Kiefer Lord
Jeff Ondich
CS338
7 April 2022

# HTTP Basic Authentication

The process starts with the TCP handshake:

```
1   0.000000000   192.168.205.128   45.79.89.123   TCP   74   54494 → 80 [SYN] Seq=0
        Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=707667696 TSecr=0 WS=128
3   0.045097962   45.79.89.123   192.168.205.128   TCP   60   80 → 54496 [SYN, ACK]
        Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5   0.045131344   192.168.205.128   45.79.89.123   TCP   54   54496 → 80 [ACK] Seq=1
        Ack=1 Win=64240 Len=0
```

For some reason, each of the 3 frames of the TCP handshake were duplicated.

Then, the client requests authentication, and the server acknowledges the request and sends the HTML for the authentication popup:

```
7   0.045326401   192.168.205.128   45.79.89.123   HTTP   395   GET /basicauth/ HTTP/1.1
8   0.045512359   45.79.89.123   192.168.205.128   TCP   60   80 → 54496 [ACK] Seq=1
        Ack=342 Win=64240 Len=0
9   0.090947959   45.79.89.123   192.168.205.128   HTTP   457   HTTP/1.1 401
        Unauthorized  (text/html)
```

Then, there are some keep-alive frames while the user types the username/password. Then the client sends the authentication request containing the username and password:

```
18   12.434407537   192.168.205.128   45.79.89.123   HTTP   438   GET /basicauth/
        HTTP/1.1
```

Here is the last piece of the data sent in that frame:
Authorization: Basic Y3MzMzg6cGFzc3dvcmQ=....

This contains the username and password information, but it is base-64 encoded, as specified in the HTTP spec documents (https://datatracker.ietf.org/doc/html/rfc7617). Base-64 is “invertible,” meaning we can figure out the username and password from the encoded version. Therefore, it seems like this protocol is not very secure. Also, this means the server does the password checking, not the browser. The server then sends an acknowledgement that it got the right username and password, and it sends the HTML of the webpage. If the user types the wrong username or password, the server simply asks for the login information again instead of sending the HTML of the webpage.