OCHRONA BAZY DANYCH X.500 ORAZ JEJ WYKORZYSTANIE DLA POTRZEB BEZPIECZNEJ POCZTY ELEKTRONICZNEJ

Maja Górecka **Tomasz Wolniewicz**

Maja.Gorecka@cc.uni.torun.pl *twoln@hpc.uni.torun.pl*

Naukowa Akademicka Sieć Komputerowa NASK

Bartycka 18, 00-716 Warszawa

Referat składa się z dwóch części.

W pierwszej omawiamy zagadnienia związane z zabezpieczeniami samego systemu X.500. Baza danych, która służy do przechowywania danych osobowych i może być wykorzystywana jednocześnie jako system dla celów wewnętrznych instytucji i jako system informacyjny na zewnątrz, musi być wyposażona w odpowiednie mechanizmy zabezpieczeń. Istotny jest zarówno mechanizm selekcji uprawnionych użytkowników, jak i system określenia uprawnień do konkretnych zasobów. Mechanizmy te, stosunkowo proste we wcześniejszych implementacjach, zostały bardzo istotnie rozbudowane w standardzie X.500 '93.

Druga część referatu jest poświęcona zastosowaniu bazy X.500 do celów wspierania bezpiecznej (szyfrowanej i sygnowanej) wymiany informacji. Omawiamy w niej rozwiązania zaimplementowane w ramach naszych prac rozwojowych w NASK.

Zakładamy, że czytelnik posiada pewną wiedzę na temat systemu X.500, dokładniejsze informacje można znaleźć w szeregu opracowań [7]. Bardzo dobrym źródłem informacji jest również książka D. Chadwicka [2]

Bezpieczeństwo w bazie X.500

Autentykacja

Autentykacją nazywamy metody identyfikacji osoby lub procesu komputerowego ubiegającego się o dostęp do pewnych zasobów. Autentykację stosuje się na ogół dla celów autoryzacji, tj. przydzielania bądź ograniczania dostępu do pewnych zasobów, niekiedy jednak autoryzacja ma na celu jedynie zbieranie danych o użytkownikach systemu, w celach statystycznych albo na użytek identyfikacji osób dokonujących prób nieuprawnionego dostępu.

Standard X.500 [1] a dokładniej X.509) określa trzy poziomy autentykacji: prosty, chroniony i silny.

- Poziom prosty (simple) zakłada, że hasło użytkownika przechowywane jest w bazie X.500. Nie określa się sposobu zabezpieczenia samego hasła, to znaczy algorytmu szyfrowania itp. Istotą tego poziomu autentykacji jest założenie, że użytkownik dowiązujący się do bazy podaje swoje dane (nazwę wyróżnioną) oraz hasło. Informacje te są następnie przesyłane przez sieć bez żadnych zabezpieczeń.
- Poziom chroniony (protected) zakłada, podobnie jak poprzednio przechowywanie hasła w bazie, różnica polega na przesyłaniu hasła w sposób zaszyfrowany dodatkowo wzbogacony stosowaniem stempla czasowego. W ten sposób hasło nie może być ani rozszyfrowane ani przechwycone w postaci zaszyfrowanej i ponownie wysłane w celu włamania.

Poziom silny (strong) stosuje metodę klucza publicznego. W bazie X.500 przechowywany jest certyfikat (a więc poświadczony klucz publiczny) użytkownika. System wysyła użytkownikowi *wyzwanie*, czyli tekst zaszy-

frowany jego kluczem publicznym. System wspierający użytkownika ma za zadanie rozszyfrować wyzwanie i odesłać je systemowi autentykacji. Poprawne rozszyfrowanie oznacza, że użytkownik jest w posiadaniu odpowiedniego klucza, a zatem jest tym, za kogo się przedstawia.

Autoryzacja

Autoryzacja dostępu określa zakres danych które są udostępniane konkretnym użytkownikom. Oczywiście zagadnienie to jest ściśle związane z autentykacją. Zagadnienia związane z autoryzacją zakładają, że autentykacją użytkownika zajmuje się osobny podsystem i mogą co najwyżej wymagać, aby dostęp do pewnych zakresów danych był poprzedzony odpowiednią metodą autentykacji.

QUIPU i standard '88

Autorzy standardu X.500 '88 nie zdefiniowali w ogóle zagadnień związanych z autoryzacją dostępu, sprawą tą zajął się dopiero standard w wersji '93. Ponieważ autoryzacja w pewnym zakresie była niezbędna, implementatorzy musieli wprowadzać swoje własne metody, fakt, który stał się dosyć uciążliwy w momencie ogłoszenia oficjalnej wersji standardu. Prawdopodobnie nacisk implementatorów spowodował, że standard '93 ma niezwykle rozbudowane metody autoryzacji dostępu, tak że większość stosowanych już metod może się obecnie pojawić jako implementacja fragmentu standardu. Niestety to oznacza jednocześnie, że różne implementacje X.500 mogą stosować zupełnie niekompatybilne metody związane z autoryzacją.

Zaimplementowanie autoryzacji było niezbędne chociażby dla potrzeb administrowania bazą, wymagającego sprawdzenia tożsamości administratora. Autentykacja typowo oparta była o metodę prostą lub chronioną, ale w każdym przypadku przewidywała, że baza X.500 będzie przechowywała hasło administratora. To z kolei oznaczało, że konieczne jest specjalne traktowanie atrybutu jakim jest hasło, tak aby umożliwić porównanie, ale nie odczyt.

Oprogramowanie QUIPU, będące fragmentem ostatniego, publicznie dostępnego pakietu Isode 8.0, implementowało dwie pierwsze metody autentykacji (prostą i chronioną) oraz własną metodę autoryzacji.

Autoryzacja w QUIPU zakładała, że informacja o dostępie do hasła (entry) jest przechowywana w samym haśle. System zakłada możliwość chronienia zawartości hasła (lub pojedynczego typu atrybutu) w operacjach:

- odczytu
- modyfikacji
- porównania

W zakresie upoważnionych użytkowników dopuszczano cztery poziomy:

- self (obiekt opisywany danym hasłem),
- group (określenie — wyliczenie — grupy obiektów mających dane prawa dostępu),
- prefix (wszystkie obiekty znajdujące się w pewnej gałęzi drzewa, na przykład wszyscy pracownicy danej instytucji),
- other (wszyscy)

Prawa dostępu przechowywane są w atrybutach `accessControlList` na przykład:

```
acl = other # read # entry
acl = self # write # entry
acl = other # compare # attributes # userPassword
acl = prefix # c=pl@o=UMK # read # attributes # telephoneNumber
```

Administrator serwera zarządzającego pewnym zbiorem danych ma zawsze nieograniczony dostęp do wszystkich danych. Jest to oczywiście uzasadnione faktem, że administrator może modyfikować dane bezpośrednio na dysku.

Przechowywanie informacji autoryzacyjnej na poziomie każdego hasła jest bardzo przejrzyste, ale równocześnie dosyć uciążliwe, gdy trzeba dokonać zmiany obiektu, który ma mieć dostęp do znacznej ilości haseł (na przykład zmiany osoby odpowiedzialnej za pewien podzakres danych w ramach instytucji prowadzącej serwis X.500). Łatwo wówczas o pomyłki. Fakt, że administrator serwera nie musi być jawnie wpisany do każdego

hasła jako osoba o uprawnionym dostępie, pozwala uniknąć modyfikacji bazy w momencie zmiany administratora.

QUIPU wprowadziło dodatkowo atrybuty dziedziczone, pozwalające na przykład na wprowadzenie adresu na poziomie instytucje i spowodowanie, ze pojawia się on jako domyślny u każdego pracownika tej instytucji. System atrybutów dziedziczonych nie daje się jednak stosować do `accessControlList`. Jak widać z opisanych metod, oddelegowanie administratorów odpowiedzialnych za określone fragmenty poddrzewa zlokalizowanego na jednym serwerze jest stosunkowo skomplikowane.

Standard '93

Standard w wersji '93 wprowadza bardzo rozbudowany system ochrony dostępu do danych. Jak wspomnieliśmy powyżej, mnogość możliwych metod (przy jednoczesnej opcjonalności ich implementowania) powoduje, że obecnie nie ma pewności jakie fragmenty faktycznie są podtrzymywane przez dany produkt X.500. Ma to bardzo istotne konsekwencje dla replikacji danych. Zreplikowanie danych chronionych w określony sposób na serwerze innego producenta, może oznaczać, że dane te nie będą chronione w ogóle, jeżeli drugi serwer nie podtrzymuje metody autoryzacji zastosowanej w pierwszym. Niestety nie określono sposobów reakcji na takie sytuacje serwera, który przejmuje dane. Implementatorzy X.500 radzą zatem, aby nie dopuszczać replikacji danych chronionych pomiędzy różnymi implementacjami serwera X.500

Podstawową nowością w standardzie '93 jest ścisłe określenie obszaru zarządzanego. Punkt drzewa informacyjnego, będący wierzchołkiem obszaru zarządzanego pozwala na umieszczenie w drzewie specjalnych obiektów (subentries), które mają znaczenie wyłącznie w administrowaniu systemem, a które pozwalają na określenie, na przykład praw dostępu do odpowiednich fragmentów drzewa. (W istocie standard pozwala wyróżniać specjalne podobszary drzewa w ramach których stosuje się autoryzacje — Access Control Specific Area — ale dla uproszczenia nie będziemy o nich wspominać.) W nowym standardzie można nadawać prawa dostępu dla każdej operacji (read, modify, list, search. add, itd.). Dopuszcza się także określenie wymaganego poziomu autentykacji, potrzebnego dla określonego typu dostępu, na przykład można sobie wyobrazić, że operacja odczytu chroniona jest jedynie prostą autentykacją, ale operacja modyfikacji będzie wymagała silnego poświadczenia tożsamości. Rozbudowano również opis zbioru użytkowników, którym można nadawać prawa dostępu, najbardziej istotne jest dodanie użytkowników z pewnego spójnego obszaru drzewa, jest to system zbliżony do „prefix", ale znacznie bardziej rozbudowany. Standard przewiduje również różne poziomy ochrony w zakresie błędów zwracanych przez system. Można dopuścić, aby system informował, że szukana informacja istnieje, ale nie ma do niej dostępu, albo też zachowywał się identycznie jak gdyby informacja nie istniała.

Poza ochroną poddrzew nadal możliwa jest ochrona poszczególnych haseł poprzez atrybuty zawarte w samym haśle.

Dopuszczenie do dostępu do danego hasła wymaga sprawdzenia, w jakich obszarach kontroli dostępu dane hasło się znajduje, dla każdego takiego obszaru konieczne jest sprawdzenie czy dany użytkownik na prawo dostępu czy nie, widać zatem, że przy skomplikowanych systemach sprawdzenie i zezwolenie na dostęp może być operacją znacznie obciążającą system. Niezbędne jest, aby brać to pod uwagę w momencie gdy definiuje się system zabezpieczeń. Implementacje serwerów '93 dostarczają specjalnych narzędzi do konfiguracji i testowania systemów ochrony danych, przyjmuje się, że konfigurowanie bezpośrednie jest zbyt skomplikowane.

Potwierdzenie prawdziwości wyników

Standard '93 przewiduje możliwość potwierdzania wyników operacji na bazie X.500 poprzez ich elektroniczne podpisywanie. W tym celu konieczne jest wyposażenie serwerów w klucze szyfrujące. Stosowanie opcji podpisywania powinno być istotne gdy odpowiedź z bazy X.500 ma kluczowe znaczenie. Na przykład baza X.500 może zarządzać fizycznym dostępem do pomieszczeń, w zależności od bezpieczeństwa sieci łączącej serwer X.500 z systemem dostępu, podpisywanie wyniku może być uzasadnione lub nie.

Ochrona przesyłanych danych

Należy podkreślić, ze standard X.500 '93, pomimo zdefiniowania bardzo wyrafinowanych metod ochrony przed niepowołanym dostępem, nie definiuje żadnej metody ochrony samych danych w czasie transmisji (a wiec ich szyfrowania). Wydaje się to znacznym niedociągnięciem i należy oczekiwać, ze kolejne wersje standardu zostaną odpowiednio rozbudowane.

Wykorzystanie bazy X.500 do celów autentykacji

Standard X.509

System X.500 od początku swojego powstawania był pomyślany jako wsparcie systemów bezpiecznej wymiany informacji i autentykacji obiektów. Podstawy takiego systemu opisuje standard X.509 wprowadzając określenie *certyfikatu*. W myśl tego standardu certyfikatem nazywa się klucz publiczny obiektu (osoby, systemu komputerowego, instytucji itp.) zaopatrzony atrybutami daty wystawienia i okresu ważności i następnie podpisany elektronicznie przez inny obiekt. Podstawowy związek pomiędzy X.509 a definicją bazy X.500 polega na nazewnictwie obiektów. Wszelkie podmioty, zarówno certyfikowane jak i certyfikujące, są identyfikowane za pomocą *nazw wyróżnionych* tworzonych zgodnie z hierarchiczną strukturą X.500.

W oparciu o standard X.509 określono standard PEM (Privacy Enhanced Mail) [3-6]. PEM poza formatem wymienianej informacji definiuje strukturę instytucji wystawiających certyfikaty. Podstawowe znaczenie dla systemu bezpieczeństwa opartego o certyfikaty ma struktura wzajemnie poświadczających się urzędów. Na to, aby system, taki jak PEM, działał sprawnie potrzebne jest spełnienie dwóch warunków:

1. klucze publiczne identyfikujące podmioty biorące udział w wymianie informacji, muszą być powszechnie i łatwo dostępne,
2. musi istnieć absolutna pewność, że klucze są istotnie związane z podmiotami, które je wykorzystują.

Drugi warunek zapewnić może tylko system urzędów certyfikacji, pierwszy wymaga utworzenia szeroko dostępnych baz danych.

Ponieważ standard X.509 stosuje nazewnictwo zgodne z bazą X.500, baza ta jest naturalnym miejscem do przechowywania informacji wymaganej dla sprawnego funkcjonowania PEM. Certyfikaty ze swojej natury są *bezpieczne*, a zatem przechowywanie ich nie wymaga, aby baza była dobrze zabezpieczona. Podmiana klucza jest wykluczona, możliwe jest jedynie jego skasowanie. Ta własność certyfikatów może być wykorzystana do zabezpieczenia samej bazy X.500, kiedy to certyfikaty, a nie hasła, są podstawą autentykacji użytkowników.

Polski projekt wspomagania bezpiecznej poczty

Powody powstania systemu

Systemy oparte o certyfikaty X.509 zaczynają być coraz bardziej popularne, wykorzystuje je na przykład przeglądarka Netscape. Z drugiej strony w zakresie poczty elektronicznej w Internecie przeważa zdecydowanie system PGP. W celu zapewnienia wsparcia takiej wymiany informacji zaprojektowaliśmy i zaimplementowaliśmy system certyfikacji i publikacji kluczy oparty o polską strukturę X.500.

Zaproponowany przez nas system może zostać wdrożony niewielkim nakładem środków, ponieważ bazuje na już istniejących strukturach — sieci serwerów X.500.

System zakłada zdalny kontakt z użytkownikiem poprzez lokalnych administratorów, rozproszenie zbioru danych, ale centralizację funkcji tworzenia certyfikatów. Taki system zapewnia na początku maksimum efektywności i minimum kosztów, przy jednoczesnej prostej skalowalności w przyszłości.

Certyfikaty użytkowników, w postaci sygnowanych kluczy PGP oraz certyfikatów X.509, przechowywane będą w bazie X.500 dając prosty i szeroki dostęp wszystkim zainteresowanym. Jednocześnie istnieje możliwość funkcjonowania systemu w oparciu o opłaty subskrybcyjne osób przechowujących certyfikaty w bazie.

Zastosowanie bazy X.500 do gromadzenia certyfikatów powinno mieć równocześnie efekt podniesienia atrakcyjności samej bazy i poprawienia aktualności przechowywanych w niej danych. Osoby przechowujące certyfikaty w bazie będą miały jednocześnie możliwość potwierdzenia swojej tożsamości, a co za tym idzie ułatwioną metodę wprowadzania poprawek do danych w bazie.

Struktura i zasady działania

Jak wspomniano, system oparty jest o obecnie istniejąca strukturę X.500. Jednostkę tworzącą certyfikaty nazwaliśmy Centralnym Urzędem Certyfikacyjnym (CUC). Zadaniem CUC jest wystawianie certyfikatów w oparciu o dane przesłane przez delegatury. CUC jest jedynym punktem certyfikacji, co oznacza, że możliwa jest bezpośrednia weryfikacja każdego certyfikatu znajdującego się w systemie. Na CUC spoczywa znaczna odpowiedzialność, gdyż skompromitowanie jego klucza oznaczałoby konieczność unieważnienia wszystkich certyfika-

tów. Z tego powodu CUC musi dysponować absolutnie bezpiecznym systemem komputerowym (bez kontaktu z siecią). W praktyce, z powodów oszczędności, zrealizowane to jest w oparciu o wymienny dysk komputerowy zawierający system operacyjny, łącznie ze wszystkimi narzędziami potrzebnymi do certyfikacji kluczy.

CUC jest przygotowany do wystawiania zarówno certyfikatów w standardzie PGP jak i PEM. W obecnej fazie certyfikaty PEM tworzone są na podstawie kluczy PGP i mają znaczenie pomocnicze (w przeciwieństwie do podpisanych kluczy PGP zawierają stemple czasowe i okresy ważności).

Pewność, że certyfikat jest faktycznie związany z konkretną osobą lub instytucją ma znaczenie absolutnie podstawowe. Z tego powodu wymagane jest osobiste przedstawienie klucza do certyfikacji z odpowiednim potwierdzeniem tożsamości. Niemożliwe jest aby każda osoba pragnąca umieścić w bazie swój certyfikat kontaktowała się bezpośrednio z CUC, ustanowione zostały zatem delegatury CUC stowarzyszone z administratorami lokalnych serwerów X.500. Do zadań delegatury należy potwierdzenie tożsamości użytkownika, ewentualne zawarcie umowy i pobranie abonamentu, a następnie wysłanie otrzymanego od użytkownika klucza do certyfikacji. Przesłanie to musi nastąpić w sposób wykluczający sfałszowanie informacji. Wykorzystywana będzie w tym celu poczta PGP. Należy przy tym podkreślić, że bezpieczeństwo kluczy delegatur jest również bardzo istotne, gdyż skompromitowanie klucza może doprowadzić do tego, że CUC poświadczy nieprawdziwy klucz, ale możliwa jest częsta zmiana kluczy delegatur, a skompromitowanie klucza może co najwyżej oznaczać konieczność zweryfikowania certyfikatów wystawionych w pewnym okresie czasu przez jedną delegaturę.

CUC stosuje zestaw narzędzi, które po utworzeniu certyfikatów przygotowują informację w postaci plików wsadowych, tak że wprowadzenie danych do bazy X.500 jest automatyczne. Wprowadzenia tych danych dokonuje delegatura opiekująca się odpowiednim serwerem X.500.

Systemy wspomagające

W ramach prac przygotowujących system do wdrożenia wykonano między innymi:

- Zaprojektowanie nowych atrybutów przeznaczonych do przechowywania kluczy PGP i wygenerowanie odpowiednich tablic systemowych dla oprogramowania QUIPU.
- Zaprojektowanie struktury gałęzi X.500 zgodnej ze strukturą domenową Internetu. Utworzenie takiej gałęzi było niezbędne w celu szybkiego odnajdywania klucza PGP na podstawie adresu e-mail. Standardowa struktura drzewa X.500 wymagałaby dokonania skomplikowanego przeszukania w zakresie całej Polski. Takie przeszukanie angażowałoby znaczne zasoby i z pewnością byłoby czasochłonne. System gałęzi domenowej tworzy poddrzewo na kształt drzewa DNS, na którego liściach umieszczone są atrybuty typu `uid` określające elektroniczny adres. Obiekty te są aliasami do odpowiednich punktów właściwego drzewa X.500, a w pewnych przypadkach, gdy trudno jest wprowadzić osobę do głównego drzewa, mogą to być również prawdziwe hasła opisujące osoby. Gałąź domenowa jest rodzajem indeksu ze względu na atrybut adresu poczty elektronicznej. Odszukanie osoby ze względu na jej adres oznacza w tej sytuacji jedynie operacje rozwikłania aliasu połączoną z operacją odczytu. Jest to znacznie bardziej efektywne od przeszukania.
- Modyfikacja polskiego interfejsu WWW do bazy X.500 w celu ułatwienia odzyskiwania kluczy PGP. Interfejs został wzbogacony o możliwość korzystania z gałęzi domenowej w celu zwrócenia albo samego klucza, albo pełnej informacji o osobie odpowiadającej danemu adresowi elektronicznemu.
- Utworzenie oprogramowania wspomagającego prace CUC. Przygotowano zestaw programów narzędziowych współpracujących z systemami PGP i SecuDE umożliwiających tworzenie certyfikatów PEM i podpisywanie kluczy PGP. Narzędzia te generują w wyniku dane dla skryptów, które automatycznie modyfikują zawartość bazy X.500. Ponieważ wprowadzanie i modyfikacje danych w bazie X.500 leży poza kompetencjami CUC niezbędne było przygotowanie systemu, który byłby bardzo prosty w obsłudze i nie wymagał przeszkolenia osób obsługujących delegatury.

Do przygotowania pozostaje jeszcze sporządzenie narzędzi wspomagających użytkownika w szybkim uzyskiwaniu informacji z bazy X.500. w chwili obecnej konieczne jest korzystanie z interfejsu WWW i samodzielne kopiowanie uzyskanego klucza PGP.

Literatura

[1] Data Networks and Open System Communications: *Directory*, ITU-T Recommendations X.500-X.525

[2] David Chadwick, *„Understanding X.500 Directory”*, 1994

[3] J. Linn, Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedure, Request for Comments RFC1421

[4] S. Kent, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, Request for Comments RFC1422

[5] D. Balenson, Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers, Request for Comments RFC1423

[6] B. Kaliski, Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services, Request for Comments RFC1424

[7] Raporty i prace na temat projektu X.500 w Polsce

http://ocelot.uni.torun.pl/raporty_pl.html