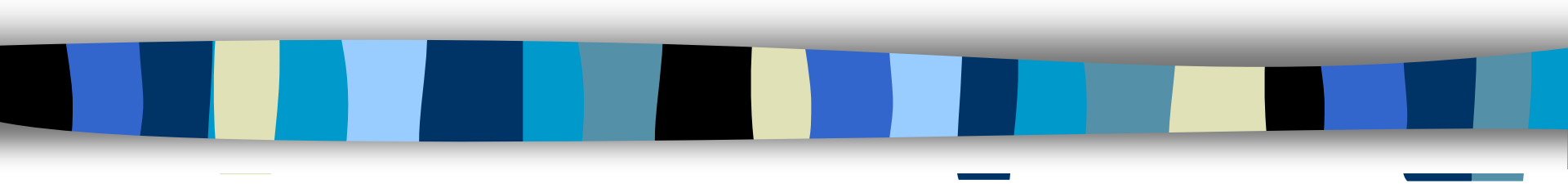
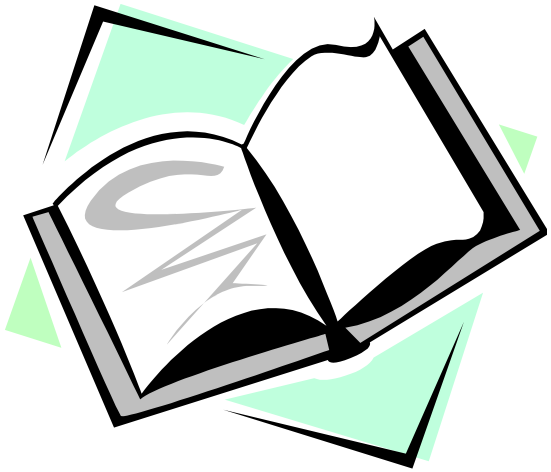
Information Security
CS 526
Topic 9



Web Security Part 2

Readings for This Lecture

- **Optional Reading**
  - Bandhakavi et al.: CANDID : Preventing SQL Injection Attacks Using Dynamic Candidate Evaluations
  - Chen et al.: Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow



Other Web Threats

- SQL Injection
  - See slides by Venkat
- Side channel leakages
  - See slides from MSR
- Web browsing privacy: third-party cookies

Browser Cookie Management

- Cookie Same-origin ownership
  - Once a cookie is saved on your computer, only the Web site that created the cookie can read it.
- Variations
  - Temporary cookies
    - Stored until you quit your browser
  - Persistent cookies
    - Remain until deleted or expire
  - Third-party cookies
    - Originates on or sent to a web site other than the one that provided the current page

Third-party cookies

- Get a page from merchant.com
  - Contains <img src=http://doubleclick.com/advt.gif>
  - Image fetched from DoubleClick.com
    - DoubleClick knows IP address and page you were looking at
- DoubleClick sends back a suitable advertisement
  - Stores a cookie that identifies "you" at DoubleClick
- Next time you get page with a doubleclick.com image
  - Your DoubleClick cookie is sent back to DoubleClick
  - DoubleClick could maintain the set of sites you viewed
  - Send back targeted advertising (and a new cookie)
- Cooperating sites
  - Can pass information to DoubleClick in URL, …

Cookie issues

- Cookies maintain record of your browsing habits
  - Cookie stores information as set of name/value pairs
  - May include *any* information a web site knows about you
  - Sites track your activity from multiple visits to site
- Sites can share this information (e.g., DoubleClick)
- Browser attacks could invade your “privacy”

Coming Attractions …

- Secure communication & key distribution