NEW TRENDS IN THE DIRECTORY SERVICE

MAJA GÓRECKA[1] AND TOMASZ WOLNIEWICZ[2]

[1]*Nicholas Copernicus University, UCTS,*
Chopina 12/18, 87–100 Torun, Poland
maja.gorecka@cc.uni.torun.pl

[2]*Nicholas Copernicus University, LSW,*
Chopina 12/18, 87–100 Torun, Poland
tomasz.wolniewicz@hpc.uni.torun.pl

(Received 14 September 1999)

Abstract: This report summarises the history of the worldwide X.500 directory project. Information on main standards and trends as well as software products is provided. We present the activities of the Polish X.500 project, research and development done since 1992.

Keywords: directory service, X.500, LDAP

1. The PARADISE project

In 1988 CCITT and ISO have defined the X.500 standard [1]. Since this standard was not based on the existing test implementations, it was open to possible mistakes and needed to be tested in a large–scale project. We must remember that at that time Internet was only starting, X.25 was the dominating networking standard, while X.400 was the main standard for e–mail. Directory service based on OSI protocols seemed very natural and certainly necessary. At the University of London Computer Centre the first version of QUIPU, an implementation of X.500, was written, financial support from COSINE was secured and in 1990 an international PARADISE project was started.

The main goal of PARADISE was to install a distributed directory service in the academic environment, test server interoperability and correctness of protocol definitions. The project started very well and has covered nearly the whole world (in cooperation with similar projects in North America and Australia). Poland entered PARADISE in 1992, after the first server was started at the Nicholas Copernicus University, Torun.

The support of COSINE to PARADISE ended in 1994 and co–ordination of the service was assigned to DANTE, under a new name of NameFlow–PARADISE.

Full participation in the service required a subscription to DANTE, but unpaid participation was still possible (with certain restrictions, especially in influencing the future of the project).

2. Directory standards and new trends

As we have mentioned the first version of the X.500 standard was published in 1988 [1]. The next one was X.500 '93 [2] (in fact published in 1995). The standard was then very much extended (about twice in volume), new definitions appeared — mainly replication and access control. Important extensions to the administration model were added (more can be found in D. Chadwick's book [3]). The newest version '97 does not introduce such large changes; it mainly corrects some mistakes in the previous version. One important addition is the concept of the attribute context, which allows the use of several language versions of one attribute and switching the access language though the entire directory entry. The work on X.500–2000 is now in progress.

In the early days of X.500 it was found that the very general directory access protocol (DAP) was difficult to implement in directory client software. This was the main reason why a lightweight version (LDAP) was defined. The most commonly used implementation was written by Tim Howes from the University of Michigan (now at Netscape).

The main concept of LDAP was the existence of a protocol gateway which communicated with X.500 in DAP and with the client in LDAP. This way an LDAP client did not have to implement any distributed operations — the gateway was the unique point of access to the Directory and serviced most of the work. The Michigan implementation contained the server (gateway), an LDAP library and several simple clients. The gopher client has made the X.500 service popular in the Internet. The true milestone was the appearance of gateways between HTTP and LDAP.

During experiments with LDAP implementation a standalone server — slapd — was created. It had no capabilities of working in the distributed system. This server becomes the starting point of an important change in the concept of a directory service: instead of a complicated server and advanced inter–server information protocol, most of the tasks were given to the client. The servers only keep knowledge information — pointers to external information and leave it to the client to follow them. This has to be seen as a total contradiction of the original idea of the directory protocol and the LDAP server itself. This new concept is now formalised as LDAPv3.

LDAPv3 is already implemented in several products. It is supported by most of the X.500 servers. Intensive work on data replication and several other aspects is still in progress. Unfortunately at this moment there are no free implementations, but it must be said that the academic price of the Netscape servers is not high (especially compared with full X.500 products). The OpenLDAP group expects to produce a free implementation still in 1999.

Microsoft will introduce its global directory service — Active Directory, as a part of Windows 2000. This service is meant to be global in the sense that it will

cover all sorts of directory services, for all objects, services and information, supporting both communication and management. According to Microsoft [8], Active Directory is based on a LDAPv3 server and will be fully compatible with other LDAP products. Active Directory will have an API (ADSI) for C, C++, Java and shell scripts. Active Directory does not implement X.500. The service will be fully integrated with the operating Windows 2000 system.

Novell has introduced a directory service supporting its network management (NDS — Novell Directory Services). In spite of the fact that the information model is based on X.500, the protocols are not. The newest version of NDS has very similar goals to Active Directory and has an unquestionable advantage of many years of use and a large user base. A disadvantage of NDS is the use of non–standard protocols, the newest version has tools for LDAP interoperability but they require a protocol gateway.

Sun Microsystems provides FNS (Federated Naming Service). This directory service extends the functionality of NIS+. Similarly to NDS its main goal is network management. It has capabilities of interoperability with LDAP and X.500. Sun Microsystems provides an independent LDAP/X.500 server.

The main concern of directory services should be the uniform protocols. Unfortunately in the situation when one product may be dominant there are natural tendencies for introducing specific extensions which finally lead to incompatibility. Such activity may be caused either by the need of extending functionality or by hope of eliminating competition.

3. Directory service in practice

Ease of use of a directory service is very important for its popularity. X.500 directory service was, by assumption, to provide efficient communication of network applications with a global database of network resources. In the beginning user interfaces (Directory User Agents — DUAs) had to rely on the Directory Access Protocol — DAP, which was difficult and "heavy" due to full OSI requirements. LDAP, which omitted many fine details, came to rescue and started development of many useful user applications of X.500. The WWW gateway to LDAP, in particular Web500gw by F. Richter from the Technical University of Chemniz was the most significant example. Based on this gateway our Polish interface was written (described in more detail in section 5). Currently there are many packages supporting communication with LDAP and creating new applications via C and Java APIs. Java can be extended by a special API library — JNDI (Java Naming and Directory Interface), a unified interface to naming services (e.g. Java RMI objects) and directory services (LDAP, NDS).

Using the X.500 database through dedicated user applications is not the best solution (except for browsing). In a typical situation the need for directory information comes from a specific task and the directory service is expected to simplify network communication. This is why directory interface should be built into both servers and clients of various services. It is not quite popular to connect an

e–mail client to an address–book using either LDAPv3 or X.500. Some servers (e.g. sendmail) can also use LDAP.

Directory Services can store and make available various type of information. The directory schema can be modified to suit any particular needs. One of the standard applications is storing security information, like PEM certificates, certificate paths, revocation lists etc. Extensions proposed in one of the Internet drafts allow for storing PGP public keys, key identifiers, user identifiers and related attributes. These possibilities have been used in the Polish project of supporting secure communication by the X.500 directory service.

4. X.500 software, the year 2000 bug

The most common software used in the PARADISE project is QUIPU, which was based on the ISODE package and became its component. Up to the 8.0 version this package was developed in ULCC and was freely available. In 1993 Isode Consortium was founded, with the goal of developing ISODE and exploiting its commercial potential. Due to strong previous participation of the academic community in the development of ISODE, the Isode Consortium was providing its products free of charge for academic use. This lasted until 1996 when subscriptions were introduced. The software is still distributed in source format.

QUIPU became the basis of a whole range of commercial products (i.e. products of Nexor and ISOCOR).

Independent implementations are provided by ICL, Lucent Technologies, Sun Microsystems and many others. Several French servers, based on INRIA in–house software, which participated in PARADISE, had certain difficulties interoperating with QUIPU servers. This has shown that QUIPU was not full X.500'88 conformant.

Currently there are no free X.500 implementations, except for the out of date QUIPU/ISODE 8.0.

It is known that the free versions of QUIPU contain the Y2K bug. Dates appear in the replica timestamps and modification timestamps. QUIPU authors have estimated that the necessary changes would require 3 man–month of programmer's work, and as the software does not support the 93 version of the standard anyway, it has been decided that no corrections will be made. In Poland only the Nicholas Copernicus University has access to the newest version of QUIPU, all other servers use versions which are not Y2000 secure. Before the end of 1999 a strategy of running the service in future will be prepared. Current assessment shows that the problems will not be grave.

5. Polish X.500 project and its results

Poland joined the PARADISE project in 1992, starting first directory servers in Torun. Still in 1992 the Polish Research and Academic Network NASK joined in and began the co–ordination of the project in Poland. A dedicated country server has been set up and work on customising the service to the Polish language began.

As the result of NASK R&D work about 20 papers, reports and conference presentations have been prepared. They can be found from the project's WWW page — `http://ocelot.uni.torun.pl`.

Nicholas Copernicus University, which is the second coordinator of the service, has been awarded KBN grants three times. As the result of these grants the service now covers most of the academic community. 13 servers are operating presenting data of organisations from their region. They are regularly monitored and the results can be found at `http://ocelot.uni.torun.pl/Wyniki/polskie_dsa.html`.

In the period of 1.01.99 — 6.05.99 the WWW–X.500 gateway in Torun serviced 61800 requests, which makes about 490 per day. The country server services about 270 connections per day (mostly on behalf of other servers). The number of connections should not be confused with the number of operations. The country server services on average 1100 search operations per hour and 2100 operations altogether.

Customising the service to the Polish language requirements was a major challenge. The Polish project, as a part of the international service had to comply with the general service rules, while at the same time a Polish user was to be given Polish–only presentation of data, including correct spelling. The design and implementation were unique within the PARADISE project ([4], [5], [6]). The implementation avoided changes of the core X.500 software (apart from bug fixes). Directory schema was extended by additional Polish object classes and attributes, customised user interfaces were prepared to handle this schema and work on those additional attributes. The first interface was the modification of a text based interface de, later, a WWW interface, basing on the Web500gw, was built. At the same time an interface for administrating data has been prepared. These applications are currently widely used within the Polish X.500 project.

Another project, prepared within NASK, was the support for PGP certificates [7]. A simple security structure was designed (certification authority and its branches) together with the protocol of information exchange. Tools for certification and database update were prepared together with a wrapper for PGP allowing it to collect keys form the X.500 database (also when called from e–mail interfaces such as elm, emacs or pine).

6. Future of Directory Service

The PARADISE Directory Service has been operational for nearly 10 years but in spite of that has not reached the popularity of DNS, e–mail or WWW. We see several main reasons for this:

1. directory services were designed to remain in the background, it was only the PARADISE that has changed them into a foreground information service;
2. up to now directory services were not necessary for computer systems and networks to run (as it is in the case of DNS), for this reason they could be found too difficult or expensive to maintain;
3. maintenance of directory service is costly, unless it is the main database of an institution or is tightly coupled with such a database;

4. publishing of information about people is restricted by law;
5. configuration of X.500 and LDAP systems is still rather complicated.

Of this whole list only the last item — difficulty in configuration — has something to do with the software, the others are of organisational nature. In spite of that one can get the impression that the current standards competition is driven by the belief that a new standard can cure all the problems. In our opinion this is quite untrue.

The growth of the Internet and the number of offered services will force the appearance of directory services and this is the reason why software vendors are now competing in this field. Changes in standards are also a result of this rivalry. Directory services are a necessity in support of security systems based on public keys. All this will cause an explosion of interest in directory services. Having such service in each Windows 2000 server will undoubtedly invite experiments.

The PARADISE project was a typical research testbed. It has shown that interoperability of various systems in such a complicated environment can be difficult. The structure of PARADISE and experience of its administrators worldwide can be used for future experiments. A serious problem is the cost of the software.

DANTE is interested in continuing the service. New applications (like support for PGP) are planned, but at this stage no concrete plans are known, which especially with year 2000 approaching, can be seen as alarming. One of the plans is to change the service to LDAPv3, but interoperability with old ISODE 8.0 servers should be maintained, which may be difficult to implement.

References

[1] Data Communication Networks: *Directory*, Recommendations X.500–X.521, CCITT, Fascile VIII.8 of Blue Book

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

[3] D. Chadwick, *Understanding the X.500 Directory*, Chapman & Hall, 1994

[4] M. Górecka and T. Wolniewicz, *Customising the X.500 database to the requirements of the Polish*, Miedzeszyn'96

[5] M. Górecka and T. Wolniewicz, *Use of national languages in X.500 Directory*, Unicode Conference, Bled 1996

[6] M. Górecka and T. Wolniewicz, *Object naming in distributed international X.500 directory*, Miedzeszyn'97

[7] M. Górecka and T. Wolniewicz, *Secure information exchange system in the Polish Internet based on the X.500 directory service*, Miedzeszyn'98

[8] Microsoft, *http://www.microsoft.com/windows/server/Technical/directory/*