
Problem Set 5

This problem set is due *via email*, to `6857-hw@mit.edu` on *Wednesday, April 30* by the beginning of class.

You are to work on this problem set in groups of three or four people. Problems turned in by individuals, pairs, pentuples, etc. will not be accepted. Be sure that all group members can explain the solutions. See Handout 1 (*Course Information*) for our policy on collaboration. If you do not have a group, let us know.

Homework must be submitted electronically! Each problem answer must appear on a separate page. Mark the top of each page with your group member names, the course number (6.857), the problem set number and question, and the date. We have provided templates for L^AT_EX and Microsoft Word on the course website (see the *Resources* page).

Grading and Late Policy: Each problem is worth 3 points. Late homework will not be accepted without prior approval.

With the authors' permission, we will distribute our favorite solution to each problem as the "official" solution—this is your chance to become famous! If you do not wish for your homework to be used as an official solution, or if you wish that it only be used anonymously, please note this on your homework.

Problem 5-1. Botnets

Read the HoneyNet Project's whitepaper "Know Your Enemy: Tracking Botnets," which is linked from the class website.

Suppose you are the Chief Technical Officer of iKnowBot, Inc., which provides services to combat the scourge of botnets.

- (a) The whitepaper lists ten common uses of botnets. Describe a different potential application of botnets that would be useful (to their operators) today or possibly in the near future. Look especially for applications that have the potential to be profitable in some direct or indirect way.
- (b) Explain how, via a partnership with a DNS provider like `dyndns.org`, it would be possible to prevent any new infected hosts from joining many existing botnets.
- (c) Through some clever detective work, you discover the operator password for a large botnet. Explain how it would be technically possible to disinfect all zombie machines in the botnet and patch any of their security vulnerabilities that might otherwise lead to further infection. Then, discuss the ethical issues of taking such action. Refer to concrete ethical guidelines, such as those in the ACM Code of Ethics. (See <http://www.acm.org/constitution/code.html>.)

Problem 5-2. Zero Knowledge and Side-Channel Attacks

Consider a smart card whose public key is (n, e, y) , such that (n, e) is an RSA public-key and y is a random element in \mathbb{Z}_n^* . The private key of the smart card is x such that $y = x^e \pmod n$.

Whenever the smart card needs random numbers, it generates them using a pseudo random generator which starts with a random seed S stored on the card. The card also has its own battery. When the battery is disconnected, the current state of the smart card is lost, and it restarts from scratch. The values (n, e, x, S) are stored in non-volatile memory, which does not require battery power to be maintained.

- (a) Design a zero-knowledge protocol for the smart-card to prove to the server that it knows an x such that $y = x^e \pmod n$ such that the probability of success for a cheater (who does not know x) is less than $1/100$.
- (b) For your protocol, what happens when an attacker has temporary access to the smart card and can, for example, disconnect the battery?

- (c) It is the year 2100, and it has been discovered that factoring is easy and so is computing discrete logarithms. Luckily, another function f has been proven to be one-way (namely, impossible to efficiently invert but easy to compute in polynomial time). Design a zero-knowledge authentication protocol using this new function. (Hint: All you need to know here is that proving that a graph is 3-colorable is NP-complete).

Problem 5-3. XSS

Cookies are used to keep state information (http is stateless) and sometimes even used to automatically login (whenever you click “remember me”). In this problem you will try to exploit a vulnerability and use it to steal a cookie.

Go to <http://courses.csail.mit.edu/6.857/vulnerable.php> (please do not try this on other pages...). This is a very secure login page for you to access your pset 4 grades.

- (a) Give two reasons why this page is actually very insecure, and justify briefly. One of the security holes should help you later. (Do not use automated tools against the page.)
- (b) Now suppose that you are a user of the page located at <http://courses.csail.mit.edu/6.857/cookie.html>. This page stores some sensitive information about you in a cookie. For simplicity this page actually allows you to set the “data” field of your cookie to some value (just click on the “Set Cookie” button). The “Get Cookie!” link is there for you to check. You might need to enable cookies in your browser.
Set “data” to some value, and check that it has been correctly stored.
- (c) Leverage the security hole(s) in `vulnerable.php` to steal the cookie, passing it to some other site (say your web.mit page). Explain your method of attack. Why doesn’t the same origin policy apply to prevent the steal? Are there some fields in the cookies that you can set to stop this attack?
- (d) If a similar vulnerability was found on a web forum, how could you leverage that to steal cookies? Will you need to trick the user into say clicking a link that you crafted?

Problem 5-4. Work on Your Project!