OVSP definitions

Protocol specification

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

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

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

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

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

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

Deduction on terms

$M \vdash t$ means that t can be deduced knowing M
$\vdash$ is the least relation with the following properties:

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

Protocol execution

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

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

Operational semantics

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

$st = \langle\!\langle \mathit{AKN}, F \rangle\!\rangle \in \mathit{State}$ where
AKN is the adversary knowledge and $F \subseteq \mathit{Run}$ are the runs that has to be executed.
$\mathit{RunEvent} = \mathit{Inst} \times (\mathit{RoleEvent} \cup \{\mathit{create}(R) \mid R \in \mathit{Role}\}$

Labeled Transition System for Operational Semantics: $(\mathit{State}, \mathit{RunEvent}, \rightarrow, st_0(P))$
where $st_0(P) = \langle\!\langle \mathit{AKN}_0(P), \emptyset \rangle\!\rangle$ where $\mathit{AKN}_0(P)$ is the initial adversary knowledge.

Transition rules for $(\mathit{State}, \mathit{RunEvent}, \rightarrow, st_0(P))$:

- $[create_P]\ \dfrac{R \in dom(P) \quad ((\theta,\rho,\emptyset),s) \in runsof(P,R) \quad \theta \notin runsIDs(F)}{\langle\!\langle AKN, F\rangle\!\rangle \xrightarrow{((\theta,\rho,\emptyset),create(R))} \langle\!\langle AKN, F \cup \{((\theta,\rho,\emptyset),s)\}\rangle\!\rangle}$

- $[send]\ \dfrac{e = send_l(R_1,R_2,m) \quad (inst,[e]\cdot s) \in F}{\langle\!\langle AKN, F\rangle\!\rangle \xrightarrow{(inst,e)} \langle\!\langle AKN \cup \{inst(m)\}, F \setminus \{(inst,[e]\cdot s)\} \cup \{(inst,s)\}\rangle\!\rangle}$
  - $[send]$ is the only rule that **changes the adversary knowledge**

- $[recv]\ \dfrac{e = recv_l(R_1,R_2,pt) \quad AKN \vdash m \quad (inst,[e]\cdot s) \in F \quad Match(inst,pt,m,inst')}{\langle\!\langle AKN, F\rangle\!\rangle \xrightarrow{(inst',e)} \langle\!\langle AKN, F \setminus \{(inst,[e]\cdot s)\} \cup \{(inst',s)\}\rangle\!\rangle}$

- $[claim]\ \dfrac{e = claim_l(R,c,t) \quad (inst,[e]\cdot s) \in F}{\langle\!\langle AKN, F\rangle\!\rangle \xrightarrow{(inst,e)} \langle\!\langle AKN, F \setminus \{(inst,[e]\cdot s)\} \cup \{(inst,s)\}\rangle\!\rangle}$

The Needham-Schroeder protocol

$$\begin{aligned} NS(i) = \ & (\{i, r, ni, sk(i), pk(i), pk(r)\},\\ & [send_1(i, r, \{\!|\, ni, i \,|\!\}_{pk(r)}),\\ & recv_2(r, i, \{\!|\, ni, V \,|\!\}_{pk(i)}),\\ & send_3(i, r, \{\!|\, V \,|\!\}_{pk(r)}),\\ & claim_4(i, synch)]) \end{aligned}$$

$$\begin{aligned} NS(r) = \ & (\{i, r, nr, sk(r), pk(r), pk(i)\},\\ & [recv_1(i, r, \{\!|\, W, i \,|\!\}_{pk(r)}),\\ & send_2(r, i, \{\!|\, W, nr \,|\!\}_{pk(i)}),\\ & recv_3(i, r, \{\!|\, nr \,|\!\}_{pk(r)}),\\ & claim_5(r, synch)]) \end{aligned}$$

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