**Reading for Lecture 9:**

**Read**

*D is for Digital:* Chapter 9. The Internet. pp. 135-160.

**Lecture 9: Exercises: Accountability, Identification, Authentication, Authorization, the Internet**

1. A company purchases a computer and software to support its business activities. The vendor of the operating system software releases a patch to remove a recently-discovered security vulnerability in its product. Before the patch can be installed, a criminal exploits the vulnerability to break into the company system and steals client information.

If the customer signed an End User License Agreement with the software vendor limiting the liability of the vendor to the cost of the purchased software, who is accountable to the client for the stolen information if the damages exceed the cost of the software?

2. Suppose the company from (1) decides to use a cloud-based service instead of purchasing its own computers. Suppose the cloud service agreement includes the following clauses (3, 4.2, 10).

Cloud service clauses:

**3. Security and Data Privacy.**

Security. Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.

…

**4.2 Other Security and Backup**. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content. Log-in credentials and private keys generated by the Services are for your internal use only and you may not sell, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your agents and subcontractors performing work on your behalf.

…

**10. Disclaimers.** The service offerings are provided “as is.” We and our affiliates and licensors make no representations or warranties of any kind, whether express, implied, statutory or otherwise regarding the service offerings or the third party content, including any warranty that the service offerings or third party content will be uninterrupted, error free or free of harmful components, or that any content, including your content or the third party content, will be secure or not otherwise lost or damaged. Except to the extent prohibited by law, we and our affiliates and licensors disclaim all warranties, including any implied warranties of merchantability, satisfactory quality, fitness for a particular purpose, non-infringement, or quiet enjoyment, and any warranties arising out of any course of dealing or usage of trade.

Who is accountable for losses resulting from exploitation of security flaws in the service?

3. You want to board a plane, but first you have to go through the security check. You present your boarding pass and a photo ID to the agent. The agent looks at you, at the documents, and also checks the ID under a special light. Finding all in order, he waves you through to the queue for the luggage and personal scanners.

Which parts of this process correspond to identification, authentication, and authorization? Note that two different authentications take place

4. In lecture, we discussed multi-factor authentication. In the situation described in (3), list the factor(s) involved and their category or categories.

5. One common attack involves sending a user an email with a link that will take the user to a spoofed website (say it’s a replica of the LeMoyne website) which may then cause malware to be downloaded onto the user’s computer. What mechanism that we discussed in lecture could allow the user to check that the LeMoyne site is not being spoofed?

6. Suppose you enroll in a service that authenticates you using a biometric – your left thumbprint. Subsequently you learn that the service has been hacked and among other things the template database for their biometric authentication system was stolen. Should you be worried about this? Discuss.

7. The Internet Protocol (IP) provides (circle one from each line)

 Reliable Unreliable

 Connection-oriented Connectionless

delivery of packets

8. The Transmission Control Protocol, layered on top of IP, provides:

 Reliable Unreliable

 Connection-oriented Connectionless

delivery of data streams.

9. An essential part of every packet is the destination IP address, which routers use to determine which way to forward the packet. There is also a source IP address, which is supposed to tell where the packet originated. The host computer that generates the packet is responsible for filling in both of these fields. What is it about this design that makes attribution difficult?

10. Kernighan writes about lossless compression on pp. 155-157. Suppose you want to email a confidential report to a colleague. Keeping in mind that compression is only possible because of regularities in the input data, which of the two sequences of operations would you expect to yield a shorter output when applied to the text of?

A. Encrypt the report, compress the encrypted file, and email it.

B. Compress the report, encrypt the compressed file, and email it.