
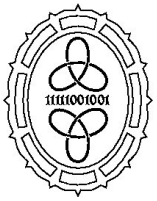

Uniwersytet Mikołaja Kopernika
w Toruniu

Wydział Matematyki i Informatyki

Wydział Fizyki, Astronomii
i Informatyki Stosowanej


Jan Werner

Bezpieczeństwo systemów i lokalnej sieci komputerowej

Praca magisterska napisana
pod kierunkiem
dra hab. Jacka Kobusa

Toruń 2005

Spis treści

1 Wstęp

Celem projektu FOLA jest stworzenie wygodnej, łatwej w rozbudowie i konfiguracji platformy narzędziowej do zarządzania grupami serwerów i stacji roboczych. W skład systemu FOLA mają wchodzić moduły automatyzujące wykonywanie większości codziennych zadań związanych z administrowaniem zasobami lokalnej sieci komputerowej. Do tych zadań między innymi należy rejestrowanie nowych maszyn w sieci, monitorowanie ich funkcjonowania oraz integralności, zarządzanie kontami użytkowników, zarządzanie pakietami oprogramowania, tworzenie kopii zapasowych. Poszczególne moduły działają niezależnie, ale docelowo oferowane przez nie funkcje powinny być dostępne z poziomu wspólnego interfejsu. Zasadniczym celem niniejszej pracy jest zbudowanie narzędzia umożliwiającego zbieranie i analizowanie danych dotyczących integralności monitorowanych systemów komputerowych oraz lokalnej sieci komputerowej oraz przygotowywanie zbiorczych raportów i wszczynanie alarmów.

Zasady i mechanizmy nadzorowania bezpieczeństwa systemów komputerowych ewoluowały wraz z ewolucją systemów informatycznych. W przypadku komputerów pracujących w trybie wsadowym problem bezpieczeństwa sprowadzał się do fizycznej ochrony zasobów. Powstanie systemów wieloprocesorowych i wielużytkownikowych zrodziło potrzebę rozgraniczania zasobów wykorzystywanych przez użytkowników na poziomie systemu operacyjnego. Dostęp do zasobów takich jak pamięć operacyjna, czas jednostki centralnej, urządzenia zewnętrzne jest możliwy tylko w trybie nadzorcy. Użytkownicy uzyskują dostęp do tych zasobów poprzez mechanizm wywołań systemowych. Oznacza to, że poziom bezpieczeństwa systemu komputerowego zależy bezpośrednio od stopnia ochrony dostępu do trybu nadzorcy.

Rozwój sieci komputerowych i gwałtowny rozwój Internetu począwszy od lat 80. ubiegłego wieku ujawnił nowe zagrożenia. Drugiego listopada 1988 roku Robert Tappan Morris Jr. wypuścił robaka internetowego, który praktycznie sparaliżował ówczesny Internet[1]. To zdarzenie uświadomiło społeczności internetowej powagę sytuacji i spowodowało powołanie specjalnego zespołu do reagowania na zdarzenia naruszające bezpieczeństwo systemów komputerowych, tj. CERT (*Computer Emergency Response Team*)[2]. Upowszechnienie się komputerów osobistych pracujących w sieci Internet przyczyniło się do łatwości rozprzestrzeniania się zagrożeń takich jak robaki i wirusy oraz wzrostu liczby ataków. Dodatkowo komputery osobiste stały się celem samych ataków polegających na wykradaniu danych, instalowaniu oprogramowania szpiegowskiego, itp.

Zarządzanie bezpieczeństwem systemów komputerowych pracujących w lokalnej sieci wymaga gromadzenia danych z wielu różnych źródeł oraz ich analizy pod kątem występowania potencjalnych zagrożeń. Problemem nie jest sam proces gromadzenia danych, ale trudność w wykryciu symptomów naruszeń integralności nadzorowanych systemów komputerowych. Celem niniejszej pracy jest

przedstawienie i scharakteryzowanie zagrożeń, na które narażone są systemy informatyczne i sieci lokalne oraz zbudowanie (zaczątków) systemu umożliwiającego wygodne zarządzanie bezpieczeństwem maszyn i sieci.

System FOLASecurity składa się z centralnej stacji zarządzającej, która gromadzi i przetwarza dane pochodzące od monitorowanych stacji. Są to komputery, które zostały zarejestrowane w systemie oraz wyposażone w odpowiednie oprogramowanie regularnie gromadzące dane o integralności systemu plików, konfiguracji interfejsów sieciowych, itp. Zakres wykonywanych przez klientów czynności jest określany przez zawartość specjalnych plików określających politykę nadzoru.

Rejestracja klienta wiąże się z utworzeniem na stacji zarządzającej specjalnego konta użytkownika związanego z daną stacją oraz ustanowieniem bezpiecznego kanału komunikacyjnego. Pozwala to z jednej strony na przekazywanie gromadzonych na stacji klienckiej danych do stacji zarządzającej, a z drugiej na przekazywanie ze stacji zarządzającej zleceń dla klientów.

Klienci z zadaną częstotliwością realizują zadania związane z przypisaną im polityką nadzoru, zlecenia pozostawione przez administratora oraz informują o wykonanych czynnościach. Dane uzyskane w trakcie realizowania zadań są porównywane z danymi wzorcowymi zebranymi podczas dodawania klienta do systemu. W razie wykrycia jakichkolwiek rozbieżności klient powiadamia administratora serwera FOLASecurity o wystąpieniu naruszenia integralności, a także przygotowuje raport i umieszcza go na serwerze. Zarządzanie systemem FOLASecurity odbywa się na serwerze za pomocą interfejsu umożliwiającego m. in. określanie i wdrażanie polityki nadzoru, przygotowywanie zleceń dla klientów, przeglądanie raportów poszczególnych klientów oraz raportów zbiorczych.

System FOLASecurity został napisany w języku Perl, który umożliwia wygodne tworzenie narzędzi systemowych, dysponuje doskonałymi narzędziami do obróbki tekstu, a także umożliwia korzystanie z ogromnej liczby modułów dostępnych w CPAN[3]. Na system składają się skrypty perlowe oraz liczne funkcje zgromadzone w odrębnych bibliotekach. Zlecenia przekazywane są w formacie dokumentów w języku XML tworzonych i parsowanych z użyciem modułu perlowego LibXML. Całość dostarczana jest w postaci archiwum tgz wraz z instalatorami oprogramowania dla maszyn klienckich i stacji zarządzającej. Brakujące w systemie moduły perlowe mogą zostać doinstalowane na życzenie użytkownika. System FOLASecurity udostępniony jest na zasadach ogólnej licencji publicznej GNU GPL[4].

Plan pracy jest następujący. Rozdział drugi przedstawia szczegółową systematykę zagrożeń oraz opisuje możliwe formy ataków. Dodatkowo przedstawione są podstawowe mechanizmy zabezpieczeń systemu Unix/Linux. Przedstawione są również pewne metody prewencji i wykrywania naruszeń bezpieczeństwa sieci i systemu komputerowego. Rozdział trzeci przedstawia architekturę systemu FOLASecurity, funkcje serwera i klientów oraz protokół komunikacyjny. Rozdział czwarty przedstawia szczegóły implementacji systemu, a piąty zawiera podsumo-

wanie. Załączniki zawierają specyfikację dotyczącą wymagań systemu FOLASecurity, szczegóły procesu instalacji, strukturę katalogów na serwerze i systemach klienckich oraz dokumentację bibliotek funkcji. Do niniejszej pracy dołączona jest płyta CD-ROM, na której zostało umieszczone oprogramowanie oraz dokumentacja w formie elektronicznej.