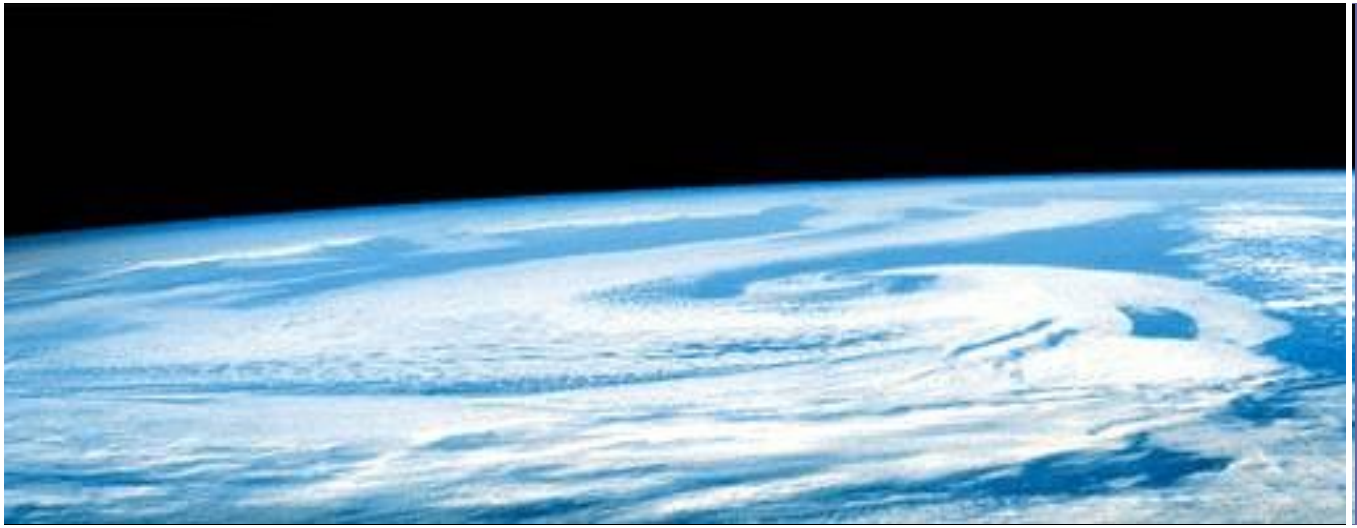
Comunicaciones Seguras en el Entorno Operativo Solaris 8

Sun microsystems



Alejandro Novo
SES Consultor Preventa
Manuel Guerreiro
SES Responsable I+D de productos

Seguridad en el Entorno Operativo Solaris 8

OpenBoot PROM Security Modes

- Firmware password protection
- **`secur ty mode`**
  - options: none, command, full
- **`secur ty password`**
  - holds/resets the prom password
- **`secur ty #badlo  n`**
  - holds the number of incorrect attempts
- NOTICE: forgotten password = new PROM!

Login

- Begin session, id / password
- Uses PAM facility
- drops tty after five failed attempts
- records successful and failed logins
- runs system & user startup scripts
- /etc/default/login : sets global options
  - ✔ ULIMIT, CONSOLE, PASSREQ, PATH, UMASK, SYSLOG, SLEEPTIME, RETRIES, PASSLENGTH

Pluggable Authentication Module (PAM)

- Modular framework for authentication:
- Used by: login, rlogin, su, dtlogin, rsh
- Modules: unix, ldap, krb5, ami, smartcard
- Rules: /etc/pam.conf
  - service types: auth, accnt mgmt, session mgmt, password mgmt
  - control flags: (behavior stacking) requisite, required, optional, sufficient
  - configurable: pass one or more modules

Basic Security Module (Audit)

- Detect potential security breeches
  - reveal suspicious or abnormal patterns of usage
  - trace suspect actions back to a specific user
  - a deterrent, users know their being watched
- Many audit classes:
  - file creation/update/deletion/attr changes
  - user login/logout
  - system calls, ioctl()'s, object operations
  - process operations, network events

Basic Security Module (Accounting)

- Track connections
  - user login
  - system reboots
  - how tty lines are being used
- Process tracking
  - UID, GID, command, time (start, duration)
  - CPU and memory usage
  - command executed
- Disk usage

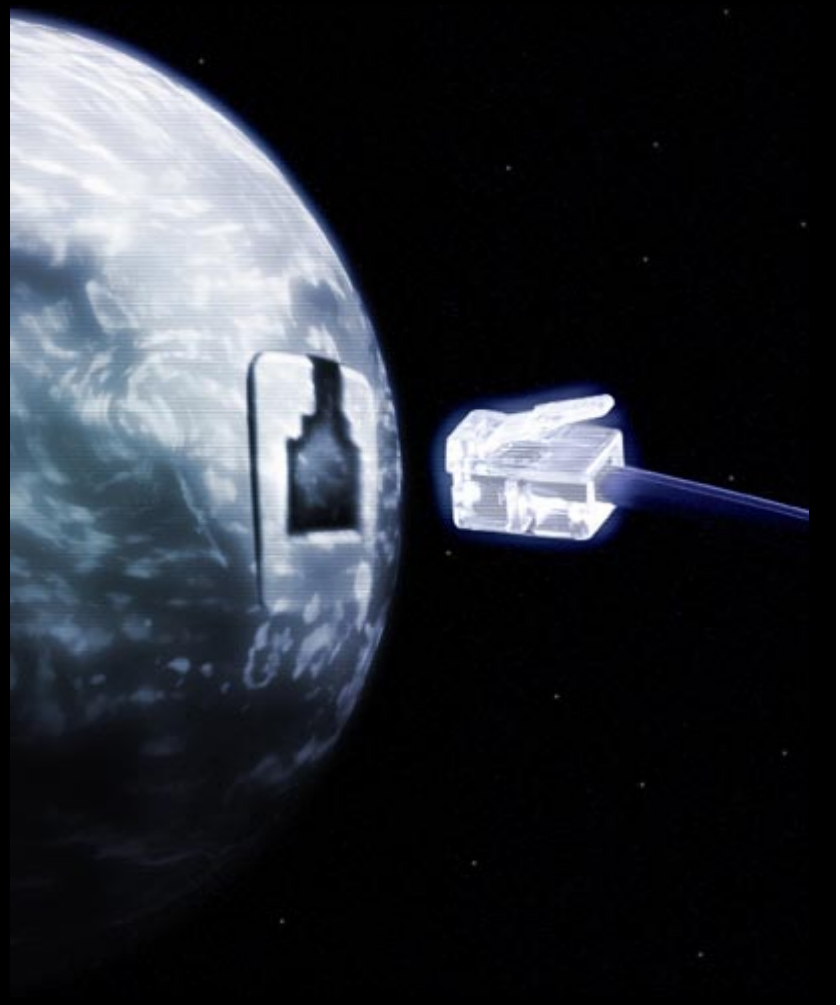
RBAC

- Role-Based Access Control
- Assign limited admin capabilities to users
  - Authorization: grant access
  - Execution Profiles: associate auth with cmds
  - Roles: set of admin tasks
- Audit classes for users and roles
- Supported in name switch
- API to create privileged functions
- **`Auths(1), prof les(1), roles(1)`**

Stack Execution

- **`/etc/system :`**
  - **`set noe ec_user_stack = 1`**
- Makes the stack non executable
- Reduces risk of buffer overflow attacks
- Solaris 2.6 or greater
- Platforms: sun4u, sun4m, sun4d
- Default mode is "disabled", value = 0

Seguridad en el Entorno de Red Solaris 8



ARP Defenses

- Delete entries manually using arp -d host_entry
- Entries will time out and be deleted by the system
  - ndd -set /dev/arp arp_cleanup_interval 60000
  - ndd -set /dev/ip ip_ire_arp_interval 60000

Broadcast attack (smurf)

- ICMP broadcast request may initiate a denial of service
  - ndd set /dev/ip ip_respond_to_echo_broadcast 0
- IP multicast (IPv6)
  - ndd -set /dev/ip ip6_respond_to_echo_multicast 0
- Timestamp Request Broadcast
  - ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
- Address Mask Broadcast
  - ndd -set /dev/ip ip_respond_to_address_mask_broadcast 0

Redirect errors

- Avoid a denial service attack if the newly specified router is not a router at all
  - ndd -set /dev/ip ip_ignore_redirect 1
- Same for IPv6
  - ndd -set /dev/ip ip6_ignore_redirect 1

IP forwarding

  - ndd -set /dev/ip ip_forwarding 0
- IPv6
  - ndd -set /dev/ip ip_forwarding 0
- Strict Destination multihoming: Prevents packet spoofing on non-rounting multihomed systems
  - ndd -set /dev/ip ip_strict_dst_multihoming 1
- IPv6
  - ndd -set /dev/ip ip6_strict_dst_multihoming 1

SYN Flood attacks

- Takes advantage of the TCP handshake protocol. The server will reach its maximum of partially connections. Increase the queue's default value to 4096
  - ndd -set /dev/tcp tcp_conn_req_max_q0 4096
- Connection Exhaustion Attacks. Increase the value to 1024
  - ndd -set /dev/tcp tcp_conn_req_max_q 1024

IPSec

- Protection for IP datagrams
- Provides confidentiality, integrity and authentication
- Authentication and encryption mechanism
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- Support added to **`fconf`** and **`snoop`**
- Implementation may be transparent to app

Alejandro Novo

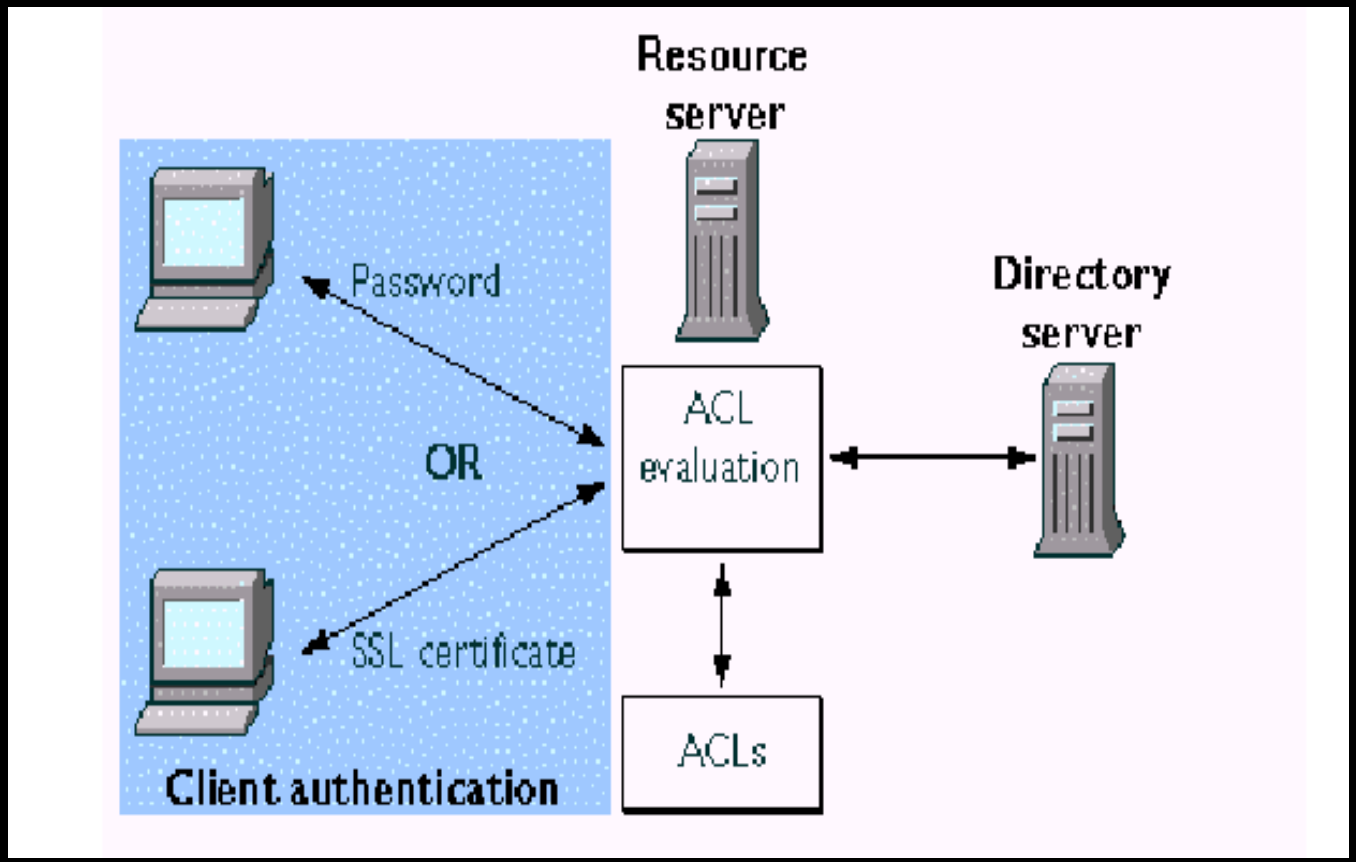
alejandro.novo@sun.com

Sun microsystems

PKIs

- Types of authentication:
  - Knowledge based: passwords
  - Token based: certificates
- one-time password authentication using PKI infraestructure and LDAP
- Web server example

PKIs


Resource server
Password
OR
SSL certificate
Client authentication
ACL evaluation
ACLs
Directory server

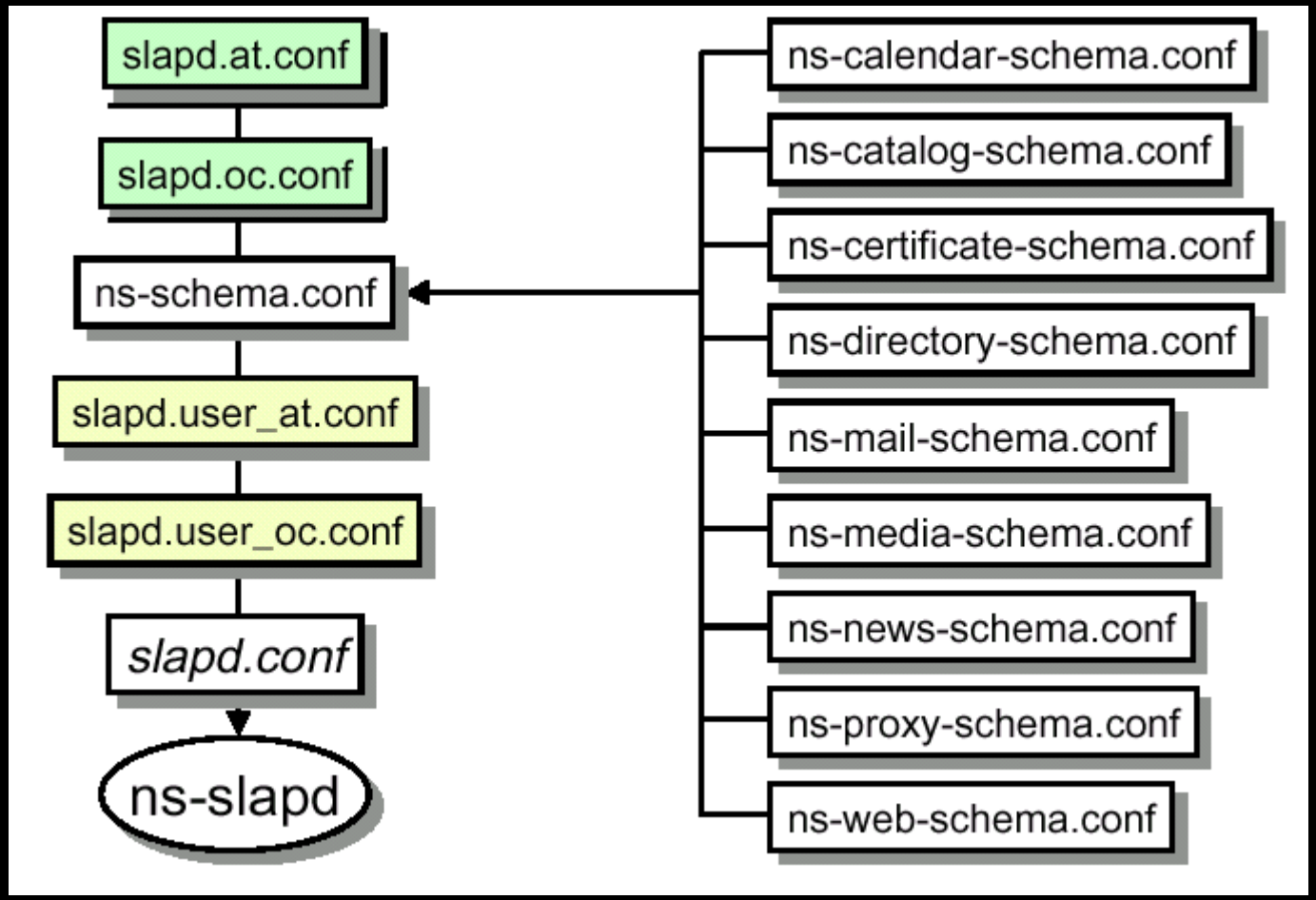
PKIs

- LDAP requirements for one-time password and PKIs
  - Directory schema CA
    - cA Certificate (required)
    - certificateRevocationList
    - authorityRevocationList
    - crossCertificatePair

PKIs

- LDAP requirements for one-time password and PKIs
  - inetOrgPerson
    - userCertificate
    - userSMimeCertificate
    - userPKCS12

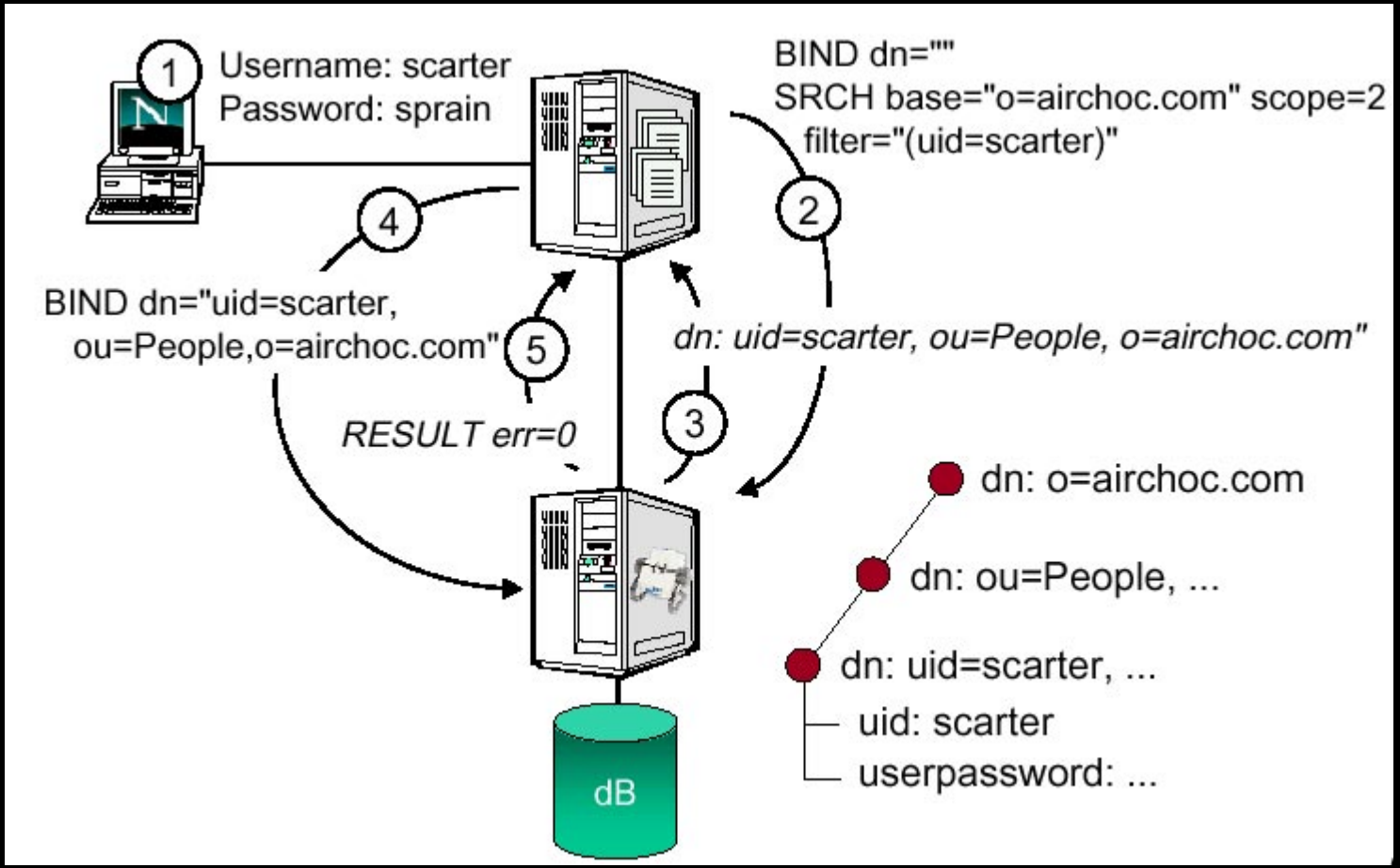
PKIs


slapd.at.conf
slapd.oc.conf
ns-schema.conf
slapd.user_at.conf
slapd.user_oc.conf
slapd.conf
ns-slapd
ns-calendar-schema.conf
ns-catalog-schema.conf
ns-certificate-schema.conf
ns-directory-schema.conf
ns-mail-schema.conf
ns-media-schema.conf
ns-news-schema.conf
ns-proxy-schema.conf
ns-web-schema.conf

PKIs

- User password access: traditional mode
  - User submits UID and password to the server
  - Server binds to directory server and performs an anonymous search for the UID
  - Directory server returns DN
  - Server attemps to bind the directory using DN and password
  - If bind succees the user is authenticated

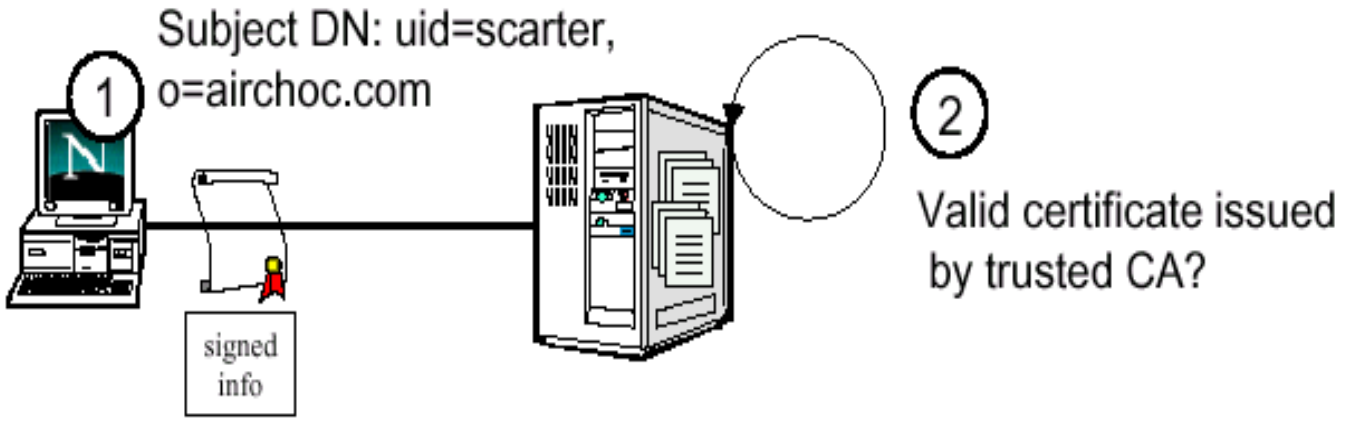
PKIs


1
Username: scarter
Password: sprain
BIND dn=""
SRCH base="o=airchoc.com" scope=2
filter="(uid=scarter)"
2
4
BIND dn="uid=scarter,
ou=People,o=airchoc.com"
5
dn: uid=scarter, ou=People, o=airchoc.com"
RESULT err=0
3
dn: o=airchoc.com
dn: ou=People, ...
dn: uid=scarter, ...
uid: scarter
userpassword: ...
dB

PKIs

- Strong authentication
  - User requests an SSL connection
  - Server authenticates itself to the user and requests a client certificate
  - Client sends the certificate and a proof that it owns the private key
  - Server checks who signed the certificate (trusted CA)
  - If the CA is trusted and the signature is valid -> OK

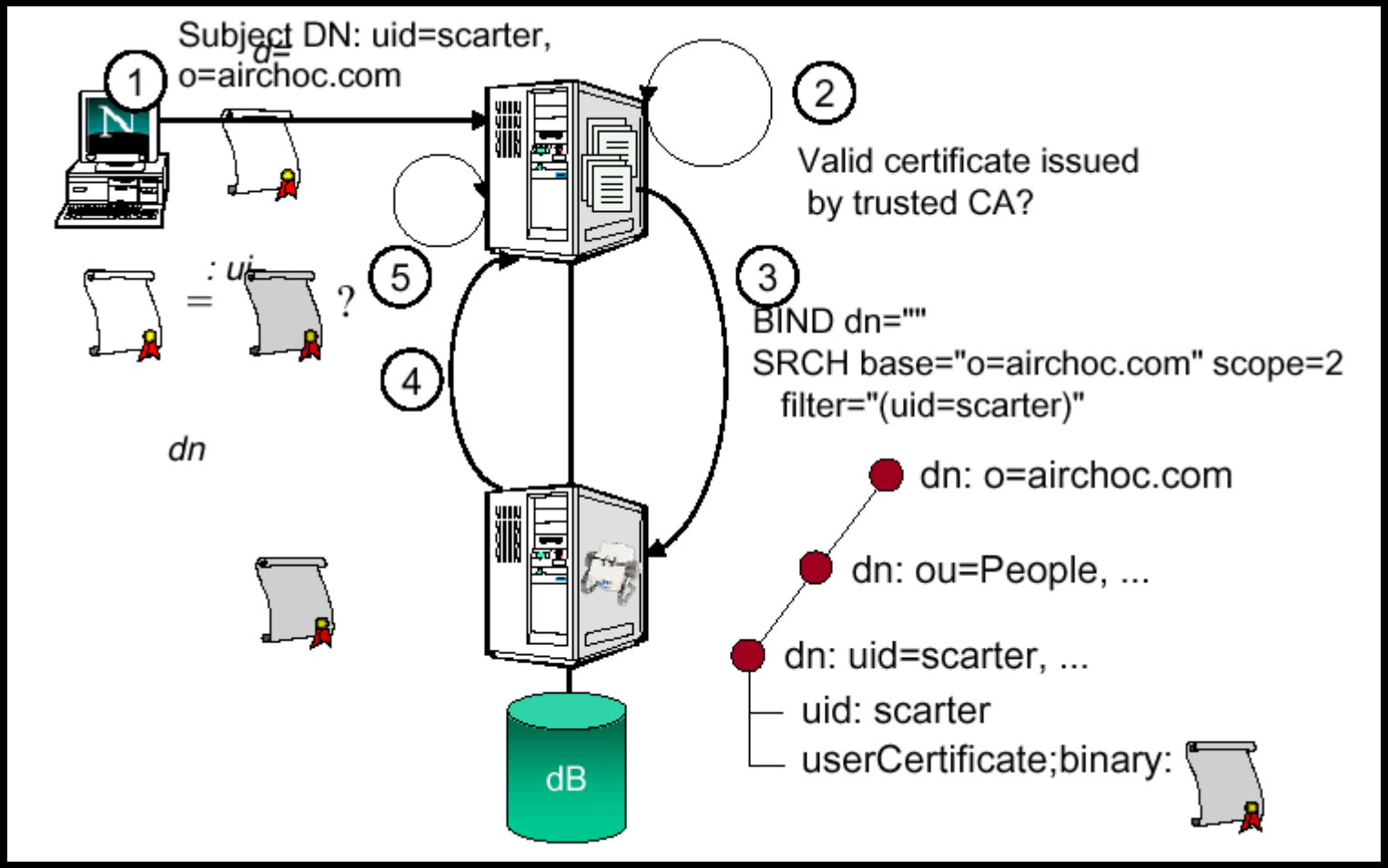
PKIs


Subject DN: uid=scarter,
o=airchoc.com
1
signed
info
2
Valid certificate issued
by trusted CA?

PKIs

- Strong authentication with certificate verification
  - As in the previous case, user connects using SSL
  - Server uses the information from the user's subject DN to make a directory search for the user's record
  - If found it reads the userCertificate attribute
  - Server compares the certificate presented by the user with the certificate retrieved from the directory
  - If they are the same, the user is authenticated

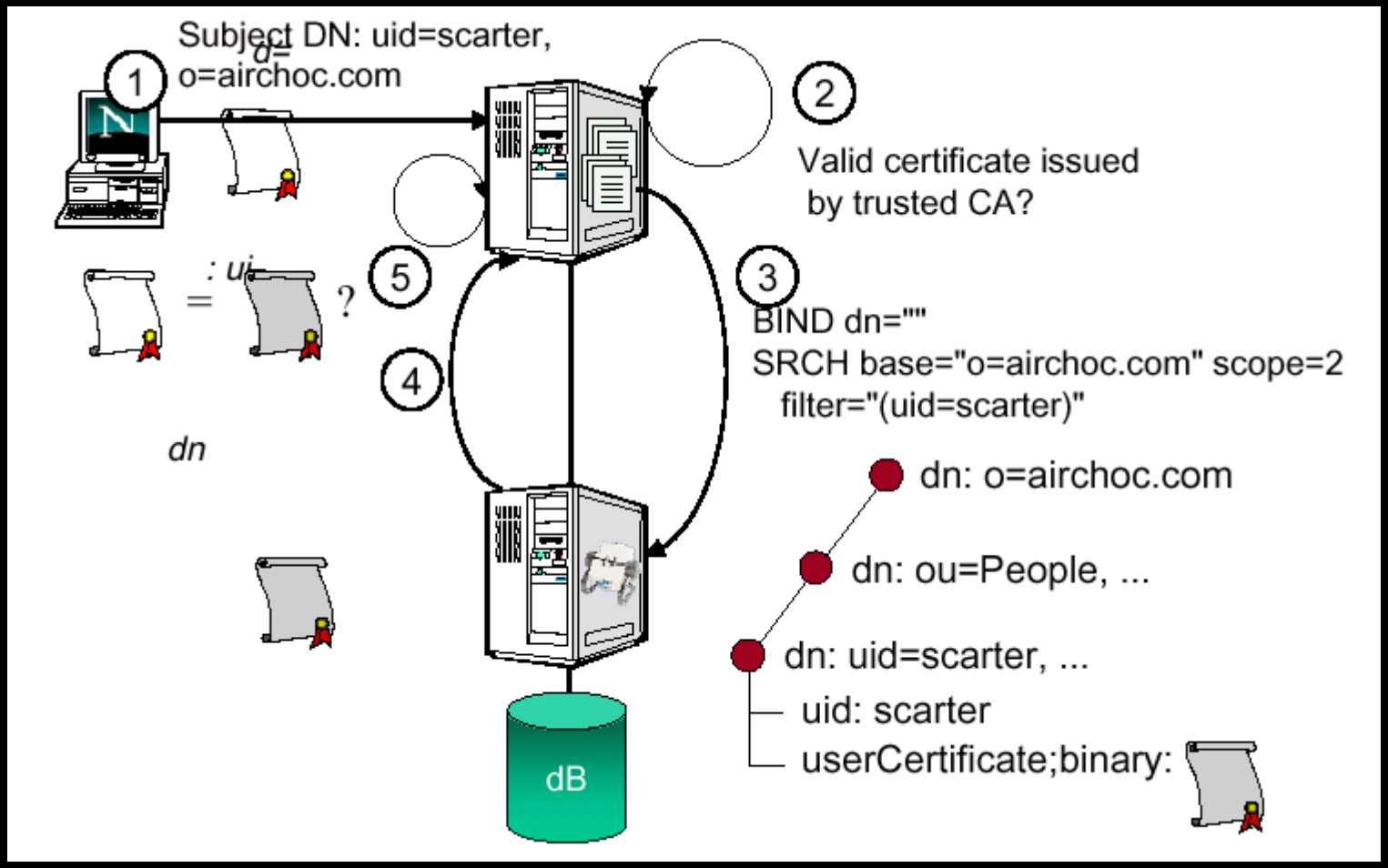
PKIs


Subject DN: uid=scarter,
o=airchoc.com
1
2
Valid certificate issued
by trusted CA?
3
BIND dn=""
SRCH base="o=airchoc.com" scope=2
filter="(uid=scarter)"
4
5
dn
dB
dn: o=airchoc.com
dn: ou=People, ...
dn: uid=scarter, ...
uid: scarter
userCertificate;binary:

PKIs

- Advantages:
  - Certificates are revoked inmediately
  - iPlanet CMS allows the users to enroll straight using LDAP user name and password by an SSL encripted conection
  - One-time password
  - Passwords don't travel across the network

PKIs


Subject DN: uid=scarter,
o=airchoc.com
1
2
Valid certificate issued
by trusted CA?
3
BIND dn=""
SRCH base="o=airchoc.com" scope=2
filter="(uid=scarter)"
4
5
dn
dB
dn: o=airchoc.com
dn: ou=People, ...
dn: uid=scarter, ...
uid: scarter
userCertificate;binary:

Manuel Guerreiro

manuel.guerreiro@sun.com

Sun microsystems