CSci 5271: Introduction to Computer Security

Exercise Set 5 **due: Tuesday, December 12th, 2017**

Ground Rules. You may choose to complete these exercises in a group of up to three students. Each group should turn in **one** copy with the names of all group members on it. You may use any source you can find to help with this assignment but you **must** explicitly reference any source you use besides the lecture notes or textbook. An electronic (plain text or PDF) copy of your solution should be submitted on the course Moodle by 11:55pm on Tuesday, December 12th.

1. Cross-site scripting variations. (15 pts) There are a lot of different kinds of cross-site scripting vulnerabilities, but for space reasons we only covered one of them in hands-on assignment 2. This question covers another. Here's an excerpt from some Java code in the 2014 implementation of question 6 from hands-on assignment 2:

```
public class MACCookieServlet extends GroupServlet {
    @Override
    protected void doGet(HttpServletRequest req, HttpServletResponse resp)
                    throws ServletException, IOException {
        String username = req.getParameter("username");
        if (username == null)
             username = "";
        String digest_hex = ...;
        resp.setStatus(HttpServletResponse.SC_OK);
        resp.setContentType("text/html;charset=utf-8");
        resp.getWriter().print("User \"");
        resp.getWriter().print(username);
        resp.getWriter().print("\" is identified with the MAC ");
        resp.getWriter().print(digest_hex);
        resp.getWriter().println("\".");
    }
}
```

This code suffers a reflected XSS vulnerability: the `username` parameter is under the control of the untrusted user, and it is copied directly into the HTML output. So if it contained JavaScript, that code would run with the site's permissions. There's no similar problem with `digest_hex`, because the omitted code ensures that it contains only hexadecimal digits.

One way to fix this vulnerability would be to sanitize the contents of the `username` string using HTML entities; for instance, translating each "`<`" into "`<`". This is what we did for the newer version of the question (in PHP, we used `htmlspecialchars`). But suppose the programmer didn't know what library would contain a good implementation of that translation or was too lazy to implement it him or herself. What other simple change could you make to this code to avoid the cross-site-scripting danger?

2. Virus Virii. (20 pts) Sam has invented a brand-new virus detector, ViruSniff, and he claims it is "100% effective" — if executable file F is a virus, then ViruSniff(F) will output "`VIRUS!!!`".

(a) Does ViruSniff's claim conflict with the undecidability of the halting problem? Why or why not? (Hints: is there another term besides "effectiveness" that describes that statistic that Sam claims is 100%? Is there a simple program that can do exactly what Sam says ViruSniff can do?)

(b) Some hackers reverse engineer ViruSniff and post its algorithm online: it turns out that ViruSniff does processor emulation of the first 10000 instructions of an executable, and then applies a fancy signature matching algorithm (that no one seems to understand) to the sequence of instructions and memory changes to decide if the program is a virus or not. Explain how to change any program that runs for at least 10001 instructions, and does not trigger the `VIRUS!!!` alert, to propagate a virus such that the altered program will also fail to trigger the alert. What does your strategy say about Sam's claim?

(c) Given your knowledge of the attack from (b), how might you enhance ViruSniff to work against the new virus-writing strategy? Evaluate the potential effect of your change on the false-positive rate.

3. Denial of Service Denial. (20 pts) Sly is concerned about the possibility of DoS attacks against his web server program.

Sly has developed a new module for his web server that he claims will prevent DoS attacks by slowing them down. In Sly's module, every incoming HTTP request is put into a queue, with a timestamp and a "delayed" bit marked as false. When it is ready to serve a request, the web server takes the first request in the queue. If the "delayed" bit is false and there are no other requests from the same IP address in the queue, it serves the request immediately. If the "delayed" bit is false and there is at least one other request from the same IP address in the queue, the "delayed" bit is set to true and the request is re-inserted at the end of the queue. If the delayed bit is set to "true," then the request is served **if** the current time is at least 1 second greater than the request timestamp, and **otherwise** the request is sent to the end of the queue again. Sly's idea is that this will allow the site to deal with requests from legitimate users in preference to DoS attack requests.

Will Sly's scheme work to prevent a DoS attack from making his web server unusable by normal users? Give a detailed explanation.

4. Remailer doppelgangers. (15 pts) The "Sybil" attack is a general attack on security protocols that involve many computers or identities. The basic idea of the attack is to acquire as many identities as necessary to violate whatever assumptions the protocol makes about parties working together. Anonymity schemes could potentially make such attacks easier, although many of the most popular schemes make it fairly easy to prevent this (for example, it's easy to block Tor users from using your website at all, if you want). On the other hand, many anonymity schemes can themselves be vulnerable to Sybil attacks.

"Remailers" are anonymous email servers that essentially implement a cascade of mixes. The "basic" mix cascade work as follows: each node assembles a "batch" of messages to decrypt and jumble together. If the batching works by waiting until N messages are received, the $N-1$ attack can be applied: the adversary sends $N-1$ messages to the mix, whose destinations he knows. Then

when a sender sends the N^{th} message, its destination is obvious. One possible defense against this is for the mix to wait to mix a batch until it has seen messages from K different senders. Explain why the Sybil attack makes this defense ineffective.

5. Vote (often) by mail. (15 pts) The reason many security folks and cryptographers who work on voting object to "vote-by-mail" or widespread use of absentee ballots is the possibility of *coercion*: it is easy to "sell" your vote (where the price could be such things as lack of physical or mental harm, or continued employment, instead of cash) because the "buyer" can watch you fill out your ballot and mail it in. One commonly proposed countermeasure to this attack is to allow each voter to cast multiple ballots, with only the most recently submitted ballot being counted. Discuss some of the trade-offs involved with this defense. If you were a vote buyer in an election with this defense deployed, what might you do? Can you think of any other negative side-effects?

6. Cut and Choose. (15 pts) Many cryptographic voting protocols use something called a "zero-knowledge proof scheme" at some point in the protocol to convince one party that another party has followed the protocol. For example, one party (the "prover") may need to prove she knows a certain secret without revealing the secret to the other party (the "verifier").

A core idea in many of these protocols is the "cut and choose" technique in which the prover produces two options for the verifier: if (and only if) the prover can guess which option the verifier will choose, she can "cheat" the other player. As long as the verifier follows the proof protocol, he can only be fooled with probability $\frac{1}{2}$. Repeating this process many times can make it exponentially difficult for the prover to cheat.

We can also apply this principle to a paper-ballot system. Suppose that a state-level authority sends ballot boxes to each precinct in the state. These boxes are locked to prevent the precincts from tampering with them, e.g. by removing votes. However this leaves the possibility of a converse problem: how do the precinct authorities know that the locked boxes delivered to them are empty? A malicious state-level authority could "pre-stuff" the ballot boxes before they even get used. On the other hand, if we just gave the precincts keys, they could open the boxes to see that they were previously empty, but then they could stuff the boxes themselves.

Suppose the "acoustic side channel" of shaking the boxes to hear if anything rattles is out of bounds. Describe instead how to use a cut and choose protocol to prevent the state-level authority from "pre-stuffing" the ballot boxes. Specifically, if there are k precincts, your protocol should allow the state authority to cheat with probability at most 2^{-k}.