Assignment 5 basics

CSE 127 Wk 9 Discussion

Agenda

Last Week

- Intro to mininet and wireshark
- Some of the challenges
- TCP Seq and Ack numbers

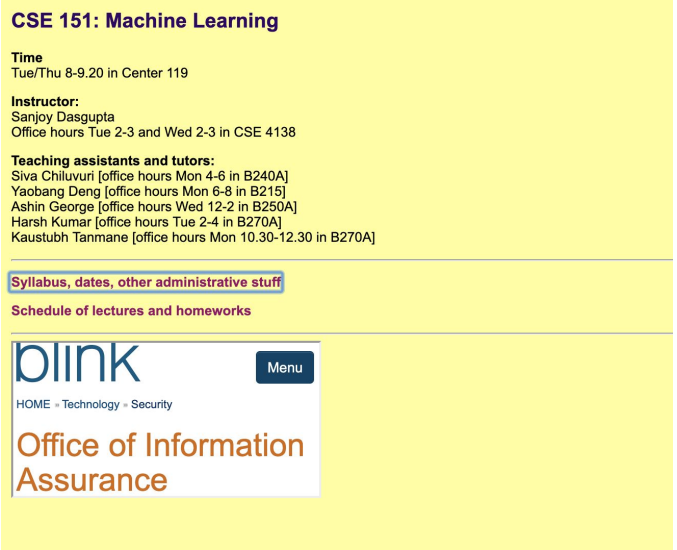
Today

- A step back: High level overview of the attack
- How to get started / High level outline of what you need to track
- Any questions

Overview of Assignment

- You are a man-in-the-middle attacker
  - You can modify packets from the client to the server, and vice-versa
- Goal: Inject an iframe of site A into site B
- Adds extra traffic to site A
- D.O.S

```
▼<iframe src="http://blink.ucsd.edu/technology/security">
  ▶#document
  </iframe>
 </body>
</html>
```



Outline

1. Identify who you are targeting / which packets you care about
2. Inject the <iframe> tag right before the </body> tag
3. Adjust the content length in the GET response header
4. Adjust TCP SEQ and ACK numbers based on new length
5. Allow only uncompressed packets

1. Who are you targeting

- Watch the **requests** from the client to the server
- target_domain_re vs Host of the GET request
- url_path_re vs the path of the GET request
- Create a **mapping** between the client/server IP/port and the domain

```
GET /hello.htm HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE5.01; Windows NT)
Host: www.tutorialspoint.com
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
```

https://www.tutorialspoint.com/http/http_requests.htm

2. Inject the iframe

- Check for the **response** packets from the IP that corresponded to “Host” from the previous slide
- Look for the HTML tag </body>
- use string slicing / substrings / string concatenation to add in <iframe src=”....”></iframe>

```
▼<iframe src="http://blink.ucsd.edu/technology/security">
  ▶#document
  </iframe>
</body>
</html>
```

3. Adjust the content length

- In your code, this will come **before** the previous slide, since the HTTP response header is sent first
- Look in the header for the “Content-Length” field
- Read the current number, and change it to:
  - Current number + len(<iframe src=.....)

```
HTTP/1.1 200 OK
Date: Mon, 27 Jul 2009 12:28:53 GMT
Server: Apache/2.2.14 (Win32)
Last-Modified: Wed, 22 Jul 2009 19:15:56 GMT
Content-Length: 88
Content-Type: text/html
Connection: Closed
```

```
<html>
<body>
<h1>Hello, World!</h1>
</body>
</html>
```

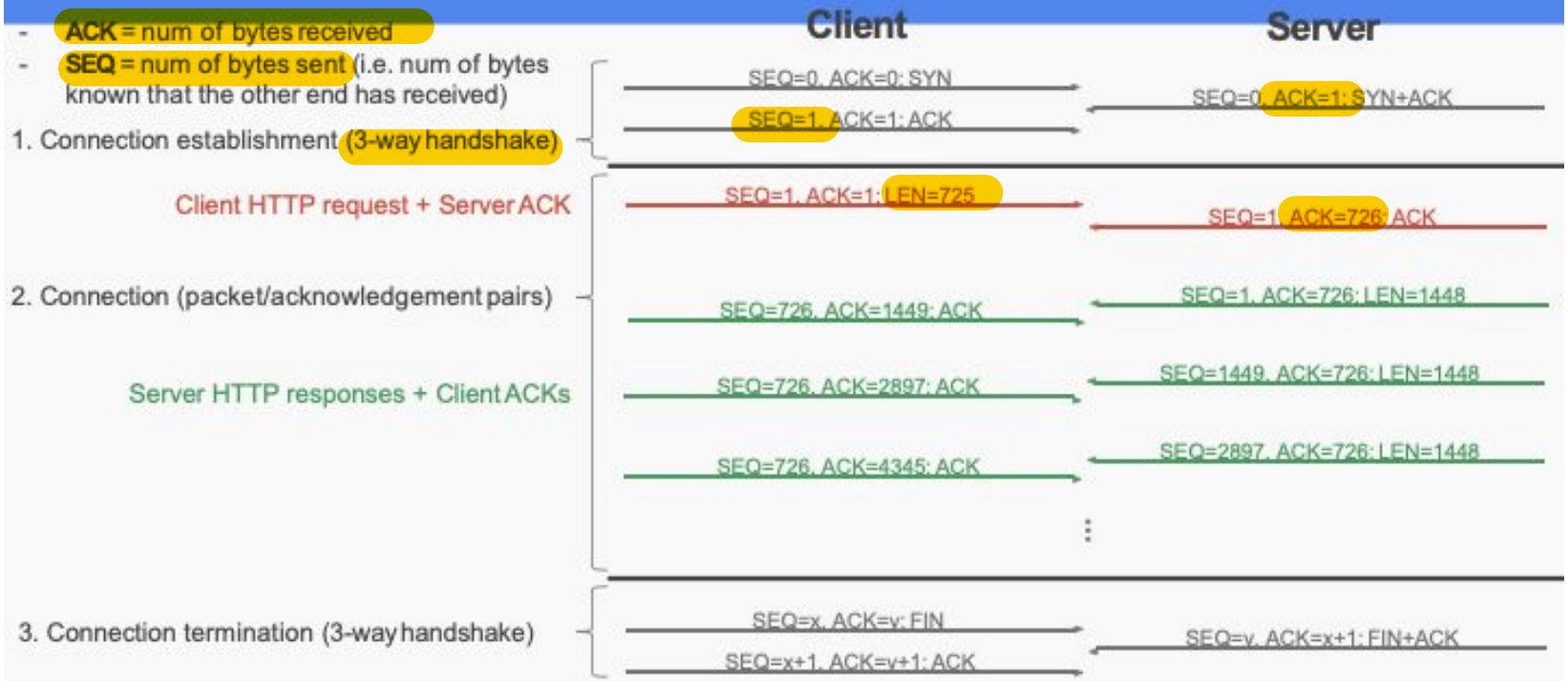
https://www.tutorialspoint.com/http/http_responses

4. Adjust the TCP Seq and Ack numbers

- Seq and Ack numbers are based on content length
- So they need to be adjusted similarly to the content-length field
- Must adjust ALL following packets, in both directions
  - The Client has received more packets than the server has sent
  - The Server expects a smaller number of total packets than the client has seen
- Edge Case: Make sure to Mod by 2^32
- Example next
- How to maintain all of this?

TCP's SEQ and ACK numbers

- **ACK** = num of bytes received
- **SEQ** = num of bytes sent (i.e. num of bytes known that the other end has received)



Slide 24 from last week

5. Accept-Encoding

- Back to the initial request
- The client chooses what kind of encodings it can handle
- We want packets uncompressed so that we can easily insert the iframe
- So we change the client's request to ensure the response is uncompressed
- Accept-Encoding: Identity

```
GET /hello.htm HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE5.01; Windows NT)
Host: www.tutorialspoint.com
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
```

Warning

- Changing the content-length and changing Accept-Encoding might change the length of the request Header
- TCP Seq/Ack numbers
- Try not to shrink the header size

Tips

- Use the outline from these slides as a starting point: write comments in manipulate_packet to indicate where you'll do each step
- I recommend starting with step 1 and proceeding in order, **however**, your code will need to be reordered
  - Header comes before body, for example
- Refer often to last week's slides for wireshark tips

- **Lab Hours and OH will end this Friday!** So please make use of time this week
- Assignment is due **Friday at 10pm**
- You are welcome to use slip days (**until Wed 6/12),** but you'll be on your own
- Final review at next Friday's discussion by Sourav