CS5430 Homework 3: Reasoning about Certificates

General Instructions. You may work alone or with one other person from our class on this assignment. If you do work with somebody then form a group on CMS and submit a single set of solutions.

Note: You are strongly urged to work with a partner. Don’t just split the work. You will learn more and the assignment will be easier to finish if you both work together on all problems. We will help you find a partner, if needed. In the past, the average grade given to a pair working together has been significantly higher than the average grade given to individuals working alone.

Due: October 8, 2021 11:59pm. No late assignments will be accepted.

Submit your solution using CMS. Prepare your solution as .pdf, as follows:

- Use 10 point or larger font.
- Submit each problem (as a separate file) into the correct CMS submission box for that problem.

Pointers to our required readings where information is given about inference rules for reasoning about logical formulae involving says and sfor:

- Slides 1-8 of Formal account of hierarchical certificate authorities
- Figure 9.3 (page 218), Figure 9.4 a and b (page 219), Figure 9.5 (page 222) in Credentials-based Authorization
Problem 1 (a). Consider a certificate chain

\[ \langle K_2, N_2 \rangle k_1, \langle K_3, N_3 \rangle k_2, \langle K_4, N_4 \rangle k_3 \]

Suppose we have: \( K_1 \text{ sfor } N_1 \).
What additional trust assumptions (formulated using says and sfor) are required to support the conclusion: \( K_4 \text{ sfor } N_4 \)? Give the formal analysis to derive \( K_4 \text{ sfor } N_4 \) by using your trust assumptions.

Problem 1 (b). In class, we have been considering certificate chains that are paths from the root to a leaf in a tree, where each node \( n_i \) of the tree is a certificate authority that stores a set \( \text{certs}( n_i ) \) of certificates signed by the \( k_i \) the private key of \( n_i \). Each of these certificates \( \langle N, K \rangle k_i \) corresponds to a formula

\[ \text{Trans}( \langle N, K \rangle k_i ) \equiv K_i \text{ says } K \text{ sfor } N \]

So, we have that

\[ \sigma_i \in \text{certs}( n_i ) \text{ implies } \text{Trans}( \sigma_i ) \in \omega( n_i ) \]

where \( \omega( n_i ) \) is the set of beliefs for node \( n_i \).

Suppose --- instead of the tree --- we are given an arbitrary directed graph \( G \), where there is at least one path from every node to every other node. Also, you may assume the following holds:

(i) \( K_i \text{ sfor } n_i \) holds for each node \( n_i \) in the case that \( n_i \) has no incoming edges and thus \( n_i \) could be the start of what we will call a certificate path in \( G \),

(ii) all trust assumptions that are needed to infer \( K_f \text{ sfor } n_f \) where there is a certificate path in \( G \) that ends at a node \( n_q \) and that certificate path contains a certificate \( \langle N_f, K_f \rangle k_q \)

What property must the various belief sets \( \omega( n ) \) satisfy for all nodes \( n \) in this graph.

Problem 2. Some have argued that having \( A \text{ sfor } B \) hold can be interpreted as saying “\( B \text{ trusts } A \)”. Do you agree or disagree with that interpretation? Justify your view by giving a mathematical argument involving beliefs that principals have.
**Problem 3.** The following inference rules assert that principals perform introspection in forming their sets of beliefs.

\[
\frac{A \text{ says } (A \text{ says } P)}{A \text{ says } P} \quad \frac{A \text{ says } P}{A \text{ says } (A \text{ says } P)}
\]

In order to define common situations, like Alice typing into her keyboard or a wire carrying a message from one machine to another, we might define a compound principal: \( A \text{ quoting } B: \)

\[
A \text{ quoting } B \text{ says } P \equiv A \text{ says } B \text{ says } P
\]

What trust assumption(s) would allow the conclusion

\( Alice \text{ says login} \)

from the formula

\( keyboard \text{ quoting Alice says login} \)

Justify why that assumption suffices and is sensible.