Computer Science 530 - Assignment #3 -- Fall 2020

Due: Monday, November 16th 2020, 11:00 p.m.

This question is taken from the Fall 2018 Final exam:

The security of many functions in computer systems is dependent on the ability to verify the integrity of statements made by third parties, second parties (the party with which one is interacting), or ones own statements. This is certainly the case for key management, where a trusted third party makes a statement about a particular key that is to be used. It also applies to attestation, accreditation, and digital signatures. In the questions that follow, I will describe a statement that is made in a system and you are to tell me who made that statement. More specifically, you are to tell me what key is used to protect the integrity of the statement and if there is a specific name for the key that is used, provide that name. You should also make it clear in your answer, who is in possession of the key needed to protect the integrity of the statement.

For example, if I were to ask: The Kerberos ticket tells us what session key has been assigned for use between a particular client and server.

You are to respond that the ticket is issued by the KDC and that the ticket is encrypted using the key shared between the KDC and the server (sometimes referred to as the server key or Ks).

Now, lets begin:

1. A Resource Record Set in DNSSec containing an A record for www.usc.edu
2. The DS Record for USC.EDU in the EDU Zone using DNSSec provides the public key signing key for the USC.EDU domain/Zone.
3. Information for the security associations (including session keys and checksums) negotiated during phase 2 of IKE (in IPSec).
4. An SSL or TLS Certificate contains the domain name of a web server and the public key that may be used to verify the identity of the server with the specified name.
5. The quoted PCR from a trusted platform module provides information about the checksum of the software running in a process. (Note, this will be covered in the lecture on November 23rd, but the slides are already in the slide deck, you might choose to hold off answering this part until we have discussion in class).
6. The Volume Encryption Key stored on a hard drive, which provides the key for decryption of the rest of the data on the hard drive (Note, this will be covered in the lecture on November 23rd, but the slides are already in the slide deck, you might choose to hold off answering this part until we have discussion in class).

Note that two of the systems that I ask about above will be discussed in the Novmeber 13th lecture. You can answer the rest of this before November 13th and then wait until lecture to answer the final two elements if you wish. Once you answer a few of these, you will know what to listen for during lecture, and that will make the final two elements pretty easy.

INSTRUCTION:

The report must be submitted by 11:00 p.m. on Monday November 16, 2020. To submit your report you will use the USC DEN D2L Assignment Dropbox for CSci530 Fall Semester 2020. Please be sure to include your name in the body of the assignment (i.e. within the Word, PDF, or Text File).

For the three reading reports in this course (of which this is one), students may receive an automatic extension of 48 hours total that may be applied across the three homework assignments. If you turn in one of your assignments 8 hours late, then you will only have 40 hours remaining in extensions to use on subsequent assignments. I suggest not using the whole 48 hours on the first assignment, because if you have an unforseen scheduling issue that arises later in the semester, it will be your problem. Late assignments (beyond any extension) will be assesed 1 full letter penalty per day they are late, and if the topic of an assignment is covered in the lecture following the due date, then the assignment will not be accepted beyond that lecture.