Chapter 4 - The Web

**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 cryptographic nonce is important for confirming that a party is active and**

**fully participating in a protocol exchange. One reason attackers can succeed**

**with many web-page attacks is that it is relatively easy to craft authentic-looking**

**pages that spoof actual sites. Suggest a technique by which a user can be assured**

**that a page is both live and authentic from a particular site. That is, design a**

**mark, data interchange, or some other device that shows the authenticity of a**

**web page.**

**3. Part of the problem of malicious code, including programs that get in the**

**middle of legitimate exchanges, is that it is difficult for a user to know what a**

**piece of code really does. For example, if you voluntarily install a toolbar, you**

**expect it to speed your search or fulfill some other overt purpose; you do not**

**expect it to intercept your password. Outline an approach by which a piece of**

**code would assert its function and data items it needed to access. Would a**

**program such as a browser be able to enforce those access limits? Why or why**

**not?**

**4. 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.**

**5. Are computer-to-computer authentications subject to the weakness of replay?**

**Why or why not?**

**6. A real attack involved a network of air defense controllers’ computer screens.**

**In that attack, false images were fed to the screens making it appear that the**

**skies were empty when an actual air attack was underway. Sketch a block**

**diagram of inputs, processing, and outputs designers of such a system might**

**have used. Show in your diagram where there are single points of failure. In**

**some situations, we can prevent single-point failures by duplicating a**

**component that might fail. Would such a strategy work in this case? Why or**

**why not? Another counter to single failure points is to triangulate, to obtain**

**different kinds of data from two or more sources and use each data piece to**

**validate the others. Suggest how triangulation could have applied in this case.**

**7. List factors that would cause you to be more or less convinced that a**

**particular email message was authentic. Which of the more convincing factors**

**from your list would have been present in the example of the South Korean**

**diplomatic secrets?**

**8. State an example of how framing could be used to trick a victim.**

**9. Explain how a forger can create an authentic-looking web site for a**

**commercial establishment.**

**10. 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.**

**11. Why does a web server need to know the address, browser type, and cookies for a**

**requesting client?**

**12. Suggest a technique by which a browser could detect and block clickjacking**

**attacks.**

**13. 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.**

**14. What security principles are violated in the Greek cell phone interception**

**example?**

**15. Is the cost, processing time, or complexity of cryptography a good justification**

**for not using it? Why or why not?**

**16. What attack is a financial institution seeking to counter by asking its customers to**

**confirm that they see their expected security picture (a hot red sports car or a plate of**

**cookies) before entering sensitive data?**