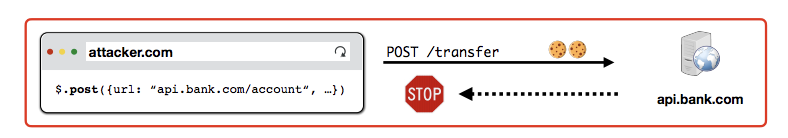
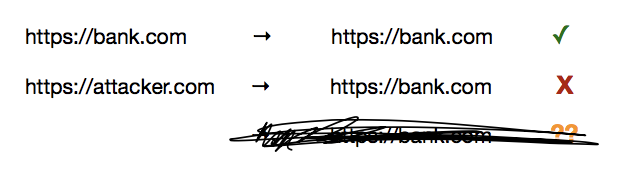
CAS CS 357

In-Class Note 7

1. CSRF
2. Cross-site request forgery attacks are type of web exploit where website transmits unauthorized commands as a user that web app trusts
3. User is tricked into submitting an unintended web request to a website
4. 
5. Whatever information from api.bank.com is not eligible to attacker.com due to the same origin policy but it does matter since action already took form 🡪 just doesn’t return anything back to the user (attacker.com can use POST method to simply attack user’s bank)
6. Preventing CSRF Attacks
7. Cookies do not indicate whether an authorized application submitted request since they’re included in every request
8. Four commonly used techniques
9. Referer Validation
10. Referer request header contains address of the previous web page from which a link to the currently requested page was followed
11. Header allows servers to identify where people are visiting from
12. 
13. If you are requesting attack from attacker.com to bank.com, it would not work since the request is not directly from bank.com
14. Only bank.com can send request to bank.com
15. Secret Validation Token
16. Bank.com or websites include secret value in every form that server can validate
17. 
18. Way to come up with a token:
19. Set static token in form (the website gives out all the token with same value)🡪 attackers know your CSRF token and can therefore attack
20. Send session-specific token as part of the page (random to all users) 🡪 each token is personalized and is random so that attacker does not know your CSRF token
21. Custom HTTP Header
22. Samesite Cookies
23. Cookie option that prevents browser from sending a cookie along with cross-site requests
24. Session cookie is stored in the website. However, you can get cookie (original cookie, not samesite cookie) from other websites without even visiting the website CSRF token
25. Samesite cookie is always stored within the website so that it blocks requests that attacker makes from attacker.com and is not stored but goes back to the server on deletion of cookie
26. Strict Mode: never send cookies in any cross-site browsing context, even when following regular link. If a logged-in user follows link to private GitHub project from email. GitHub will not receive session cookie and the user will not be able to access the project
27. Lax Mode: session cookie is be allowed when following a regular link from but blocks it in CSRF-prone request methods
28. In other words, never send cookie if not referred from the same website
29. Crypto
30. Several Important crypto properties
31. Confidentiality: the property ensuring that information is not disclosed to unauthorized parties
32. Integrity: property of maintaining and assuring the accuracy and completeness of information
33. Authenticity: property that information originated from its purported source
34. How do we define encryption scheme

Plaintext m Key k Ciphertext c = Enck(m)

Correctness: Deck(Enck(m))=m The message is decryptable

Security = The adversary cannot read the message without k

1. Some institution – The Caesar Cipher

Plaintext I ATE THE CHEESE

Ciphertext F XQB QMB ZMBBPB