CPSC 329 W17 - Assignment 1

University of Calgary

Due Feb 8, 11:59 pm

Question 1 (6 pts)

Write one suggestion that you would like to see implemented in lectures/tutorials. A one-line answer is sufficient.

Question 2 (24 pts)

For each of the following categories:

Hacktivism , Cyber Warfare , Cyber Crime , Cyber Espionage

find one reported incident on the Internet, and write a summary report (at most 2 paragraphs per category) that includes the following:

- the attacker and the victim;
- a description of the attack in your own words;
- how the attack was detected/contained and what were the attack consequences;
- motivation of the attackers, and justification of why it falls into category that you have identified;
- link to the reported incident on a *credible* website;
- two evidences that the source is credible.

Although it is not easy to define what "*credible* " means, here are a couple of guidelines that you can apply to the chosen websites:

https://uknowit.uwgb.edu/page.php?id=30276

http://library.columbia.edu/locations/undergraduate/evaluating_web.html

Question 3 (25 pts)

Attack trees provide a graphical method of analyzing attacks. Consider a scenario where Jane, the CEO of a company, has stored the company's highly confidential investment plan on her laptop. Jane has a busy travel schedule, passing through airports and staying at hotels in different cities. In addition to doing work, she uses her laptop for email as well as browsing internet for per personal purposes. Draw an attack tree assuming the goal of the attacker is to gain access to the investment plan document. The tree should have at least 3 levels (including root).

Further reading on attack trees: B. Schneier, Attack Trees, Dr. Dobb's Journal, December 1999

https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Question 4 (8 pts)

Estimate the entropy of passwords of length 10 for the following scenarios:

a) passwords consist of lowercase characters only, e.g. **`helloworld`**;
b) passwords consist of lowercase and uppercase characters, e.g. **`HelloWorld`**;
c) passwords consist of lowercase and uppercase characters, and also digits, e.g. **`He110W0r1d`**
d) password consists of lowercase and uppercase characters, digits, and also 11 symbols

e.g. **He!!0W0r1d**

Only the following 11 symbols are used: ? ! @ # $ % * ( ) - + .

Question 5 (14 pts)

Estimate the entropy of 4 passwords (from previous question) by doing your own calculations, and also by using two tools, such as:

https://apps.cygnius.net/passtest/

http://rumkin.com/tools/password/passchk.php

Record your results in a table (4 pts):

Password	My estimate	Tool 1 estimate	Tool 2 estimate
helloworld			
HelloWorld			
He110W0r1d			
He!!0W0r1d			

Briefly describe your conclusions from this study and in particular comment on

a) the effect of password set size of on the entropy of passwords, (5pts)

b) the effectiveness of tools for password estimation (5 pts).

Question 6 (23 pts)

Consider a password system that uses password hashing for password verification. Each password consists of a string of 4 digits: $(a_3a_2a_1a_0)$, that is each a_i can be a digit $\{0,1,2,...,9\}$. So a_0 represents the rightmost digit, while a_3 is the leftmost digit in the password. The hash function is defined as:

$$h(a_3a_2a_1a_0) = (a_3{}^4 + a_2{}^3 + a_1{}^2 + a_0)\ mod\ 100$$

where "*mod 100*" is the remainder of integer division by 100.

1. How many different passwords are possible in this system? (1 pt)
2. Calculate *h(7819)*. (2 pt)
3. Find a password *x* such that *h(x) = h(7819)* but *x ≠ 7819*. (5 pts)
4. How many different passwords will have hash value equal to h(7819)? You may find it useful to write a program to get a precise answer. (5 pts)
5. Suppose an attacker wants to access John's account using an online attack. What is the probability the attacker will guess John's password if no hashing is involved, and when hashing is involved? (5 pts)
6. Suppose the password system is used with a 2 digit salt (s_1s_0) .The salt will be simply added to the hash value (integer addition) and (mod 100) operation will be used to make it into a 2 digit number. In other words, the hash function is now:

$$h(s_1s_0, a_3a_2a_1a_0) = (10s_1 + s_0 + a_3{}^4 + a_2{}^3 + a_1{}^2 + a_0)\ mod\ 100$$

For example, the hash for password 2745 given salt 39 is:

h(39,2745) = (39 + 2^4 + 7^3 + 4^2 + 5) mod 100 = 19.

Explain how adding salt affects success chance of an attacker who tries to guess the password. Explain your answer using the password 7819. (5 pts)

Submission details for this assignment:

1. Submit a single PDF file for the entire assignment. Use a text editor or word processor to write your assignment, then convert to PDF. This is to ensure that handwriting will not impede marking and evaluation of your work.
2. Write your name, student ID and tutorial section on the first line of the submitted assignment and use the following naming convention to name your file.

   `A1-<surname>-<student id>-<tutorial section>.pdf`
3. Submit your PDF file to D2L submission system. Submit on time. Late submissions will not be possible!

General information about all assignments:

1. **Due time:** All assignments are due at **23:59** on the due date listed on the assignment. Late assignments or components of assignments will not be accepted for marking without approval for an extension beforehand. What you have submitted in D2L as of the due date is what will be marked.
2. **Extensions** may be granted for reasonable cases, but only by the course instructor, and only with the receipt of the appropriate documentation (e.g., a doctor's note). Typical examples of reasonable cases for an extension include: illness or a death in the family. Cases where extensions will not be granted include situations that are typical of student life, such as having multiple due dates, work commitments, etc. Forgetting to hand in your assignment on time is not a valid reason for getting an extension.
3. After you submit your work to D2L, make sure that you check the content of your submission. It's your responsibility to do this, so make sure that your submit your assignment with enough time before it is due so that you can double-check your upload, and possibly re-upload the assignment.
4. All assignments should include contact information, including full name, student ID and tutorial section, at the very top of each file submitted.
5. Assignments must reflect **individual** work. Group work is **not allowed** in this class nor can you copy the work of others. For further information on plagiarism, cheating and other academic misconduct, check the information at this link: http://www.ucalgary.ca/pubs/calendar/current/k-5.html.
6. You can and should submit many times before the due date. D2L will simply overwrite previous submissions with newer ones. It's better to submit incomplete work for a chance of getting partial marks, than not to submit anything.
7. Only one file can be submitted per assignment. If you need to submit multiple files, you can put them into a single container. The container types supported will be ZIP and TAR. No other formats will be accepted.
8. Assignments will be marked by your TAs. If you have questions about assignment marking, contact your TA first. If you still have question after you have talked to your TA then you can contact your instructor.