Modelling and Analysis of Security Protocols:
Homework 1

Handed out on: 14/9/2007 Return to me in class on: 28/9/07

1 Type attacks

• 1) What is a typing attack on a protocol?

1 mark

• 2) The following protocol lets $A$ and $B$ authenticate using a trusted server $S$. The principals $A$ and $B$ share the keys $K_{AS}$ and $K_{BS}$ with the server.

1. $A \rightarrow B : A$
2. $B \rightarrow A : N_B$
3. $A \rightarrow B : \{A, B, N_B\}_{K_{AS}}$
4. $B \rightarrow S : \{A, B, \{A, B, N_B\}_{K_{AS}}\}_{K_{BS}}$
5. $S \rightarrow B : \{A, B, N_B\}_{K_{BS}}$

Show how, by using a typing attack, an attacker can convince $B$ that they are $A$. The attacker will act as $A$ and intercept messages to the server. Assume that the attacker can pick any string it wants as a nonce. Write down the attack using $A \rightarrow B$ notation.

4 marks

2 Early Version SSL

An early version of the Secure Sockets Layer protocol from Netscape included the following exchange:

1. $A \rightarrow B : E_B(K_{ab})$
2. $B \rightarrow A : \{N_B\}_{K_{ab}}$
3. $A \rightarrow B : \{CA, Sign_A(N_B)\}_{K_{ab}}$

$CA$ is a certificate that is used later in the protocol
• 1) In one paragraph describe what this protocol is trying to achieve and how it works.

1 mark

• 2) The protocol is flawed, describe an attack on the protocol and write it down using the $A \rightarrow B$ notation.

5 marks

• 3) Fix the protocol by changing a single line.

2 marks

You will be relieved to hear the flawed version of the protocol is no longer used in web browsers.

3 Design A Protocol

Imagine that you are designing an online game, the framework consists of a player $A$, a game host $H$ and a trusted central server $S$.

The player $A$ has a symmetric key $K_{AS}$ and id $A$ that is known to the trusted central server (these would be set up using a registration key printed on the CD box). The host and server have well known public keys $(E_H(\_)$ and $E_S(\_))$

The player will connect to the host $H$ and set up a symmetric session key with which to play the game. You want to ensure that only people who have brought the game can play online. Therefore the host $H$ will have to check with the server $S$ that the player $A$ really does have a key.

Design a protocol that will let $A$ connect to the host $H$ and let $H$ check with the server $S$ to see if $A$ is a legitimate player (i.e., really does have a shared key with $S$). There is only one server but there may be a number of hosts and players. In particular, your protocol should make it impossible for an attacker to wrongly authenticate with a host by intercepting and replaying messages or by acting as a man-in-the-middle.

Write your protocol down using $A \rightarrow H$ notation and briefly describe how it works and exactly what goals your protocol achieves.

12 marks.