Christopher LaJon Morgan

CS 465

Sep 23, 2013

MAC Attack Homework

The attack works by modifying a SHA-1 algorithm in such a way that one can replicate the state of an original SHA-1 algorithm at the time it finished hashing a given message. If one knows the original message and the MAC generated for a message, then knowing something about the way SHA-1 pads its messages one can replicate the state of the original SHA-1 algorithm and generate an authentic extended message. This is possible because SHA-1 operates on fixed block sizes and a subsequent hash is only dependent upon its preceding block’s hash. Therefore, with a final MAC and original message we have all we need to continue a hash.

The process works by one simply creating a new message that contains the original message, plus the additional padding, size info, and any new additions to the message one would like to make. One now has a new message to send off as the “original”. Then we generate a new MAC by feeding in our new message to our modified SHA-1 that will take the original MAC and being applying it to our modified message. The application of the original MAC begins precisely at our additions to the original message, this is just after the original message’s padding and size info. It is important to note that at this point one must also add some extra bits to the new extended message in order to take into account the size of the secret key. By doing this one will be able to generate a new MAC that appears authentic.