SunSoft
A Sun Microsystems Company

Public Filehandles

- Every use of a filehandle is now checked.
- Filehandles can now be “public”.
- No advantage in obtaining a filehandle “illegally”.

SunSoft
A Sun Microsystems Company

Share Syntax

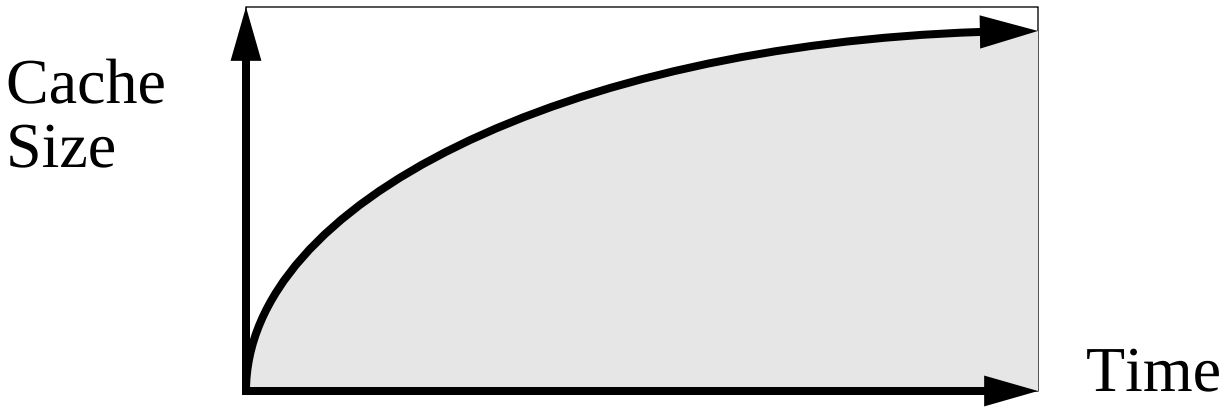
- Lists bound to previous flavor list

```
auth=kerb,rw=pop:pip,auth=unix,ro=pcgroup

auth=secure:kerb,rw

auth=secure:kerb,rw,auth=unix,ro
```

SunSoft
A Sun Microsystems Company

Kernel Cache

- Calls to authd typically at mount time, or any NFS request after a server reboot.
- For each export, caches client address, flavor & permission.
- Cached entries flushed only if filesystem unshared or if share information changes or upon VM request.



SunSoft
A Sun Microsystems Company

Mountd & Authd

- Two RPC services in the same daemon.
- Share cached export information
- Multi-threaded.
  - **Easy to dispatch a thread per request:**
    `rpc_control(RPC_SVC_MTMODE_SET, &rpc_svc_mode)`
  - **Need mutex & readers/writers lock protection for shared data structures.**
  - **Look out for static data, e.g. `strtok()`**

SunSoft
A Sun Microsystems Company

Authd (cont)

- Authd converts client's address to hostname
- Uses export path to find export information
- Checks client against export information making netgroup calls to name service if necessary.
- Very similar to existing code in mount daemon - so.....

SunSoft
A Sun Microsystems Company

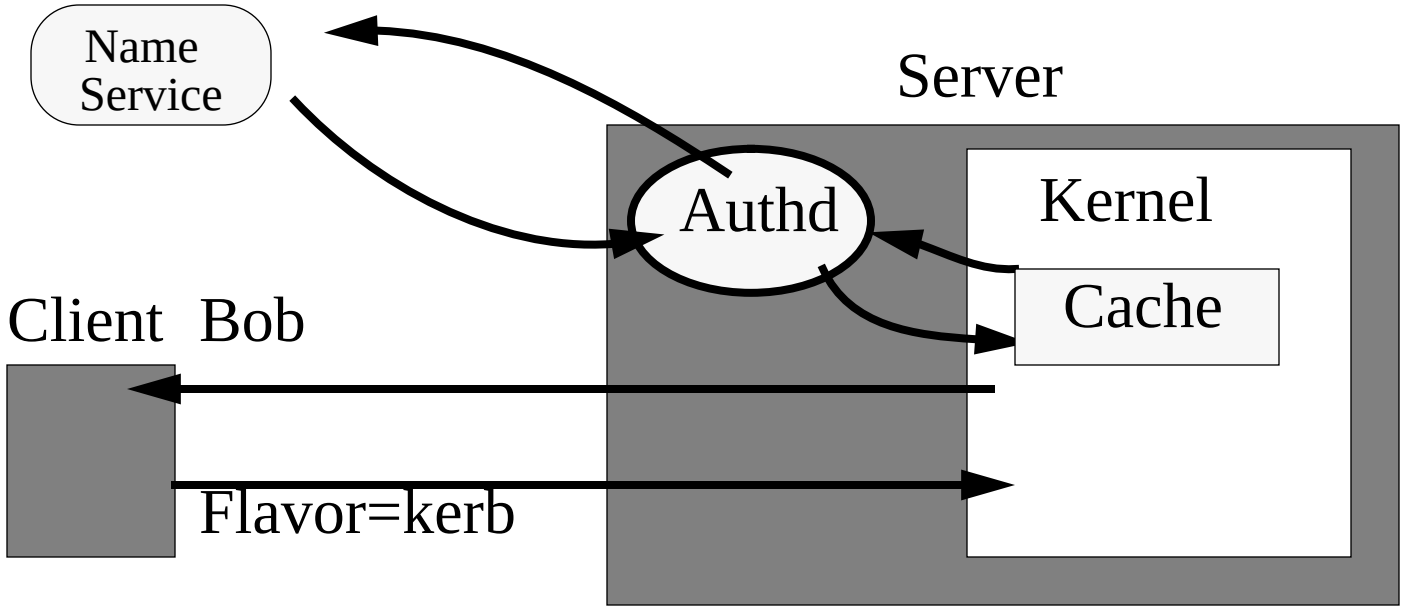
Authd

- Services request from kernel:
  - **Exported path, e.g. “/export/home”**
  - **Client’s address, e.g. “129.144.40.3”**
  - **Client’s flavor, e.g. “3”**
- Replies either:
  - **No access**
  - **Read-only access**
  - **Read-write access**

SunSoft
A Sun Microsystems Company

Request Checking

- A netgroup check on every request is too slow.
- Cannot cache the whole netgroup in the kernel
- Have kernel call a user-level auth service and cache the result.



SunSoft
A Sun Microsystems Company

Need Dynamic Authentication

- Authorized flavor depends on client
- Need to check every NFS request from client against list of authorized flavors for the client
- Static mount-time checking is inadequate and insecure.
- **Wow**! Check *every* NFS request ?
  - **What about netgroups ?**

SunSoft
A Sun Microsystems Company

Static Client Authentication

- Client transmits mount request
- Mount daemon checks client against host list or netgroup
- Returns filehandle or “permission denied”
- Security problem:
  - **File handles can be guessed.**
  - **File handles can be snooped.**

SunSoft
A Sun Microsystems Company

Multiple Flavors: Who ?

- Two choices:
  - **Treat all clients equally**

```
share -o auth=secure:kerberos,rw=group /stuff
```

  - **Supported flavors depend on client**

```
share -o auth=secure,rw,auth=unix,rw=pcnfs /stuff
```

  - **We went with the second choice.**
- Different clients may get different flavor lists for the same filesystem.

SunSoft
A Sun Microsystems Company

Mount Protocol: V2 & V3

- V2 Mount request:
  - **Returns 32 byte file handle**
- V3 Mount request:
  - **Returns V3 file handle and authentication list.**
  - **Auth list is list of acceptable RPC auth flavors**
  - **Auth list is ordered. First in list is “most preferred”.**

Multiple Flavors per Export

Brent Callaghan

- Work in Progress!
- Authentication with V2 and V3
- Multiple flavor requirement
- Dynamic address checking
- Changes