CS5432 Homework 2: Authentication Logics

General Instructions. You may (but do not have to) collaborate with one other student on this assignment. If you do collaborate then both students should form a CMS group and submit their solution to that group. Both students are responsible for all of the answers.

Due: April 12, 2021 at 11:59pm. No late assignments will be accepted.

Submit your solution using CMS. Typeset your solution to produce .pdf, as follows:

- Use 10 point or larger font.
- Start each problem on a separate page.

Problem 1. Slides 61 - 63 (CAL Model for Spec Access) give hints to suggest a formal CAL proof that

A@Intel **says** (read page: Spec)

Fill-in the details by giving a full CAL proof as a list of CAL formulas with a formal justification for each. A justification you give must reference a CAL inference rule from the reading (where such a rule exists) or state a new axiom or rule that arises from the CAL modelling of the protocol.

Problem 2. CAL currently supports two kinds of group principals: Conjunctive Group Principals and Disjunctive Group Principals. A proposal has been made to extend CAL with k-Group Principals (for integer k).

Given a set of principals $G = \{P_1, P_2, \ldots P_n\}$, the worldview $\omega(G^k)$ of the k-Group Principal G^k is defined to contain a belief C if and only if there are exactly k principals $P_i \in G$ satisfying $P_i \; says \; C$.

Are there technical reasons to oppose this extension to CAL? Explain them.

Problem 3. Consider a future where any person can carry an ID card that contains a certificate for the holder's public key. The card carried by a person P would contain $P's$ public key K_P and, to prevent spoofing, a PIN pin_P that P uses to authenticate:

$$Card_P = \langle\, pin_P\, , P\, , K_P\, \rangle$$

Here is a proposed protocol that P might use to start a session with some system that has a card-reader input device.

1. $P \rightarrow Sys:\ \ Card_P$

2. $Sys \rightarrow P$: $challenge\ is$: $\ \ r\ \ (where\ r\ is\ a\ fresh\ nonce)$

3. P uses a calculator to compute $\mathcal{H}(r, mypin)$ where $\mathcal{H}$ is a well known hash function and $mypin$ is a value that P is claiming to be its PIN. (The real P will get this right; an imposter won't guess the right value.)

4. $P \rightarrow Sys:\ \mathcal{H}(r, mypin)$

5. Sys: Compute $v := \mathcal{H}(r, pin_P)$ using stored info from lines 1 and 2. Compare v with $\mathcal{H}(r, mypin)$ received in line 4. If they are equal then conclude
$K_P\ speaksfor\ P$

where P is a sub-principal of P corresponding to this session.

Give a CAL model for how this protocol works, including a CAL derivation of conclusion $K_P\ speaksfor\ P$.

Problem 4. It is not unusual in security discussions to hear somebody say "A is trusted by B", meaning that A will only undertake actions that B is expecting. Give a CAL formula for modelling this situation. Justify your answer.