STUDIA INFORMATICA 2001
Volume 22 Number 1 (43)

Adam ZIELONKA
PWPT WASKO Sp. z o.o. Zakład Systemów Telekomunikacyjnych

ZAGADNIENIA SKALOWALNOŚCI I ZAPEWNIENIA DOSTĘPU DO BAZ DANYCH UWIERZYTELNIEŃ W SYSTEMACH ROZPROSZONYCH

Streszczenie. Sieć komputerowa, zapewniająca bezpieczeństwo swoich zasobów, nie może się dzisiaj obyć bez silnych i skutecznych mechanizmów uwierzytelniania użytkowników. Zagadnienia związane z budową skalowalnych i wygodnych w zarządzaniu, a także uniwersalnych systemów z centralnym serwerem bazy danych uwierzytelnień są tematem niniejszego artykułu.

SCALABILITY AND ACCESS TO AUTHENTICATION DATABASE ISSUES IN DISTRIBUTED SYSTEMS

Summary. Computer networks that ensure resource security need strong and effective user authentication methods. In this study the concept of distributed systems with centrally located authentication database has been presented. Furthermore the scalability, management and flexibility issues of such systems have been described.

1. Wprowadzenie

Współczesne systemy rozproszone stają coraz bardziej rozbudowane i skomplikowane. W sieci komputerowej, będącej środowiskiem heterogenicznym, łączącym różnego typu rozproszone serwery zasobów czy aplikacji oraz korzystających z nich użytkowników, znajdują się też urządzenia należące do infrastruktury, takie jak routery i switche, a także bramy łączące sieć ze światem, jak serwery dostępowe NAS (*Network Access Server*) dla użytkowników zdalnych czy urządzenia typu firewall, odgradzające i zapewniające bezpieczną współpracę z Internetem. Dostęp do wszelkich zasobów sieci oraz urządzeń aktywnych musi być kontrolowany. Ich mnogość, a także fakt zróżnicowania pod względem funkcjonalności czy choćby

sposobu zarządzania, powoduje, że sterowanie dostępem do zasobów systemu oraz sterowanie uprawnieniami do zarządzania infrastrukturą sieci wymaga nowoczesnego podejścia do tego problemu. Podejście to musi uwzględniać takie zagadnienia, jak centralizacja oraz maksymalne ograniczenie kosztów powyższych czynności, a także zapewnienie jak najwyższego poziomu bezpieczeństwa. W dużych systemach rozproszonych z wielką ilością użytkowników, którym należy zapewnić swobodny, a jednocześnie bezpieczny dostęp do określonych, ogólnie rozumianych zasobów systemu, do których można również zaliczyć aktywne składniki infrastruktury sieci, utrzymanie spójnej, a jednocześnie elastycznej i skalowalnej bazy informacji o użytkownikach i ich prawach dostępu do zasobów sieci jest jednym z podstawowych problemów, jakie stoją przed projektantami czy administratorami.

Artykuł porusza kilka podstawowych zagadnień związanych z problemem centralnych baz danych uwierzytelnień w dużych, heterogenicznych systemach rozproszonych, a także z problemami komunikacji urządzeń sieciowych z taką bazą. Przytoczone zostaną również przykłady protokołów, które mogą zostać wykorzystane do konstrukcji systemu z uwierzytelnianiem użytkowników na podstawie centralnej bazy danych, a także praktycznego przykładu takiego systemu.

2. Pojęcie uwierzytelnienia w systemie rozproszonym

2.1. Co to jest uwierzytelnienie?

Uogólniając można powiedzieć, że jest to proces mający na celu ustalenie tożsamości nadawcy i/lub odbiorcy informacji na podstawie pewnych danych, które przekazuje strona uwierzytelniana [1]. Technologie uwierzytelniające w ostatnich latach niezwykle rozwinęły się i zarazem rozmnożyły, odpowiadając na zapotrzebowanie rynku. Wiąże się z tym zróżnicowany charakter informacji, jakie musi zgromadzić strona uwierzytelniająca, aby na ich podstawie skutecznie zidentyfikować użytkownika. Wynikiem procesu uwierzytelnienia jest zazwyczaj prosta informacja, czy użytkownik jest upoważniony do dostępu do określonych zasobów, co jest równoznaczne ze stwierdzeniem, że użytkownik jest znany stronie uwierzytelnianej lub też nie. Często z procesem uwierzytelniania łączy się proces autoryzacji, który określa, co użytkownikowi wolno robić po prawidłowym uwierzytelnieniu się w systemie.

2.2. Metody uwierzytelniania

Przyjęto podział metod uwierzytelniania na trzy główne grupy [2].

1. Uwierzytelnienie na podstawie tego, co użytkownik wie. Nazwą to można określić wszystkie metody uwierzytelnienia z użyciem tajnego hasła znanego jedynie użytkownikowi.
2. Uwierzytelnienie na postawie tego, co użytkownik ma. Można do tej grupy zakwalifikować metody takie jak certyfikaty cyfrowe umieszczone na stacji użytkownika czy na osobnej karcie, systemy wykorzystujące różnego rodzaju tokeny sprzętowe.
3. Uwierzytelnienie na podstawie tego, kim użytkownik jest. Chodzi tutaj o cały szereg metod identyfikacji biometrycznej.

Istnienie tak wielu metod uwierzytelnienia, które, by sprostać oczekiwaniom użytkowników oraz wymogom bezpieczeństwa, mogą być jednocześnie zaimplementowane w systemie rozproszonym, narzuca konieczność stosowania elastycznych protokołów współpracy urządzeń składowych systemu rozproszonego z bazą danych.

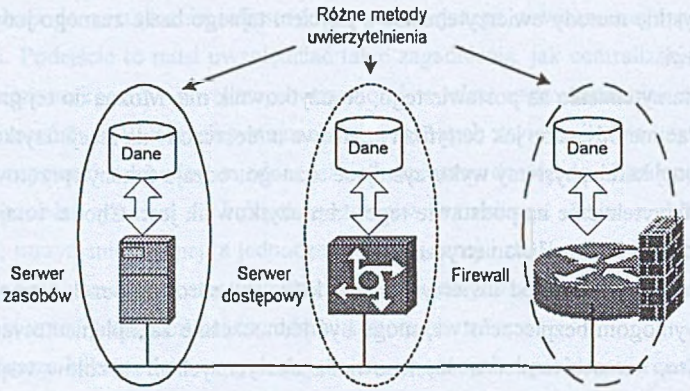
3. Modele składowania i przekazywania informacji o uwierzytelnieniu

Nieodzownym elementem potrzebnym, aby możliwe było kontrolowanie dostępu do zasobów z uwierzytelnieniem jest baza danych użytkowników. Taka baza zawiera informację o użytkownikach, którzy mają prawo uzyskania dostępu do określonych zasobów systemu. Uogólniając, można powiedzieć, że informacja ta bazuje zwykle na powiązaniu unikalnego identyfikatora użytkownika z informacją, która może być pomocna w ustaleniu tożsamości użytkownika. Funkcją bazy danych uwierzytelnień jest więc przyporządkowanie pewnej sekretnej informacji, np. hasła, do identyfikatora użytkownika (nazwy) i na życzenia serwerów zasobów dokonywanie weryfikacji czy próbujący się zalogować użytkownik podał właściwe informacje uwierzytelniające. Należy tutaj wspomnieć o potrzebie zabezpieczenia informacji, jakie przechowuje baza danych uwierzytelnień. W przypadku używania haseł nie mogą one być po prostu przechowywane w postaci niezabezpieczonej. Zwykle dokonuje się szyfrowania haseł lub poddaje się je mieszaniu za pomocą funkcji skrótu, jak np. MD5, tak, iż nawet włamanie do bazy i wykradzenie informacji o hasłach nie pozwoli na ich odgadnięcie.

Informacja o uwierzytelnieniu może być przechowywana lokalnie lub na podstawie centralnej bazy danych dostępnej przez sieć [2]. Zastosowanie każdej z tych dwu metod ma swoje uzasadnienie. Dalej zostaną one pokrótce scharakteryzowane.

3.1. Uwierzytelnienie lokalne

Informacja niezbędna do uwierzytelnienia jest przechowywana na lokalnej maszynie, na której proces uwierzytelniania zachodzi.

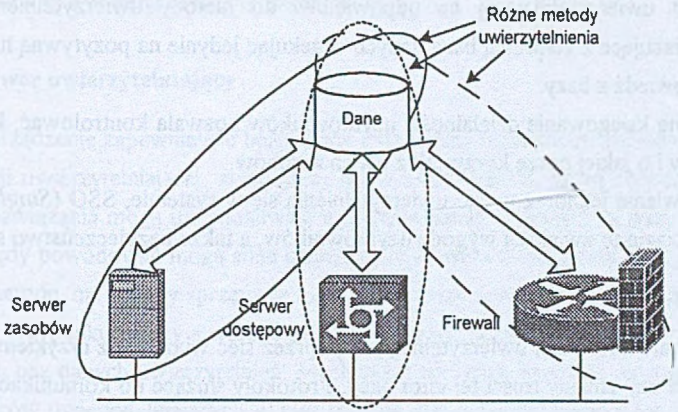


Rys.1. Model systemu z lokalnymi bazami danych uwierzytelnień
Fig. 1. The Model of system based on the local authentication database

Rysunek 1 przedstawia taką konfigurację. W systemie rozproszonym takie rozwiązanie prowadzi do nieuchronnej fragmentacji bazy danych uwierzytelnień. Administrator jest zmuszony do nieustannego wysiłku, mającego na celu utrzymanie synchronizacji pomiędzy rozproszonymi i odciętymi od siebie w tym przypadku bazami. Użytkownicy zmuszeni są do wielokrotnego uwierzytelniania się w systemie, co przy stosowaniu metody użytkownik/hasło zniechęca ich do stosowania trudnych do złamania, bezpiecznych haseł. Rozwiązanie to zupełnie nie skaluje się i nadaje się tylko dla małych sieci. Do jego zalet można zaliczyć fakt, że informacje uwierzytelniające wymieniane pomiędzy serwerem a bazą nie są przesyłane przez sieć. Problem różnorodności metod uwierzytelnienia dla poszczególnych składowych heterogenicznego systemu rozproszonego jest również łatwiejszy do rozwiązania, ponieważ każdy autonomiczny serwer współpracuje tylko ze swoją lokalną bazą danych oraz wprowadza swoją metodę uwierzytelnienia.

3.2. Model uwierzytelnienia oparty na centralnej bazie danych

Koncepcja tej metody zakłada istnienie w systemie rozproszonym centralnej bazy danych, która przechowuje informacje uwierzytelniające dla wszystkich użytkowników.



Rys. 2. Model systemu opartego na centralnej bazie danych uwierzytelnień
Fig. 2. The Model of system based on the centrally located authentication database

Każde urządzenie w systemie podczas procesu uwierzytelnienia użytkownika komunikuje się z serwerem uwierzytelniającym, zarządzającym bazą uwierzytelnień, w celu dokonania weryfikacji poprawności informacji przekazanej przez użytkownika. Rysunek 2 przedstawia schemat takiego rozwiązania.

3.2.1. Zalety systemu z centralną bazą danych uwierzytelnień

1. Podstawową zaletą takiego rozwiązania jest jego skalowalność. System rozproszony zbudowany w oparciu o centralną bazę danych uwierzytelnień działa równie dobrze w małej sieci, jak i dużej. Ograniczeniem może tu być jedynie wydajność przetwarzania maszyny, na której znajduje się baza danych.
2. Łatwość zarządzania użytkownikami. Utrzymując jedną centralną bazę danych użytkowników unika się kłopotów z synchronizacją poszczególnych lokalnych baz danych.. Prawa dostępu użytkowników mogą być ściśle kontrolowane, co umożliwia szybką reakcję w przypadku zaistnienia konieczności ograniczenia dostępu do zasobów konkretnej osobie, np. pracownikowi zwalnianemu z pracy, który dotychczas miał możliwość korzystania z zasobów firmy poprzez jeden z wielu serwerów dostępowych za pośrednictwem łącza komutowanego. Możliwe staje się wprowadzenie automatycznego czasowego blokowania użytkownikom dostępu do zasobów o określonej porze dnia czy określonego dnia tygodnia.
3. Wprowadzenie różnych technologii uwierzytelniających np. oprócz prostego rozwiązania użytkownik/hasło, zastosowanie metod biometrycznych czy tokenów sprzętowych. Serwery zasobów czy urządzenia dostępowe przerzucają ciężar weryfikacji in-

formacji uwierzytelniającej na odpowiednie do metody uwierzytelnienia systemy współpracujące z centralną bazą danych oczekując jedynie na pozytywną lub negatywną odpowiedź z bazy.

4. Centralne księgowanie działalności użytkowników pozwala kontrolować, którzy użytkownicy i o jakiej porze korzystali z jakich zasobów.
5. Umożliwienie jednorazowego uwierzytelnienia się w systemie, SSO (*Single Sign On*). Rozwiązanie to zwiększa wygodę użytkowników, a także bezpieczeństwo systemu.

3.2.2. Wady

1. Przesyłanie informacji uwierzytelniającej poprzez sieć wiąże się z ryzykiem podsłuchania haseł czy zmiany treści tej informacji. Protokoły służące do komunikacji serwerów zasobów z serwerem uwierzytelniającym muszą umożliwiać szyfrowanie przenoszonej informacji uwierzytelniającej. Wiąże się to z ryzykiem dokonania kryptoanalizy szyfru lub przechwycenia klucza szyfrującego, który np. w protokole TACACS+ jest stały i uzgadniany ręcznie w chwili konfigurowania urządzeń.
2. Centralna baza danych użytkowników ze względu na kluczową funkcję, jaką pełni w procesie uwierzytelniania, może być narażona na ataki mające na celu zablokowanie jej działania, wykradzenia lub zniszczenia informacji o użytkownikach lub nawet podszycia się w celu uzyskania nieuwierzytelnionego dostępu do zasobów. Problemem jest również zapewnienie ciągłości działania bazy, bez względu na możliwość zaistnienia awarii sprzętowych, poprzez zastosowanie redundantnej architektury serwera bazy danych uwierzytelnień.
3. Niekompatybilność rozwiązań dotyczących komunikacji poszczególnych, niejednorodnych, serwerów zasobów z centralnym serwerem uwierzytelniającym zarządzającym bazą danych uwierzytelnień.

4. Składowe systemu opartego na centralnej bazie uwierzytelnień

Podstawowymi elementami skalowalnej, niewrażliwej na problem heterogeniczności sieci, na której system rozproszony jest oparty, infrastruktury uwierzytelnienia użytkowników, są:

1. Serwery zasobów, do których można również zaliczyć serwery dostępowe dla użytkowników wdzwaniających się oraz bramy dla użytkowników łączących się z zewnętrznych sieci, takich jak Internet.
2. Serwery uwierzytelniające.
3. Protokoły umożliwiające komunikację pomiędzy tymi dwoma elementami.

Dalej omówione zostaną dwa ostatnie elementy.

4.1. Serwer uwierzytelniający

Jest to urządzenie zapewniające bezpieczny i skuteczny mechanizm składowania i dostępu do informacji uwierzytelniającej, znajdującej się w bazie danych, którą serwer ten zarządza. Istniejące rozwiązania mogą uniemożliwiać uzyskanie pełnej spójności tej bazy danych. Techniczne względy powodować mogą silne uzależnienie serwera uwierzytelniającego w oparciu o konkretną metodę, np. tokeny sprzętowe, od lokalnej bazy danych użytkowników tego serwera. W takim przypadku należy stworzyć możliwość przeźroczystego, dla użytkownika, dostępu do innych baz danych uwierzytelnień. Mechanizm taki musi bazować na wzajemnej współpracy serwerów uwierzytelniających w taki sposób, aby dla użytkownika ich odrębność była niezauważalna.

4.2. Protokoły komunikacyjne

Są to protokoły zapewniające komunikację pomiędzy urządzeniami zlecającymi uwierzytelnienie a serwerem uwierzytelniającym. Umożliwiają one wymianę informacji niezbędnej do prawidłowej współpracy tych urządzeń, niezależnie od platformy programowej czy sprzętowej, jakie reprezentują. Mechanizmy, jakie zaimplementowano w protokołach, muszą być na tyle uniwersalne, aby sprostać wymaganiom, jakie stawia heterogeniczność sieci, a także różnorodność metod uwierzytelnienia. Poniżej opisano bardziej szczegółowo kilka popularnych protokołów wykorzystywanych do uwierzytelniania użytkowników.

4.2.1. Protokół TACACS+

Protokół TACACS+ jest najnowszą generacją protokołu TACACS. TACACS+ używa TCP do transportu. Daemon serwera zwykle nasłuchuje portu nr 49, czyli portu LOGIN przypisanego do protokołu TACACS+. Ten port jest zarejestrowany w RFC zarówno dla UDP, jak i TCP. TACACS+ jest protokołem klient-serwer; klientem TACACS+ jest zwykle NAS (*Network Access Server*), lecz może to być każdy serwer zasobów systemu. Serwer TACACS+ współpracuje z bazą danych uwierzytelnień. Podstawowym elementem projektu TACACS+ jest rozdzielenie uwierzytelnienia, autoryzacji oraz obsługi kont.

TACACS+ umożliwia wymianę uwierzytelnień o narzuconej długości i zawartości, co umożliwia zastosowanie w klientach TACACS+ dowolnego mechanizmu uwierzytelnienia (włączając w to PAP PPP, CHAP PPP EAP PPP, tokeny sprzętowe czy inne)

W uwierzytelnieniu TACACS+ istnieją trzy rodzaje pakietów:

1. START, wysyłany przez klienta

2. CONTINUE, wysyłany przez klienta
3. REPLY, wysyłany przez serwer

Uwierzytelnienie rozpoczyna się od wysłania przez klienta do serwera komunikatu START. Komunikat START opisuje rodzaj uwierzytelnienia, jakie ma być wykonane, np. proste tekstowe hasło. Poza tym może zawierać nazwę użytkownika i dane uwierzytelniające. Pakiet START jest wysyłany tylko jako pierwszy komunikat sesji uwierzytelniającej TACACS+ lub jako pakiet pojawiający się natychmiast po restarcie. Pakiet START ma zawsze numer sekwencyjny równy 1. W odpowiedzi na pakiet START serwer wysyła pakiet REPLY. Komunikat ten sygnalizuje czy uwierzytelnienie jest już zakończone, czy powinno być kontynuowane. Jeśli REPLY sygnalizuje, że uwierzytelnienie powinno być kontynuowane, komunikat ten sygnalizuje, jakie nowe informacje są wymagane. Klient zdobywa te informacje i wysyła je w pakiecie CONTINUE. Proces ten powtarza się, dopóki nie zostaną zgromadzone wszystkie potrzebne do uwierzytelnienia informacje. Jeśli ten fakt nastąpi, to proces uwierzytelnienia kończy się. Oprócz procedury uwierzytelnienia protokół TACACS+ przeprowadza również proces uwierzytelnienia, a także księgowania działalności użytkownika. Transakcje pomiędzy klientem a serwerem TACACS+ są uwierzytelniane za pomocą wspólnych kodowanych informacji, które nigdy nie są przesyłane siecią. Zwykle są one ręcznie ustawiane na obu jednostkach. TACACS+ szyfruje cały ruch pomiędzy klientem TACACS+ oraz demonem serwera TACACS+. Więcej informacji na temat protokółu TACACS+ można znaleźć w pozycji oznaczonej nr [3].

4.2.2. Protokół Kerberos

Kerberos jest stworzonym przez MIT (*Massachusetts Instisute of Technology*) sieciowym protokołem uwierzytelnienia z tajnym kluczem, używającym kryptograficznego algorytmu DES do szyfrowania i uwierzytelnienia.

Kerberos został zaprojektowany do uwierzytelnienia żądań użytkowników dotyczących zasobów sieci. Jest oparty na koncepcji zaufanej strony trzeciej, przeprowadzającej weryfikacje użytkowników oraz usług. Ta zaufana strona trzecia nosi nazwę KDC (*Key Distribution Center*), czasami określana jako serwer uwierzytelnienia. W celu uwierzytelnienia użytkowników serwer Kerberos wydaje „bilety", które mają ograniczony czas życia. Mogą być one później użyte w miejsce standardowego mechanizmu uwierzytelnienia, używającego np. nazwy użytkownika oraz hasła.

Gdy klient chce utworzyć powiązanie z konkretnym serwerem zasobów, używa żądania oraz odpowiedzi uwierzytelnienia, aby najpierw zdobyć od KDC bilet oraz klucz sesji. Procedura ta składa się z następujących kroków:

1. Klient wysyła żądanie uwierzytelnienia do KDC, w którym zawiera swoją tożsamość, nazwę serwera zasobów, oczekiwany termin ważności biletu, pewną losową liczbę.
2. KDC weryfikuje prawa dostępu klienta i tworzy odpowiedź uwierzytelnienia.
3. KDC odsyła klientowi odpowiedź, w której zawiera klucz szyfrujący sesję, termin ważności biletu, losowy numer umieszczony pierwotnie w żądaniu klienta, nazwę serwera aplikacji. Informacje te są zaszyfrowane hasłem użytkownika, które było mu przypisane na serwerze uwierzytelnienia. W odpowiedzi tej znajduje się również bilet, w którym zawarty jest klucz szyfrujący sesję potrzebny do uwierzytelnienia klienta serwerowi zasobów.
4. Kiedy klient otrzymuje odpowiedź, wzywa użytkownika do podania hasła. Hasło to jest używane do rozszyfrowania odpowiedzi z KDC.

Teraz klient może już komunikować się z serwerem zasobów. Komunikacja ta polega na udowodnieniu konkretnemu serwerowi, że zna klucz szyfrujący sesję, wbudowany do biletu. Procedura jest następująca:

1. Klient wysyła do serwera zasobów żądanie, w którym zawiera otrzymany od KDC bilet zaszyfrowany znanym tylko KDC i serwerowi zasobów kluczem oraz uwierzytelnienie zawierające aktualny czas i sumę kontrolną zaszyfrowane kluczem sesji z towarzyszącego im biletu.
2. Po odebraniu żądania serwer zasobów rozszyfrowuje bilet tym samym kluczem, który KDC użyło do zaszyfrowania. Z biletu pobiera klucz sesji i rozkodowuje uwierzytelnienie. Jeśli do zaszyfrowania został użyty ten sam klucz, który był używany do rozszyfrowania, suma kontrolna będzie się zgadzać. Na tej podstawie serwer zasobów może przyjąć, że klient o nazwie podanej w bilecie jest tym, za kogo się podaje. Dodatkowym zabezpieczeniem uwierzytelnienia, chroniącym przed powtórzeniem, jest sprawdzenie znacznika czasu, który musi się zgadzać z aktualnym czasem weryfikującego z wcześniej zdefiniowaną dokładnością.
3. Serwer generuje odpowiedź do klienta, w której umieszcza znacznik czasu z uwierzytelnienia oraz inne informacje. Wszystko jest zaszyfrowane kluczem sesji.

Więcej informacji na temat protokołu Kerberos można znaleźć w pozycjach oznaczonych nr [1,4].

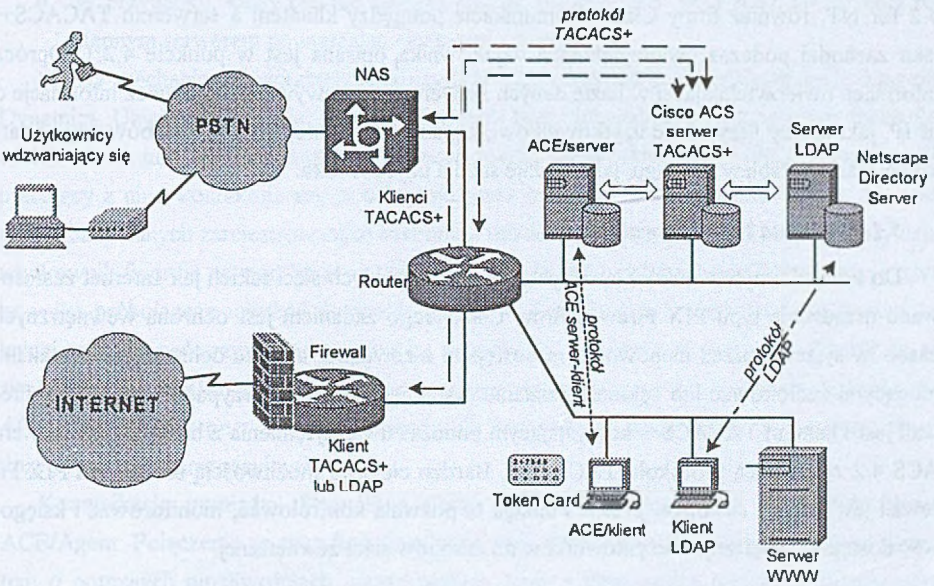
4.2.3. Protokół EAPOE

Dla użytkowników komputerów PC, znajdujących się w obszarze ograniczonym zaporą ogniową, istnieje kilka metod legalizacji. Nowa specyfikacja protokołu EAPOE [5] zapożycza protokół EAP [6] z mechanizmu transportowego protokołu PPP [7] i następnie przydziela go do nowego mechanizmu transportowego, jakim jest Ethernet. Protokół EAPOE rozpoczyna

akcję natychmiast, gdy ethernetowy port przełącznika sieci LAN wykryje nowe połączenie. Przełącznik, wysyłając pakiet EAPOE z komunikatem *Request Identity*, wyszukuje nowo podłączone urządzenia. Nowe urządzenie, takie jak komputer PC użytkownika, umieszcza identyfikator ID użytkownika w polu danych EAPOE i wysyła pakiet z powrotem do przełącznika. Następnie przełącznik przekazuje tę informację do serwera RADIUS [8] w komunikacie *Access Request* protokołu EAP. Podczas komunikowania się z serwerami RADIUS pakietu protokołu EAP nie wolno kapsułkować w ramki Ethernet, ponieważ, podobnie jak w protokole PPP, protokół EAP nie jest w stanie użyć protokołu RADIUS jako mechanizmu transportowego. Serwer RADIUS odpowiada wysyłając zwrotnie do przełącznika komunikat *Access Challenge*, faktycznie prosząc o hasło. Przełącznik kapsułkuje prośbę w EAOPOE i wysyła do żądającego komputera PC. Z kolei komputer PC wprowadza swoje hasło i wysyła je za pośrednictwem protokołu EAPOE z powrotem do przełącznika. Zazwyczaj hasła są wysyłane w formie zaszyfrowanej - kompatybilnej z oprogramowaniem szyfrującym. Jest to dodatkowa zaleta protokołu EAP i co się z tym wiąże protokołu EAPOE. Przełącznik umieszcza hasło w pakiecie *Access Response* protokołu EAP, kapsułkując go w protokole RADIUS dla transmisji do serwera RADIUS. Z chwilą gdy serwer RADIUS stwierdzi zgodność identyfikatora ID i hasła ze swoją bazą danych, wysyła komunikat *success* do przełącznika, który natychmiast aktywuje połączenie portu użytkownika. Jeśli topologia sieci nie dopuszcza zatorów związanych z obsługą We/Wy, to przy rozsądnych szybkościach dostępu do bazy danych cały proces nie powinien zająć więcej niż jedną sekundę. Chociaż proces ten wydaje się prosty, to protokół EAPOE oferuje wyrafinowany mechanizm w celu zabezpieczania sieci LAN z różnymi topologiami i rozmaitymi metodami zabezpieczeń. W dużej mierze dzięki zmiennej długości pola danych w protokole EAP, które może przystosować szeroki zakres techniki bezpieczeństwa, standard może być użyty z praktycznie wszystkimi obecnie istniejącymi i przyszłymi metodami zabezpieczeń, w tym MD5 lub kartami token.

5. Przykład implementacji systemu rozproszonego z centralną bazą danych uwierzytelnień

Poniższa implementacja jest przykładem heterogenicznej sieci komputerowej opartej na protokole IP, do której przewidziano wszechstronny dostęp z zewnątrz przy jednoczesnym zapewnieniu szeregu metod uwierzytelnienia użytkowników. Jak widać na rysunku 3 w sieci oprócz serwerów zasobów i serwerów dostępowych istnieją też urządzenia aktywne, takie jak routery i switche, które wymagają zdalnego zarządzania.



Rys. 3. Praktyczny przykład systemu rozproszonego z centralnie umieszczoną bazą danych uwierzytelnień

Fig. 3. Example of distributed system with centrally located user authentication database

5.1. Elementy systemu

System składa się z kilku podstawowych elementów zapewniających użytkownikom zdalnym jak i lokalnym bezpieczny i kontrolowany dostęp do zasobów. Wszystkie urządzenia wymagające uwierzytelnienia użytkowników podczas zdalnego dostępu współpracują z odpowiednim dla metody uwierzytelnienia serwerem. Spójność centralnej bazy danych, która de facto rozsiana jest na trzech różnych urządzeniach, zapewniają odpowiednie mechanizmy współpracy między poszczególnymi serwerami. Żądanie uwierzytelnienia użytkownika w oparciu o przypisaną mu metodę na serwerze zasobów lub serwerze dostępowym zostaje automatycznie przekierowane do właściwego serwera.

5.1.1. Serwer dostępowy NAS (Network Access Server)

Urządzenie to służy jako serwer dostępowy dla użytkowników uzyskujących dostęp do zasobów systemu poprzez komutowaną abonencką sieć telefoniczną analogową PSTN lub cyfrową ISDN. W omawianej implementacji wykorzystano Access Server AS5300 firmy Cisco. Urządzenie to udostępnia również funkcję routera. Do komunikacji z serwerem uwierzytelniającym stosuje się, opisywany w punkcie 4.2.1, protokół TACACS+. Serwer dostępowy jest klientem TACACS+, natomiast rolę serwera TACACS+ pełni Access Control Server ACS

4.2 for NT, również firmy Cisco. Komunikacja pomiędzy klientem a serwerem TACACS+, jaka zachodzi podczas uwierzytelnienia użytkownika, opisana jest w punkcie 4.2.1. Oprócz informacji uwierzytelniającej w bazie danych serwera przechowywane są również informacje o nr IP, jaki należy przydzielić użytkownikowi, ograniczeniach dostępu do zasobów czy dodatkowej trasie w tablicy routingu, jaką dodaje się dla użytkownika.

5.1.2. Brama typu Firewall

Do kontroli użytkowników łączących się z zewnętrznych sieci takich jak Internet zastosowano urządzenie typu PIX Firewall firmy Cisco. Jego zadaniem jest ochrona wewnętrznych zasobów systemu przed niepowołanym dostępem z zewnątrz, a także ochrona przed atakami mogącymi zablokować lub zakłócić działanie systemu. Tak jak w przypadku NAS, PIX firewall jest klientem TACACS+, korzystającym podczas uwierzytelnienia z bazy danych serwera ACS 4.2 za pomocą protokołu TACACS+. Bardzo ciekawą możliwością urządzenia PIX Firewall jest funkcja *cut-throw proxy*. Funkcja ta pozwala kontrolować, monitorować i księgować dostęp wewnętrznych użytkowników do zasobów sieci zewnętrznej.

5.1.3. Serwery uwierzytelniające

W systemie zastosowane zostały trzy serwery uwierzytelniające. Każdy obsługuje określoną klasę użytkowników wymagających uwierzytelnienia w określony dla siebie sposób. Rozwiązanie takie jest kompromisem pomiędzy kwestią zapewnienia spójności i skalowalności bazy danych uwierzytelnień a wprowadzeniem do systemu wielu metod uwierzytelnienia odpowiadających potrzebom bezpieczeństwa oraz wygody użytkowników.

Dla urządzeń, które posiadają możliwość współpracy z protokołem TACACS+, czyli są klientami TACACS+, serwerem uwierzytelniającym, serwerem TACACS+, jest Cisco ACS 4.2. Serwer ten posiada lokalna bazę danych użytkowników, lecz może również korzystać z zewnętrznych baz danych uwierzytelnień, takich jak oferują LDAP, NDS i wiele innych. Mechanizm integrujący bazy danych zewnętrznych serwerów jest następujący:

1. Po otrzymaniu od klienta wezwania do uwierzytelnienia użytkownika serwer Cisco sprawdza w swojej lokalnej bazie danych, czy użytkownik istnieje.
2. Jeśli tak, to następuje jego uwierzytelnienie, a jeśli nie to zależnie od konfiguracji serwer albo odrzuca użytkownika, albo rozpoczyna współpracę z zewnętrzną bazą danych.
3. Jeśli użytkownik ma być uwierzytelniony na podstawie zewnętrznej bazy danych, serwer Cisco ACS porozumiewa się z serwerem zewnętrznym zlecając mu uwierzytelnienie użytkownika i pośrednicząc pomiędzy zlecającym uwierzytelnienie klientem TACACS+ a określonym serwerem uwierzytelniającym.

4. W przypadku, kiedy i to nie daje rezultatów, serwer Cisco ACS komunikuje się z następnym serwerem powtarzając czynności z punktu 3.

Mocny mechanizm uwierzytelnienia użytkowników zapewnia ACE/Server firmy Security Dynamics. Użytkownicy zdalni muszą podać swój kod PIN oraz kod podany przez token SecurID w celu udostępnienia zasobów wewnętrznych. Serwer dostępowy (ACE/Agent współpracujący z nim) kontaktuje się, w celu dokonania uwierzytelnienia, z ACE/Server. Na podstawie bazy danych zarejestrowanych tokenów i użytkowników ACE/Server określa, czy dany użytkownik figuruje na jego liście czy też nie. Pozwala to na jednoznaczną identyfikację użytkownika próbującego uzyskać dostęp do zasobów. Rozwiązanie uwierzytelnienia w sieci lokalnej zakłada wykorzystanie agentów na wszystkich urządzeniach mających dostęp do tej sieci. Agenci kontaktują się z oprogramowaniem zarządzającym danymi o użytkownikach - ACE/Server, który pozwala na wprowadzenie scentralizowanych usług uwierzytelnienia w dużych sieciach korporacyjnych.

Komunikacja pomiędzy SecurID a Cisco ACS wykonywana jest przez API klienta ACE/Agent. Połączenie ze sobą funkcjonalności tych dwóch narzędzi daje do dyspozycji system o potężnych możliwościach, umożliwiający ścisłą i niezawodną kontrolę dostępu użytkowników do poszczególnych zasobów.

Obok serwera Cisco ACS i ACE/Serwera w systemie zastosowano również serwer LDAP *(LDAP – Lightweight Directory Access Protocol)* [9]. Protokół LDAP jest wykorzystywany do komunikacji w modelu klient-serwer pomiędzy klientami LDAP a serwerem LDAP. Głównym zadaniem serwera LDAP jest przechowywanie informacji w swoim „drzewie informacji". Obecnie serwery LDAP służą głównie do przechowywania informacji na temat użytkowników systemów komputerowych. Za ich pomocą można tworzyć systemy centralnego zarządzania profilami użytkowników, tzn.: w rozproszonym środowisku komputerowym, gdzie dany użytkownik posiada dostęp do zasobów na różnych komputerach np.: serwery domeny NT, serwery bazo-danowe, serwery usług internetowych (e-mail, www, itp.), itp. za pomocą serwera LDAP można logować się do tych systemów z użyciem jednego i tego samego konta (np.: serwer UNIX'owy podczas próby logowania nie sprawdza hasła z pliku /etc/passwd, lecz komunikuje się z serwerem LDAP w celu uwierzytelnienia danego użytkownika). Serwery LDAP mogą również służyć jako narzędzie do tworzenia usług logowania typu SSO (*Single Sign On*). Jako serwer LDAP zastosowano jeden z popularniejszych produktów na rynku, Netscape Directory Server. Serwer Cisco ACS może korzystać z bazy danych uwierzytelnień serwera LDAP i uwierzytelniać użytkowników tam zapisanych, na klientach TACACS+, których obsługuje.

LITERATURA

1. Kaeo M.: Tworzenie bezpiecznych sieci. Mikom, Warszawa 2000.
2. Seiferd K.: WWW Authentication. http://www.securityportal.com/.
3. Carrel D.: Grant L.: The TACACS+ Protocol ver. 1.76. Cisco Systems, 1996.
4. Tung B.: The Moron's Guide to Kerberos. http://www.isi.edu/.
5. Nowy standard zabezpieczy sieci LAN. http://www.networld.pl/.
6. Blunk L., Vollbrecht J.: PPP Extensible Authentication Protocol (EAP). RFC 2284.
7. Perkins D., Hobby R.: The Point-to-Point Protocol (PPP). RFC 1172.
8. Rigney C., Rubens A., Simpson W., Willens S.: Remote Authentication Dial In User Service (RADIUS). RFC 2138.
9. Kosiur D.: LDAP: The next-generation directory? http://www.sunworld.com/swol-10-1996/swol-10-ldap.html.

Recenzent: Dr inż. Dariusz Augustyn

Wpłynęło do Redakcji 15 marca 2001 r.

Abstract

This study focuses reader attention on building distributed systems with user authentication based on the centrally located authentication database issues.
It also consider access to the authentication database information problem which occurs because the database is a separate device, accessible only through the network.

Chapter 2 describes the idea of authentication users in the computer network that form a distributed system with common available resources. Three main authentication method groups with short descriptions have been also shown.

Chapters 3 and 4 present two authentication information storing models that are used today in computer networks. The first method is storing authentication information locally, directly on the machine that has to authenticate the user, as it shown on Figure 1. Second, depicted on Figure 2, is gathering this information in one place in central database, managed the by authentication server. Each, widely understood, resources server (access servers and internet gateways can be numbered among them) have to communicate with an authentication server, to get authentication information concerned with given user. Some of authentication protocols which enable communication between resource servers and authentication database

server have been described. There are also in those chapters a multi protocol integration and coherent database maintaining problem issues covered.

In chapter 5, a hypothetical, but based on existing solutions network has been presented. This network (Figure 3) is an example of system with spread resources and centrally located authentication servers. They cooperate to maintain coherent user database, in the presence of a number of authentication methods implemented in the system.