Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej Nr 21

XV Seminarium
ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE' 2005
Oddział Gdański PTETiS

ZAGADNIENIA BEZPIECZEŃSTWA SYSTEMÓW OPERACYJNYCH

Jerzy KACZMAREK[1], Michał WRÓBEL[2]

1. Politechnika Gdańska, ul. G. Narutowicza 11/12, 80-952 Gdańsk
   tel: (058) 347 2682 fax: (058) 347 2727 e-mail:jkacz@eti.pg.gda.pl
2. Politechnika Gdańska, ul. G. Narutowicza 11/12, 80-952 Gdańsk
   tel: (058) 348 6085 fax: (058) 347 1006 e-mail:wrobel@task.gda.pl

Bezpieczeństwo systemów komputerowych wymaga ochrony takich zasobów jak konfiguracja systemu operacyjnego, aplikacje oraz dane. W pracy przedstawiono metodę zabezpieczania systemu operacyjnego Linux poprzez podział zasobów i ich zapis na różnych typach nośników: niemodyfikowalnych, z możliwością fizycznego zablokowania zapisu oraz modyfikowalnych. Opisany sposób pozwala na eliminację większości zagrożeń spowodowanych przełamaniem przez intruza zabezpieczeń programowych w komputerze.

1. WSTĘP

Największym zagrożeniem przy wykorzystywaniu komputerów podłączonych do sieci Internet jest niebezpieczeństwo utraty danych i niszczenia konfiguracji poprzez świadome ataki intruzów. Konieczne jest poszukiwanie nowych metod zabezpieczenia, które zminimalizują skutki takich ataków.

Zaproponowana w artykule metoda polega na podziale na grupy zasobów zgromadzonych w komputerze na trzy grupy: system operacyjny, aplikacje i dane użytkowników. Dla wyróżnionych zasobów możliwe jest zastosowanie oddzielnej polityki dostępu, począwszy od całkowitej lub czasowej blokady, aż do niezabezpieczenia danych, które jednak będą systematycznie i okresowo archiwizowane.

W artykule zaproponowano wykorzystanie mechanizmów zabezpieczeń dostępnych w typowych urządzeniach, takich jak całkowicie niemodyfikowalne płyty CD czy urządzenia typu pamięci flash, które posiadają możliwość fizycznego zablokowania zapisu danych. Istnieją jednak takie zbiory danych, które, z uwagi na częstą modyfikację, muszą znajdować się na dyskach twardych. Dla nich należy dokonywać zgodnie z istniejącymi procedurami archiwizacji całkowitej i przyrostowej.

Znane metody zabezpieczania polegające na uniemożliwianiu dostępu do zasobów, takie jak zapora ogniowa (ang. *firewall*), nie zawsze są skuteczne. Przedstawiona metoda pozwala na eliminację zagrożeń wynikających z dostępu intruza do systemu operacyjnego.

Recenzent: Dr inż. Piotr Szpryngier - Wydział Elektroniki, Telekomunikacji i Informatyki Politechniki Gdańskiej

2. ZAPEWNIANIE BEZPIECZEŃSTWA SYSTEMU OPERACYJNEGO

Poprawnie działający system operacyjny umożliwia pracę komputera, a zwłaszcza uruchamianie programów użytkowych przetwarzających dane. System operacyjny Linux składa się z jądra zarządzającego pamięcią RAM, procesami i plikami oraz programu zwanego interpretatorem poleceń shell, który umożliwia wydawanie poleceń przez użytkownika do systemu operacyjnego. Jedną z ważniejszych funkcji jądra systemu jest rozpoznawanie i sterowanie urządzeniami zewnętrznymi, których duża różnorodność i dynamiczny rozwój prowadzą do licznych problemów z ich obsługą.

Jądro systemu operacyjnego jest zbiorem programów, które są niemodyfikowalne po zainstalowaniu danej wersji systemu operacyjnego Linux. Mogą być zatem zapisywane na nośnikach trwałych. Inne dane, takie jak aplikacje, dane konfiguracyjne i dane użytkownika, wymagają odmiennej polityki bezpieczeństwa.

2.1. Problemy bezpieczeństwa systemów operacyjnych

Zapewnianie bezpieczeństwa komputera polega na zabezpieczaniu konfiguracji systemu operacyjnego i danych w nim zawartych. Najpoważniejszym zagrożeniem występującym obecnie są włamania osób niepowołanych do systemów komputerowych za pośrednictwem sieci Internet.

Zagadnienie bezpieczeństwa systemu operacyjnego można podzielić na ochronę przed niepowołanym dostępem do danych (ang. *security*) oraz na zapewnienie stabilność pracy komputera (ang. *safety*).

Terminem *security* określane jest stosowanie takich zabezpieczeń systemów komputerowych, które umożliwiają użytkownikom wykonywanie tylko tych operacji, które są zgodne z polityką bezpieczeństwa. Oznacza to, że dostęp do zasobów programowych i danych mają tylko autoryzowani użytkownicy. Głównym celem tak rozumianego bezpieczeństwa jest uniemożliwienie dostępu do zasobów przez osoby do tego nieuprawnione. Pomimo istnienia polityki haseł, programów uniemożliwiających zdalny dostęp typu firewall, podziału sieci lokalnych na grupy komputerów o różnych priorytetach dostępu, nie istnieją w pełni bezpieczne systemy operacyjne w sensie *security*.

Zapewnienia bezpieczeństwa w sensie *safety* polega na utrzymaniu stabilności pracy systemu komputerowego. Polega to na takim zabezpieczaniu danych, że nawet włamanie do systemu nie spowoduje znacznych strat. Metody pozwalające na takie zabezpieczania wydają się bardziej skuteczne z punktu widzenia zabezpieczania samego systemu operacyjnego oraz aplikacji w nim zawartych, natomiast nie zapewniają całkowitego bezpieczeństwa danych.

Należy zauważyć, że obie wymienione wyżej grupy bezpieczeństwa są ważne w przypadku włamania. Uzyskanie przez intruza dostępu do systemu może skutkować zarówno utratą danych, jak również doprowadzić do niestabilności w pracy komputera. Pierwszy przypadek ma miejsce, jeżeli system został zaatakowany z zamiarem dokonania destrukcji. Niestabilność pracy systemu operacyjnego będzie miała miejsce w przypadku zainstalowania na zaatakowanym komputerze programów umożliwiających późniejszy dostęp do jego zasobów, tzw. koni trojańskich. Są one wykorzystywane przede wszystkim do rozsyłania wiadomości reklamowych oraz do atakowania innych maszyn za pomocą techniki *Distributed Denial-of-Service*.

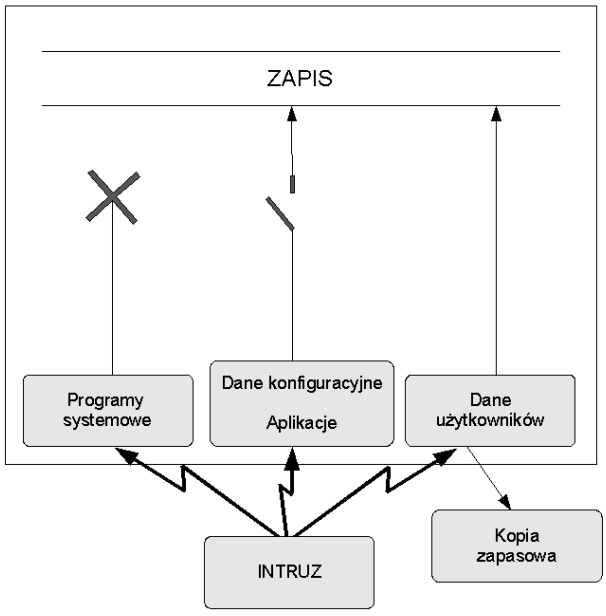
W celu zabezpieczenia systemu operacyjnego należy wyeliminować przede wszystkim możliwość zmiany lub modyfikacji programów systemowych przez włamywacza. Należy również zapewnić możliwości szybkiego przywrócenia usuniętych lub zmienionych danych z plików archiwalnych, poprzez specjalne programy do tego przeznaczone.

2.2. Proponowany model bezpieczeństwa

Podstawową zasadą w proponowanym modelu jest podział danych w komputerze na grupy i wykorzystanie sprzętowych możliwości urządzeń do blokady modyfikacji tych danych. Urządzenia te mogą zapisywać dane jednorazowo w sposób całkowicie niemodyfikowalny, lub pozwalać również na modyfikację zapisanych danych .

Chronione zasoby można podzielić na programy systemowe, dane konfiguracyjne, aplikacje oraz dane użytkowników.

W celu zapewnienia bezpieczeństwa działania systemu operacyjnego dla każdej z tych grup należy zastosować inną politykę bezpieczeństwa. Przy wyborze sposobu zabezpieczania należy wziąć pod uwagę częstość zmian danych oraz ryzyko, jakie niesie za sobą ich zmiana. Na rysunku 1 przedstawiono typy danych stanowiących oprogramowanie komputera oraz proponowane tryby zapisu danych.



Rys. 1. Model bezpieczeństwa systemu komputerowego.

Według proponowanego modelu pliki programów systemowych powinny być zablokowane przed możliwością modyfikacji. Zmiana kodu programów systemowych dokonana przez intruza niesie za sobą poważne skutki. Atak tego typu może spowodować niestabilność systemu operacyjnego, a nawet zawieszenie go i utratę dostępu do komputera.

Pliki konfiguracyjne programów wymagają czasami modyfikacji z uwagi na zmiany sprzętu i oprogramowania. Dane te mogą być zwykle zabezpieczone przed zapisem i udostępnione w trybie tylko do odczytu. W przypadku konieczności zmiany w konfiguracji komputera można udostępnić pliki w trybie do zapisu. Jest korzystne, aby w chwili zmian konfiguracji nie było możliwości dostępu przez sieć do komputera. Oznacza to, że na czas zapisu nowej konfiguracji należy wyłączyć połączenie z siecią Internet.

Aplikacje zainstalowane w komputerze zmieniają się w przypadku instalacji nowych wersji tych programów lub rozszerzania ich rodzajów. Czynności te nie są jednak częste, a zdarzają się sporadycznie. Po zainstalowaniu aplikacji pliki z nią związane mogą być zapisane w trybie tylko do odczytu, co w żadnym stopniu nie ogranicza możliwości wykorzystania tych aplikacji. Dlatego programy użytkowe mogą znajdować się na nośnikach niemodyfikowalnych, jak również na tych z czasową możliwością modyfikacji.

Ostatnią grupą są dane użytkowników oraz dane generowane przez aplikacje i system podczas ich pracy. Nie jest możliwe całkowite zablokowanie zapisu tego typu danych. W takiej sytuacji mogą być one usunięte lub zmienione przez intruza. Proponowanym sposobem zabezpieczenia tych danych jest regularne ich archiwizowanie. Może ona polegać na tworzeniu tzw. kopii przyrostowej, czyli zapisywaniu tylko danych stworzonych i zmienionych od ostatniej archiwizacji lub przez tworzenie pełnej kopii całego systemu. Konieczne jest również zapewnienie szybkiego przywrócenia zarchiwizowanych danych w przypadku stwierdzenia włamania.

Proponowany model wymaga wyboru sposobu jego realizacji poprzez dostosowanie typu urządzeń do zapisu danych, podziału danych w ramach systemu i wyboru odpowiedniego trybu dostępu do danych.

3. REALIZACJA MODELU BEZPIECZEŃSTWA

Istnieje wiele możliwych sposobów realizacji proponowanego modelu bezpieczeństwa, który polega na podziale danych i wyborze dla nich odpowiednich nośników zapisu. Obecnie opracowano mechanizmy pozwalające na tworzenie dystrybucji systemu Linux, które mogą być uruchamiane bezpośrednio z płyty CD-ROM. Dystrybucje takie nazywane są LiveCD. Charakteryzują się tym, że nie wymagają instalacji na dysku twardym. System operacyjny znajdujący się na tych płytach jest przenoszony bezpośrednio do pamięci RAM i komputer może pracować nawet bez żadnego dysku twardego.

Wszystkie dystrybucje typu LiveCD umożliwiają szybkie przywrócenie stanu pierwotnego systemu operacyjnego. W przypadku stwierdzenia nieprawidłowej pracy, np. w skutek włamania, wystarczające jest ponowne uruchomienie komputera.

Ważną cechą dystrybucji LiveCD jest fakt, że dane przechowywane na nośnikach takich jak CD-ROM są niemodyfikowalne. Ograniczenia te nie wynikają z zabezpieczeń programowych, które zawsze mogą zostać złamane, lecz z fizycznej natury nośnika.

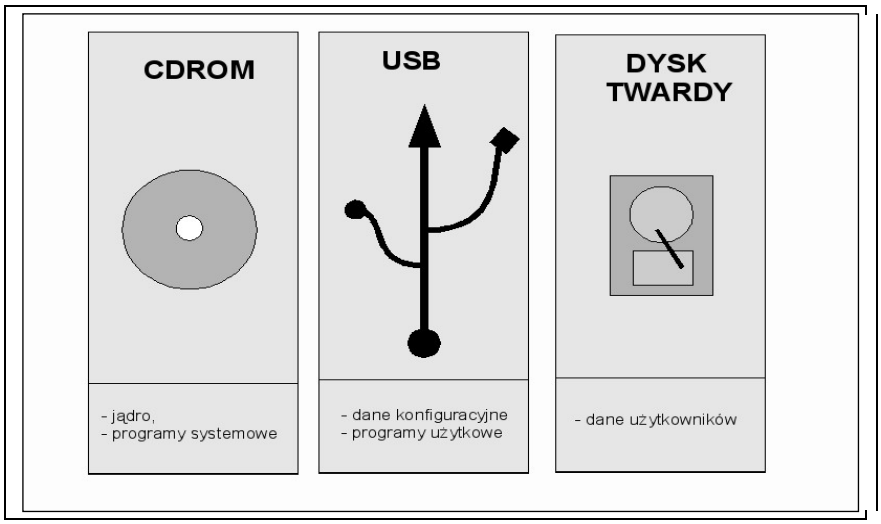
Rozszerzeniem możliwości płyt LiveCD jest wykorzystanie podręcznych pamięci flash podłączanych do portu USB, tzw. *pendrivów*. Niektóre typy tych urządzeń mają sprzętową możliwość czasowego blokowania zapisu.

Część danych obecnych w systemie operacyjnym wymaga jednak ciągłej modyfikacji podczas pracy systemu. Konieczne jest również okresowa aktualizacja oprogramowania oraz instalacja nowych programów. W popularnych dystrybucjach LiveCD problem przechowywania zmieniających się danych rozwiązano poprzez wykorzystanie części pamięci RAM jako dysk (tzw. *ram dysk),* na którym zapisywane są dane, które ulegają zmianom.

Z uwagi na cechy pamięci RAM dochodzi do utraty tego typu danych w przypadku wyłączenia komputera.

3.1. Bezpieczeństwo danych z uwzględnieniem typu nośników

Wykorzystując fakt, że dane zapisane na nośnikach takich jak CD-ROM, czy pendrive są fizycznie zabezpieczone przed modyfikacją, możliwe jest zastosowanie proponowanego modelu bezpieczeństwa. Jedną z możliwych implementacji tego modelu bezpieczeństwa jest podzielenie zasobów na grupy i zapisanie ich na nośnikach w zależności od niezbędnej konieczności ich modyfikacji, co zilustrowano na rysunku 2.



Rys. 2. Sposób realizacji modelu bezpieczeństwa

Proponuje się, aby jądro systemu i programy systemowe zapisane były na niemodyfikowalnej płycie CD-ROM i stanowiły tzw. płytę LiveCD. Dane te nie ulegają częstej modyfikacji, występuje ona tylko w momencie zmiany jądra lub typu systemu. Dane konfiguracyjne oraz programy użytkowe mogą znajdować się również na płycie LiveCD lub pamięć flash ze sprzętową blokadą zapisu. Przy właściwym zaplanowaniu zapotrzebowania użytkowników na aplikacje instalacja nowego oprogramowania odbywa się okresowo. W przypadku dokonywania częstych zmian w zainstalowanym oprogramowania oraz danych konfiguracyjnych korzystne jest stosowanie pamięci flash. Dane użytkowników, które są z zasady permanentnie modyfikowane muszą być umieszczane na dyskach twardych. Przestrzeganie procedur archiwizacji zapewnia bezpieczeństwo tych danych od strony serwera. W przypadkach ataków intruzów występuje groźba utraty tych danych, lecz nie jest to zagrożenie dla stabilności systemu operacyjnego.

Należy dodatkowo zwrócić uwagę na jądro systemu operacyjnego. W systemie operacyjnym Linux części kodu jądra, tzw. moduły, mogą być dołączane dynamicznie już podczas pracy systemu. W proponowanym modelu bezpieczeństwa należy zablokować taką możliwość w celu eliminacji zagrożenia załadowania modułu jądra przez włamywacza. Możliwość taką daje zastosowanie czysto monolitycznego jądra z wyłączoną funkcją dołączania modułów.

Proponowane rozwiązanie chroni dane, ale nie zabezpiecza procesów uruchomionych przez system operacyjny, których kod znajduje się w pamięci RAM.

Rozwiązaniem tych problemów jest zmiana organizacji przechowywania i uruchamiania plików aplikacji. Na nośnikach fizycznie zabezpieczonych przed zapisem można trzymać oryginalne pliki aplikacji, jak również dodatkowe pliki z ich sumą kontrolną. Podczas każdorazowego uruchamiania programów użytkowych dokonywana powinna być kontrola zgodności kodu aplikacji z jej niemodyfikowalnym wzorcem. W przypadku stwierdzenie niezgodności zawartości pliku z zapisaną sumą kontrolną, uruchamiany powinien być oryginalny program z nośnika niemodyfikowalnego. Podobny mechanizm można zastosować dla plików konfiguracyjnych. Ponieważ te mechanizmy uruchamiane są tylko w nadzwyczajnych okolicznościach, nie powinny zmniejszać wydajności systemu operacyjnego.

Mechanizm sprawdzania integralności plików programów z ich niemodyfikowalnymi sumami kontrolnymi może zostać zintegrowany z jądrem systemu operacyjnego. Dzięki temu zapewniona jest wydajność działania tych mechanizmów. Jądro systemu operacyjnego jest ładowane tylko raz, podczas startu systemu i nie jest możliwa jego modyfikacja przez potencjalnych intruzów.

Taka organizacja danych w systemie operacyjnym zgodna z proponowanym modelem podnosi znacznie poziom bezpieczeństwa systemu operacyjnego.

4. WNIOSKI KOŃCOWE

Zapewnienie bezpieczeństwa systemów komputerowych jest jednym z najważniejszych i najtrudniejszych problemów w dziedzinie informatyki. Przyjmuje się, że nie ma możliwości zapewnienia całkowitego bezpieczeństwa. Wszelkie metody i mechanizmy, które zwiększają poziom bezpieczeństwa powinny być stosowane. Proponowana metoda uzależnienia sposób zapisu danych od charakteru tych danych i częstości ich modyfikacji. Może być powszechnie stosowana, ponieważ nie wymaga dodatkowego oprogramowania czy narzędzi wspomagających.

5. BIBLIOGRAFIA

1. Silberschatz A., Galvin P. B.: Podstawy systemów operacyjnych, WNT, 2002.
2. Nemeth E., Snyder G.: Przewodnik administratora systemu Unix, WNT, 1998
3. Love R.: Linux Kernel. Przewodnik programisty, Helion. 2004

A PROBLEMS OF OPERATING SYSTEM SECURITY

Computer systems security requires protection of operating system configuration, applications and frequently modified data. The work presents a method of increasing data security by assigning adequate access rights and access media to data. Data is divided into three categories stored on different media: read-only CD-ROM drives, written only flash disks and read/write hard drives. The described solution eliminates many threats resulting from breaking of software protections.