Kieren Ng

2/28/18

Homework 6

1

1. Using your own crypto algorithms
   1. You should use standard crypto algorithms because smart people figured them out, and you’ll probably do it wrong if you make it yourself tbh
2. Misuse of library
   1. Make sure to use standard libraries as they were meant to be used, because some people have assumed incorrectly
3. Poor key management
   1. Protection of keys is important, and so is choosing keys that are not weak
4. Randomness that isn’t random enough
   1. There’s a difference between statistically random and crypographically random, and you should use the latter.
5. Not allowing for changing algorithms in the future
   1. You need to design for changes in the future, for changes in security
6. Not considering the user
   1. Users may, accidently or not, do unintended things, and in design you should try to catch these things
7. Not authorizing after the first time
   1. After the initial auth, you should still check to make sure they can perform actions
8. Not paying attention to addons
   1. Adding new external components may create security problems
9. Not handling sensitive data properly
   1. Make sure data is handled properly by having data levels, etc.
10. Assuming trust
    1. Basically don’t assume trust, and never trust data from clients.

2

In some of my code I don’t really consider what other users might do besides me, and if they wanted to they could probably go in on my code and mess things up. I should probably sanitize my database inputs and stuff too.

16.1

According to the textbook, computers should be kept between 50 and 90 degrees F, and outside this range the computers might continue to operate but produce undesirable results. If too high, the computer cannot cool itself properly and components might be damaged, and thermal shock may occur if too low. High humidity is also a problem because possible corrosion, and too low may cause problems with static electricity (pg 512)

16.7

For brief power interruptions, a “uninterruptible power supply (UPS) should be employed for each piece of critical equipment (518)”, and for larger blackouts “critical equipment should be connected to an emergency power source, such as a generator”

16.8

“The general approach to human-caused physical threats is physical access control…These methods can be used in combination:

1. Physical contact with a resource is restricted by restricting access to the building in which the resource is housed.
2. Physical contact with a resource is restricted by putting the resource in a locked cabinet, safe, or room
3. A machine may be secured, to an object that is difficult to move
4. A security device controls the power switch
5. A movable resource is equipped with a tracking device to trigger if taken out.
6. A portable object is equipped with a tracking device to show location and be monitored.

(text pg 518)