

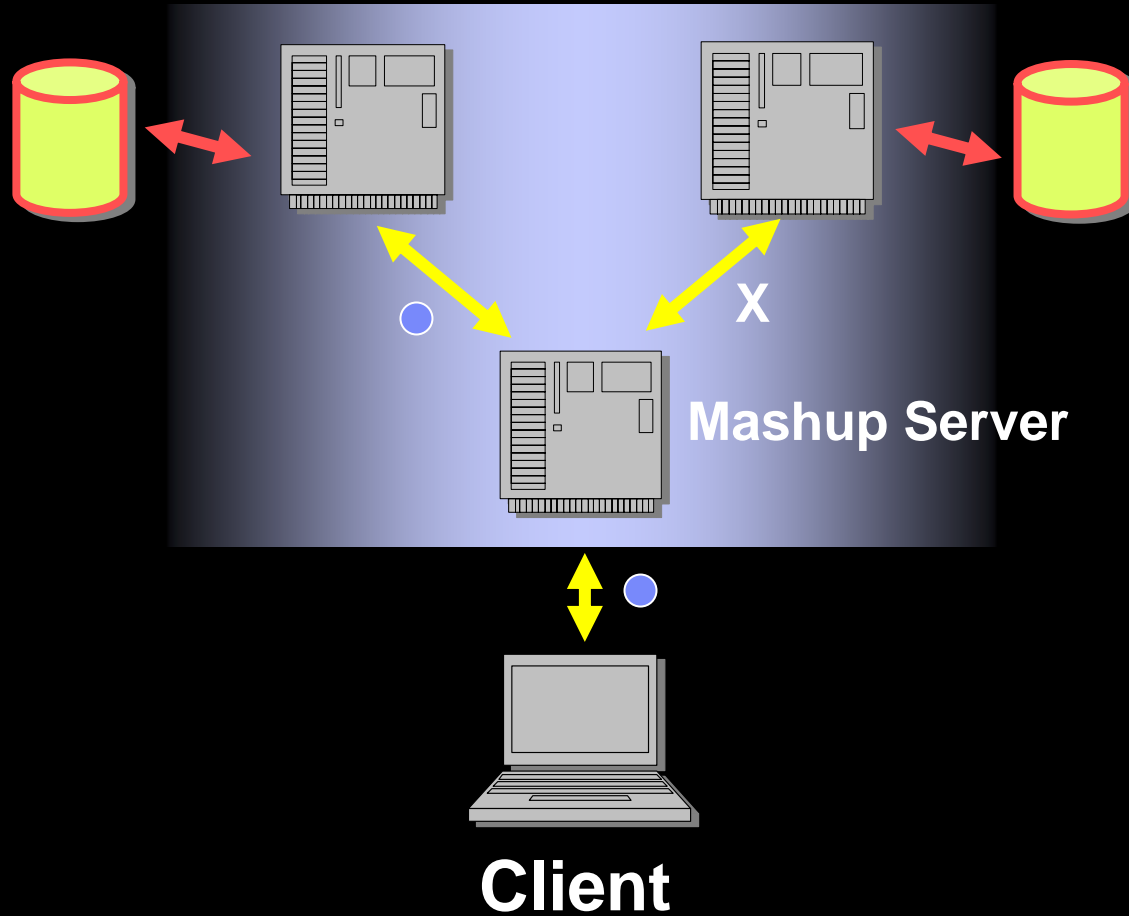
Outline

- **Authentication – who are you?**
 - Authentication without “giving away the store”?
- **Access Control (limited delegation)**
 - Authorization without “giving away the store”?

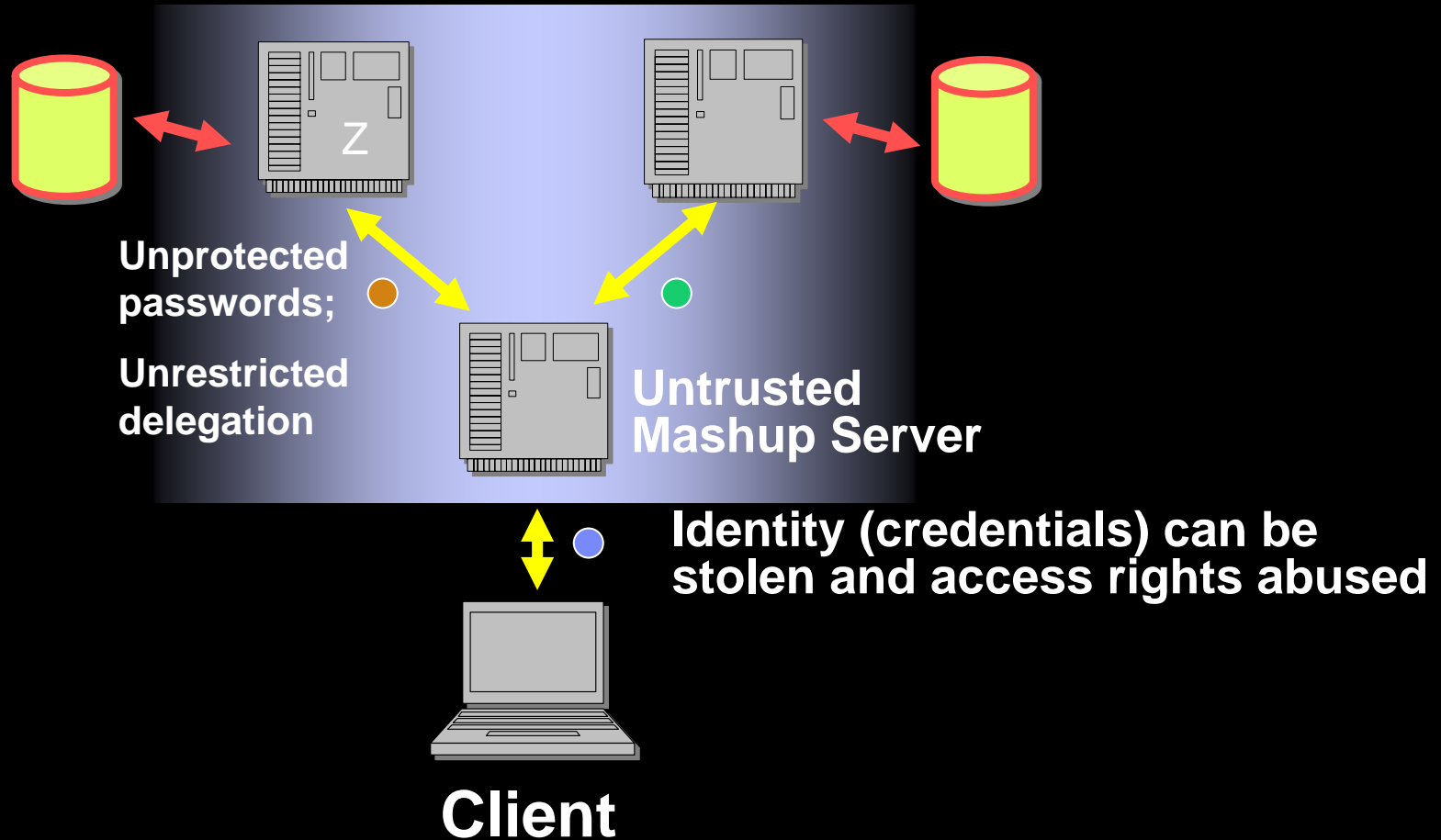
Basic Web 2.0 Authorization Issues

- **How do you authenticate when there is an untrusted intermediary?**
- **How do you limit the access rights given to the intermediary (limited delegation), such as a Mashup service?**

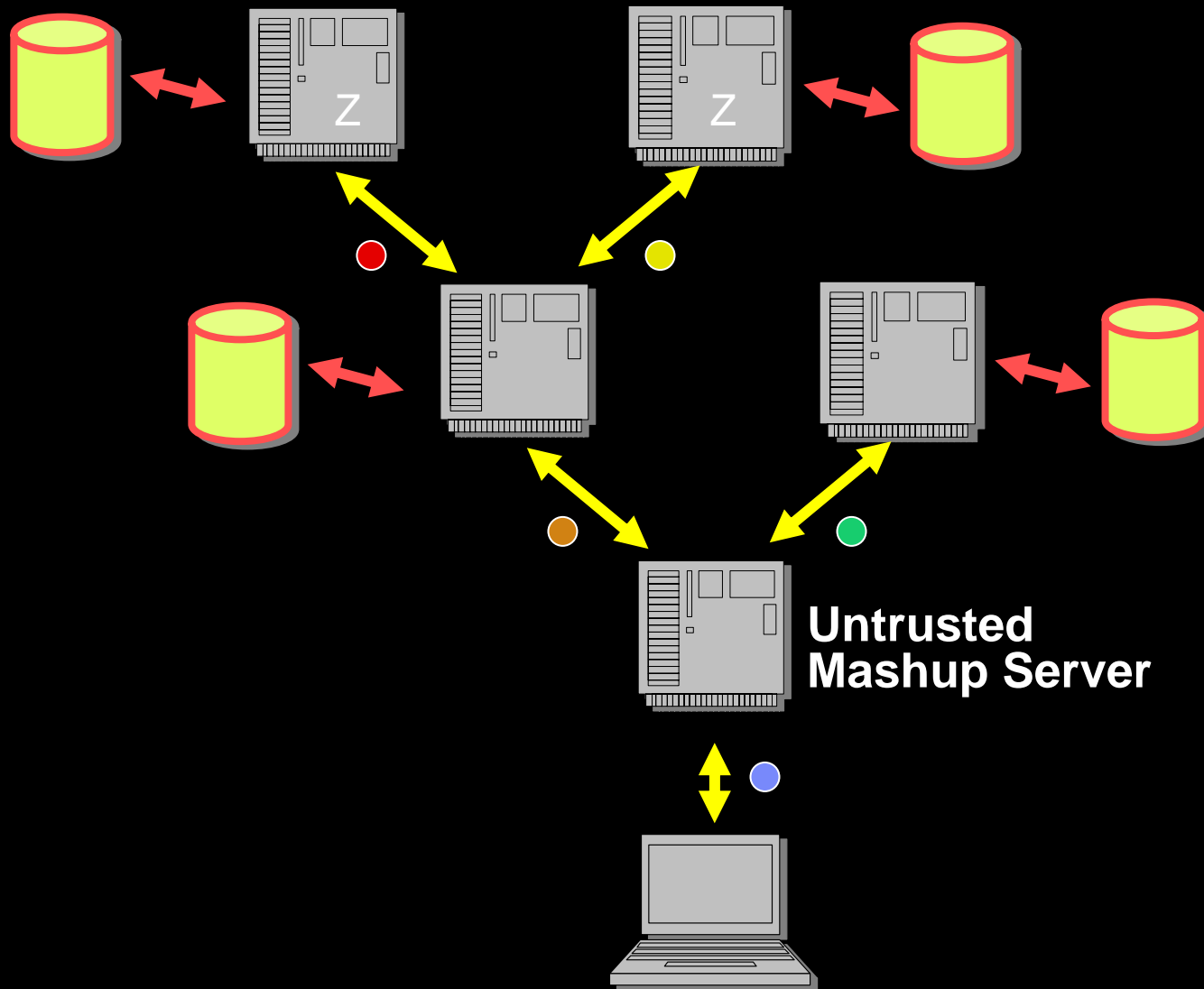
Authentication and Delegation-Problems



Current Security Vulnerability



Generalized View of Mashup Authentication



OpenID

Authentication & Federation

Possible Authentication & Federation Protocol: **OpenID**

- **Radically decentralized mechanism for single sign-on on the web**
 - Any number of identity providers and identity consumers
 - User specifies which identity to the application
- **Pervasively implementable**
 - Assumes standard browser capabilities
- **Specifications controlled by the OpenID Foundation (openid.net)**
- Early adopters: Blogging and social networking sites
- Some useful enterprise extensions possible

OAuth

Authorization & Limited Delegation

Delegation-Requirements

- Users need to **authenticate** to back end services without sharing credentials with Mashup Server
- Users need to **delegate** the right to access a back end service to the Mashup Server so that it can act on the user's behalf
- User should be able to specify specific rights to **delegate** to the Mashup Server (limited delegation)
- Mashup Server is **authorized** to access services based on delegation rights
- Users need to manage the rights delegated to Mashup Servers
 - Review / revoke rights given to Mashup Server to access services
- Usable protocols and interfaces!

OAuth Protocol Outline

