

Protocoles et clauses de Horn

Exercice 1

On considère l'ensemble de clauses $\mathcal{C}_{\mathcal{I}}$ correspondant aux règles de l'intrus pour le chiffrement symétrique :

$$\mathcal{C}_{\mathcal{I}} = \{\neg I(x) \vee \neg I(y) \vee I(\{x\}_y), \neg I(\{x\}_y) \vee \neg I(y) \vee I(x)\}$$

On considère l'ordre \leq sur les termes suivant : soient t_1 et t_2 deux termes, $t_1 \leq t_2$ si t_1 est un sous-terme de t_2 .

1. Montrer que l'ensemble de clauses $C_1 = \mathcal{C}_{\mathcal{I}} \cup \{I(k_1), I(\{k_2\}_{k_1}), I(a), \neg I(\{a\}_{k_2})\}$ est insatisfiable.
2. Montrer que l'ordre \leq est un ordre relevable. On rappelle que \leq est relevable si pour tous termes t_1, t_2 , pour toute substitution θ , $t_1 \leq t_2 \Rightarrow t_1\theta \leq t_2\theta$.
3. Montrer *par résolution ordonnée* que C_1 est insatisfiable.
4. Montrer que l'ensemble de clauses $C_1 = \mathcal{C}_{\mathcal{I}} \cup \{I(k_1), I(a), \neg I(\{a\}_{k_2})\}$ est satisfiable. On pourra utiliser la résolution ordonnée pour l'ordre \leq .

Exercice 2

On considère le protocole suivant :

$$\begin{aligned} A &\rightarrow S : \{A, B, K_{ab}\}_{K_{as}} \\ S &\rightarrow B : \{A, B, K_{ab}\}_{K_{bs}} \end{aligned}$$

Chaque agent X partage une clef symétrique K_{xs} avec le serveur. A envoie au serveur une clef de session K_{ab} à l'aide d'une clef partagée K_{as} avec le serveur, en indiquant son identité et celle de B . Le serveur S répond en transmettant la clef de session à B à l'aide de sa clef partagée K_{bs} . On souhaite bien sûr que la clef de session K_{ab} reste secrète entre A et B (et le serveur).

On souhaite montrer que le protocole est sûr pour un nombre *quelconque* de sessions.

Les règles de l'intrus sont représentées par l'ensemble de clauses \mathcal{C}_I .

$$\mathcal{C}_I = \left\{ \begin{array}{l} \neg I(x) \vee \neg I(y) \vee I(\langle x, y \rangle) \\ \neg I(x) \vee \neg I(y) \vee I(\{x\}_y) \\ \neg I(\{x\}_y) \vee \neg I(y) \vee I(x) \\ \neg I(\langle x, y \rangle) \vee I(x) \\ \neg I(\langle x, y \rangle) \vee I(y) \end{array} \right\}$$

Les connaissances initiales sont représentées par l'ensemble de clauses $\mathcal{C}_{\text{init}}$.

$$\mathcal{C}_{\text{init}} = \{I(a), I(b), I(i), I(k_{is})\}$$

1. Modéliser le protocole en clauses de Horn.

2. Montrer *par résolution ordonnée* (pour l'ordre donné en cours) que l'ensemble de clauses $\mathcal{C}_I \cup \{I(\langle a, k \rangle), I(\{s\}_k), \neg I(s)\}$ est insatisfiable.
3. Comment montrer que le protocole préserve le secret de la donnée k_{ab} ?
4. On considère le protocole modifié :

$$\begin{aligned} A &\rightarrow S : A, \{B\}_{K_{as}}, \{K_{ab}\}_{K_{as}} \\ S &\rightarrow B : A, B, \{K_{ab}\}_{K_{bs}} \end{aligned}$$

- (a) Comment modifier l'ensemble de clauses \mathcal{C}_P pour qu'il corresponde au nouveau protocole ? On notera l'ensemble ainsi obtenu par \mathcal{C}'_P .
- (b) Montrer, par résolution ordonnée (pour l'ordre donné en cours), que $\mathcal{C}'_P \cup \mathcal{C}_I \cup \mathcal{C}_{\text{init}} \cup \{\neg I(k_{ab})\}$ est insatisfiable.

Exercice 3 (explique pourquoi ProVerif trouve de fausses attaques)

Exhiber un protocole qui préserve le secret d'une donnée et tel que l'ensemble de clauses associé ne soit pas satisfiable.

Indice : La modélisation en clauses de Horn modélise mal la fraîcheur des nonces : le même nonce (la même clef) peut être obtenu plusieurs fois.

Exercice 4 (court mais difficile)

Montrer que la résolution binaire seule (sans la factorisation) n'est pas complète. Autrement dit, exhiber un ensemble de clauses insatisfiable pour lequel la classe fausse n'est pas dérivable par résolution binaire seule.