HW3 Short Answers

Author: Jiahao Dong(jd787), Ming-Han Tsai(mt627)

1.5

1. Why does using GCM prevent mauling and padding oracle attacks?

GCM hashes the plain text so it can prevent mauling attacks. On the other hand, in padding oracle attacks, attackers need to use the previous block and attempt to find the good result by trial-and-error. But GCM's hash result for each block depends on the value of IV and a counter instead of the previous cypher block. Therefore GCM can also prevent padding oracle attacks.

2. For each attack above, explain whether enabling HTTPS for the entire payment site (as opposed to just the login page) prevents the attack if no other counter-measure is applied

HTTPS encrypts data sending via the website, so it could prevent mauling attacks where attackers need to know the paintext cookies. It could also prevent from padding oracle attacks since padding oracle attacks rely on information leakage. HTTPS encrypts the returned messages as well, so it is not possible for the attackers to know if the attack is successful.

2.3

This attack relies on the attacker having knowledge of the SipHash key. Assuming SipHash is a pseudo-random function, does sampling a fresh random SipHash key for the hash table every time the web server is started prevent this attack? Why or why not?

ans:

If the SipHash key is refreshed everytime the server started over, the attacker won't know the key in advance this makes pre-computing collided value list significantly more expensive which then makes the attack loss the computation advantage over the server.

2.5

One suggested countermeasure to denial-of-service attacks is proof of work: forcing clients to perform some computational work and including a proof in the request. Is this an effective countermeasure? Why or why not?

ans:

PoW can be effective against DoS attacks as it makes attack behavior less computationally advantage compare to the server, it also make it possible to offload the limit of number of connections from the memory to CPU power for the server so that it can handle significantly more connection requests coming from PoW protocal. However PoW sheild itself will not suffice as perfect defense mechanism against DDoS when huge data stream is to be received by the server so the core defense has to be designed and deployed upstream in infrastructure components which is load balanced against gigabits of data per second.