CSE135

- A Review of Some Fundamental Ideas
- Generation of App Patterns
- HTTP Overview
- Web Servers Overview
- Server Side Web Programming Intro

State and Session Management

- Addressing HTTP Statelessness
  - HTTP being stateless, or when each request/response pair or page view/in-page view, can make Web programming a challenge, so various solutions this are used including:
    - Hidden form fields
    - Extra URLs
    - Cookies
    - Messy – client-side
    - Memory or session cookies
    - Persistent cookies
  - Fortunately, most modern programming environments such as PHP, ColdFusion, Ruby on Rails, ASP.NET, provide a session concept which will abstract many many of the details of state preservation.
    - Sessions are most often implemented on cookies which are used to store a unique session data stored on the server
- Stateless Implications
  - Statefulness implies being able to track and remember things of a particular user/session (cookies, urls, storage, fingerprints, etc.)
  - It never seems to have state is to have "missing" of someone and their activities
  - This is tremendous as described this way but the question is "Is this ethically tenuous?"
    - "Hey, pick 5 items in this contents of your shopping cart"
- Anonymity and State
  - P3 Cookiless implies no cookies, or at least not using cookies to identify a particular user. But what about IP Addresses? Are they good if a concurrence exists?
  - If however, I can associate that identifier (fingerprint) with other identifying information such as your phone number, location, username, browser history, etc. then it is tremendous for you by creepy-creepy hater
  - This is tough to do if I don't have given my identifying info with a particular site. But what about if they give it to someone else?
- Reality of Anonymity
  - The reality is that you are NOT anonymous online! In fact I would argue that you are more anonymous in a physically speaking IRL than you are online
    - Tomorrow's metaverse is now today's reality. Welcome to THE COMPUTER AGE!
    - Well I am not that dumb! I change my IP address frequently! Anyway, I use a VPN!
      - Also it's logged (maybe for a long long time)
      - Thanks for letting me know you are a particular type of person. Some particular type of person. Some are legitimate
      - 就算用了隐私模式和VPN也不能完全保障匿名性
- The Reasonableness of Expecting Monitoring
  - The 'Ms. Story of 'Big' Thomas and Its Helpful Gentle Moral
    - Moralis: The expectation of being pitch to by many important activities political (available identity or IRL, or any) has
    - So far not really, but is this a "reasonable" expectation? Just as it
  - Logical Conclusion: If similar is now so important as life for many important activities (the same actions follows)
    - So far not really, but is this a "reasonable" expectation? Just as it
- Observation
  - How do I know identity online?
    - Email, profile, etc
  - How do I know who/what is real or not
    - Fin. Catfishing
    - Ex. Social Puppets & Concern Trolling
  - We are currently at a level 0.25 a worse high incident emergency. Not a Cyberwar yet but close to the "Fraud" we have been perpetrating in cyberspace after 9/11 and the Patriot Act has some bad implications
    - Ex. Fake People and Bots

- Setting for State
  - We have three primary places (just like the law of 3 - wonder why) where we can store state
    - Hidden Form Fields
    - Extra URLs
    - Cookies
    - Memory – client-side
    - Memory or session cookies
    - Persistent cookies
    - Sessions are most often implemented on cookies which are used to store a unique session data stored on the server
  - We can also never state anonymous! Cookies are always storage - using classification
    - Ultimately that isn't very secure and it is not good for state to be outsourced, instead of
    - We could also argue this either way, but it is better to be safe than sorry, we are storing decidedly-sensitive data only in these

- Hidden fields
  - 1. The Message Body (hidden form fields)
    - All pages wrapped in forms with each action causing a form post
    - Forms contain <input type="hidden" name="name" value="value" /> tags, which is a special string with name/pairs
    - Subsequent page loads are forms with hidden fields in them
    -
  - Notes
    - Open for easy parameter tampering
      - Countermeasure: integrity checks
    - Data is not persistent data refreshes across a user cost
    - Requests that a form be sent to the URL specified in the hidden data
      - HAT cases hidden form fields to remember selected and wrap the whole page in a single gigant form
- Query string
  - 2. The Request-uri (query string or URL)
  - Dirty URLs
    - All links are rewritten with query strings in them
    - All forms pass the value on the query string as well (either direct or through changes in the hidden field)
    -
    -
    -