Jordan Bayles
April 25, 2014

Homework 3
ECE 478: Network Security

## 0. Disclaimer

*This submission reflects my own understanding of the homework and solutions. All of the ideas are my own, unless I explicitly acknowledge otherwise.*

## 1. The secret name of the cookie

This page sets a cookie upon new account creation called **ecbhw**.

```
    $cookie = CGI::Cookie->new(
        -name  => "ecbhw",
        -value => encode_base64(encrypt($data))
    );
```

## 1 2. What must a token for the admin user contain?

The script uses the cookie to check authorization, and splits up the base64 cookie value into three sections:

1. "ok" - did we decode correctly?
2. "timestamp" - account creation time
3. "username" - what is the account username?

```
if ($cookie && $cookie->value) {
    my $dat = decrypt(decode_base64($cookie->value));
    my ($ok, $timestamp, $username) = split /\|/, $dat;
    if ($ok eq "ok") {
        $AUTHORIZED = $username;
        my $t = localtime($timestamp);
        msg "Welcome back, $username (member since $t)";
    } else {
        msg "Invalid authentication cookie detected";
    }
```

### 3. Manual verification of use of ECB

You would have to manually modify the cookie and see how the resulting value is decoded. For example, I created a cookie with username **metatron**. The login page is thus this:

```
Info: Welcome back, metatron (member since Wed Apr 23 07:15:49 2014)
```

With this cookie currently set to the following content value:

```
qLIsoB4lE%2FacKIMVqXvlmw9s%2Fw0cRcV%2B7Oxx8e%2BolY8%3D%0A
```

We can modify the content in an area that is presumably the username:

```
qLIsoB4lE%2FacKIMVqXvlmw6s%2Fw0cRcV%2B7Oxx8e%2BolY8%3D%0A
```

And it turns out it is bizarrely easy to make modifications to the cookie without affecting the resulting output, like this example

```
qLIsoB4lE%2FacKIMVqXvlmw9s%2Fw0cRcV%2A%2C%2B%2A7Oxx8e%2BolY8
```

and even easier to get a bad decryption:

```
bad decrypt 140286217791304:error:06065064:digital envelope
routines:EVP_DecryptFinal_ex:bad decrypt:evp_enc.c:596:

Info: Welcome back, me (member since Wed Apr 23 07:15:49 2014)
```

The HTML encoding used to represent the cookie content in this example makes it extremely difficult to get a working modification. This example results in a modified user name:

```
qLIsoB4lE%2F%2AacKIMVqXvlmw9s%2Fw0cRcV%2F%2C%2B7Oxx8e%2BolY8
```

Although it really isn't what we are after either.

```
bad decrypt 140703959312200:error:0606506D:digital envelope
routines:EVP_DecryptFinal_ex:wrong final block length:evp_enc.c:589:

Info: Welcome back, meWZQ:nAs7m6i (member since Wed Apr 23 07:15:49 2014)
```

On the plus side, this error does tell us the server is using OpenSSL at least.

### 4. Block length?

It is difficult to tell the block length from part 3, but it is likely a 32 bit block (4 ASCII characters), as the dissimilar portion in my attempts to solve is 22, meaning it's not a 64 bit block.

```
aaaaaaaaaaaaaaabaaaaaaaaaaaaa
IpdkZbQ21zpl%2BcTuK4LwV04wrzlBaDIzrNZLfdvqatcxR60eGLT8AB2%2Bbqrb%2F3Ay%0A
 9yeCyPYO8sQPrG5XG2m09k4wrzlBaDIzrNZLfdvqatcxR60eGLT8AB2%2Bbqrb%2F3Ay%0A

Dissimilar portion (timestamp + error check)
len(9yeCyPYO8sQPrG5XG2m09k) = 22 characters
Similar portion (username)
4wrzlBaDIzrNZLfdvqatcxR60eGLT8AB2%2Bbqrb%2F3Ay%0A

aaaaaaaaaaaaaaaaaaaaaaaaaaaaa
m%2FALEoX8P3yeQ7tqDXWGRrTGxF5pBZUDA1Zhe0nGotIxR60eGLT8AB2%2Bbqrb%2F3Ay%0A
```

Judging by the attempts in section (6), the blocks are a size that is a factor of both 22 and

### 5. What parts can you control?

You can control the username portion of the token data, as the time is set on the server side and the authentication portion must remain unchanged.

### 6. Encrypted blocks for the admin token

You can't have a username start with "admin," however you can get partial blocks for the admin token, by having a username be "ad(junk)" and another username being "(junk 2)min."

```
admia
KgjljG6nHbNqmd9jZT9DU8an7r7UdMs2U6Jpupi1gb0%3D%0A
admib
kduH7RIaHWtwrLMMZItmLlahAjClu6XQUcqneXZOVD0%3D%0A
admic
91G3nc0vwMGRzaGLWD5BzVx2iqMk%2BvEoKBClkTw5mug%3D%0A
admid
8L9oPg8A2lmvX6lWlzW5bA7XmaKTUgKvcI3WyXmZqDQ%3D%0A

bdmin
nQyk1IaVSnF1uxMndw4wv9d0u2qIbHUsko8Rf9tMues%3D%0A
cdmin
%2FrQUOX77Dt39OhxkwnyD2Nd0u2qIbHUsko8Rf9tMues%3D%0A
```

```
ddmin
SdTBw37M%2FJsPjMpWGnKNANd0u2qIbHUsko8Rf9tMues%3D%0A

SIMILAR *dmin:
***********************d0u2qIbHUsko8Rf9tMues%3D%0A
```

The block length is necessary to know which pieces you need to grab and set to ensure you modify the blocks you properly need to.

### 7. Cookie token use to get an admin token

You can synthesize parts of the cookie containing partial admin tokens–you are not allowed to create an account starting with admin–in order to create a single cookie containing a functioning admin cookie. Because the encryption mode is set to electronic codebook mode, the plaintext in each block is subject to the same encryption schema (assuming same key), meaning that the position in the block chain that each piece is subject to is more important than they are together (such as username `1admin`, which offsets the encryption and cannot help find the proper token.

### 8. Javascript set cookie

You can set a cookie in javascript by editing `document.cookie`:

```
document.cookie='ecbhw=<new value>'
```

### 9. Secret admin message