CS142 Project 3

Abusing Side Channels

Overview

- 3 Attacks
- Port Scan in Javascript
- Password Timing Attack
- Determining if a user is logged in or not
- Avoid using Google, start early

Part 1: Port Scan

- How do you detect if a port is open or not?
- onerror/onload/setTimeout

```
<script type=”text/javascript” language=”javascript”>
   var img = new Image();
   img.onerror = function() {
      // The image didn’t load or wasn’t an image!
   }
  img.onload = function() {
     // The image loaded successfully!
  }
   img.src = "http://www.example.com/page.html";
</script>
```

Part 1: Port Scan

- Idea: load host:port with Image objects, if it errors (not an image) then the port is open, if it times out, then the port is not open.
- setTimeout() is non-blocking, takes a callback or string to eval.
- Set up handlers load the image start a setTimeout, see which one finishes first.

Part 1: Port Scan

- Output the ports and status
- Don't use document.write, make a div and use innerHTML to append to the div i.e. blah.innerHTML = blah.innerHTML+"2939
"
- Should the ports/status be printed out in the same order which you scan the ports?
- You'll need to vary the timeout length

Part 2: Timing Attack

- Skim the paper - linked on syllabus "Exposing Private Information by Timing Web Applications"
- Idea is: When a username is correct, the web app will do additional lookup on password in database. This introduces extra delay.
- In our case, we give you the username, find the password.

Part 2: Timing Attack

- How do we determine how long something took to load?

```
start = new Date();
// wait awhile
end = new Date();
timePassed = end - start;
```

- Use the javascript password list

Part 2: Timing Attack

- Looking at latencies - mostly are the same, occasional lag spikes (especially over wifi)
- Need to do a "calibration"
- We need a baseline measure of logins that aren't valid to compare against one that is valid
- Calculate a threshold using the baseline measure
- Write in your README how you calculated it

Part 3: Is a user logged in?

- This part should be the easiest, I won't give any hints

General Tips

- Use firebug
- Use alert() to find out what's happening