SCIT-EIS-UOW
CSCI262/CSCI862 Spring 2018

Laboratory Week Two: Set One

1. The first questions relate to passwords and entropy:

   (a) Is there any harm in revealing old passwords? Why or why not?

   (b) What is the entropy associated with a password chosen with uniform randomness from the set of length 8 strings with symbols taken from the lowercase alphabet {a,...,z}?

   (c) How much entropy is there associated with a typical ATM PIN?

   (d) Look at `http://www.datagenetics.com/blog/september32012/`

   (e) Is `fDtk53$e3W22eSDmvfFp-4F` a good password?

   (f) Without writing down your password, or the method of choosing your password, estimate the entropy associated with the password you use most.

   (g) How much confidence do you have in the method of choosing your password not being guessed?

   (h) How much confidence do you have in your password under the assumption the method of choosing your password was known by an attacker?

   (i) How does considering options that are not all equally likely impact on the entropy?

2. The next set of questions relate to hashing, partially in the context of password systems:

   (a) Does taking $H(M)$, for H a cryptographic hash function, provide confidentiality for M?

   (b) How might hashing be used in generating a password? How does it influence the entropy?

   (c) What is the advantage of using a hash function like `bcrypt` rather than a classical cryptographic hash function such as MD5 or SHA1?

   (d) Hashing ”produces a fingerprint” of a message. In what way does this misrepresent the relationship between hash and message, relative to the relationship between human fingerprint and human?

   (e) Look at `Trapped.gif`. What is the relevance to cryptographic hashing?

   (f) Read `Time-Oct3-2011.pdf`, not necessarily in the lab but at some point.

3. MD5 is a commonly used hash function. You should experiment with the code provided to make sure you understand the use of it, in C/C++ or Java, as appropriate. Test how long it takes to hash files of varying sizes. You can generate files of random data using the following instruction:

   ```
   cat /dev/urandom > /tmp/myname-rubbish.junk
   ```

   and typing Ctrl-C before the file gets too large. You can use the command `time` to time programs. If you create large junk files please remove them.

4. Use MD5 or SHA1 to build some rows of a rainbow table. Think about the requirements of a reduction function.

5. The utility `crypt` can be used to encrypt and decrypt files.

   (a) Perform appropriate experiments to measure the time required to `crypt` files of different sizes.

   (b) How does `crypt` encryption time compare with the `md5` hashing time?

   (c) What effect does the order of encrypting and zipping have? Why?