OVSP definitions

Protocol specification

$$\begin{array}{lll} \mathit{RoleTerm} & ::= & \mathit{Var} \,|\, \mathit{Fresh} \,|\mathit{Role}|\, \mathit{Func}\,(\mathit{RoleTerm}^*) \\ & & |\, (\mathit{RoleTerm}, \mathit{RoleTerm}) |\, \{\!|\, \mathit{RoleTerm} \,|\!\}_{\mathit{RoleTerm}} \\ & & |\, \mathit{sk}(\mathit{RoleTerm}) \,|\, \mathit{pk}(\mathit{RoleTerm}) \,|\, k(\mathit{RoleTerm}, \mathit{RoleTerm}) \end{array}$$

$$\begin{array}{lll} \mathit{RoleEvent}_R & ::= & \mathit{send}_{\mathit{Label}}(R, \mathit{Role}, \mathit{RoleTerm}) \\ & & |\, \mathit{recv}_{\mathit{Label}}(\mathit{Role}, R, \mathit{RoleTerm}) \\ & & |\, \mathit{claim}_{\mathit{Label}}(R, \mathit{Claim}[, \mathit{RoleTerm}]) \end{array}$$

$$\mathit{RoleEvent} = \bigcup_{R \in \mathit{Role}} \mathit{RoleEvent}_R$$

$$P(R) = (KN_0(R), s) \in \mathcal{P}(\mathit{RoleTerm}) \times \mathit{RoleEvent}^*_R$$

$$\mathit{RoleSpec} = \{(kn, s) \mid kn \in \mathcal{P}(\mathit{RoleTerm}) \ \wedge \ \forall rt(rt \in kn \rightarrow vars(rt) = \emptyset) \\ \wedge\, s \in \mathit{RoleEvent}^* \wedge \ \ wellformed(s)\}$$

$$Protocol = \mathit{Role} \rightharpoondown \mathit{RoleSpec}$$

Deduction on terms

$M \vdash t$ means that t can be deduced knowing M

$\vdash$ is the least relation with the following properties:

$$\begin{array}{lrll} \text{if} & t \in M & \text{then} & M \vdash t \\ \text{if} & M \vdash t_1 \text{ and } M \vdash t_2 & \text{then} & M \vdash (t_1, t_2) \\ \text{if} & M \vdash (t_1, t_2) & \text{then} & M \vdash t1 \text{ and } M \vdash t_2 \\ \text{if} & M \vdash t \text{ and } M \vdash k & \text{then} & M \vdash \{\!|\, t \,|\!\}_k \\ \text{if} & M \vdash \{\!|\, t \,|\!\}_k \text{ and } M \vdash k^{-1} & \text{then} & M \vdash t \\ \text{if} & M \vdash t_1 \text{ and } \ldots \text{ and } M \vdash t_n & \text{then} & M \vdash f\,(t_1, \ldots, t_n) \end{array}$$

Protocol execution

$$\begin{array}{lll} \mathit{RunTerm} & ::= & \mathit{Var}^{\#RID} \,|\, \mathit{Fresh}^{\#RID} \,|\mathit{Role}^{\#RID}|\, \mathit{Agent}|\, \mathit{Func}\,(\mathit{RunTerm}^*) \\ & & |\, (\mathit{RunTerm}, \mathit{RunTerm}) |\, \{\!|\, \mathit{RunTerm} \,|\!\}_{\mathit{RunTerm}} \\ & & |\, \mathit{AdversaryFresh} \\ & & |\, \mathit{sk}(\mathit{RunTerm}) \,|\, \mathit{pk}(\mathit{RunTerm}) \,|\, k(\mathit{RunTerm}, \mathit{RunTerm}) \end{array}$$

$$\mathit{Inst} = \mathit{RID} \times (\mathit{Role} \rightharpoonup \mathit{Agent}) \times (\mathit{Var} \rightharpoonup \mathit{RunTerm}) \ \mathit{inst} = (\theta, \rho, \sigma) \in \mathit{Inst}$$

$Match \subseteq \mathit{Inst} \times \mathit{RoleTerm} \times \mathit{RunTerm} \times \mathit{Inst}$
$Match(\mathit{inst}, \mathit{pt}, m, \mathit{inst}')$ holds if
$\mathit{inst} = (\theta, \rho, \sigma)$, $\mathit{inst}' = (\theta, \rho, \sigma')$, $\mathit{dom}(\sigma') = \mathit{dom}(\sigma) \cup vars(\mathit{pt})$,
$\mathit{inst}'(\mathit{pt}) = m$ for $\mathit{pt} \in \mathit{RoleTerm}$ and $m \in \mathit{RunTerm}$,
$\sigma \subseteq \sigma'$ and $\sigma'(v) \in \mathit{type}(v)$ for any $v \in \mathit{dom}(\sigma')$,

where $vars(\mathit{pt})$ is the set of variables from Var which appear in pt, and $\mathit{type}(v)$ is a function that depends on the agent model.

$Run = Inst \times RoleEvent^{*}$ $runsof : Protocol \times Roles \to \mathcal{P}(Run)$

$$\begin{aligned} runsof(P, R) = \{(inst, s) \mid & \text{ there exists } kn \text{ such that } P(R) = (kn, s) \\ & inst = (\theta, \rho, \sigma) \text{ with } dom(\rho) = roles(s)\} \text{ where } R \in dom(P). \end{aligned}$$

For $F \subseteq Run$ we define $runIds(F) = \{\theta \mid ((\theta, \rho, \sigma), s) \in F \text{ for some } \rho, \sigma, s\}$

Operational semantics

$State = \mathcal{P}(RunTerm) \times \mathcal{P}(Run)$

$st = \langle\!\langle AKN, F \rangle\!\rangle \in State$ where AKN is the adversary knowledge and $F \subseteq Run$ are the runs that has to be executed.

$RunEvent = Inst \times (RoleEvent \cup \{create(R) \mid R \in Role\}$

Labeled Transition System for Operational Semantics: $(State, RunEvent, \to, st_0(P))$
where $st_0(P) = \langle\!\langle AKN_0(P), \emptyset \rangle\!\rangle$ where $AKN_0(P)$ is the initial adversary knowledge.

The Needham-Schroeder protocol

$$\begin{array}{llll} NS(i) = & (\{i, r, ni, sk(i), pk(i), pk(r)\}, & NS(r) = & (\{i, r, nr, sk(r), pk(r), pk(i)\}, \\ & [send_1(i, r, \{\!| ni, i |\!\}_{pk(r)}), & & [recv_1(i, r, \{\!| W, i |\!\}_{pk(r)}), \\ & recv_2(r, i, \{\!| ni, V |\!\}_{pk(i)}), & & send_2(r, i, \{\!| W, nr |\!\}_{pk(i)}), \\ & send_3(i, r, \{\!| V |\!\}_{pk(r)}), & & recv_3(i, r, \{\!| nr |\!\}_{pk(r)}), \\ & claim_4(i, synch)]) & & claim_5(r, synch)]) \end{array}$$

$AKN_0(NS) = AdversaryFresh \cup Agent \cup \{pk(A) \mid A \in Agent\} \cup \{sk(A) \mid A \in Agent_C\}$