STUDIA INFORMATICA 2001
Volume 22 Number 4 (46)

Tomasz Jordan KRUK, Andrzej MACHNACZ
Politechnika Warszawska, Instytut Automatyki i Informatyki Stosowanej

SYSTEMY WYKRYWANIA ANOMALII W ZABEZPIECZENIACH TECHNICZNYCH

Streszczenie. W artykule dokonano wprowadzenia do tematyki systemów wykrywania włamań. Szczególny nacisk położono na systemy wykrywania anomalii. Przedstawiono klasyfikację technik wykrywania anomalii oraz metody wykorzystywane do realizacji wykrywania włamań.

ANOMALY DETECTION SYSTEMS IN TECHNICAL PROTECTION

Summary. In this article some introduction to the intrusion detection systems has been done. The paper concentrates on the anomaly detection systems. The classification of the anomaly detection techniques has been presented. Moreover, different methods used in intrusion detection has been described.

1. Wstęp

Coraz częściej zaawansowana technologia (ang. *high technology*), a w szczególności systemy informatyczne odgrywają istotną rolę w życiu całej rasy ludzkiej. Jednak wraz ze wzrostem wykorzystania tej technologii pojawia się problem zapewnienia odpowiedniego poziomu bezpieczeństwa. Dostępność rozproszonych sieciowych środowisk obliczeniowych, transgraniczność sieci, a także rozmycie pewnych zagadnień związanych z komputerami i telekomunikacją (np. PBX to komputer) powodują, że zapewnienie poufności i integralności wytwarzanych, przetwarzanych, przechowywanych oraz przesyłanych informacji nie jest zadaniem trywialnym. Ponadto, kompatybilność coraz większej ilości zdalnych systemów, dostępność niedrogiego sprzętu i oprogramowania, przyjmowane standardy dla sprzętu i oprogramowania, takie jak: TCP/IP, przeglądarki internetowe, platformy UNIX, Windows

9x/NT/2k, sprawiają, że przełamanie zabezpieczeń i skompromitowanie systemu jest zadaniem stosunkowo łatwym. Z drugiej strony, duża część potencjału intelektualnego informatyków skierowana jest na znalezienie skutecznych metod ochrony zasobów informatycznych. W związku z tym systemy zabezpieczeń stały się jedną z najbardziej dynamicznie rozwijających się technologii przemysłu informatycznego. Rozwój zabezpieczeń zmierza w kierunku centralnie zarządzanych oraz zintegrowanych systemów sieciowych, zawierających środki ochrony rezydujące na serwerach, stacjach roboczych, urządzeniach sieciowych oraz różnego rodzaju systemach dedykowanych, w tym serwerach uwierzytelniania, systemach zaporowych, urzędach certyfikacji PKI, a także systemach wykrywania włamań.

2. Systemy wykrywania włamań

Stosowanie mocnych technologii autoryzacji i certyfikacji oraz szerokiej gamy rozwiązań, niezbędnych do stworzenia infrastruktury pozwalającej wykorzystywać bezpiecznie system, nie zawsze pozwala na zapewnienie wysokiego poziomu bezpieczeństwa. Ponadto, biorąc pod uwagę fakt, że największe zagrożenie dla bezpieczeństwa systemów komputerowych niesie ze sobą czynnik ludzki, często newralgiczne węzły systemu komputerowego muszą być zabezpieczane przy użyciu dodatkowych mechanizmów. Nie istnieją jednak idealne rozwiązania zabezpieczające, trudno byłoby je zresztą zbudować na bazie systemów operacyjnych, z których większość w swoich założeniach nie jest dobrze przygotowana do realizacji właściwej ochrony przed atakami z zewnątrz. Wiele do życzenia pozostawia również protokół TCP/IP, w którym w niewystarczającym stopniu uwzględniono aspekty dotyczące bezpieczeństwa transmisji danych - uwierzytelniania, integralności i poufności. Dlatego też właśnie powstają dodatkowe urządzenia i programy, których zadaniem jest zwiększenie poziomu bezpieczeństwa systemów informatycznych.

Biorąc pod uwagę wrażliwość informacji przetwarzanych w systemach informatycznych korporacji w ostatnim czasie wiele uwagi i środków finansowych przeznacza się na implementację zaawansowanych zabezpieczeń. Do grupy takich systemów zalicza się wszelkie systemy wczesnego ostrzegania, typu *systemy wykrywania włamań* określane również mianem *systemów wykrywania intruzów* (ang. *IDS - Intrusion Detection Systems*). Głównym zadaniem systemu IDS jest wykrycie intruza i o ile jest to możliwe, przedsięwzięcie ustalonych środków zaradczych zapobiegających włamaniu, a w przypadku wykrycia włamania – minimalizacji konsekwencji kompromitacji systemu.

Wyróżnia się następujące grupy programów, które wspólnie określa się mianem systemów IDS: *sieciowe systemy wykrywania intruzów* (ang. NIDS - network intrusion

detection systems), *weryfikatory integralności systemu* (ang. SIV - system integrity verifiers), *monitory plików dziennika systemowego* (ang. LFM - log files monitors) oraz *emulatory-pułapki* (ang. deception systems, honey pots).

Systemy NIDS monitorują pakiety w sieci, starając się wykryć niedozwoloną działalność krakerów. System NIDS może być uruchomiony zarówno na maszynie docelowej, która śledzi swój własny ruch sieciowy, bądź też na dedykowanej maszynie analizującej cały ruch w sieci. Systemy SIV monitorują pliki systemowe sprawdzając, czy nie zostały zmodyfikowane przez intruza. Systemy LFM analizują pliki rejestrujące działalność poszczególnych usług sieciowych. W sposób podobny jak w systemach NIDS szukają pewnych wzorców, których wystąpienie implikowałoby zaistnienie włamania do systemu.

System wykrywania włamań może zostać również uzupełniony o różnego rodzaju pułapki. Ich zadaniem jest zwrócenie na siebie uwagi po przełamaniu przez intruza pierwszych linii obrony. Pułapka może być zrealizowana na poziomie komputera, którego jedynym zadaniem jest udawanie jakiegoś prawdopodobnego systemu, np. systemu księgowego. Pułapka może być również zrealizowana na poziomie pojedynczej usługi na pełniącym rzeczywiste funkcje komputerze. Przykładowo, może być to usługa serwera WWW z własnym zestawem stron, która 'przedstawia się' intruzowi w sytuacji, gdy uzyskał on już logiczny dostęp do serwera. Zadaniem pułapki może być nie tylko odciąganie od rzeczywiście krytycznych systemów czy usług, ale i działania mające na celu utrudnienie kompromitacji systemu przez intruza. Na przykład system komputerowy z pułapką może zacząć symulować, czy wręcz generować duże obciążenie ruchem sieciowym albo duże opóźnienia. Umożliwi to spowolnienie działań intruza, a przez to albo zupełne zerwanie połączenia albo namierzenie źródła ataku. Jak można się domyśleć, pułapki wymagają bardzo dużych nakładów i tylko nieliczne organizacje, w których bezpieczeństwo informacji jest priorytetem ich całej działalności, decydują się na ich pełną implementację.

Bardzo często opisana powyżej klasyfikacja systemów wykrywania włamań ogranicza się jedynie do podziału na dwie generalne grupy systemów. Pierwszą są *oparte na sieci systemy wykrywania intruzów* (ang. network-based IDS), których zasada działania opiera się na monitorowaniu całej sieci komputerowej oraz komputerów podłączonych do tej sieci. Sieciowe systemy potrafią analizować i korelować informacje pochodzące z całej sieci. Drugą grupę stanowią *lokalne systemy wykrywania włamań* (ang. host-based IDS). Systemy lokalne dokonują zarówno analizy ruchu sieciowego danego komputera, jak i dokonują analizy plików dziennika systemowego oraz monitorują stan systemu komputerowego. Zadaniem systemów sieciowych jest ochrona całej sieci, zadaniem systemów lokalnych jest ochrona pojedynczego komputera. Systemy sieciowe są zazwyczaj w ogólnym rozrachunku tańsze i łatwiejsze w zarządzaniu, jednak systemy lokalne z racji większej liczby źródeł analizowanej

informacji są dokładniejsze. Ponadto, rozwój technologii informatycznych istotnie ograniczył zakres możliwości stosowania sieciowych systemów IDS. Pierwszym utrudnieniem było upowszechnienie się podziału sieci na segmenty, co przeważnie ogranicza do pojedynczego segmentu zakres analizy ruchu sieciowego przez jednego agenta systemu sieciowego. Kolejnym utrudnieniem było rozpowszechnienie korzystania z wirtualnych sieci prywatnych (ang. VPN). Zawartość łączy VPN nie może być analizowana podczas przesłania, a jedynie w punkcie nadawczym oraz odbiorczym. Gdyby pokusić się o prognozę, wydaje się, że sieciowe systemy IDS będą stosowane tam, gdzie powyższe ograniczenia daje się w jakiś sposób ominąć, jednak ogólną tendencją będzie coraz szersze stosowanie lokalnych systemów IDS.

Jakość systemów wykrywania włamań mierzona być może poziomem charakteryzowania się następującymi cechami:

- dokładność – system nie może identyfikować prawidłowego zachowania użytkownika jako próby kompromitacji systemu,
- wydajność – przetwarzanie musi być zoptymalizowane, tak aby można było rozpoznać próbę ataku w czasie rzeczywistym,
- kompletność – system nie może nie zauważyć żadnej techniki włamania. Jest to najtrudniejsze do realizacji wymaganie, gdyż najpierw powstają nowe typy ataków, a dopiero z pewnym opóźnieniem metody ochrony,
- odporność na uszkodzenia – sam system IDS nie może być podatny na żadne próby ataków,
- czas odpowiedzi – nie tylko samo wykrycie ataku, ale i czas samej obsługi wykrycia powinien być bardzo krótki, gdyż w przypadku ataku jak najszybciej muszą być uaktywnione środki zaradcze.

Decydując się na wybór pewnego rozwiązania zabezpieczającego, powinno się uwzględnić nie tylko aspekty funkcjonalne docelowego rozwiązania, ale i aspekty ekonomiczne związane z nabyciem takiego systemu. Należy rozpatrzyć między innymi:

- koszt produktu,
- koszt wymaganych dodatkowych zasobów sprzętowych,
- koszt administracji.

Tak jak w przypadku innych zakupów dotyczących bezpieczeństwa (np. firewall czy oprogramowanie antywirusowe, czy też jedno i drugie) decyzja o wyborze rozwiązania musi być poprzedzona dokładną analizą, która odpowie na pytania: co należy chronić i ile warte jest to, co ma być chronione. Odpowiedź na te pytania powinna być dobrym wyznacznikiem przede wszystkim przy podjęciu decyzji, jak duży budżet należy przeznaczyć na zabezpieczenia.

Istnieją dwa generalne podejścia do wykrywania intruzów: *wykrywanie anomalii* (ang. *anomaly detection*) oraz *wykrywanie nadużyć* (ang. *misuse detection*). Wykrywanie anomalii opiera się na profilowaniu zachowań użytkowników. Definiowany jest pewien model normalnych, poprawnych zachowań użytkowników systemu informatycznego. Każde odchylenie, niestandardowe zachowanie, uznawane jest za anomalię.

Systemy wykrywania nadużyć korzystają z dostarczonych a priori, np. przez producenta oprogramowania IDS, wzorców ataków określanych mianem sygnatur ataków. Wykrywanie włamań polega na porównywaniu ruchu sieciowego ze wzorcami z bazy sygnatur. W systemach wykrywania nadużyć pewną rolę odgrywa efektywność metody analizy danych, jednak jest to tylko miara wydajności systemu. Tymczasem w systemach wykrywania włamań główną miarą jakości jest trafność wykrywania ataków. W tym kontekście systemy wykrywania nadużyć są tak dobre, jak dobra jest dostarczona przez twórcę czy producenta oprogramowania baza sygnatur ataków.

W dalszej części referatu skoncentrowano się na systemach wykrywania anomalii.

3. Systemy wykrywania anomalii

Każdy użytkownik systemu komputerowego jest w stanie wykonywać pewne zadania. Inaczej mówiąc, każdy użytkownik ma pewną funkcjonalność w systemie. Zazwyczaj funkcjonalność ta jest łatwo identyfikowalna i stosunkowo nieznacznie zmienia się w czasie. Przykładowo, sekretarka podczas pracy przeważnie wykonuje ograniczoną liczbę czynności, takich jak: tworzenie i drukowanie różnych dokumentów, czy też czytanie i wysyłanie poczty. Administrator przetwarza pliki konfiguracyjne systemu, analizuje statystyki i pliki dziennika systemowego. Programista dokonuje edycji plików tekstowych, dokonuje kompilacji i uruchamiania oprogramowania. Oznacza to, że na pewnym poziomie ogólności możliwe jest zdefiniowanie zestawu czynności zazwyczaj wykonywanych przez użytkownika. Zestaw ten określany jest właśnie mianem *profilu użytkownika*.

Po zdefiniowaniu profili możliwe jest już śledzenie zachowań użytkowników w celu wykrycia odchyleń od tychże zachowań. Takie odchylenia określane są mianem anomalii i zazwyczaj świadczą o zaistnieniu włamania do systemu.

Systemy wykrywania anomalii są przygotowywane korzystając z ogromnej liczby danych statystycznych w celu jak najwierniejszego ustalenia profilu użytkownika. O ile w przypadku systemu wykrywania nadużyć jakość systemu warunkowana jest aktualnością i kompletnością sygnatur ataków, o tyle w przypadku anomalii jakość systemu jest warunkowana trafnością i dokładnością zdefiniowania profili poszczególnych użytkowników systemu.

4. Klasyfikacja technik wykrywania anomalii

Systemy wykrywania anomalii stosują wiele technik. Część z nich daje się sklasyfikować, zaś część stanowi własne nietypowe rozwiązania związane ze specyfiką instytucji czy branży. Wśród technik standardowych można wyróżnić:

- monitorowanie progów (ang. threshold monitoring),
- profilowanie pracy użytkownika (ang. user work profiling),
- profilowanie pracy grupy (ang. group work profiling),
- profilowanie zasobów (ang. resource profiling),
- profilowanie procesów (ang. executable profiling),
- statyczne profilowanie pracy (ang. static work profiling),
- adaptacyjne profilowanie pracy (ang. adaptive work profiling),
- profilowanie adaptacyjne oparte na regułach (ang. adaptive rule based profiling).

Poniżej pokrótce opisane zostaną wymienione techniki.

4.1. Monitorowanie progów

W technice tej ustala się wartości graniczne, które w pewnej metryce, reprezentującej zachowania, definiują zachowania akceptowalne. Przykładem może być ustalenie za wartość graniczną dopuszczalnej liczby rejestracji do systemu w ustalonym przedziale czasowym. Progi udostępniają przejrzystą i zrozumiałą definicję działań nieakceptowalnych i poza dziennikiem systemowym (tzw. logami) mogą wykorzystywać inne źródła informacji. Niestety, rzadko kiedy można scharakteryzować zachowanie intruza wyłącznie poprzez ustalenie pewnej wartości progowej zachowania wyznaczanego na podstawie rekordów audytu.

4.2. Profilowanie pracy użytkownika

W technice tej zarządza się indywidualnymi profilami użytkowników, do których użytkownik powinien się stosować w trakcie wykonywania swego zakresu obowiązków. W sytuacji, gdy zmienia się zakres obowiązków użytkownika, aktualizowany jest również jego profil. Niektóre systemy wyróżniają krótko- i długoterminowe profile użytkowników. Profile krótkoterminowe dotyczą zmian chwilowych bieżących, profile długoterminowe pewnych cech stałych charakteryzujących działalność pracownika. Profilowanie tego typu ma ograniczone zastosowanie w sytuacji nieregularnej pracy użytkowników bądź też częstej rotacji pracowników. Profile zdefiniowane na zbyt ogólnym poziomie nie będą w praktyce spełniać żadnej roli, gdyż będą akceptować dowolne zachowania.

4.3. Profilowanie pracy grupy

W większości instytucji wielu pracowników realizuje zbliżone bądź identyczne zadania. Tak więc ze względu na profilowanie warto jest ustalić wspólny profil dla całej grupy pracowników. Profil grupy jest opracowywany na bazie historii dotychczasowych działań grupy. Osoby należące do grupy powinny funkcjonować zgodnie z przyjętym dla grupy profilem. Główną zaletą tej metody jest istotna redukcja liczby profilów wymaganych w instytucji. Ponadto, nie ma użytkowników "równych i równiejszych", osoby merytorycznie pełniące te same funkcje mają jednakowe przywileje i ograniczenia. Oczywiście pojawia się problem prawidłowej klasyfikacji użytkowników. Zaś w przypadku użytkowników o specyficznych zadaniach istnieje potrzeba tworzenia indywidualnych, jednoosobowych grup.

4.4. Profilowanie zasobów

Profilowanie zasobów monitoruje ogólnosystemowe wykorzystanie zasobów, takich jak konta, aplikacje, systemy dyskowe, protokoły, porty komunikacyjne i tworzy profil użycia poszczególnych zasobów.

4.5. Profilowanie procesów

Monitorowane jest wykonanie wszystkich programów, niezależnie od tego, kto jest ich właścicielem. W szczególności analizowane są te procesy, dla których ustalenie kto jest ich rzeczywistym właścicielem, nie może być w łatwy sposób określone. Wirusy, konie trojańskie, robaki sieciowe, tylne wejścia, bomby logiczne i inne potencjalne metody ataków mogą zostać wykryte właśnie poprzez analizę wykorzystania obiektów systemowych przez procesy, takie jak pliki czy drukarki. W większości klasycznych systemów operacyjnych oprogramowanie jawnie bądź niejawnie (ze względu na automatyzację pewnych czynności) uruchomione przez użytkownika, bądź w jego imieniu dziedziczy wszystkie przywileje użytkownika, który uruchamia program, przykładowo zainfekowany wirusem. Dziedziczenie przywilejów, poniekąd uzasadnione w przypadku wykorzystywania normalnego oprogramowania, umożliwia złośliwemu oprogramowaniu skryte skopiowanie, zniszczenie bądź zainfekowanie wszystkich zasobów, do których użytkownik ma nadane prawa. Monitorowanie zasobów niezależne od użytkownika-właściciela zwiększa również prawdopodobieństwo wykrycia współpracy złośliwego oprogramowania, uruchamianego w imieniu różnych użytkowników systemu.

4.6. Statyczne profilowanie pracy

Ten typ profilowania polega na okresowej aktualizacji profilów poszczególnych użytkowników na żądanie oficera bezpieczeństwa (osoby odpowiedzialnej za wszystkie aspekty bezpieczeństwa w danej instytucji). Postępowanie ma na celu zabezpieczenie przed stopniowym rozszerzaniem profilów przez użytkowników poprzez kolejne przejawianie zachowań coraz odleglejszych od ustalonego profilu wstępnego (np. zakresu obowiązków). Takie podejście chroni przed niewłaściwymi adaptacyjnymi redefinicjami profilów, które w przeciwnym razie mogłyby zacząć stopniowo obejmować zachowania uznane za nieprawidłowe/ zabronione. Zachowywanie migawek profili poszczególnych użytkowników umożliwia analizę porównawczą zmian zachowań użytkowników wykonywaną przez oficera bezpieczeństwa.

Niedogodnością podejścia statycznego profilowania pracy jest fakt, iż w praktyce profile te muszą być stosunkowo ogólne i o ograniczonej wrażliwości bądź też bardzo często aktualizowane. W przeciwnym razie, w przypadku istotnej planowej zmiany zadań użytkownika, system może fałszywie wygenerować wiele alarmów o wystąpieniach anomalii. Statyczne profilowanie pracy wymaga również sumienności i staranności pracy oficera bezpieczeństwa, który musi bardzo szybko reagować na zmiany zadań poszczególnych użytkowników, a jednocześnie weryfikować poprawność zmian w zachowaniu każdego użytkownika.

4.7. Adaptacyjne profilowanie pracy

Ta metoda automatycznie zarządza profilami roboczymi, odzwierciedlając akceptowalne zmiany aktywności użytkowników. Aktualizowane profile mogą dotyczyć użytkownika, grupy użytkowników bądź konkretnych aplikacji. Profilowanie automatyczne umożliwia oficerowi bezpieczeństwa dokonywanie oceny, czy sygnalizowana zmiana zachowania może świadczyć o próbie włamania, czy może nie jest intruzyjna i wymaga zmiany profilu, czy wreszcie jest nieintruzyjna, a nie wymaga zmiany profilu, gdyż liczba wystąpień mieści się w granicach błędu statystycznego. Oczywiście cała procedura może być zautomatyzowana i nie wymagać kontroli oraz podejmowania decyzji przez oficera bezpieczeństwa.

4.8. Profilowanie adaptacyjne oparte na regułach

Metoda ta różni się od pozostałych tym, że na bazie zachowań użytkownika w pewnym okresie próbnym konstruuje się zestaw reguł definiujących normalne zachowanie użytkownika, po czym we właściwym okresie profilowania monitoruje się każde odstępstwo od zaobserwowanych zachowań. Od badania zgodności na podstawie reguł w systemach

wykrywania nadużyć metoda ta różni się brakiem konieczności posiadania na wstępie bazy wiedzy (np. sygnatur ataków). Problemem zastosowania tego podejścia jest konieczność posiadania ogromnej liczby reguł. Sprawdzanie dużej liczby reguł może istotnie obniżyć wydajność systemu w porównaniu do klasycznych statystycznych metod profilowania. Dodatkową trudnością jest złożone zarządzanie samymi regułami, szczególnie w przypadku dużej dywersyfikacji profilów użytkowników.

5. Metody wykorzystywane do realizacji wykrywania włamań

Systemy IDS, w tym systemy wykrywania anomalii, wykorzystują różne metody do reprezentacji wiedzy i analizy informacji w celu wykrycia potencjalnych ataków. Najczęściej stosowane metody wykorzystują następujące środki:

- systemy ekspertowe oparte na regułach (ang. rule-based expert systems),
- analiza przejść stanów (ang. state transition analysis),
- bayesowskie sieci alarmowe (ang. Bayesian alarm networks).

Poniżej pokrótce opisane zostaną wymienione metody.

5.1. Systemy ekspertowe oparte na regułach

Systemy wykorzystujące reguły są podstawą większości komercyjnych systemów wykrywania włamań. Wynika to z faktu, iż systemy komercyjne wykorzystują przeważnie techniki związane z systemami wykrywania nadużyć, w bardzo ograniczonym stopniu decydując się na wykorzystanie technik służących do wykrywania anomalii. W systemach takich zebrana przez producenta baza faktów (przeważnie binarnych wzorców ataków sieciowych) jest dana z góry, zaś sam motor realizujący wnioskowanie o bazie faktów jest osobnym komponentem. W systemach tego typu można wyróżnić następujące składowe:

- bazę faktów zawierającą fakty na temat stanów systemu (wstępnie przetworzone rekordy audytowe),
- bazę reguł zawierającą reguły odpowiadające scenariuszom włamań,
- motor wnioskowania, który zajmuje się analizą faktów i reguł w celu identyfikacji potencjalnych włamań.

Systemy ekspertowe wykorzystywane są jednak również do wykrywania anomalii. Takie podejście zakłada wstępny etap uczenia mający na celu zidentyfikowanie normalnych zachowań użytkowników, jak i zachowań, które trzeba będzie zidentyfikować jako anomalie. Jest to zasadnicza różnica pomiędzy wykorzystaniem systemów ekspertowych do wykrywania nadużyć i wykrywania anomalii. W przypadku wykrywania nadużyć reguły są

zadane a priori (z oczywistą możliwością uaktualniania poprzez pobieranie nowych reguł, sygnatur ataków, od producenta oprogramowania IDS). W przypadku wykrywania anomalii baza reguł jest tworzona w inny sposób.

Istnieje wiele metod uzyskania reguł opisujących zachowania użytkowników. Jedną z nich jest eksploracja wiedzy (ang. data mining). Ogólnie polega ona na ekstrakcji modeli opisowych z ogromnej ilości danych. Wykorzystywane są przede wszystkim trzy typy algorytmów posługujące się technikami z różnych dziedzin wiedzy, takich jak statystyka, rozpoznawanie wzorców i uczenie maszyn:

- klasyfikacja, czyli zaliczanie wybranych danych jednostkowych do jednej z predefiniowanych kategorii, na przykład podział na zachowania normalne i zachowania nienormalne,
- analiza powiązań, czyli ustalanie korelacji między różnymi czynnikami w informacjach audytowych, na przykład analiza powiązań między wykonywaną komendą a czasem jej wykonania,
- analiza sekwencji, czyli modelowanie wzorców sekwencyjnych, kojarzenie konsekwencji wystąpienia po sobie pewnych sekwencji zdarzeń.

5.2. Analiza przejść stanów

Przejścia stanów reprezentują sekwencję akcji, które intruz wykonuje w celu włamania się do systemu. Akcje oraz warunki ich zaistnienia są reprezentowane w postaci diagramu przejść stanów. Metoda opiera się na założeniu, iż wszyscy intruzi mają dwie wspólne cechy: intruz uzyskuje w pewien sposób dostęp do systemu oraz fakt włamania implikuje uzyskanie przez intruza pewnych uprawnień, których nie posiadał wcześniej. Tak więc włamanie jest rozpatrywane jako ciąg akcji intruza, które przeprowadzają chroniony system z pewnego stanu wstępnego do stanu kompromitacji systemu w wyniku działań intruza i poprzez pewną liczbę stanów pośrednich. Stan początkowy reprezentuje stan systemu przed atakiem, stan końcowy - stan systemu po ataku zakończonym sukcesem. Kroki wykonywane przez intruza reprezentowane są poprzez przejścia między kolejnymi stanami pośrednimi.

Poza stanami definiuje się sygnatury akcji (ang. signature actions), czyli minimalne zbiory akcji niezbędnych do przeprowadzenia zakończonego sukcesem ataku. Jeżeli choć jedna z nich jest pominięta, atak na system nie zostanie zakończony powodzeniem.

Stany, przejścia między stanami i sygnatury akcji mają swoją reprezentację graficzną w postaci diagramu przejść stanów. Dobrą cechą tej metody jest możliwość reprezentacji scenariuszy w łatwo przyswajalnej postaci graficznej. Rzeczywiste systemy nie operują jednak na postaci graficznej. Zamiast tego stosowane są dedykowane języki do reprezentacji

stanów i opisu przejść między stanami. Bardzo często analiza przejść stanów jest wykorzystywana jako baza w opartych na regułach systemach ekspertowych.

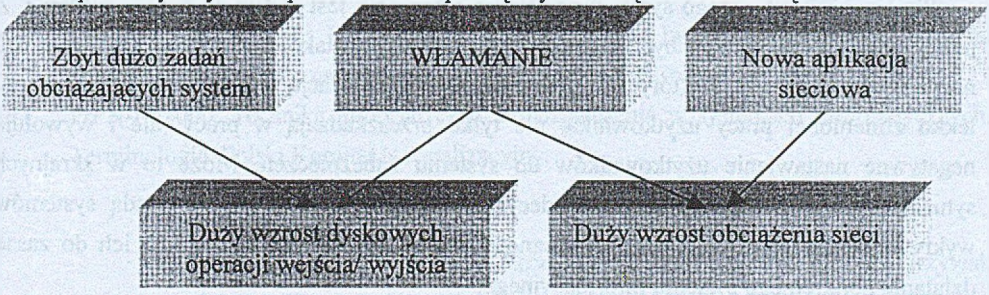
5.3. Bayesowskie sieci alarmowe

Prawdopodobieństwo i sieci bayesowskie są podejściem alternatywnym wobec klasycznej teorii prawdopodobieństwa. Prawdopodobieństwo bayesowskie reprezentuje nie tyle prawdopodobieństwo wystąpienia pewnego zdarzenia, ale raczej poziom przekonania, iż dane wydarzenie rzeczywiście wystąpi. Istotną różnicą pomiędzy prawdopodobieństwem bayesowskim a klasyczną teorią prawdopodobieństwa jest to, iż w przypadku bayesowskiego nie ma potrzeby powtarzania prób. Zamiast tego definiowane jest prawdopodobieństwo wystąpienia następnego zdarzenia w badanej sekwencji.

Sieci bayesowskie tworzą skierowany graf acykliczny, który reprezentuje połączoną dystrybucję prawdopodobieństwa dla dużego zbioru zmiennych losowych. Krawędzie reprezentują stochastyczne zależności ojciec-potomek pomiędzy parą węzłów. Węzły reprezentują zmienne stochastyczne, których wartości implikują normalny bądź nienormalny stan zmiennej. Idea metody pasuje do środowiska wykrywania włamań, w którym występuje ogromna liczba wzajemnie powiązanych zmiennych i istotnie ułatwia reprezentację scenariuszy włamań.

Metoda ta wymaga zadania prawdopodobieństw dla wszystkich węzłów nie mających węzła ojca (określanych mianem korzeni jak w drzewie). Wymagane jest również zadanie prawdopodobieństw warunkowych dla pozostałych węzłów. Jest to nietrywialne zadanie będące największą trudnością opisywanej metody ze względu na skalę przetwarzanej informacji, którą należy przeanalizować.

Na poniższym rysunku przedstawiono prostą bayesowską sieć alarmową.



Rys. 1. Bayesowska sieć alarmowa modelująca włamanie
Fig. 1. Bayesian alarm network modelling an intrusion

Sama technika obliczeniowa nie jest skomplikowana. Kiedy znane są wartości zmiennych stochastycznych w węzłach-korzeniach, obliczane są wartości prawdopodobieństw zmiennych warunkowych. Uznaje się, że wystąpiło włamanie do systemu, o ile związane z nim zmienne warunkowe otrzymają wartości większe od pewnych ustalonych progów.

6. Podsumowanie

Techniki wykrywania włamań nie są jeszcze dyscypliną dojrzałą i na pewno nie powinny być uznawane za wystarczająco samodzielne zabezpieczenie przed różnymi atakami. W samej dziedzinie zabezpieczeń technicznych należy je wspomagać przez odpowiednie systemy filtrujące ruch, oprogramowanie antywirusowe oraz skuteczne metody nadawania uprawnień i uwierzytelniania.

Istnieje wiele systemów komercyjnych typu IDS. W ogromnej większości systemy te wykorzystują techniki wykrywania nadużyć, czyli wykrywają włamania poprzez porównywanie różnych akcji z sygnaturami włamań przechowywanymi w bazach dostarczanych przez producentów. Aktualizacja tych baz jest zawsze opóźniona w stosunku do momentu wystąpienia ataku. Jest to analogiczne do sytuacji w oprogramowaniu antywirusowym - nie można stworzyć sygnatury wirusa, który jeszcze nie zaatakował, gdyż wirus ten nie jest jeszcze znany.

Szansą na możliwość wykrywania ataków, które nie były jeszcze znane w momencie tworzenia systemu IDS, jest wykorzystanie podejścia analizującego anomalie. W przypadku dobrze zdefiniowanych profili użytkowników czy też aplikacji istnieje duże prawdopodobieństwo, że system wychwyci również ataki nieznane w chwili definiowania profili.

Stworzenie skutecznego systemu wykrywania anomalii jest zadaniem bardzo trudnym. Z jednej strony system musi być skuteczny w wykrywaniu ataków, z drugiej nie może być nadwrażliwy. Sytuacje, w których system zareaguje sygnalizacją ataku w trakcie rutynowej, lekko zmienionej pracy użytkownika, nie tylko przeszkadzają w pracy, ale i wywołują negatywne nastawienie użytkowników do systemu zabezpieczeń. Może to w skrajnych sytuacjach doprowadzić do odgórnej decyzji wyłączenia systemu IDS. Wadą systemów wykrywania anomalii jest zatem konieczność bardzo dokładnego dostrojenia ich do zasad działania konkretnego systemu informacyjnego.

Patrząc na bezpieczeństwo z szerszej perspektywy, nie wolno zapominać, że celem włamywacza jest przede wszystkim uzyskanie dostępu do systemu, niekoniecznie poprzez przełamywanie jakichkolwiek zabezpieczeń technicznych. Dokonując dużych inwestycji na zabezpieczenia techniczne, nie można zapominać o bezpieczeństwie fizycznym, a także o ustaleniu odpowiedzialności za poszczególne zasoby systemu. Ponadto, należy pamiętać o

implementacji i wdrożeniu procedur bezpiecznej eksploatacji zasobów informatycznych. W bezpieczeństwie, jak w żadnej innej dziedzinie, obowiązuje zasada najsłabszego ogniwa. Aby kompleksowo zabezpieczyć system przed włamaniami, należy wdrożyć, opracowaną uprzednio dla danej instytucji, globalną politykę bezpieczeństwa systemu informacyjnego.

LITERATURA

1. Denning D.: An Intrusion-Detection Model. Proceedings of the IEEE Symposium on Security and Privacy, Oakland 1986.
2. Graham R.: FAQ: Network Intrusion Detection Systems, 03.2000, http://www.robertgraham.com/pubs/network-intrusion-detection.html.
3. Halme L. R., Bauer R. K.: AINT Misbehaving: A Taxonomy of Anti-Intrusion Techniques. SANS Institute resources, http://www.sans.org.
4. Amoroso E.: Wykrywanie intruzów. Wydawnictwo RM, 1999.
5. Trzeszkowski T., Wykrywanie włamań do systemów komputerowych. Studia Informatica Vol. 21, No 1(39), Gliwice 2000.
6. Wrzesień J., Kruk T. J.: Sieciowe systemy wykrywania intruzów. IAilS Politechnika Warszawska, materiał wewnętrzny, 2001.
7. Gordeev M.: Intrusion Detection: Techniques and Approaches. 10.2000, http://www.infosys.tuwien.ac.at/Teaching/Courses/AK2/vor99/t13.
8. McHugh J., Christie A., Allen J.: Intrusion Detection: Implementation and Operational Issues. CERT/Coordination Center, 2000, http://www.cert.org.
9. NN: A Strict Anomaly Detection Model for IDS. Phrack Magazine. Vol. 0xa Issue 0x38, 01.2000.
10. Lee W., Stolfo S. J.: Data Mining Approaches for Intrusion Detection. Columbia University, http://www.cs.columbia.edu/~sal/hpapers/USENIX/usenix.html.
11. PrPN-I-02000, Technika informatyczna, Zabezpieczenia w systemach informatycznych, Terminologia. Polski Komitet Normalizacyjny.

Recenzent: Prof. dr hab. inż. Andrzej Grzywak

Wpłynęło do Redakcji 17 października 2001 r.

Abstract

Considering importance and sensitiveness of the information held in our information systems more and more effort is involved in implementaion of advanced security mechanisms. Among others in the group of the most important security mechanisms we can find IDS systems (i.e. intrusion detection systems). The main role of IDS is to detect any inappropriate, incorrect or anomalous activities in the system, report these activities and take any countermeasures foreseen for specific attacks or system misuses.

Intrusion detection consists mainly of two different approaches: misuse detection and anomaly detection. Misuse detection compares some data (taken from network traffic or audit logs) against well known attack patterns, usually gathered in delivered by an IDS producer signatures database. Anomaly detection compares observed activity against expected normal usage profiles which may be developed for users or resources. Different techniques are used in anomaly detection, i.e. threshold monitoring, user work profiling, resource profiling, static and adaptive work profiling, etc.

There are different scientific methods utilized by anomaly detection to analyse audit information. Among others we can specify rule-based expert systems, state transition analysis and Bayesian alarm networks.

Although anomaly detection still cannot be regarded as a mature approach and is not used as broadly as misuse detection in commercial IDS systems, it becomes more and more popular.