OCHRONA I BEZPIECZEŃSTWO INFORMACJI.

Omówimy zasady bezpieczeństwa w systemach operacyjnych. Niektóre narzędzia ogólnego przeznaczenia mogą być wbudowane w komputery i systemy operacyjne (OS), które obsługują różne mechanizmy ochrony i bezpieczeństwa. Generalnie chodzi o problem kontroli dostępu do systemów komputerowych i przechowywanych w nich informacji. Jedną z podstawowych koncepcji wszystkich takich dyskusji jest proces, który jest definiowany jako wykonanie określonego fragmentu kodu przez określonego użytkownika w określonym czasie na określonym procesorze. Zidentyfikowano cztery rodzaje ogólnych polityk ochrony o rosnącym stopniu trudności:

1. Bez udostępniania. W takim przypadku procesy są całkowicie odizolowane od siebie, a każdy proces ma wyłączną kontrolę nad zasobami przypisanymi mu statycznie lub dynamicznie. Dzięki tej zasadzie procesy często „współużytkują" program lub plik danych, wykonując jego kopię i przenosząc ją do własnej pamięci wirtualnej.

2. Udostępnianie oryginałów programów lub plików danych. Przy użyciu kodu z powtórnym wprowadzeniem pojedyncza fizyczna realizacja programu może pojawić się w wielu wirtualnych przestrzeniach adresowych, podobnie jak pliki danych tylko do odczytu. Do udostępniania zapisywalnych plików danych wymagane są specjalne mechanizmy blokujące, aby uniemożliwić jednoczesnym użytkownikom wzajemne zakłócanie się.

3. Zamknięte lub pozbawione pamięci podsystemy. W tym przypadku procesy są pogrupowane w podsystemy w celu wymuszenia określonej polityki ochrony. Na przykład proces „klienta" wywołuje proces „serwera" w celu wykonania jakiegoś zadania na danych. Serwer ma być chroniony przed odkryciem przez klienta algorytmu, za pomocą którego wykonuje zadanie, a klient ma być chroniony przed zatrzymaniem przez serwer jakichkolwiek informacji o wykonywanym zadaniu.

4. Kontrolowane rozpowszechnianie informacji. W niektórych systemach klasy bezpieczeństwa są definiowane w celu wymuszenia określonej polityki rozpowszechniania. Użytkownikom i aplikacjom nadaje się uprawnienia bezpieczeństwa określonego poziomu, podczas gdy dane i inne zasoby (np. Urządzenia wejścia / wyjścia [I / O]) otrzymują klasyfikacje bezpieczeństwa. Polityka bezpieczeństwa wymusza ograniczenia dotyczące tego, którzy użytkownicy mają dostęp do jakich klasyfikacji. Model ten jest przydatny nie tylko w kontekście wojskowym, ale także w zastosowaniach komercyjnych.

Większość prac związanych z bezpieczeństwem i ochroną w odniesieniu do systemów operacyjnych można z grubsza podzielić na trzy kategorie.

1. Kontrola dostępu. Zajmuje się regulowaniem dostępu użytkowników do całego systemu, podsystemów i danych oraz regulowaniem dostępu procesów do różnych zasobów i obiektów w systemie.

2. Kontrola przepływu informacji. Reguluje przepływ danych w systemie i ich dostarczanie do użytkowników.

3. Certyfikacja. Odnosi się do udowodnienia, że mechanizmy kontroli dostępu i przepływu działają zgodnie ze swoimi specyfikacjami oraz że egzekwują pożądane zasady ochrony i bezpieczeństwa.

WYMAGANIA DOTYCZĄCE BEZPIECZEŃSTWA SYSTEMU OPERACYJNEGO

Wymagania. Zrozumienie typów zagrożeń dla bezpieczeństwa systemu operacyjnego wymaga zdefiniowania wymagań bezpieczeństwa. Bezpieczeństwo systemu operacyjnego spełnia cztery wymagania:

1. Poufność. Wymaga, aby informacje w systemie komputerowym były dostępne tylko do odczytu przez upoważnione osoby. Ten rodzaj dostępu obejmuje drukowanie, wyświetlanie i inne formy ujawnienia, w tym zwykłe ujawnienie istnienia obiektu.

2. Integralość. Wymaga, aby tylko upoważnione osoby mogły modyfikować zasoby systemu komputerowego. Modyfikacja obejmuje pisanie, zmienianie, zmianę statusu, usuwanie i tworzenie.

3. Dostępność. Wymaga, aby zasoby systemu komputerowego były dostępne dla upoważnionych stron.

4. Uwierzytelnienie. Wymaga, aby system komputerowy był w stanie zweryfikować identyfikator użytkownika, urządzenia lub procesu.

Zasoby systemu komputerowego.

Aktywa systemu komputerowego można podzielić na sprzęt, oprogramowanie i dane.

Sprzęt komputerowy

Głównym zagrożeniem dla sprzętu komputerowego jest dostępność. Sprzęt jest najbardziej podatny na ataki, a najmniej podatny na zautomatyzowane kontrole. Zagrożenia obejmują przypadkowe i celowe uszkodzenie sprzętu, a także kradzież. Rozpowszechnianie się komputerów osobistych i stacji roboczych oraz coraz częstsze wykorzystywanie sieci lokalnych (LAN) zwiększa potencjalne straty w tym obszarze. Aby poradzić sobie z tymi zagrożeniami, potrzebne są fizyczne i administracyjne środki bezpieczeństwa.

Oprogramowanie

System operacyjny, narzędzia i aplikacje sprawiają, że sprzęt komputerowy jest przydatny dla firm i osób prywatnych. Należy wziąć pod uwagę kilka różnych zagrożeń. Kluczowym zagrożeniem dla oprogramowania jest atak na dostępność. Oprogramowanie, zwłaszcza aplikacje, jest zaskakująco łatwe do usunięcia. Oprogramowanie może również zostać zmienione lub uszkodzone, aby uczynić je bezużytecznymi lub niebezpiecznymi. Staranne zarządzanie konfiguracją oprogramowania, które obejmuje tworzenie kopii zapasowych najnowszej wersji oprogramowania, może zapewnić wysoką dostępność. Trudniejszym problemem jest modyfikacja oprogramowania, w wyniku której program nadal działa, ale zachowuje się inaczej niż wcześniej. Ostatnim problemem jest kontrola lub posiadanie oprogramowania. Chociaż dostępne są pewne środki zaradcze, w zasadzie problem nieautoryzowanego kopiowania oprogramowania nie został rozwiązany.

Dane

Bezpieczeństwo sprzętu i oprogramowania zwykle dotyczy komputerów pracowników centrów lub indywidualne obawy użytkowników komputerów osobistych. O wiele bardziej rozpowszechnionym problemem jest bezpieczeństwo danych, które obejmuje pliki i inne formy danych kontrolowane przez osoby, grupy i organizacje biznesowe. Kwestie bezpieczeństwa danych są szerokie i obejmują poufność, kontrolę lub posiadanie, integralność, autentyczność, dostępność i użyteczność. W celu rzetelnego teoretycznego potraktowania atrybutów informacji, które należy chronić za pomocą środków bezpieczeństwa. W przypadku dostępności problemem jest zniszczenie plików danych, które może nastąpić przypadkowo lub w umyśle, oraz opóźnienia w dostępie do danych. Oczywistym

problemem związanym z poufnością jest nieuprawnione odczytywanie plików lub baz danych, a ten obszar był być może przedmiotem większej liczby badań i wysiłku niż jakikolwiek inny obszar bezpieczeństwa komputerowego. Mniej oczywiste zagrożenie tajemnicą wiąże się z analizą danych i przejawia się w korzystaniu z tak zwanych statystycznych baz danych lub eksploracji danych, które dostarczają informacji podsumowujących lub zagregowanych i potencjalnie prowadzą do wykrycia niepublikowanych tendencji, powiązań lub trendów. Informacje zbiorcze niekoniecznie zagrażają prywatności zainteresowanych osób. Jednak wraz ze wzrostem wykorzystania statystycznych baz danych rośnie potencjał ujawniania danych osobowych poprzez wprowadzenie lub dedukcję. Zasadniczo cechy poszczególnych osób można zidentyfikować poprzez dokładną analizę. Aby wziąć prosty przykład, jeśli jedna tabela rejestruje sumę dochodów respondentów A, B, C i D, a druga sumę dochodów osób A, B, C, D i E, różnica między nimi agregatami byłby dochód E. Problem ten pogłębia rosnąca chęć łączenia zbiorów danych. W wielu przypadkach dopasowanie kilku zestawów danych w celu uzyskania spójności na poziomach agregacji odpowiednich dla problemu wymaga wycofania się do jednostek elementarnych w procesie konstruowania niezbędnych agregatów. Zatem jednostki elementarne, które są przedmiotem obaw o prywatność, są dostępne na różnych etapach przetwarzania zbiorów danych. Wreszcie integralność danych jest głównym problemem w większości instalacji. Modyfikacje plików danych mogą mieć konsekwencje od drobnych po katastrofalne.

Zasady projektowania

Saltzer i Schroeder określają szereg zasad projektowania środków bezpieczeństwa dla różnych zagrożeń dla systemów komputerowych. Obejmują one:

* Najmniejszy przywilej. Każdy program i każdy użytkownik systemu powinien działać przy użyciu najmniejszego zestawu uprawnień niezbędnych do wykonania zadania. Prawa dostępu powinny być nabywane wyłącznie za wyraźną zgodą; domyślną wartością powinno być „brak dostępu”.

* Ekonomia mechanizmów. Mechanizmy bezpieczeństwa powinny być jak najmniejsze i jak najprostsze, pomagając w ich weryfikacji. Zwykle oznacza to, że muszą one stanowić integralną część projektu, a nie mechanizmy dodatkowe do istniejących projektów.

* Dopuszczalność. Mechanizmy bezpieczeństwa nie powinny nadmiernie ingerować w pracę użytkowników. Jednocześnie mechanizmy powinny odpowiadać potrzebom osób upoważniających dostęp. Jeśli mechanizmy nie są łatwe w obsłudze, prawdopodobnie są nieużywane lub niewłaściwie używane.

* Pełna mediacja. Każdy dostęp należy porównać z informacjami dotyczącymi kontroli dostępu, łącznie z dostępami występującymi poza normalną eksploatacją, na przykład podczas odtwarzania lub konserwacji.

* Otwarta konstrukcja. Bezpieczeństwo systemu nie powinno zależeć od zachowania w tajemnicy projektu jego mechanizmów. Dzięki temu mechanizmy mogą być przeglądane przez wielu ekspertów, a użytkownicy mogą mieć do nich duże zaufanie

MECHANIZMY OCHRONY

Wprowadzenie multiprogramowania zaowocowało możliwością współdzielenia zasobów pomiędzy użytkownikami. To współdzielenie obejmuje nie tylko procesor, ale także:

* Pamięć

* Urządzenia we / wy, takie jak dyski i drukarki

* Programy

* Dane

Możliwość współdzielenia tych zasobów wprowadziła potrzebę ochrony. Pfleeger i Pfleeger zwracają uwagę, że system operacyjny może zapewniać ochronę w tym spektrum:

* Bez ochrony. Jest to właściwe, gdy wrażliwe procedury są uruchamiane w innym czasie.

* Izolacja. Takie podejście oznacza, że każdy proces działa oddzielnie od innych procesów, bez udostępniania lub komunikacji. Każdy proces ma własną przestrzeń adresową, pliki i inne obiekty.

* Udostępnij wszystko lub nic nie udostępniaj. Właściciel obiektu (np. pliku lub segmentu pamięci) deklaruje, że jest on publiczny lub prywatny. W pierwszym przypadku każdy proces może uzyskać dostęp do obiektu; w drugim przypadku tylko procesy właściciela mają dostęp do obiektu.

* Udostępnij przez ograniczenie dostępu. System operacyjny sprawdza dopuszczalność każdego dostępu określonego użytkownika do określonego obiektu. System operacyjny działa zatem jako strażnik lub strażnik między użytkownikami i obiektami, zapewniając, że występują tylko autoryzowane dostępy.

* Udostępnij za pomocą funkcji dynamicznych. Rozszerza to koncepcję kontroli dostępu, umożliwiając dynamiczne tworzenie praw współużytkowania obiektów.

* Ogranicz użycie obiektu. Ta forma ochrony ogranicza nie tylko dostęp do obiektu, ale także sposób wykorzystania tego przedmiotu. Na przykład użytkownik może mieć możliwość przeglądania poufnego dokumentu, ale nie może go wydrukować. Innym przykładem jest to, że użytkownik może mieć dostęp do bazy danych w celu uzyskania podsumowań statystycznych, ale nie w celu określenia określonych wartości danych.

Powyższe pozycje są wymienione z grubsza w kolejności rosnącej trudności w realizacji, ale także w kolejności rosnącej próby ochrony, którą zapewniają. Dany system operacyjny może zapewniać różne stopnie ochrony dla różnych obiektów, użytkowników lub aplikacji. System operacyjny musi równoważyć potrzebę umożliwienia współużytkowania, co zwiększa użyteczność systemu komputerowego, z potrzebą ochrony zasobów indywidualnych użytkowników. W tej sekcji omówiono niektóre mechanizmy, za pomocą których systemy operacyjne wymuszały ochronę tych obiektów.

Ochrona pamięci

W środowisku wieloprogramowym ochrona pamięci głównej (pamięć o dostępie swobodnym lub RAM) jest niezbędna. Problem tutaj to nie tylko bezpieczeństwo, ale prawidłowe funkcjonowanie różnych aktywnych procesów. Jeśli jeden proces może nieumyślnie zapisać w przestrzeni pamięci innego procesu, ten drugi proces może nie zostać wykonany poprawnie. Rozdzielenie przestrzeni pamięci różnych procesów jest łatwe do wykonania za pomocą schematu pamięci wirtualnej. Segmentacja lub stronicowanie, albo te dwa w połączeniu, zapewniają efektywny sposób zarządzania pamięcią główną. Jeśli dąży się do całkowitej izolacji, system operacyjny musi po prostu zapewnić, że każdy segment lub strona jest dostępna tylko dla procesu, do którego jest przypisany. Można to łatwo osiągnąć, wymagając, aby nie było zduplikowanych wpisów w tabelach stron i / lub segmentów. Jeśli udostępnianie ma być dozwolone, ten sam segment lub strona może pojawić się w więcej niż jednej tabeli. Ten typ udostępniania jest najłatwiejszy w systemie, który obsługuje segmentację lub połączenie segmentacji i stronicowania. W takim przypadku struktura segmentów jest widoczna dla aplikacji, a aplikacja może zadeklarować, że poszczególne segmenty mogą być współużytkowane lub niewymagalne. W czystym środowisku stronicowania rozróżnienie między dwoma typami pamięci

staje się trudniejsze, ponieważ struktura pamięci jest przezroczysta dla aplikacji. Szczególnie segmentacja nadaje się do wdrażania zasad ochrony i udostępniania. Ponieważ każdy wpis tablicy segmentu zawiera zarówno długość, jak i adres bazowy, program nie może nieumyślnie uzyskać dostępu do głównej lokalizacji pamięci poza ograniczeniami segmentu. Aby osiągnąć współdzielenie, możliwe jest odniesienie do segmentu w tabelach segmentów więcej niż jednego procesu. Te same mechanizmy są dostępne w systemie stronicowania. Jednak w tym przypadku struktura stron programów i danych nie jest widoczna dla programisty, przez co specyfikacja wymagań dotyczących ochrony i udostępniania jest trudniejsza.. Przykładem wsparcia sprzętowego, które można zapewnić dla ochrony pamięci, jest rodzina maszyn IBM System / 370, na których działa system OS / 390. Powiązany z każdą ramką strony w pamięci głównej jest 7-bitowy klucz sterujący magazynem, który może być ustawiony przez system operacyjny. Dwa z bitów wskazują, czy strona zajmująca tę ramkę została przywołana i zmieniona; te bity są używane przez algorytm zastępowania stron. Pozostałe bity są używane przez mechanizm ochrony: 4-bitowy klucz kontroli dostępu i bit ochrony pobierania. Procesor odnosi się do pamięci i bezpośredniego dostępu do pamięci (DMA). Odniesienia do pamięci DMA I / O muszą używać pasującego klucza, aby uzyskać pozwolenie na dostęp do tej strony. Bit ochrony pobierania wskazuje, czy klucz kontroli dostępu ma zastosowanie do zapisów, czy zarówno do odczytu, jak i do zapisu. W procesorze znajduje się słowo statusu programu (PSW), które zawiera informacje sterujące dotyczące aktualnie wykonywanego procesu. Zawarte w tym słowie jest 4-bitowy klucz PSW. Gdy proces próbuje uzyskać dostęp do strony lub zainicjować operację DMA na stronie, bieżący klucz PSW jest porównywany z kodem dostępu. Operacja zapisu jest dozwolona tylko wtedy, gdy kody są zgodne. Jeśli bit pobierania jest ustawiony, klucz PSW musi być zgodny z kodem dostępu do operacji odczytu

Kontrola dostępu zorientowana na użytkownika

Środki podejmowane w celu kontroli dostępu w systemie przetwarzania danych dzielą się na dwie kategorie: związane z użytkownikiem i związane z danymi. Najpopularniejszą techniką kontroli dostępu użytkowników w systemie współdzielonym lub serwerze jest logowanie użytkownika, które wymaga zarówno identyfikatora użytkownika (ID), jak i pewnej formy uwierzytelnienia, takiej jak podanie hasła, tokena lub atrybutów biometrycznych. Uwierzytelnianie odnosi się do powiązania rzeczywistej tożsamości (na przykład nazwanego pracownika lub nazwanej roli w organizacji) i prezentowanego identyfikatora. System zezwoli użytkownikowi na zalogowanie się tylko wtedy, gdy identyfikator tego użytkownika jest znany w systemie i jeśli użytkownik zna hasło skojarzone przez system z tym identyfikatorem. Gdy użytkownik ustanowi sesję, system operacyjny może następnie autoryzować różne formy dostępu (np. Odczyt, zapis, dołączanie, blokowanie lub wykonywanie) do różnych typów danych (np. Określonych plików, baz danych, urządzeń lub komunikacji) . Kontrola dostępu użytkowników w środowisku rozproszonym może być scentralizowana lub zdecentralizowana. W podejściu scentralizowanym sieć zapewnia usługę logowania, określając, kto może korzystać z sieci i z kim użytkownik może się łączyć. Zdecentralizowana kontrola dostępu użytkowników traktuje sieć jako przezroczyste łącze komunikacyjne, a host docelowy przeprowadza zwykłą procedurę logowania. Nadal należy się zająć kwestiami bezpieczeństwa dotyczącymi przesyłania haseł w sieci. W wielu sieciach można zastosować dwa poziomy kontroli dostępu. Poszczególnym hostom można zapewnić funkcję logowania w celu ochrony zasobów i aplikacji specyficznych dla hosta. Ponadto sieć jako całość może zapewniać ochronę ograniczającą dostęp do sieci dla upoważnionych użytkowników. Ta dwupoziomowa funkcja jest pożądana w powszechnym obecnie przypadku, w którym sieć łączy różne hosty i po prostu zapewnia wygodny sposób dostępu terminal-host. W bardziej jednolitej sieci hostów niektóre scentralizowane zasady dostępu mogą być egzekwowane w centrum sterowania siecią.

Kontrola dostępu zorientowana na dane.

Po pomyślnym zalogowaniu, użytkownik uzyskuje dostęp do jednego lub kilku hostów i aplikacji. Zwykle nie jest to wystarczające dla systemu, który zawiera wrażliwe dane w swojej bazie danych. Dzięki procedurze kontroli dostępu użytkownika, użytkownik może zostać zidentyfikowany w systemie. Z każdym użytkownikiem może być powiązany profil, który określa dozwolone operacje i dostęp do plików. System operacyjny może następnie wymuszać reguły na podstawie profilu użytkownika. System zarządzania bazami danych musi jednak kontrolować dostęp do określonych rekordów lub nawet ich części. Na przykład każda osoba w administracji może mieć możliwość uzyskania listy pracowników firmy, ale tylko wybrane osoby mogą mieć dostęp do informacji o wynagrodzeniach. Problem jest czymś więcej niż tylko poziomem szczegółowości. Podczas gdy system operacyjny może przyznać użytkownikowi uprawnienia dostępu do pliku lub korzystania z aplikacji, po czym nie ma dalszych kontroli bezpieczeństwa, system zarządzania bazą danych musi podejmować decyzję o każdej indywidualnej próbie dostępu. Decyzja ta będzie zależeć nie tylko od tożsamości użytkownika, ale także od konkretnych części danych, do których uzyskiwany jest dostęp, a nawet od informacji już ujawnionych użytkownikowi.

Ogólny model kontroli dostępu realizowany przez system zarządzania plikami lub bazami danych to macierz dostępu. Podstawowymi elementami modelu są:

* Podmiot. Jednostka posiadająca dostęp do obiektów. Ogólnie rzecz biorąc, pojęcie podmiotu jest tożsame z pojęciem procesu. Każdy użytkownik lub aplikacja faktycznie uzyskuje dostęp do obiektu za pomocą procesu, który reprezentuje tego użytkownika lub aplikację.

* Obiekt. Wszystko, do czego dostęp jest kontrolowany. Przykłady obejmują pliki, fragmenty plików, programy i segmenty pamięci.

* Prawo dostępu. Sposób, w jaki podmiot uzyskuje dostęp do obiektu. Przykłady to odczyt, zapis i wykonanie.

Jeden wymiar macierzy składa się ze zidentyfikowanych podmiotów, które mogą próbować uzyskać dostęp do danych. Zazwyczaj lista ta będzie się składać z indywidualnych użytkowników lub grup użytkowników, chociaż dostęp może być kontrolowany dla terminali, hostów lub aplikacji zamiast lub dodatkowo do użytkowników. Drugi wymiar zawiera listę obiektów, do których można uzyskać dostęp. Na najwyższym poziomie szczegółowości obiekty mogą być pojedynczymi polami danych. Bardziej zagregowane grupy, takie jak rekordy, pliki, a nawet cała baza danych, również mogą być obiektami w macierzy. Każdy wpis w macierzy wskazuje prawa dostępu tego podmiotu do tego obiektu. W praktyce macierz dostępu jest zwykle rzadka i jest implementowana przez dekompozycję na jeden z dwóch sposobów. Macierz może być rozłożona na kolumny, dając listy kontroli dostępu. Dlatego dla każdego obiektu lista kontroli dostępu zawiera listę użytkowników i ich dozwolonych praw dostępu. Lista kontroli dostępu może zawierać wpis domyślny lub publiczny. Dzięki temu użytkownicy, którzy nie są wyraźnie wymienieni jako mający uprawnienia specjalne, mogą mieć domyślny zestaw uprawnień. Elementy listy mogą obejmować zarówno pojedynczych użytkowników, jak i grupy użytkowników. Dekompozycja według wierszy daje bilety możliwości. Bilet możliwości określa autoryzowane obiekty i operacje dla użytkownika. Każdy użytkownik ma kilka biletów i może być upoważniony do pożyczania lub przekazywania ich innym. Ponieważ bilety mogą być rozproszone w systemie, stanowią one większy problem bezpieczeństwa niż listy kontroli dostępu. W szczególności bilet musi być niemożliwy do podrobienia. Jednym ze sposobów na osiągnięcie tego polega na tym, aby system operacyjny przechowywał wszystkie bilety w imieniu użytkowników. Bilety te musiałyby znajdować się w obszarze pamięci niedostępnym dla użytkowników.

Zagadnienia sieciowe dotyczące kontroli dostępu zorientowanej na dane są równoległe z tymi, które dotyczą kontroli dostępu zorientowanej na użytkownika. Jeśli tylko niektórym użytkownikom zezwala

się na dostęp do pewnych elementów danych, może być potrzebne szyfrowanie, aby chronić te elementy podczas transmisji do upoważnionych użytkowników. Zazwyczaj kontrola dostępu do danych jest zdecentralizowana, to znaczy kontrolowana przez systemy zarządzania bazami danych oparte na hoście. Jeśli sieciowy serwer bazy danych istnieje w sieci, wówczas kontrola dostępu do danych staje się funkcją sieciową.

Ochrona oparta na trybie systemu operacyjnego.

Jedna technika stosowana we wszystkich systemach operacyjnych w celu zapewnienia ochrony opiera się na trybie wykonywania procesora. Większość procesorów obsługuje co najmniej dwa tryby wykonywania: tryb normalnie związany z systemem operacyjnym i tryb zwykle związany z programami użytkownika. Niektóre instrukcje mogą być wykonywane tylko w bardziej uprzywilejowanym trybie. Obejmowałyby one odczyt lub zmianę rejestru sterującego, takiego jak słowo statusu programu; prymitywne instrukcje we / wy; oraz instrukcje dotyczące zarządzania pamięcią. Ponadto dostęp do niektórych regionów pamięci można uzyskać tylko w bardziej uprzywilejowanym trybie. Tryb mniej uprzywilejowany często nazywany jest trybem użytkownika, ponieważ program użytkownika zwykle wykonywałby się w tym trybie. Bardziej uprzywilejowany tryb nazywany jest trybem systemowym, trybem sterowania lub trybem jądra. Ten ostatni termin odnosi się do jądra systemu operacyjnego, czyli tej części systemu operacyjnego, która obejmuje ważne funkcje systemowe. Powód używania dwóch trybów powinien być jasny. Konieczne jest zabezpieczenie systemu operacyjnego oraz kluczowe tabele systemu operacyjnego, takie jak bloki sterowania procesami, przed zakłóceniami ze strony programów użytkownika. W trybie jądra oprogramowanie ma pełną kontrolę nad procesorem i wszystkimi jego instrukcjami, rejestrami i pamięcią. Ten poziom kontroli nie jest konieczny, a ze względów bezpieczeństwa nie jest pożądany w przypadku programów użytkownika. Powstają dwa pytania: skąd procesor wie, w jakim trybie ma wykonywać pracę i jak zmienia się tryb? Odnośnie pierwszego pytania, zazwyczaj w słowie statusu programu znajduje się bit, który wskazuje tryb wykonywania. Ten bit jest zmieniany w odpowiedzi na pewne zdarzenia. Na przykład, gdy użytkownik wywołuje usługę systemu operacyjnego, tryb jest ustawiany na tryb jądra. Zwykle odbywa się to poprzez wykonanie instrukcji zmieniającej tryb. Gdy użytkownik wykonuje wywołanie usługi systemowej lub gdy przerwanie przekazuje kontrolę do procedury systemowej, procedura wykonuje instrukcję zmiany trybu, aby przejść do bardziej uprzywilejowanego trybu i wykonuje ją ponownie, aby przejść do mniej uprzywilejowanego trybu przed zwróceniem kontroli użytkownikowi proces. Jeśli program użytkownika spróbuje wykonać instrukcję zmiany trybu, spowoduje to po prostu wywołanie systemu operacyjnego, które zwróci błąd, chyba że zmiana trybu ma być dozwolona. Można również zapewnić bardziej wyrafinowane mechanizmy. Powszechnym schematem jest użycie struktury zabezpieczającej pierścień. W tym schemacie pierścienie o niższych numerach lub pierścienie wewnętrzne cieszą się większym przywilejem niż pierścienie o wyższych numerach lub pierścienie zewnętrzne. Zazwyczaj pierścień 0 jest zarezerwowany dla funkcji jądra systemu operacyjnego z aplikacjami na wyższym poziomie. Niektóre narzędzia lub usługi systemu operacyjnego mogą zajmować pierścień pośredni. Podstawowe zasady systemu pierścieniowego to:

* Program może uzyskać dostęp tylko do tych danych, które znajdują się w tym samym pierścieniu lub w mniej uprzywilejowanym pierścieniu.

* Program może wywoływać usługi znajdujące się w tym samym lub bardziej uprzywilejowanym dzwonku.

Przykład podejścia do ochrony pierścienia można znaleźć w systemie VAX VMS OS, który wykorzystuje cztery tryby:

1. Jądro. Wykonuje jądro systemu operacyjnego VMS, które obejmuje zarządzanie pamięcią, obsługę przerwań i operacje we / wy.

2. Wykonawczy. Wykonuje wiele wywołań usług systemu operacyjnego, w tym procedury zarządzania plikami i nagraniami (dyski i taśmy).

3. Nadzorca. Wykonuje inne usługi systemu operacyjnego, takie jak odpowiedzi na polecenia użytkownika.

4. Użytkownik. Wykonuje programy użytkownika oraz narzędzia, takie jak kompilatory, edytory, konsolidatory i debuggery.

Proces wykonywany w mniej uprzywilejowanym trybie często musi wywołać procedurę, która jest wykonywana w bardziej uprzywilejowanym trybie; na przykład program użytkownika wymaga usługi systemu operacyjnego. To wywołanie jest osiągane za pomocą instrukcji zmiany trybu (CHM), która powoduje przerwanie przekazujące sterowanie do procedury w nowym trybie dostępu. Zwrot jest wykonywany przez wykonanie instrukcji REI (powrót z wyjątku lub przerwania).

Typowe funkcje systemu operacyjnego w trybie jądra

Zarządzanie procesem

* Tworzenie i kończenie procesów

* Planowanie i wysyłanie procesów

* Przełączanie procesów

* Synchronizacja procesów i obsługa komunikacji międzyprocesowej

* Zarządzanie blokami sterowania procesami

Zarządzanie pamięcią

* Alokacja przestrzeni adresowej do procesów

* Zamiana

* Zarządzanie stronami i segmentami

Zarządzanie I / O

* Zarządzanie buforami

* Alokacja kanałów I / O i urządzeń do procesów

Funkcje wspierające

* Obsługa przerwań

* Księgowość

* Monitorowanie

str. 24.10

Ochrona oparta na wirtualizacji.

Wraz z rosnącą dostępnością pamięci (np. Od dziesiątek do setek gigabajtów pamięci RAM), miejsca na dysku (od terabajtów do petabajtów pamięci), szybszych procesorów (dziesiątki gigaherców) i systemów wielordzeniowych (potencjalnie tysiące procesorów pracujących równolegle), wirtualizacja komputerów osiągnął praktyczną i powszechną użyteczność. Instancje środowiska operacyjnego mogą współistnieć przy użyciu współdzielonych zasobów, nie pozwalając na bezpośrednią komunikację między nimi. Każda instancja jest hermetyzowana i całkowicie chroniona przed włamaniami lub zakłóceniami ze strony procesów uruchomionych na innych maszynach wirtualnych współdzielących te same zasoby fizyczne.

UDOSTĘPNIANIE PLIKÓW

Systemy dla wielu użytkowników prawie zawsze wymagają, aby pliki mogły być współużytkowane przez wielu użytkowników. Powstają dwie kwestie: prawa dostępu i zarządzanie równoczesnym dostępem.

Prawa dostępu.

System plików powinien zapewniać elastyczne narzędzie umożliwiające szerokie udostępnianie plików między użytkownikami. System plików powinien zapewniać kilka opcji, aby można było kontrolować sposób uzyskiwania dostępu do określonego pliku. Zwykle użytkownikom lub grupom użytkowników przyznaje się określone prawa dostępu do pliku. Zastosowano szeroki zakres praw dostępu. Następna lista zawiera prawa dostępu, które można przypisać określonemu użytkownikowi do określonego pliku.

* Żaden. Użytkownik może nawet nie dowiedzieć się o istnieniu pliku, a tym bardziej uzyskać do niego dostęp. Aby wymusić to ograniczenie, użytkownik nie będzie mógł odczytać katalogu użytkownika zawierającego ten plik.

* Wiedza, umiejętności. Użytkownik może określić, czy plik istnieje i kto jest jego właścicielem. Użytkownik może wówczas zwrócić się do właściciela o dodatkowe prawa dostępu.

* Wykonanie. Użytkownik może załadować i uruchomić program, ale nie może go skopiować. Programy własnościowe często są udostępniane z tym ograniczeniem.

* Blokowanie. Użytkownik może zmienić stan flagi logicznej, która wskazuje tymczasowe ograniczenia dostępu do danych. Systemy zarządzania bazami danych zapewniają blokowanie w celu kontrolowania równoczesnego dostępu do rekordów, dzięki czemu różne procesy mogą uniknąć wzajemnego nadpisywania modyfikacji.

* Czytanie. Użytkownik może czytać plik w dowolnym celu, w tym kopiowanie i wykonywanie. Niektóre systemy są w stanie wymusić rozróżnienie między przeglądaniem a kopiowaniem. W pierwszym przypadku zawartość pliku może zostać wyświetlona użytkownikowi, ale użytkownik nie ma możliwości wykonania kopii.

* Dołączanie. Użytkownik może dodawać dane do pliku, często tylko na końcu, ale nie może modyfikować ani usuwać żadnej zawartości pliku. Prawo to jest przydatne przy zbieraniu danych z wielu źródeł.

* Aktualizacja. Użytkownik może modyfikować, usuwać i dodawać dane do pliku. Zwykle obejmuje to początkowe zapisanie pliku, przepisanie go w całości lub w części oraz usunięcie całości lub części danych. Niektóre systemy rozróżniają różne stopnie aktualizacji.

* Zmiana ochrony. Użytkownik może zmieniać prawa dostępu przyznane innym użytkownikom. Zwykle tylko właściciel pliku ma to prawo. W niektórych systemach właściciel może rozszerzyć to prawo na

inne. Aby zapobiec nadużyciom tego mechanizmu, właściciel pliku zazwyczaj jest w stanie określić, które prawa może zmienić posiadacz tego rozszerzonego prawa.

* Usunięcie. Użytkownik może usunąć plik z systemu plików.

Można uznać, że prawa te tworzą hierarchię, przy czym każde prawo implikuje te, które je poprzedzają. Tak więc, jeśli określonemu użytkownikowi zostanie przyznane prawo do aktualizacji określonego pliku, wówczas również temu użytkownikowi zostaną przyznane te prawa: wiedza, wykonywanie, odczyt i dołączanie. Jeden użytkownik jest wyznaczony jako właściciel danego pliku, zwykle jest to osoba, która pierwotnie utworzyła plik. Właściciel ma wszystkie wymienione wcześniej prawa dostępu i może przyznawać je innym. Dostęp można zapewnić różnym klasom użytkowników:

* Określony użytkownik. Indywidualni użytkownicy, którzy są określani przez identyfikator użytkownika

* Grupy użytkowników. Zestaw użytkowników, którzy nie są definiowani indywidualnie. System musi mieć jakiś sposób na śledzenie członkostwa w grupach użytkowników.

* Wszyscy. Wszyscy użytkownicy, którzy mają dostęp do tego systemu. To są pliki publiczne.

Jednoczesny dostęp

Gdy przyznano dostęp w celu dołączenia lub aktualizacji pliku dla więcej niż jednego użytkownika, system operacyjny lub system zarządzania plikami musi wymusić dyscyplinę. Podejście brutalnej siły polega na umożliwieniu użytkownikowi zablokowania całego pliku, gdy ma zostać zaktualizowany. Dokładniejsza kontrola polega na blokowaniu poszczególnych rekordów podczas aktualizacji. Projektując możliwość współdzielonego dostępu, należy uwzględnić kwestie wzajemnego wykluczania i impasu.

ZAUFANE SYSTEMY

Wiele z tego, co dotychczas dyskutowano, dotyczyło ochrony danej wiadomości lub przedmiotu przed pasywnym lub aktywnym atakiem ze strony danego użytkownika. Nieco innym, ale szeroko stosowanym wymogiem jest ochrona danych lub zasobów na podstawie poziomów bezpieczeństwa. Jest to często spotykane w wojsku, gdzie informacje są klasyfikowane jako jawne (U), poufne (C), tajne (S), ściśle tajne (TS) lub poza nimi. Pojęcie to ma również zastosowanie w innych obszarach, w których informacje można uporządkować w kategorie brutto, a użytkownikom można przyznać zezwolenia na dostęp do pewnych kategorii danych. Na przykład najwyższy poziom bezpieczeństwa może dotyczyć dokumentów i danych dotyczących planowania strategicznego, do których dostęp mają tylko urzędnicy korporacji i ich pracownicy; W następnej kolejności mogą pojawić się wrażliwe dane finansowe i osobowe, dostępne tylko dla personelu administracyjnego, pracowników korporacji i tak dalej. W przypadku zdefiniowania wielu kategorii lub poziomów danych wymaganie określa się jako wielopoziomowe zabezpieczenia. Ogólne stwierdzenie wymogu wielopoziomowego bezpieczeństwa mówi, że temat na wysokim poziomie nie może przekazywać podmiotowi informacji na niższym lub nieporównywalnym poziomie, chyba że przepływ ten dokładnie odzwierciedla wolę upoważnionego użytkownika. Ze względów wdrożeniowych wymóg ten składa się z dwóch części i jest po prostu określony. Wielopoziomowy bezpieczny system musi wymuszać:

1. Nie czytaj dalej. Podmiot może czytać tylko obiekt o niższym lub równym poziomie bezpieczeństwa. W literaturze jest to określane jako prosta właściwość zabezpieczająca.

2. Nie zapisuj. Podmiot może pisać tylko w obiekcie o wyższym lub równym poziomie bezpieczeństwa. W literaturze jest to określane jako właściwość $*$ (wymawiane właściwości gwiazdy).

Te dwie reguły, jeśli są odpowiednio egzekwowane, zapewniają wielopoziomowe bezpieczeństwo. W przypadku systemu przetwarzania danych podejście, które zostało przyjęte i było przedmiotem wielu badań i rozwoju, opiera się na koncepcji monitora referencyjnego. Monitor referencyjny jest elementem sterującym w sprzęcie i systemie operacyjnym komputera, który reguluje dostęp badanych do obiektów na podstawie parametrów bezpieczeństwa podmiotu i obiektu. Monitor referencyjny ma dostęp do pliku, znanego jako baza danych jądra bezpieczeństwa, który zawiera listę uprawnień dostępu (poświadczenie bezpieczeństwa) każdego podmiotu oraz atrybuty ochrony (poziom klasyfikacji) każdego obiektu. Monitor referencyjny wymusza reguły bezpieczeństwa (bez odczytu, bez zapisu) i ma następujące właściwości:

* Pełna mediacja. Zasady bezpieczeństwa są egzekwowane przy każdym dostępie, a nie tylko, na przykład, podczas otwierania pliku.

* Izolacja. Monitor referencyjny i baza danych są chronione przed nieautoryzowaną modyfikacją.

* Sprawdzalność. Poprawność monitora referencyjnego musi być możliwa do udowodnienia. Oznacza to, że musi istnieć możliwość matematycznego wykazania, że monitor referencyjny egzekwuje zasady bezpieczeństwa i zapewnia pełną mediację i izolację.

To są sztywne wymagania. Wymóg pełnej mediacji oznacza, że każdy dostęp do danych w pamięci głównej oraz na dysku i taśmie musi być zapośredniczony. Czyste implementacje oprogramowania nakładają zbyt duży spadek wydajności, aby były praktyczne; rozwiązanie musi być przynajmniej częściowo sprzętowe. Wymóg izolacji oznacza, że atakujący, bez względu na to, jak sprytny, nie może mieć możliwości zmiany logiki monitora referencyjnego lub zawartości bazy danych jądra zabezpieczeń. Wreszcie wymóg dowodu matematycznego jest poważny w przypadku czegoś tak złożonego, jak komputer ogólnego przeznaczenia. System, który może zapewnić taką weryfikację, nazywany jest systemem zaufanym.

Ważne zdarzenia dotyczące bezpieczeństwa, takie jak wykryte naruszenia bezpieczeństwa i autoryzowane zmiany w bazie danych jądra zabezpieczeń, są przechowywane w pliku kontroli. Starając się zaspokoić własne potrzeby i jako usługę dla społeczeństwa, Departament Obrony USA w 1981 r. Utworzył Centrum Bezpieczeństwa Komputerowego w ramach Agencji Bezpieczeństwa Narodowego (NSA), mając na celu zachęcanie do powszechnej dostępności zaufanych systemów komputerowych. Cel ten jest realizowany poprzez produkt Commercial Product Evaluation Program. Zasadniczo centrum próbuje ocenić produkty dostępne na rynku jako spełniające właśnie nakreślone wymagania bezpieczeństwa. Centrum klasyfikuje ocenione produkty według zakresu zapewnianych przez nie zabezpieczeń. Oceny te są potrzebne w przypadku zamówień Departamentu Obrony, ale są publikowane i bezpłatnie dostępne. W związku z tym mogą służyć jako wskazówki dla klientów komercyjnych przy zakupie dostępnego na rynku, gotowego sprzętu.

Obrona przed koniem trojańskim

Atak konia trojańskiego obejmuje oprogramowanie, które wydaje się mieć akceptowalne funkcje, ale ukrywa dodatkowe, nieautoryzowane funkcje. Jednym ze sposobów zabezpieczenia się przed atakami koni trojańskich jest użycie bezpiecznego, zaufanego systemu operacyjnego. W tym przypadku koń trojański jest używany do obejścia standardowego mechanizmu bezpieczeństwa używanego w większości systemów zarządzania plikami i systemów operacyjnych: listy kontroli dostępu. W tym przykładzie użytkownik o imieniu Bob wchodzi w interakcję za pośrednictwem programu z plikiem danych zawierającym krytyczny ciąg znaków „CPE170KS”. Użytkownik Bob utworzył plik z uprawnieniami do odczytu / zapisu nadanymi tylko programom wykonującym się we własnym imieniu: to znaczy, że dostęp do pliku mają tylko procesy, których właścicielem jest Bob. Atak konia trojańskiego

rozpoczyna się, gdy wrogi użytkownik o imieniu Alice uzyskuje legalny dostęp do systemu i instaluje zarówno program konia trojańskiego, jak i plik prywatny, który ma być użyty w ataku jako „tylna kieszeń”. Alice przyznaje sobie prawo do odczytu / zapisu tego pliku i daje Bobowi prawo tylko do zapisu. Alicja skłania teraz Boba do wywołania programu będącego koniem trojańskim, być może poprzez reklamowanie go jako użytecznego narzędzia. Kiedy program wykryje, że jest wykonywany przez Boba, odczytuje wrażliwy ciąg znaków z pliku Boba i kopiuje go do pliku Alice. Zarówno operacje odczytu, jak i zapisu spełniają ograniczenia narzucone przez listy kontroli dostępu. Alicja ma wtedy dostęp do pliku Roberta tylko później, aby poznać wartość ciągu. Rozważ teraz użycie bezpiecznego systemu operacyjnego w tym scenariuszu. Poziomy bezpieczeństwa są przypisywane podmiotom podczas logowania na podstawie kryteriów, takich jak terminal, z którego uzyskiwany jest dostęp do komputera, oraz zaangażowany użytkownik, określony hasłem / identyfikatorem. W tym przykładzie istnieją dwa poziomy bezpieczeństwa, wrażliwy (szary) i publiczny (biały), uporządkowane w taki sposób, że wrażliwy jest wyższy niż publiczny. Procesom należącym do pliku danych Roberta i Roberta przypisywany jest poziom bezpieczeństwa wrażliwy. Plik i procesy Alicji są ograniczone do publicznego. Jeśli Bob wywołuje program konia trojańskiego, program ten uzyskuje poziom bezpieczeństwa Roberta. Jest więc w stanie, w ramach prostej właściwości security, obserwować wrażliwy ciąg znaków. Jednak gdy program próbuje zapisać łańcuch w pliku publicznym (w pliku z tylną kieszenią), naruszana jest właściwość $*$ i monitor referencyjny nie zezwala na próbę. W związku z tym próba zapisu do pliku z tylną kieszenią jest odrzucana, mimo że lista kontroli dostępu na to zezwala: Polityka bezpieczeństwa ma pierwszeństwo przed mechanizmem listy kontroli dostępu.