Scribe Notes

Administrative Logistics
Each week a scribe is selected to summarize the main points of the lecture. The scribe has a week to turn in a pdf
Paper summaries for that day's lecture due 2 hours before class
15 minutes are set aside each class for someone to be a discussion lead to lead a discussion for that lectures topic

- Please make it as interactive as possible. Could use presentation as an aide.

Course Project can be executed in teams of 2-3

Please have your camera on if you can. Feel free to reach out to the professor privately if there are any comments or concerns with this.
Majority of students in the class are in favor of recordings. Feel free to reach out to the professor privately if there are any comments or concerns with this. Please keep the recording within the class

There will be a google form sent out to select which paper you prefer to be discussion lead for

Warm up- "Is online banking secure"

- You're still trusting the banks with information
- Phishing attacks - someone impersonates the bank through an email
- Someone can impersonate you and withdraw all your money
- Once the attacker has convinced me that they are the website, they can get your userid, password and challenge questions
- The website could try to steal your cookies if browser is not secure enough
- Browser extensions have a lot of permissions and information
- What does secure mean? - unauthorized transactions was what WE focused on
    - Might care about anonymity/privacy
- David uses online banking. Why? Considering what we just talked about
    - Its convenient
    - Amount of risk
    - Severity of risk
    - Unauthorized transactions are nulled for credit cards - just dispute the charge
    - Security Analysis is not black and white- do benefits outweigh the risks?
- Three questions - if a website is allowed to display stuff onto your screen.
    - What security risks does this introduce?
    - What could users do to protect themselves?
    - What could browsers do to protect users?

What could users do? Browser must request permission with a notification so user can be aware of what they are allowing. Relying on browser vendors to have done this. Use a

password manager cause it checks passwords for you. With firefox, it lets you know you are full screen when your mouse goes to the top

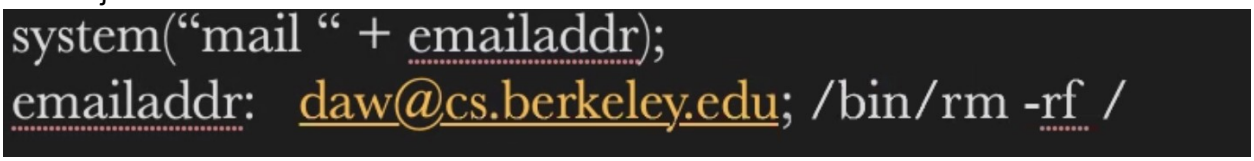
Threat Model - what kind of attacks are you worried about that your system is trying to protect against

Data-driven attacks- send malicious data and causes the program to run a muck
Command Injection Attack is a type of Data-driven attack
Command Injection Attack examples-

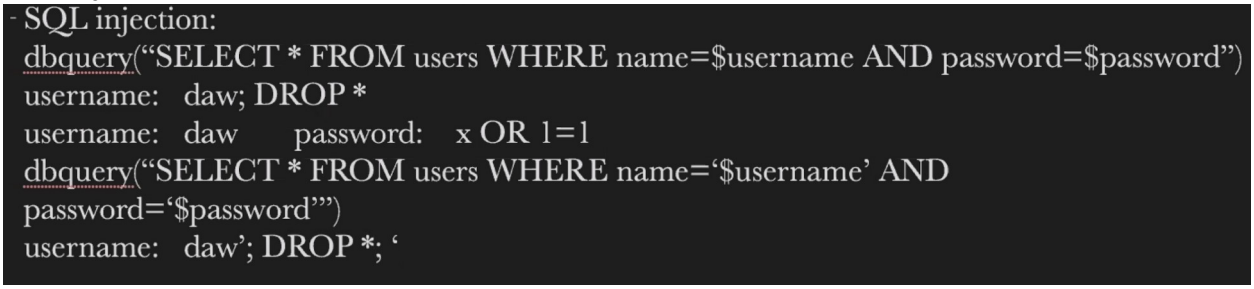
Capn Crunch attacker - used a whistle to fake the pay phone. Phone emitted a 2600 hertz tone when quarter was dropped. So the hacker could imitate the tone. Commands coming from pay phone itself in the same place data was being recieved

Xterm Attack - when downloading something a certain sequence of escapes and echo to write a command as if it were you typing it.

Shell Injection-



SQL Injection -



Solutions:
- Input sanitization
- Prepared statements — Strings bad, work with pre-parsed data structures
- Keep data separate from control

Another solution: Taint Tracking

Legacy systems: taint tracking

```
String x = 'Al';
y = 'Hello ' + x;

===>

TrackedString x = new TrackedString('Al', false);
Y = new TrackedString('Hello ', false).append(x)

Class TrackedString {
   String val;
   boolean taint[];
}
```