Assignment 6: Problems on Trusting Trust
15-316 Software Foundations of Security and Privacy

Due: **11:59pm**, Friday 12/11. **No late days!**
Total Points: 50

1. *A* **speaks for** *B* **(15 points).** Suppose that $\mathsf{mfredrik}$ wishes to *delegate* his authority to claim students using $\texttt{studentOf}(x, \mathsf{mfredrik})$ to his assistant bcook, so that statements of the form $\mathsf{bcook}\ \texttt{says}\ \texttt{studentOf}(x, \mathsf{mfredrik})$ are treated the same as statements of the form $\mathsf{mfredrik}\ \texttt{says}\ \texttt{studentOf}(x, \mathsf{mfredrik})$.

   - **Part 1 (5 points).** Write an authorization logic policy formula Q_d that accomplishes this.
   - **Part 2 (10 points).** Use your policy from Part 1, in addition to the formula wherein bcook says that urvia is a student of $\mathsf{mfredrik}$, i.e. $Q_b \equiv \mathsf{bcook}\ \texttt{says}\ \texttt{studentOf}(\mathsf{urvia}, \mathsf{mfredrik})$, to prove the judgement below.

     $$Q_d, Q_b \vdash \mathsf{mfredrik}\ \texttt{says}\ \texttt{studentOf}(\mathsf{urvia}, \mathsf{mfredrik})$$

2. **Rooting out trust (20 points).** In the questions below, you can use the following identifiers to denote the relevant formulas.

$$
\begin{aligned}
Q_1 &\equiv \texttt{isKey}(\mathsf{ca}, \texttt{pk}_{\mathsf{ca}}) \\
Q_2 &\equiv \texttt{sign}_{\mathsf{sk_{ca}}}(\texttt{isKey}(\mathsf{tpm}, \texttt{pk}_{\mathsf{tpm}})) \\
Q_3 &\equiv \texttt{sign}_{\mathsf{sk_{tpm}}}(\texttt{isKey}(\mathsf{os}, \texttt{pk}_{\mathsf{os}})) \\
Q_4 &\equiv \texttt{sign}_{\mathsf{sk_{mfredrik}}}(\forall x.(\mathsf{os}\ \texttt{says}\ \texttt{read}(x)) \rightarrow (\mathsf{mfredrik}\ \texttt{says}\ \texttt{read}(x))) \\
Q_5 &\equiv \texttt{sign}_{\mathsf{sk_{os}}}(\texttt{read}(\text{'15316-grades.xlsx'})) \\
Q_6 &\equiv \forall x.(\mathsf{tpm}\ \texttt{says}\ \texttt{isKey}(x, \texttt{pk}_x)) \rightarrow \texttt{isKey}(x, \texttt{pk}_x) \\
Q_7 &\equiv \texttt{isCA}(\mathsf{ca}) \\
Q_8 &\equiv \texttt{isKey}(\mathsf{mfredrik}, \texttt{pk}_{\mathsf{mfredrik}})
\end{aligned}
$$

Part 1 (10 points). Which formulas are needed to establish the authenticity of the TPM's public key ($\texttt{pk}_{\mathsf{tpm}}$), and which are needed to authenticate the operating system's, i.e. to prove that $\texttt{isKey}(\mathsf{tpm}, \texttt{pk}_{\mathsf{tpm}},)$ and $\texttt{isKey}(\mathsf{tpm}, \texttt{pk}_{\mathsf{os}},)$?

Part 2 (10 points). It is possible that the network connection between mfredrik's laptop and the file server cannot be trusted, and that a nefarious party is able to intercept, modify, or drop any messages sent between the two. Explain how the scheme outlined in Section 5 of lecture 24 is vulnerable to a replay attack, and how this vulnerability could be addressed.

3. **Countersignatures (15 points).** It is common practice in PKI to have the CA issue weaker certificates that rely on a *countersignature* for verification. So suppose that ca is the certificate authority and cs is the countersigner. Then ca might issue a certificate to cmu that consists of the following.

$$\texttt{sign}_{\mathsf{sk}_{\mathsf{ca}}}(\mathsf{cs}\ \texttt{says}\ \texttt{isKey}(\mathsf{cmu}, \texttt{pk}_{\mathsf{cmu}}) \to \texttt{isKey}(\mathsf{cmu}, \texttt{pk}_{\mathsf{cmu}})) \tag{1}$$

Then cs must issue a second certificate, which comes with an expiration date.

$$\texttt{sign}_{\mathsf{sk}_{\mathsf{cs}}}(\texttt{isbefore}(exp) \to \texttt{isKey}(\mathsf{cmu}, \texttt{pk}_{\mathsf{cmu}})) \tag{2}$$

Explain how one can verify the authenticity of $\texttt{pk}_{\mathsf{cmu}}$ from (1) and (2), along with assumptions $\Gamma = \texttt{isCA}(\mathsf{ca}), \texttt{isKey}(\mathsf{cs}, \texttt{pk}_{\mathsf{cs}}), \texttt{isbefore}(exp)$. That is, prove the following judgement:

$$\Gamma, (1), (2) \vdash \mathsf{ca}\ \texttt{says}\ \texttt{isKey}(\mathsf{cmu}, \texttt{pk}_{\mathsf{cmu}})$$