ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1999
Seria: INFORMATYKA z. 36 Nr kol. 1414

Henryk KRAWCZYK
Politechnika Gdańska, Wydział Elektroniki, Telekomunikacji i Informatyki

WYKRYWANIE INTRUZÓW W ROZPROSZONYCH SYSTEMACH INFORMATYCZNYCH

Streszczenie. Przedstawiono charakterystykę typowych zagrożeń, podstawowe modele zabezpieczeń w rozproszonych systemach informatycznych. Zaprezentowano protokoły uwierzytelniania w systemie Kerberos oraz sposoby wykrywania intruzów w systemie IDES. Zaproponowano proste metody ochrony środowiska bazy danej przed intruzami oraz wykorzystanie mobilnych agentów do śledzenia intruzów.

INTRUSION DETECTION IN DISTRIBUTED INFORMATION - PROCESSING SYSTEMS

Summary. Typical treads, basic secure models implemented in information - processing systems are characterised. Authentication protocols in the Kerberos system and methods of intrusion detection in the IDES system are described. The simple mechanisms improving security of database environment are proposed and the way of tracing intrusions by mobile agents is suggested.

1. Wprowadzenie

Współczesne systemy informatyczne obsługują setki użytkowników, wykorzystując dane o ogromnej ilości i wartości. Poziom wiarygodności systemów [10] zależy od metod tolerowania i unikania uszkodzeń (safety), zachowania spójności przesyłanych lub przechowywanych danych (integrity), autoryzacji dostępu i poufności (security) oraz monitorowania określonych zdarzeń i stanów w systemie (historical records). Zwiększenie wiarygodności funkcjonowania uzyskuje się poprzez wykorzystanie odpowiednich metod

archiwizacji danych (przechowywanie na różnych dodatkowych nośnikach w możliwie bezpiecznym miejscu), zapis lustrzany (jednoczesne zapisywanie tych samych danych na dwóch lub więcej urządzeniach fizycznych [10]) czy replikację danych (utrzymanie wielu kopii danych na różnych węzłach sieci [5]). Zachowanie spójności danych polega na uwzględnianiu pewnych zależności logicznych pomiędzy poszczególnymi elementami bazy danej. Sprowadza się to do kompletnego wykonywania transakcji (tzn. transakcje mogą być albo wykonywane w całości, albo zaniechane [4, 3]), za co odpowiadają na ogół systemy zarządzania bazami danych. Autoryzacja dostępu do danych i zapewnienie ich poufności polegają na przestrzeganiu zdefiniowanych reguł dostępu i kontroli uprawnień użytkowników [9], a także wykorzystaniu systemów kryptograficznych [14]. Monitorowanie zachowania się systemu ma na celu wykrycie anomalii pojawiających się w systemie. Może ono być wykorzystane dla detekcji i lokalizacji źródeł błędów (defektów). W zależności od typu monitorowanej informacji, techniki te mogą zostać również użyte do detekcji i lokalizacji intruzów danego systemu [16].

W sieciach komputerowych występuje podstawowa sprzeczność pomiędzy nieograniczonymi możliwościami komunikacyjnymi a wymaganym poziomem ochrony pracy użytkownika [7, 15]. Jest to wyzwaniem do wprowadzenia rozwiązań kompromisowych oraz ciągłego ich udoskonalania [2, 6]. Wraz z rozwojem aplikacji rozproszonych zapewnienie odpowiedniej równowagi pomiędzy komunikacją a zabezpieczeniem systemu stało się sprawą najwyższej wagi [1, 8, 13, 17, 18]. Istnieją już standardy określające dopuszczalne poziomy zabezpieczeń. Przykładem może być „Pomarańczowa Książka" [12] lub Protokół Zarządzania SNMP [15]. Pierwsza pozycja przedstawia różne klasy ochrony systemów i podaje warunki, które powinna spełniać każda z tych klas. Protokół SNMP specyfikuje trzy klasy bezpieczeństwa: integralność danych, autentyfikację danych oraz poufność danych. Co więcej, istnieje standard IEEE 802.10 (SILS - Standard for Interoperable LAN Security [9]), który określa wymagane usługi bezpieczeństwa, definiuje logiczne i fizyczne mechanizmy dla zapewnienia wymaganego poziomu bezpieczeństwa. Poza tym podaje standardy dotyczące usług, protokołów, formatów danych i interfejsów. W przypadku zabezpieczeń definiuje: wymianę danych w warstwie danych, sposoby zarządzania kluczami kryptograficznymi oraz zasady zarządzania siecią, w tym zarządzanie bezpieczeństwem. Dokument ISO/IEC 7498 - 2 definiuje zbiór usług związanych z bezpieczeństwem

systemu [14]. Należy wyjaśnić, że w języku angielskim istnieją dwa różne słowa: safety (bezpieczeństwo) i security (zabezpieczenie, ochrona). Określane przez standardy usługi systemów związane są z ich zabezpieczeniem, tj. security.

W pracy ograniczamy się do problemu metod wykrywania intruzów pracujących w sieci. Intruzem nazywamy osobę, która wykorzystuje dany system informatyczny bez pozwolenia bądź posiada autoryzację, ale przekracza dopuszczalne uprawnienia. Działalność intruza w sieci może być aktywna bądź pasywna. Działalność pasywna ma miejsce wówczas, gdy intruz korzysta z cudzej informacji, ale nie dokonuje żadnych zmian w systemie. Aktywna działalność związana jest z wprowadzeniem różnych zmian, włączając w to niszczenie informacji. W obu przypadkach może prowadzić to do poważnych zagrożeń. W związku z tym niezbędne są mechanizmy uniemożliwiające włamanie się do systemu, a gdy to już nastąpi - wykrycie i odizolowanie sprawców włamania. W pracy przedstawiono podstawowe strategie ochrony systemu przed intruzami (system KERBEROS [3]) oraz metody ich wykrywania (system IDES [4]). Podano również wybrane mechanizmy zabezpieczeń, które mogą być wykorzystywane w różnych sieciowych systemach informatycznych [1].

2. Podstawowy model zabezpieczeń

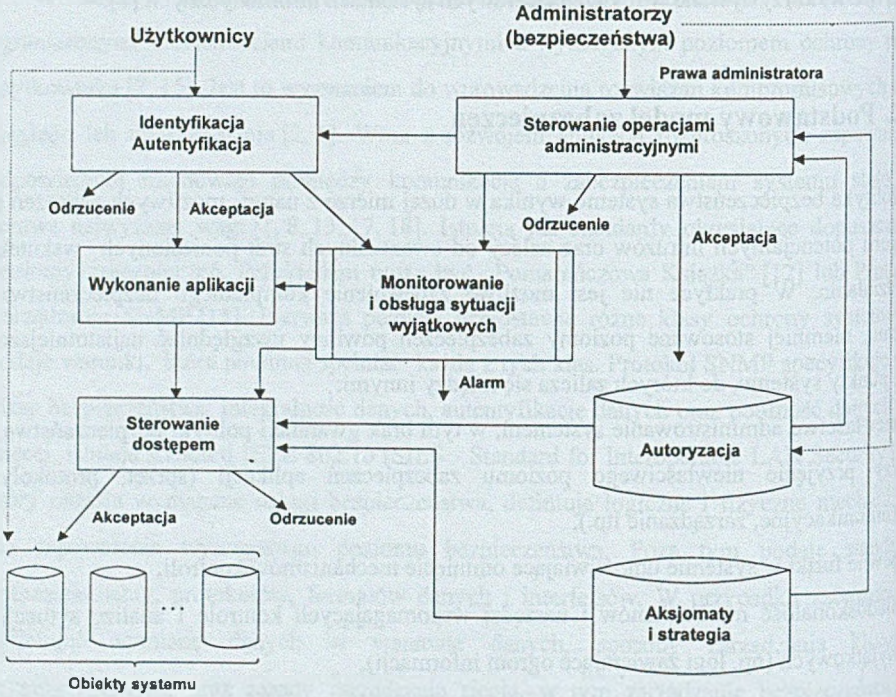
Polityka bezpieczeństwa systemu wynika w dużej mierze z natury możliwych zagrożeń i kategorii potencjalnych intruzów oraz zależy od ewentualnych strat poniesionych wskutek ich działania. W praktyce nie jest możliwe zapewnienie kompletnego bezpieczeństwa systemu, niemniej stosowane poziomy zabezpieczeń powinny uwzględniać najistotniejsze słabe punkty systemu, do których zalicza się między innymi:

- niewłaściwe administrowanie systemem, w tym brak gwarancji polityki bezpieczeństwa, czy przyjęcie niewłaściwego poziomu zabezpieczeń aplikacji (sprzęt, protokoły komunikacyjne, zarządzanie itp.),
- pewne furtki w systemie umożliwiające ominięcie mechanizmów kontroli,
- niedoskonałość mechanizmów i narzędzi wspomagających kontrolę i analizę sytuacji wyjątkowych (np. logi zawierające ogrom informacji),
- niepowtarzalność czy nieprzewidywalność pewnych działań intruzów i uwzględnienie tylko typowych charakterystyk ich zachowań.

Koncepcja detekcji obecności intruzów w systemie polega na monitorowaniu systemu, sygnalizowaniu niedozwolonych działań, śledzeniu podejrzanego zachowania się użytkowników, a także stawianiu odpowiednich pułapek i ewentualnie podejmowaniu właściwych reakcji kryzysowych.

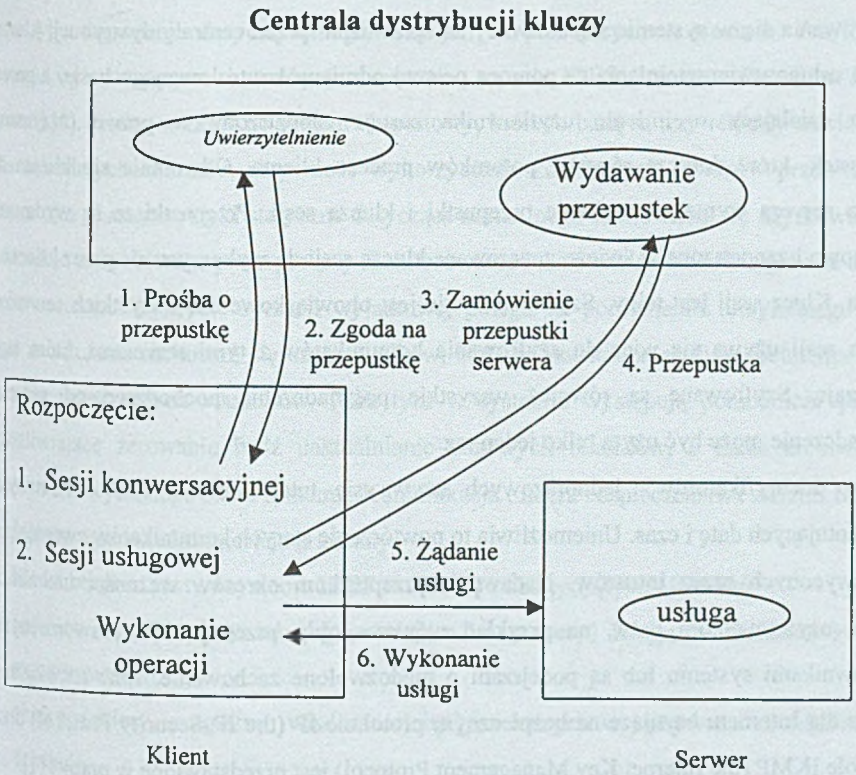
Jednoznaczne sprecyzowanie wymagań odnośnie do zabezpieczeń wymaga opracowania odpowiedniego modelu bezpieczeństwa. Opracowane modele dotyczące baz danych dzielą się na dwie kategorie:

- DSM (Discretionary Security Model) kontroluje dostęp użytkowników do informacji na podstawie identyfikatora użytkownika, praw określanych dla użytkownika i obiektów systemu. Innymi słowy, dostęp do obiektu zapewnia autoryzacja użytkownika. Z kolei użytkownik może autoryzować innych użytkowników w celu dostępu do jego obiektów.
- MSM (Mandatory Security Model), który kontroluje indywidualny dostęp do informacji na bazie klasyfikacji, obiekt aktywny (proces, transakcja) - obiekt pasywny (zbiór danych, rekord, pole rekordu itp.).



Rys. 1. Elementy modelu zabezpieczeń
Fig. 1. Elements of security model

Rysunek 1 podaje model zabezpieczeń na ogólnym poziomie bazy danej. Wyróżniamy w nim model użytkowników, którzy poprzez procesy wymagają dostępu do różnego typu obiektów. Na początku następuje identyfikacja użytkownika i sprawdzenie jego autentyczności. Następnie występuje drugi stopień ochrony związany z dostępem do obiektów. Obiekty zawierają informację, która jest chroniona przed nieautoryzowanym dostępem lub jej modyfikacją. Blok sterowania dostępem zawiera różne reguły dostępu, które w przypadku spełnienia umożliwiają dostęp do obiektu. Odpowiednie reguły czy aksjomaty przechowywane są w bazie danych. Zasady autoryzacji i prawa dostępu mogą być zmienione przez administratora, który również może być kontrolowany. Sytuacje wyjątkowe są monitorowane i sygnalizowane. W krytycznych sytuacjach, gdy funkcjonowanie systemu jest zagrożone, włącza się alarm.



Rys. 2. Mechanizmy uwierzytelnienia w systemie Kerberos
Fig. 2. Authentication mechanisms in Kerberos

Wówczas staje się konieczna niezależna interwencja służb specjalnych. Z rysunku 1 wynika prosta metoda detekcji intruzów.

Wykorzystuje się trzy podstawowe strategie:

- analizę anomalii w zachowaniu się użytkownika,
- uczulenie systemu na typowe akcje związane z wkradaniem się do systemu (trop doors),
- audytowanie systemu i analizę zebranych informacji.

Dwie pierwsze strategie są typu on-line, ostatnia z uwagi na ilość zapisanej informacji jest typu off-line. Wszystkie wymagają pewnych narzędzi wspomagających.

Przykładem standardowego systemu zabezpieczeń przed nieupoważnionym dostępem jest system Kerberos. Jest to protokół uwierzytelniania oparty na protokole Needhama i Schroedera z kluczem tajnym [5]. Rys. 2 wyjaśnia jego zasadę działania. Bierze pod uwagę trzy rodzaje obiektów bezpieczeństwa: przepustki, poświadczenia i klucze sesji. Podczas rejestrowania się w systemie użytkownicy są sprawdzani przez centralę dystrybucji kluczy. Jest to usługa uwierzytelniania za pomocą pewnej odmiany kontrolowanego hasła, a proces klienta działający w imieniu użytkownika zostaje zaopatrzony w prawo otrzymania przepustek, które dotyczą również potomków procesu klienta. Odwołanie się klienta do danego servera wymaga uzyskania przepustki i klucza sesji. Przepustki te są wydawane terminowo i zaopatrzone w świeżo generowane klucze sesji do wykorzystania przez klienta i servera. Klucz sesji jest tajny. Szyfrowanie nie jest obowiązkowe dla wszystkich serverów. Klucza sesji używa się więc do szyfrowania komunikatów z tymi serverami, które tego wymagają. Szyfrowane są również wszystkie poświadczenia pochodzące od servera. Poświadczenie może być użyte tylko jeden raz.

Jako identyfikatorów jednorazowych używa się tutaj wartości liczb całkowitych reprezentujących datę i czas. Uniemożliwia to powtórzenie starych komunikatów ewentualnie przechwyconych przez intruzów. Nadawanie przepustkom okresów ważności umożliwia cofanie użytkownikom praw, na przykład wówczas, gdy przestają być prawomocnymi użytkownikami systemu lub są podejrzani o niedozwolone zachowanie. Inne rozwiązanie typowe dla Internetu bazujące na bezpiecznym protokole IP (the IP Security Protocol) oraz protokole IKMP (the Internet Key Management Protocol) jest przedstawione w pracy [11].

3. System wykrywania intruzów

System wykrywania intruzów powinien być systemem czasu rzeczywistego, który uczulony jest na zadaną klasę zdarzeń. Dotyczą one:

1) odgadywania lub pozyskiwania hasła użytkowników,
2) ominięcia mechanizmów ochrony i dokonywania penetracji systemu,
3) próby wykorzystania sytuacji specyficznej, np. generowania większej ilości kopii niż wymagano, logowania się w nietypowym czasie bądź zapisywania w nietypowy sposób (np. wiele operacji typu read),
4) interferencji z prawowitymi użytkownikami,
5) wprowadzenia odpowiednich wirusów czy robaków,
6) spowodowania odmowy usług, np. poprzez zamknięcie resursów.

Tego typu zagrożenia dotyczą na ogół baz danych pracujących w sieciach. Przykładem systemu wykrywającym intruzów jest system o nazwie IDES (Intrusion Detection Expert System) [4]. Jest to w zasadzie system ekspertowy, którego bazą są trzy rekordy zawierające opis zaistniałych anomalii, aktywność wykorzystania konkretnych resursów przez danego intruza oraz charakterystyki statyczne dotyczące normalnego zachowania się użytkowników. Informacje te są zbierane przez procesy monitorowania i testowania i stanowią główne dane o stanie systemu. Wykrycie sytuacji wyjątkowej polega na porównaniu otrzymanego stanu bądź ze wzorami zachowań się użytkowników, bądź na podstawie analizy spełnienia przez ten stan wymaganych warunków. Poza tym w systemie występują pomocnicze procesy umożliwiające zerowanie bądź uaktualnianie bazowych rekordów, a także archiwizację każdego lub wybranego stanu systemu. Komunikacja oficera bezpieczeństwa z IDES odbywa się poprzez odpowiedni interfejs graficzny.

Model bezpieczeństwa systemu IDES składa się z następujących elementów:

- podmioty (użytkownicy lub odpowiadające im procesy) inicjujące działanie systemu monitorowania,
- obiekty (zbiory, programy, wiadomości itp.), na których wykonywane są odpowiednie działania,
- rekordy audytowe charakteryzujące monitorowaną informację (patrz rys. 3),

- profile opisujące zachowanie się podmiotów w odniesieniu do wykorzystywanych obiektów,
- rekordy anomalii rejestrujące nieprawidłowe zachowanie się użytkowników,
- zasady aktywności określające akcje, które muszą być wykonane, kiedy spełnione są podane warunki zachowania się użytkownika.

Rekord anomalii składa się z trzech pól: <zdarzenie, czas, charakterystyka>, rekord aktywności użytkownika zawiera 4 pola <zasady generowania rekordu, zasady jego uaktualniania, zdarzenia lub charakterystyki, zasady okresowej analizy anomalii>.

Rekordy kontrolne

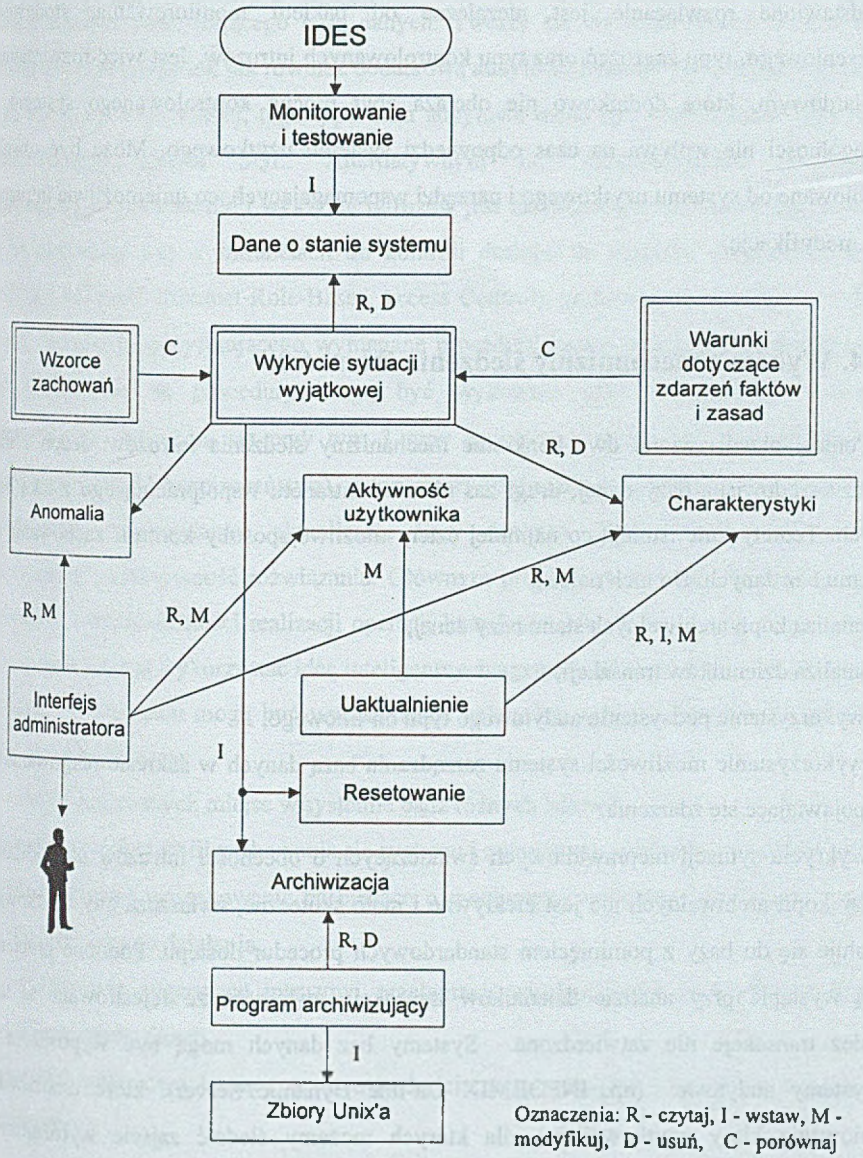
Wykonana operacja	Podmiot żądający operacji	Obiekt, na którym wykonano operację	Warunki wyjątkowe	Wykorzystanie resursów	Czas

Rys. 3. Struktura rekordu audytowego
Fig. 3. Audit record format

Rekordy profili określone są za pomocą dziesięciu następujących parametrów: <nazwa zmiennej, akcja, warunek wyjątkowy, wykorzystanie resursów, okres obserwacji, typ zmiennej, waga, użytkownik, obiekt, wartość obserwowanej zmiennej>.

Zmienna może dotyczyć liczby zdarzeń, akcji, ilości wykonywanych instrukcji w zadanym okresie obserwacji. Uwzględnia się przy tym takie akcje, jak: login, read, execute. Czas obserwacji może być definiowany jako czas między dwoma skorelowanymi zdarzeniami. Przez wykorzystanie resursów rozumiemy: zaangażowanie czasu procesora czy urządzeń we-wy, liczby odczytanych rekordów itp.

Takie charakterystyki są zbierane dla wszystkich użytkowników. Określa się dla nich parametry statystyczne, jak średnie wartości i odchylenia standardowe. Zmiana tych wartości w analizowanym okresie czasu oznaczać może obecność intruza w sieci. Co więcej, dokładniejsza analiza może określić, jakiego typu zagrożenia mogły się pojawić w systemie. Do tej analizy wykorzystać można metody sztucznej inteligencji czy komputery neuronalne.



Rys. 4. Architektura sytemu IDES
Fig. 4. IDES Architecture

Współpracę bazowych komponentów IDES przedstawia rys. 4. Podano na nim wykorzystywane opcje kontroli, jak i prawa dostępu dotyczące podstawowych zbiorów. Przedstawione rozwiązanie jest niezależne od pakietu monitorowania, środowiska obliczeniowego, typu zagrożeń oraz typu kontrolowanych intruzów. Jest więc rozwiązaniem standardowym, które dodatkowo nie obciąża zbyt mocno kontrolowanego systemu, w szczególności nie wpływa na czas odpowiedzi systemu użytkowego. Może być również odizolowane od systemu użytkowego i narzędzi wspomagających, co uniemożliwia intruzowi jego modyfikację.

4. Wybrane mechanizmy śledzenia intruzów

Poniżej przedstawiono dwa konkretne mechanizmy śledzenia intruzów. Jeden z nich dotyczy środowiska bazy danej, drugi zaś również intranetu współpracującego z taką bazą danych. Teoretycznie istnieją co najmniej cztery możliwe sposoby kontroli zachowania się systemu baz danych. Do nich należą:

- analiza kopii archiwalnych stanu bazy danej,
- analiza dzienników transakcji,
- wykorzystanie podsystemu audytowego typu on-linowego,
- wykorzystanie możliwości systemu zarządzania bazą danych w zakresie reagowania na pojawiające się zdarzenia.

Wykrycie sytuacji nieprawidłowych świadczących o obecności intruzów na podstawie analizy kopii archiwalnych nie jest efektywne i mało skuteczne, zwłaszcza gdy użytkownik odwołuje się do bazy z pominięciem standardowych procedur dostępu. Podobne problemy mogą wystąpić przy analizie dzienników transakcji, zwłaszcza że rejestrowane są tam również transakcje nie zatwierdzone. Systemy baz danych mogą być wyposażone w podsystemy audytowe (np. INFORMIX On-line Dynamic Server), które umożliwiają definiowanie klasy użytkowników, dla których możemy śledzić zajście wyróżnionych zdarzeń. Lista tych zdarzeń może być długa i obejmuje dostęp do obiektów czy utworzenie różnych obiektów (tablica, widok), uruchomienie procedur, programów czy transakcji, ustawianie trybów, priorytetów, a także usunięcie obiektów czy ich maskowanie. Na ogół informacje z tego typu narzędzi trafiają do plików systemu operacyjnego, co utrudnia ich

dodatkową analizę poza wykorzystaniem dostępnych funkcji systemu operacyjnego. Dla uwzględnienia specyficznych zdarzeń w systemie możliwe jest wykorzystanie również funkcji systemu zarządzającego bazą danych. Tworzy się wówczas własny format zapisu monitorowanych zdarzeń, jak również dodatkową audytową bazę danych przechowującą tego typu informacje. Co więcej, tego typu baza audytowa może być analizowana przy użyciu standardowego języka SQL. Alternatywnym lub uzupełniającym rozwiązaniem pozwalającym na śledzenie i wykrycie intruzów jest zastosowanie mobilnych agentów. Ideę tę wykorzystano już w intranetach do kontroli dostępu do zasobów logicznych. Jest to podejście I-RBAC (Intranet-Role-Based Access Control), gdzie agenci składają się z dwóch części: *interfejsu* specyfikującego wymagane procedury bezpieczeństwa oraz *implementacji* określającej, jak te procedury mogą być wykonane przy współpracy z serwerem internetowym. Wyróżnia się przy tym 3 typy agentów: koordynatory (odpowiadające za utrzymanie polityki bezpieczeństwa), autoryzatory (dokonujące autoryzacji użytkowników) i aktualizatory (zapewniające aktualizację bazy danych). Takie rozwiązanie zapewnia elastyczność i efektywność rozwiązania. Głównym problemem jest zapewnienie zgodności informacji i współbieżności realizacji operacji bazodanowych. Wzorując się na powyższym przykładzie, można wykorzystać ideę inteligentnych agentów także do kontroli i identyfikacji intruzów. W tym celu mogą być wykorzystane aplety lub aglety oferowane w środowisku Javy. Umożliwiają one:

- obserwację różnych miejsc w systemie bądź różnych zdarzeń,
- wykonanie fotografii zachowania się systemu i zarządzanie archiwami takich fotografii,
- komputerowe wnioskowanie na bieżąco o możliwości występowania intruza i miejscu jego aktualnego działania,
- pozorowanie sugerujące intruzowi przełamanie mechanizmów ochrony w celu jego bliższej identyfikacji.

Pakiet taki, częściowo łączący te dwa podejścia, jest rozwijany obecnie w ramach prac dyplomowych.

5. Uwagi końcowe

Przedstawiono podstawowe mechanizmy kontroli dostępu użytkowników do zasobów systemu. Mechanizmy takie mają możliwości definiowania różnych poziomów zabezpieczeń oraz generacji sygnałów alarmowych o usiłowaniu włamania się do tych zasobów. Analiza sygnałów alarmowych umożliwia również identyfikację intruzów.

Powyższa strategia jest najprostszą metodą ochrony w systemach rozproszonych. W wielu przypadkach włamanie do systemu oznacza jednak, niezauważalne przez mechanizmy ochrony, przeniknięcie intruza. W związku z tym w systemie muszą być zaszyte dodatkowe wyszukane procedury kontrolne polegające na analizie wyróżnionych zdarzeń zachodzących w systemie. Praca przedstawia właśnie główne koncepcje takich rozwiązań. Szczegółowe ich implementacje zależą już od wielu czynników i na ogół są utajnione. Gwarantuje to również wyższe prawdopodobieństwo wykrycia intruzów.

LITERATURA

1. Arbaugh A. A., Dawin J. R., Farber D. J., Smith J. M: Security for Virtual Private Intranets. IEEE Computer, September, 1998.
2. Atkinson R. J.: Toward a More Secure Internet. IEEE Computer, January, 1997.
3. Brazier F. M. T., Johansen D.: Distributed Open Systems. Wyd. IEEE Computer Society, Los Alamitos 1994.
4. Castano S., Fugini M., Martello G., Samarati P.: Database Security. Wyd. Addison - Wesley, Wokingham 1994.
5. Coulouris G., Dollimore J., Kindberg T.: Systemy rozproszone - podstawy i projektowanie. Wyd. Queen Mery and Westfield College, University of London, tłumaczenie WNT, Warszawa 1998.
6. Dowd P. W., McHenry J. T.: Network Security: It's Time to Take It Seriously. IEEE Computer, September, 1998.
7. Frish A.: Unix - administracja systemu. Wyd. O'Reilly & Associates, Inc., tłumaczenie Oficyna Wydawnicza Read Me, Warszawa 1996.
8. Gong L.: Secure Java Class Loading. IEEE Internet Computer, Nr 6, 1998.
9. Kaufman Ch., Perlman R., Speciner M.: Network Security. Private communication in Public World. Wyd. PTR Prentice Hall,, 1995, Englewid Cliffs.

10. Krawczyk H.: Dependable processing. Skrypt PG, Gdańsk 1996.
11. Oppliger R.: Security at the Internet Layer. IEEE Computer, September, 1998.
12. Raszkiewicz M.: Bezpieczeństwo sieci komputerowych. Wyd. Fundacji Postępu Technicznego, Kraków 1995.
13. Rubin A. D., Geer D. F.: Mobile Code. Security IEEE Internet Computer, December, 1998.
14. Schneier B.: Applied Cryptography, Protocols, Algorithms, and Source Code in C. Wyd. John Wiley & Sons, New York 1998.
15. Shaffer L., Simon R. A.: Network Security. Wyd. AP Professional, Cambridge 1994.
16. Skałecki P.: Zastosowanie mechanizmu procedur wyzwalanych do tworzenia baz audytowych. Praca dyplomowa, Politechnika Gdańska, 1995.
17. Tari Z., Chan S. W.: A Role-Bazed Acces Control for Intranet Security. IEEE Internet Computing, September-October, 1997.
18. Wallman S. M. H.: Technology Takes to Securities Trading. IEEE Spectrum, February, 1997.

Recenzent: Prof. dr hab. inż. Andrzej Grzywak

Wpłynęło do Redakcji 24 marca 1999 r.

Abstract

Information processed by distributed system plays an important role in economy, industry and organisation of human life. This causes a deep interest of numerous people (not legal users) in having access to various system resources. Moreover, the more complex the system becomes, the greater the number of possible attacks. Two main approaches to eliminate intrusions are considered (see Fig. 1). One of them uses cryptographic security mechanisms to protect access to resources. A complementary approach is to equip a system with specific security mechanisms to detect presence of intrusions in the system and to isolate their dangerous activities.

Two standardised solutions are considered in the paper. At first authentication protocols implemented in the Kerberos system (Fig. 2) are analysed. Some general design rules are suggested. Next, intrusion detection mechanisms in the IDES system (Fig. 3 and Fig. 4) are presented. Based on these representative practical examples, a detailed concept of intrusion

detection strategy in a database environment is proposed. This strategy bases on small size audit memory, and intelligent moving agents. Some agents observe behavior of the system on different levels of abstractions and put essential information to the audit memory. Other agents can analyze information stored in the memory and conclude about presence of intrusions in the observed environment.