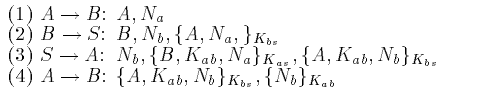
Jan Rehwaldt, 2012-04-13, University of Tartu

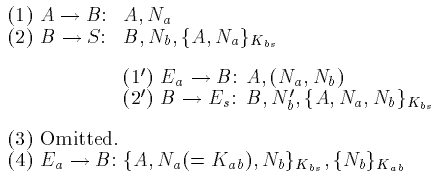
Exercise 6, Principles of Secure Software Design

**Will be convinced that is fresh?**

According to the attack description below KAB may be hijacked by an attacker masquerading the initiator Ann. Therefore KAB may not be fresh when using this protocol.



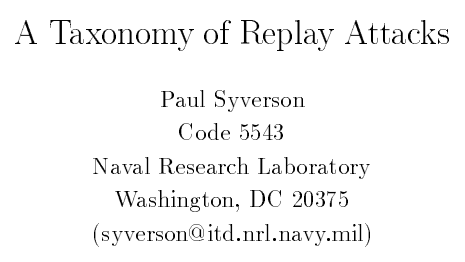
1. Ann send name A and nonce NA (random number used to prove freshness) to Bob
2. Bob replies to server his name, an own nonce NB, KBS and {A + NA} encrypted with Key KBS
3. Server sends to Ann NB, {B, KAB, NA} encrypted with KAS and {A, KAB, NB} encrypted with KBS
   1. {B, KAB, NA} shows name of target (B), session key (KAB) and freshness of message (NA)
   2. {A, KAB, NB} should be passed on to Bob
4. Ann sends chunk {A, KAB, NB} and NB encrypted with session key to Bob



For attacking this protocol attacker E may intercept the messages and send own messages in-between acting like Ann (after step 2).

1. Ann send name A and nonce NA (random number used to prove freshness) to Bob
2. Bob replies to server own nonce NB, KBS and {A + NA} encrypted with Key KBS
   1. Attacker masquerades as Ann sending NE = NA + NB to Bob
   2. Bob replies to attacker his name, an new nonce NB2, KBS and {NA + NA} encrypted with Key KBS
3. Omitted: ~~Server sends to Ann N~~~~B~~~~, {B, K~~~~AB~~~~, N~~~~A~~~~} encrypted with K~~~~AS~~ ~~and {A, K~~~~AB~~~~, N~~~~B~~~~} encrypted with K~~~~BS~~
4. Ann sends chunk {A, KAB, NB} and NB encrypted with session key to Bob
5. Attacker sends encrypted chunk from omitted message {B, KAB, NB} and NB encrypted with NA, which became the session key KAB, to Bob
6. Attacker overtook the communication masquerading Ann

Source:



**What attack is possible if the intruder learns an old session key?**

Session may be recovered, **overtaken by impersonation** or if messages are stored for requesting them depending on the session they may be obtained later on. Additionally if the session key is used for de- and encryption caught encrypted messages may be decrypted with this information. Therefore session keys may be assumed as being secret, especially after their expiration.