X.500 JAKO ZAPLECZE BEZPIECZNYCH SYSTEMÓW WYMIANY INFORMACJI

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

Ogólnouczelniany Ośrodek Obliczeniowy

Tomasz Wolniewicz
twoln@mat.uni.torun.pl

Wydział Matematyki i Informatyki

Uniwersytet Mikołaja Kopernika, 87-100 Toruń, Chopina 12/18
oraz
JBR NASK

1 Wstęp

Popularność sieci komputerowych i rosnąca ilość ich użytkowników pociąga za sobą konieczność tworzenia zabezpieczeń systemów informatycznych.

Niniejszy artykuł przedstawia problemy związane z zapewnianiem bezpieczeństwa systemów i zasobów komputerowych oraz jest propozycją realizacji funkcji ochrony poprzez wykorzystanie standardów opracowanych w ramach międzynarodowej rekomendacji ITU-T X.509, p.t. *„The Directory: Authentication Framework”*. W szczególności uwydatniamy znaczenie rozproszonej bazy informacyjnej X.500 w gromadzeniu danych dotyczących zasobów sieciowych.

Omówiamy również podstawy rozwijających się obecnie systemów bezpiecznej transmisji danych PEM (*Privacy Enhancement for Internet Electronic Mail*) oraz PGP (*Pretty Good Privacy*) i wskazujemy na rolę jaką X.500 Directory powinno odegrać w konsolidowaniu tych systemów. W części 6 opisujemy konkretną implementację systemu PEM zintegrowaną z X.500 Directory. Implementacja ta została próbnie uruchomiona na UMK w Toruniu i będzie przedmiotem dalszych testów w najbliższej przyszłości.

Zwracamy uwagę na możliwość wykorzystania reguł, na których opiera się standard X.509 do bezpiecznej współpracy systemów komputerowych oraz ochrony ogólnodostępnych aplikacji, jak również prezentujemy mechanizmy stosowane do ochrony samej bazy X.500.

W rozdziale 7 zamieszczamy również propozycję zastosowania X.500 Directory do uruchomienia usługi bezpiecznej poczty elektronicznej w polskim środowisku sieciowym.

Tematyka związana z pojęciem X.500 Directory została przybliżona w naszych poprzednich pracach [1], [2], [3].

W artykule wykorzystujemy materiał zawarty w książce Davida Chadwicka p.t. „Understanding X.500 the Directory" [4], opieramy się również na dokumentacji pakietu SecuDE [8], RFC opisujących systemy PEM i PGP, książce Simsona Garfinkela p.t. „PGP — Pretty Good Privacy" [5] oraz dyskusjach prowadzonych na liście administratorów X.500.

W toruńskim archiwum X.500, pod adresem:

`ftp://ocelot.mat.uni.torun.pl/pub/isode/Polska/security.ps`

dostępne jest rozszerzone opracowanie na prezentowany temat, zawierające m.in. opis algorytmów kryptograficznych oraz szczegółowe omówienie zagadnień bezpieczeństwa związanych z bazą X.500.

2 Rodzaje zagrożeń w systemach komunikacyjnych i sposoby ochrony danych

Istotnym wymaganiem większości systemów eksploatowanych w środowisku sieciowym jest konieczność ochrony zasobów danych przed dostępem niepożądanych użytkowników.

Chroniona informacja może być różnego typu: bazy danych, zasoby informacyjne, usługi komputerowe, czy prywatne dane, korespondencja, kontrakty, umowy. Na ogół proste metody zabezpieczenia takich danych za pomocą hasła nie są wystarczające.

Bezpieczeństwo systemu leży w interesie zarówno użytkownika, który musi mieć pewność, że stosowana usługa jest wiarygodna, jak i dostawcy serwisu, chroniącego swój system przed nieuprzywilejowanym dostępem.

Podstawowe zagrożenia, z jakimi mamy do czynienia w systemach komunikacyjnych to:

- uzyskanie nieuprawnionego dostępu do danych przez „podsłuch" sieci,
- przechwycenie danych identyfikujących nadawcę czy odbiorcę komunikatu przez osobę trzecią w celu późniejszego wykorzystania,
- nieuprawnione rozpowszechnianie informacji, czyli umożliwienie dostępu do danych niepożądanym odbiorcom,
- nieuprawniona modyfikacja danych (zmiana, duplikacja, zniekształcenie),
- występowanie w imieniu innego użytkownika, „podszycie się" (*masquerade*) w celu uzyskania dostępu do zasobów danych czy zdobycia dodatkowych przywilejów,
- powtórzenie wcześniej przechwyconego komunikatu w dowolnej postaci (*replay*),
- odmówienie udziału w komunikacji lub jej części,
- zablokowanie wykonania określonej usługi czy operacji.

W celu zminimalizowania opisanych zagrożeń systemy bezpieczeństwa realizują następujące funkcje:

– identyfikacja tożsamości stron biorących udział w komunikacji,
– kontrola dostępu do zasobów,
– poufny transfer komunikatów w celu ochrony danych poprzez szyfrowanie przy użyciu technik kryptograficznych,
– kontrola integralności danych za pomocą podpisów cyfrowych,
– uniemożliwienie nieuzasadnionej odmowy komunikacji, weryfikacja tożsamości na podstawie podpisów cyfrowych.

Techniki bezpieczeństwa pozwalają na ochronę przesyłanych danych na dwa sposoby: przez ich zaszyfrowanie przed nadaniem, wówczas mamy do czynienia z poufną wymianą danych lub wyłącznie przez kontrolę spójności komunikatu, metoda ta gwarantuje, że informacja odebrana jest identyczna z nadaną.

3 Podstawy kryptografii wykorzystywane w publicznych systemach przesyłania danych

Podstawowym celem kryptografii jest przekształcenie informacji do postaci, która uniemożliwi niepowołanym osobom odtworzenie przesyłanej wiadomości.

Czasami stosuje się przekształcanie za pomocą funkcji nieodwracalnych. Ponieważ taka funkcja (w znaczeniu matematycznym) zastosowana do jakiegoś argumentu zawsze produkuje ten sam rezultat, funkcje nieodwracalne można stosować do sprawdzania czy informacja nie została zmieniona.

Innym zastosowaniem kryptografii jest szyfrowanie wiadomości za pomocą funkcji odwracalnej. Zastosowanie funkcji odwrotnej przywraca informację do postaci niezaszyfrowanej. Podstawowym problemem w takiej sytuacji jest to, że przy powszechnym stosowaniu krytpografii nie można stosować jednej pary funkcji. W tym celu wprowadza się do operacji szyfrowania dodatkowe argumenty — klucze. Rozróżnia się klucze szyfrujące i deszyfrujące, w przypadku, gdy klucze te są identyczne mamy do czynienia z algorytmem symetrycznym, w przeciwnym razie algorytm jest niesymetryczny.

3.1 Algorytmy symetryczne

Istotnym problemem wszelkich algorytmów symetrycznych jest wymaganie dotyczące współdzielenia z odbiorcą tajnego klucza, gdyż obaj partnerzy wymieniający poufne dane muszą dysponować tym samym kluczem. Ponadto w przypadku użytkowników odległych konieczna jest transmisja klucza przez sieć. Przesyłanie z kodowaniem symetrycznym stosuje metodę tworzenia niezależnych kluczy. Pierwszy, jednorazowy (*session key, data exchange key*) stosuje się dla potrzeb jednokrotnego przesłania danych, drugi (*interchange key*) jest stosowany do szyfrowania pierwszego. Pociąga to za sobą konieczność częstego tworzenia nowych kluczy, co wprowadza wiele trudności w zarządzaniu bazą takich zasobów.

Najpopularniejszym algorytmem symetrycznym jest DES — **Data Encription Standard**, opracowany przez Amerykańskie Biuro Standardów. Ten rodzaj szyfrowania jest bardzo efektywny (istnieją układy realizujące ten algorytm sprzętowo z szybkością nie wpływającą na transmisję danych). Inny standard (stosowany przez system PGP) to **International Data Encription Algorithm** — IDEA, opracowany w Szwajcarii. Obydwa standardy uważane są obecnie za bezpieczne.

3.2 Algorytmy asymetryczne

Wykorzystanie algorytmu niesymetrycznego powoduje, że każdy użytkownik dysponuje parą kluczy, jeden, zwany kluczem publicznym (*public*), jest ogólnie dostępny, drugi, prywatny (*private*), jest tajny, znany wyłącznie właścicielowi. Metoda ta zwana jest również systemem kryptografii kluczy publicznych (*Public-Key CryptoSystem* — PKCS). W klasie algorytmów asymetrycznych istnieją techniki kodowania **odwracalnego** (*reversible*) oraz **nieodwracalnego** (*irreversible*). Przy szyfrowaniu odwracalnym można zakodowaną informację odzyskać poprzez zastosowanie odpowiedniego klucza. Powszechnie stosowaną implementacją tej techniki jest algorytm RSA.

Kryptografia asymetryczna wykorzystuje bardzo skomplikowane algorytmy matematyczne, co znacznie obniża efektywność. Nie zaleca się stosowania tych technik do poufnego przesyłania komunikatów o dużych rozmiarach. Korzystniej jest zastosować algorytm symetryczny z jednorazowym kluczem, a za pomocą odwracalnej kryptografii asymetrycznej przesłać poufny klucz.

3.3 Podpisy cyfrowe

Algorytm kodowania asymetrycznego może również służyć do **kontroli tożsamości nadającego**. Obie strony, aby zostać uwiarygodnione muszą udowodnić posiadanie swojego tajnego klucza (*secret key*). Istotną cechą systemów kryptografii kluczy publicznych jest permutowalność (*permutability*), oznaczająca, że oba klucze mogą być stosowane zarówno do szyfrowania jak i deszyfrowania. Własność ta jest wykorzystywana w ramach identyfikacji i jest podstawą funkcjonowania podpisów cyfrowych (*digital signatures*).

Podpis cyfrowy powstaje poprzez poddanie przesyłanej informacji działaniu tzw. funkcji mieszającej (*hash-function*), następnie zaszyfrowanie przekształconej informacji za pomocą prywatnego klucza nadawcy. Podpis jest dołączany wraz ze wskazaniem zastosowanej funkcji mieszającej do komunikatu (który sam może, ale nie musi, być zaszyfrowaną wcześniej wiadomością).

Prawdziwość otrzymanego komunikatu, zaopatrzonego w podpis cyfrowy jest uwiarygadniana przez adresata, który stosuje do deszyfrowania klucz publiczny nadawcy. Należy zwrócić uwagę, że w ten sposób realizowane może być uwiarygodnienie autora komunikatu i faktu autentyczności treści wiadomości, to czy wiadomość sama jest zaszyfrowana, czy nie zależy wyłącznie od decyzji nadającego.

3.4 Certyfikaty

Jednym z podstawowych problemów stosowania szyfrów jest dystrybucja kluczy. Szyfrowanie oparte o klucze publiczne pozwala wprawdzie na publiczne ogłaszanie kluczy, ale problemem staje się zapewnienie prawdziwości informacji o tym, że dany klucz należy do danej osoby. Ponieważ klucze są jednocześnie stosowane jako metoda uwierzytelniania tożsamości, problem ich autentyczności staje się podwójnie ważny.

Rozwiązaniem jest stosowanie kluczy podpisanych cyfrowo przez zaufane osoby lub instytucje. Tak potwierdzone klucze nazywa się certyfikatami. Różne systemy mogą stosować własne metody wykorzystywania mechanizmu poświadczania kluczy, w następnej części podamy dwa takie przykłady, zasada pozostaje jednak niezmienna — podpis zaufanej osoby czy instytucji pozwala mieć pewność, że nikt niepowołany nie podsuwa nam falsyfikatu.

4 Zarządzanie kluczami publicznymi

W obecnej chwili funkcjonują dwa najważniejsze systemy uwierzytelniania i szyfrowania poczty elektronicznej — Pretty Good Privacy (PGP) oraz Privacy Enhanced Mail (PEM). Obydwa wykorzystują zbliżone mechanizmy zapewnienia ochrony danych, różnica polega na stosowanym przez nie symetrycznym algorytmie szyfrującym oraz, co ważniejsze, sposobie uwierzytelniania kluczy publicznych.

4.1 PGP

PGP jest systemem powstałym w typowo „internetowy" sposób — zbudowano system, który następnie w trakcie eksploatacji dociera się, jest zmieniany, aż wreszcie awansuje do roli standardu. System ten służy do bezpiecznego przesyłania poczty oraz do szyfrowania zbiorów na dyskach i zawiera cały zestaw narzędzi do generowania kluczy, wysyłania i czytania poczty, poświadczania kluczy, tworzenia własnej bazy kluczy itp. Nas interesuje wyłącznie przyjęta w PGP metoda zarządzania kluczami.

W opisywanym systemie każdy użytkownik pracuje w oparciu w własną bazę kluczy (*keyring*). Baza taka zawiera klucze osób, z którymi wymieniana jest korespondencja. W sytuacji, kiedy konieczne jest rozszerzenie bazy robi się to albo w oparciu o klucz otrzymany bez żadnych potwierdzeń (wierząc, że przekłamanie w trakcie transmisji jest mało prawdopodobne), albo otrzymuje się certyfikat poświadczony przez osobę, której klucz już mamy i jednocześnie mamy zaufanie, że nie potwierdzi ona fałszywej informacji.

Zaletą PGP jest jego całkowita niezależność od struktur administracyjnych, wadą — konieczność polegania na własnej ocenie prawdomówności innych osób oraz prawdopodobne kłopoty z otrzymaniem poświadczonych kluczy osób, których bezpośrednio nie znamy.

Aby ułatwić dystrybucję kluczy uruchomiono szereg serwerów kluczy PGP pozwalających na przeszukiwanie bazy danych i pobieranie kluczy, problemy z ich poświadczeniem nadal jednak pozostają.

Podsumowując, można ocenić, że o ile PGP jest systemem o dużym stopniu pewności i nadaje się do bezpiecznej komunikacji pomiedzy osobami, to nie można by go uznać za wystarczający w sytuacjach związanych z obrotem finansowym pomiędzy nie znającymi się partnerami.

4.2 PEM

PEM, w przeciwieństwie do PGP wyrósł jako standard (RFC1421–4), na którym bazują konkretne implementacje. Sam standard opisuje mechanizmy związane z szyfrowaniem i podpisywaniem poczty, jak również bardzo dokładnie określa strukturę organizacyjną związaną z administrowaniem kluczami.

W zakresie administracyjnym PEM bazuje na zaleceniach standardu X.509, definiującego strukturę bezpieczeństwa na użytek dostępu do X.500 Directory i innych aplikacji OSI.

Certyfikat w rozumieniu X.509, to klucz publiczny użytkownika poświadczony przez powołane specjalne urzędy wydające świadectwa (*Certification Authorities* — CA). **Urzędy certyfikacyjne** tworzą certyfikaty z upoważnienia i w imieniu użytkowników. Urząd certyfikacyjny musi być w stanie zapewnić wysoki stopień poufności działania i musi być absolutnie wiarygodny. Z tego powodu przewiduje się funkcjonowanie sieci urzędów certyfikacyjnych w ramach administracji państwowej (i z tego dokładnie powodu nie należy oczekiwać szybkiego wprowadzenia tego systemu w życie).

Certyfikat X.509 składa się z:
- nazwy urzędu wystawiającego świadectwo,
- nazwy użytkownika, do którego certyfikat należy,
- publicznego klucza użytkownika,
- identyfikatora algorytmu stosowanego do generowania podpisu oraz związanych z nim parametrów,
- czasu ważności certyfikatu,
- numeru seryjnego,
- wersji X.500 (obecnie zawsze 0).

Cała powyższa informacja jest potwierdzona podpisem cyfrowym urzędu certyfikacyjnego.

Znając klucz publiczny urzędu poświadczającego, który jest odpowiedzialny za określonego użytkownika można dokonać weryfikacji poprawności certyfikatu klucza publicznego użytkownika.

Jeżeli kontaktujące się strony mają wspólnego wystawcę certyfikatu, to obie znają klucz publiczny poświadczającego, a więc może być realizowana wymiana informacji uwiarygodnionej podpisami. W przypadku, gdy mamy do czynienia z duża ilością partnerów w poufnym systemie nie wystarcza jedna organizacja uprawniona do tworzenia certyfikatów. Wówczas klucz publiczny jednego urzędu CA musi otrzymać certyfikat wydany przez inny urząd poświadczający. W ten sposób tworzone są skomplikowane struktury drzewiaste lub sieciowe zawierające opisy ścieżek (*certification path*), jakie musi przebyć certyfikat, aby został uwierzytelniony. Jeżeli urzędy certifikacyjne obu stron znajdują się w jednym drzewie, to możliwa jest weryfikacja podpisu użytkownika, poprzez kolejne weryfikowanie podpisów urzędów coraz wyższych szczebli, aż do osiągnięcia szczebla najwyższego. Podpis urzędu centralnego musi być powszechnie znany.

W szczególnych przypadkach, gdy np. wiadomo, że użytkownicy znajdujący się pod opieką dwóch urzędów certyfikacyjnych często się komunikują, można na podstawie dwustronnego uzgodnienia pomiędzy tymi urzędami ustalić certyfikat wzajemny (*cross certificate*), będący parą certyfikatów (np. klucz publiczny urzędu A poświadczony przez urząd B oraz klucz publiczny urzędu B poświadczony przez urząd A). Metoda ta musi być również stosowana w przypadkach komunikacji pomiędzy stronami nie posiadającymi urzędów certyfikujących formalnie umieszczonych w jednym drzewie.

Do poprawnego funkcjonowania mechanizmu potwierdzania tożsamości niezbędne jest utrzymywanie aktualnych **list unieważnionych certyfikatów** (*revocation lists*). Są to zestawy certyfikatów odwołanych, z różnych powodów, przed upływem ich terminu ważności. Gdyby nie brać pod uwagę możliwości kradzieży kluczy, to można określić pewny system komunikacji pomiędzy nie znającymi się partnerami, wystarczy, że jeden z nich przyśle drugiemu komplet certyfikatów (od swojego aż do szczytu drzewa). Niestety spójność takiej ścieżki nie daje gwarancji, że jej fragment nie został zmodyfikowany przez fałszerza będącego w posiadaniu skradzionego klucza. Pewność da dopiero skonfrontowanie wszystkich kolejnych certyfikatów z listami certyfikatów unieważnionych (oczywiście pod warunkiem, że fakt kradzieży klucza został uświadomiony).

5 Baza X.500 jako miejsce przechowywania kluczy

Oczywiste jest, że stosowanie na szeroką skalę kryptografii w przesyłaniu danych wymaga ogromnych, ogólnodostępnych baz zawierających klucze publiczne. X.500 jest bazą, która może się do tego bardzo dobrze nadawać. Dostosowanie X.500 do systemu używanego przez PEM wynika z faktu, ze X.509 jest fragmentem standardu X.500; przechowywanie kluczy na użytek PGP jest również możliwe i aktualnie prowadzone są prace przygotowawcze mające doprowadzić do zdefiniowania odpowiednich atrybutów.

X.500 użyte do celów kryptografii publicznej spełnia równocześnie dwa zadania:

– jest systemem zapewniającym jednorodne nazewnictwo osób i obiektów, którym można przyporzadkowywać klucze identyfikacyjne,
– przechowuje certyfikaty w postaci odpowiednich atrybutów obiektów.

Istnienie ogólnodostępnej bazy certyfikatów umożliwia stosowanie automatyczych metod poświadczania tożsamości.

Stosowanie systemu PEM (i w ogóle metod poświadczania tożsamości) może wprowadzać znaczne opóźnienia systemowe w sytuacjach, kiedy trzeba kontrolować długie ścieżki poświadczeń ulokowane w odległych fragmentach drzewa informacji X.500. Aby temu zapobiec standard proponuje wprowadzanie optymalizacji (lokalne buforowanie informacji, stosowanie certyfikatów pośrednich). W ramach projektu PASSWORD opracowano system przeglądający drzewo informacji i zbierający z niego dane o urzędzach certyfikacyjnych. Zebrane dane służą następnie do utworzenia lokalnej struktury odwzorowującej system ścieżek poświadczeń. System taki zapewnia znaczne przyspieszenie poświadczeń, wprowadzajac niewielkie niebezpieczeństwo w postaci możliwości manipulowania lokalną informacją. Szczegóły systemu opisano w opracowaniu [7].

6 Pakiet SecuDE jako implementacja kontroli bezpieczeństwa systemów informacyjnych

Oprogramowane o nazwie SecuDE (Security Development Environment) jest rozwijane przez niemiecką organizację GMD (Gesellschaft für Mathematik und Datenverbereitung) jako zestaw narzędzi programowych wspomagających tworzenie poufnych systemów. Początkowo sponsorem projectu *SecuDE* była narodowa organizacja sieci komputerowych — DFN (Deutsches Forschungsnetz).

Dystrybucja SecuDE zawiera pakiet kryptograficzny DES oraz oprogramowanie implementujące algorytmy kodujące MD2, MD4, MD5, pochodzące z RSA Data Security Inc.

Obecnie, wersja SecuDE opiera się na technologiach pochodzących z pakietu ISODE (ICR1.1v3), m.in. w celu implementacji funkcji translacji formatu ASN.1.

Oprogramowanie SecuDE może zosać zainstalowane na systemach SunOS 4.1.x, Solaris 2.x, HP-UX, OSF1, IRIX, Linux, NetBSD, SCO Unix jak również w systemie MS-DOS, a w trakcie opracowywania są wersje na IBM OS/2 i Microsoft Windows NT/95.

Na kwiecień 1996 zapowiadana jest edycja SecuDE-5.0, która będzie dystrybuowana w dwóch wersjach: jako „public domain" oraz komercyjnie. Pakiet komercyjny będzie zawierał dodatkowo podręczniki instalacyjne, szczegółową dokumentację, GSS-API (Generic Security Service Application Program Interface), biblioteki DLL oraz nowe interfejsy użytkowe.

6.1 Opis funkcjonalny pakietu

Pakiet SecuDE oferuje zestaw programów oraz funkcji bibliotecznych, przeznaczonych do tworzenia aplikacji ukierunkowanych na zapewnienie bezpieczeństwa komunikacji. W jego skład wchodzą:

- podstawowe funkcje kryptograficzne implementujące algorytmy RSA, DES, funkcje mieszające itp.,
- funkcje zabezpieczające realizujące identyfikację użytkowników, spójność danych, poufność przesyłanych komunikatów na podstawie podpisów cyfrowych oraz kryptografii symetrycznej i asymetrycznej,
- funkcje poświadczania (certyfikacji), zrealizowane według standardu X.509, obsługujące ścieżki certyfikacji, certyfikaty wzajemne oraz listy unieważnionych certyfikatów,
- programy i funkcje zarządzające urzędami certyfikacyjnymi oraz zapewniające współpracę między tymi urzędami a użytkownikiem, którego tożsamość jest poświadczana,
- programy służące do tworzenia podpisów cyfrowych, weryfikacji, kodowania i dekodowania,
- implementację systemu PEM według RFC1421–4,
- metody przetwarzania list odwołanych certyfikatów zgodne z definicją zawartą w RFC1422,
- obsługa bezpiecznego dostępu do danych w ramach X.500 Directory, gromadzenie w ramach bazy X.500 informacji związanych z bezpieczeństwem, realizacja silnie poświadczanych operacji pomiędzy interfejsem użytkowym i serwerem oraz pomiędzy serwerami X.500 (w oparciu o pakiet ICR1.1v3),
- zarządzanie danymi dotyczącymi użytkowników w prywatnym otoczeniu PSE (*Private Security Environment*), dostęp do środowiska PSE jest realizowany za pomocą specjalnego identyfikatora zwanego PIN (*Personal Identification Number*).

6.2 Bezpieczna poczta elektroniczna PEM w pakiecie SecuDE

SecuDE dostarcza filtry transformujące dowolne zbiory wejściowe do formatu PEM i odwrotnie. Narzędzia te mogą zostać zintegrowane z interfejsami poczty elektronicznej (np. *MH*, *elm*), czy programami administrującymi urzędami certyfikacyjnymi CA.

SecuDE realizuje wszystkie formaty zdefiniowane w RFC1421–4, ale implementuje wyłącznie zarządzanie kluczami według kryptografii asymetrycznej. Udostępnia określone w RFC1424 metody certyfikacji oraz administrowania listami odwołanych certyfikatów CRL. Dodatkowo, jest to rozszerzenie w stosunku do definicji standardu, SecuDE-PEM może zostać tak skonfigurowany, aby współpracował z X.500-DUA w celu m.in. automatycznego wyszukiwania certyfikatów, czy list odwołań w bazie danych.

6.3 Integracja SecuDE z X.500

Jedną z istotniejszych cech pakietu jest możliwość wykorzystywania go w połączeniu z X.500 Directory.

Pakiet SecuDE dopuszcza konfigurację na jeden z trzech sposobów:

- Bez możliwości współpracy z X.500.
- Jako zintegrowany z X.500-DUA, przy czym dostęp do X.500 następuje poprzez proste poświadczanie oraz niechronione operacje typu DAP; w tej sytuacji konieczne jest udostępnienie w trakcie kompilacji bibliotek ISODE.
- Jako zintegrowany z X.500-DUA z dostępem na zasadzie silnego poświadczania oraz możliwością poświadczania (*sign*) operacji DAP; SecuDE używa w tym celu zmodyfikowanej wersji oprogramowania QUIPU, dystrybuowanego przez GMD.

  Wersja QUIPU zawierająca rozserzenia związane z bezpieczeństwem systemu umożliwia również instalację tzw. bezpiecznych serwerów DSA.

7 Propozycja realizacji usługi bezpiecznej poczty elektronicznej dla potrzeb polskiego Internetu

7.1 Cel

W bieżącym rozdziale przedstawiamy propozycję realizacji usługi bezpiecznej poczty elektronicznej dla potrzeb polskich użytkowników sieci Internet. Usługa ta ma z jednej strony dawać możliwość wygodnego dostępu do bazy kluczy publicznych korespondentów, z drugiej zapewniać pełną wiarygodność uzyskiwanych danych.

7.2 Wymagania

Usługa bezpiecznej poczty elektronicznej musi bazować na ogólnie obowiązujących standardach: X.509 – *The Directory, Authentication Framework* oraz PEM (*Privacy Enhancement Mail*). Przewiduje się również wykorzystanie „internetowego" standardu PGP (*Pretty Good Privacy*). W celu umożliwienia szybkiej realizacji zadania należy wykorzystać dostępne w ramach oprogramowania *„public domain"* pakiety, takie jak PGP, czy SecuDE. Wskazane jest powiązanie bazy kluczy publicznych z rozproszoną bazą danych, oferowaną środowisku sieciowemu Polski poprzez usługę X.500.

W sytuacji, kiedy dostępne są narzędzia programowe, jedynym prawdziwym problemem przy wprowadzaniu bezpiecznej wymiany informacji jest zapewnienie dostępu do kluczy publicznych. Powszechna dystrybucja klucza poświadczającego umożliwia prostą weryfikację faktu, że certyfikat nie został zmieniony.

Użytkownik otrzymujący certyfikat musi mieć jednak absolutną pewność, że opisuje on osobę, która jest wymieniona jako właściciel. Pewność taką można uzyskać wyłącznie poprzez bezpośrednią weryfikację danych osoby zgłaszającej swój akces do systemu, przy jednoczesnym, całkowitym zaufaniu do jednostki przyjmującej i potwierdzającej dane. Jest to zatem zagadnienie bardziej natury organizacyjnej niż implementacyjnej.

Przewiduje się oferowanie usługi na dwóch poziomach:

1. potwierdzenie danych (utworzenie certyfikatu) i umieszczenie ich w bazie danych,
2. dodatkowe dostarczenie odpowiednio skonfigurowanych narzędzi do obsługi poczty.

Jest całkiem prawdopodobne, że część użytkowników stosuje już bezpieczną wymianę korespondencji i jest zainteresowana jedynie dystrybucją kluczy.

Przyjmuje się założenie, że każdy użytkownik umieszczający swoje dane w bazie jest zainteresowany jak najszerszym do nich dostępem. W sytuacji funkcjonowania w Polsce publicznej usługi X.500 najwłaściwsze wydaje się umieszczanie danych w tej właśnie bazie, w przeciwnym wypadku użytkownicy próbujący odszukać certyfikaty nie będą mieli pewności do jakich zasobów sięgać.

7.3 Założenia

Zgodnie z zaleceniami standardów X.509 oraz PEM planuje się funkcjonowanie dla potrzeb zarządzania kluczmi publicznymi jednostek zwanych urzędami poświadczającymi (CA — *Cetification Authority*). Zadaniem CA jest wystawianie certyfikatów kluczy publicznych użytkowników oraz administrowanie bazą danych certyfikatów. W gestii CA jest również unieważnianie kluczy publicznych, które zostały zagubione, zagrożone, itp.

7.4 Problemy

Główne problemy pełnej realizacji bezpiecznej poczty elektronicznej dotyczą zapewnienia odporności systemu na próby narażenia na wprowadzenie nieprawdziwych danych, czy na dostęp nieodpowiedzialnych osób do tajnych informacji przy jednoczesnym szerokim dostępie do bazy danych.

Istotną sprawą jest konieczność zapewnienia wiarygodności danych przesyłanych do certyfikacji, wiążąca się z potrzebą osobistego poświadczenia tożsamości przed „zaufaną” jednostką. W przypadku dużej ilości użytkowników oznacza to, że należy utworzyć rozbudowaną sieć urzędów certyfikujących, odpowiedzialnych za poświadczanie kluczy publicznych określonych grup użytkowników. Ponieważ każdy urząd posiada swój klucz publiczny, niezbędne jest wówczas zapewnienie dostępu do bazy kluczy publicznych CA, bądź umieszczenie informacji dotyczącej tych kluczy w rozproszonej bazie X.500. Taka realizacja wymaga funkcjonowania skomplikowanych algorytmów wyszukiwania odpowiednich danych, konieczne jest wówczas również administrowanie przez CA listami unieważnionych certyfikatów, które muszą być ogólnodostępne (wiarygodność każdego certyfikatu musi zostać potwierdzona poprzez sprawdzenie, że nie występuje on na liście odwołanych certyfikatów utrzymywanej przez CA będącego wystawcą certyfikatu).

Zbieranie informacji dotyczącej kluczy publicznych w ramach bazy X.500 pociąga za sobą konieczność dostosowania struktury tej bazy. Każde hasło, w którym przewidywane jest umieszczanie tych danych musi należeć do odpowiedniej klasy obiektów (`strongAuthenticationUser`). Niezbędny jest również dostęp do wygodnego interfejsu modyfikującego atrybuty związane z bezpieczeństwem (m.in. `userCertificate`). Adaptacji takiej wymagają bazy X.500 wszystkich serwerów biorących udział w projekcie.

Umieszczenie certyfikatów w publicznej bazie X.500 wymaga zatem współpracy wszystkich administratorów bazy. Należy jednak podkreślić, że fakt wprowadzenia do bazy certyfikatów jest czynnikiem znacznie podnoszącym jej atrakcyjność i z tego powodu należy oczekiwać zainteresowania ze strony administratorów.

Prowadzenie CA przy znacznej ilości zgłoszeń jest zadaniem czasochłonnym i odpowiedzialnym. Wymaga utrzymywania lokalnej bazy wystawionych i unieważnionych certyfikatów przy zapewnieniu najwyższego stopnia jej bezpieczeństwa.

7.5 Przyjęte ograniczenia

W projekcie założono, że początkowo usługa bezpiecznej poczty zostanie udostępniona ograniczonej ilości użytkowników. Oznacza to, że zbędne jest funkcjonowanie licznych urzędów certyfikujących CA i uproszczone staje się zarządzanie kluczami.

7.6 Projekt realizacji usługi

Przewiduje się we wstępnej fazie realizacji projektu powołanie **centralnego urzędu poświadczającego (CCA)**. Urząd ten ma realizować zlecenia certyfikacji klucza publicznego ze wszystkich regionów. W ramach regionów funkcjonują jednostki pełniące rolę „zaufanego” administratora **regionalne urzędy poświadczające (RCA)**. RCA zbiera zlecenia certyfikacji klucza i ewentualnie również generuje klucze użytkownikom. RCA przesyła zlecenia do CCA odbiera zwrotnie rezultaty. Następnie administrator regionalnego serwera X.500 (funkcja administratora może być rozdzielona od funkcji RCA) aktualizuje bazę danych wprowadzając potwierdzone klucze publiczne, zgodnie z danymi odebranymi od CCA.

Klucz publiczny CCA, t.j. urzędu, który wystawił certyfikaty wszystkim użytkownikom systemu bezpiecznej poczty jest dostarczany użytkownikowi systemu w momencie rejestracji. Klucz ten bedzie również dostępny w bazie X.500.

CCA zarządza listą zawierającą dane o wszystkich zaufanych regionalnych administratorach RCA. Lista ta jest zamknięta i wyłącznie CCA decyduje o jej zawartości. CCA zna klucze publiczne wszystkich RCA, RCA w ramach X.500 Directory posiada, jak każdy inny użytkownik, klucz publiczny poświadczony przez CCA. RCA zabezpiecza korespondencję z CCA podpisem cyfrowym, analogicznie CCA każdą informację uwiarygadnia swoim podpisem.

Opisana technika realizacji bezpiecznej poczty elektronicznej wymaga wdrożenia następujących narzędzi programowych:

1. użytkownicy oraz RCA muszą dysponować programem dającym możliwość generowania pary kluczy (publiczny i prywatny), do tego celu nadaje się pakiet PGP lub programy pomocnicze dostarczane w ramach oprogramowania SecuDE,
2. RCA przesyła zlecenia certyfikacji do CCA używając typowego interfejsu *e-mail*, dającego możliwość dodawania podpisów cyfrowych (`pgp-elm, mh`, itp.), bądź stosuje program pakietu SecuDE dający obsługę typową dla standardu PEM,
3. CCA dokonuje certyfikacji za pomocą programu SecuDE, wysyła podpisaną odpowiedź stosując typowy interfejs *e-mail* lub program `pem` z SecuDE,
4. RCA odbiera odpowiedź od CA przez interfejs *e-mail* lub program `pem` z SecuDE,
5. administrator regionalnego DSA otrzymuje od RCA w ustalonej postaci zestaw danych aktualizujących hasła w ramach bazy X.500, dysponuje odpowiednimi narzędziami translującymi te dane do formatu bazy X.500, następnie za pomocą udostępnionych dodatkowych metod aktualizacji wykonuje tzw. „wsadową” modyfikację bazy,
6. użytkownik A chcąc wysłać bezpieczną pocztę do użytkownika B może poświadczyć wiarygodność komunikatu własnym podpisem cyfrowym, lub zaszyfrować ją kluczem publicznym odbiorcy B, lub wykonać obie te czynności; chcąc zaszyfrować przesyłaną pocztę kluczem publicznym użytkownika B (B_p), A wyszukuje w bazie X.500 certyfikat użytkownika B, następnie na podstawie klucza publicznego CCA odzyskuje z certyfikatu B_p,
7. użytkownik B odebrając bezpieczną pocztę, jeżeli jest ona zaszyfrowana, stosuje do odszyfrowania swój klucz prywatny (B_s), jeśli jest poświadczona podpisem cyfrowym nadawcy, wyszukuje certyfikat użytkownika A w X.500, odzyskuje A_p i na jego podstawie sprawdza wiarygodność komunikatu,
8. przewiduje się, że w początkowej fazie wdrażania projektu proces przeszukiwania bazy X.500 byłby niezależny od interfejsu *e-mail*, w dalszych etapach niezbędna jest integracja operacji na X.500 Directory z popularnymi programami obsługi poczty.

7.7 Realizacja

Szybkie i skuteczne wdrożenie usługi uzależnione jest od stosowania w maksymalnym zakresie gotowych, powszechnie dostępnych narzędzi.

Gotowe interfejsy WWW do X.500 umożliwią pobieranie certyfikatów. Weryfikacja podpisów jest realizowana przez pakiety bezpiecznej poczty.

Konieczne jest utworzenie interfejsu tekstowego do X.500 pozwalającego na zapis otrzymywanych informacji, w początkowej fazie jest to do zrealizowania za pomocą modyfikacji typowych interfejsów do bazy.

W pierwszej fazie należy uruchomić CCA i sieć RCA. Niezbędne jest w tym celu spotkanie koordynacyjne, na którym ustalone zostaną zasady funkcjonowania wymiany informacji pomiędzy urzędami.

Konieczne jest opracowanie zasad finansowana usługi i sposobów weryfikacji danych zgłaszanych do potwierdzenia.

W początkowej fazie dopuszczalna jest modyfikacja bazy X.500 w oparciu o standardowe interfejsy, przy wzmożonej aktywności konieczne będzie stworzenie wygodnych systemów przetwarzania wsadowego.

Bibliografia

[1] M. Górecka, T. Wolniewicz, J. Żenkiewicz, *X.500 Directory*, kwiecień 1994, materiały konferencyjne Miedzeszyn '94

[2] M. Górecka, T. Wolniewicz, *X.500 — standard i usługi katalogowe*, kwiecień 1995, materiały konferencyjne Polman '95

[3] M. Górecka, T. Wolniewicz, J. Żenkiewicz, *X.500 — usługa katalogowa w sieci Internet*, maj 1995, materiały konferencyjne Miedzeszyn '95

[4] David Chadwick (1994) *Understanding X.500 The Directory*, Chapman & Hall 1994

[5] Simson Garfinkel (1995) *PGP — Pretty Good Privacy*, O'Reilly & Associates, Inc

[6] J. Linn (February 1993) *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedure*, Request for Comments RFC1421
S. Kent (February 1993) *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management* Request for Comments RFC1422
D. Balenson (February 1993) *Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers* Request for Comments RFC1423

B. Kaliski (February 1993) *Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services* Request for Comments RFC1424

[7] B. Jerman-Blažič, D. Trček, T. Klobučar, F. Bračun, *A Tool Support of Key Distribution and Validy Certyficate Check in Global Directory Service*, Ljubljana, Slovenia

[8] W. Schneider, (March 1995) *SecuDE, Overview, Vol. 1: Principles of Security Operations, Vol. 2: Security Commands, Functions and Interfaces, Vol. 3: Security Applications' Guide*, GMD

[9] ITU-T Recommendation X.500–X.521 (93) *Information Technology — Open Systems Interconnection — The Directory*