Analyzing Computer Security: A Threat–Vulnerability–Countermeasure Approach

Instructor’s Manual

Charles P. Pfleeger
Shari Lawrence Pfleeger

September 2011

Analyzing Computer Security: A Threat–Vulnerability–Countermeasure Approach

Instructor's Manual

This manual is intended to help you as an instructor who has adopted *Analyzing Computer Security: A Threat–Vulnerability–Countermeasure Approach* for use in classes. It provides suggestions to help plan, prepare for, and conduct courses based on this book.

Building a Course

Analyzing Computer Security is intended for a one- or two-semester college course on computer security. As you are well aware from your first look at this book, it does not use a traditional, taxonomic progression of material; that is, it does not necessary start with the simplest concept and build progressively through to the most complex. There is, therefore, no "networks" chapter nor any single place in which we address security issues with programs. Instead, we have chosen an organization that we think will appeal to students while at the same time helping them develop the creative problem-spotting skills they need to truly understand computer security. Our approach is based on case studies, one or more per chapter, that lay a groundwork for the concepts we develop in that chapter. A helpful outcome of this structure is that the book is not tied to a rigid front-to-back progression. You can largely pick and choose topics and deal with them in almost any order. Of course, the topics do have dependencies; for example, you cannot present advanced uses of encryption without first having laid the basic foundations of cryptography. But we have worked to reduce these dependencies when we could.

Because of the topic-based book design, you can structure your course in any order you find comfortable. Front-to-back order is conventional and easy for both you and your students. But while planning your course, if you decide you want to omit certain topics, you can do so. Furthermore, everyone has certain favorite topics. You may decide you want to cover a later topic early in the course, perhaps because you know students are interested in it, or a recent news story has made that topic especially relevant, or you have particular insight or expertise in that area. You will likely find that you can shuffle the order of topics to cover with little difficulty.

Each chapter begins with what we call a chapter spotlight, a listing of the several topics addressed in the chapter. To build your course, we suggest you look through the spotlights and choose chapters in an order so that the spotlight topics suit your preferences. To further help you navigate the book, each chapter has a high-level table of contents that points to the major sections of the chapter.

Support for Instructors

This manual contains suggested solutions to exercises from the book. These answers are intended to guide you if you assign these exercises as homework or classroom discussion projects.

Naturally, creative students may come up with answers different from the ones we suggest here. Few of these exercises have a single “right” answer. Instead, their purpose is to challenge students to analyze a situation from a threat–vulnerability–countermeasure approach and present the steps of their reasoning. In this solutions manual we suggest some possibilities, but you will want to encourage your students’ imagination by gently nudging them toward acceptable answers. And remember that your students may come up with acceptable answers different from the ideas we present here. We tend to present only outlines of answers, such as phrases that suggest a line of reasoning; you and your students will amplify these outlines into complete thoughts.

In this solutions manual we have also added more exercises that you may use for discussion or homework, to help students learn the material. We have also included any suggestions for how to approach teaching the content of each chapter.

Interludes

We also include three unnumbered chapters that we call “interludes.” Each presents a current, real-life situation with computer security implications. These chapters are intended as extended student exercises to give students a chance to apply the analytical framework of threat–vulnerability–countermeasure creatively. You may want to use them in general class discussion, assign them to students to work on individually or in small groups, set them as competing team exercises, or invite students to delve into them for term papers or class presentations.

In this manual we offer some suggestions of probing questions you can use to stimulate students. Keep in mind that broad topics such as these have many possible threats and vulnerabilities, so the students should come up with numerous problems and potential approaches.

Afterword

This book ends with an Afterword, which is not so much a summary chapter as it is a means for looking forward. This book covers numerous specific attacks and vulnerabilities, with countermeasures tailored to each. However, the Afterword takes a broader perspective: What could improve cybersecurity in general, not in response to one specific threat?

Table of Contents

Chapter 1: Security Blanket or Security Theater?

This chapter is intended to introduce the student to the entire field of computer and information security. It defines important terms and concepts, such as threat, vulnerability, countermeasure, method, opportunity, motive, attack, harm, confidentiality, integrity, and availability. The student must understand these terms well, because they are fundamental to understanding everything else in this book. Therefore, these exercises are important for determining whether a student is ready to move on to the more specific chapters of the rest of the book.

Instructional Suggestions

Because this chapter introduces the student to many fundamental concepts, it is important to present them slowly and carefully. You may want to present a topic, such as method–opportunity–motive, and then challenge your students to cite examples of those elements from everyday experience or recent incidents. Fortunately, the news media are replete with examples in the area of computer security.

Chapter Exercises

1. List at least three kinds of harm a company could experience from electronic espionage or unauthorized viewing of company confidential materials.

Loss of business or competitive advantage, public embarrassment (leading to loss of business), legal action for failing to maintain secrecy of protected data (such as healthcare data, employee private data, personal financial data).

2. List at least three kinds of harm a student could experience from electronic espionage or unauthorized viewing of personal materials.

Public humiliation, loss of friends' confidence, legal action for failing to maintain secrecy of protected data.

3. Describe a situation in which complete denial of service to a user (that is, the user gets no response from the computer) is a serious problem to that user. Describe a situation in which 10% denial of service (that is, the response from the computer is 10 percent slower than normal) is a serious problem to a user.

Complete denial of service: any critical computing task, such as computer-assisted education, real-time accounting, or word processing for a student preparing a paper. Loss of 10 percent service: Computer-assisted medicine (surgery or drug dosing), streaming audio or video, or competitive online merchandising.

4. Consider the web site of an organization many people would support, for example, an environmental group or a charity. List at least three classes of people who might attack that web site. What are their motives? Consider the web site of a controversial organization, for example, a group of extreme ideology. List at least three classes of people who might attack that web site. What are their motives? Can you build a list of three classes that would attack both types of sites?

Charity: opponents of the cause, rivals, undirected (random) attackers. Controversial: same.

5. Do you think attempting to break in to (that, is obtain access to or use of) a computing system is ethical? Why or why not? Do you think that act should be illegal? Why or why not? Base your answer on harm: Who is harmed, to what degree, and does benefit to the person breaking in override the harm?

First point: Ethics is not the same as law. Something can be unethical (for example, cheating on an exam) but not illegal. Breaking in harms the victim through loss of confidentiality, inappropriate modification, denial or disruption of service, or even just a sense of violation. Thus, even if nothing is "taken," it is hard to argue that breaking in is not unethical. As to legality, there are laws against breaking into certain computing systems, even without causing apparent damage. (Passing a law does not make unwanted behavior disappear, however; there are laws against murder, but murders occur daily.) Having a law may improve the likelihood or ease of prosecution.

6. Consider electronic medical records. Which of confidentiality, integrity and availability do their users require? Cite examples of each of these properties you think are required. Describe at least two kinds of people or situations that could threaten each property you name.

All three. Confidentiality to preserve patients' privacy; integrity to ensure correct treatment, and availability to ensure necessary data are available for treatment. Confidentiality, integrity, and availability can be attacked by careless medical professionals, hackers, or unscrupulous people in the industry (for example, drug manufacturers or even medical software developers).

7. Distinguish among threat, threat agent, vulnerability, harm, and control.

A *threat* is a situation with the potential to cause harm. A *threat agent* is an actor— often a person but sometimes an object such as a vicious dog, an exposed electrical wire, or a windstorm—that allows a threat to be actualized. A *vulnerability* is a weakness, a hole through which harm takes place. *Harm* is unwanted behavior. A *control* prevents, detects, deters, or otherwise mitigates the harm of a threat exploiting a vulnerability.

8. Not all kinds of computer harm are illegal. List five examples of harm that is not illegal.

Fire, floods, and other kinds of physical disasters. Harm from inadvertent human errors (other than negligent behavior). Failed or degraded access because of inadequate capacity. Hardware failures. Access failure from forgetting a password.

9. Consider the example with which this chapter began: a series of seemingly unrelated events, including failure of the communications and electrical power networks. Describe a scenario in which these could all occur concurrently but not be related. Describe a way at least one could lead to another. Describe a way you could determine the root cause of each failure.

Concurrent but unrelated: accident of nature. One leading to another: electrical failure leads to communications failure (because communications providers, such as mobile phone networks, cannot operate without power). Root cause: difficult to discern. A precise timeline would show which event occurred before, especially immediately before, others, and error logs of the electrical and communications networks would show which conditions were detected when (although time of detection is not necessarily the same as time of occurrence.)

10. Continuing from question 9, suppose you were a malicious agent assigned to cause failure of the telecommunications and electric power systems. What steps could you take to make it difficult to determine who you are? What steps could you take to make it difficult to determine that the attack was malicious and not a natural accident? What steps could you take to make it seem as though the cause was someone else, for example, a particular foreign country?

Protecting identity: Obvious first step: work remotely. Second, employ local agents as necessary, but give each only partial information so no one person understands full plot. Third, work through several layers of intermediaries. Malicious or accident: Time activity to coincide with convenient natural disaster, for example, power disruption during a thunderstorm. Cause a "natural" disaster that diverts attention, for example, an truck accident that blocks traffic on a significant highway or an electrical power surge that affects a newspaper publisher or the emergency response telephone network. Redirecting the blame: Plant "seeds" that seem to come from the country, such as messages warning of an attack or stories leaked to friendly journalists.

11. Consider a restaurant with an online reservation system for patrons. What confidentiality, integrity, and availability threats might such a system experience? Hypothesize vulnerabilities in such a system that an attacker might try to exploit. What countermeasures could be applied against these threats?

Confidentiality: acts to determine identities of patrons or to learn how much business the restaurant is doing; integrity: acts to create fictitious reservations, delete reservations, or modify existing reservations. Availability: threats of hardware failure, software failure, unacceptable performance. Vulnerabilities: software faults, unstable hardware. Countermeasures: redundancy (paper backup).

12. Suppose a payroll system secretly leaks a list of names of employees earning more than a certain amount each pay period. Who would be harmed by such a vulnerability? How could such a vulnerability come about? What controls could be instituted to counter such a vulnerability? Suppose the leakage were not just names but also employees' identification numbers and full pay amounts. Would the people harmed or the degree of harm be different? Why or why not? If the employees are the ones suffering the greatest harm, who should be responsible for countering this vulnerability: the employee or the employer? Why?

Harm: Employees, company management. Names and personal details: People harmed, the same; degree of harm, greater (more sensitive details exposed). Responsibility: The employee has little control over a payroll system, and thus can do little to protect against its faults (other than, perhaps, giving a false name to the employer, which has other negative consequences).

13. A letter arrives in the surface mail apparently from your bank, but you are skeptical of its origin. What factors would make you skeptical? How could the bank help allay your skepticism in advance of sending the letter? What could the bank put in the letter itself that would reduce your skepticism? Would your answers be the same if the bank sends email instead of a surface mail letter?

Factors: quality of stationery and printing, appearance of envelope, wording of message (including spelling and grammar), also whether the content seems reasonable. Advance warning: a notice included with the regularly-sent monthly statement alerting customers that the bank would soon send a letter and outlining the topic. In the letter: some characteristic of the account, for example, part of the account number or reference to a recent transaction. Email: same answers.

14. Consider a program you could install on your own personal web page to display your city's current time and temperature. What threats could this program cause to you? To people who visit your web site? What controls could counter those threats?

This question is a precursor for Chapter 4 on malicious code. Any program can affect other programs in concurrent execution by modifying the other programs' code, intercepting data before or after processing by the other program, or denying access. The fact that a program has an apparently benign function—in this case time and temperature—is irrelevant.

15. Consider a program that allows people to order goods over the Internet. What threats could this program cause to users (purchasers)? What threats could this program cause to the merchant? Hypothesize three vulnerabilities that could allow these threats to be actualized.

Threats to users: confidentiality, exposure of personal data (credit card number); integrity, incorrect order (wrong item, wrong quantity, wrong price); availability: inability to order desired merchandise. Threats to merchant: exposure of customers' personal data, disclosure of customer list, disclosure of business condition (number of orders, for which products, at what prices); integrity: failure to record or retain order, recording incorrect order or modification of order, deletion of existing order; availability: customers' inability to access system (and to place orders). Vulnerabilities: software fault, power failure, inadequate capacity.

16. Suppose you are a talented sailor about to race your boat in a yachting competition. A possible threat to winning is cancellation of the event because of adverse weather conditions. List three other threats you might encounter as you try to win by posting the fastest finishing time. List three vulnerabilities those threats might exploit. List three countermeasures against those threats.

Threats: foul weather, mechanical failure of boat, inaccurate (or maliciously faulty) officials. Vulnerabilities: wind causes boat to capsize (countermeasure: mechanical stabilizers, waiting out bad weather in a safe position); rotting wood cause boat to leak (countermeasure: inspection before race); bribery (countermeasure: multiple official, independent skeptical observers).

17. Suppose you are a spy, and you need to pass secret materials to another spy, Agent Smart. However, you and Smart have never before met. You are aware that hostile forces are all around, any one of whom might try to impersonate Smart; if you approach someone and asked if she is Agent Smart, she might say she is even if she is not. Suggest a control for this threat—that is, a way you could be convinced the person to whom you are talking is really Agent Smart. Would your technique work if you assumed your telephone and mail were being monitored by the hostile agents? Suggest a way that would work even if your communications were monitored.

This problem is hard; establishing a basis for trust between two previously-unknown parties is a continuing difficulty for computer situations. This exercise leads to the shared secret problem for cryptographic key exchange (of Chapters 11 and 13). If you and Smart had a common friend (or co-worker) you could cite some common characteristic or event. You could also ask a mutual friend to supply each of you with an identifying phrase. The situation is even more difficult if you assume communications are monitored, because then asking a common friend for an introductory pass phrase could also be intercepted. The question asks about phone and postal communications being intercepted, or perhaps modified, but it does not preclude direct person-to-person communication. If you and Smart have a common friend or associate with whom you can feasibly arrange direct interaction, the friend can supply you each with an introductory phrase.

Additional Exercises

1. Theft usually results in some kind of harm. For example, if someone steals your car, you may suffer financial loss, inconvenience (loss of your means of transportation) and emotional upset (because of invasion of your personal property and space). List three kinds of harm a company might experience from theft of computer equipment.

Inability to do business, loss of confidentiality of sensitive data stored on the computers, financial loss of the value of the equipment itself.

2. Describe two examples of vulnerabilities in automobiles for which auto manufacturers have instituted controls. Tell why you think these controls are effective.

Exposure of occupants to rain, controlled by roof and body, an effective control. Ability of car to turn over in an accident, countered by weight and balance, only sometimes effective (as evidenced by automobile crashes).

3. Cite an example of data whose confidentiality has a short timeliness (say, a day or less). Describe an example of data whose confidentiality has a timeliness of more than a year.

Short: Name of an award winner, for example, the Nobel prizes. Long: individuals' personal data (for example, private identification numbers or birthdates), patentable laboratory research.

4. Do you currently use any computer security controls? If so, what? Against what threats are you trying to protect?

Anti-virus software: to protect against malicious code. Firewall: to protect against intrusion by outside programs or agents. Automatic code update programs, to protect against exploitation of newly-discovered faults in operating system or application code.

5. Consider a program that allows a surgeon in one city to assist with an operation in another city, either by manipulating the actual instruments remotely, or just by observing the operation and offering suggestions to the on-site surgical team. Who might want to attack such a program? What nature of attack might be attempted? How could such attacks be prevented?

Random attackers might go after this application or its computing platform without attention to the program being run. Furthermore, if the patient was an important political person, adversaries might want to interfere maliciously with the operation. The most likely attack, because it would probably be easiest, would be denying availability, probably by severing the communications link between the surgeon and the operating room. For such an attack, dual, redundant links would be a suitable countermeasure.

6. Cite an example in which a failure of one security property, for example confidentiality, leads to failure of another property, for example availability.

If a person's password becomes known (confidentiality), an attacker could use that password to impersonate the user, login, and change the password, thereby denying the user legitimate access.

7. A classroom teacher and her students share use of one computer. What problems does this present for the teacher? How can the teacher protect her computing against threats from the students?

Confidentiality and integrity of the teacher's materials are at risk; thus the teacher might decide not to keep sensitive data (such as students' grades) on the computer. Furthermore, actions of the students might harm the computer or its software, thereby denying other students and the teacher access. The teacher might keep a backup version of the operating system and critical applications on a separate medium (such as a DVD).

8. Cite three problems with using the legal system to protect computer systems.

Police forces and prosecutors are not always competent at investigating computer crime cases and trying criminals. Computer crimes can be committed remotely, sometimes from foreign countries, which limits the ability of one country's judicial system from prosecuting criminals. Legal penalties are not always strong enough to deter criminals.

9. Various cyber security exercises have been performed throughout the world. Describe the limitations of such analysis.

Each such exercise is exactly that: an exercise. It is limited by the seriousness of the participants and the creativity of the organizers. Few people are involved, so the effect on all relevant parties is limited.

10. Cite an example of each of the following: Computer as target of attack, method of attack, enabler of attack, enhancer of attack.

Target: web site modification. Method: malicious code (for example, virus, Trojan horse). Enabler: email (sending spam to hundreds of thousands of recipients with the click of one button). Enhancer: chat rooms by which hackers exchange attack knowledge.

11. Describe the concepts of method, opportunity, and motive as they apply to disabling a car by removing a key component.

First you must know which components are essential for starting or running the car. Then you must be able to recognize those components and know how to detach them. Finally, you must have the necessary tools to perform this act. These three pieces are aspects of method. For opportunity, you must have access to the car's engine, and you must be able to work on it in such a way that will not attract attention. For example, you might want to wear a mechanic's uniform and arrive in a truck bearing the sign of an auto repair shop. Motive is up to the attacker: why do you want to disable this car? Is it one step in a larger attack, in which you harm the victim and then prevent the victim from getting into the car and driving away?

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 letter to 1 if the letter is A–M or 3 if N–Z, and (6) end the string with a question mark. With this scheme, Microsoft would become jcmr3?

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 I, 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?