Announcements

Tomorrow

- *Authentication in Distributed Systems: Theory and Practice*, Butler Lampson, Martin Abadi, Michael Burrows, Edward Wobber
  - Butler Lampson (MSR) - He was one of the designers of the SDS 940 time-sharing system, the Alto personal distributed computing system, the Xerox 9700 laser printer, two-phase commit protocols, the Autonet LAN, and several programming languages.
  - Martin Abadi (Bell Labs)
  - Michael Burrows, Edward Wobber (Compaq SRC)

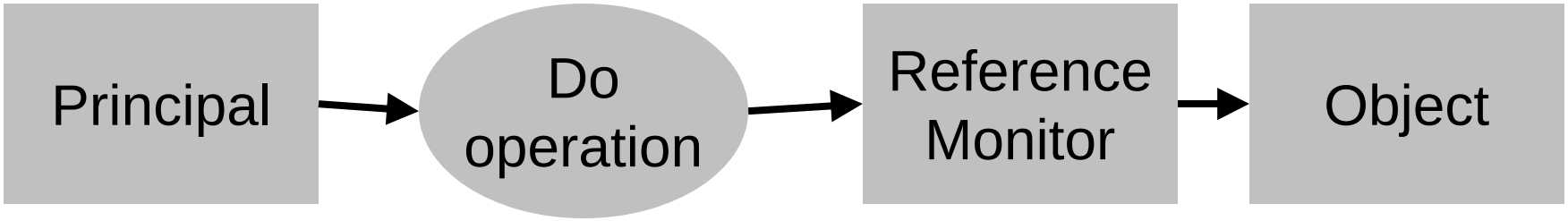
Authentication

- Method for obtaining the source of the request
  - Who said this?
- Interpreting the access rule – authorization
  - Who is trusted to access this?
  - Access control list (ACL)
- Easier in central servers because the server knows all the sources

Distributed authentication (ala searchget)

- Autonomy: Request might come through a number of untrusted nodes. So “Surendar” is not the same as “Surendar working through @Home network”
- Size: Multiple authentication sources
- Heterogeneity: Different methods of connecting
- Fault-tolerance: Parts of the system may be broken

Access Control Model

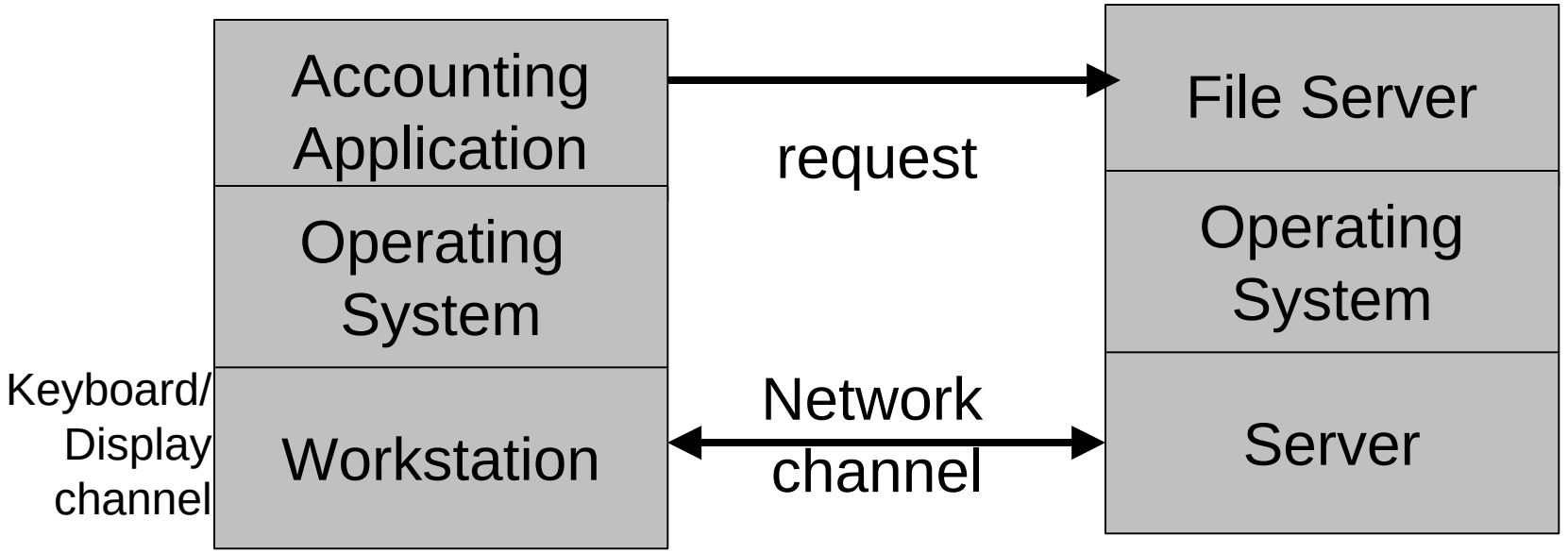


- Principal: source for requests
- Requests to perform operations on objects
- Reference monitor: a guard for each object that examines each request for the object and decides whether to grant it
- Objects: Resource such as files, processes ..

Trusted Computing Base

- A small amount of software and hardware that security depends upon
  - You have to trust something
- Possible to obtain trusted statements from untrusted source
  - end-to-end argument
- TCB typically includes:
  - Operating system
  - Hardware
  - Encryption mechanisms
  - Algorithms for authentication and authorization

Example scenario



- One user, two machines, two operating systems, two subsystems, and two channels
- All communication over channels (no direct comm.)

Encryption channels

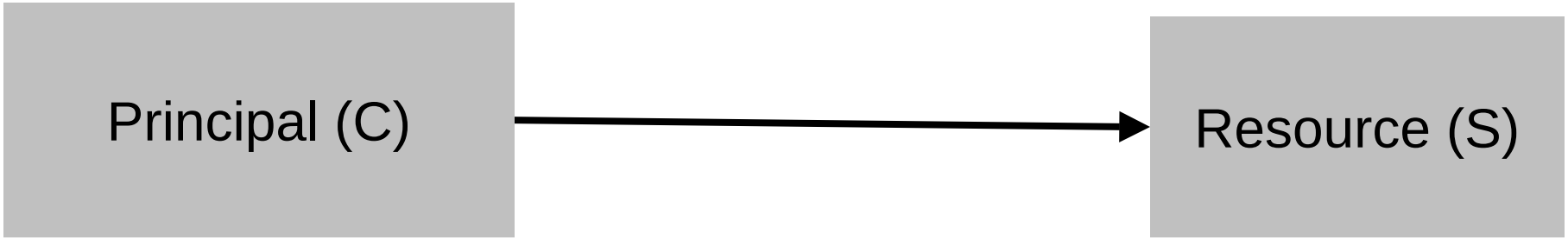
- Shared vs public key cryptography
  - Shared is fast
  - Public key systems are easy to manage
  - Hybrids offer best of both worlds (e.g. SSL)

- Broadcast encryption channels
  - Public key channel is broadcast channel: you can send a message without knowing who will receive it
  - Shows how you can implement broadcast channel using shared keys
- Node-to-node secure channels

Principals with names

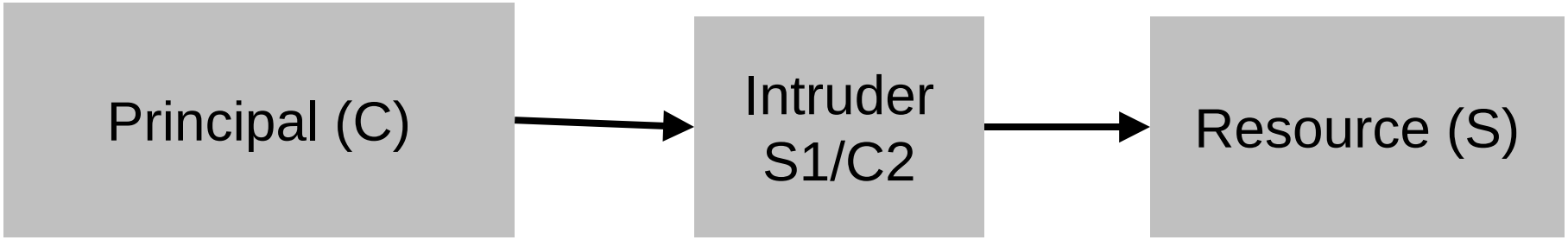
- When requests arrive on a channel it is granted only if the channel speaks for one of the principals on the ACL
  - Push: sender collects A's credentials and presents them when needed
  - Pull: receiver looks up A in some database to get credentials for A

Man in the middle attach



1. C requests server certificate from S
2. S sends server certificate with Spublic to C
3. C verifies validity of Spublic
4. C generate symmetric key for session
5. C encrypts Csymmetric using Spublic
6. C transmits Csymmetric(data) and Spublic(Csymmetric) to S

Man in the middle attach



1. C requests server certificate from S
2. S sends server certificate with Spublic to C
3. C verifies validity of Spublic
4. C generate symmetric key for session
5. C encrypts Csymmetric using Spublic
6. C transmits Csymmetric(data) and Spublic(Csymmetric) to S

– Certification authorities

Certification Authority

- Difficult to make system highly available and highly secure
  - Leave CA offline, endorse certificates with long timeout
  - Online agent highly available, countersign with shorter timeout
  - Cache while both timeouts fresh
  - Invalidation at cache granularity
- Simple Certification Authority
  - CA speaks for A and is trusted when it says that C speaks for A
    - Everyone trusts CA to speak for named principal
    - Everyone knows public key of CA
- Pathnames and Multiple authorities
  - Decentralized authority, Parents cannot unconditionally speak for children

Groups

- Each principal speaks for the group
- Group membership certificates
  - Impossible to tell the membership

- Alternate approach is to distribute certificates to all principals
  - Revocation?

Roles and programs

- Role that a user play; a normal user or sysadmin?
- ACL may distinguish the role

- Delegation:
  - Users delegate to compute server

Auditing

- Formal proof for every access control decision

Discussion