BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 17, 2002

System ochrony poczty elektronicznej wykorzystujący oprogramowanie PGP

Zbigniew ŚWIERCZYŃSKI

Zakład Teleinformatyki, Instytut Automatyki i Robotyki WAT
ul. Kaliskiego 2, 00-908 Warszawa

STRESZCZENIE: W artykule przedstawiona została propozycja konfiguracji oprogramowania PGP, które służy do zabezpieczania wiadomości poczty elektronicznej oraz zapewnia mechanizmy bezpiecznego dystrybuowania kluczy publicznych.

1. Wstęp

W miarę postępu technologii teleinformatycznej coraz większa ilość korespondencji wymieniana jest w postaci elektronicznej. Ponieważ przesyłanie informacji poprzez Internet w żadnym wypadku nie może zostać uznane za bezpieczne, ochrona kryptograficzna staje się koniecznością. Wraz z rozwojem komputerów i ich mocy obliczeniowych rosną też możliwości łamania zabezpieczeń chroniących dane przed przestępcami. Dlatego aby skutecznie chronić cenne dane należy wprowadzać zaawansowane, dostosowane do potrzeb rozwiązania umożliwiające szyfrowanie i elektroniczne podpisywanie przesyłanych wiadomości.

Aby zapewnić szyfrowanie oraz elektroniczny podpis wiadomości pocztowych można wykorzystać oprogramowanie PGP (Pretty Good Privacy – nazwa często tłumaczona jest jako Całkiem Niezła Prywatność). Oprogramowanie wykorzystuje kryptosystem (tzn. systemem szyfrująco-deszyfrujący), który bazuje na idei szyfrowania asymetrycznego. Feewarowe oprogramowanie PGP można skopiować z różnych serwerów internetowych np. ze strony http://web.mit.edu/network/pgp.html lub http://pgp.com/. Wersje komercyjne oprogramowania PGP są oferowane przez firmę PGP Corporation.

Wykorzystanie tego produktu daje możliwość dołączenia opcji szyfrowania do pulpitu użytkownika Windows oraz m.in. do programów pocztowych Microsoft Outlook, Outlook Express, czy Lotus Notes. Szyfrowanie wiadomości poczty elektronicznej transmitowanej przez kanały nie dające gwarancji poufności ani integralności jest podstawową dziedziną stosowania oprogramowania PGP. Przez poufność rozumie się tu niemożność zrozumienia treści wiadomości np. przez osoby, których nie uprawniał do tego nadawca; przez zapewnienie integralności - niemożność wprowadzania modyfikacji np. przez osoby nieuprawnione w sposób, który uniemożliwiałby wykrycie tej ingerencji przez odbiorcę.

Oprogramowanie PGP pozwala nie tylko szyfrować listy, aby uniemożliwić poznanie ich treści, ale także podpisywać listy zaszyfrowane lub niezaszyfrowane w sposób umożliwiający adresatowi (adresatom) stwierdzenie, czy list pochodzi rzeczywiście od nadawcy, oraz czy treść wiadomości nie była po podpisaniu modyfikowana. Dodatkową korzyścią jest uzyskanie niezaprzeczalności przekazywanej informacji.

Szczególnie istotny z punktu widzenia użytkownika poczty elektronicznej jest fakt, że techniki szyfrowania asymetrycznego nie wymagają wcześniejszego przekazania kanałem gwarantującym poufność klucza służącego do szyfrowania. Rozwiązuje to tzw. „problem dystrybucji kluczy. Dzięki temu, używając PGP, mogą ze sobą korespondować np. osoby, dla których poczta elektroniczna (kanał niepoufny) jest jedyną formą kontaktu.

Oprogramowanie PGP w obecnie dostępnej wersji należy do grupy systemów hybrydowych – zostały w wykorzystane zarówno algorytmy szyfrowania symetrycznego (DES, IDEA) jak i asymetrycznego (RSA). Pierwszą operacją wykonywaną przez oprogramowanie PGP na danych wejściowych jest ich kompresja, następnie są one zaszyfrowane za pomocą algorytmu symetrycznego. Klucz wymagany do tego szyfrowania zostaje wygenerowany losowo. Kolejną operacją jest zaszyfrowanie użytego w algorytmie symetrycznym klucza, za pomocą tzw. klucza publicznego adresata, czyli odbiorcy przesyłki. Kluczem publicznym nazywa się jeden z pary kluczy wykorzystywanych w szyfrowaniu asymetrycznym, klucz ten jest publicznie udostępniany. Wysyłaną wiadomość tworzą: zaszyfrowane dane i zaszyfrowany klucz.

Do odszyfrowania należy użyć klucza prywatnego odbiorcy (drugi z pary kluczy wykorzystywanej w szyfrowaniu asymetrycznym, ten klucz powinien być znany tylko jego właścicielowi). Użytkownik odszyfrowuje najpierw klucz wykorzystany do szyfrowania symetrycznego, a następnie przy jego użyciu odszyfrowuje wiadomość. Operacje kryptograficzne przy wykorzystaniu

algorytmów symetrycznych są około 1000 razy szybsze niż szyfrowanie asymetryczne.

2. Problem wiarygodności kluczy publicznych

Aby zaszyfrować wiadomość pocztową lub sprawdzić podpis elektroniczny dołączony do otrzymanej wiadomości konieczne jest posiadanie klucza publicznego użytkownika, z którą wymieniana jest korespondencja. Klucz publiczny można pozyskać metoda bezpośrednią (np. poprzez uzyskanie dyskietki z kluczem publicznym od użytkownika, który jest jego właścicielem) lub metodą pośrednią (np. przesłanie klucza poczta elektroniczną lub pobranie z serwera kluczy). Serwerem kluczy nazywa się oprogramowanie dedykowane do przechowywania, udostępniania i zarządzania kluczami publicznymi. Serwery kluczy umożliwiają określenie zasad i ograniczeń związanych z wymianą kluczy. Funkcje serwera kluczy w rodzinie produktów PGP realizuje program PGP Keyserver, który dokładniej został opisany w punkcie 4.1.

Gdy użytkowników, z którymi należy wymieniać informacje w postaci zaszyfrowanej, jest niewielu i dodatkowo jest z nimi bezpośredni kontakt problem wymieniania się kluczami publicznymi jest niewielki. Nie ma też powodów do podejrzeń, iż pozyskany klucz nie należy do użytkownika, z którym nadawca zamierza korespondować. Jednakże w sytuacji gdy nie ma kontaktu z danym użytkownikiem, nie zna go nadawca, a dodatkowo jest takich odbiorców kilku lub więcej, pozyskanie kluczy publicznych może być uciążliwe. Istotnym problemem w takiej sytuacji jest również zapewnienie wiarygodności udostępnionych kluczy. Jeśli uzyskano taki klucz z niepewnego źródła i nie posiada on cech, które jednoznacznie wskazywały by rzeczywistego właściciela, to można mieć wątpliwość co do jego autentyczności, czyli nie ma pewności, że zaszyfrowanej wiadomości nie może odczytać i zrozumieć ktoś inny niż ten, do którego jest ona kierowana.

W celu zwiększania wiarygodności kluczy publicznych można podpisywać je kluczem prywatnym użytkownika, który w ten sposób poręcza autentyczność podpisanego klucza. Istotne jest aby użytkownik chcący korzystać z tak podpisanego klucza publicznego miał zaufanie do złożonego podpisu.

3. Organizacja potwierdzania kluczy

Ponieważ w procesie generowania kluczy każdy może podać dowolne dane personalne oraz adres e-mail, istnieje możliwość, iż np. klucz skojarzony z nazwiskiem „Poważny” faktycznie będzie należał do pana o nazwisku

„Oszust" i to on będzie mógł zapoznać się z treścią zaszyfrowanej wiadomości. Aby przeciwdziałać umieszczaniu na serwerze kluczy przez osoby podszywające się za kogoś innego, każdy klucz powinien zostać potwierdzony, czyli odpowiednio podpisany. Osiągnąć to można wprowadzając system potwierdzania kluczy. Tylko klucze podpisane kluczem tajnym przez osobę wyznaczoną arbitralnie w ramach organizacji będą uznawane za godne zaufania. Dodatkowo należy tak skonfigurować serwer kluczy, aby podpis ten stał się warunkiem koniecznym umieszczenia klucza publicznego w bazie kluczy, co zminimalizuje prawdopodobieństwo omyłkowego pobrania i użycia klucza publicznego nie posiadającego odpowiedniego potwierdzenia.

System potwierdzania kluczy ma także zapewnić, że żaden fałszywy (zawierające nieprawdziwe dane użytkownika) klucz nie zostanie opatrzony podpisem zaufanej osoby. Należy zaznaczyć, iż klucz publiczny powinien być dostarczony w celu jego pierwszego podpisania osobie godnej zaufania przez właściciela tego klucza, w przeciwnym razie potwierdzenie takowe traci sens. W większych organizacjach, gdzie podpisanie wszystkich kluczy przez jedną i tą samą osobę zaufaną jest trudne do zrealizowania, powinny zostać wprowadzone pośrednie szczeble ufności. Polega to na tym, że główna osoba zaufana podpisze tylko klucze, które zostaną przedstawione jej osobiście przez użytkowników, lub które zostały wcześniej opatrzone podpisem osób odpowiednio uprawnionych dla mniejszych grup. Takie zaufane osoby uprawnione są do podpisywania wyłącznie kluczy przedstawianych im osobiście przez użytkowników. Uniemożliwia to podmianę kluczy przy przesyłaniu do potwierdzenia niechronionym kanałem, a co za tym idzie potwierdzenie sfałszowanego klucza. Następnie klucze zostaną przesłane do potwierdzenia przez główną osobę zaufaną i dopiero po podpisaniu przez nią zostaną umieszczone na serwerze kluczy, skąd mogą je pobrać je inni użytkownicy.

4. Propozycja konfiguracji oprogramowania PGP

System szyfrowania wiadomości pocztowych wykorzystujący oprogramowanie PGP zorganizowany na potrzeby organizacji liczącej np. 1000 osób wymaga (poza zainstalowaniem oprogramowania na stacjach roboczych użytkowników) opracowania i wdrożenia systemu dystrybucji kluczy publicznych. Do tego celu można wykorzystać aplikację PGP Keyserver.

We wdrożeniu systemu szyfrowania i jego późniejszej obsługi warto wykorzystać program PGPadmin, który służy do zarządzania środowiskiem klienckim PGP.

Wdrażanie oprogramowania PGP należy rozpocząć od zainstalowania i skonfigurowania serwera kluczy, co szczegółowo zostało opisane w punkcie

4.2 niniejszego opracowania. Kolejnym etapem po zainstalowaniu serwera kluczy będzie stworzenie szablonu instalacyjnego oprogramowania PGP dla stacji roboczych (w tym celu należy skorzystać z programu PGPadmin). Opis czynności związanych z tworzeniem szablonu instalacyjnego zawarty został w punkcie 6. Szablonem instalacyjnym nazwano specjalnie skonfigurowaną wersje instalacyjną oprogramowania PGP. Skorzystanie z szablonu w trakcie instalacji oprogramowania PGP zapewnia odpowiednią jego konfiguracje. Opis czynności związanych z instalacją oprogramowania PGP na stacji roboczej został zamieszczony w punkcie 5. Ważnym elementem systemu szyfrowania wiadomości pocztowych jest mechanizm potwierdzania kluczy zwiększający ich wiarygodność, który opisano w punkcie 3.

4.1 Serwer kluczy

Na potrzeby sprawnego dystrybucji kluczy publicznych między użytkownikami PGP można zainstalować serwer, na którym przechowywane będą klucze publiczne użytkowników. Każdy użytkownik może na tego typu serwerze opublikować swój klucz publiczny oraz odszukać i pobrać klucze publiczne osób, do których zamierza wysyłać zaszyfrowane wiadomości poczty elektronicznej. Jest to wygodna metoda dystrybucji kluczy, szczególnie w dużych organizacjach, gdzie przekazywanie klucza w wiadomości pocztowej lub na nośniku (np. dyskietce), ewentualnie umieszczanie kluczy publicznych na ogólnie dostępnych, publicznych serwerach są niewystarczające ze względu dostępność lub wiarygodność przechowywanych tam kluczy. Przy szyfrowaniu asymetrycznym wymiana kluczy publicznych użytkowników jest warunkiem koniecznym do prowadzenia zaszyfrowanej wymiany informacji drogą elektroniczną. Dlatego też klucze publiczne powinny być dostępne dla użytkowników w każdej chwili, z zapewnieniem autentyczności, czyli prawdziwości informacji opisujących klucz publiczny, np. nazwy właściciela klucza. Aby zapewniać autentyczność kluczy publicznych konieczne jest wprowadzenie mechanizmów programowych i organizacyjnych, które nie dopuszczą do podłożenia klucza, którego właściciel domniemany (przez użytkownika) i rzeczywisty nie są tą samą osobą.

Do przechowywania i zarządzania kluczami publicznymi można wykorzystać oprogramowanie PGP Keyserver (w artykule opisywana jest wersja 7.0), wchodzące w skład pakietu PGP Corporate Desktop Suite (do niedawna w ofercie firmy NAI). W pakiecie znajdują się, poza serwerem kluczy, następujące programy:

- PGP Desktop Security, na który składają się następujące elementy składowe:

- PGP Mail & File – moduł programowy odpowiedzialny za szyfrowanie i cyfrowe podpisywanie poczty elektronicznej. Oprogramowanie to integruje się z popularnymi klientami poczty, np. Microsoft Outlook, Microsoft Outlook Express, Eudora.
- PGP Disk – moduł zapewniający wirtualne, szyfrowane dyski logiczne. Dostęp do zaszyfrowanych danych możliwy jest przy użyciu prywatnego klucza PGP uprawnionej osoby.
- PGP Distributed Firewall – moduł chroniący stacje robocze przed atakami ze strony Internetu i intranetu. Oprogramowanie pozwala zdefiniować reguły, na podstawie których filtrowany jest ruch wchodzący i wychodzący ze stacji.
- Moduł IDS generuje ostrzeżenia, jeżeli jakieś zdarzenie zostanie rozpoznane jako próba włamania do systemu.
- PGP Keys – moduł programowy służący do zarządzania lokalnie przechowywanymi kluczami publicznymi (zbiór kluczy przechowywanych lokalnie określa się mianem keyring), tworzenia własnej pary kluczy, importowania i eksportowania kluczy z lub do serwera kluczy.

- PGPadmin –program służący do generowania szablonów instalacyjnych oraz administrowania już zainstalowanymi programami PGP na stacjach roboczych, np. do automatycznego uaktualnienia oprogramowania. Możliwości programu PGPadmin opisane zostały szerzej w punkcie 6.

PGP Keyserver składa się z trzech ściśle ze sobą współpracujących elementów, mianowicie:

- PGP Keyserver – program umożliwiający użytkownikom umieszczanie na serwerze oraz wyszukiwanie i pobieranie kluczy z baz danych programu PGP Keyserver.
- Web Console – narzędzie pozwalające zarządzać i konfigurować PGP Keyserver poprzez przeglądarkę internetową.
- Replication Engine – element pozwalający replikować bazy kluczy pomiędzy programami PGP Keyserver, zainstalowanymi na różnych komputerach.

Program PGP Keyserver 7.0 może zostać zainstalowany na platformie systemowej Windows NT Serwer 4.0 z uaktualnieniem Service Pack w wersji co

najmniej 6a lub Windows 2000 z Service Pack w wersji 1. Jeżeli na tym samym komputerze mają funkcjonować inne programy pakietu PGP Corporate Desktop Suite, to powinny być one zainstalowane w pierwszej kolejności. Zasady instalacji PGP Mail & File, PGP Disk, PGP Distributed Firewall, PGP Keys oraz PGPadmin zostały opisane w punkcie 5. Po zainstalowaniu tych modułów można przystąpić do instalacji programu PGP Keyserver. Wymagania sprzętowe, jakie muszą zostać spełnione, aby serwer kluczy mógł funkcjonować to: 64 MB pamięci RAM, 15 MB wolnego miejsca na twardym dysku (w celu zainstalowania oprogramowania), dodatkowo od 10 do 500 MB miejsca na bazę danych przechowującą klucze (przy założeniu, że przechowywanych będzie ok. 1000 kluczy potrzebne jest ok. 20 MB). Ponieważ Web Console – narzędzie służące do konfiguracji parametrów programu PGP Keyserver uruchamiane jest w przeglądarce internetowej, a transmisja danych jest chroniona, do zarządzania aplikacją Keyserver konieczne jest posiadanie przeglądarki umożliwiającej szyfrowanie 128 bitowym kluczem (Microsoft Internet Explorer w wersji minimum 5.5 lub Netscape Communicator wersja minimum 4.76.).

Dla zapewnienia ciągłej dostępności do przechowywanych kluczy oprogramowanie powinno zostać zainstalowane na dwóch komputerach znajdujących się w różnych lokalizacjach (w celu zminimalizowania skutków sytuacji kryzysowych np. pożaru). Aplikacje PGP Keyserver zainstalowane na dwóch komputerach mogą współpracować poprzez mechanizm replikacji bazy kluczy. Narzędzie potrzebne do wykonywania replikacji dostarczane jest jako element programu PGP Keyserver. Replikacja może być uruchamiana ręcznie lub automatycznie jako usługa Windows NT 4.0 Server lub Windows 2000.

Replikacja baz danych zawierających klucze publiczne umożliwia utrzymanie synchronizacji informacji między dwoma serwerami. Zapewnia to większą odporność danych na sytuacje kryzysowe, w razie zbyt dużego obciążenia lub awarii jednego z serwerów daje możliwość uzyskania klucza z drugiego serwera. Aby możliwy był wybór, z którego serwera pobierany będzie klucz, oba serwery powinny być dostępne poprzez sieć komputerową dla każdego uprawnionego użytkownika.

Spośród dostępnych rodzajów replikacji interesującym wydaje się być mechanizm replikacji wykorzystującej dwa serwery: nadrzędny i podrzędny. Polega on na tym, iż jeden z serwerów zostaje wskazany jako nadrzędny i tylko na nim można umieszczać nowe klucze lub modyfikować już istniejące. Sposób promowania serwera do roli nadrzędnego został opisany w punkcie 4.2. Baza kluczy na drugim, podrzędnym serwerze uaktualniana jest przez automatyczną, jednokierunkową replikację wykonywaną natychmiast po wprowadzeniu modyfikacji kluczy na serwerze nadrzędnym. Możliwe jest zablokowanie replikowania usunięć kluczy, co przy ewentualnym usunięciu kluczy przez osoby nieuprawnione nie pozwoli na przeniesienie tych zmian na serwer

podrzędny. Ten typ replikacji polecany jest ze względu na to, iż proces replikacji przebiega natychmiast po wprowadzeniu zmian w bazie kluczy i wykonuje się tylko w jedną stronę (z serwera nadrzędnego do podrzędnego), co zapewnia wysoką dostępność i bezpieczeństwo danych przechowywanych na serwerach. Ze względu na to, iż do serwera podrzędnego (przechowuje aktualną kopię bazy kluczy) w trakcie prawidłowego funkcjonowania serwera nadrzędnego ma dostęp tylko administrator (użytkownicy nie muszą nawet wiedzieć o istnieniu serwera podrzędnego) konfiguracja taka wydaje się być odporną na ewentualne złośliwe kasowanie lub uszkadzanie przechowywanych kluczy. W przypadku włamania do serwera nadrzędnego i wprowadzenia zmiany np. skasowania części kluczy, na serwerze podrzędnym w dalszym ciągu znajduje się baza kluczy sprzed włamania i wystarczy zmiana praw dostępu do tej bazy aby udostępnić użytkownikom przechowywane tam klucze.

4.2 Instalacja i konfiguracja serwera kluczy

Jeżeli na jednym komputerze maja zostać zainstalowane wszystkie programy pakietu PGP Corporate Desktop Suite, to instalację oprogramowania pakietu PGP Corporate Desktop Suite, należy rozpocząć od zainstalowania programu PGP Desktop Security, następnie zainstalować PGPadmin, a na końcu PGP Keyserver. W tym celu należy uruchomić program instalacyjny programu PGP Desktop Security, następnie po automatycznym rozpakowaniu potrzebnych do instalacji plików uruchomiony zostaje instalator, który prowadzi użytkownika poprzez kolejne etapy instalacji. Po zatwierdzeniu warunków licencyjnych instalator pyta, czy użytkownik posiada już parę swoich kluczy. Po wybraniu opcji „No, I'm a new user" (generowanie nowych kluczy zostało opisane w punkcie 7) instalator proponuje miejsce instalacji oprogramowania oraz rodzaj instalowanych składników. Jeżeli program jest instalowany na stacji roboczej, to zalecane jest wybranie elementów integrujących funkcje szyfrowania i podpisywania (pluginy) z odpowiednimi aplikacjami pocztowymi.

Po restarcie można rozpocząć instalacje serwera kluczy. Pierwsza faza instalacji aplikacji PGP Keyserver polega na właściwym rozmieszczeniu plików programu na dysku oraz wprowadzeniu podstawowych parametrów konfiguracyjnych. Pierwsze okno programu konfiguracyjnego pozwala na określenie miejsca przechowywania plików konfiguracyjnych (domyślnie: C:\Program Files\Network Associates\PGP Keyserver\Etc\PGPcertd.cfg). Kolejne okno umożliwia wprowadzenie nazwy użytkownika, który będzie administrował programem PGP Keyserver oraz jego hasła. Następne okno służy do określenia numeru portu na potrzeby usług HTTP (domyślnie: 11371), kolejne okno umożliwia podanie numeru portu obsługującego połączenie z Web

Console (domyślnie: 443) oraz adres konta poczty elektronicznej administratora programu PGP Keyserver. Ostatnie okno daje możliwość wygenerowania certyfikatu X.509 dla organizacji, którą będzie obsługiwał serwer kluczy.

Po wprowadzeniu opisanych wyżej informacji należy uruchomić narzędzie Web Console i przystąpić do ustawiania parametrów pracy serwera. Na komputerze, na którym zainstalowany jest PGP Keyserver możliwe jest uruchomienie Web Console przez wybranie kolejno: *Start* → *Programy* → *PGP Keyserver* → *Web Console*. Zawsze istnieje możliwość uruchomienia tego narzędzia poprzez wpisanie na dowolnej stacji w przeglądarce adresu: https://„nazwa_komputera lub adres IP":„nr_portu"/keyserver/, np.: https://172.16.50.137:443/keyserver/. W trakcie uruchamiania konsoli służącej do administrowania serwerem kluczy, użytkownik autoryzowany jest poprzez sprawdzanie jego nazwy i hasła.

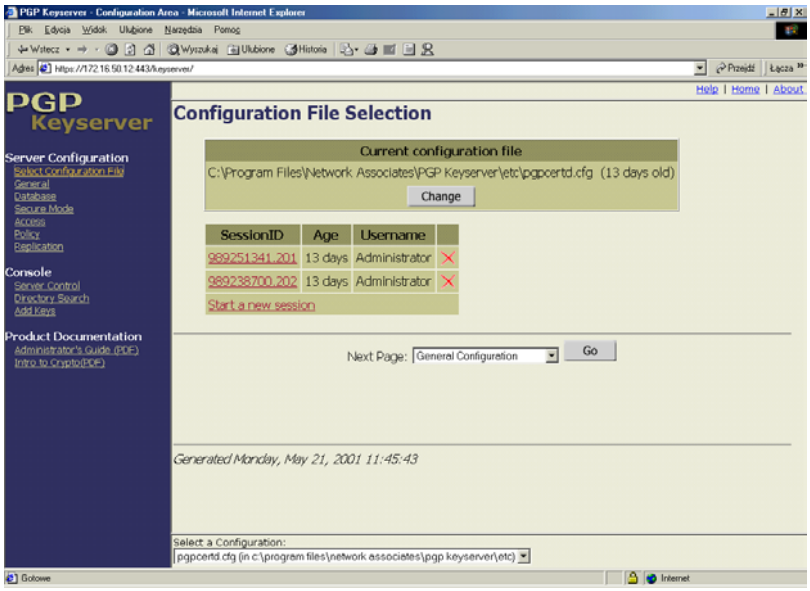
Po uruchomieniu konsoli konfiguracyjnej po lewej stronie ekranu znajduje się lista możliwych do wyboru widoków. Każdy z nich dotyczy odpowiedniej grupy parametrów konfiguracyjnych serwera kluczy.

Pierwszy z ekranów, „Select Configuration File" umożliwia wybór profilu konfiguracyjnego dla programu PGP Keyserver. Ekran „Select Configuration File" został przedstawiony na Rys 1. Ustawienia serwera zapisywane są w pliku, który można również modyfikować w edytorze tekstowym.

Pliki konfiguracyjne domyślnie znajdują się w katalogu C:\Program Files\Network Associates\PGP Keyserver\Etc i posiadają rozszerzenie .cfg. Można wybrać dowolny istniejący plik konfiguracyjny i nakazać wykorzystywanie go przez program PGP Keyserver. Dokonuje się tego w oknie „Current configuration file" ekranu „Select Configuration File". Aby nowe ustawienia zostały uwzględnione należy każdą zmianę zapisać a następnie zrestartować PGP Keyserver. Służą do tego odpowiednie przyciski znajdujące się na każdym ekranie konfiguracyjnym.

Na ekranie „General" znajdują się pola służące do wprowadzenia numeru portu dla połączeń LDAP (uproszczonego protokołu dostępu do katalogów, który jest wykorzystywany przy łączeniu się z serwerem kluczy w celu pobrania lub umieszczenia na nim klucza poprzez sieć komputerową) Na tym ekranie ustawia się parametry dotyczące gromadzenia opisów zdarzeń dotyczących pracy serwera. Ekran „General" został przedstawiony na rys. 2. Administrator określa w tym miejscu zdarzenia jakie maja być odnotowywane, co jaki czas listy zdarzeń będą archiwizowane i w jaki sposób będą przedstawiane na ekranie.

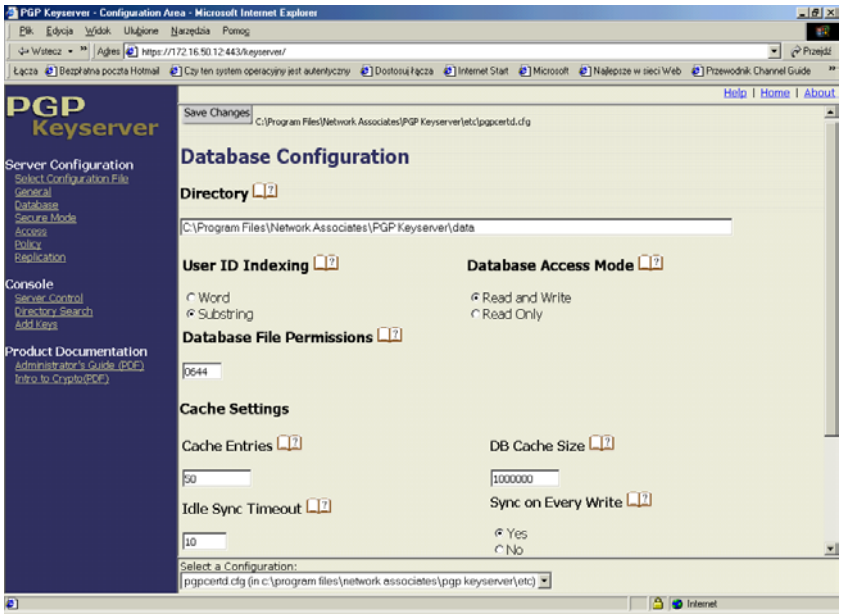
Rys. 1. Widok ekranu „Select configuration file”



Rys. 2. Widok ekranu „General”

W grupie ustawień nazwanych „Database” zapisana jest ścieżka dostępu do katalogu, w którym przechowywane są klucze publiczne. Na tym ekranie

określane są prawa dostępu do bazy przechowującej klucze oraz sposób indeksowania bazy kluczy. Ekran „Database" przedstawiony został na rys. 3.

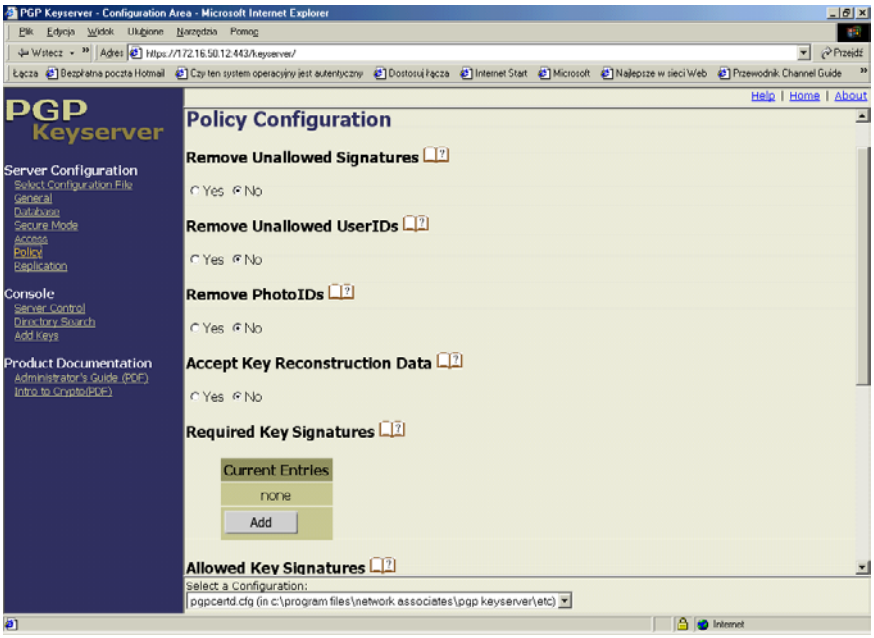


Rys. 3. Widok ekranu „Database"

Rys. 4. Widok ekranu „Access"

Aby pozwolić na serwerze nadrzędnym nie tylko na pobieranie i wyszukiwanie kluczy, ale również na dodawanie przez użytkowników nowych kluczy konieczne jest na stronie konfiguracyjnej „Access", w miejscu „Default Access" zaznaczenie opcji „Add". Na serwerze podrzędnym należy ustawić tą opcję na „Read". Można wskazać grupę osób lub komputerów, które będą miały inne prawa dostępu. Służy do tego opcja „Allow Access By", gdzie specyfikuje się np. adresy IP i nadane im uprawnienia. Należy dodać w tym miejscu prawo dostępu na poziomie „Admin" dla adresu IP komputera centralnego administratora PGP. Na ekranie można wyspecyfikować rodzaje dostępu do bazy kluczy, które będą odnotowywane w liście „Access Log File". Ekran „Access" przedstawiony został na rys. 4.

Ekran „Policy" (rys. 5) służy do wprowadzania reguł ustanawiających, jakie klucze mogą być przechowywane na serwerze. Wprowadzając w miejscu „Required Key Signatures" dane identyfikujące klucz głównego administratora PGP (pozycja ID na zakładce General we właściwościach klucza oglądanych w aplikacji PGP Keys) można ograniczyć umieszczanie na serwerze kluczy tylko do tych, które zostały podpisane przez zaufanego użytkownika.



Rys. 5. Widok ekranu „Policy"

Opisana w punkcie 3 proponowana struktura potwierdzania kluczy wyklucza możliwość podszywania się pod inną osobę poprzez publikowanie

fałszywie podpisanego klucza publicznego. Inaczej mówiąc zminimalizuje to prawdopodobieństwo umieszczenia w bazach danych programu PGP Keyserver klucza opatrzonego danymi innymi niż rzeczywistego właściciela klucza.

W celu ograniczenia rozmiaru oraz poprawienia czytelności informacji o kluczach umieszczonych w bazach danych programu PGP Keyserver można uaktywnić opcję usuwania niedozwolonych sygnatur oraz zdjęć użytkowników. Sygnatury, które mogą pozostać po umieszczeniu klucza na serwerze definiuje lista na ekranie „Policy" o nazwie „Allowed Key Signatures". Ze względu na wymagania związane z opisaną w punkcie 3 strukturą potwierdzania kluczy należy do tej listy dodać sygnaturę kluczy głównego administratora PGP. W wyniku uruchomienia wyżej opisanego ograniczenia kasowane będą informacje o potwierdzeniach (podpisach) klucza innych niż potwierdzenie głównego administratora PGP.

Na ekranie „Replication" serwera nadrzędnego w polu „Hosts to Replicate Database to" należy wpisać adres IP serwera podrzędnego. Ustawienie tego parametru wypromuje serwer, na którym dokonano wpisu do roli nadrzędnego i wskaże serwer, z którym replikowana będzie baza kluczy (serwer podrzędny).

Do monitorowania i sprawdzania wpisów w logach dostępu do serwera oraz przebiegu procesów replikacji służą opcje na ekranie „Server Control". Z tego miejsca można również dokonać restartu usług Keyserver i Replication Engine.

Ekran „Directory Search" służy do przeszukiwania bazy kluczy podczas korzystania z narzędzia Web Console. Opcje na ekranie umożliwiają definiowanie reguł wyszukiwania kluczy, np. ze względu na nazwisko właściciela klucza.

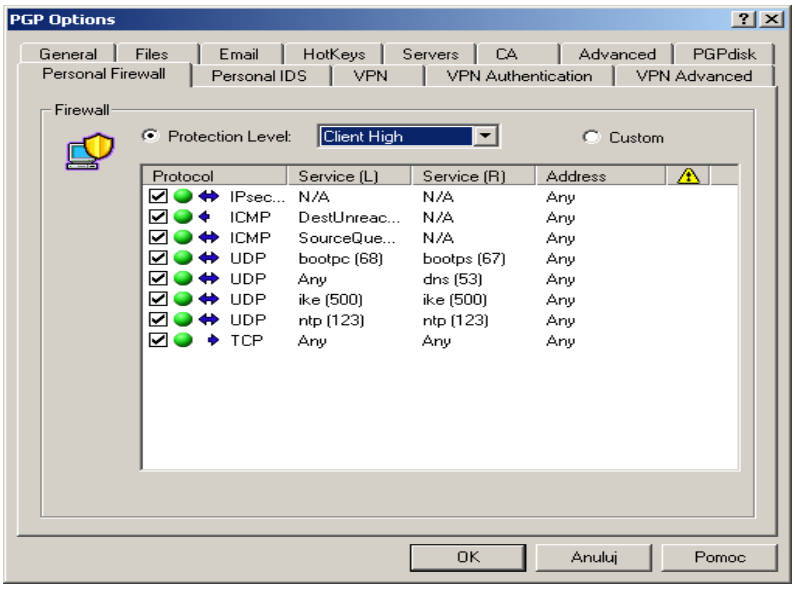
Korzystając z opcji ekranu „Add Keys" można dodać do serwera nowe klucze. W tym celu należy zaznaczyć klucz w programie PGP Keys, skopiować go do schowka i wkleić w obszarze nad przyciskiem „Add" w widoku „Add Keys", po czym przycisnąć przycisk „Add".

Zawartość bazy kluczy należy cyklicznie archiwizować. Częstotliwość archiwizacji powinna być większa w fazie wdrażania systemu dystrybucji kluczy, czyli w czasie, kiedy zmiany zawartości bazy kluczy szybsze niż w okresie ustabilizowanej pracy systemu dystrybucji kluczy. W późniejszym okresie proces ten powinien być powtarzany w odstępach zależnych od dynamiki zmian informacji w bazie nadrzędnego serwera kluczy. Archiwizacje można wykonać wykorzystując program PGP Export (instalowany razem z programem PGP Keyserver) lub poprzez kopiowanie w bezpieczne miejsce zawartości katalogu Data programu PGP Keyserver (domyślna ścieżka dostępu to C:\Program Files\Network Associates\PGP Keyserver).

5. Oprogramowanie instalowane na stacji roboczej użytkownika

Aby każdy użytkownik mógł szyfrować i podpisywać wiadomości pocztowe należy zainstalować na jego stacji roboczej oprogramowanie PGP Desktop Security. Gdy program ten jest instalowany w środowisku Windows NT Server 4.0 minimalne wymagania sprzętowe to: procesor Intel Pentium 166 MHz, 64 MB pamięci operacyjnej i 32 MB wolnego miejsca na dysku twardym. Aby umożliwić szyfrowanie, deszyfrowanie oraz podpisywanie wiadomości poczty elektronicznej należy zainstalować komponent PGP Mail & PGP File. Razem z PGP Mail & PGP File instalowany jest również moduł służący do zarządzania kluczami na stacji klienckiej. Ułatwia ono zarządzanie lokalnie przechowywanymi kluczami, generowanie własnej pary kluczy, importowanie i exportowanie kluczy z lub do serwera kluczy.

Program można zintegrować z aplikacjami pocztowymi Microsoft Outlook, Outlook Express lub Lotus Notes. Po zainstalowaniu oprogramowania na pasku narzędzi wymienionych aplikacji pojawią się dwie dodatkowe ikony służące do wywołania szyfrowania wiadomości oraz dołączania elektronicznego podpisu.



Rys. 6. Ustawienia filtrów pakietów dla poziomu ochrony Client High

Oprogramowanie PGP dostarcza funkcji zaawansowanej ochrony informacji przechowywanych na stacji roboczej. Aby uaktywnić te funkcje należy zainstalować dodatkowo PGP Disk i PGP Distributed Firewall (moduły te zostały już opisane przy okazji charakteryzowania składników pakietu PGP Corporate Desktop Suite). Jednym z zabezpieczeń informacji przechowywanej na stacji roboczej jest ograniczenie dostępu z sieci poprzez ustawienie reguł filtrowania pakietów. PGP Distributed Firewall proponuje jeden z kilku standardowo wbudowanych konfiguracji zabezpieczeń (konfiguracje te różnią się restrykcjami nakładanymi na ruch pakietów wchodzących i wychodzących). Istnieje również możliwość ustawienia ochrony według własnych kryteriów. Standardowe ustawienia konfiguracyjne dla wbudowanego poziomu Client High (najwyższy stopień zabezpieczeń) przedstawia rys. 6.

6. Program PGPadmin i konfiguracja szablonu instalacyjnego

Aby uprościć, ujednolicić i przyspieszyć instalacje oprogramowania PGP na stacjach użytkowników należy wykorzystać możliwości kolejnego produktu z rodziny PGP – PGPadmin. Wchodzi on skład pakietu rozprowadzanego pod nazwą PGP Corporate Desktop Suite. Program PGPadmin można zainstalować na dowolnym komputerze, na którym wcześniej zostało zainstalowanie oprogramowanie PGP Desktop Security. Przy pomocy programu PGPadmin można stworzyć szablon instalacyjny, czyli wygenerować nowy instalator oprogramowania PGP. Korzystając przy instalacji PGP z wygenerowanego szablonu otrzymuje się od razu skonfigurowaną odpowiednio aplikację. Użycie szablonu instalacyjnego oprogramowania PGP daje możliwość zabezpieczenia pewnych ustawień przed ingerencją w nie użytkownika, w ten sposób pewne reguły zgodne z przyjętą polityką bezpieczeństwa poczty elektronicznej będą wstępnie wymuszane.

Można tak skonfigurować szablon instalacyjny, aby zainstalowane przy jego pomocy oprogramowanie PGP charakteryzowało się pewnymi właściwościami np.: domyślnie zawsze proponowało szyfrowanie poczty elektronicznej. Zaś wiadomość będzie szyfrowana z użyciem kluczy wskazanych przez użytkownika oraz klucza korporacyjnego. Pozwoli to na odszyfrowanie wiadomości użytkownikom posiadającym prywatny klucz korporacyjny. Publiczny klucz korporacyjny może być zawarty w szablonie instalacyjnym. Więc będzie dostępny na stacji roboczej użytkownika zaraz po zainstalowaniu programu

W szablonie instalacyjnym można również skonfigurować opcje dotyczące ochrony stacji roboczej.

Szablony instalacyjne powinny być udostępnione wszystkim administratorom stacji roboczych użytkowników, którzy powinni stosować się do pewnych, ustalonych reguł szyfrowania poczty. PGPadmin umożliwia również tworzenie plików konfiguracyjnych służących do aktualizowania ustawień PGP na stacjach roboczych.

Aby stworzyć szablon instalacyjny należy uruchomić program PGPadmin i wybrać przycisk „PGP Options", a następnie ustawić opcje zgodnie z ustalonymi wcześniej wytycznymi zgodnymi z polityką bezpieczeństwa. Ustawienia dotyczące dodatkowych kluczy PGP, ograniczeń dotyczących hasła i typów kluczy użytkowników oraz instalowanych komponentów oprogramowania PGP można skonfigurować po wyjściu z ustawień „PGP Options" i otworzeniu „Administrative Options". W „Administrative Options" znajduje się również zakładka „Access", na której można zablokować poszczególne ustawienia przed ingerencją użytkowników stacji roboczych. Tak więc szablon można skonfigurować w ten sposób, iż część ustawień będzie miała charakter domyślny (możliwość zmiany po zainstalowaniu oprogramowania PGP z szablonu instalacyjnego), zaś części ustawień użytkownik nie będzie mógł zmienić. Wszystkie istotne ustawienia dotyczące konfiguracji oprogramowania PGP na stacjach roboczych zostały opisane poniżej.

Tworząc szablon instalacyjny można wybrać:

- Instalacje elementów oprogramowania odpowiedzialnego za integrację z programem Microsoft Outlook lub Lotus Notes. Ułatwi to obsługę szyfrowania, deszyfrowania i podpisywania wiadomości pocztowych osobom korzystającym z programu Microsoft Outlook (ustawienie dotyczy również programu Outlook Express) lub Lotus Notes.
- Domyślne uruchamianie PGP/MIME przy wysyłaniu poczty. Opcja ta wymusza domyślne szyfrowanie załączników.
- Domyślne szyfrowanie poczty. Ustawienie to powoduje wyświetlenie komunikatu ostrzegawczego w trakcie każdej próby wysłania niezaszyfrowanej wiadomości pocztowej. Wymaga potwierdzenia jeśli wiadomość ma zostać wysłana w formie jawnej.
- Dostarczenie użytkownikowi w trakcie instalacji oprogramowania na stacji roboczej publicznego klucza korporacyjnego.
- Zaznaczenie publicznego klucza korporacyjnego jako obowiązkowego klucza do szyfrowania poczty. Ustawienie to wymusi szyfrowanie każdej wiadomości kluczem publicznym adresata oraz publicznym kluczem korporacyjnym, co umożliwi osobom uprawnionym odszyfrowanie wiadomości.

- Uaktywnienie skrótów klawiszowych przyspieszające wykonywanie operacji szyfrowania, składania podpisu elektronicznego i deszyfrowania wiadomości.
- Uaktywnienie restrykcji dotyczących długości hasła użytkownika.
- Opcje zezwalające lub nie na generowanie kluczy przez użytkowników.
- Okres ważności generowanych kluczy.
- Domyślną (lub obligatoryjną) metodę szyfrowania oraz długość klucza.
- Zabezpieczenia stacji roboczej, na której zostanie wykonana instalacja oprogramowania PGP z szablonu instalacyjnego.

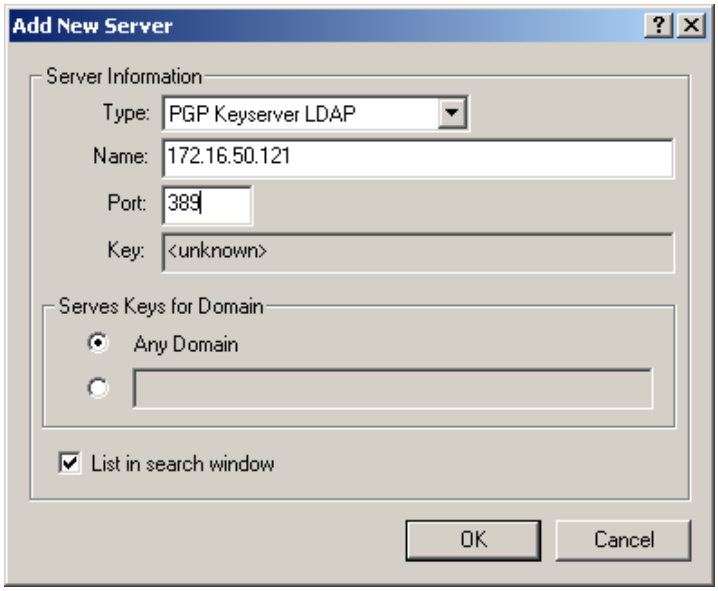
7. Generowanie nowej pary kluczy

Nową parę kluczy generuje się używając program PGPkeys, który służy do zarządzania lokalnym zbiorem kluczy, tworzenia własnej pary kluczy, importowania i eksportowania kluczy z lub do serwera kluczy.

Aby stworzyć nowa parę kluczy należy uruchomić program PGPkeys i z menu Keys wybrać opcję New Keys. Uruchomiony program instalacyjny poprowadzi użytkownika poprzez procedurę tworzenia kluczy. Najważniejszymi danymi są nazwa użytkownika, z którą będą identyfikowane nowe klucze, oraz hasło, którym będzie zabezpieczony klucz prywatny. Jeżeli wprowadzone hasło będzie miało mniej niż 8 znaków, program wyświetli ostrzeżenie na temat zalecanej długości hasła. Po wprowadzeniu tych informacji pojawi się komunikat o poprawnym wygenerowaniu nowych kluczy, które będą widoczne w głównym oknie programu PGPkeys.

8. Wysyłanie kluczy do bazy kluczy programu PGP Keyserver

Wysyłanie kluczy do bazy kluczy programu PGP Keysever najłatwiej wykonać wykorzystując program PGPkeys. Aby wysłać klucz do serwera kluczy należy uruchomić program PGPkeys, wskazać klucz, który ma być wysłany i z menu Server wybrać opcję Send to, oraz wskazać serwer kluczy, na który ma zostać wysłany klucz. Umieszczenie klucza na serwerze potwierdzone zostanie odpowiednim komunikatem na ekranie monitora.



Rys. 8. Ekran konfiguracyjny dodawanego serwera kluczy

Jeżeli na liście dostępnych serwerów nie ma właściwego serwera należy w dowolnym programie PGP np. PGPkeys otworzyć z menu Edit ekran Opions. Na zakładce Servers wybrać przycisk New i wypełnić pola ekranu pokazanego na rys. 8. Należy wpisać nazwę lub adres IP komputera, na którym zainstalowany jest PGP Keyserver oraz port obsługujący komunikację z tym programem.

Po zatwierdzeniu wprowadzonych danych dodany serwer powinien być widoczny na zakładce Servers i powinna również być możliwość komunikowania się z nim za pomocą innych aplikacji PGP.

9. Podsumowanie

W opracowaniu został przedstawiony problem dystrybucji kluczy publicznych, które wykorzystywane są w szyfrowaniu informacji metodami asymetrycznymi. Przedstawiony został mechanizm potwierdzania kluczy publicznych w celu zapewnienia autentyczności kluczy wymienianych bez bezpośredniego kontaktu zainteresowanych stron. Przedstawiono przykładowe możliwości aplikacji PGP Keyserver, która służy do przechowywania kluczy publicznych i zarządzania nimi. W opracowaniu zawarto przykładowe elementy konfiguracji tego oprogramowania, które zapewnią wyegzekwowanie

zaproponowanych zaleceń organizacyjnych. Uzupełnieniem informacji na temat tworzenia bezpiecznego systemu dystrybucji kluczy publicznych są opisy i wskazówki dotyczące działania i konfiguracji innych aplikacji spod znaku PGP czyli oprogramowania instalowanego u użytkowników PGP oraz wspomagającego administrację oprogramowaniem PGP. W artykule celowo pominięto oferowaną przez niektóre wersje oprogramowania PGP możliwość tworzenia wirtualnych sieci prywatnych (moduł PGP VPN w ramach PGP Net) ze względu na nieco inną metodę szyfrowania: szyfrowanie jest zawsze symetryczne z okresową negocjacją i wymianą kluczy szyfrowanymi asymetrycznie. PGP oferuje najbardziej dojrzałą formę użytkowego wykorzystania kryptografii asymetrycznej i wyznacza kierunek rozwoju oraz praktyczny standard w tej dziedzinie. Zapewnia skuteczną ochronę zarówno pojedynczych stacji roboczych, jak i rozproszonych sieci dużych firm.

Literatura:

[1] PGP Keyserver, Enterprise Edition, *Administrator's Guide*.

[2] PGP Desktop Security, *Administrator's Guide*.

[3] PGP Desktop Security, *User's Guide*.

[4] Klander L. *Hacker Proof czyli jak bronić się przed intruzami*, Mikom, Warszawa.

[5] Garfinkel S., Spafford G., *Bezpieczeństwo w Unixie i Internecie,* Wydawnictwo RM, Warszawa 1997

Recenzent: dr inż. Adam Patkowski

Praca wpłynęła do redakcji 20.05.2002