Secure X.500 Border Directory Proxy Server

K.M. GOERTZEL
Secure Solutions Development
Wang Government Services, Inc.
TEL: 703-698-5605
FAX: 703-689-4765
km.goertzel@wang.com

DIRECTORY SERVICE

Key Component of Distributed Computing

- Central repository: enterprise or global
- User names, email addresses, phone numbers, security credentials
- Supports email/MHS & PKI
- Can support directory-enabled user registration, personnel management, physical security

DIRECTORY TECHNOLOGIES

- *Legacy:* Document-based, proprietary databases
- LDAP directories (IETF RFC 1777) - Client-to-Server only, with referrals
- X.500 Directories (ITU) - Client-to-Server, Server-to-Server
- Directory firewalls - application-layer security filtering
- Meta-directories - synchronize multiple directories into common, central “logical” directory

BORDER DIRECTORY

- Defined in ACP 133
- Bridges boundary between internal network/directory and external network
- Makes subset of internal directory accessible to external network
- By acting as release gateway
- By acting as shared repository

BORDER DIRECTORY PHILOSOPHY

Internal Domain...

- Can define/restrict what information it will share
- Cannot dictate how external users handle that information once shared

BORDER DIRECTORY AS GATEWAY

- Allows "on-demand" release of internal information
- Information is managed/maintained only in internal directory
- Very small amount of information released at any given time (in response to DAP or DSP request)

BORDER DIRECTORY AS REPOSITORY

- May be driven by performance needs
- Performance needs outweigh fears of integrity loss
- Strong protections of trusted host desirable for Border Directory/Repository

BORDER DIRECTORY PROXY SERVER

on B3 XTS-300

- Directory information sharing among U.S. and CCEB, NATO, collaborative task forces, etc.
- Any organization to secure internal directory while allowing strictly controlled release of some info to external entities
- Creation of single "virtual" global directory of logically-integrated but physically separate directory subsets
- Owner control of directory information ensures integrity

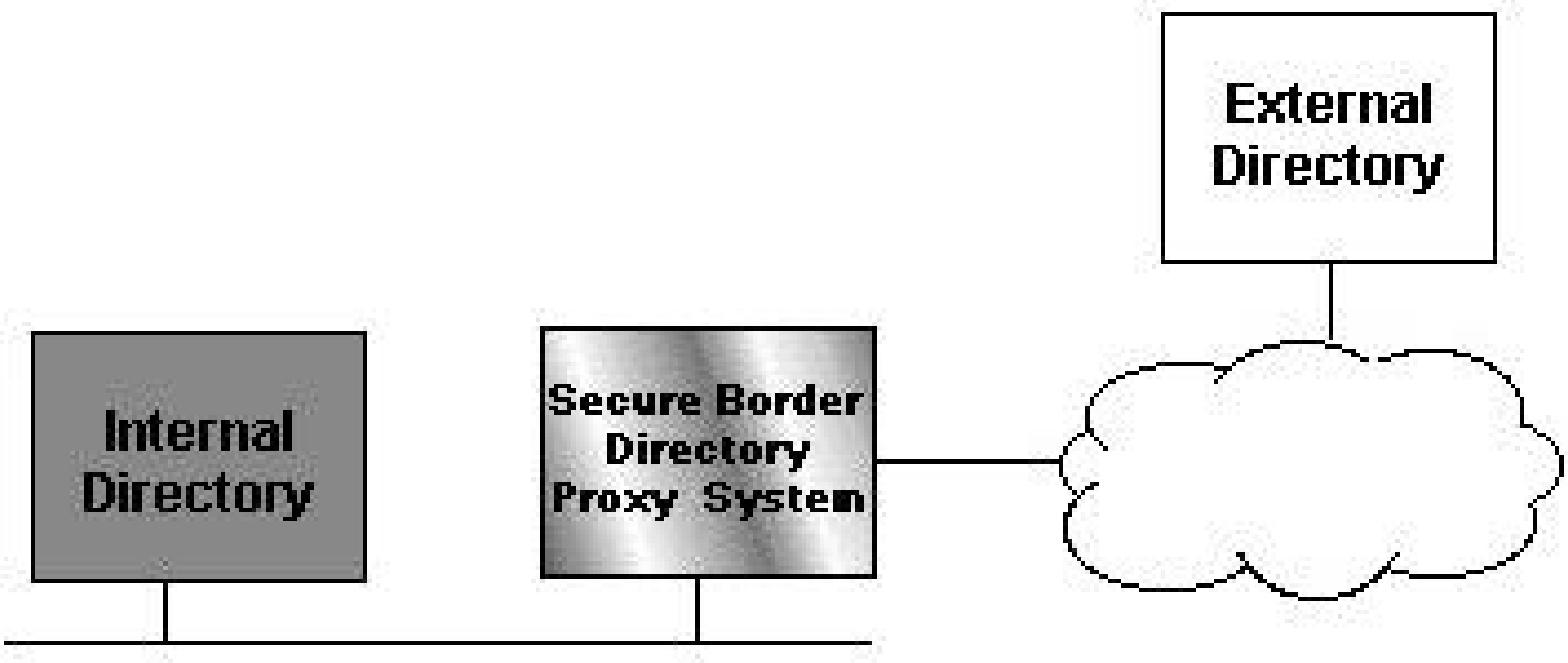
FUNCTIONALITY

- Secure X.500 interface/interconnection point between X.500 domains
- Trusted gateway controlling release of internal information
- Shared repository storing externally-accessible subset of internal information
- A combination of the two

CHAINING vs. SHADOWING

- Chaining requests directory information between external & internal DSAs
- Can limit response to external requests to as-needed basis
- Can maintain strict owner control of directory information
- Can restrict what requests can be chained out of domain, past Border Directory

OPERATIONAL ENVIRONMENT



BORDER DIRECTORY

as Trusted Gateway

- Would enforce release policy: set of rules specifying exactly which internal information will be shared externally
- Releasability based on "need to know" (discretionary) in most organizations
- Releasability further restricted by Mandatory Access Policy in system-high operations

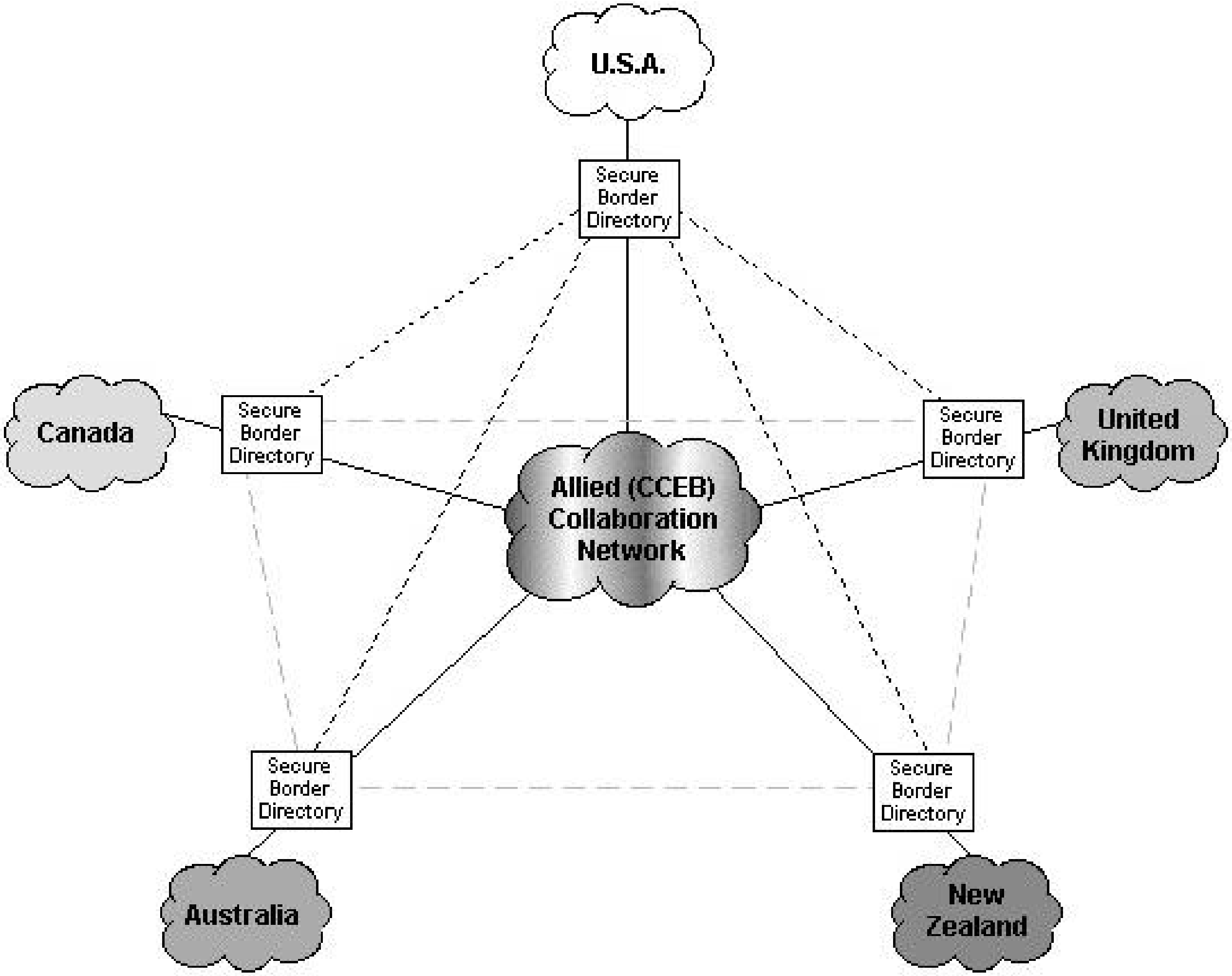
FILTERING CAPABILITIES

- Firewall filters: modify/delete ("sanitize") specific directory information in conformance with releasability policy
- Trusted guard filters:
  - validate correctness of firewall filters
  - enforce release strictly according to organization's mandatorysecurity policy
  - DII Guard X.500 filters
  - additional new trusted guard filters

CONCEPT OF OPERATION

- Separation of internal and external domains
- Strictly-controlled publication of directory information from internal to external
- Could be used for:
  - Directory info sharing among U.S. and its allies
  - Sharing info while maintaining "Community of Interest" separation
  - Inter-agency directory sharing
  - Directory-enabled applications/PKIs between banks, health care organizations, etc.

EXAMPLE OF OPERATION



INFORMATION FILTERING

Directory Firewall Filtering

- To prevent release of some information
- To modify/sanitize some information to ensure compliance with releasability policy, then release

DIRECTORY FIREWALL FILTERS

- *Attribute filter:* Rejects or sanitizes operation attributes that may or may not be requested by inside users querying outside directories
- *Knowledge Reference Filter:* Removes specified knowledge references, referal info, trace information, cross-references, etc. from operations
- *Shadowing Subset Filter:* Checks and possibly sanitizes to restrict shadowed subset to only releasable info
- *Releasability Authorization Attribute Filter:* Releases or denies shadowing of entry based on releasability "flag"

INFORMATION FILTERING

Trusted Guard Filtering

- To validate correctness of firewall filtering
- To validate other releasability criteria
- To ensure strict conformance with releasability policy, especially for Mandatory Access enforcement

TRUSTED GUARD FILTERS

Existing DII Guard X.500 Filters

- *Directory Protocol Filter:* Releases or denies on per-protocol/ per-flow basis (e.g., DSP chaining allowed only in one direction, i.e., internal-to-external)
- *Directory Operation Filter:*
  - Releases or denies based on of operation type
  - Requires certain operation types to be digitally signed and/or strongly authenticated
- *Distinguished Name (DN) Filter:*
  - Checks requester's DN for presence on Guard ACL
  - Ensures that requested operation type can be performed by requester's user class (access control group or role-based permission category)
- *Directory Information Shadowing Protocol (DISP) Filter:* Verifies correct configuration of shadowing agreement info

TRUSTED GUARD FILTERS

New Trusted Guard Filters

- *Override Access Control Filter:* Enforces more restrictive access control policy for data leaving domain vs. access to same data from within domain
- *Hide Internal User Information Filter:* Replaces internal originator information with Guard information on operations leaving domain
- *LDAP Version 3 support and filters:* TBD

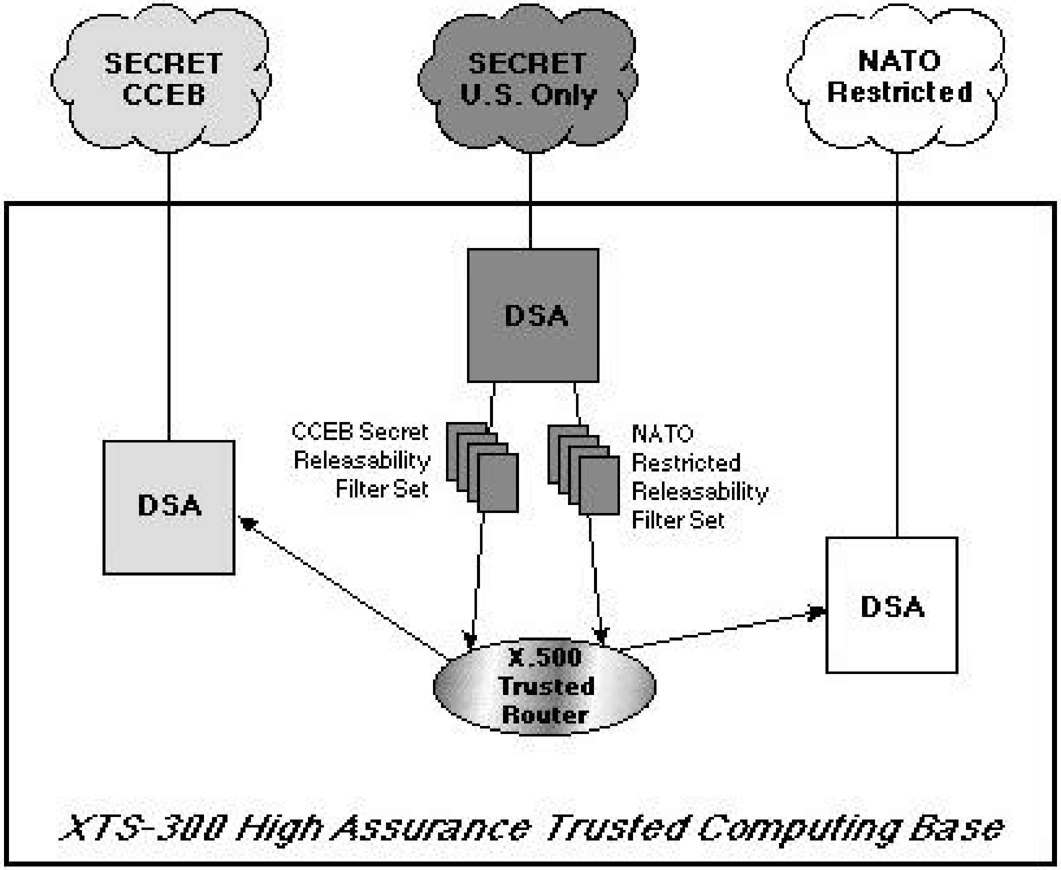
OTHER POLICY ENFORCEMENT

Possible Policies

- Ensure that no external directory can chain into internal network
- Enforce different access control policies based on which side of boundary the requester is on
- Enforce separate domain-based policies for different external users (e.g., different alliance members)

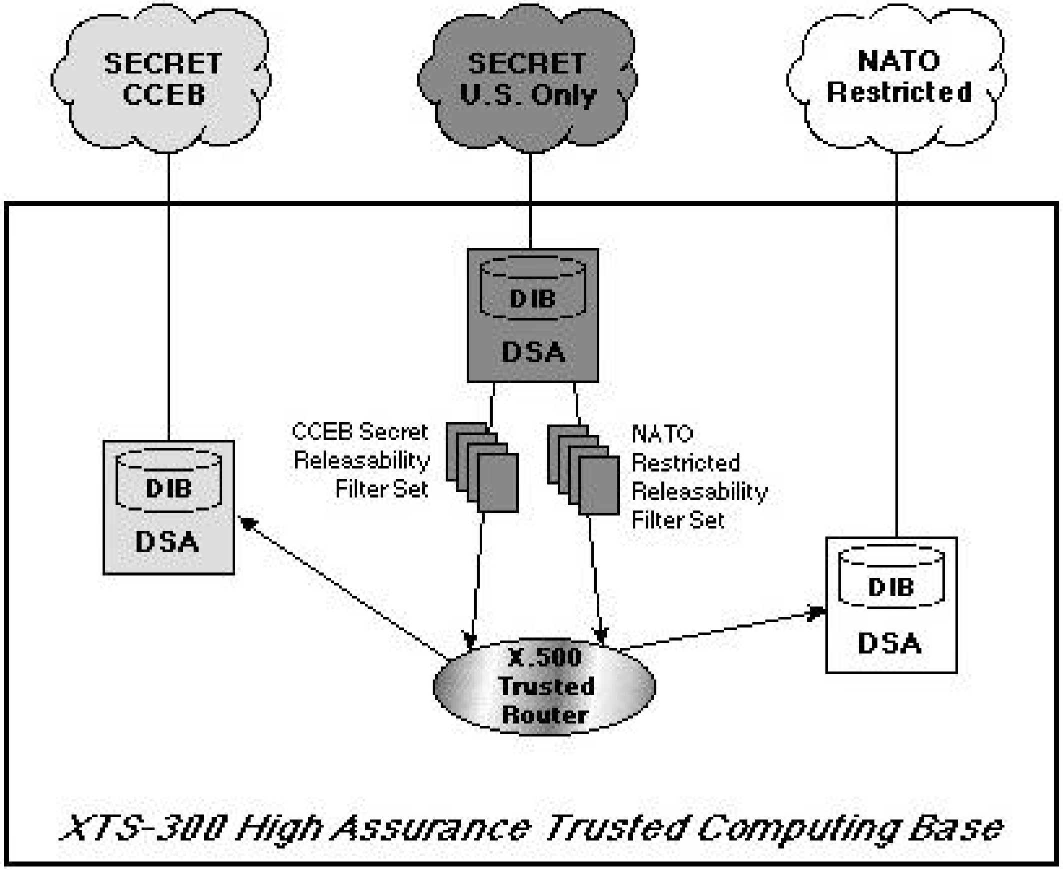
INTERNAL ARCHITECTURE

Phase 1: Trusted Gateway



INTERNAL ARCHITECTURE

Phase 2: Border Repository


SECRET
CCEB
SECRET
U.S. Only
NATO
Restricted
DIB
DSA
CCEB Secret
Releasability
Filter Set
NATO
Restricted
Releasability
Filter Set
DIB
DSA
DIB
DSA
X.500
Trusted
Router
XTS-300 High Assurance Trusted Computing Base