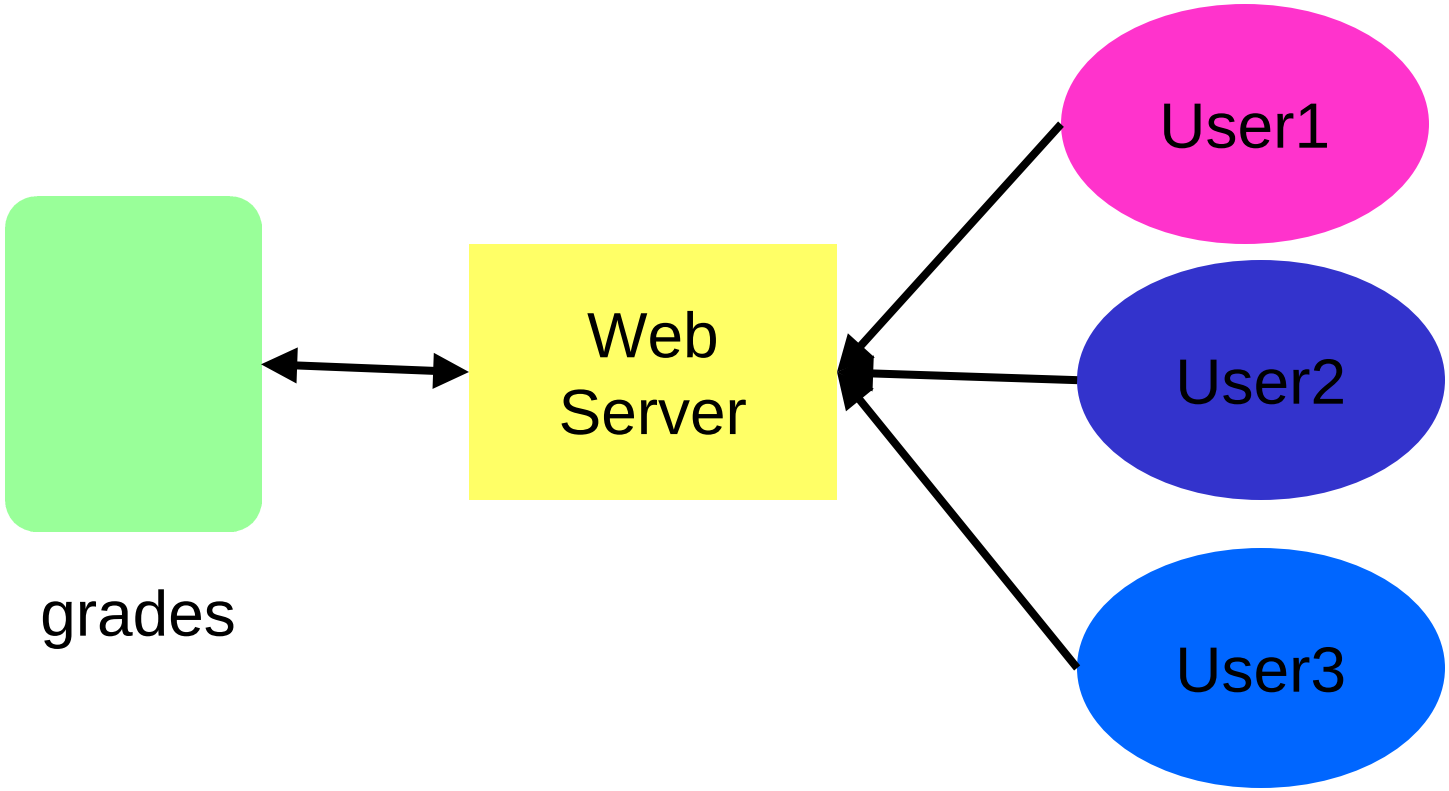
Announcements

Outline

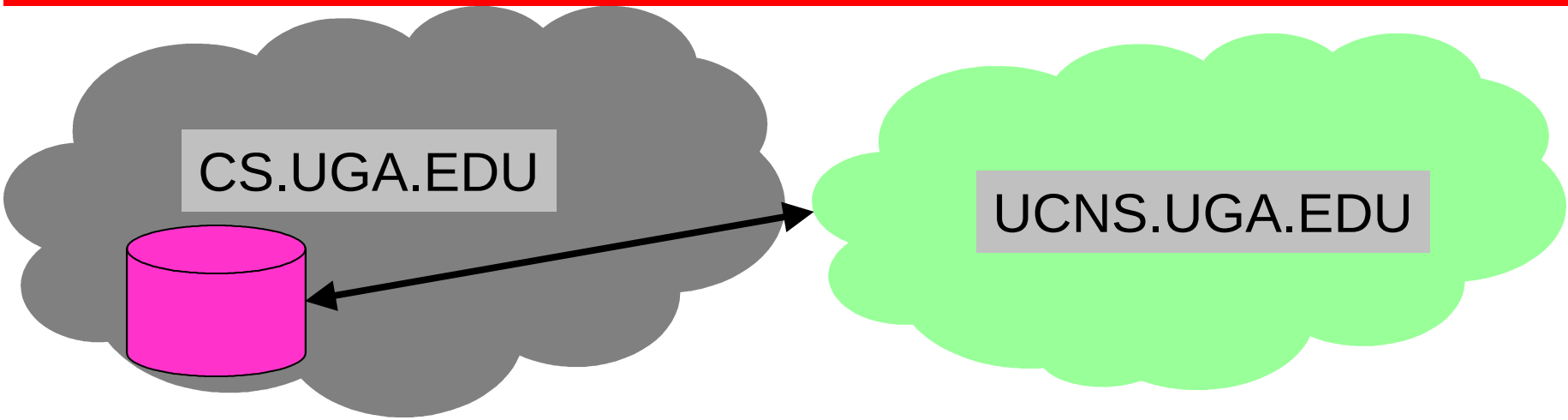
- *End-to-end authorization* – Jon Howell and David Kotz, in USENIX OSDI 2000
  - Source code available at http://www.cs.dartmouth.edu/~jonh/research/osdi2000/software/

Problem scenario



- Have to make sure that each user only access his or her grades through the gateway(web server)

1. Administrative Domains



- When sharing across admin. boundaries, server has no local knowledge of the recipient's identity
  - Local administrator creates a local account for remote user
  - Share passwords
  - Gateway that accesses as local user on behalf of remote user

2. Spanning network scale

- Network scale affects hop-by-hop authorization
  - Wide-area network: strong encryption protocol
  - Inside firewall: IP address based authorization
  - Local machine: trust OS to provide identity info.

- Built a toolkit that utilized the specific protocol for the network scale used

3. Spanning levels of abstraction

- Lower level resource server.
- For eg for accessing secure data in disk, we can spread trust across entities
  - Have the disk block allocator allow reads if user and kernel agree

4. Spanning protocols

- Gateways employed between different wire-protocols

- Gateways impede the flow of authorization information from client to server – gateways talk on behalf of the client to the server. The server has to be aware of this “speaks for” relationship

Unified authorization

- B=^{T}>A
  - B speaks for A regardng statements in set T
  - “Speaks for” captures delegation
  - “regarding” captures restriction

- Logical assumptions based on results outside the system (digital signatures)

Infrastructure – Snowflake

- Statements
  - Use a s-expression based system for statements
- Principals
  - Entities that can speak for others but can utter no statements directly
- Proofs
  - Describes the system that it proves and can verify upon request
- Prover
  - Helps Snowflake applications collect and create proofs. Collects delegations, caches proofs, and constructs new delegations

Channels

- Secure channels:
  - Use ssh or ssl based scheme to provide a secure channel
- Local channel:
  - Vouched by the local VM
- Signed request:
  - HTTP based authentication

Applications

- Protected web server
- Protected web server
- Quoting protocol gateway

Performance figures

- Performance figures in paper. In general, performance comparable to similar systems.

Discussion