A Directory Application Level Firewall - the Guardian DSA

David W CHADWICK & Andrew J YOUNG
University of Salford, IS Institute, University of Salford, Salford, M5 4WT, England

Abstract *The Internet White Pages Service has been slow to materialise for many reasons. One of them is the security concerns that organisations have, over allowing the public to gain access to either their Intranet or their directory database. The Guardian DSA is a firewall application proxy for X.500 and LDAP protocols that is designed to alleviate these fears. Sitting in the firewall system, it filters directory protocol messages passing into and out of the Intranet, allowing security administrators to carefully control the amount of directory information that is released to the outside world. This paper describes the design of our Guardian system, and shows how relatively easy it is to configure its filtering capabilities. Finally the paper describes the working demonstration of the Guardian that was built for the 1997 World Electronic Messaging Association directory challenge. This linked the WEMA directory to the NameFLOW-Paradise Internet directory, and demonstrated some of the powerful filtering capabilities of the Guardian.*

This paper was originally presented at The Internet Society 1998 Symposium on Network and Distributed Systems Security (NDSS 98), March 10-12, San Diego, California

1. Introduction

Experience gained over the last seven years with the Internet White Pages Directory Service (IWPS), has shown that universities and other public institutions are primarily the only organizations that are prepared to publish their entire directories on the Internet. These are the only organizations that have joined the pilot/operational service in any significant numbers. For example, in the UK NameFLOW-Paradise service [1] there are 147 organizations listed, the vast majority of which are universities, research organizations and publicly funded institutions. Only 21 entries are of commercial organizations, and of these, the majority are computer hardware, software and telecommunications suppliers, or consultancy companies specialising in computer communications. Only 2 entries are of commercial organisations whose main businesses are unrelated to IT, e.g. electricity generation. Similarly (although to a lesser extent) in the US IWPS there are 258 organisations listed, 126 being universities, research laboratories or other publicly funded institutions, 82 being commercial organisations whose primary business is related to IT, with only 50 listings being for other types of commercial organisation. This contrasts quite dramatically with the large number of widely varying types of commercial organisation that have a presence on the Web. Given that commercial organizations outnumber universities by over a thousand to one, the former are conspicuous by their absence in the IWPS. Indeed, private discussions with a number of commercial organizations that do operate

X.500 or LDAP directories reveal that these organizations are willing to connect to the IWPS in order to retrieve directory information from it, but never to give directory information to it. Those commercial organizations that have joined the IWPS have usually only participated in a half hearted way, by adding no more than a token entry or two. It was this realization, coupled with the growing demand from commercial organizations to have a firewall system, running a number of application proxies, positioned between their corporate Intranet and the Internet, that lead to the development of the Guardian DSA. The Guardian is a firewall directory application proxy, that intercepts all directory protocol messages between the Internet and the organization's Intranet, and only allows through those messages that the local security policy has sanctioned.

The Guardian DSA development project started in December 1995, with funding from the EC IV Framework RTD program. The Guardian was originally designed to intercept only X.500 [2] protocols i.e. DAP, DSP, DISP and DOP, but with the recent wide acceptance of the LDAPv2 protocol [3] in the market place, coupled with the rapidly expanding market for stand alone LDAP servers, support for inbound LDAPv2 protocol has also been added to the Guardian. Support for outbound LDAPv2 protocol will be added in 1998.

2. The Functionality of the Guardian

The Guardian provides two quite distinct services to the private Intranet[1]. First and foremost, the Guardian is a directory application proxy designed to run in a security firewall system. It ensures the integrity and confidentiality of directory information on the Intranet, by only allowing properly authorized directory messages to flow into and out of the Intranet.

Secondly, the Guardian is the Intranet's directory gateway to the outside world, acting as a connectivity enabler, particularly for standalone LDAP servers. It is in this second context that organizations running LDAP-only directories can gain real administrative benefit. LDAP clients and servers will no longer need to be continually re-configured to learn about other LDAP servers on the Internet - they only ever need to know about their own internal LDAP servers and the Guardian. All new configuration information is added to the Guardian, making it a central point for administration and knowledge management. The Guardian builds up its own 'world's eye' view of the IWPS, and has its own internal skeleton DIT from which it hangs knowledge references to other LDAP and X.500 directory servers. If operating in a purely X.500 context, the knowledge configuration information is extremely simple (one of the Intranet's DSA's must hold a superior reference to the Guardian, and the Guardian must hold a superior reference to NameFlow Paradise). In a mixed LDAP and X.500 context, references to external LDAP servers are also added to the Guardian.

The remainder of this paper will concentrate on the security functionality of the Guardian and will describe its powerful filtering capabilities.

---

[1] Like any firewall, the Guardian can sit between any two networks, protected by different security policies. For the purposes of this paper, we only consider the case of the publicly accessible Internet (representing a low security network) and a corporate Intranet (representing a high security network).

3. Filtering Rules

It is important to realize that the Guardian itself does not hold any directory entry information, but rather holds a set of rules that dictate which directory information (in the form of directory requests and responses) can flow between the Internet and the Intranet. In this respect, it is quite independent of any access control information that may be applied internally to the database holding the directory information. Indeed, it would be possible to operate the local directory service with little or no local access control information, thereby giving employees free access to most of the corporate directory, and to place all the controls in the Guardian, thereby restricting access to everyone else (i.e. the hard shell and soft inner model of security). The rules that drive the Guardian are derived from the overall security policy of the organization.

The filtering rules that are configured into the Guardian operate at a number of levels, and are separately configurable for each direction of information flow. One configuration file (ToSecurityDomain.ini) contains the rules for filtering requests originating from the Internet, and the other configuration file (FromSecurityDomain.ini) contains the rules for filtering requests originating from the Intranet. At the highest level, the security administrator configures which protocols e.g. LDAPv2 and DAP, are allowed to pass through the Guardian. At the next level, the security administrator configures which users are allowed to bind with these protocols, and below this, which operations e.g. Search and List, are allowed to pass through the Guardian. So for example, the integrity of Intranet directory information can be protected by forbidding modification operations that originate from the Internet. At the next level, the administrator configures which entries are accessible to which operations, and by which alias names they should be known in the other domain. Below this, the administrator lists which attribute types may be included in particular entries, and at the lowest level, the administrator configures which attribute values are allowed to pass through the Guardian. Thus confidentiality of information is assured by preventing sensitive attributes, entries and even the names of entries from leaking out to the Internet. All filtering rules have a default of DENY everything, so that the administrator has to progressively release the locks in order to let directory information leave the Intranet.

Because an application proxy has no inherent way of knowing whether a request has originated from the Internet or the Intranet, the Guardian is configured with the names and addresses of trusted directory servers on both sides of the firewall. Every other directory server is assumed to be un-trusted and residing on the Internet. Note that trusted directory servers on the Internet are still not allowed to receive sensitive information from the Intranet unless an encrypted communication session is employed. Finally, the Guardian will never relay requests within one of the domains, as none of the directory protocols require this functionality. (A consequence of this is that the Guardian will never relay a request from one unknown directory server to another.)

4. User Authentication and Authorization

In a distributed directory service, a user may bind to and be authenticated by any directory server, and the servers may pass user requests between themselves (in

the X.500 model the DSP is used for this, whereas LDAP currently does not support such a protocol). A configuration parameter informs the Guardian of the minimum level of authentication required for each directory protocol. If the user meets this minimum level, the bind will be accepted, otherwise it will be rejected.

In the case where the user does not bind directly to the Guardian, the Guardian needs to know if a particular user was authenticated by a trusted directory server, or by an un-trusted one. Its list of trusted directory servers will tell it this, and if it transpires that the user was authenticated by an un-trusted server, then the Guardian removes the authentication privileges from the user's request and treats him or her as un-authenticated before either rejecting the request or passing the DSP request onto the other network (see Figure 1). If the user was authenticated by a trusted directory server, then his/her level of authentication (simple or strong) is believed and passed on as-is to the other network.

If the user binds directly to the Guardian, then his/her credentials are checked. If simple (password based) authentication is used, the Guardian checks the password against its internal list (the passwords are actually stored as attributes of user entries with the equivalent distinguished names). If strong (digital signature based) authentication is used, the Guardian checks the signature for authenticity, and also that there is a chain of trust leading from the public key of a trusted CA to the public key of the user. In this context, our Guardian is shortly due to become a certified user of the ICE-TEL CA infrastructure [4]. If the user's credentials prove to be false or untrustworthy, a configuration parameter directs the Guardian to either reject the bind or downgrade the session to un-authenticated if this level is acceptable.

In addition to session authentication, individual directory operations can be digitally signed by a user. The Guardian will check the digital signatures of signed operations, retrieving the CRLs as necessary, and if the signature proves to be false, will either reject or downgrade the operation according to the security policy input by the administrator.

4.1. Authenticating and Authorising Outgoing Operations

Some organizations have a requirement to restrict the number of users who are allowed access to the Internet. The security administrator has to configure the Guardian with the distinguished names of users and non-leaf nodes (typically organizational units) that are allowed access to the Internet directory. If the Intranet user is not within this name space his request will be denied. Finally, for authorized users, the DN of the user can either be hidden (for example by replacing with a generic name) or made visible in the requests that flow onto the Internet. An X.500 user will typically bind to his/her local DSA, and the request will be chained to the Guardian by this. In some circumstances the user will need to bind directly to the Guardian, for example, when using LDAP servers, or when external directory servers wish to directly authenticate the user. In these circumstances the Guardian acts as a proxy user. For these outgoing sessions, the Guardian performs DAP-DAP chaining or LDAP-DAP chaining (see Figure 1). Outgoing DAP or LDAP to DSP chaining is not supported. LDAP-LDAP chaining will be added towards the end of 1997, although the same functionality can be obtained now by using the X.500 Enabler from Critical Angle [5].

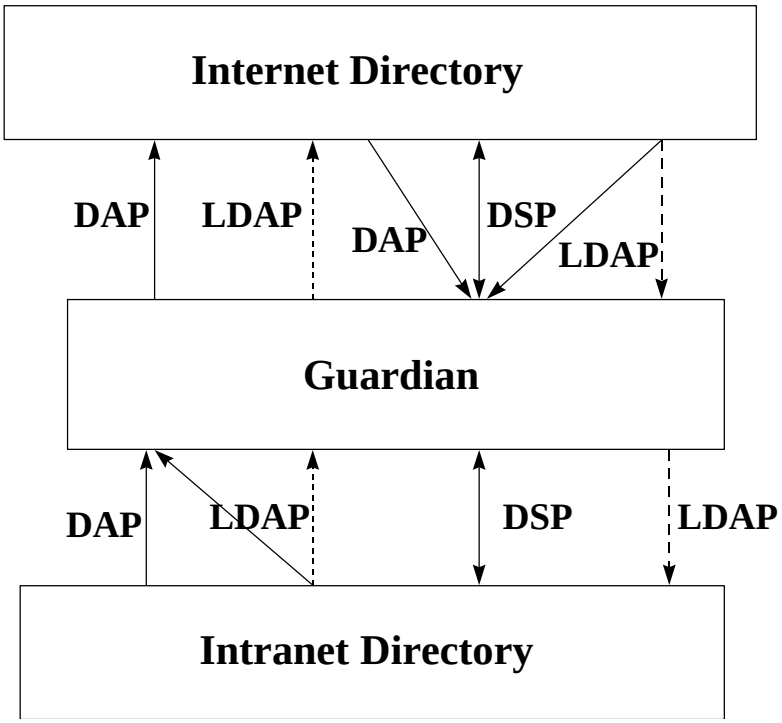

Figure 1. Protocol Chaining Supported by the Guardian

4.2. Authenticating and Authorising Incoming Operations

For incoming sessions, a similar situation applies. The Guardian is configured with the list of remote users (DNs of leaf and non-leaf nodes) who are allowed to access the Intranet. It is also possible to give blanket access by using the keyword ALL. Because the Guardian is trusted by the Intranet directory servers, it does not need to act as a proxy for a remote user. The remote user must be authenticated by the Guardian before he/she is allowed access to the Intranet. Consequently the Guardian always performs standard DAP-DSP chaining or LDAP-DSP chaining (see Figure 1) on incoming operations. LDAP-LDAP chaining will be added towards the end of 1997 to support LDAP stand alone directory systems on the Intranet.

5. Processing of Referrals

It is important that the names and addresses of the corporate directory servers can be hidden from the Internet, and that only the address of the Guardian server is made known publicly. Referrals to Intranet directory servers would compromise this situation, if they were to be released to the Internet. Consequently, the Guardian always acts on referrals to Intranet servers. Similarly for incoming referrals, there is little point in passing these to the corporate user, since he has no direct path to the Internet. Again, the Guardian will always endeavour to follow incoming referrals, and pass a complete set of directory information back to the user.

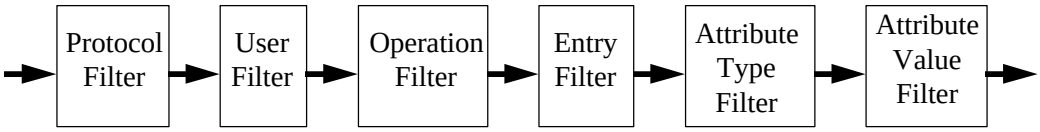

Figure 2. The Filters of the Guardian

6. Configuring the Guardian

One of the key factors in security is KISS (keep it simple, stupid). If it is extremely complex to configure a firewall system of any type then it is likely that, sooner or later, a security administrator will make a mistake that compromises the security of the Intranet. Consequently, ease of configuration has been a key design aim for our Guardian.

The Guardian acts as a 6 stage filter, progressively refining and reformatting messages that pass through it. The filters act sequentially, as depicted in Figure 2.

Configuration of the Guardian involves the specification of two distinct security policies:

- the Intranet Access Policy (this specifies the protocols and operations that external users can use to access the internal domain; and the entries, attributes and values that can be returned in outgoing results); and
- the Internet Access Policy (this specifies the protocols and operations that internal users can use to access the external domain; and the entries, attributes and values that can be returned in incoming results).

To make clear the fact that these two policies are distinct, two configuration files are specified, and each contains specifications for all six filters. The syntax and semantics of each is the same, though it is very likely that the content will be different e.g. see Appendix 1.

The Guardian configuration uses a "default deny" principle, which means that anything that is not explicitly enabled will be disabled. Therefore, if both configuration files are empty then the Guardian will not allow any X.500 or LDAP protocols to pass through it in either direction. Additionally, by ensuring that only permitted actions are specified, rather than prohibited actions, the configuration file does not contain any prohibited information and so it can be made public if required.

Various other parameters are supported in the configuration files. Briefly these are: a parameter to control the amount of logging, whether to downgrade or reject failed authentications, the list of trusted DSAs, and the action to take if a request attempts to retrieve restricted information (remove from result or return error).

6.1. Specification of the filters

The syntax for each filter is formally defined in Figure 3, where:

<specification> ::= description of the items accepted by the filter. The format is specific to each type of filter.

<qualifier> ::= a restriction, allowing an item to be accepted under specified conditions. The format is specific to each type of filter.

<modifier> ::= description of the item in the namespace of the calling domain (if this is different to the called domain)

```
<filter> ::= '[' <filter_name> ']'  <filter_specs>

<filter_name> ::= 'Protocols'
                  | 'Users'
                  | 'Operations'
                  | 'Entries'
                  | 'Attribute Types'
                  | 'Attribute Values'

<filter_specs> ::= <filter_spec> [ <filter_specs> ]

<filter_spec> ::= [ 'FOR' <branch> ] <allow>

<allow> ::= 'ALL'
            | 'ONLY' <refinements>
            | 'NONE'

<refinements> ::= <refinement> [ ',' <refinements> ]

<refinement> ::= <specification> ['(' <qualifier> ')']
                 [ 'KNOWN AS' <modifier> ]
```

Figure 3. BNF for the filter

<branch> ::= boolean condition in terms of previous filters. The format is specific to each type of filter.

7. Examples

This section gives an example of each type of filter, and shows some of the capabilities that are possible.

7.1. The [protocols] filter

Here, the list of enabled directory protocols is given.

```
[Protocols]
  ONLY DAP, LDAP(no authentication), DSP(simple)
```

Each protocol may take an optional argument indicating the minimum bind strength of authentication that is acceptable. In this example, a DAP bind must be strongly authenticated (this is the default if no bind strength is mentioned), an anonymous LDAP bind is acceptable and a DSP bind must have at least a password (simple). DISP and DOP are not mentioned, so the Guardian will block any DISP or DOP binds that it receives.

7.2. The [users] filter

This specifies the distinguished names of the users who are allowed to bind to the Guardian for each of the above protocols. Distinguished names are specified

according to Internet standard [6], with the extension that names may be specified using wild cards. Four forms of wild card are supported:

if an RDN of "*at*=*" is included in the name then it will match any single valued RDN of attribute type *at*, e.g. cn is used for commonName etc.;

if an RDN of "*at*=**" is included in the name then it will match any multivalued RDN of where one part of the RDN is of attribute type *at*;

if an RDN of "*=*" is included then it will match exactly one RDN of any attribute type; and

if an RDN of "**=**" is included then it will match one or more RDNs, of any attribute type, up to the end of the name.

```
[Users]
    FOR Protocol=DAP, LDAP
    ONLY <cn=A J Young,ou=Information Technology
Institute,o=University of Salford,c=GB> (simple) KNOWN AS <cn=A J
Young,o=University of Salford via guardian,c=gb>

FOR Protocol=DSP
ONLY <cn=DSA Manager,cn=DSA,o=University of
     Salford,c=gb> (strong)
```

Each user DN is followed by two optional parameters. The first indicates the level of authentication that this particular user or group of users must present. If absent, it defaults to that specified for the individual protocols, but can be set to a higher level if the security policy so directs. A lower value will be ignored (as would be the case for DAP in the examples above, since the DAP protocol requires strong authentication). The second parameter, starting with keywords KNOWN AS, allows an alias name for the user to be used in the other domain.

7.3. The [operations] filter

Here, we specify which directory operations will be allowed to pass through the Guardian for each group of users.

```
[Operations]
   FOR  User=<cn=DSA Manager,cn=DSA,o=University
   of Salford,c=gb>
   ONLY READ(unsigned),LIST(unsigned 20, signed
   100),COMPARE
```

Each operation may take an optional argument indicating whether or not it may be unsigned in order to pass through the Guardian. The LIST and SEARCH operations additionally can specify an optional argument giving the maximum number of entries that may be returned in the results (this may be different for signed and unsigned operations). The default value for this is one entry. In this example, READ may be unsigned, COMPARE must be signed (this is the default if no signature requirement is mentioned), and LIST may return more entries if the operation is signed. SEARCH and the modification operations are not mentioned here, and so these operations would not be allowed to pass through the Guardian.

7.4. The [entries] filter

Here, we specify which entries will be allowed to pass through the Guardian. In addition to specifying which entries can pass through, it is also possible to specify

what their names should be known as in the external domain i.e. a form of aliasing. This is especially useful if an organisation wishes to protect its Intranet DIT structure from being visible on the Internet.

```
      [Entries]
          ONLY <cn=A J Young,ou=Information Technology
Institute,o=University of Salford,c=GB> KNOWN AS <cn=A J
Young,o=University of Salford via guardian,c=GB>,
                <cn=D W Chadwick,ou=Information Technology
Institute,o=University of Salford,c=GB> KNOWN AS <cn=D W
Chadwick,o=University of Salford via guardian,c=GB>
```

In the above example, only two entries (for the authors of this paper) may pass through the filter, and these will be visible in the other domain with their organisational unit affiliations stripped off.

7.5. The [attribute types] filter

Here we specify which attribute types will be allowed to pass through the Guardian.

The second part of the example is needed if the administrator wishes to over-ride the default-deny stance and say that all attribute types can be released for all allowed entries other than those explicitly named in the first part of the example.

```
[Attribute Types]
    FOR Entry=<cn=*,ou=Information Technology
    Institute,o=University of Salford,c=GB>
    ONLY objectClass, commonName, surname,
    title, postalAddress, postalCode,
    telephoneNumber, userid, rfc822Mailbox,
    roomNumber, userClass, userPassword,
    favouriteDrink
    FOR Entry=*
    ALL
```

7.6. The [attribute values] filter

Here we specify, for each attribute type, the values which are allowed to pass through the Guardian. The example here specifies that all direct dial telephone numbers will be made available in international format, whether they are stored in international, national or internal format. Non-direct dial extensions (these do not start with a 5) will not be released.

The second part of the example is needed to over-ride the default-deny stance and say that, for all other allowed attribute types, all values can be released.

In the specification of a value, a * may be used to match any number of characters, and a ? to match a single character.

```
 [Attribute Values]
    FOR Attribute Type=telephone number
    ONLY "+44 161 745 *",
         "0161 745 *" KNOWN AS "+44 161 745 *"
         "5????" KNOWN AS "+44 161 745 ????"
    FOR Attribute Type=*
    ALL
```

7.7. Specification of local names

The configuration file allows the Guardian administrator to define local names for groups of users, and to specify the DNs of users and entries using these short name forms. This makes the specification much easier for the administrator, since he/she does not have to re-enter lots of DNs. As well as allowing for more readable specifications, the mechanism also provides a single place where the names of the group members is defined, thereby making maintenance and audit easier.

Local names are defined in an extra section of the tailor file, which is usually located after the filters (though it can be located anywhere). They are specified as follows:

```
[Local naming]
    NAME <distinguished name> ... KNOWN AS
    <local name>
```

The short local name must not contain a comma, an = or a *.

The distinguished name may contain wild cards, as defined earlier in the document. Any number of names may be specified, separated by a comma. An example is:

```
[Local Naming]
    NAME <cn=A J Young, ou=Information Technology Institute,
o=University of Salford, c=GB> , <cn=D W Chadwick, ou=Information
Technology Institute, o=University of Salford, c=GB> KNOWN AS
<guardian developers>
```

This allows the Guardian administrator to say:

```
[Users]
ONLY <guardian developers>(strong)
```

to restrict use of the Guardian to just the named people, or to say:

```
[Operations]
FOR User=<guardian developers>
ALL
FOR User=*
ONLY Read,Compare,List
```

to give the named people higher privileges than other users. If staffing details change then the Guardian filters do not need to be changed.

8. Piloting the Guardian

The Guardian was successfully piloted at the EMA meeting in Philadelphia in April 1997, and again at the EEMA meeting in Maastricht in June 1997. It is now permanently operational, and demonstrable from our Web site [7].

Because the Internet White Pages Service and NameFLOW-Paradise service use Quipu based X.500 products, that incorporate Internet defined extensions to the X.500 1988 protocols [e.g.8], WEMA decided to set up a parallel infrastructure using products that conform to the LDAPv2 protocol and 1993 X.500 standards. The Guardian is quite happy to talk to both flavours of X.500 products, and in fact does so in our demonstration, with the Salford directory (representing the Intranet) being held

in a Quipu DSA, and the WEMA directory infrastructure (representing the Internet) being held in 1993 conformant DSAs.

If we were to connect the University of Salford directory to the EEMA infrastructure via the Guardian in the conventional way (Figure 1), then it would only be possible to see a subset of the information contained in the University of Salford directory, as directed by our security policy. Furthermore, it would not be possible to verify the full protection effects of the Guardian, because no-one from the Internet would have access to the unfiltered directory. Consequently, we built a configuration that allows users to see both behind and in front of the firewall, so that they can see for themselves the effect of the Guardian. To do this, we have added subordinate knowledge references to the EEMA GB DSA to point to both the University of Salford operational DSA, and the University of Salford Guardian (see Figure 4). By displaying the contents of the University of Salford operational DSA, one will see the entire directory of the University of Salford. By displaying the contents of the University of Salford via the Guardian DSA, one will only see the entries that our security policy has decided should be available to the public directory.

8.1. The University of Salford Directory

There are approximately 26,000 entries held in the University of Salford directory, and these are all held in a single Quipu DSA. The Salford directory tree is structured with departments (organizational units) below the University of Salford entry, and people below the departments, as shown in Figure 5.

All people within the University of Salford have access to all of this information from the corporate Intranet. The Guardian has been configured so that the WEMA public directory can only see 3 person entries in the University of Salford directory, and cannot see any of the departments, as shown in Figure 6.

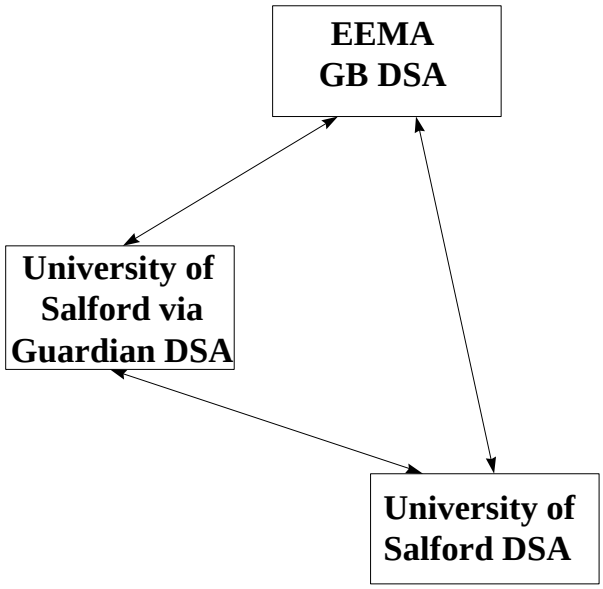

Figure 4. The Configuration of the Demonstrator

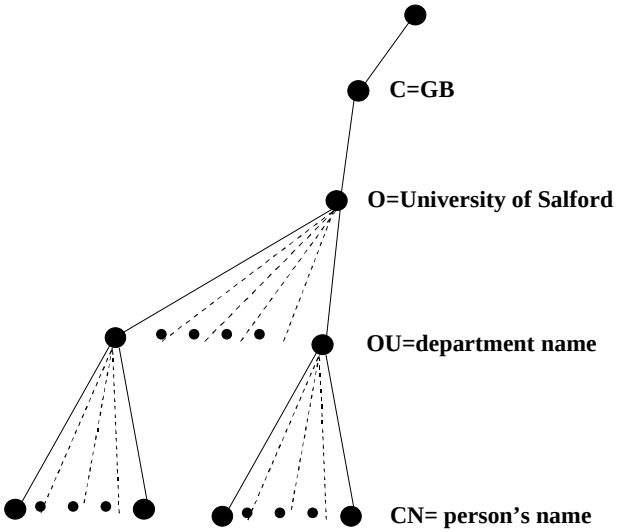

Figure 5. The University of Salford's DIT

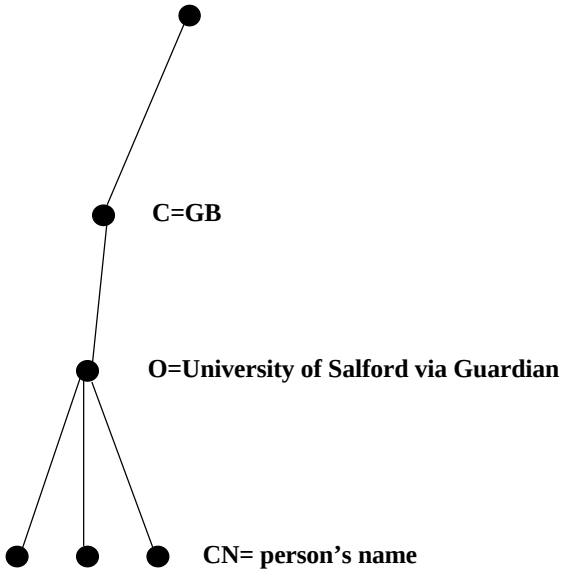

Figure 6 The University of Salford's DIT visible to the public

This shows the powerful filtering effects of the Guardian, in that not only can it remove leaf entries and subtrees from public view, but it can also remove non-leaf nodes, thereby appearing to alter the structure of the corporate DIT. Finally, the Guardian can rename non-leaf nodes, thereby allowing the private directory and the public directory to use different naming conventions (for example, in our demonstration, the internal name O=University of Salford, is given the name O=University of Salford via Guardian in the public directory). The Guardian thus allows you to gateway between two DITs with different name-spaces. Such capabilities are not normally provided by standard access control lists.

8.2. Attribute Filtering by the Guardian

The three entries that are visible via the Guardian have had some of their attributes filtered from public view. If you read the contents of the entry:

CN=D W Chadwick, OU=Information Technology Institute, O=University of Salford, C=GB

via the operational University of Salford DSA, you will see that the Email address, Fax number, Telex number and Telephone number attributes are all present. However, if you read the contents of the entry:

CN=D W Chadwick, O=University of Salford via Guardian, C=GB

via the Guardian, you will see that the Telex number and Fax number attributes have been filtered out. It is also possible to filter particular attribute values, if your security policy so requires.

9. Performance

A limited number of performance measurements have been carried out in our laboratory, in which the Salford DIT was searched for SN=Chadwick, both directly and via the Guardian. These have revealed that the deviation in real time performance (as seen by the user agent), for both access routes, is as great as the delay in going via the Guardian. Specifically, for 20 requests sent via both routes, the average time and standard deviation for a response was 15.5±6.5 secs for a direct request and 20.3±7.5 secs for a request sent via the Guardian. We are currently performing additional tests to determine how much of the delay is caused simply because we are chaining via another directory server, and how much is actually caused by the filtering functionality of the Guardian.

10. Conclusion

The provision of a Guardian directory application proxy should give organisations that wish to publish only a part of their corporate directory, the confidence to connect their corporate directory service to the Internet White Pages Service, safe in the knowledge that they can fully filter the amount of directory information that leaves their domain. The Guardian implementation built at Salford University provides such a functionality. Furthermore, a major design goal has been to ensure that the two configuration files, used to input the organisation's security policy into the Guardian, are both easy to understand and secure in the way that they operate, using the default deny principle.

References

[1] Details about the NameFLOW-Paradise service can be obtained from http://www.dante.net/nameflow.html
[2] ITU-T X.500 | ISO 9594 (1993) The Directory, Parts 1 to 9.
[3] Yeong, Howes and Kille. "Lightweight Directory Access Protocol", RFC 1777, March 1995
[4] Details about the ICE-TEL project can be found at http://www.darmstadt.gmd.de/ice-tel/
[5] Details about Critical Angle's X.500 Enabler can be found at http://www.critical-angle.com
[6] Wahl, M., Kille, S., Howes, T. "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names", RFC2253, December 1997.
[7] For a live demonstration of the Guardian, see http://fw4.iti.salford.ac.uk/ice-tel/guardian/demo
[8] Hardcastle-Kille, S.E. "Replication and distributed operations extensions to provide and Internet directory usingX.500", RFC 1276, Nov 1991

Appendix 1. Example Configuration Files

```
      # This is an example ToSecurityDomain.ini file,
      # specifying the Intranet Access Policy used in
      # the EEMA demonstration Guardian (enhanced to
      # take account of some new features that are not
      # currently implemented)
      # This   file   specifies   the  protocols   and
      # operations  that  external  users  can  use to
      # access the internal domain; and the entries /
      # attributes / values  that  can be returned in
      # results (incoming operations outgoing results)

      [Protocols]
      ONLY DSP(simple),LDAP(no authentication)

      [Users]
      ALL

      [Operations]
      FOR User=<andrew>,<chad>
      ONLY Read (unsigned), List (unsigned 100, signed
      100), Compare(unsigned)


      FOR User=*
      ONLY Read (signed), List (signed 100), Compare(signed)

      [Entries]
      ONLY <andrew> KNOWN AS <cn=A J Young, o=University of Salford
via guardian, c=GB>,
           <chad> KNOWN AS <cn=D W Chadwick, o=University of Salford
via guardian, c=GB>

      [Attribute Types]
      FOR Entry=<**=**,o=University of Salford,c=gb>
ONLY objectClass, commonName, surname, title, postalAddress,
  postalCode, telephoneNumber, userid, rfc822Mailbox, roomNumber,
  userClass, userPassword, favouriteDrink

      FOR Entry=*
ONLY objectClass, commonName, surname, organizationName, countryName,
  localityName, stateOrProvinceName, street, title, postalAddress,
  postalCode, telephoneNumber, userid, rfc822Mailbox, roomNumber,
  userClass, lastModifiedTime, lastModifiedBy, accessControlList,
  associatedDomain, businessCategory, description, iattr, masterDSA,
  slaveDSA, userPassword, favouriteDrink

      [Attribute Values]
      FOR Attribute Type=favouriteDrink
      ONLY tea, coffee

      FOR Attribute Type=objectClass
ONLY top, person, organizationalPerson, newPilotPerson, quipuObject,
  organization, domainRelatedObject, quipuNonLeafObject,
  organizationalRole, organizationalUnit, country, locality, dsa

      FOR Attribute Type=telephoneNumber
      ONLY +44 161 745 *,
           0161 745 * KNOWN AS +44 161 745 *,
           5???? KNOWN AS +44 161 745 ????

      FOR Attribute Type=*
```

```
      ALL

# End of filters - the following items are basic configuration items

      [General]
      LOGGING "level=exception level=notice
file=guardian/intranet.log"
      AUTHENTICATION downgrade
      QUERY PROHIBITED ITEM return error

      [Local Naming]
      NAME <cn=A J Young, ou=Information Technology Institute,
o=University of Salford, c=GB> KNOWN AS <andrew>
      NAME  <cn=D W Chadwick, ou=Information Technology Institute,
o=University of Salford, c=GB> KNOWN AS <chad>
```

```
      # This  is  an  example  FromSecurityDomain.ini
      # file, specifying the  Internet  Access  Policy
      # used  in  the  EEMA  demonstration   Guardian
      # (enhanced to take account of some new features
      # not currently implemented)

      # This  file   specifies   the   protocols  and
      # operations  that  internal  users  can use to
      # access the external domain; and the entries /
      # attributes / values  that can be  returned  in
      # results (outgoing operations incoming results)

      [Protocols]
      ONLY DSP

      [Users]
      ONLY <c=GB,o=University of Salford, ou= Information Technology
Institute, cn=A J Young> (simple) KNOWN AS <c=gb,o=University of
Salford via guardian,cn=A J Young>

      [Operations]
      ALL

      [Entries]
      ALL

      [Attribute Types]
ALL

      [Attribute Values]
      ALL

# End of filters - the following items are basic configuration items

      [Trusted DSAs]
      NAME <cn=University of Salford DSA 1,c=gb> (simple)

      [General]
      LOGGING "level=exception level=notice
file=guardian/internet.log"
      AUTHENTICATION downgrade
```