Realizacja usługi bezpiecznej wymiany informacji w sieci Internet w Polsce — stan bieżący

Maja Górecka
Maja.Gorecka@cc.uni.torun.pl

Tomasz Wolniewicz
twoln@mat.uni.torun.pl

NASK

1 Założenia

Projekt ma na celu uruchomienie systemu stanowiacego podstawę dla bezpiecznej wymiany informacji za pomocą udostępnienia bazy poświadczonych kluczy publicznych.

Zakłada się wykorzystanie funkcjonującej w Polsce bazy X.500, po odpowiednim jej przygotowaniu do wprowadzania certyfikatów kluczy publicznych w postaci zalecanej przez standardy PEM oraz PGP.

Projekt przewidywał utworzenie niezbędnego zestawu narzędzi służacych do dokonywania certyfikacji oraz wprowadzania danych do bazy X.500.

2 Składowe systemu

Zgodnie z zamierzeniami określonymi w naszym raporcie „Propozycja realizacji usługi bezpiecznej wymiany informacji w sieci Internet w Polsce" zostało ustalone, że wydawaniem poświadczeń zajmować sie będzie specjalnie w tym celu powołany Centralny Urząd Certyfikacyjny, zwany dalej CUC. Urząd ten będzie poświadczał klucze publiczne otrzymane ze wszystkich regionów Polski za pośrednictwem delegatur. Wbrew nazwie CUC nie będzie oczywiście urzędem państwowym. Trzeba od razu zaznaczyć, że CUC nie może ponosić odpowiedzialności prawnej za straty związane z błędami w obsłudze kluczy. Całe przedsięwzięcie musi być przygotowane tak, aby było jak najmniej wrażliwe na uszkodzenia i włamania, ale przyjęcie zasady, że CUC można pociągnąć do odpowiedzialności oznaczałoby konieczność podniesienia kosztów jego działania.

Drugim niezbędnym składnikiem są Delgatury CUC. W celu uproszczenia zarówno samego systemu, jak i drogi weryfikacji klucza przez użytkowników, ustalone zostało, że jedynym zadaniem Delegatur jest umożliwienie użytkownikom bezpośredniego kontaktu z Urzędem Certyfikacyjnym. Kontakt taki jest niezbędny przy pierwszej weryfikacji tożsamości użytkownika przez Urząd.

Trzecim składnikiem jest baza danych przechowująca certyfikaty. Jak już wspomniano, zakłada się, że wykorzystywany będzie wdrożony już system X.500. Dane muszą być wprowadzane przez odpowiedzialnych za nie administratorów. Tam, gdzie to możliwe należy uruchamiać Delegatury w powiązaniu z serwerami DSA, należy jednak pamiętać, że na Delegaturze spoczywa znacznie większa odpowiedzialność niż na administratorze DSA, gdyż podszycie się pod delegaturę umożliwia wstawianie do bazy fałszywych certyfikatów, podczas gdy włamanie na serwer może spowodować jedynie skasowanie danych, ale nie może w żadnym razie doprowadzić do wprowadzenia danych nieprawdziwych. Z tego powodu przy rozszerzaniu systemu X.500 konieczne będzie ograniczanie ilości Delegatur, a w konsekwencji stosowanie odpowiedniego systemu współpracy i rozliczeń pomiędzy Delegaturami i DSA.

3 Opis realizacji

W ramach realizacji projektu ustalono zasady wprowadzania do bazy X.500 danych związanych z bezpieczną wymianą informacji. Powstały programy służące do poświadczania dostarczonych przez użytkowników kluczy publicznych oraz narzędzia wspomagające umieszczenie tych danych w bazie X.500.

3.1 Postać danych bezpiecznej wymiany informacji w bazie X.500

W celu udostępnienia publicznie danych umożliwiających bezpieczną komunikację do bazy X.500 zostają wprowadzone następujące dane:

- klucz publiczny PGP w postaci tekstowej, poświadczony przez Centralny Urząd Certyfikacyjny (atrybut `pGPKey`),
- identyfikator klucza publicznego PGP (atrybut `pGPKeyID`),
- identyfikator użytkownika klucza publicznego PGP (atrybut `pGPUserId`),
- certyfikat w standardzie PEM (atrybut `userCertificate`).

Dopuszcza sie również umieszczenie w X.500 informacji dotyczącej odwołanego klucza PGP (na skutek jego zniszczenia lub zagubienia) w postaci atrybutu `pGPKeyRev`.

Certyfikaty PEM i PGP korzystają z różnych sposobów identyfikacji użytkownika. W PEM jest to Distingushed Name, w PGP przyjęto stosowanie adresu RFC-822. W typowym przypadku użytkownik powinien występować w bazie danych X.500 w ramach jakiejś instytucji, a zatem posiadać DN, dopuszcza się jednak udostępnianie usługi użytkownikom, którzy nie mogą być w naturalny sposób wprowadzeni do drzewa instytucji. W tym przypadku, użytkownikowi nadany zostanie DN bedący naturalną transformacją jego adresu e-mail. Na przykład `twoln@mat.uni.torun.pl` podlega transformacji na

`dc=pl@dc=torun@dc=uni@dc=mat@uid=twoln`.

3.2 Procedura generowania środowiska bezpiecznej wymiany informacji

3.2.1 Przygotowanie kluczy przez użytkownika

Użytkownik, zamierzający korzystać z usługi bezpiecznej wymiany informacji generuje samodzielnie niezbędne klucze, tj. klucz prywatny (*secret key*) oraz klucz publiczny (*public key*). W tym celu wykorzystuje program `pgp` (najnowsza wersja pakietu `pgp-2.6.3i` jest dostępna publicznie na platformy systemów UNIX i DOS).

Użytkownik następnie przekazuje Delegaturze Urzędu Certyfikacyjnego klucz publiczny (wyodrębniony za pomocą komendy `pgp -kxa`), poświadczając wobec niej swoją tożsamość.

Delegatura wcześniej zapewnia sobie warunki bezpiecznej wymiany komunikatów z CUC (poprzez wzajemne przekazanie publicznych kluczy PGP). Po uzyskaniu zlecenia od użytkownika przesyła do CUC, dane przeznaczone do certyfikacji. Dane te zawierają w pierwszej linii identyfikator użytkownika w bazie X.500, t.j. jego *Distinguished Name*, dalej umieszczony jest w postaci ASCII (armor) klucz publiczny.

3.2.2 Poświadczanie kluczy przez CUC

CUC po odebraniu zlecenia wydziela informację dotyczącą nazwy użytkownika i tekstową postać jego klucza publicznego. Z odebranego klucza publicznego usuwa wszelkie podpisy, a następnie sam dokonuje poświadczenia tego klucza.

Tak uzyskany klucz publiczny PGP jest informacją wejściową do przygotowanego w ramach realizacji projektu programu `pgp2cert`[1] generującego na jego podstawie certyfikat w systemie PEM. `pgp2cert` pobiera z klucza publicznego komponenty *modulus n* oraz *exponent e* i zapisuje jako certyfikat w formacie określonym w ramach standardów X.509 i PEM. Jednocześnie tworzona jest postać certyfikatu akceptowana przez bazę X.500, tzn. zgodna z syntaksem `Cetrificate`. Ma ona formę uzupełnień do bazy X.500 dotyczącących atrybutu `userCertificate`.

Następnie CUC produkuje na podstawie poświadczonego przez siebie klucza publicznego PGP plik mający format uzupełnień do bazy X.500 i gromadzący pary typu:

pGPKey=(postać „armor" klucza publicznego)
pGPKeyID=(identyfikator klucza)
pGPUserId=(identyfikator użytkownika klucza)

CUC łączy oba pliki zmian do X.500, wprowadza jako pierwszą linię identyfikator użytkownika w bazie X.500 (DN) i wysyła przygotowane dane za pośrednictwem bezpiecznej poczty elektoronicznej do odpowiedniego administratora lokalnego X.500.

3.2.3 Wprowadzenie danych do X.500

Administrator lokalny po odebraniu danych od CUC i potwierdzeniu ich wiarygodnosci dokonuje na ich podstawie modyfikacji bazy X.500. Wykorzystuje do tego celu przygotowany skrypt w języku Perl, automatycznie operujący na zawartości opisu obiektu.

Wykorzystywanie bazy X.500 do celów potwierdzania tożsamości wymaga odwoływania się do danych użytkownika (certyfikatu PGP) poprzez adres e-mail nadawcy. W typowej sytuacji adresat jest znany bazie X.500 poprzez identyfikator DN lokalizujący go w drzewie instytucji. Odszukanie nadawcy poprzez jego adres poczty elektronicznej wymagałoby zatem bardzo czasochłonnego przeszukania całej bazy w Polsce. Aby tego uniknąć równolegle z wprowadzaniem certyfikatów tworzy się strukturę wskaźników (aliasów) w ramach odrębnej podgałęzi drzewa informacji. Gałąź ta jest ustrukturalizowana zgodnie z domenową postacią Internetu, co pozwala na bardzo prostą transformację adresu e-mail na odpowieni DN w X.500. Odwołanie się do takiego aliasu powoduje odczytanie odpowiedniego hasła we właściwym drzewie X.500. Operacja rozwikłania aliasu i pojedynczego odczytu jest bardzo szybka i nie wymaga żadnych operacji przeszukiwania. Domenowa gałąź drzewa X.500 może być jednocześnie wykorzystana do umieszczania w niej użytkowników, których nie można zlokalizować w gałęzi instytucji.

[1]Program `pgp2cert` został napisany w oparciu o biblioteki pakietu SecuDE (Security Development Environment). Jest to oprogramowanie rozwijane przez niemiecką organizację GMD, jako zestaw narzędzi programowych wspomagających tworzenie poufnych systemów.

Z punktu widzenia użytkownika nie ma żadnej różnicy pomiędzy odwołaniem do aliasu czy do faktycznego hasła.

Tworzenie aliasu jest zautomatyzowane podobnie jak modyfikacja zawartości haseł. System w razie potrzeby tworzy również brakujące wyższe poziomy drzewa, o ile są one obsługiwane przez DSA wprowadzające dane. Przewiduje się, że w pierwszej fazie działania systemu aliasy będą przechowywane na centralnym serwerze i rozdystrybuowanie ich nastąpi dopiero po opracowaniu zasad, na jakich konkretne DSA będą miały nadzór nad odpowiednimi domenami.

4 Korzystanie z systemu

Pierwsza faza zakłada wykorzystywanie przez użytkowników standardowych wersji PGP oraz interfejsów poczty elektronicznej, które z PGP współpracują. Pobieranie kluczy z bazy X.500 następuje za pomocą pomostu do WWW. Pomost ten umożliwia wprowadzenia adresu e-mail i zwraca certyfikat PGP w postaci tekstowej. Certyfikat ten można następnie skopiować do pliku i wprowadzić do lokalnego zbioru kluczy PGP. Działanie systemu wymaga, aby klucz publiczny CUC był powszechnie znany. Powinien on być publikowany w szeregu archiwów, będzie również udostępniany przez pomost WWW.

W drugiej fazie przewiduje się modyfikację systemu PGP tak, aby zamiast lokalnego zbioru kluczy wykorzystywany był bezpośredni dostęp do bazy X.500, co znakomicie przyspieszy działanie systemu. Modyfikacje te w pierwszej kolejności powstaną dla PGP pracującego pod systemem UNIX.