Scott Christensen

09/19/16

C.S. 465

H.W. #4 MAC Attacks

From what I understand of performing a MAC Attack, we want to try and manipulate a message from one person to the next in such a way that when encoded and decoded it comes out to be the original message plus some additional message we want to add, thus fooling the authentication. To do this we must first know what the original message is, the message digest, and length of message. What we will attempt to do is to continue the hash from the original MAC by adding a bit of padding and then an additional segment of message that fits in the 512 bit blocks. We can take this new MAC, encrypt it, then when it is decrypted later, should come out as the original message plus the additional segment we added in.

That is about the basis of everything I understand about a Mac Attack, but am still a bit uncertain about it all. Specifically, I'd like to know if this high level process is correct at all. Is it the correct implementation? If so, how can we best add the padding and new message in to fit into the correct block size? How do we get the correct digest? These are some things I'd like to find out in class tomorrow afternoon.