Enabling the Internet WPS

The Directory Guardian

D W Chadwick
A J Young
University of Salford

Contents

- *Rationale for Development*
- *Overview of Guardian Functionality*
- *Description of Configuration Files*
- *Example in Use*
- *Performance Data*

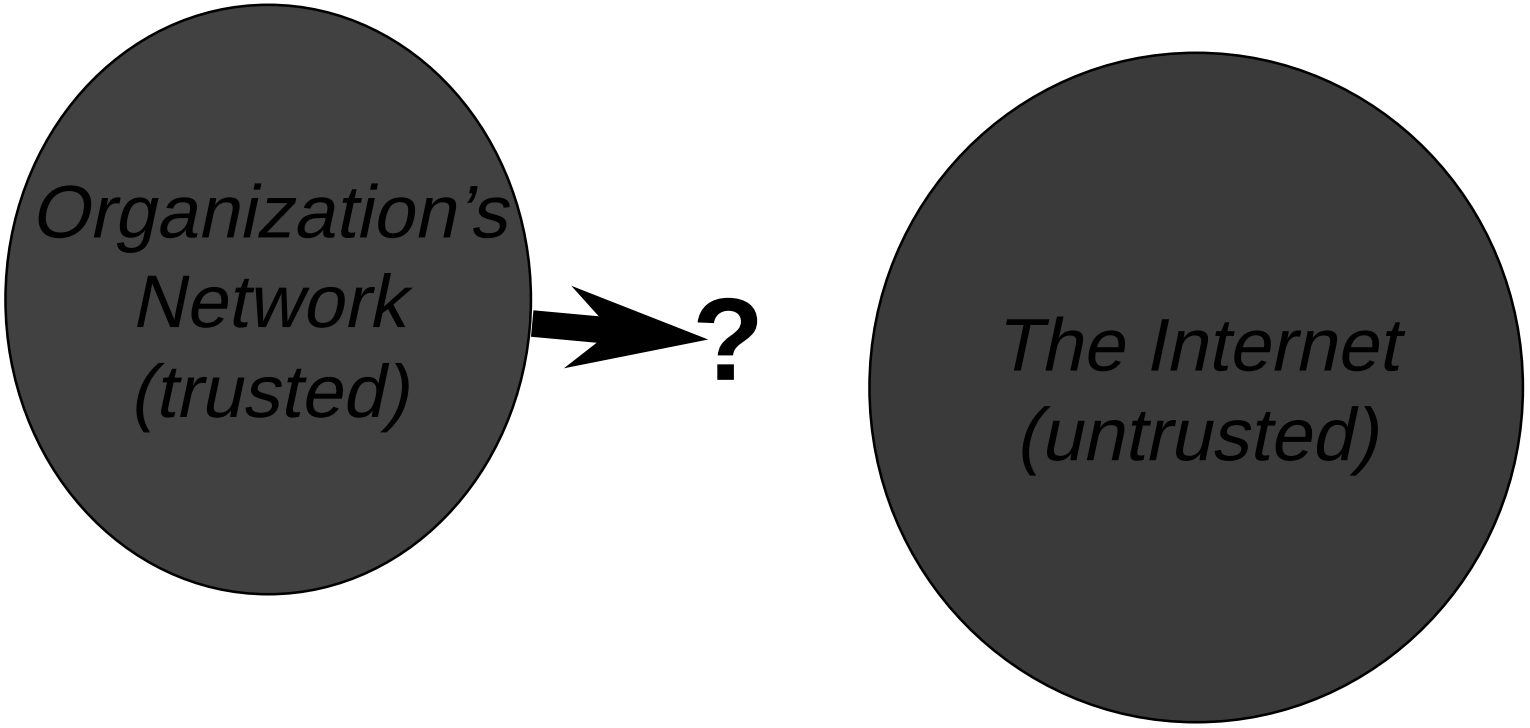
X.500/LDAP Global Directory Service

- *Holds information about employees, organizational units and applications*
- *Telephone and Fax numbers, Email Postal and Application addresses etc.*
- *Already ~2 million entries from 30 countries in NameFLOW-Paradise service - but MAJORITY ARE ACADEMIC*

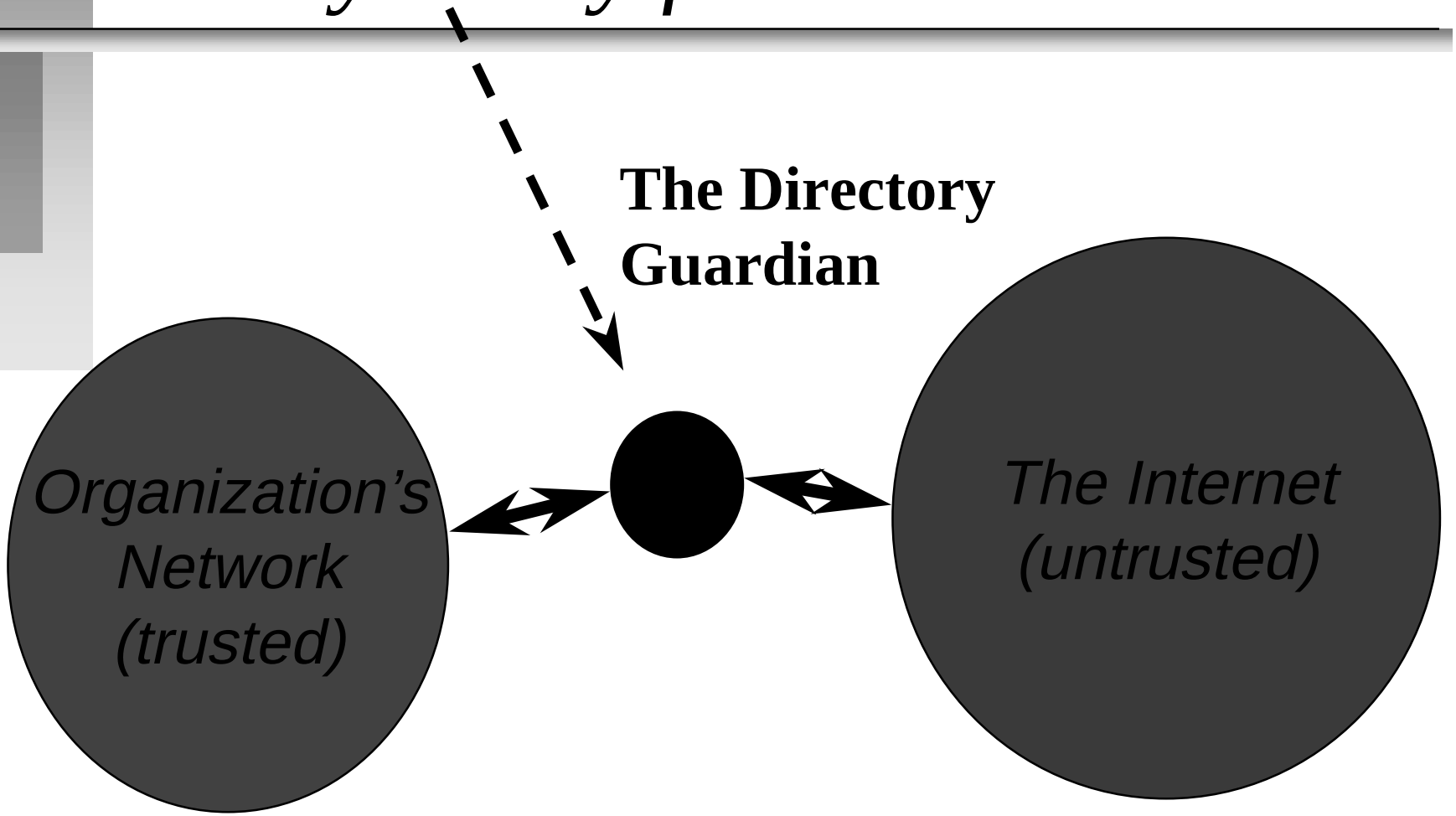
Some Statistics for NameFLOW-Paradise

- *147 organisations under C=GB, 126 Academic/Public, 19 commercial IT organisations and 2 non-IT commercial*
- *258 organisations under C=US, 126 universities&public, 82 commercial IT organisations and 50 non-IT commercial organisations*
- *Compare this with the Web, which is predominantly commercial*

Why the reluctance?



Directory Proxy for the Firewall



The Directory Guardian - Overall Requirements

- *Incoming filter*
  - *Prevent access to sensitive information*
  - *Prevent overwriting of important information*
- *Outgoing filter*
  - *Prevent accidental release of confidential information*

Requirements in Detail

- *Incoming requests*
  - *Check credentials and refuse or replace untrustworthy ones*
  - *Block suspicious Interrogation operations*
  - *Block all Modification operations*
- *Outgoing responses*
  - *Remove confidential attributes, names, referrals, cross references, signatures*

Requirements in Detail (cont)

- *Outgoing requests*
  - *Block unauthorized ones*
  - *Remove trace information, confidential names and signatures*
- *Incoming responses*
  - *Check credentials and replace untrustworthy ones*
  - *Act on referrals, remove cross references*

Implementation

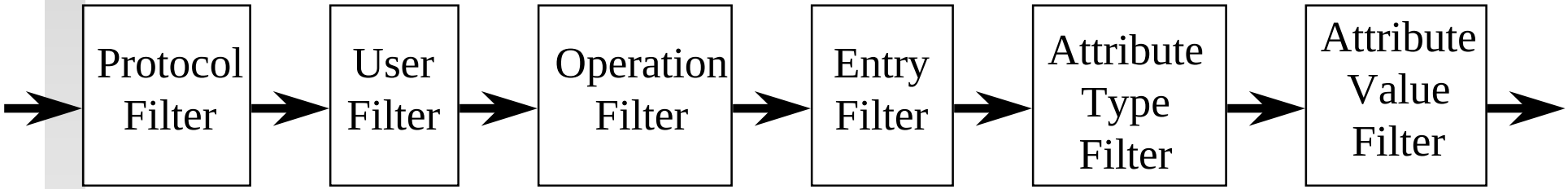
- *Used Source Code Of Directory Server from Isode Ltd*
- *Runs on Sun Sparc, written in C*
- *Supports LDAP, DAP, DSP, DISP*
- *Supports password and digital signature based authentication*

Configuring the Guardian

- *KISS (Keep it Simple, Stupid)*
- *Two configuration files - one specifies incoming filter and other outgoing filter*
- *Default is DENY everything*
- *So filters only contain what is allowed to pass through them i.e. non-confidential information, therefore they are not a large security risk*

The Filters

- *Series of filters which act in sequence to progressively refine the information flow*
- *Can have branching so that subsequent filters act on instances of previous filter e.g. different entries are visible to different operations*



Protocols Filter

- *Lists the protocols that can pass through with the minimum Bind authentication required (default being digital signature)*

[Protocols]

ONLY DAP, LDAP(no authentication), DSP(protected password)

Users Filter

- *Lists the users who are allowed to Bind for each of the protocols, with their minimum authentication (defaults to that of the protocol), and an optional alias name that is to be used in the other domain*
- *User names are specified as LDAPv3 DNs, with wildcarding*

Users Filter example

[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)

Local User Names

- *Allows groups of users to be given a local name, for ease of reference e.g.*

[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>

Operations Filter

- *Specifies which operations can pass with parameter indicating if each is to be signed or not, plus for List and Search the max entries that can be returned*

[Operations]

FOR User=<cn=DSA Manager,o=University of Salford,c=gb>

ONLY READ(unsigned),LIST(unsigned 20, signed 100),COMPARE

Entry Filter

- *Specifies which entries are visible, optionally with an alias name*

[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>

Attribute Types Filter

- *Specifies which attribute types can pass through, with optional mapping of types*

[Attribute Types]

FOR Entry=<cn=,ou=Information Technology Institute,o=University of Salford,c=GB>*

ONLY objectClass, commonName, surname, title, postalAddress, postalCode, telephoneNumber, rfc822Mailbox

Attribute Values Filter

- *Specifies which attribute values (including wild cards) can pass, with optional mapping of values*

[Attribute Values]

FOR Attribute Type=telephone number

*ONLY "+44 161 745 *", "0161 745 *"*
*KNOWN AS "+44 161 745 *"*

"5????" KNOWN AS "+44 161 745 ????"

Knowing the Calling Domain

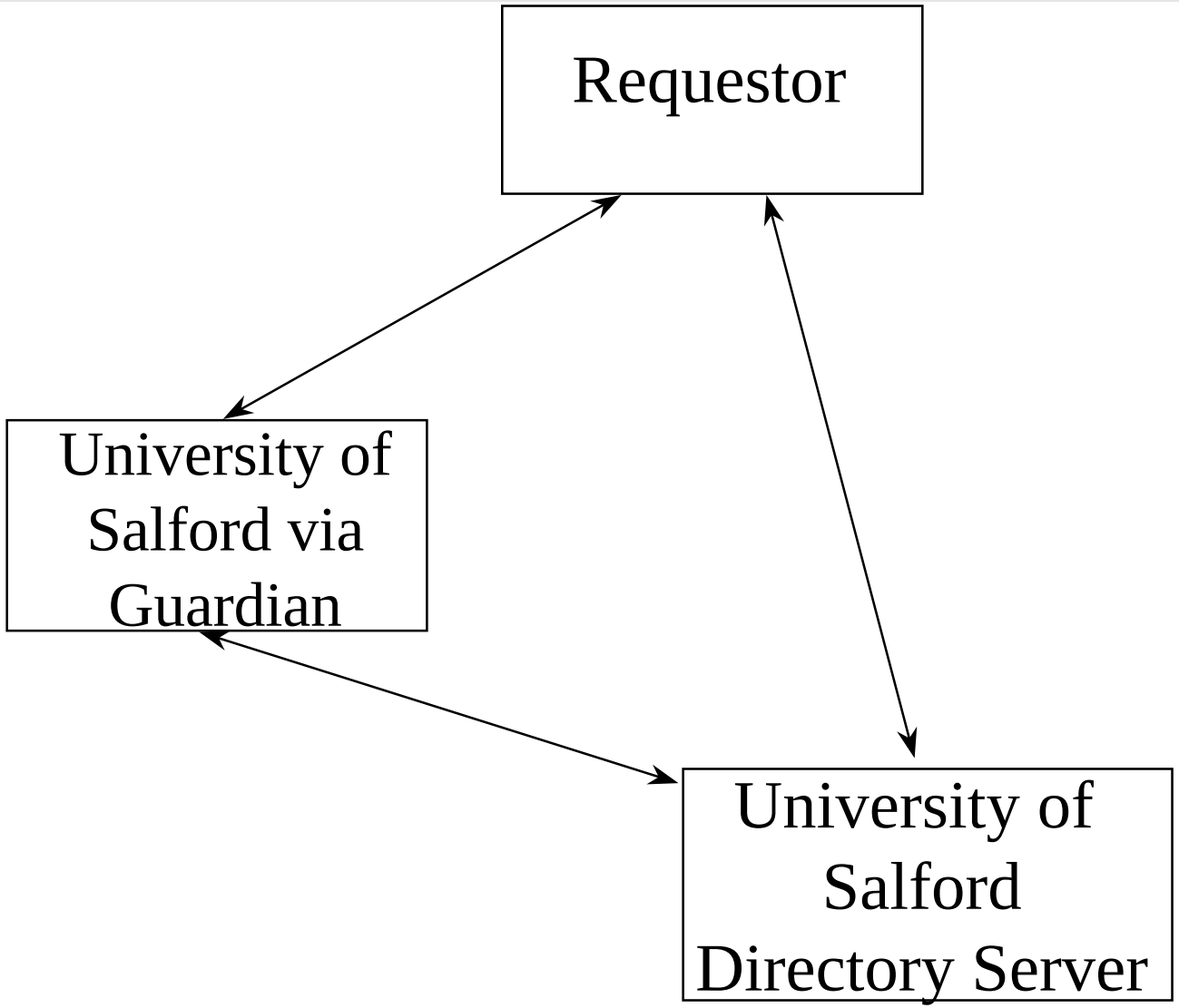
- *Servers - Guardian is configured with list of trusted directory servers from trusted domain*
- *Users who directly Bind to Guardian are assumed to be coming from opposite domain to where their request is directed, therefore no security risk*
- *Guardian will not (knowingly) relay within the same domain*

The Demonstration

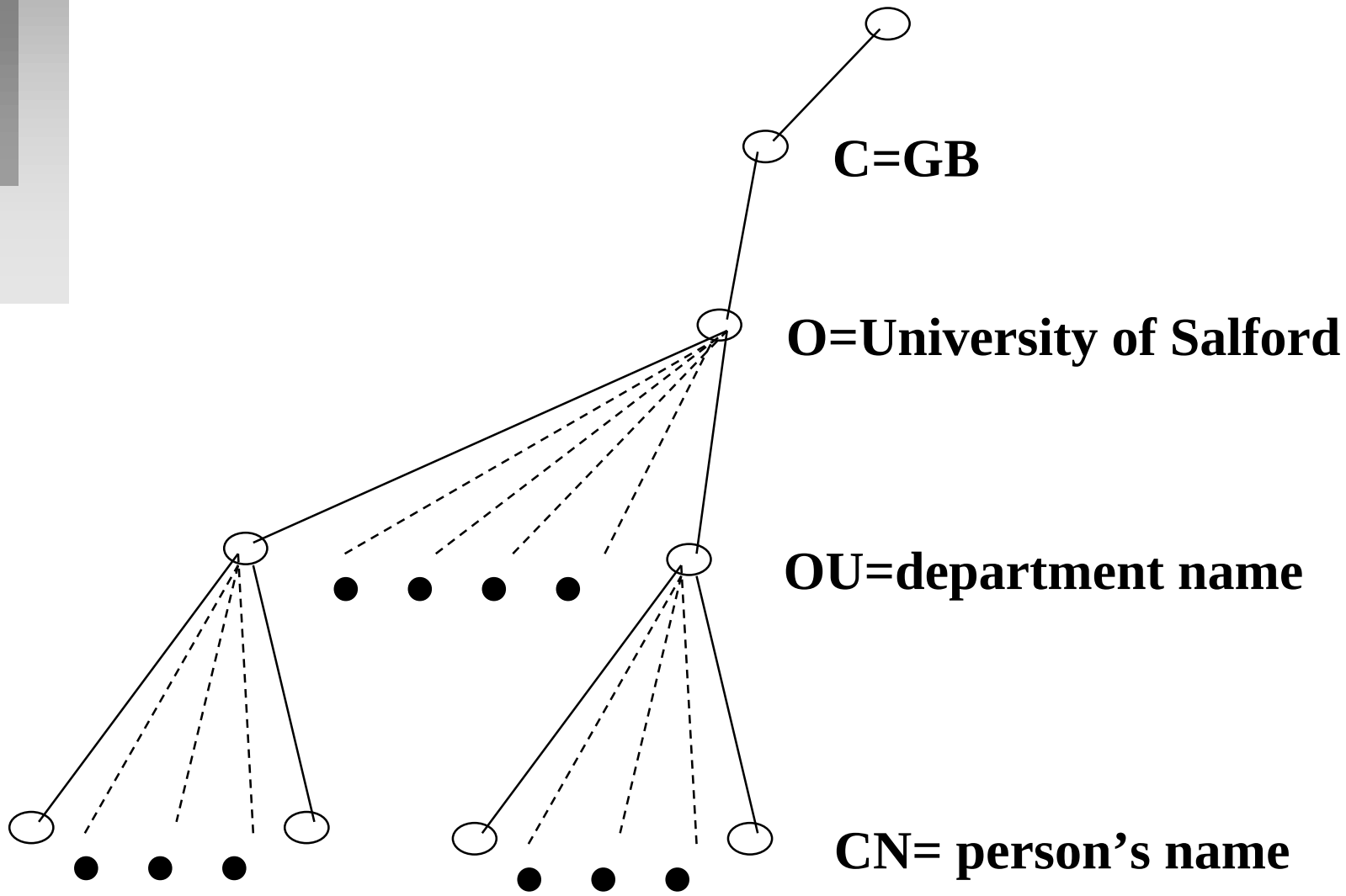
- *Salford directory directly visible*
- *Salford directory visible via Guardian*
- *publicly available at*

http://fw4.iti.salford.ac.uk/ice-tel/guardian/demo/

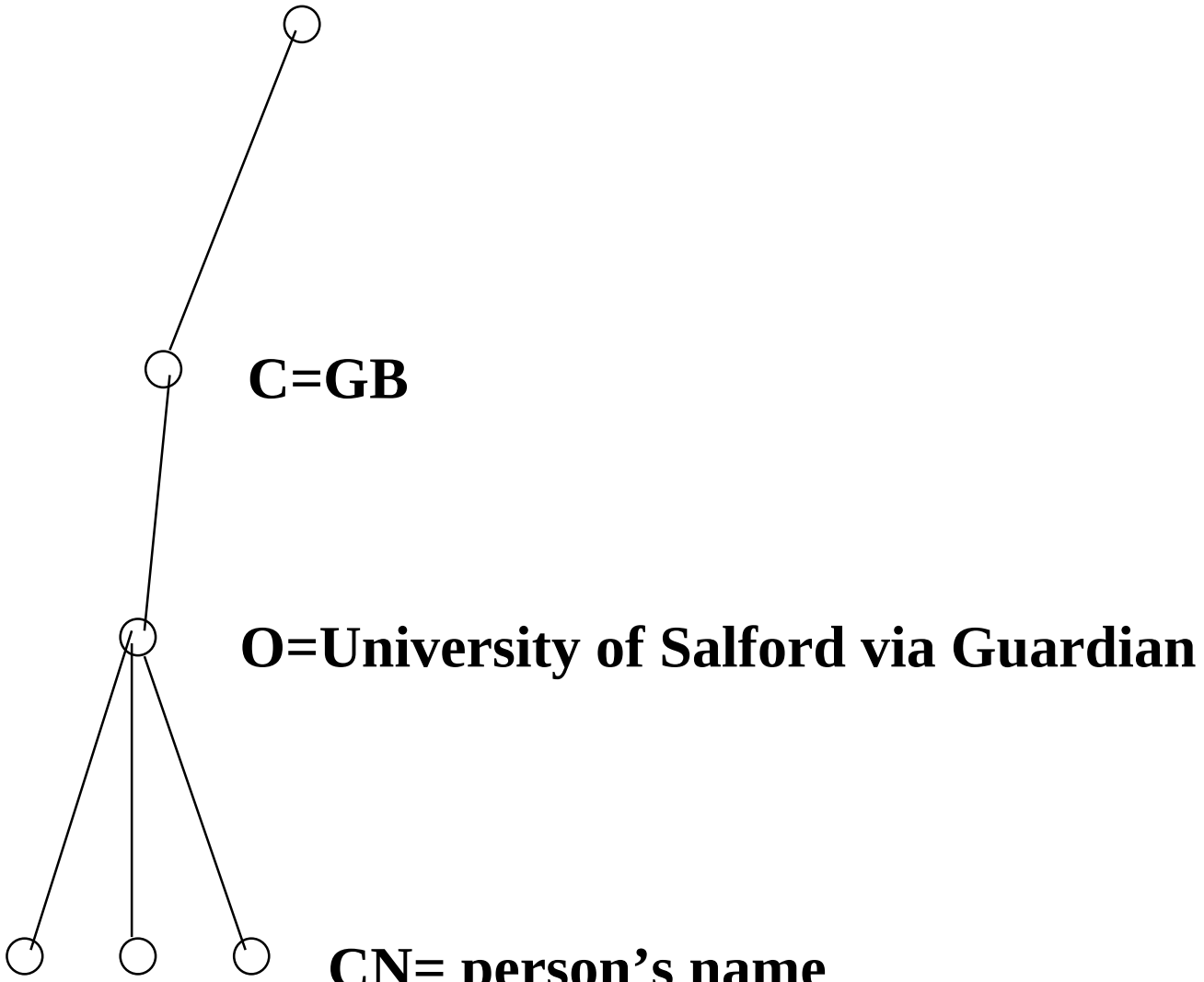
The Demo Configuration



The Salford DIT (directly visible)



Salford Directory Tree (visible via the Guardian)



Example Entry

- *Salford entry*
- *Common name = D W Chadwick*
- *Telephone number = 0161 295 5351*
- *Fax number = 0161 745 8169*

- *Salford via Guardian*
- *Common name = David Chadwick*
- *Telephone number = +44 161 295 5351*

Performance

- *800 Read and List measurements taken over several nights (8pm to 8am)*
- *Measured*
  - *direct connection to Salford DSA*
  - *connection via Guardian with filtering off*
  - *connection via Guardian with filtering on*
- *Network performance was biggest factor, with times varying from 0.4s to 361s*
- *Statistician advised us to discount List results over 5 secs, and Read results over 2 secs*

Read Operation

- *Read an entry directly or via the Guardian*
- *Effect of extra Guardian node (with no filtering) was degradation of 13% (0.78 →0.88s)*
- *Effect of Guardian with filtering was degradation of extra 5% (0.04s)*

List Operation

- *List a node with 1000 subordinates, filter but let them all pass*
- *Effect of extra Guardian node (with no filtering) was degradation of 13% (1.76s→1.98s)*
- *Effect of Guardian with filtering was degradation of extra 24% (0.6ms per entry)*