ARNOULD Alexis
MAUCOTEL Benoit

TP Security Models

Exercice 1

Question 1

```
$ avispa NSPK.hlpsl --output=. --ofmc
% OFMC
% Version of 2006/02/13
SUMMARY
  UNSAFE
DETAILS
  ATTACK_FOUND
PROTOCOL
  ./NSPK.if
GOAL
  secrecy_of_nb
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
   searchTime: 0.01s
 visitedNodes: 10 nodes
  depth: 2 plies
ATTACK TRACE
i -> (a,6): start
(a,6) -> i: {Na(1).a}_ki
i -> (b,3): {Na(1).a}_kb
(b,3) -> i: {Na(1).Nb(2)}_ka
i -> (a,6): {Na(1).Nb(2)}_ka
(a,6) -> i: {Nb(2)}_ki
i -> (i,17): Nb(2)
i -> (i,17): Nb(2)


% Reached State:
%
% secret(Nb(2),nb,set_70)
% witness(b,a,alice_bob_nb,Nb(2))
% contains(a,set_70)
% contains(b,set_70)
% secret(Na(1),na,set_74)
% witness(a,i,bob_alice_na,Na(1))
% contains(a,set_74)
% contains(i,set_74)
% state_bob(b,i,ki,kb,1,dummy_nonce,dummy_nonce,set_78,10)
% state_alice(a,i,ka,ki,4,Na(1),Nb(2),set_74,6)
```

```
% state_bob(b,a,ka,kb,3,Na(1),Nb(2),set_70,3)
% state_alice(a,b,ka,kb,0,dummy_nonce,dummy_nonce,set_62,3)
% request(a,i,alice_bob_nb,Nb(2),6)

$ avispa NSPK.hlpsl --output=. --cl-atse

SUMMARY
   UNSAFE

DETAILS
  ATTACK_FOUND
  TYPED_MODEL

PROTOCOL
  ./NSPK.if

GOAL
  Secrecy attack on (n5(Nb))

BACKEND
  CL-AtSe

STATISTICS
 Analysed   : 9 states
 Reachable  : 8 states
 Translation: 0.00 seconds
 Computation: 0.00 seconds


ATTACK TRACE
i -> (a,6):  start
(a,6) -> i:  {n9(Na).a}_ki
          & Secret(n9(Na),set_74);  Add a to set_74;  Add i to set_74;

i -> (a,3):  start
(a,3) -> i:  {n1(Na).a}_kb
          & Secret(n1(Na),set_62);  Witness(a,b,bob_alice_na,n1(Na));
          & Add a to set_62;  Add b to set_62;

i -> (b,4):  {n9(Na).a}_kb
(b,4) -> i:  {n9(Na).n5(Nb)}_ka
          & Secret(n5(Nb),set_70);  Witness(b,a,alice_bob_nb,n5(Nb));
          & Add a to set_70;  Add b to set_70;

i -> (a,6):  {n9(Na).n5(Nb)}_ka
(a,6) -> i:  {n5(Nb)}_ki

$ avispa NSPK.hlpsl --output=. --satmc
SUMMARY
 UNSAFE
```

```
DETAILS
  ATTACK_FOUND
  BOUNDED_NUMBER_OF_SESSIONS
  BOUNDED_SEARCH_DEPTH
  BOUNDED_MESSAGE_DEPTH

PROTOCOL
  NSPK.if

GOAL
  secrecy_of_nb(nb0(b,4),set_70)

BACKEND
  SATMC

COMMENTS

STATISTICS
  attackFound              true      boolean
  upperBoundReached        false     boolean
  graphLeveledOff          no        boolean
  satSolver                sim       solver
  maxStepsNumber           30        steps
  stepsNumber              5         steps
  atomsNumber              379       atoms
  clausesNumber            993       clauses
  encodingTime             0.04      seconds
  solvingTime              0.0       seconds
  if2sateCompilationTime   0.01      seconds

ATTACK TRACE
  i      ->   (a,6)   : start
  (a,6)  ->   i       : {na0(a,6).a}_ki
  i      ->   (b,4)   : {na0(a,6).a}_kb
  (b,4)  ->   i       : {na0(a,6).nb0(b,4)}_ka
  i      ->   (a,6)   : {na0(a,6).nb0(b,4)}_ka
  (a,6)  ->   i       : {nb0(b,4)}_ki


$ avispa NSPK.hlpsl --output=. --ta4sp
SUMMARY
   INCONCLUSIVE

DETAILS
   OVER_APPROXIMATION
   UNBOUNDED_NUMBER_OF_SESSIONS
   TYPED_MODEL

PROTOCOL
   ./NSPK.if.ta4sp
```

GOAL
  SECRECY - Property with identitier: nb

BACKEND
  TA4SP

COMMENTS
  Use an under-approximation in order to show a potential attack
  The intruder might know some critical information

STATISTICS
  Translation: 0.00 seconds
  Computation 0.40 seconds

ATTACK TRACE
  No Trace can be provided with the current version.

Question 2

L'outils AVISPA analyse le protocole qu'on lui donne. Il est capable ensuite de nous donner différentes informations sur le protocole. Il nous indique si ce dernier est sécurisé ou non et s'il a trouvé une attaque. Il nous donne également le but du protocole ainsi que des statistiques des performance sur l'exécution.

Question 3

Il suffit que Bob envoie (lors du SND) son Identité à Alice avec Na, Nb et qu'Alice s'attende à recevoir (lors du RCV) l'identité de Bob.

Exercice 2

a)

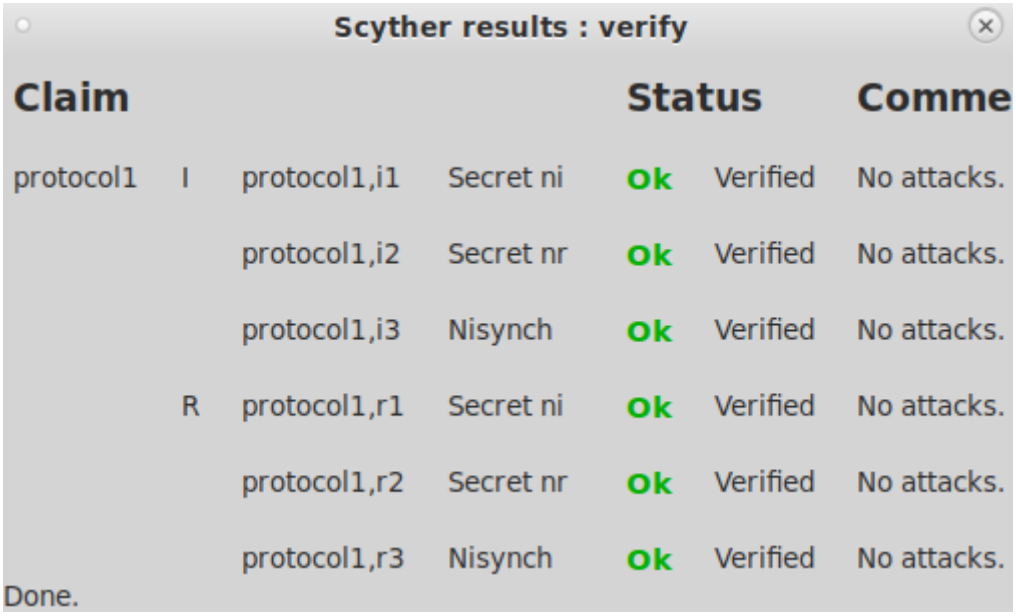
Attaque 1
Le Secret ni est mis en cause, c'est une attaque de type Man In The Middle.

Attaque 2
C'est une attaque de type Man In The Middle, Alice pense recevoir un message de Bob, mais en réalité de Eve, et chiffre donc sa réponse avec la clé publique d'Eve.
C'est le Secret nr qui est en cause.

Attaque 3
Même attaque que précédemment mais ici c'est le Nisynch qui est en cause.

Attaque 4
Même attaque que la première.

b)



Exercice 3

Exercice 4

Question 1

```
$> proverif -in horn needham.horn
Initial clauses:
Clause 14: c:(v_25,v_26) -> c:v_26
Clause 13: c:(v_20,v_21) -> c:v_20
Clause 12: c:v_18 & c:v_19 -> c:(v_18,v_19)
Clause 11: c:c[]
Clause 10: c:pk(sA[])
Clause 9: c:pk(sB[])
Clause 8: c:x_17 & c:encrypt(m_16,pk(x_17)) -> c:m_16
Clause 7: c:x_15 -> c:pk(x_15)
Clause 6: c:x_14 & c:y_13 -> c:encrypt(x_14,y_13)
Clause 5: c:pk(x_12) -> c:encrypt((Na[pk(x_12)],pk(sA[])),pk(x_12))
Clause 4: c:pk(x_10) & c:encrypt((Na[pk(x_10)],y_11),pk(sA[])) ->
c:encrypt((y_11,k[pk(x_10)]),pk(x_10))
Clause 3: c:encrypt((x_8,y_9),pk(sB[])) -> c:encrypt((x_8,Nb[x_8,y_9]),y_9)
Clause 2: c:encrypt((x_6,pk(sA[])),pk(sB[])) & c:encrypt((Nb[x_6,pk(sA[])],z_7),pk(sB[])) ->
c:encrypt(secret[],pk(z_7))
Clause 1: c:new-name[!att = v_4]
Completing...
goal reachable: c:secret[]
Abbreviations:
Na_190 = Na[pk(x_174)]
Nb_191 = Nb[Na_190,pk(sA[])]
k_192 = k[pk(x_174)]
clause 8 c:secret[]
    duplicate c:x_188
    clause 2 c:encrypt(secret[],pk(x_188))
```

```
duplicate c:encrypt((Na_190,pk(sA[])),pk(sB[]))
clause 6 c:encrypt((Nb_191,x_188),pk(sB[]))
   apply 2-tuple c:(Nb_191,x_188)
      apply 1-proj-2-tuple c:Nb_191
         clause 8 c:(Nb_191,k_192)
            duplicate c:x_174
            clause 4 c:encrypt((Nb_191,k_192),pk(x_174))
               duplicate c:pk(x_174)
               clause 3 c:encrypt((Na_190,Nb_191),pk(sA[]))
                  clause 6 c:encrypt((Na_190,pk(sA[])),pk(sB[]))
                     apply 2-tuple c:(Na_190,pk(sA[]))
                        apply 1-proj-2-tuple c:Na_190
                           clause 8 c:(Na_190,pk(sA[]))
                              duplicate c:x_174
                              clause 5 c:encrypt((Na_190,pk(sA[])),pk(x_174))
                                 clause 7 c:pk(x_174)
                                    any c:x_174
                        clause 10 c:pk(sA[])
                     duplicate c:pk(sB[])
      any c:x_188
   clause 9 c:pk(sB[])
```

RESULT goal reachable: c:secret[]

Question 2

Proverif à atteint son but de trouver le secret. Pour cela il effectuer une attaque de type man in the middle, et a réussi à récupérer la clef pour déchiffrer le secret.

Question 3

Pour éviter cette attaque, il faut que a et b signe leur envoies.

Exercice 5