

User Authentication

- Know each factor that the paper used to judge authentication methods (i.e. Resilient-to-Physical-Observation)
- Be ready to explain why one authentication scheme would work better than another for some specified system

Private Browsing

- Two threat models
 - Attacker with your machine after you're done browsing
 - Attacker who has compromised a web server you've visited

Local Attack

- Attack surface includes:
 - Cookies, DOM storage
 - Browser cache
 - History of visited addresses
 - Configuration of browser
 - Downloaded files
 - New plugins/browser extensions
 - Persistent data in RAM

Remote Attack

- Attack surface includes:
 - IP address
 - Browser fingerprinting
 - Link Colors (attack has been depreciated)
 - Cookies

Browser State Bleeding

- Public state that bleeds into private state
 - Easier for remote attacker to link public and private sessions
- Private state that bleeds into public state
 - Makes job easier for both remote and local attacker
- Private state persisting in session
 - If private state does not persist, remote attacker can recognize private mode
- Private state persisting across session
 - Should not occur, but happens if there are state bleeds from private to public or public to private (certificates, downloads, etc)