CS181S – Systems Security Fall 2020

Problem Session 5: Authentication Protocols

Wednesdahy September 30, 2020

1. **Replay and Reflection Attacks.** Consider each of the following proposed authentication protocols. In each case, determine whether the protocol is vulnerable to a replay attack. If so, show the attack. If not, determine whether it is instead vulnerable to a reflection attack. If so, show the attack. In all cases, assume `k` is a secret key shared betwen Alice and Bob.

   (a) Protocol 1

   1. `B --> A:` `B,r` (where `r` is a fresh, random nonce generated by `B`)
   2. `A --> B:` `Enc(A^B; k)` (where `^` denotes bitwise xor)

   (b) Protocol 2

   1. `B --> A:` `B,r` (where `r` is a fresh, random nonce generated by `B`)
   2. `A --> B:` `Enc(A^B+r; k)` (where `^` denotes bitwise xor)

   (c) Protocol 3

   1. `B --> A:` `B,r` (where `r` is a fresh, random nonce generated by `B`)
   2. `A --> B:` `Enc(A**B+r; k)` (where `**` denotes exponentiation)

2. **MITM Attacks.** Consider a schematic version of the key distribution protocols we discussed in the second lecture video.

   1. `A --> KDC: A, B, r` (where `r` is a fresh, random nonce generated by `A`)
   2. `KDC --> A: A, B, Enc(x, k; K_A), Enc(y, k; K_B)`
   3. `A --> B:  A, B, Enc(y, k; K_B)`

   where `x` and `y` denote finite strings constructed from the three symbols `A`, `B`, and `r`. Different choices of `x` and `y` that a protocol designer makes could lead to protocols having different properties. This question explores the implications of the choices that the protocol designer might make.

   (a) Give replacements for `x` and `y` that make it possible to perform man-in-the-middle attacks and possible to perform replay attacks of message 2. Show the attacks.

   (b) Give replacements for `x` and `y` that make it possible to perform man-in-the-middle attacks but impossible to perform replay attacks of message 2. Show the man-in-the-middle attack.

   (c) Give replacements for `x` and `y` that make it impossible to perform man-in-the-middle attacks but possible to perform replay attacks of message 2. Show the replay attack.

   (d) Give replacements for `x` and `y` that make it impossible to perform man-in-the-middle attacks and impossible to perform replay attacks of message 2.