p8 q1

Distributed Systems Paper 8 Outline solution

JMB

2000

broad categories of users have the right to use services
&/or access broad categories of objects. It is efficient to
2 decouple role from current list of members --

- on issue: f(SECRET, role, obj-id) → signature
  held securely by server one-way function eg 128 bits ... (this year)
- check again on presentation with access request

+ protects fields from tampering
6 - not theft, not transfer - any principal can use

an extra field containing the principal's persistent
name, such as the user-id, can be included in
the cap. or just put through the fn.
Persistent name must, securely, accompany request.

+ prevents theft
4 + transfer only via server creating new cap.

a transient principal-id such as process-id
can be used as above.

+ less susceptible to attack as of shorter lifetime.
- overhead of reissuing/session + on crash
4 - how to capture long-term role membership? <discuss>

Revocation.

change SECRET - non-selective - all need re-issuing
hot-list - consider checking overhead cf ACL check.
easier to set up revocation/status data structure
4 cf hot list if pointer in transient capability.

(20)