Client-Side Storage
Ashok Malhotra
<ashok.malhotra@oracle.com
Client-Side Storage

• Two Intertwined Threads
  – Client-Side Storage
    • Need to maintain state
    • Need for cacheing/offline storage
    • Need to share information among websites
  – Privacy Considerations
    • Client-side information is valuable for tracking behavior and, thus, encourages thievery
    • Large amounts of persistent information makes the situation worse
    • Other ways of tracking client behavior
Cookies

• The Web is stateless
• Cookies were invented by Netscape to add state
  – Allow, for example, session tracking and personalization
  – Does personalization (different views of same resource) break WebArch? i.e. compromise our ability to give URIs to things which can be distributed effectively?
• What are the properties of these two types of systems?
• Session cookies and persistent cookies
• Third-party cookies
• IETF drafts on cookies
Privacy Problems

- Cookies contain valuable tracking information and are much coveted by marketeers
- Subject to hijacking
- Same Origin Policy is supposed to prevent against this
  - Problems with SOP
- Sandboxing and security
- Why does encrypting cookies not work?
Limitations of Cookies/New Requirements

- Cacheing and offline usage
- Access from multiple websites
- Management of personal storage -- pruning, query
- Large amounts of storage
- Control over what is transmitted with each request
Responses to These Requirements

- CORS and UMP
- Other means of making Cross Domain Requests
- Web Storage
- Web Indexed DB
Privacy Problems

- Persistence and Large Amounts of Storage Exacerbates Privacy Issues
- Evercookie
- Private vs. Public Machines
- Other means of tracking
  - Clickjacking, mouse movements ...
  - This discussion forks the thread