Homework 4: Secure System Design

See Webcourses and the syllabus for due dates.

What to turn in

For problems that require an English answer, please paste the text of your answer into the text box on webcourses.

General Directions

This homework is intended for individuals. You can do it in groups, but if you do so, be sure to follow the course grading policy, especially the cooperation section of the course grading policy, so that you properly certify that everyone in the group understands and participates in the solutions.
For each of the following problems, choose the one answer you believe is best, and give a brief justification for that.

Problems

1. (10 points) [SecurelyConstruct] You are thrilled to have a job on the security team for a major photo-sharing site. When you meet the rest of the team, you meet Alan, who has a Ph.D. in mathematics and did a dissertation about cryptography. Later, in a meeting, Alan proposes that all of the customer personally identifiable information (PII) should be encrypted using a new cryptographic algorithm that he has just invented. In the conversation about this idea, everyone turns to you: what do you say?

    A. "Sure, no one will know the algorithm, so the customer PII will be safer than if we continue to use the algorithm we're using now. This will raise the bar for attackers and give us more defense in depth for the customer PII."

    B. "No, this is a bad idea. Although Alan is brilliant, we don't really know if this algorithm that he's proposed is any good, and the stakes for our company are too high. After all many experts have proposed flawed algorithms before."

    C. "Why not use it? I think it's fine. After all it doesn't really matter how we encrypt the PII on our own servers, because with all the other defenses we have, there is no way an attacker will even get to our systems, let alone read the data. So it doesn't really matter and this is a good way to try out Alan's algorithm."

    D. "Well, that sounds okay, but let me look over the algorithm first, to see if I can find any weaknesses in it. After all, I had a great course in secure software development at UCF and so I'm familiar with this kind of thing. It will be a good way for me to get my feet wet."

    E. Either (A) or (C) is a fine answer in this situation.

2. (10 points) [SecurelyConstruct] A week later, at the same job, you talk to Bjorne, who tells you that he is canceling the code review for the new C++ library that he has written. His reasoning is that all the security problems in software are caused by writing the software in C, and that by using C++ he automatically avoids all those problems. Your boss, Emily, is passing by in the hallway and stops to listen to this conversation; both Emily and Bjorne look at you waiting to hear what you will say about Bjorne's proposal to cancel the code review. What do you say?

    A. "No, I think that's a bad idea, Bjorne. There are several possible vulnerabilities that can affect C++ code, and there are many design issues that are language independent. So we should still have that review."

B. "Sure, no problem, we can skip the review. I know you're a big fan of using the STL, Bjorne, and that avoids lots of problems with buffer overflow attacks, and so on. Besides, this will give us all more time to work on that thing we identified as the highest risk in our system during our risk analysis. It's always important to secure the weakest link first."

C. "Sure, Bjorne, there's no problem with canceling the code review. I agree that using C++ guarantees that there aren't any vulnerabilities in the code. And I know that you used that Boost library shared pointer class that I suggested."

D. "I don't know, Bjorne. Has the design already been reviewed for security problems?" Both Emily and Bjorne affirm that the design has been reviewed already. "Then OK, it should be fine. Using C++ will avoid all the detailed implementation problems you would have had if you had used C."

E. Both (B) and (D) are correct answers.

3. (10 points) [SecurelyConstruct] The following week you talk with an intern, Tommy, who is reviewing some Java code for the server, developed by another group at your company. Tommy asks: "I'm reviewing this Java code, and I since I'm new at this, I was wondering if there are any security implications that arise from the way that checked exceptions are handled in the code?" You ask what Tommy means, and the reply is: "Most of the time the code catches 'Exception' around anything that deals with the database or the file system. But we know that we have plenty of storage and that the hardware is reliable... So I was just wondering if that is okay?" What do you say?

   A. "Sure, back at UCF, where I studied, I always caught all exceptions like that in my homework solutions. Otherwise I could never get everything to compile. And in my security courses no one ever said anything about that being a problem. So I'm sure it's fine. But be sure to be careful about integer overflow problems in that Java code."

   B. "Sure, everybody does that. Java's a pain that way. Unless you put in those exception handlers, the code won't compile! The only thing I remember about Java and security from my class is to be careful with integer overflow problems, because Java uses signed integers always and never throws an exception when there is an overflow."

   C. "Yes it's okay. Those guys on the server team are all the best coders, so I'm sure that they wouldn't do anything if it wasn't safe."

   D. "No, it's always a problem sign if code catches all exceptions like that. Such code should be carefully looked at to see if any invariants are broken..." Tommy interrupts you with a quizzical look and asks: "Invariants?" You continue: "Right, an invariant is a condition that is supposed to be maintained by the code, like that transactions and problems are always logged properly."

   E. Both (A) and (B) are correct.

4. (10 points) [SecurelyConstruct] Later, another intern, Teri, wanders down the hall and stops at your office. She says she is working on the system's user interface in Javascript, and has been tasked with creating a new set of menus for one of the system's new features. She says: "I came up with this cool way of getting the menu items to call the right function, by constructing the name of the function from a string in the menu item. But then my boss said that some of the old time power users like to type things, and so I thought I could take their input and use that to construct the function also. The code uses the JavaScript eval function to call the function to do what the user wants, but I saw in the security guidelines that we aren't supposed to ever use JavaScript's eval function. Can you tell me why I can't do that? It would be really convenient for me and for those old time power users!" What do you say?

   A. "Well, I suppose those guidelines are there for a reason, but it seems unlikely that an old time user would try to attack the system. So it's probably okay. Would you like me to ask my boss for an exception to the guidelines?"

   B. "I can see how that would be more convenient, but you have to make sure to take out all fof the possibly bad characters from the user input. I'm pretty sure it suffices to just take out forward slashes (which start comments) and both kinds of quotation marks (that is, both

single and double quotes), to make sure that the user input is safe. If you do that, then I'll ask my boss for an exception to the guidelines."

C. "Look, the guidelines are right in this case. What you should do is write a function to parse the user's input, to make sure it's one of the choices you want, and then call one of the functions that needs to be called directly. If you use eval in JavaScript you open the code up for command injection attacks; that's the reason the guidelines prohibit the use of eval."

D. "Those guidelines are old; nobody uses that kind of attack anymore. Besides, you could write code that sanitizes the user's input by checking for a short list of characters that would enable an attack. If you do that, I'm sure we can get an exemption from the guidelines for you."

E. "Well, one way you could to that would be to have a list of the exact inputs that the users would be allowed to type. If you check for just those inputs in that 'allowed list', then it will be safe to use one of those strings to construct the call and use eval. If you do that we could get an exception for the code."

F. Both (B) and (D) are correct.

G. Both (C) and (E) are correct.

5. (10 points) [SecurelyConstruct] In trying to get ahead at the company, you come in to work on a weekend. One weekend, you are in your office, and a senior vice president, Mary, knocks on your door. She complains that she has to change her password, and that the system won't accept the new password she is trying to use, because it is a password that she used previously. She asks if you can change the password system or tell her what to do so she can get on with her work. What do you say?

   A. "Sorry, but you need to have a good password for the security of the system, especially because you are a privileged user. Why don't you get an app on your iPhone to generate a random password for you, and then just write it down on paper?"

   B. "Yes, ma'am, I can help you with that. It turns out that Joe put in a back door in the password changing routine, because he also doesn't like to change his password. If you try to use the passwords 'password' and then 'password1', the system will reject those, but after that the system will allow you to use an old password. Then you can get on with your work."

   C. "Sure, ma'am, what you should do is to call the system administrator, Joe, on the phone and have him reset your password for you to what you want. It's okay to tell him the password, as he already has root privileges for the system. Here's his phone number. . . "

   D. "Well, ma'am, what I recommend you do is something simple. Just add a number to the end of your password. For example, put the number one at the end of it, and then you just have to remember that it's your old password with a '1' at the end. I do that all the time and it works great."

6. (10 points) [SecurelyConstruct] One day Fred from the backend server performance task force comes to you and says: "Say, we noticed a problem with our app's start times. It seems to be slow due to calling Java's SecureRandom constructor, which is taking seconds, literally, to execute. If the load is heavy, then there aren't enough fresh VM's available that have gone through the start up, and our customers have to wait for SecureRandom to finish, but most of them just terminate the connection instead of waiting, so we're losing customers. Can't we just use java.util's Random class instead of SecureRandom in the code? That's *way* faster." What do you say?

   A. "Of course, you can use java.util's Random class. I mean, what's more important than keeping our customers?"

   B. "I see. Maybe what you should do is to use the Java Native Interface to call out to C code that calls the function random(). C is a lot faster than Java so I'm sure that will improve the performance a lot."

   C. "Well, if it's that slow, then sure. Just be sure to call java.util's Random some random number of times. What you do is to call Random, then get a random number between say 1 and 100,000, and then call Random that many times before returning the number. No attacker would be able to guess that algorithm, because I just made it up."

D. "Now we have to be very careful about this. If all of the places where SecureRandom is used are places where we need cryptographically secure random numbers, then we have to keep using it. Since our server runs on Linux, we could use the system's /dev/urandom as a seed for Java's SecureRandom constructor, and that will save on start up time. Alternatively, you could call the constructor in a concurrent thread to avoid waiting for it."

E. Both (A) and (B) are a correct answers.

7. (10 points) [SecurelyConstruct] Several months later, due to your success in the security team, you are transferred to the development team. When you first arrive you are given several bug reports to fix. Unfortunately, none of the bug reports has any of the kind of information you need to find and resolve the problems in the code. You complain about this to a co-worker, Dan, who says that this is because of the company's security guidelines, which prohibit giving debugging information such as stack backtraces and version numbers in error messages to customers. He asks you to go talk to Emily, your old boss in the security team, and ask her to change those guidelines, so that customer bug reports will have the information needed to properly fix problems in the code. What do you say?

   A. "You're right. Now that I'm in development, I see that the needs of the company as a whole should come first, before those old security guidelines. I'm sure Emily will be impressed with the importance of this problem, so I'll go talk to her about it. We certainly need that debugging information; there just isn't enough to go on in these bug reports!"

   B. "Now wait a minute. Maybe the old guidelines are right... We shouldn't give out information that attackers could use to help launch attacks against our software. And besides, our customers don't really want to see all those technical details when something goes wrong anyway!"

   C. "Sure, I'll talk to my old boss, no problem. Attackers can usually figure out this kind of information anyway, and one thing I learned in the security team is that 'there's no such thing as security through obscurity.' Why should the attackers have that kind of information but not our own development staff? What's more important: speeding up development or security?"

   D. "OK, sure, I'll talk to Emily about it. I've actually done a study, and I found that with detailed information about errors, we could speed up our development cycle by about 10 percent, and we could improve our customer satisfaction by about the same amount. I talked to Roger in marketing and he thinks that those numbers are a compelling case for changing those old security guidelines."

   E. Both (A) and (D) are correct answers.

8. (10 points) [SecurelyConstruct] While on the development team, your boss asks you to rewrite parts of the system to encrypt local network traffic on the server's LAN. He strongly suggests using the RC4 algorithm, which he implemented a long time ago. "Use RC4 because it's really fast, and we can't afford to waste too much time on a new implementation for this job." What do you say?

   A. "I understand, but wouldn't it be better to use some standard implementation of some more up to date algorithm? Even if we are only using this on our LAN, RC4 isn't secure nowadays. So we really should use some other tired-and-true algorithm."

   B. "Yes, I'll work on it right away. I agree that the choice of an encryption algorithm matters much in our own LAN. And if you implemented it, I'm sure it must be done right."

   C. "Sure I'll work on it right away. I remember reading about how to make RC4 more secure by throwing away some of the first bytes it produces."

   D. "Sure, I'll work on it right away. We'll just need to add an MD5 checksum onto the messages so that we don't have the possibility of bit tampering, although even that doesn't really matter much on our own LAN."

   E. All of (B), (C), and (D) are correct.

Points

This homework's total points: 80.