Computer Security – Tutorial 2: Protocols

David Aspinall and Luke Shrimpton

8th February 2013

This is the second question sheet for the Computer Security course, covering topics in protocols. Tutorial question sheets are provided to help guide your self-study on the course and measure your progress. The process for this tutorial sheet is as follows:

1. Read and try to answer these questions before your Week 5 tutorial.
2. Your tutor will discuss answers to some questions at the Week 5 tutorial.
3. After the Week 5 tutorial, write down your answers to all questions.
4. In Week 7, a solution sheet will be issued. To measure your understanding of the material, use the solution sheet to assess your own answers.
5. In the final tutorial, there will be an opportunity to raise problem points in any of the tutorial questions with your tutor.

You are encouraged to discuss this tutorial with other students and work together to ensure that you fully understand the concepts covered. This does not apply to questions on the assessed practical exercises, issued separately.

Part A: Where is the secret and where is the trust?

Investigate and discuss each of the following authentication activities. In each case, discuss what secret(s) are being used to authenticate, what the assumptions are regarding the secret (and where the trust is being placed). Explain what countermeasures may be employed to protect the secret.

1. Alice logs into her Gmail account using her Gmail address and a password.
2. Alice logs into her online bank account, using her bank account number and answering a challenge of 3 letter positions from her 8 character alphanumeric password.
3. Alice connects to a secure e-commerce web site over TLS. Behind the scenes, the server uses Diffie-Hellman key agreement to establish a key to encrypt data.

You should also be able to enumerate some particular attacks that are possible in each case.

Part B: Replaying the Wide-Mouthed Frog

The *Wide Mouthed Frog* protocol allows two principals, A and B, to establish a shared key using a trusted server S. The protocol has two messages:

$$\begin{array}{lll} \text{Message 1.} & A \to S: & A, \{\, T_a, B, K_{ab} \,\}_{K_{as}} \\ \text{Message 2.} & S \to B: & \{\, T_s, A, K_{ab} \,\}_{K_{bs}} \end{array}$$

In message 1, A sends a session key to S, including a time-stamp T_a. The server S checks that the message is timely, and if so, forwards the message to B, together with a new time-stamp T_s. After receiving message 2, B checks that the time-stamp T_s is later than any other received from S, and if so, accepts the key K_{ab} to communicate with A.

1. What are the assumptions made before and during the execution of this protocol? What is the unusual one compared with most TTP-based protocols?
2. By replaying the second message within an appropriate time window, it is claimed that an intruder M can make the server update the time-stamp of a non-fresh key K_{ab}, extending its lifetime indefinitely.

(a) What are this risks associated with this attack? Give a real-world scenario.

(b) Explain how this attack proceeds, beginning from the message:

$$\text{Message 3.} \quad M(B) \rightarrow S: \quad B, \{\, T_s, A, K_{ab} \,\}_{K_{bs}}$$

where $M(B)$ denotes M masquerading as B. You should show a pattern which can be repeated after four messages.

(c) Considering the assumptions made in the analysis, do you consider this attack to be possible? If so, provide a fix; if not, explain why.

3. By replaying the second message, it is claimed that an intruder masquerading as the server can cause B to think that A has established multiple sessions with him.

(a) What are the risks associated with this attack? Give a real-world scenario.

(b) Considering the assumptions made in the analysis, do you consider this attack to be possible? If so, provide a fix; if not, explain why.

Part C: Multi-party Key Exchange Protocol

The two protocols which follow below are proposed for use in an ATM system. The user (represented by their ATM card) wants to be sure they are communicating with their real bank before sending their PIN. The bank wants to be sure the user is authorised to access the account, by checking both the card specifications and the PIN.

Index:

U	User
A	ATM Terminal
B	Bank Computer
C_s	Card Specifications
T_s	Terminal Specifications
K_{TB}	Secret key shared between Terminal and Bank
K_{UB}	Secret key shared between User and Bank
K_B^{Pub}	Bank's public key
K_B^{Pri}	Bank's private key
PRN	Previous random sequence number (from last run of the protocol)
NRN	New random sequence number
c_i	Random secrets shared between card and bank.
f	A function the user and bank has agreed upon.

Protocol 1

Message 1.0.	U	$\rightarrow$	$A:$	C_s
Message 1.1.	A	$\rightarrow$	$B:$	$\{C_s, A_s\}_{K_{AB}}$
Message 1.2.	B	$\rightarrow$	$A:$	$Sign(PRN)_{K_B^{Pri}}$
Message 1.3.	A	$\rightarrow$	$U:$	PRN
Message 1.4.	U	$\rightarrow$	$A:$	PIN, NRN
Message 1.5.	A	$\rightarrow$	$B:$	$\{PIN, NRN\}_{K_B^{Pub}}$

Protocol 2

Message 2.0. $U \rightarrow A: \{f(C_s, c_1), C_s\}_{K_{UB}}$
Message 2.1. $A \rightarrow B: \{\{f(C_s, c_1), C_s\}_{K_{UB}}, A_s\}_{K_{TB}}$
Message 2.2. $B \rightarrow A: \{f(C_s, c_2)\}_{K_{UB}}$
Message 2.3. $A \rightarrow U: \{f(C_s, c_2)\}_{K_{UB}}$
Message 2.4. $U \rightarrow A: \{PIN\}_{K_{UB}}$
Message 2.5. $T \rightarrow B: \{PIN\}_{K_{UB}}$

1. Consider each protocol in careful detail. To understand the protocol, explain the steps by commenting on the beliefs of each principal (U,A,B) at each stage in the protocol: what assumptions they have, and what conclusions they may derive from receiving each message. How do the beliefs relate to the goal of the protocol?

2. Consider at least one practical attack on these protocols. What would be a sensible goal for the attack and where would you mount an attack from?

3. For each protocol, find and explain an attack which targets a design flaw in the protocol. Explain carefully in each case what the attack allows the attacker to achieve.

4. Give a third protocol which avoids both of the protocol design flaws you have shown.