Problem Set 6: Security

due Thursday, 8 December 2005, by 5:30 P.M. ET

The World of Devious Hackers. (25 points each.)

The following questions are designed to allow you an opportunity to synthesize material from Lectures 8 and 9 with that from previous lectures. It is without hesitation that we admit that these questions are meant to challenge you. However, rest assured that for none of these questions is there a single, correct answer; there are many intelligent answers possible for each.

What we expect from you, then, is exactly the latter—intelligent (daresay clever) solutions backed up by sound arguments and qualified with critiques. Bear in mind that a solution to a technical problem need not be technical itself. For instance, trashing is a perfectly reasonable (albeit unpleasant) mechanism for discovering someone's password.

For each question, do not limit your proposed solutions to one; three or more are expected. Be sure to justify the appropriateness and feasibility of each. Moreover, critique your own proposals and suggest (potential) flaws therein. In short, the teaching staff should be hard-pressed to find fault with your ideas; if there exists some weakness in one of your proposals, point it out before we get the chance!

These questions are deliberately open-ended and, to some extent, vague. If your response depends on some technical details that we haven't covered, then simply state your assumptions.

Your responses will be graded on the basis of their ingenuity, feasibility, and quality of support; **each should be more than a paragraph but no more than one page in length**.

Without further ado, **please answer four of the following six questions**. If you attempt to answer more than four questions, we will only grade your first four responses.

1. Suppose that you are shopping for widgets at an e-commerce site. Suppose also that you already have an account with the site and that all of your personal information (name, shipping and billing addresses, credit card numbers, and username and password) are stored in its database.

   You pick your merchandise, login with your username and password, select a credit card, and click "Submit" to confirm your order. Naturally, the information exchange between your home computer and the company's server occurs over the network. Naturally, there is a devious hacker sitting elsewhere on the network and trying to steal your credit card number.

   Describe several security vulnerabilities that an e-commerce site and its customers may encounter with such a scenario. (Do *not* assume that the e-commerce website is using the industry's best practices to secure their service.) Mention a possible preventive technique for each of the vulnerabilities you propose. You may (but need not) incorporate one or more of the following terms into your answer (consider them hints): client, server, browser, cookie, session, ISP, IP address, router, port, packet, packet filtering, keylogger, username, password, dictionary attack, database, encryption, denial of service, phishing, identity theft. You are encouraged to use the Internet to research your answers.

2. In the field of computer security, hackers and security professionals often use the same tools to fight each other, much like criminals and police use the same weapons.

   A packet sniffer is a tool that lets you filter TCP/IP packets on the network based on a set of properties you set. For example, you might only be interested in packets coming from a particular IP address (or set of addresses), or a particular destination address, or certain content, and so forth.

   i. Hypothesize how a hacker might use such a tool. What information could he or she collect? What are some of the difficulties he or she might encounter?

   ii. Hypothesize how a network administrator or security professional might use this tool to defend a computer (or a network segment) against hackers. What workarounds might the hackers apply to some of these defense systems?

3. Suppose that some hacker wishes to access the Internet on her laptop by way of Harvard's network. However, she hasn't a Harvard ID number and, therefore, cannot register her Ethernet card's MAC address. Accordingly, she cannot simply plug her computer into the network or wander near an access point and obtain an IP address via DHCP, since her Ethernet card isn't authorized for a DHCP lease.

   How might this hacker access the Internet on her laptop by way of Harvard's network without having a Harvard ID number?

4. Suppose that, for some reason, some hacker has a bone to pick with the world and wishes to interfere with the operation of or damage as many computers on the Internet as possible.

   How might this hacker accomplish her goal? In other words, invent (but do not implement) a virus or worm, explaining its payload and mode of propagation.

5. Suppose that some hacker wishes to send a fellow hacker a private email via the Internet but doesn't want to rely on existing ciphers.

   How might this hacker encrypt his email in such a way that it'd be fairly difficult for authorities to decrypt it? (In other words, invent for this hacker a new cipher.)

6. Suppose that a hacker gets caught (for committing devious hacking crimes) and appears in court. Where should the prosecutors look to find evidence of this hacker's devious crimes? (Do not limit your answers to the hard drive, or even to the hacker's computer for that matter). What specialized tools will the court likely use? How do those tools work?

Etymology. (0 points.)

7. Where does the word "hacker" come from, anyway?

Extra Credit. (5 points.)

8. 19923108241787117701 is the product of what two 10-decimal-digit prime numbers?