Analyse des versions

Version 1 du protocole :

Résultat cl-atse

```
session engagée :   session(b,s,pkb,pks,idemploye, idbadgeuse) /\ session(b,i,pkb,pki,idemploye, i
dbadgeuse)
```

```
SUMMARY
  UNSAFE

DETAILS
  TYPED MODEL

PROTOCOL
  calp-v1.if

GOAL
  Secrecy goal () on idemploye)

BACKEND
  CL-AtSe

STATISTICS
  Analysed   : 6 states
  Reachable  : 3 states
  Translation: 0.00 seconds
  Computation: 0.00 seconds

ATTACK TRACE
 i -> (b,3):  start
 (b,3) -> i:  {idemploye.idbadgeuse}_pks
              & Secret(idemploye,(),set_52);  Add b to set_52;  Add s to set_52;
              & Built from step_0

 i -> (b,6):  start
 (b,6) -> i:  {idemploye.idbadgeuse}_pki
              & Secret(idemploye,(),set_59);  Add b to set_59;  Add i to set_59;
              & Built from step_0
```

Explications

L'intrus initie la connexion et récupère l'id de l'employé et l'id de la badgeuse.

Analyse v2

Résultat de cl-atse

```
SUMMARY
  UNSAFE

DETAILS
  TYPED MODEL

PROTOCOL
  calp-v2.if

GOAL
  Secrecy goal () on n1(Nb))

BACKEND
  CL-AtSe

STATISTICS
  Analysed   : 6 states
  Reachable  : 2 states
  Translation: 0.00 seconds
  Computation: 0.00 seconds

ATTACK TRACE
 i -> (b,3):  start
 (b,3) -> i:  {idemploye.idbadgeuse.n1(Nb)}_pks
              & Secret(n1(Nb),(),set_70);  Secret(idemploye,(),set_69);
              & Witness(b,s,badgeuse_serveur,n1(Nb));  Add b to set_69;
              & Add s to set_69;  Add b to set_70;  Add s to set_70;
              & Built from step_0

 i -> (s,7):  {idemploye.idbadgeuse.n1(Nb)}_pks
 (s,7) -> i:  {ok.n1(Nb).n7(Ns)}_pki
              & Secret(n7(Ns),(),set_85);  Add s to set_85;  Add i to set_85;
              & Built from step_2
```

Explications

L'intrus initie la demande, la badgeuse lui envoie le bon message qu'il transmet au serveur, le serveur renvoie alors un message à l'intrus chiffré avec la clef de l'intrus qui peut alors voir le nonce.

Analyse v3

Résultat cl-atse

```
SUMMARY
  SAFE

DETAILS
  BOUNDED NUMBER OF SESSIONS
  TYPED MODEL

PROTOCOL
  calp-v3.if

GOAL
  As specified

BACKEND
  CL-AtSe

STATISTICS
  Analysed   : 45 states
  Reachable  : 8 states
  Translation: 0.02 seconds
  Computation: 0.00 seconds
```

Conclusion

Les sécurités mises en place sur cette version du protocole semble empêcher les attaques précédentes tentées par un intrus. Toutefois, nous ne pouvons pas conclure que le protocole est parfaitement sûre car il n'est pas possible de garantir une sécurité parfaite.