Chapter 2: Knock, Knock. Who’s There?

Students relate well to this chapter because they are familiar with passwords and can identify the weakness of guessed or disclosed passwords. The material is relatively easy, and biometric authentication devices appeal to students with a technology bent.

Instructional Suggestions

As computer security specialists, we like to think our subject and our needs are paramount: No system should be allowed unless it has strong authentication. That position, however, can be at odds with usability. Taken to the extreme, every user would need a distinct authenticator for each system, and there would be no relationship between authenticator (that is, no user could have the same password—or even a similar one—for two systems). Clearly that position would be unpopular with users, and when users find a restriction too harsh, they tend to try to override or undermine it. Students should learn the security rationale for strong authentication, but they should also learn how to judge which systems require strong authentication and which can accept weaker forms, or perhaps even none at all.

This chapter is a good point at which to begin discussion of ethics, because students can relate to the potential harm of a purloined email account, even without being a candidate for public office. It is also a good time to emphasize the difference between ethics and the law, as investigators were lucky to identify and arrest Kernell, and to secure a conviction.

Chapter Exercises

1. How do many computer applications thwart password-guessing attacks?
   Many programs employ a password lockout by which they refuse to accept new password entry attempts after a small number (typically three to five) successive password failures.

2. List advantages and disadvantages of assigned passwords, that is, an application program assigns an initial password to each user and, at an appropriate time, assigns a new password. The user has no role in choice of passwords or frequency of change.
   Advantages: passwords can be chosen from a large character set, of a given length, and changed with a certain regularity. Disadvantages: users have trouble remembering a long, meaningless string of characters, and consequently they dislike using assigned passwords.

3. List several applications for which a weak but easy-to-use password may be adequate protection.
   Depends on the threat. If the goal is to discourage a not-very-dedicated attacker, any password, no matter how weak, will do. A fair analogy is to the lock on a bedroom or bathroom door in a private home. Many such locks can be opened with a pin or screwdriver; the purpose of such locks is to say “I want privacy” but allow an override for emergency access.

4. For authentication based on something you are, both false negatives and false positives are problems. Discuss whether one of these is more important than
the other by citing situations in which one is more important and justifying that those kinds of situations are more prevalent.

False negatives deny legitimate access, so for a system in which availability is critical, a low false negative rate would be more important than a low false positive rate.

5. Construct an experiment to estimate the speed at which a particular computer can process an authentication password. From that estimate, determine how long it would take to test common password candidate lists, such as a list of 100 or 1000 popular passwords, the same list enhanced with orthographic substitutions (3 for e, zero for O, one for l, 2 for z, and so forth), and a word list from a common online dictionary. There is no single right answer to this question. The point of the question is to perform the analysis to determine the number of possibilities and the rate at which those possibilities can be checked.

Experimental

6. Conventional rules for password use include not writing down a password. Is this always necessary? That is, can you cite a situation in which writing down a password is only a minor vulnerability?

Writing down passwords is a vulnerability only if the written form can be readily found. In a setting with strong physical security, in which the threat from malicious insiders is low, written passwords are not seriously harmful. For example, a family computer in a private home may be of low risk if the users keep a shared list of passwords of shared, common sites, for example, news media or travel sites.

7. Discuss the algebra of authentication: Assume a situation with two-factor authentication and call the factors A and B. Considering the four cases in which each is either strong or weak, what conclusion can you draw about the result: weak A + weak B = ?, weak A + strong B = ?, etc. Does order matter, for example, is weak A + strong B = strong A + weak B? Does it matter if the two factors are of the same type, for example, two things you know? What happens if you add a third factor C? This question does not have a single right answer. You should base your discussion on analysis of examples.

It is up to the students to present results based on analysis, but students may find more countermeasure examples than simple algebraic relationships. No such algebra has yet emerged in the research community.

8. List four questions about yourself whose answers you would easily remember but an imposter would be unlikely to guess or find elsewhere. Exchange your list with another classmate and see if either of you can determine the answers to any of the other's questions.

Example questions: shoe size, last three digits of a previous phone number, favorite food, earliest childhood memory, kind of objects collected (e.g., coins, play programs).

9. You forget your password to a web site, so you click the box saying “forgot my password” to have a password sent to you by email. Sometimes the site tells you what your password was; other times the site sends you a new password. What are the security ramifications of these two approaches? Is one more secure than the other? Why would a site use one instead of the other?
If the site sends you your actual password, the password was stored in the system, where it could be found by an attacker or a malicious insider. Some sites store only a scrambled (encrypted) version of each password; when a user enters a password, the site applies the scrambling algorithm and compares the scrambled result with what is stored. In this way, assuming the scrambling cannot be reversed, no attacker can extract a user’s password from the system.

10. Defeating authentication follows the method–opportunity–motive paradigm described in Chapter 1. Discuss how these three factors apply to an attack on authentication.

Authentication is the step before access is granted to some sensitive resource. Thus, the attractive resource provides motive for wanting to defeat authentication. Method entails skills and knowhow: Passwords are of some finite length from a finite alphabet, so in theory all passwords can be enumerated (although the process takes a long time). For technology, used with biometrics and tokens, design specifications and usage manuals are often widely available, so the attacker can obtain details with which to attack. Finally, opportunity translates into time and physical access, which may be the controlling factors in an authentication attack.

11. Strong authentication can also risk availability. A simple example is that forgetting your password denies you access to that which required a password. Sometimes the stakes are high, for example, if a network administrator is the only one who knows the password to (or holds the only token for access to) a network device needed to block an ongoing attack. Even network administrators get sick, have accidents, are unreachable, or lose things. This situation is known as a single point of failure because the ability to access depends on one critical link: the administrator. How can a company prevent such a single point of failure?

   (1) Maintain a help desk, available 24x7 (which many companies have to support computer operation), and empower the help desk administrators to allow access to an individual user who can pass certain validity test or questions. (2) Pair each employee with a small number of people (but more than one) who can authorize emergency access. (3) For the specific case of the network administrator or any other single critical person, identify backup people who know the necessary access authenticators. (4) Record the authentications in a book or file kept securely. (Note that the “do not write it down” rule for passwords applies only in situations in which physical security of the written list is an issue. In a network monitoring center, for example, physical security will necessarily be high any way, and all persons in the monitoring center will be trusted to use the written password list responsibly.)

12. Remembering multiple passwords is difficult. Suggest a scheme by which a person can create easy-to-derive but hard-to-guess passwords for many different cases.

   A person can define a personal password algorithm, involving a few easy-to-perform steps on a character string related to the destination to which access is sought. Assume the destination is a web site. The algorithm might be: (1) take the first five letters of the site name and make them all lower case, (2) move the first letter to the third position, (3) change the (current) first letter to the letter one later in the alphabet, changing Z to A, (4) make the fourth letter uppercase, (5) change the last
Additional Exercises

1. List three reasons people might be reluctant to use biometrics for authentication.
   (1) Fear of physical harm (for example, looking into a lighted shaft for a retina scan),
   (2) Fear of physical contact (because of hygiene) for fingerprint or hand geometry readers, (3) Fear of false negative (for example, a cut or bandage on a finger needed for fingerprint recognition)

2. A dictionary attack can be augmented to try orthographic substitutions, such as 2 for z and @ for a. Assume a common dictionary has 100,000 words and (to make calculations easy), all letters are lower case and the 26 letters are evenly distributed (that is, “a” occurs exactly 1/26 of the time as does “z”). How many extra substitute word possibilities are there, allowing @ for a? (That is, the attack would try the word “bay” and also “b@y”.) If there are ten such orthographic substitutions (2 for z, @ for a, 1 for l, 6 for b, $ for s, etc.), how many word possibilities would an attacker need to try?

   Substituting @ for a adds 1/26 * 100,000 words, which is approximately 4,000 more. Ten such substitutions adds approximately 40,000 words (ignoring the fact that some of these “words” will have two substitutions, both z and a, for example, so that three new possibilities need to be tried: substitute for z, substitute for a, and substitute for both). The point of this question is to show that the substitutions increase the attackers work by 40% which, although not insignificant, is not infeasible on a computer.

3. If a user is prohibited from using any of the most recent $n$ passwords, why should the system still protect those passwords from viewing, just as strongly as it protects the current password?

   Users who must periodically change may use passwords consisting of a string and a number, where the number is changed each time the password must be changed. Thus, if an attacker obtains two prior passwords, the pattern may be obvious, which discloses the current password.

4. Discuss the security impact of a biometric device that sends simply “yes” or “no” to the computer to show the user passed or failed authentication, versus one that sends a full representation of the biometric credential to be evaluated on the computer. For example, a user might insert a coded card (with his or her biometric pattern secretly encoded) into a reader and then place a finger over a print reader. The reader can then inform the computer that the user did or did not match the pattern described on the coded card.

   Moving the decision to the reader allows an attacker to substitute a phony or modified reader that always says “yes” for the attacker. Furthermore, the computer system has no knowledge of gradual changes, for example, if a person’s appearance gradually changes as hair gets gray.

5. When police investigators perform DNA analysis are they doing identification or authentication?

Chapter 2: Knock, Knock. Who’s There?
Typically, and in the best situation, police are using DNA for authentication: They already have a suspect with high probability of involvement, and they want to authenticate that the person was at the scene where the DNA was collected.

   (1) People underestimate the threat of impersonation, (2) they want to choose a password that is easy to remember, and (3) they are more accustomed to remerging words instead of complex character strings.

7. Describe a social engineering attack that could be used to obtain a user’s password.
   Write the user a message saying the system is undergoing an upgrade, and the user will need to send (you) the user’s current username and password.

8. Explain the tension between frequency of password change and security.
   More frequent change limits the risk of someone’s obtaining a password, but frequent changes are inconvenient for users.

9. Explain what it means to say that a biometric device can be a single point of failure.
   A single point of failure is one item that, if it fails, denies access to an entire system. Any single authentication device is a potential single point of failure. For this reason, critical systems typically have two or more authentication readers, and two or more redundant computers processing authentication data from a replicated copy of the authentication database.

10. Must identities be unique? Must authentication data be unique? Explain your answer.
    Identities must be unique; authentication data can be non-unique, although it should be impossible for anyone to detect which authentication data items match.