5.5

LASEC
SECURITY AND CRYPTOGRAPHY LABORATORY

Cryptography and Security
http://lasecwww.epfl.ch/cs2007/

Cryptography and Security

2006 – 2007

Survey n° 6

Name:

1. S/Key is ...

   - ☐ an encryption scheme used in GSM.
   - ☒ a one-time password based protocol.
   - ☐ a secret key used in Bluetooth.
   - ☐ a secret key involved in Kerberos.

2. In Kerberos, a client that would like to authenticate to a server (S) has to interact successively with three entities that are: the server (S), the Authentication Server (AS), the Ticket Granting Server (TGS). In which order does the client have to interact with the entities?

   - ☒ AS-TGS-S
   - ☐ S-TGS-AS-S
   - ☐ TGS-AS-S
   - ☐ TGS-S-AS-S

3. In the GSM infrastructure, which of the following entity contains Ki?

   - ☐ MS (Mobile Station)
   - ☐ VLR (Visitor Location Register)
   - ☒ SIM (Subscriber Identity Module)
   - ☐ TGS (Ticket Granting Server)

4. In a MAC-based challenge-response authentication protocol ...

   - ☐ the challenge is sent by the client.
   - ☐ the challenge is sent after the response.
   - ☐ the password is sent in clear.
   - ☒ the server must keep the password and protect the database.

5. The names of Needham and Schroeder refers to ...

   - ☐ an authentication protocol involving only a client and a server.
   - ☒ an authentication protocol involving a client, an authentication server, and a server.
   - ☐ a theorem about the security of Kerberos.
   - ☐ the inventors of GSM.

6. Tick the *false* assertion about Bluetooth.

- ☐ The term Bluetooth comes from a Viking King of the 10th Century.
- ☒ The mode 1 of Bluetooth is secure.
- ☐ The specifications of Bluetooth 2.0 have already been released. ✓
- ☐ Bluetooth was designed for a variety of mobile devices. ✓

7. Using salt for UNIX passwords ...

- ☐ allows to speed up the verification for the server.
- ☐ makes the protocol secure against computationally unbounded adversary.
- ☐ allows to transmit the password over a non confidential channel without compromising the security.
- ☒ helps preventing dictionary attacks.

8. CHAP stands for ...

- ☐ Commitment Hash Authentication Protocol
- ☐ Controlled Human Access Protocol
- ☐ Challenge Human Authentication Protocol
- ☒ Challenge-Handshake Authentication Protocol

9. Which cryptographic primitive(s) is (are) used in S/Key - OTP ?

- ☐ Only encryption and a hash function
- ☒ Only a hash function
- ☐ Only encryption and a MAC algorithm
- ☐ Only a MAC

10. Tick the *true* assertion.

- ☐ No server-aided authentication protocol resists against "replay attack".
- ☒ GSM authentication is based on a challenge-response protocol.
- ☐ S/Key - OTP does *not* provide resistance against eavesdroppers.
- ☐ In the GSM infrastructure, HLR stands for "High Level Register".