Birds of a Feather Session

- To discuss :
  - Vendor requirements.
  - Possible implementation approaches.
  - Where some of the component code pieces are available.
- When : Immediately following this talk
- Where : Right here

What do we plan to make available?

- Specifications :
  - Kerberos V5 based flavor protocol supporting integrity and privacy
- White papers :
  - Describing the new ONC RPC security architecture.

Use the Generic Security Service API (GSSAPI)

- The emerging standard security services programming interface.
- Can support multiple security “mechanisms.”
  - Currently supports three varieties of Kerberos V5 (MIT, DCE, SESAME).
  - Also DASS, DEC’s public-key based technology.
- Advantages and Disadvantages.
  - Is somewhat complicated, but
  - It is the only standard available.

New authentication flavors using Kerberos V5

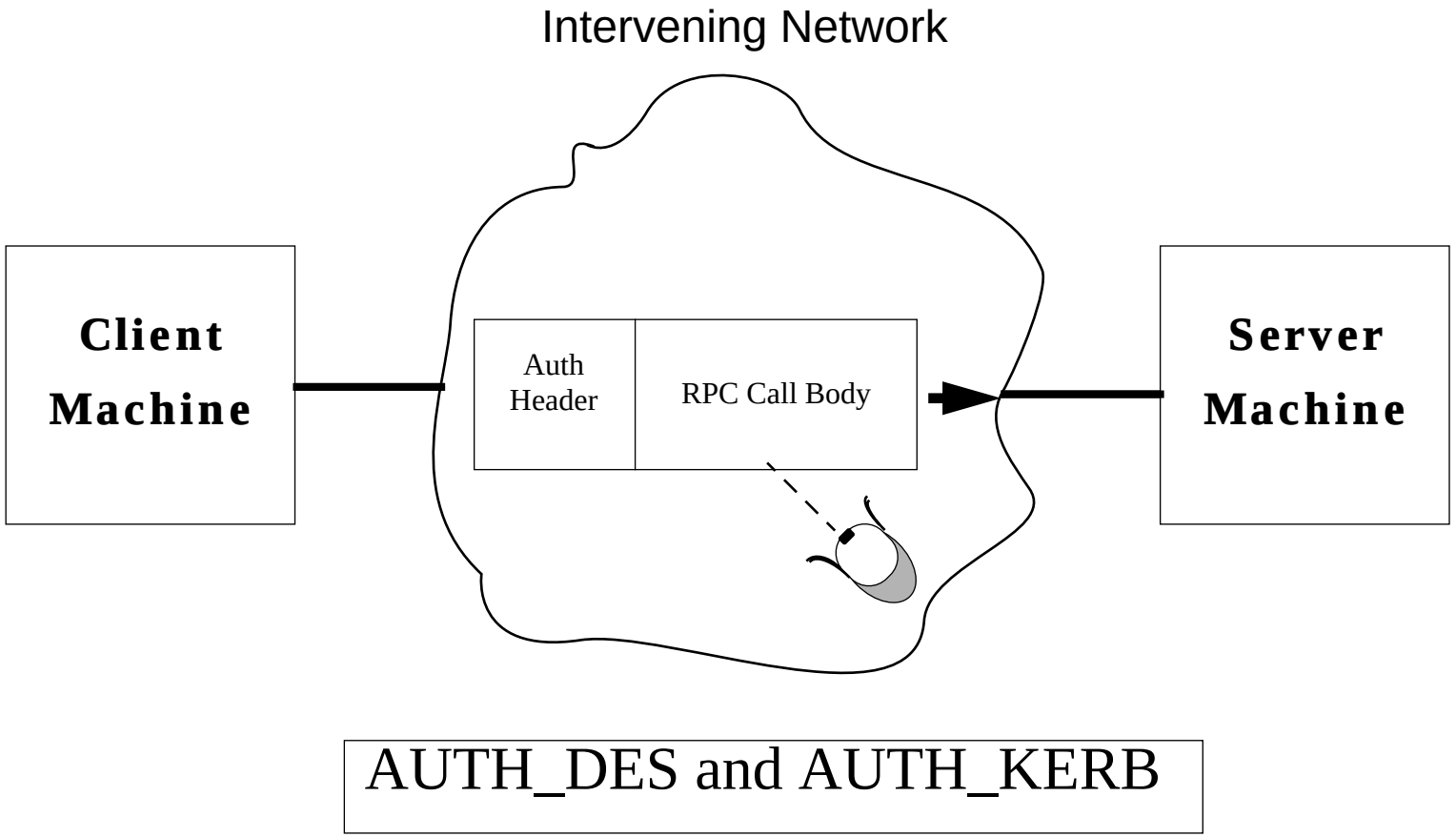
- Kerberos V5 is becoming an industry standard.
  - Emerged from the Internet standards process.
  - Used for DCE security services.
  - Used for SESAME.
- Kerberos will gradually move toward public-key [draft-ietf-cat-kerberos-pk-init-00.txt]
- Significant customer interest in Kerberos V5.
- Almost no interest in Kerberos V4.

How do we solve these problems?

- Institute new authentication flavor based on Kerberos V5.
- Use emerging Industry Standard General Security Services API (GSSAPI).
- Incorporate new security technology into NFS.

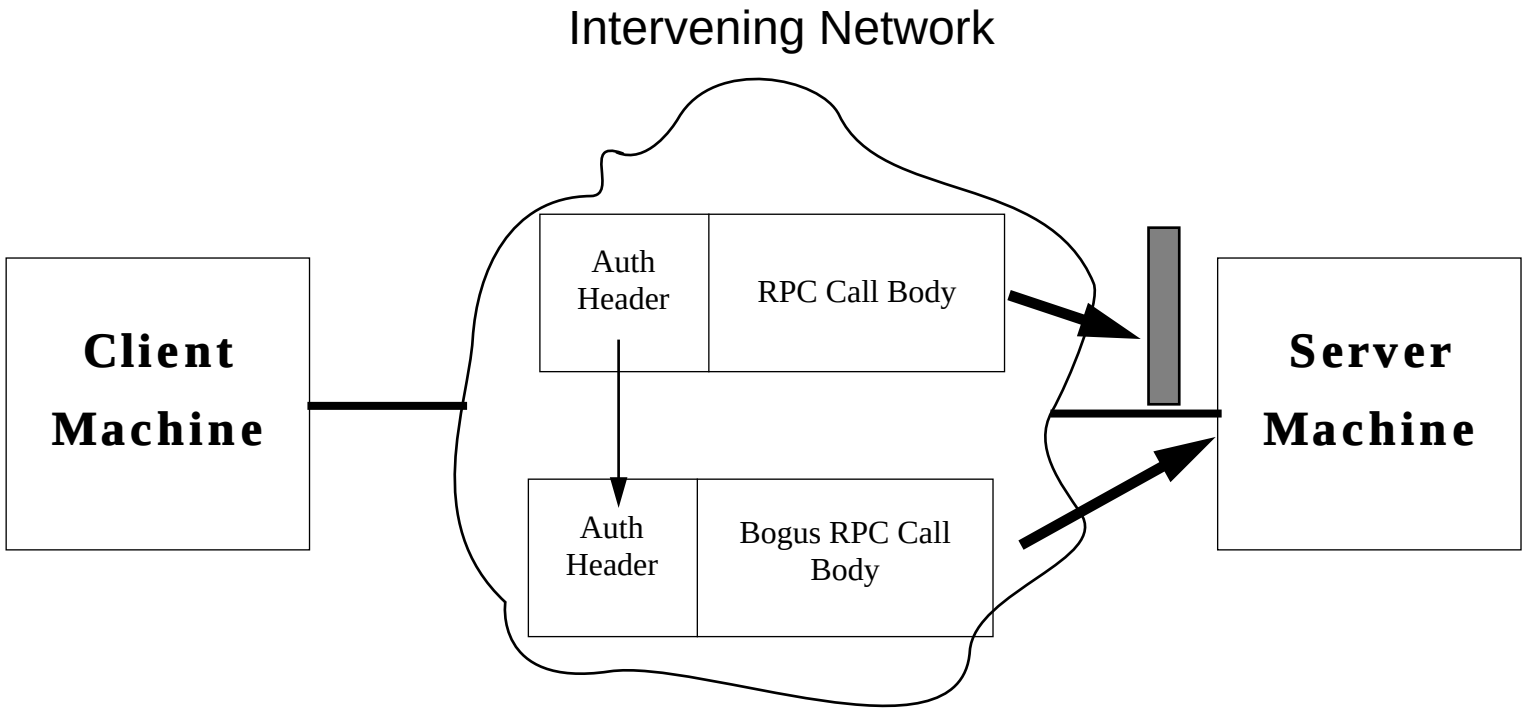
What is wrong with ONC+ security?

Release of Message Contents



What is wrong with ONC+ security?

Message Integrity : Splicing auth. header into bogus message



AUTH_DES and AUTH_KERB

Why do we need new security services in ONC+?

Our existing security technology is vulnerable in these environments.

- AUTH_UNIX requires client and server machines to trust each other.
- AUTH_DES is vulnerable to active wiretap ("man-in-the-middle") attacks and does not provide privacy protection.
- AUTH_KERB has the above problems and there is a general lack of interest in Kerberos V4 (on which AUTH_KERB is based).

Why do we need new security services in ONC+?

The existing services do not meet the needs of customers

Most customers have a heterogeneous computing environment:

- Multiple administrative boundaries.
    - Trust may not cross boundaries.

- Networks are generally unsecure.
    - Traffic can be snooped or modified.

New Security Services for ONC+

CONNECTATHON '95

Dan Nessett

Security Group

Enterprise Networking Group

SunSoft