

Homework 1

Solutions

Problem 1

1. Public key cryptography.
2. Hashing the files individually and providing it for download with the file.
3. Your boss can digitally sign the message using a hash and public key cryptography.
4. He can also use a certificate signed by an authority to further prove that it is him and not an imposter.

Problem 2

1. All parties commit to a hash algorithm $h(x)$ and a length for their nonces in bits b .
2. Each party i ($i = 0 \dots n - 1$) generates a b -bit random number r_i and sends a commitment $h(r_i)$ to all of the other participants.
3. In the reveal phase everyone sends out their r_i to all other participants, and they can verify that it matches the $h(r_i)$ received earlier.
4. The participants determine the value of the dice by calculating $r_0 \oplus r_1 \oplus r_2 \dots \oplus r_{n-1} \bmod k$.

\oplus is the best operation for this because it prevents the distribution of bit from having a high probability of going to ones or zeroes. To think by counterpoint if we ORed it then it is likely that at some point all of the bits would go to one eventually because at some point a participant would set each bit to one. If we AND it there is a higher probability of going to zero because we need both values to go to one to pass. A simpler way to think of this is that for the truth table of \oplus there are two ways it can go true and two it can go false. AND and OR (and NOR) both have three going one way and one going another. Basically this will assure that one participant can not unduly affect the distribution of bits (i.e. by setting them to all 0 or 1).

The power of two assures that the most significant bit is set to 1, which makes it so more bits must be used in the modulus. This is because $x \% 2^n = x \& 2^n - 1$ (i.e. all of the bits less than n are set to one).

Problem 3

1. Boot with EBCD and back up the SAM (password list). Then use EBCD to blank out the administrator password. Boot into Windows and it will have a blank password.
2. Then add it to your startup procedures There are two correct answers for this step:
SC:
You need to create a service by running “sc create (servicename) (absolute path of binary)”

Regedit:

- (a) Run regedit
 - (b) Add it under HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services
3. Load up the EventViewer and delete the records of your accesses (or clearing the log is an acceptable answer). Reboot with EBCD again and put the old password list back on the machine. This should effectively put the system back to where you found it, plus the rogue service.

Problem 4

1. Valid answers include installing a firewall to prevent the rest of the world from infecting you, deploying an intrusion detection system to trap when it looks like a worm is trying to spread and routine hard drive scans to prevent well-known worms from remaining resident on your systems.
2. You can attempt to make a signature with its jump-off code. You can also attempt to notice when it is making calls to an encryption/decryption installs on your system (make a list of what programs are allowed to access these libraries).
3. You can compare your system files against known OEM copies on the disk to make sure they have not been tampered with. Another approach is sniffing incoming and outgoing traffic to see if it looks like your computer is reporting information it should not. This is most useful when paired with you actually copying the disc.
4. There are several answers for this, but some include:
 - Having the program recompile itself to change how it appears (i.e. junk instructions)
 - Making your virus encrypt itself with varying keys
 - Having your virus look like something else that should always pass, but would be a pain to remove (think kernels).
 - Make it so your virus is concealed as hidden files that the standard user cannot access (i.e. a service that no one can see)
 - Really anything that inconveniences your target or makes it constantly appear different or invisible.

Problem 5

1. A high level plan of action should detail their main angle (what is the hole they are exploiting). It should include the timing of their attack and a vague plan of mapping or other preparation that needs to be provided/done.
2. The student can pick any of the three options, although some are better than others. They would have to take efforts to intercept a work order and show up early for it under the pest control. (Or could show up randomly as a building inspector, making reservations via email). The main thing is that they need to have their pretext lined up or create fake credentials to pose as a new employee. At any rate they need to justify their answers in terms of ease, access to the back room, etc.
3. In this part they should talk about either piggybacking from other employees, using

their cover to convince the staff to let them in, etc. But if the staff helps they still need to get rid of them long enough to plant the bug.

4. Defenses include having strict protocols for guests, inspecting their areas of work before and after and sweeping for bugs regularly. Many high security places also have escort protocols for temporary workers, so this is another option.