Crypto Engineering - verifying crypto primitives and security protocols
2016/2017

C. Ene

Exercices

Exercise 1
We recall the rules of the Deduction System for Dolev Yao theory: $T_0 \vdash s$, where $\{\!\{\_\}\!\}_\_$ represents a symmetric encryption scheme, $\{\ \_\ \}_\_$ an asymmetric encryption scheme, and we suppose that $pr(u)$ is the inverse secret key associated to $pk(u)$:

$$(\mathbf{A}) \quad \frac{u \in T_0}{T_0 \vdash u} \qquad\qquad (\mathbf{UL}) \quad \frac{T_0 \vdash \langle u, v\rangle}{T_0 \vdash u}$$

$$(\mathbf{P}) \quad \frac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash \langle u, v\rangle} \qquad\qquad (\mathbf{UR}) \quad \frac{T_0 \vdash \langle u, v\rangle}{T_0 \vdash v}$$

$$(\mathbf{C}) \quad \frac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash \{\!\{u\}\!\}_v} \qquad\qquad (\mathbf{D}) \quad \frac{T_0 \vdash \{\!\{u\}\!\}_v \qquad T_0 \vdash v}{T_0 \vdash u}$$

$$(\mathbf{AD}) \quad \frac{T_0 \vdash \{\ u\ \}_{pk(v)} \qquad T_0 \vdash pr(v)}{T_0 \vdash u} \qquad\qquad (\mathbf{AC}) \quad \frac{T_0 \vdash u \qquad T_0 \vdash pk(v)}{T_0 \vdash \{\ u\ \}_{pk(v)}}$$

Prove or disprove that a passive Dolev Yao intruder can deduce the message s with the initial knowledge T_0.

1.) $T_0 = \{a, k\}$ and $s = \langle a, \{\!\{a\}\!\}_k\rangle$

2.) $T_0 = \{a, k, n1, \{\!\{k2\}\!\}_{\langle n1,n2\rangle}, \{\!\{\langle n2, \{\!\{n1\}\!\}_{\langle n3,n3\rangle}\rangle\}\!\}_k\}$ and $s = k2$

3.) $T_0 = \{a, b, k1, k2, \{\!\{k4\}\!\}_{\langle k1,k3\rangle}, \{\!\{\langle k2, n\rangle\}\!\}_{\langle k2,k1\rangle}\}$ and $s = k4$

Exercise 2
Consider the following protocol:

$$\begin{array}{ll} A \to B : & \langle \{\!\{\langle K, N\rangle\}\!\}_{sk(A,B)}, A\rangle \\ B \to A : & \{\!\{\langle N, S\rangle\}\!\}_K \end{array}$$

Assume that $sk(a, b)$ is a shared secret key between honest participants a and b. Consider a session $R_A(a, b, n_a, k)||R_B(b, s)$ between a and b and show that s (the instantiation of variable S in this session) remains secret in presence of a passive Dolev-Yao intruder.

Exercise 3
Consider the following protocol:

$$\begin{array}{lllll} 1. & A & \rightarrow & B & : \{\, A, N_a \,\}_{pk(B)} \\ 2. & B & \rightarrow & A & : \{\, N_a, N_b \,\}_{pk(A)} \\ 3. & A & \rightarrow & B & : \{\, N_b \,\}_{pk(B)} \end{array}$$

Assume that $\{\ \_\ \}_{\_}$ is an asymmetric encryption scheme, $pk(x)$ (respectively $pr(x)$) is the public key (respectively private key) of participant x.

1.) Give the role based specification $R_1(A, B, N_a)||R_2(B, N_b)$ of the protocol (denote by act_1, act'_1 the actions associated to role R_1, and by act_2, act'_2 the actions associated to role R_2).

2.) Consider the scenario $R_1(a, i, n_a)||R_2(b, n_b)$ corresponding to a session of a as initiator with i, and to a session of b as responder (where at the end b will thinks that he is talking and sharing a secret value n_b with a - this will be highlighted by b sending $ok(a, b, n_b)$[1] as part of action $act'_2(s2)$). Give the constraint system associated to the interleaving $act_1(s1) < act_2(s2) < act'_1(s1) < act'_2(s2)$, where $act_1(s1), act'_1(s1)$ are the actions made by a in the first session, and $act_2(s2), act'_2(s2)$ are the actions made by b in the second session.

3.) Suppose that the initial knwoledge of the intruder i is the set $T_1 = \{a, b, pk(a), pk(b), pk(i), pr(i), init\}$ Solve the constraint system and find an attack where the intruder i learn n_b.

[1] *The message $ok(a, b, n_b)$ is just a symbolic message, it does not reveal anything about its content to the intruder.*