CSE 265: System and Network Administration

• Namespaces – the lists and directories in your environment
**CSE 265: System and Network Administration**

- Namespaces – the lists and directories in your environment
  - files in filesystem
  - account names in use
  - printers available
  - names of hosts
  - ethernet addresses
  - service-name/port-number lists
  - home directory location maps
Namespaces

- Some namespaces are flat
  - there are no duplicate names
- Some namespaces are hierarchical
  - duplicate items within different branches of a tree
- Need policies to govern namespaces
  - Ideally, written policies
    - Can become training for new SAs
    - Needed to enforce adherence to policy
Namespace policies

● Naming policy
  - What names are permitted/not permitted?
    - Technology – specific syntax
    - Organizational – not offensive
    - Standards compliance
  - How are names selected?
  - How are collisions resolved?
  - How do you merge namespaces?
    - Technological and political concerns
Namespace policies (2)

- Naming policy
  - How are names selected?
    - Formulaic
      - e.g., hostname: pc-0418; user-id: xyz210
    - Thematic
      - e.g., using planet names for servers; coffee for printers
    - Functional
      - e.g., specific-purpose accounts: admin, secretary, guest; hostnames dns1, web3; disk partitions /finance, /devel
    - Descriptive
      - e.g., location, object type (pl122-ps)
    - No method
      - Everyone picks their own, first-come first-serve
  - Once you choose one scheme, difficult to change – choose well!
Namespace policies (3)

- Comments on naming
  - Some schemes are easier to use than others
    - easier to remember/figure out, to type, etc.
  - Some names imply interesting targets
    - secureserver, sourcecodedb, accounting, etc.
    - avoid exceptions to formulaic names
  - Formulaic names suggest problems when incomplete
    - server1, server2, server4, server7
  - Sometimes helpful when desktop matches user's name
    - Assuming user wants to be easily identified
Namespace policies (4)

• Protection policy
  – What kind of protection does the namespace require?
    • password list
    • UIDs
    • login IDs, e-mail addresses
  – Who can add/delete/change an entry?
    • Need backups or change management to roll back a change
Namespace policies (5)

- Longevity policy
  - When are entries removed?
    - after IP address not used for months
    - contractor ID each year
    - student accounts a year after graduation
    - employee accounts the day they leave
  - Functional names might be exceptions
    - sales@company.com
    - president@university.edu
Namespace policies (6)

- **Scope policy**
  - Where is the namespace to be used?
    - How widely (geographically) shall it be used?
      - Global authentication is possible with RADIUS
      - NIS often provides a different space per cluster
    - How many services will use it? (thickness)
      - ID might serve for login, email, VPN, name on modem pools
      - Across different authentication services
        - ActiveDirectory, NIS, RADIUS (even with different pw)
  - What happens when a user must span namespaces?
    - Different IDs? Confusing, lead to collisions
  - Single flat namespace is appealing; not always needed
Namespace policies (7)

- **Consistency policy**
  - Where the same name is used in multiple namespaces, which attributes are also retained?
    - E.g., UNIX name, requires same (real) person, same UID, but not same password for email, login

- **Reuse policy**
  - How soon after deletion can the name be reused?
    - Sometimes want immediate re-use (new printer)
    - Sometimes long periods (prevent confusion and old email from being sent to new user)
Namespace Management

- Namespace change procedures
  - Need procedures for additions, changes, and deletions
  - Likely restricted to subgroup of admins
  - Documentation can provide for enforcement, training and step-by-step instruction

- Namespace management
  - Should be centralized
    - Maintain, backup, and distribute from one source
    - Difficult to enforce uniqueness when distributed
  - Centralization provides consistency