Homework 5

This homework is due **Monday, December 6** at **5 p.m.** and counts for 4% of your course grade. Late submissions will be penalized by 10% plus an additional 10% every 12 hours until received. (The professor may grant individual extensions, but only under truly extraordinary circumstances.)

You are free to discuss the problems with other members of the class, but the answers you turn in must be your own work. Email your submission (as text or as a PDF attachment) to `eecs398@umich.edu` with "`HW5 Submission`" as the subject. You should receive a confirmation email within 15 minutes.

Solve the following three problems.

1. **Privacy and anonymity**

   A service lets users browse the Internet anonymously through a network of proxy servers. To avoid having their identities compromised, users must install special software that modifies the way their web browsers behave.

   In the absence of each change or action listed below, describe an attack that would reveal information about the user's identity. Assume that the user regularly visits web sites under adversarial control, but that the adversary is physically separated from the user.

   Changes that apply while the anonymous browsing service is enabled:

   (a) Disable the HTTP Referer header

   (b) Disable Java and Flash

   (c) Set the HTTP User-Agent header to a generic value

   (d) Resize browser windows to multiples of 35 pixels

   Actions that occur each time the user enables or disables the anonymous browsing service:

   (e) Close all open sites

   (f) Clear the history list

   (g) Clear the cookie store

   (h) Clear the browser cache

2. **Secure programming.** StackGuard is a mechanism for defending C programs against stack-based buffer overflows. It detects memory corruption using a *canary*, a known value stored in each function's stack frame immediately before the return address. Before a function returns, it verifies that its canary value hasn't changed; if it has, the program halts with a security error.

   (a) In some implementations, the canary value is a 64-bit integer that is randomly generated each time the program run. Why does this prevent the basic buffer-overflow attack discussed in lecture?

   (b) What are the security drawbacks to choosing the canary value at compile time instead of at run time? Why do some implementations use 0 for the canary anyway?

   (c) No matter how the canary is chosen, StackGuard cannot protect against all buffer overflow vulnerabilities. Describe two kinds of bugs that can corrupt the stack and allow the adversary to take control, even with StackGuard in place.

3. **Ethics and law.** Consider the following scenario: A worm is infecting systems by exploiting a bug in a popular server program. It is spreading rapidly, and systems where it is deleted quickly become reinfected. A security researcher decides to launch a counterattack in the form of a defensive worm. Whenever a break-in attempt comes from a remote host, the defensive worm detects it, heads off the break-in, and exploits the same bug to spread to the attacking host. On that host, it deletes the original worm. It then waits until that system is attacked, and the cycle repeats.

   (a) Many people would claim that launching a counterattack in this scenario is ethically unacceptable. Give at least three arguments that support this view.

   (b) Are there circumstances or conditions under which a counterattack would be ethically justified? Explain your reasoning.

   In 1988, a graduate student accidentally unleashed one of the first Internet worms. It deleted no files but caused widespread service interruptions. Cleaning it up and implementing defenses were costly. The student was convicted of violating the Computer Fraud and Abuse Act. Despite demands that he be sent to prison for the maximum time possible (to make an example of him), the judge sentenced him to pay a fine and perform community service. Today that student is a professor at MIT.

   (c) What factors do you think caused the judge to hand down this sentence? Do you believe the outcome was fair?

   (d) Would you expect a different outcome if a similar case happened today? Suppose you were the judge; what information would you take into account in making your decision?

□