Protokollsicherheit

Resolutionsalgorithmus

Horn Klauseln

Terme

$$M, N ::= x \mid a[M_1, \ldots, M_n] \mid f(M_1, \ldots, M_n)$$

Fakten

$$F ::= \mathsf{att}(M) \mid p(M_1, \ldots, M_n)$$

Horn-Klausel

$$R ::= F_1 \wedge \cdots \wedge F_n \supset F$$

Wir fassen $F_1 \wedge \cdots \wedge F_n$ als Multimenge von Fakten auf.

Horn Klauseln

Terme

$$M, N ::= x \mid a[M_1, \ldots, M_n] \mid f(M_1, \ldots, M_n)$$

Fakten

$$F ::= \mathsf{att}(M) \mid p(M_1, \ldots, M_n)$$

Horn-Klausel

$$R ::= F_1 \wedge \cdots \wedge F_n \supset F$$

Wir fassen $F_1 \wedge \cdots \wedge F_n$ als Multimenge von Fakten auf.

Die Klausel $H_1 \supset C_1$ **subsumiert** die Klausel $H_2 \supset C_2$, falls es eine Subsitution σ gibt, so dass $C_1\sigma = C_2$ und $H_1\sigma \subseteq H_2$ gilt.

(Für den obigen Resolutionsalgorithmus ist es wichtig, dass $H_1\sigma \subseteq H_2$ als Multimengeninklusion aufgefasst wird.)

Herleitung

Die Herleitbarkeit von Fakten aus einer Klauselmenge lässt sich direkt wie folgt definieren:

Die Herleitungsregel

$$\frac{F_1 \qquad \dots \qquad F_n}{F_0}\,(R)$$

kann angewendet werden falls

- $F_0, \dots, F_n$ geschlossene Fakten sind, und
- die Klausel $F_1 \wedge \dots \wedge F_n \supset F_0$ von R subsumiert wird.

(Kurzschreibweise für Backchaining-Regel von letzter Woche).

Ein geschlossener Fakt F ist **herleitbar**, falls es einen Herleitungsbaum ohne Blätter mit Wurzel F gibt.

Tiefensuche

Beginne mit dem zu zeigenden Fakt F.
Baue einen Herleitungsbaum auf:

1. Wähle einen noch zu zeigenden Fakt aus (ein Blatt).
2. Wähle eine Klausel $R = H \supset C$ aus, so dass C mit F unifiziert. Wende Regel (R) am ausgewählten Blatt mit der allgemeinstmöglichen Substitution an.
3. Kann man die Herleitung so nicht weiter aufbauen, so geht man zur letzten Position zurück, bei der eine andere Auswahl hätte getroffen werden können, und probiert diese aus.
4. Man geht ebenfalls zurück, wenn man in einen Zyklus geraten ist, d.h. wenn die partielle Herleitung schon von ein Spezialfall einer bereits früher betrachteten ist.

Wir sind vor allem auch daran interessiert, was *nicht* auf diese Art hergeleitet werden kann ($\mathtt{att}(secret)$).

Resolutionsregel

$$R = F_1 \wedge \cdots \wedge F_n \supset F \qquad R' = F'_1 \wedge \cdots \wedge F'_{n'} \supset F'$$

Angenommen F unifiziert mit F'_i.
Sei θ der allgemeinste Unifikator von F und F'_i.

Dann sei $R \circ_{F_i} R'$ die Klausel

$$F_1\theta \wedge \cdots \wedge F_n\theta \wedge F'_1\theta \wedge \cdots F'_{i-1}\theta \wedge F'_{i+1}\theta \wedge \cdots \wedge F'_{n'}\theta \supset F'\theta.$$

Diese Klausel ist *die Resolution von R' mit R bezüglich F_i*.

Tiefensuche

Die Tiefensuche kann rekursiv implementiert werden.

$$\text{deriv}(R, \mathcal{K}, \mathcal{R}) = \begin{cases} \emptyset & \text{falls } R \text{ von Klausel in } \mathcal{K} \text{ subsumiert wird,} \\ \{R\} & \text{falls } R \text{ die Form “} \supset F\text{” hat,} \\ \bigcup\{\text{deriv}(R' \circ_F R, \mathcal{K} \cup \{R\}, \mathcal{R}) & \\ \qquad \mid R' \in \mathcal{R}, R' \circ_F R \text{ definiert}\} & \text{sonst.} \end{cases}$$

Um Termination bei der Analyse von Protokollen zu erreichen, wird die Suche durch eine Auswahlfunktion gelenkt: Die Resolutionsregel wird nur auf ausgewählte Fakten angewendet.

Auswahlfunktion

Eine **Auswahlfunktion** ist eine beliebige Funktion mit der Eigenschaft $\mathsf{sel}(F_1 \wedge \cdots \wedge F_n \supset F) \subseteq \{F_1, \ldots, F_n\}$.

Konkret für Protokolle:

$\mathsf{sel}(F_1 \wedge \cdots \wedge F_n \supset F) = \emptyset$ wenn $F_i = \mathsf{att}(x)$ für allel $1 \leq i \leq n$.

$\mathsf{sel}(F_1 \wedge \cdots \wedge F_n \supset F) = \{F_i\}$ andernfalls (F_i ist der größte Fakt).

Beispiel:

$$\mathsf{sel}(\mathsf{att}(\mathsf{enc}(m, \mathsf{pk}(sk))) \wedge \mathsf{att}(sk) \supset \mathsf{att}(m)) = \{\mathsf{att}(\mathsf{enc}(m, \mathsf{pk}(sk)))\}$$

Sättigungsalgorithmus

Forme die Klauselmenge äquivalent so um, dass es nur noch Klauseln R mit $\mathsf{sel}(R) = \emptyset$ gibt.

Eingabe: Menge von Horn-Klauseln $\mathcal{R}_0$.

1. Setze $\mathcal{R} := \emptyset$.
   Für alle $R \in \mathcal{R}_0$, setze $\mathcal{R} := \{R\} \cup \mathcal{R}$ und eliminiere subsumierte Regeln.

2. Solange, bis sich $\mathcal{R}$ nicht mehr ändert:
   Für alle $R \in \mathcal{R}$ mit $\mathsf{sel}(R) = \emptyset$:
   Für alle $R' \in \mathcal{R}$, alle $F_0 \in \mathsf{sel}(R')$, so dass $R \circ_{F_0} R'$ definiert ist:
   Setze: $\mathcal{R} := \mathcal{R} \cup \{R \circ_{F_0} R'\}$ und eliminiere subsumierte Regeln von $\mathcal{R}$.

3. Das Ergebnis ist $\mathsf{saturate}(\mathcal{R}_0) := \{R \in \mathcal{R} \mid \mathsf{sel}(R) = \emptyset\}$.

Sättigungsalgorithmus

Lemma: Sei F ein geschlossener Fakt. Dann ist F aus $\mathcal{R}$ herleitbar genau dann wenn F aus $\mathsf{saturate}(\mathcal{R})$ herleitbar ist.

Beweis: Tafel.
Siehe auch [Blanchet – Using Horn Clauses for Analysing Security Protocols].

Tiefensuche mit Auswahlfunktion

$$\text{deriv}(R, \mathcal{K}, \mathcal{R}) = \begin{cases} \emptyset & \text{falls } R \text{ von Klausel in } \mathcal{K} \text{ subsumiert ist,} \\ \{R\} & \text{falls } \text{sel}(R) = \emptyset, \\ \bigcup\{\text{deriv}(R' \circ_F R, \mathcal{K} \cup \{R\}, \mathcal{R}) & \\ \quad \mid R' \in \mathcal{R}, F \in \text{sel}(R), R' \circ_F R \text{ definiert}\} & \text{sonst.} \end{cases}$$

$$\text{derivable}(F, \mathcal{R}) = \text{deriv}(F \supset F, \emptyset, \mathcal{R})$$

Lemma: Sei F' eine geschlossene Instanz von F. Dann ist F' aus $\text{saturate}(\mathcal{R}_0)$ herleitbar, genau dann wenn es eine Klausel $H \supset C$ in $\text{derivable}(F, \text{saturate}(\mathcal{R}_0))$ und eine Substitution σ gibt, so dass $F' = C\sigma$ gilt und so dass alle Fakten in $H\sigma$ mit den Klauseln aus $\text{saturate}(\mathcal{R}_0)$ herleitbar sind.

Hauptergebnis

Theorem:
Sei sel die konkret gewählte Auswahlfunktion für $\mathsf{att}(x)$. Sei $\mathcal{R}_0$ eine Klauselmenge, die eine Klausel der Form $\supset \mathsf{att}(a[\,])$ enthält.

Dann ist ein geschlossener Fakt F aus $\mathcal{R}_0$ herleitbar genau dann wenn $\mathsf{derivable}(F, \mathsf{saturate}(\mathcal{R}_0)) \neq \emptyset$ gilt.

(Für F wird insbesondere $\mathsf{att}(\mathsf{secret})$ verwendet.)