznych, partnerskich serwisach internetowych. Pomiędzy kontami serwisów internetowych i kontami użytkowników istnieje powiązanie „wiele do wielu". Umożliwia to serwisom internetowym uwierzytelnianie i autoryzację wielu użytkowników, a także zwykłym użytkownikom logowanie się do wielu kooperujących z SRU serwisów internetowych. Operacja przypisywania użytkownika do serwisu internetowego rozpoczyna się od wysłania prośby o autoryzację do wybranego serwisu. Użytkownik może to zrobić za pomocą panelu zarządzania kontem, gdzie dostępna jest lista zarejestrowanych w systemie serwisów internetowych, do których można wysyłać zgłoszenia. Po pomyślnym zatwierdzeniu zgłoszenia użytkownika przez administratora serwisu internetowego, użytkownik uzyskuje dostęp do żądanej strony WWW po wpisaniu jej adresu URL w polu adresu przeglądarki internetowej. Na rys. 7 został przedstawiony panel zarządzania dostępem do przykładowych serwisów internetowych, w którym użytkownik może monitorować statusy dostępu oraz wysyłać nowe zgłoszenia.



Rys. 7. Panel zarządzania dostępem do serwisów internetowych

2.4. Mechanizm grup

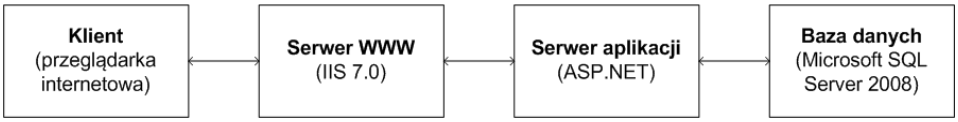
Mechanizm ról wbudowany w ASP.NET nie jest wystarczająco elastyczny, aby można było tworzyć drzewiaste struktury, umożliwiające na przykład dziedziczenie uprawnień. Obsługa w zakresie zarządzania użytkownikami SWPN rozgranicza dostęp do wybranych części i usług serwisu dla różnych grup użytkowników. W systemie tym istnieją trzy podstawowe grupy użytkowników, które dzielą się na podgrupy. Są to: Administratorzy, Nauczyciele, Studenci oraz należące do grupy studentów grupy szkoleniowe.

Wymagania nakładane na sposób kontroli dostępu (opartego o grupy użytkowników) do wybranych zasobów serwisu wymusiły opracowanie specjalizowanego mechanizmu grup. Każdy serwis internetowy, dzięki takiemu rozwiązaniu, ma możliwość tworzenia niezależnej struktury grup użytkowników, niewidocznej dla innych serwisów internetowych współpracujących z SRU. Administrator serwisu internetowego, dzięki udostępnionym usługom sieciowym do tworzenia grup nadrzędnych, podrzędnych, usuwania ich oraz ich modyfikacji, a także przypisywania i usuwania użytkowników z grup, ma możliwość kontroli nad strefami, w których użytkownik może poruszać się w serwisie. Przykładowo student należący do grupy głównej „studenci” ma dostęp do części e-learningowej, ale ze względu na przynależność do podgrupy „I9H1S4” posiada dostęp do materiałów zgromadzonych tylko w obrębie tej grupy szkoleniowej. Problem implementacji mechanizmu autoryzacji dostępu do tych zasobów pozostaje w gestii aplikacji wspomagającej pracę nauczyciela.

3. Bezpieczeństwo

3.1. Analiza bezpieczeństwa przesyłanych danych

Zanim informacja od nadawcy trafi do odbiorcy przetwarzana jest przez pewną liczbę urządzeń sieciowych. Na każdym z nich możliwe jest, jeśli informacja nie jest odpowiednio zabezpieczona, podejrzenie, skopiowanie lub zmiana przesyłanej informacji. W przypadku naszego systemu do informacji poufnych należą dane identyfikacyjne, potrzebne do uwierzytelniania użytkowników w systemie. Wrażliwymi informacjami są także identyfikatory sesji zestawionych między użytkownikami a aplikacją. Przechwycenie obiektu sesji, zwane potocznie „Session hijacking", pozwala na przejęcie stanu aplikacji uwierzytelnionego użytkownika oraz kontroli nad jego kontem [3, s. 564]. Niebezpieczeństwo wzrasta, jeśli komponenty aplikacji znajdują się na oddzielnych maszynach komunikujących się przez sieć (rys. 8).



Rys. 8. Model działania Systemu Rejestracji Użytkowników

Aby zapewnić prywatność oraz integralność przesyłanych danych, SRU wykorzystuje do zabezpieczenia połączeń z klientami oraz serwisami internetowymi protokół SSL [3, s. 14-15, 55].

3.2. Analiza bezpieczeństwa przechowywanych danych

W pierwszej kolejności należy zastanowić się, jak i w jakiej postaci najbezpieczniej będzie można przechowywać dane gromadzone przez system. Informacje wymagane do uwierzytelnienia użytkowników można przechowywać w takiej postaci, aby były one bezużyteczne dla intruza, który zdołał przedostać się przez wszystkie bariery zabezpieczeń. Pozwalają na to metody z dziedziny kryptografii. Dobrym przykładem jest kryptograficzny algorytm funkcji skrótu SHA1, który z długiego ciągu tekstowego tworzy 160-bitowy skrót. Kluczową własnością funkcji haszujących (skrótów) jest ich jednokierunkowość oraz to, że najmniejsza zmiana w wejściowym ciągu tekstowym powoduje otrzymanie zupełnie innego wyniku na wyjściu [2, s. 2]. W bazie danych SRU hasła przechowywane są właśnie pod postacią skrótów SHA1. Hasło wprowadzane przez użytkownika podczas logowania do systemu zamieniane jest za pomocą

tego samego algorytmu na skrót, a następnie porównywane z przechowywanym w bazie, utworzonym podczas rejestracji, skrótem prawidłowego hasła. W SRU dokonuje tego mechanizm ASP.NET Membership, który dodatkowo przed utworzeniem skrótu poddaje hasło wielu operacjom konwersji, jeszcze bardziej utrudniających odgadnięcie ciągu wejściowego [4].

Przechowywanych danych nie możemy jednak chronić jedynie przed odczytem przez niepowołane osoby. Dostępność systemu oraz integralność bazy danych jest równie ważna, dlatego też SRU został wyposażony w mechanizmy chroniące go przed znanymi atakami sieciowymi. Newralgicznym punktem SRU są pola logowania, w które użytkownik sam wprowadza tekst. Wprowadzenie odpowiednio spreparowanych danych może wyrządzić w systemie wiele różnych szkód, a także pozwolić na przejęcie nad nim kontroli.

W systemie zaimplementowano szereg mechanizmów filtrujących wszystkie dane pochodzące od klientów. Analiza danych wejściowych w SRU pozwala na uniknięcie ataków typu SQL Injection lub Cross-site scripting.

4. Projekt i implementacja wybranych mechanizmów SRU

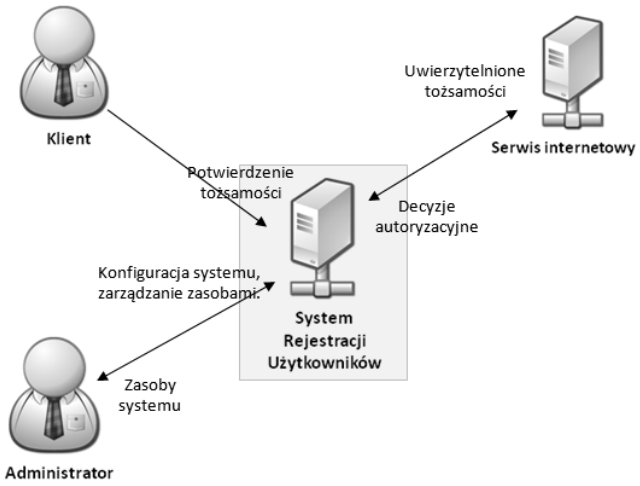
4.1. Zrealizowane cele

Celem zaprojektowanego systemu jest oferowanie usług uwierzytelniania, autoryzacji i zarządzania użytkownikami na wysokim poziomie bezpieczeństwa. Gotowe rozwiązania SRU w wyżej wymienionych dziedzinach są przydatne dla serwisów niemających mechanizmów zarządzania użytkownikami, autoryzacji i bezpiecznego uwierzytelniania. Podczas projektowania systemu skoncentrowano się na bezwzględnym spełnieniu wszystkich stawianych wymagań oraz na zapewnieniu jak największej skalowalności i elastyczności aplikacji.

Wdrożenie usług SRU w serwisie internetowym nie ingeruje w strukturę serwisu internetowego oraz jest proste w instalacji. SRU udostępnia gotową klasę *Authorization*, zawierającą metody, które wystarczy wywołać w aplikacji internetowej. System po wywołaniu wyżej wspomnianych metod przekazuje sterowanie do SRU, a następnie przejmuje obsługę uwierzytelnienia i autoryzacji użytkownika. Na koniec udostępnia tożsamość uwierzytelnionego użytkownika po pomyślnej weryfikacji poświadczeń. SRU udostępnia także szereg usług umożliwiających kontrolę dostępu użytkowników do serwisów internetowych.

Użytkownik korzystający z SWPN jest uwierzytelniany i autoryzowany do dostępu do zasobów aplikacji docelowej w sposób przezroczysty, tak jakby poruszał się w ramach jednego spójnego systemu. SRU udostępnia także mechanizmy służące zarządzaniu kontem użytkownika w systemie.

Przykładową zależność pomiędzy SRU a elementami korzystającymi z jego usług (ang. *Web Services*) przedstawiono na rys. 9.



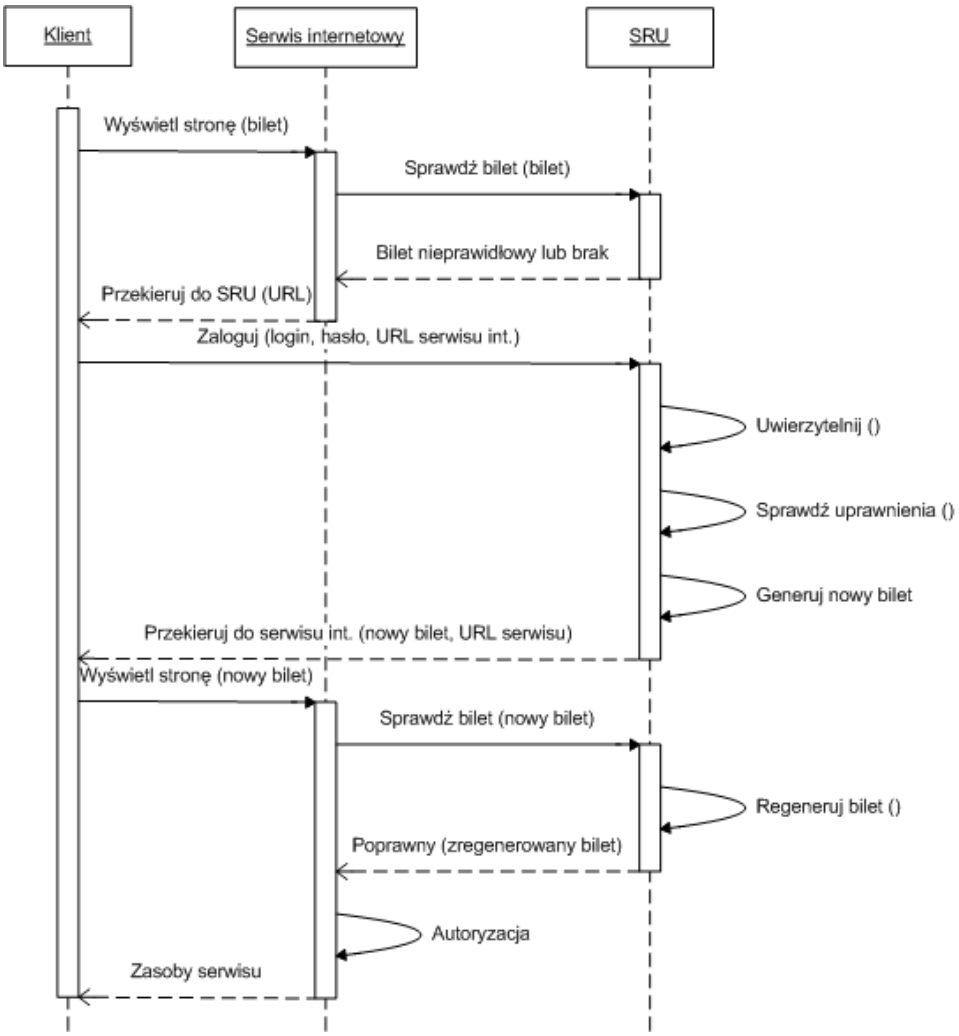
Rys. 9. Diagram współpracy SRU z elementami zewnętrznymi

4.2. Przebieg uwierzytelnienia i autoryzacji użytkownika

Na diagramie sekwencji, przedstawionym na rys. 10, pokazano mechanizm współpracy oraz kolejność wykonywanych czynności przez obiekty biorące udział w procesie uwierzytelniania użytkownika. W poniższym scenariuszu założono, że uwierzytelnienie przebiega pomyślnie i tożsamość zostaje potwierdzona.

Zgodnie z założeniami wyspecyfikowanymi w wymaganiach funkcjonalnych oraz celach projektowych SRU, opracowano zautomatyzowany mechanizm, delegujący proces uwierzytelniania z serwisu internetowego do SRU. Proces ten rozpoczyna się w momencie wysłania żądania dostępu do zasobów serwisu internetowego przez anonimowego internautę, oznaczonego na diagramie jako „Klient". Anonimowy jeszcze użytkownik nie posiada tzw. biletu (ang. *ticket*) pozwalającego na uwierzytelnienie. Przyjmuje się, że bilet ten jest nieprawidłowy lub nieważny. Serwis internetowy, odbierając żądanie, wykonuje próbę uwierzytelnienia klienta, przesyłając przedstawiony przez klienta bilet do SRU poprzez usługę „web service". System sprawdza przesłany bilet i wysyła odpowiedź do serwisu internetowego. Dla pełnego zobrazowania procesu

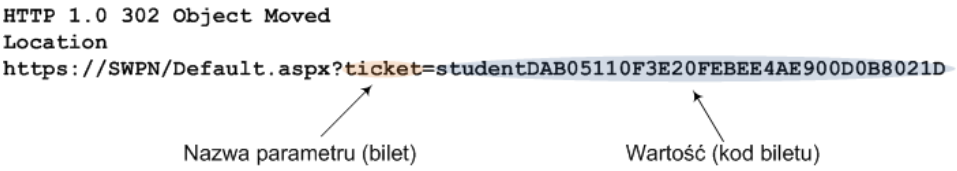
uwierzytelniania założono, że użytkownik odwiedza serwis internetowy po raz pierwszy i nie posiada ważnego biletu. W takim wypadku serwis internetowy przenosi użytkownika do stron SRU, delegując proces uwierzytelniania. W czasie kiedy użytkownik pozostaje w interakcji z SRU, serwis internetowy nie ma żadnej kontroli nad operacjami wykonywanymi w SRU.



Rys. 10. Pomyślne uwierzytelnienie i autoryzacja użytkownika – diagram sekwencji

Klient za pomocą odpowiedniego formularza przekazuje poświadczenia, czyli nazwę użytkownika i hasło, do SRU. Jeśli podane poświadczenia są prawidłowe, system uwierzytelnia klienta jedynie w obrębie SRU. Po uwierzytelnieniu klient otrzymuje bilet, składający się z nazwy użytkownika

oraz unikalnego losowego ciągu znaków. Poświadcza on poprawne uwierzytelnienie w SRU. Należy podkreślić, że SRU po pomyślnym uwierzytelnieniu i wygenerowaniu biletu nie komunikuje się w żaden sposób z serwisem internetowym, z którego użytkownik przybył. Bilet identyfikujący tożsamość użytkownika przekazywany jest do przeglądarki klienta wraz z nagłówkiem HTTP o kodzie 302 (rys. 11).



Rys. 11. Uproszczony nagłówek HTTP przenoszący klienta do strony serwisu internetowego

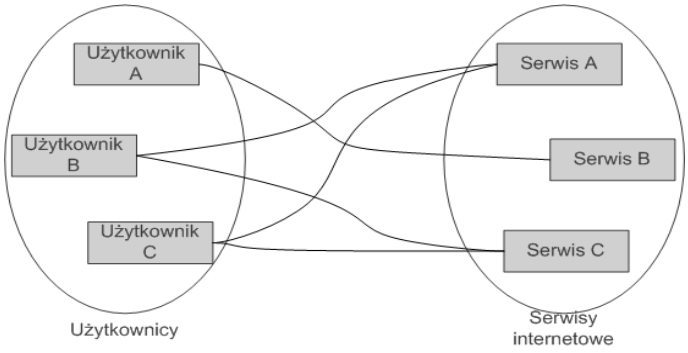
Odebranie przez przeglądarkę internetową takiego nagłówka HTTP wymusza przekierowania na stronę serwisu internetowego SWPN oraz przesłanie metodą GET biletu uwierzytelniającego. Rozwiązanie to pozwala na w pełni automatyczne i przezroczyste dla klienta przekazywanie sterowania pomiędzy serwisami. Serwis internetowy, po otrzymaniu żądania HTTP wraz z nowym biletem, wykonuje tę samą operację weryfikacji biletu co na początku. Sprawdzane jest, czy użytkownik faktycznie otrzymał przedstawiany w nagłówku HTTP bilet od SRU. Za pomocą sieciowej usługi weryfikacji biletów SRU serwis internetowy sprawdza bilet. Na tę procedurę składa się odnalezienie biletu w bazie danych, sprawdzenie, czy nie wygasł, skojarzenie biletu z użytkownikiem oraz wygenerowanie nowego biletu. SRU zwraca informację o błędzie w przypadku jakiegokolwiek błędu weryfikacji lub nowy, zregenerowany bilet. Regeneracja biletu przeprowadzana jest w celu podwyższenia bezpieczeństwa wspieranej aplikacji. Serwis internetowy po otrzymaniu odpowiedzi od SRU decyduje, czy udostępnić swoje zasoby. Wraz z odpowiedzią serwisu internetowego klient otrzymuje nowy bilet, ważny przez ustalony czas lub do następnego żądania dostępu.

Bilet jest jedną z najbardziej poufnych informacji, ponieważ posiadanie ważnego biletu wystarczy do uzyskania autoryzacji. Kod biletu przesyłany między klientem a serwisem internetowym może zostać odczytany w sieci przez osobę postronną. To, czy połączenie między klientem a serwisem internetowym będzie szyfrowane, leży już w gestii programisty serwisu internetowego. Aby zwiększyć wiarygodność tego, że przesyłany bilet pochodzi faktycznie od uwierzytelnionego w SRU klienta, stworzono mechanizm sprawdzania ważności oraz regeneracji biletu, który zmniejsza ryzyko podszycia się intruza pod uwierzytelnioną w danej chwili tożsamość. Sam mechanizm sprawdzania biletu bada, czy w kontekście danego użytkownika nie było konfliktów w użyciu biletów. Oznacza to, że jeśli

dla danego użytkownika bilet został użyty podwójnie lub klient przesłał błędny kod biletu, aktualny także traci ważność. Przy założeniu, że sesja pomiędzy użytkownikiem a SRU jest bezpieczna i trwała, można przyjąć, że uczciwy użytkownik zostanie automatycznie ponownie uwierzytelniony w serwisie internetowym, a intruzowi przedstawiony zostanie formularz logowania SRU. Serwis internetowy po otrzymaniu informacji o błędnej weryfikacji biletu, bez względu na powód tego niepowodzenia, przekierowuje klienta do formularza logowania SRU. Użytkownik już uwierzytelniony w SRU automatycznie otrzyma nowo wygenerowany bilet, a następnie zostanie przekierowany z powrotem do serwisu internetowego. Intruz natomiast, z powodu braku aktywnej sesji z SRU, zatrzyma się na formularzu logowania.

4.3. Relacja użytkowników z serwisami internetowymi

Teoretycznie dokładnie jedno konto wystarcza do tego, aby móc uzyskać autoryzację we wszystkich serwisach internetowych, implementujących mechanizm uwierzytelniania SRU. Rozwiązanie to jest wygodne, ponieważ użytkownik nie musi korzystać z wielu kont o różnych poświadczeniach do logowania się na wybranej stronie internetowej. SRU udostępnia odpowiednie usługi sieciowe dla serwisów internetowych, umożliwiające kontrolę nad tym, które konta mogą uzyskiwać autoryzację. Rys. 12 przedstawia przykładowe przyporządkowanie kont o roli użytkownik do kont o roli serwis internetowy.



Rys. 12. Przykładowe przyporządkowanie użytkowników do serwisów internetowych

Przykład z rys. 12 pokazuje, że użytkownik B może mieć dostęp do serwisów A oraz C, natomiast użytkownik A może mieć dostęp tylko do serwisu B.

Proces przypisywania użytkownika do serwisu internetowego rozpoczyna się od zgłoszenia przez użytkownika chęci dostępu do wybranego serwisu internetowego. SRU udostępnia mechanizm, dostępny z poziomu panelu

zarządzania kontem, umożliwiający przesyłanie takich zgłoszeń. Użytkownik po wysłaniu zgłoszenia z prośbą o dostęp do konkretnego serwisu internetowego, musi czekać na reakcję ze strony jego administratora. Serwis internetowy, korzystając z usługi sieciowej udostępnionej przez SRU, akceptuje lub odrzuca nadesłane zgłoszenia. Przebieg tego procesu przedstawia poniższy scenariusz:

1. SRU: Wyświetla panel zgłaszania wniosków o autoryzację w serwisach internetowych.
2. Użytkownik: Wybiera serwis internetowy i wysyła wniosek.
3. SRU: Udostępnia listę zgłoszeń wysłanych do serwisu internetowego.
4. Serwis internetowy: Pobiera listę.
5. Serwis internetowy: Akceptuje lub odrzuca zgłoszenie użytkownika.
6. SRU: Nadaje użytkownikowi nowe uprawnienia do serwisu internetowego.
7. SRU: Powiadamia użytkownika.

Powyższy scenariusz opisuje pełny przebieg procesu przydziału uprawnień użytkownikowi w serwisie internetowym. SRU udostępnia ponadto metody, dzięki którym administrator serwisu internetowego może autoryzować wybranych użytkowników SRU bez otrzymania ich zgłoszeń. Użytkownik o fakcie autoryzacji w danym serwisie może dowiedzieć się z panelu zarządzania kontem w SRU.

4.4. Rejestracja i aktywacja nowego konta

Zgodnie ze wcześniejszymi założeniami, SRU udostępnia mechanizm umożliwiający samodzielne utworzenie i aktywację konta. W procesie rejestracji użytkownika bierze udział tylko anonimowy internauta i SRU.

Rejestracja nowego użytkownika rozpoczyna się od wypełnienia formularza rejestracyjnego:

- Login – proponowana nazwa konta w systemie,
- Hasło,
- E-mail – wymagany w celu późniejszej aktywacji konta,
- Rodzaj konta – w zależności od tego wyboru, konto zostanie przypisane do roli zwykłego użytkownika lub serwisu internetowego.

Wprowadzone do formularza dane podlegają walidacji zanim zostaną przesłane do funkcji tworzącej konto w systemie. Każde pole podlega różnym regułom walidacji:

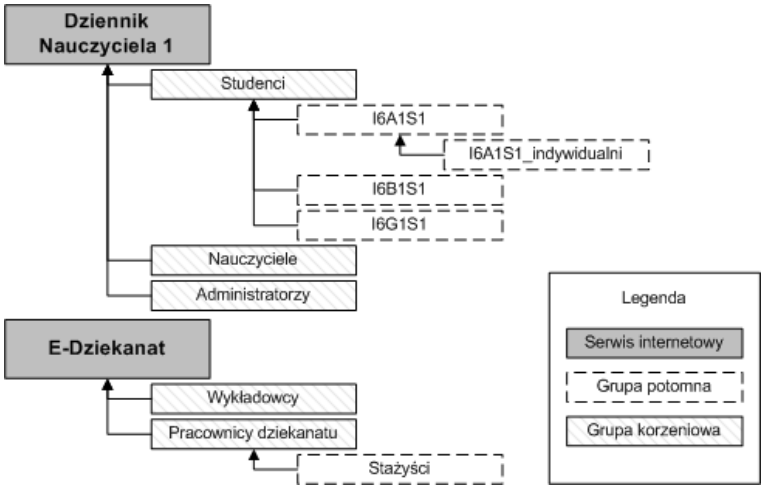
- Login
    - Czy nazwa nie jest już zajęta?
    - Czy nazwa pasuje do wzorca prawidłowej nazwy użytkownika, tzn. czy nie zawiera niedozwolonych znaków, nie jest za krótka lub za długa itp.?
- Hasło
    - Czy pasuje do wzorca prawidłowego hasła, tzn. zawiera odpowiednią liczbę cyfr, znaków specjalnych oraz jest odpowiednio długie?
    - Czy jest identyczne z zawartością pola potwierdzenia hasła?
- E-mail
    - Czy ma prawidłowy format?
    - Czy adres nie jest już przypisany do innego konta?

W przypadku napotkania na jakikolwiek konflikt z regułami poprawności wprowadzanych danych, formularz musi zostać poprawiony. Po usunięciu ewentualnych błędów, konto w systemie zostaje utworzone, ale może być jeszcze nieaktywne. System w zależności od konfiguracji, w celu zabezpieczenia przed seryjnym zakładaniem kont oraz w celu potwierdzenia adresu e-mail podanego w formularzu, może wysłać na podany adres e-mail wiadomość ze specjalnym kodem aktywacyjnym. Konto pozostaje nieaktywne do chwili wprowadzenia kodu aktywacyjnego na stronie SRU. Jeśli użytkownik odbierze wiadomość e-mail i zdecyduje się aktywować swoje konto, musi wykonać operacje zawarte w wiadomości e-mail. Po przesłaniu klucza do SRU system sprawdzi go i jeśli jest poprawny, aktywuje powiązane z kluczem konto. Funkcja potwierdzania konta e-mail może zostać wyłączona przez administratora SRU. W takim wypadku konto aktywowane jest natychmiast po rejestracji. Użytkownik może zalogować się na swoje konto zaraz po jego założeniu.

4.5. Grupy kont

Dla mechanizmu grup wymagane jest, aby każdy serwis internetowy mógł tworzyć niezależną, drzewiastą strukturę grup. Struktura i nazwy grup są niezależne dla każdego serwisu internetowego. Ograniczając się do struktury zależności grup w obrębie jednego serwisu internetowego, można wyróżnić trzy rodzaje grup: grupę główną, grupę nadrzędną oraz grupę potomną. Grupa główna nie ma rodzica, natomiast grupa potomna powiązana jest grupą nadrzędną – rodzicem. Grupą nadrzędną dla grupy potomnej wcale nie musi być grupa główna, ponieważ nie istnieje ograniczenie co do liczby poziomów

struktury grup. Oznacza to, że grupa potomna może być jednocześnie grupą nadrzędną, ale nie może być grupą główną. Przykładem jest grupa I6A1S1 na rys. 13.



Rys. 13. Przykładowa struktura grup w SRU

Użytkownik przypisany do serwisu internetowego może być przydzielany bez ograniczeń do różnych grup należących do tego serwisu. W nawiązaniu do powyższego przykładu, użytkownik może znajdować się jednocześnie w grupie Studenci i grupie I6G1S1. W kontekście całego SRU, użytkownik teoretycznie może być przypisany do wielu grup, należących do różnych serwisów internetowych bez ograniczeń. W praktyce, z faktu, że tylko serwis internetowy może przydzielać użytkowników do swoich grup, wynika, że użytkownik nie może należeć do grup w obrębie serwisów internetowych, z którymi nie jest powiązany.

5. Podsumowanie

Analizując stosowane w różnych serwisach internetowych mechanizmy uwierzytelniania, można stwierdzić, że niejednokrotnie mają one wiele podatności na ataki, przez co poświadczenia użytkowników i sam serwis są narażone na zagrożenia zewnętrzne. Wynika to najczęściej z potrzeby zbilansowania kosztów przeznaczonych na budowę systemu, przez co mechanizm uwierzytelniania nie zawsze jest w pełni przetestowany i bezpieczny. Implementacja zewnętrznej usługi uwierzytelniania jest rozwiązaniem tańszym i bezpieczniejszym.

Występowanie aktywnej sesji uwierzytelnienia z SRU pozwala na dostęp do wszystkich serwisów internetowych współpracujących z SRU bez każdorazowego podawania poświadczeń. Dodatkowo użytkownik musi zapamiętać tylko jeden identyfikator i hasło. W rzeczywistości użytkownicy Internetu bardzo często korzystają z jednakowych identyfikatorów i haseł na wielu stronach internetowych, podając je przy logowaniu do każdej z nich. Nie każdy serwis jest dostatecznie bezpieczny i nie każdy zapewnienia szyfrowane połączenia z klientem. Wyciek danych, identyfikatorów i haseł z jednego serwisu dość często otwiera drogę do uzyskania dostępu w innych serwisach internetowych, gdzie ten sam użytkownik zakładał konto. Włamanie do bazy danych serwisu internetowego kooperującego z SRU wyklucza możliwość pozyskania przez intruza poświadczeń użytkowników. Korzystanie z usług SRU zapewnia również, że poświadczenia użytkowników nigdy nie zostaną przesłane w postaci otwartej, niezaszyfrowanej.

Wdrożenie SRU w Internecie jest możliwe, aczkolwiek liczba wykonanych do tej pory testów penetracyjnych nie pozwala na uznanie SRU za system w pełni bezpieczny. Aplikację należałoby wyposażyć w podpisany cyfrowo certyfikat SSL. Umożliwiłoby to uodpornienie jej na atak typu ARP Spoofing oraz DNS Spoofing. Na tym etapie rozwoju systemu z powodzeniem można używać go w wewnętrznych sieciach firmowych lub uczelnianych, w których zagrożenia są mniejsze ze względu na bardziej zaufanych użytkowników sieci.

Literatura

[1] DUBISZ S., *Uniwersalny słownik języka polskiego PWN*, Wydawnictwo Naukowe PWN, 2006.

[2] EASTLAKE D., JONES P., *US Secure Hash Algoritm 1 (SHA1)*, The Internet Society, 2001.

[3] KWIATEK P., *System rejestracji użytkowników w serwisie internetowym*, Praca dyplomowa, Wydział Cybernetyki WAT, 2010.

[4] LITWINIUK P., *Aplikacja ASP.NET wspomagająca pracę nauczyciela*, Praca dyplomowa, Wydział Cybernetyki WAT, 2010.

[5] MEIER J. D., MACKMAN A., DUNNER M., VAASIREDDY S., *Building Secure ASP.NET Applications. Authentication, Authorization and Secure Communication*, Microsoft Corporation, 2002.

[6] MSDN LIBRARY, *Membership Element*, http://msdn.microsoft.com/en-us/library/1b9hw62f.aspx [stan na: 05.07.2010 r.]

[7] POLKOWSKI S., *System zdalnego zarządzania współdzielonymi danymi oparty o usługi WWW*, Praca dyplomowa, Wydział Cybernetyki WAT, 2010.

A project of a user registration centralized web service

ABSTRACT: In this paper a project and implementation of a user registration web service is presented. An idea of the system application as a centralized point of users authentication and authorization in the Internet is discussed. Security aspects of the system are considered too. An example of practice use of the system is presented.

KEYWORDS: authentication, authorization, user registration, web services security

Praca wpłynęła do redakcji: 14.09.2010