FMSP: Solution Attempt for exam 2020-07

Pizzaiolo

June 24, 2022

Preamble

Feel free to edit it to add more examples, fix mistakes, etc. If you do so, please update both the .tex and .pdf files. And obviously no guarantee for anything.

Problem 1

a)

Does following program perserve secrecy and/or integrity? If yes, give a type derivation. If not, give a counter-example.

$$(\nu v_1 \colon HH)(\nu v_2 \colon HL)(\nu k_1 \colon SymK^{HH}[LH])(\nu k_2 \colon SymK^{HH}[HL, HL, HH])\overline{b}\langle\{|[v_1, v_2, k_1]|\}^s_{k_2}\rangle.0$$

Intuition: First of, the channel b has no restriction, thus it has type $C^{LL}[LL, \ldots, LL]$. The ciphertext has low confidentiality (see the SymEnc rule), therefore for secrecy $\mathcal{L}_C(c) \sqsubseteq_C \mathcal{L}_C(b)$ should hold. For integrity, we use a channel with $\mathcal{L}_I(b) = L$, therefore $\mathcal{L}_I(c) \sqsubseteq_I \mathcal{L}_I(b)$ should always hold.

So if the intuition is right, type checking should work.

Defining Γ We will try to typecheck it for a Γ, where all unspecified values in the program have type LL. In our case this is $\Gamma = \{b \colon LL\}$. Note that $img(\Gamma) = \{LL\}$ holds, as gamma only maps to LL (this is necessary to use Theorem 1).

Moving restrictions into the typing environment .

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(1)}{\Gamma, v_1 \colon HH, v_2 \colon HL, k_1 \colon SymK^{HH}[LH], k_2 \colon SymK^{HH}[HL, HL, HH] \vdash \overline{b}\langle\{|[v_1, v_2, k_1]|\}^s_{k_2}\rangle.0}}{\Gamma, v_1 \colon HH, v_2 \colon HL, k_1 \colon SymK^{HH}[LH] \vdash (\nu k_2 \colon SymK^{HH}[HL, HL, HH])\overline{b}\langle\{|[v_1, v_2, k_1]|\}^s_{k_2}\rangle.0}\ \text{RES}}{\Gamma, v_1 \colon HH, v_2 \colon HL \vdash (\nu k_1 \colon SymK^{HH}[LH])(\nu k_2 \colon SymK^{HH}[HL, HL, HH])\overline{b}\langle\{|[v_1, v_2, k_1]|\}^s_{k_2}\rangle.0}\ \text{RES}}{\Gamma, v_1 \colon HH \vdash (\nu v_2 \colon HL)(\nu k_1 \colon SymK^{HH}[LH])(\nu k_2 \colon SymK^{HH}[HL, HL, HH])\overline{b}\langle\{|[v_1, v_2, k_1]|\}^s_{k_2}\rangle.0}\ \text{RES}}{\Gamma \vdash (\nu v_1 \colon HH)(\nu v_2 \colon HL)(\nu k_1 \colon SymK^{HH}[LH])(\nu k_2 \colon SymK^{HH}[HL, HL, HH])\overline{b}\langle\{|[v_1, v_2, k_1]|\}^s_{k_2}\rangle.0}\ \text{RES}$$

Applying the OUT rule and changing the ciphertext type I already used subsumption for the ciphertext at this stage, to give it type LH. This will later on allow us to make the key of type HH (because it must have the same integrity label as the ciphertext). For the sake of readability, let $\Gamma_2 = \Gamma, v_1 \colon HH, v_2 \colon HL, k_1 \colon SymK^{HH}[LH], k_2 \colon SymK^{HH}[HL, H$

$$\dfrac{\dfrac{\dfrac{(2)}{\Gamma_2 \vdash \{|[v_1, v_2, k_1]|\}^s_{k_2} \colon LH} \quad LH \leq LL}{\Gamma_2 \vdash \{|[v_1, v_2, k_1]|\}^s_{k_2} \colon LL}\ \text{SUBSUMPTION} \quad \dfrac{\dfrac{(3)}{\Gamma_2 \vdash \diamond}}{\Gamma_2 \vdash 0}\ \text{STOP} \quad \dfrac{(4)}{\Gamma_2 \vdash b \colon C^{LL}[LL]}}{\Gamma_2 \vdash \overline{b}\langle\{|[v_1, v_2, k_1]|\}^s_{k_2}\rangle.0}\ \text{OUT}}{(1)}$$

Proving the key type and extracting the messages Continuation of (2).

$$\dfrac{\dfrac{\dfrac{(3)}{\Gamma_2 \vdash \diamond} \quad k_2 \colon SymK^{HH}[HL, HL, HH] \text{ in } \Gamma_2}{\Gamma_2 \vdash k_2 \colon SymK^{HH}[HL, HL, HH]}\ \text{ATOM} \quad \dfrac{\dfrac{(5)}{\Gamma_2 \vdash v_1 \colon HL} \quad \dfrac{(6)}{\Gamma_2 \vdash v_2 \colon HL} \quad \dfrac{(7)}{\Gamma_2 \vdash k_1 \colon HH}}{\Gamma_2 \vdash [v_1, v_2, k_1] \colon [HL, HL, HH]}\ \text{LIST}}{\Gamma_2 \vdash \{|[v_1, v_2, k_1]|\}^s_{k_2} \colon LH}\ \text{SymEnc}}{(2)}$$

Proving the channel type Continuation of (4):

$$\dfrac{\dfrac{\dfrac{(3)}{\Gamma_2 \vdash \diamond} \quad b \colon LL \text{ in } \Gamma}{\Gamma_2 \vdash b \colon LL}\ \text{ATOM} \quad LL \leq C^{LL}[LL]}{\Gamma_2 \vdash b \colon C^{LL}[LL]}\ \text{SUBSUMPTION}}{(4)}$$

Proving the message types Continuation of (5), (6) and (7):

$$\dfrac{\dfrac{\dfrac{(3)}{\Gamma_2 \vdash \diamond} \quad v_1 \colon HH \text{ in } \Gamma_2}{\Gamma_2 \vdash v_1 \colon HH}\ \text{ATOM} \quad HH \leq HL}{\Gamma_2 \vdash v_1 \colon HL}\ \text{SUBSUMPTION}}{(5)}$$

$$\dfrac{\dfrac{\dfrac{(3)}{\Gamma_2 \vdash \diamond} \quad v_2 \colon HL \text{ in } \Gamma_2}{\Gamma_2 \vdash v_2 \colon HL}\ \text{ATOM}}{(6)}$$

$$\dfrac{\dfrac{\dfrac{(3)}{\Gamma_2 \vdash \diamond} \quad k_1 \colon SymK^{HH}[LH] \text{ in } \Gamma_2}{\Gamma_2 \vdash k_1 \colon SymK^{HH}[LH]}\ \text{ATOM} \quad SymK^{HH}[LH] \leq HH}{\Gamma_2 \vdash k_1 \colon HH}\ \text{SUBSUMPTION}}{(7)}$$

Proving the well-formedness ($\Gamma_2 \vdash \diamond$) Here we prove, that it is well-formed with respect to Γ_2. Essentially we go through all types in the typing environment Γ_2 and assert that **if** they are a key or channel type, they are HH. (I've abbreviated ENVIRONMENT as ENV and I'm using an inofficial shortcut syntax for the 3rd precondition of environemnt (the implication), just to save space.)

$$\dfrac{\dfrac{\dfrac{\dfrac{(8) \quad v_2 \notin dom(\Gamma) \quad HL \notin \{\dots\}}{\Gamma, v_1 : HH, v_2 : HL \vdash \diamond}\,\text{ENV} \quad k_1 \notin dom(\Gamma) \quad HH = HH}{\Gamma, v_1 : HH, v_2 : HL, k_1 : SymK^{HH}[LH] \vdash \diamond}\,\text{ENV} \quad k_2 \notin dom(\Gamma) \quad HH = HH}{\Gamma, v_1 : HH, v_2 : HL, k_1 : SymK^{HH}[LH], k_2 : SymK^{HH}[HL, HL, HH] \vdash \diamond}\,\text{ENV}}{\Gamma_2 \vdash \diamond}}{(3)}$$

Continuing with (8). The same as before, but now we insert our definition of Γ and finish it with the EMPTY rule.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\emptyset \vdash \diamond}\,\text{EMPTY} \quad b \notin dom(\emptyset) \quad LL \notin \{\dots\}}{\emptyset, b : LL \vdash \diamond}\,\text{ENV}}{\Gamma \vdash \diamond}\,\text{our definition of } \Gamma \quad v_1 \notin dom(\Gamma) \quad HH \notin \{\dots\}}{\Gamma, v_1 : HH \vdash \diamond}\,\text{ENV}}{(8)}$$

Conclusion All preconditions for our program are satisfied, hence it typechecks. Looking at Theorem 1 (Typing implies Secrecy and Integrity), for our $\Gamma = \{b : LL\}$, we have already proven $\Gamma \vdash P$. Furthermore, our Γ maps every type to LL, so it fulfills the condition $img(\Gamma) = LL$). Thus it preserves secrecy and integrity.