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

Due: **11:59pm**, Friday 12/6/19. **No late days!**
Total Points: 50

1. **Countersigning (25 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.

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

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

$$\mathtt{sign}_{\mathsf{sk}_{\mathsf{cs}}}(\mathtt{isbefore}(\mathit{exp}) \rightarrow \mathtt{isKey}(\mathsf{cmu}, \mathsf{pk}_{\mathsf{cmu}})) \tag{2}$$

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

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

Part 2. Explain how countersigning can mitigate the effects of key compromise. In particular, describe the consequences of cmu's private key being compromised if the corresponding public key is certified in this way, and how they are less severe than if cmu had obtained a certificate directly from ca. Then describe the consequences of cs's signing key being compromised, and why this is less severe than if ca's signing key is compromised.

2. **Rooting out trust (25 points).** For this question, you should read Section 5 of Lecture 24 for an example application of trusted computing to networked file storage. In the questions below, you can use the following identifiers to denote the relevant formulas.

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

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

Part 2 (10 points). Having authenticated the keys of the TPM and operating system, describe in words the steps that the filesystem will need to take to conclude mfredrik `says` `read`('15316-grades.xlsx'). Note that you are not required to provide a sequent calculus proof for this part.

Part 3 (5 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.