Homework Assignment 5

1. The SilentBanker man-in-the-browser attack depends on malicious code that is integrated into the browser. These browser helpers are essentially unlimited in what they can do. Suggest a design by which such helpers are more rigorously controlled. Does your approach limit the usefulness of such helpers?
2. A computer-to-computer authentications subject to the weakness of replay? Why or why not?
3. Suggest a technique by which a browser could detect and block clickjacking attacks.
4. Why does a web server need to know the address, browser type, and cookies for a requesting client?
5. The issue of cross-site scripting is not just that scripts execute, for they do in many sites. The issue is that the script is included in the URL communicated between sites, and therefore the user or a malicious process can rewrite the URL before it goes to its intended destination. Suggest a way by which scripts can be communicated more securely.
6. Explain why spam senders frequently change from one email address and one domain to another. Explain why changing the address does not prevent their victims from responding to their messages.
7. List factors that would cause you to be more or less convinced that a particular email message was authentic.
8. Explain how a forger can create an authentic-looking web site for a commercial establishment.
9. What attack is a financial institution seeking to counter by asking its customers to confirm that they see their expected security picture before entering sensitive data?
10. A CAPTCHA puzzle is one way to enforce that certain actions need to be carried out by a real person. However, CAPTCHAs are visual, depending not just on a person’s seeing the image but also on a person’s being able to recognize distorted letters and numbers. Suggest another method usable by those with limited vision.