Song
Spring 2015

CS 161
Computer Security

Discussion 10

March 31 & April 1, 2015

Question 1 ***Cross Site Request Forgery (CSRF)*** **(10 min)**

In a CSRF attack, a malicious user is able to take action on behalf of the victim. Consider the following example. Mallory posts the following in a comment on a chat forum:

```
<img src="http://patsy-bank.com/transfer?amt=1000&to=mallory"/>
```

Of course, Patsy-Bank won't let just anyone request a transaction on behalf of any given account name. Users first need to authenticate with a password. However, once a user has authenticated, Patsy-Bank associates their session ID with an authenticated session state.

(a) Explain what could happen when Victim Vern visits the chat forum and views Mallory's comment.

(b) What are possible defenses against this attack?

Question 2 ***Session Fixation*** **(15 min)**

Some web application frameworks allow cookies to be set by the URL. For example, visiting the URL

`http://foobar.edu/page.html?sessionid=42`.

will result in the server setting the `sessionid` cookie to the value "42".

(a) Can you spot an attack on this scheme?

(b) Suppose the problem you spotted has been fixed as follows. `foobar.edu` now establishes new sessions with session IDs based on a hash of the tuple `(username, time of connection)`. Is this secure? If not, what would be a better approach?

Question 3 ***Encryption Modes*** **(15 min)**

Consider the following encryption mode for applying AES-128 with a key K to a message M that consists of l 128-bit blocks M_1,...,M_l. The sender first picks a random 128-bit string, C_0, which is the first block of the ciphertext. Then for $i > 0$, the i^{th} ciphertext block is given by $C_i = C_{i-1} \oplus$ AES-128$_K(M_i)$. The ciphertext is the concatenation of these individual blocks: $C = C_0 \parallel C_1 \parallel C_2 \parallel ... \parallel C_l$.

(a) What is the intent behind the random value C_0? (I.e., what is it meant to achieve.)

(b) Is this mode of encryption secure? If so, state what the desirable properties it has that make it secure. If not, sketch a weakness.

(c) Suppose we replace the computation of C_i with $C_i = \text{AES-128}_k(C_{i-1} \oplus M_i)$. Does this make the mode of encryption more secure, less secure, or unchanged? Briefly explain your answer.