

1. (20 points) Consider the following plausible inference rule:

$$\frac{P \mid P \text{ says } \varphi}{P \text{ says } \varphi}$$

Determine whether or not this rule is *sound*, and justify your answer as follows:

- If you determine that the rule is sound, prove its soundness.
- If you determine that the rule is not sound, give (and explain!) a particular Kripke structure, principal P and formula φ that demonstrate the lack of soundness.

SAMPLE ANSWER: The rule is **not sound**, as demonstrated by the Kripke structure $\mathcal{M} = \langle W, I, J \rangle$, where:

$$\begin{aligned} W &= \{a, b\} \\ I(p) &= \{a\} \\ J(Pat) &= \{(a, b)\} \end{aligned}$$

Note that $J(Pat \mid Pat) = J(Pat) \circ J(Pat) = \emptyset$.

- $\mathcal{M} \models Pat \mid Pat \text{ says } p$, because:

$$\begin{aligned} \mathcal{E}_{\mathcal{M}}[Pat \mid Pat \text{ says } p] &= \{w \mid J(Pat \mid Pat)w \subseteq \mathcal{E}_{\mathcal{M}}[p]\} \\ &= \{w \mid J(Pat \mid Pat)w \subseteq \{a\}\} \\ &= \{a, b\} = W. \end{aligned}$$

- In contrast, $\mathcal{M} \not\models Pat \text{ says } p$, because:

$$\begin{aligned} \mathcal{E}_{\mathcal{M}}[Pat \mid Pat \text{ says } p] &= \{w \mid J(Pat)w \subseteq \mathcal{E}_{\mathcal{M}}[p]\} \\ &= \{w \mid J(Pat)w \subseteq \{a\}\} \\ &= \{b\} \neq W. \end{aligned}$$

2. (14 points) Ed and Beth have recently signed a contract to purchase Alexander's house. The contract has two provisions by which Ed and Beth can cancel the sale:

- A *home-inspection condition*: Ed and Beth have seven business days to have the house inspected by an official inspector.

If they are unhappy with the results, then they can back out of the sale; if they are happy with the results, they will both need to sign paperwork that indicates that they are **waiving the home-inspection condition**.

- A *home-finance condition*: Ed and Beth have fifteen business days to arrange for a bank loan.

If they are unable to find suitable financing, then they can back out of the sale; if they arrange financing, they will both need to sign paperwork that indicates that they are **waiving the financing condition**.

For the purposes of this question, there are two specific access rights of interest:

- $\langle waive, insp \rangle$: the waiving of the home-inspection condition
- $\langle waive, fin \rangle$: the waiving of the financing condition

Answer the following questions regarding the relevant certifications, credentials, and access-control policies needed for Alexander's lawyer to recognize Ed and Beth's actions with respect to the purchase contract. **All your answers should be expressions in the access-control logic.**

IMPORTANT NOTE: For this question, you **do not** need to distinguish between a principal and his/her signature or signed name.

- (a) For the sale to happen, Ed and Beth must **jointly** waive **each** of the two conditions. However, the two conditions do not have to be waived at the same time (for example, they could waive one today and the other next Tuesday).

Express Ed and Beth's joint authority to waive the home-inspection and financing conditions.

$$\begin{aligned} & Ed \& Beth \text{ controls } \langle waive, insp \rangle \\ \wedge & Ed \& Beth \text{ controls } \langle waive, fin \rangle \end{aligned}$$

- (b) Ed will be traveling to Antarctica soon. Therefore, Ed and Beth's lawyer has arranged for Ed to sign a *power-of-attorney form* that gives Beth the legal right to sign financial and real-estate documents on Ed's behalf.

This form corresponds to a delegation certificate (signed by Ed) stating that Beth is Ed's proxy with respect to each of the waivable conditions. Express this form in the access-control logic.

$$\begin{aligned} & Ed \text{ says } ((Beth \text{ reps } Ed \text{ on } \langle waive, insp \rangle) \\ & \wedge (Beth \text{ reps } Ed \text{ on } \langle waive, insp \rangle)) \end{aligned}$$

- (c) The home inspection is successfully completed while Ed is away, so Beth signs a form to waive the home-inspection condition. Specifically, Beth signs twice: (1) she signs her name as a purchaser, and (2) she signs Ed's name as a purchaser, including her own initials to indicate that she is signing his name on his behalf.

Express this signed waiver form as an expression in the logic.

$$Beth \& (Beth | Ed) \text{ says } \langle waive, insp \rangle$$

- (d) Assume that Alexander's lawyer has been provided a copy of Ed's power-of-attorney form.

What **addition certificates, recognition(s) of authority, or trust assumptions** must Alexander's lawyer make to accept the legality of the waiver of the home-inspection condition? (Include only those that are absolutely necessary.)

Ed controls (Beth reps Ed on ⟨waive, insp⟩)

3. (26 points) A local consortium of hospitals and medical centers—guided by the state's Health Authority (HA)—has recently established an electronic system for maintaining patient medical records. Among this consortium are Local Community Hospital (LCH) and and Medical Research Hospital (MRH).

The following operating protocols have been established:

- All requests to access the patient-records server must be digitally signed.
- Authorizations to access patient records are group-based: only doctors are allowed to modify patient records, while doctors and nurses are allowed to read patient records.

Note: For the purposes of this question, *any* doctor can modify *any patient's* records, and *any* doctor or nurse can read *any patient's* records.

- Medical personnel must be jointly credentialed by the Health Authority and by a member institution.
For example, to be recognized as a doctor, an individual must provide digital certificates from the HA as well as from a member institution.
- Each medical institution in the consortium is responsible for certifying the public keys of its employees.
- As part of its role as consortium guide, HA is willing to certify the top-level public keys of member institutions.
- For practical reasons, the patient-records server and the electronic-medical records themselves are housed at MRH. Consequently, the public keys of MRH (K_M) and of the Health Authority (K_H) are directly installed on the patient-record server.

In addition, the following facts pertain to LCH:

- The public key of LCH is K_L .
- Ty is a doctor employed at LCH, which has assigned him the public-key K_T .
- Rae is one of Ty's patients at LCH.

In the questions that follow, let the propositions *read* and *write* correspond to efforts to read and write to Rae's medical records. Let DR and NURSE refer to the recognized groups of doctors and nurses, respectively.

Answer the following questions regarding the certifications, credentials, and access-control policies needed for the patient-records system. **All your answers should be expressions in the access-control logic.**

- (a) What is the patient-records server's **access policy** with regards to Rae's medical records?

$$(\text{DR controls read}) \wedge (\text{DR controls write}) \wedge (\text{NURSE controls read})$$

- (b) LCH must digitally certify that Ty is a doctor. What is the form of this certificate?

$$K_L \text{ says } (Ty \Rightarrow \text{DR})$$

- (c) What is the patient-records server's **recognition of authority** with respect to Ty's credentials as a doctor?

$$HA \ \& \ LCH \text{ controls } (Ty \Rightarrow \text{DR})$$

- (d) When Ty attempts to access Rae's medical records from the patient-records server, what is the form of his request?

$$K_T \text{ says read}$$

- (e) What are the additional **certificates, recognition of authority, and trust assumptions regarding keys** that are necessary for the patient-records server to determine that the request to access Rae's records should be granted?

$$K_H \Rightarrow HA$$

$$K_H \text{ says } (K_L \Rightarrow LCH)$$

$$HA \text{ controls } (K_L \Rightarrow LCH)$$

$$K_L \text{ says } (K_T \Rightarrow Ty)$$

$$LCH \text{ controls } (K_T \Rightarrow Ty)$$

$$K_H \text{ says } (Ty \Rightarrow \text{DR})$$