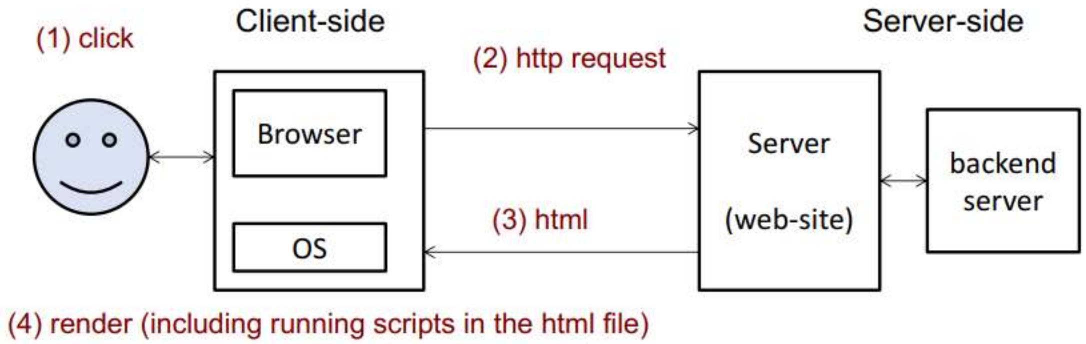
# Web Security

Friday, April 13, 2018 12:04 PM

## The Web



- Html file likely contains a cookie (server wants browser to keep some information)
- More features -> more weaknesses
- Script files
    - Browser runs html file -> constructs query from script -> sends to server

## Complications

- Browser
    - Same access privilege as user
    - Content providers can render content (rich c2 set)
    - Managing sensitive user information (cookies)
- Android: each app = one user, different access rights

## Attack Models

- Attacker = end system (Malicious web-server or user)
- Attacker = MITM
- Combination of different attacks

## SSL/ TLS Secure Communication Channel

- TLS renegotiation
- Attacker = MITM between browser and server, able to sniff/ spoof packets at TCP/IP layers
    - HTTPS: attacker cannot compromise confidentiality/ authentication
- Heartbleed (improper input validation), wannacry, superfish, BEAST (crypto - CBC)

## Misleading the User

- URL = uniform resource locator
    - Consists of a few components, like the path and query
    - Usually displayed with 2 levels of intensity (hostname vs. pat
    - Intentional phising emails sent by NUS.
- Safari only displays hostname, does not display path

### Address Bar Spoofing

- Browsers should not allow webpages to display over the address bar (only way user can know website)

### Clickjacking

- User Interface redress attack
- Another page loading in transparent layer
  - Solution = force frames to be visible
- Likejacking = get likes, cursorjacking = fake cursor

## Cookies

- HTTP cookie = response from server
- Previously-saved cookies will be automatically sent to server
  - Web server stateless, does not record who visits how many times. Info stored in cookie
  - Single sign-on, token-based authentication
  - SSO can be for a single site/ multiple in same enterprise
  - Usually has an expiry date
  - Token can be mac or concatenation (latter relies on security by obscurity, bad)
- With multiple web servers: which cookie to send?
  - Policy of same origin (PROTOCOL, hostname, port #)
- Server must remember previous tokens
  - Best is server keeps only one secret key k
  - Server verifies that the mac is correct by looking at stored user info

Can MITM steal cookies? No. even with fake website. Not same origin. (different hostname)

## Cross Site Scripting (XSS) Attacks

- Cookies may be stolen
- User inputs data - what if data = script?
  - < converted to &lt and &gt
  - Browser does not interpret it as a program
- Attacker tricks user to click on link which sends script to server
  - Script can steal cookie
  - Privilege escalation of script (exploits client's trust of server)
  - Phishing: cookie sent to attacker website/ third party instead of original website
- XSS can be reflection (non-persistent)/ stored (e.g. forum)

### Defence

- Most on server-side to filter malicious scripts in request
- Not fool proof
- E.g. Browser can convert all open brackets to ascii &lt
  - Other formats will surface

## Cross Site Request Forgery (XSRF)

- Sea surf, reference forgery, session riding
- Reverse XSS: exploits server's trust of client
- Attacker makes use of client's cookie to send malicious requests to server
- Common prevention: additional authentication information

## Other Attacks and Terminologies

- Misconfiguration, searching for filename
- Drive-by download
  - May be authorised/ unauthorised
  - User unaware of content/ consequences
- Web Bug/ Beacon
  - Checks if user has accessed content
  - Small image that is downloaded (request sent to server) when user visits web page

    - Image may be requested every visit or once and stored
    - Mostly unobtrusive/ invisible
- CAPTCHA
    - Completely Automated Public Turing test to tell Computers and Humans Apart
    - Challenge-response
- Click fraud = fake clicking advertisements
    - Pay-per-Click (PPC) online advertising